Staatliche Identifizierung mit Fingerabdrücken und biometrischen Lichtbildern

Von der analogen Ermittlungsmethode zum globalen Personenkennzeichen

Stand: 08.03.2021

Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
0431 9719742
www.netzwerk-datenschutzexpertise.de

Inhalt

Am 11.12.2020 wurde das „Gesetz zur **Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen**“ im Bundesgesetzblatt veröffentlicht.[1] Das Gesetz soll die Verfügbarkeit und Zuverlässigkeit staatlicher Identifizierungsmittel durch eine Bereitstellung von authentischen Gesichtsbildern und Fingerabdrücken verbessern. Dem dient die Verhinderung des sog. „Morphing“, also des Verfälschens von Gesichtsbildern zum Zweck der Identitätstäuschung, und die Bereitstellung von automatisiert abgleichbaren Lichtbildern. Dem dient außerdem die verpflichtende Aufnahme der Fingerabdrücke der Zeigefinger in Personaldokumenten, insbesondere in Personalausweisen, so wie dies schon für Reisepässe vorgesehen ist. Die Regelung des § 5 Abs. 9 S. 1 PAuswG, die zum Fingerabdruck auf dem Ausweis verpflichtet, tritt am 02.08.2021 in Kraft.

Damit wird die EU-Verordnung v. 20.06.2019 zur Erhöhung der Sicherheit der **Personaldokumente für in der Europäischen Union** (EU) freizügigkeitsberechtigte Personen, die VO (EU) Nr. 2019/1157 (Perso-VO), umgesetzt, wo es in Art. 3 Abs. 5 S. 1 heißt: *Die Personalausweise werden mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweiseinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält.* Die Bürgerrechtsorganisation Digitalcourage hat am 30.06.2020 unter dem Schlagwort #PersoOhneFinger eine Informationskampagne gestartet und eine Petition initiiert, die sich gegen die Pflicht zur Speicherung von Fingerabdrücken wendet.[2] Schon zuvor hatten sich im März 2019 Digitalcourage, Privacy International (UK), Homo Digitalis (EL), ApTi (Ro) und Statewatch (UK) in einem offenen Brief gegen die Fingerabdruckpflicht ausgesprochen.[3]

Die Gesetzesnovellierung ist Anlass, den staatlichen Einsatz biometrischer Identifizierungsverfahren darzustellen und aus Datenschutzsicht zu hinterfragen. Fingerabdrücke und Gesichtsbilder sind die Vorreiter biometrischer Identifizierungsmerkmale, mit denen die analoge Welt mit der digitalen Welt verknüpfbar wird und Menschen aus dem Schutz der Anonymität in der Menge herausgezogen werden. Die Nutzung biometrischer Identifizierung durch staatliche Einrichtungen ist aus Datenschutzsicht problematisch. Sie eignet sich als Schlüssel für eine **hoheitliche Totalkontrolle** der Menschen und für die Einschränkung von deren individuellen Freiheitsrechten.

1 Einordnung der biometrische Identifizierung

Biometrische Identifizierung beschränkte sich lange Zeit darauf, bei Straftaten hinterlassene Spuren dem Täter oder beteiligten Personen zuzuordnen und durch optischen Vergleich die Identität eines Menschen zu belegen.[4] Mit der Methode automatisierter Mustererkennung eröffnen sich neue Möglichkeiten die Zuordnung von Menschen zu Sachverhalten und Berechtigungen. Sowohl im privaten wie im hoheitlichen Bereich wird die Biometrie eingesetzt, um sich der Identität einer Person zu vergewissern. Diese Entwicklung wird durch private Anwendungen vorangetrieben. Aus Sicht des Freiheitsschutzes ist aber der hoheitliche Einsatz besonders brisant, da hierüber eine einheitliche und **verbindliche zweckübergreifende Identifizierungs-Infrastruktur** entsteht, der sich der Einzelne nicht entziehen kann und mit der diesem Rechte und Pflichten verbindlich zugeordnet werden.

[1] BGBl. I 2020 S. 2744; Anti-Morphing und Fingerabdrücke künftig im Personalausweis, DANA 4/2020. 243 f.
[2] Ebelt, DANA 3/2020, 177 ff.; Digitalcourage, Stellungnahme 22.10.2020, Deutscher Bundestag Innenausschuss A-Drs. 19(4)613 B.
[3] https://digitalcourage.de/blog/2020/no-fingerprinting-for-id-cards.
[4] Zur geschichtlichen Entwicklung aufschlussreich Gröbner, Der Schein der Person, 2004.

Im Folgenden werden die beiden derzeit **gängigsten Methoden** biometrischer Identifizierung im Hinblick auf ihre Regulierung und ihren Einsatz untersucht: die Zuordnung von Fingerabdrücken und Gesichtsbildern. Die technische Entwicklung läuft darauf hinaus, dass sich weitere biometrische Merkmale etablieren werden. Die Ultima Ratio dürfte künftig die an Eindeutigkeit nicht zu überbietende genetische Identifizierung anhand der menschlichen DNA werden. Diese hat sich aber noch nicht als Standard etabliert; mit ihr sind zudem Fragestellungen verbunden, die teilweise weit über die der biometrischen Identifizierung generell hinausgehen.[5] Sie wird deshalb hier nur am Rande erwähnt.

1.1 Rechtliche Einordnung

Bei automatisiert auslesbaren Gesichtsbildern und Fingerabdrücken handelt es sich um „**biometrische Daten zur eindeutigen Identifizierung**“. Für diese Datenkategorie gab es bis 2016 keine übergreifenden Datenschutzregelungen. Dies änderte sich mit der europäischen Datenschutz-Grundverordnung (DSGVO)[6] und der parallel dazu verabschiedeten europäische Datenschutzrichtlinie für Polizei und Justiz (DSRl-JI)[7]. Dort werden diese Daten in Art. 4 Nr. 14 DSGVO und Art. 3 Nr. 13 DSRl-JI definiert als *mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten*.[8]

Diese Daten werden gemäß Art. 9 Abs. 1 DSGVO und Art. 10 DSRl-JI als eine „besondere Kategorie personenbezogener Daten“ wegen ihrer Sensitivität unter einen **besonderen Schutz** gestellt. Der Begriff „Biometrie“ leitet sich aus dem Griechischen (Bios = Leben, Metrein = Messen) ab und beschreibt die numerische Vermessung im Bereich der Biologie. Das Vermessen, das ursprünglich analog erfolgte, geschieht zunehmend mit digitalen Verfahren, teilweise vollautomatisiert und unter Einsatz teilweise komplexer Algorithmen der Mustererkennung.[9]

Biometrische Daten von Menschen sind wegen ihrer Sensitivität unter besonderen Schutz gestellt, wenn die gemessenen Merkmale eine besondere Individualität aufweisen. Nicht notwendig für die Einordnung als **sensitive Daten** ist, dass die Angaben weltweit eindeutig sind. Es genügt, dass eine genaue Identifizierung in einer mit abstrakten Merkmalen beschriebenen Gruppe einer großen unbestimmten Zahl von Personen möglich ist. Relevant ist, dass die über die natürliche Person erfassten Daten objektiv unverwechselbar sind. Wegen ihrer Verbindung mit dem menschlichen Körper sind sie nicht oder nur schwer zu verändern oder zu verfälschen. Dessen ungeachtet können sich z.B. auf Grund des Alters oder von Krankheiten Veränderungen ergeben, die eine Zuordnung erschweren oder gar unmöglich machen.

Der besondere Schutzbedarf der biometrischen Identifizierungsdaten liegt darin, dass diese mit modernen technischen Mitteln einfach zu erlangen und vom Betroffenen nicht oder nur schwer beeinflussbar sind. Die Merkmale ermöglichen es, eine Person **mit hoher Sicherheit zu identifizieren**

[5] Weichert in Kühling/Buchner, Art. 4 Nr. 13 Rn. 5, Art. 4 Nr. 14 Rn. 3.
[6] VO (EU) 2016/679 v. 27.04.2016, ABl. L 119/1.
[7] RL (EU) 2016/680 v. 27.04.2016, ABl. L 119/89.
[8] DSK, Positionspapier, S.18 ff.
[9] DSK, Positionspapier, S. 21 ff.; Golembiewski/Probst, S. 9.

und von dieser Person erfasste Daten systematisch aus unterschiedlichen Kontexten zusammenzuführen. Über diese Merkmale wird eine Schnittstelle zwischen realer und digitaler Welt hergestellt. Bemächtigt sich eine dritte Person dieser Daten, so kann sie sich als die Person mit den biometrischen Merkmalen ausgeben. Biometrische Identifizierungsdaten eignen sich also in besonderem Maße zum Identitätsdiebstahl. Im Darknet werden solche Daten für diese Zweck zum Kauf angeboten. Selbst gefälschte Reisedokumente mit validen biometrischen Daten werden dort gehandelt.[10] Mit Hilfe biometrischer Identifizierungsdaten erlangte Informationen sind schwer abstreitbar.[11]

Diese Daten eignen sich damit auch als nationale oder gar übernationale Kennzeichen, also als persönliche zweckübergreifende Zuordnungsmerkmale. Die biometrischen Merkmale können durch private Unternehmen, staatlich, in mehreren Staaten einheitlich, ja weltweit verwendet werden.[12] Erfolgt zweckübergreifend und umfassend eine staatliche Nutzung, so bedarf es hierfür gemäß Art. 87 S. 2 DSGVO „geeigneter Garantien für die Rechte und Freiheiten“ der Betroffenen. Dies gilt für **nationale Kennzeichen** generell, aber insbesondere, wenn als Kennzeichen biometrische Merkmale zum Einsatz kommen (Art. 9 Abs. 2 lit. g DSGVO, Art. 10 DSRl-JI). Die datenschutzrechtlich geforderten Garantien können in Beschränkungen bzgl. der Nutzungsberechtigten, der Zwecke und/oder der Art der Datenverarbeitung, in besonderen Betroffenenrechten, etwa in Bezug auf die Transparenz der Verarbeitung, sowie in technischen Vorkehrungen liegen.[13]

Es ist keine Voraussetzung für die Annahme eines **nationalen Kennzeichens** nach Art. 87 DSGVO, dass dieses in einem nationalen Register gespeichert ist. Vielmehr genügt eine Speicherung auf einem vom Betroffenen mitgeführten Dokument, wenn dieses Dokument bei einer Vielzahl staatlicher Aktivitäten vorzulegen ist und dabei jeweils ein Auslesen des Kennzeichens, z.B. des biometrischen Merkmals, erfolgt.

Tatsächlich werden automatisiert auslesbare Lichtbilder und Fingerabdrücke als **hoheitlich genutzte Identifikatoren** eingesetzt. Sie werden auf Ausweisdokumenten gespeichert und für unterschiedliche Zwecke durch unterschiedliche Stellen, insbesondere Behörden, genutzt. Diese Funktion wird verstärkt, wenn die biometrischen Daten zugleich in Datenbanken abgelegt sind, so dass Abgleiche zwischen den analog vorhandenen Daten, den Daten auf einem Ausweisdokument sowie den in der Datenbank hinterlegten Daten vorgenommen werden können.

Biometrische Rohdaten haben oft mit genetischen Daten gemein, dass ihnen Aussagekraft über gesundheitliche oder sonstige **körperliche oder seelische Zustände** zukommen kann, was dann zu einer noch höheren Sensitivität führt. Im Interesse der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sind solche zur Identifikation nicht nötigen Zusatzinformationen zu vermeiden.[14]

[10] Gefälschte Pässe – Biometrischer Datenhandel im Dark Web, www.br.de 02.08.2018.
[11] Zur Eingriffsintensität Bäumler u.a., S. 35 ff.
[12] Wedde in Däubler u.a., Art. 87 Rn. 8 ff.; Golembiewski/Probst, S. 28 f.; Weichert CR 1997, 369.
[13] Wedde in Däubler u.a., Art. 87 Rn. 15-18; Deutscher Bundestag Wissenschaftlicher Dienst, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 16.09.2020.
[14] Weichert in Kühling/Buchner, Art. 4 Nr. 14 Rn. 9; Bäumler u.a., S. 18 f.

1.2 Technik

Die datenschutzrechtliche Definition von sensitiven biometrischen Identifizierungsdaten nimmt Bezug auf „spezielle technische Verfahren“. Biometrische Daten sind sowohl die sog. **Rohdaten**, also die direkt mit einem Sensor erfassten Merkmale, wie auch sog. **Templates**, also aus den Rohdaten gewonnene und typisierte Merkmals-Vektoren, die auf der Grundlage eines mathematischen Modells standardisiert erfasst und regelmäßig zur Grundlage für digitale Zuordnungen genommen werden.[15]

Bei der Identifizierung wird unterschieden zwischen dem 1:1-Vergleich und der Identifikation durch Abgleich mit einem großen Datenbank (1:n-Vergleich). Insbesondere beim Datenbankabgleich (Matching) mit Templates, also einer codierten Darstellung, kann es zu **Zuordnungsfehlern** kommen. Dies kann eine fälschliche Nichtübereinstimmung (false NonMatch) oder eine fälschliche Übereinstimmung (false Match) sein. Aus unterschiedlichen Gründen lässt sich eine hundertprozentige Trefferquote in der Praxis kaum erreichen, weshalb regelmäßig mit Toleranzwerten gearbeitet wird (False Acceptance Rate – FAR, False Rejection Rate – FRR). Bei niedrigen Toleranzwerten eines Verfahrens verlieren biometrische Daten nicht ihre Eigenschaft als sensitive Daten.[16]

1.3 Funktionen in der Geschichte

Lange Zeit war in Deutschland die biometrische Identifizierung mit Hilfe technischer Mittel in Verwaltungsverfahren verpönt und wurde als eine Maßnahme angesehen, die der Strafverfolgung zwecks Zuordnung von Tatortspuren und zur **Überführung von Straftätern** vorbehalten ist.

Ein historischer Hintergrund für die deutsche Skepsis bei der Nutzung solcher Identifizierungsmethoden liegt in deren Verwendung im Nationalsozialismus wie auch in der DDR zur Kontrolle und Unterdrückung der Menschen. Dass eine Eignung der Methode für **Kontroll- und Unterdrückungszwecke** heute weiterhin – verstärkt – besteht, zeigt deren Einsatz in autoritären Staaten wie z.B. in China, wo die biometrische Identifizierung als ein zentraler Bestandteil eines totalitären staatlichen Kontrollapparats eingesetzt wird (s.u. 2).[17]

In der **Bundesrepublik Deutschland** wurde es für den identifizierenden Lichtbilderabgleich lange Zeit als ausreichend angesehen, dass ein Beamter das Gesichtsbild aus einem Ausweisdokument oder einer Datenbank mit dem Gesicht des sich Ausweisenden per Augenschein verglich. Von dieser Sichtweise ging man zunächst im Ausländerrecht ab. Die biometrischen Verfahren wurden dann aber bei immer mehr staatlichen Prozessen eingeführt und betreffen immer mehr Menschen und auch solche mit einer deutschen oder einer EU-Staatsangehörigkeit.

Der Prozess der Ausweitung des Einsatzes biometrischer Identifizierung hat verschiedene Gründe. Treibender Faktor ist zweifellos der technische Fortschritt, mit dem die **biometrisch-technische Identifizierung** immer einfacher und zuverlässiger wurde. Die Akzeptanz der Methode wurde zudem dadurch erhöht, dass sie auch von privaten Anbietern genutzt wird, im Arbeits- und insbesondere im

[15] Busch/Korte u.a. DuD 2011, 183; Gomez-Barrero DuD 2017, 448; Weichert in Kühling/Buchner, Art. 4 Nr. 14 Rn. 7; Golembiewski/Probst, S. 13 f.; Bäumler u.a., S. 7 ff,
[16] DSK, Positionspapier, S. 7; Weichert in Kühling/Buchner, Art. 4 Nr. 14 Rn. 8; Golembiewski/Probst, S. 16 ff.; Bäumler u.a., S. 29 ff.
[17] Überblick bei Hornung, S. 81 ff.

Konsumbereich.[18] Der Komfortgewinn durch die Nutzung des Fingerabdrucks oder eines Gesichtsscans bei der betrieblichen Eingangskontrolle, dem Freischalten eines Smartphones oder dem digitalen Bezahlen geht mit einem Gewöhnungseffekt einher, von dem auch der staatliche Einsatz „profitiert".

Hinzu kommen europäische und **weltweite Entwicklungen**: Der globale Personenverkehr ist auf eine eindeutige Identifizierung der mobilen Menschen angewiesen. So legte z.B. die Internationale Zivilluftfahrtorganisation (International Civil Aviation Organisation - ICAO) das Lichtbild, den Fingerabdruck und Irismerkmale auf maschinenlesbaren Reisedokumenten als einheitlichen Identifizierungsstandard fest.[19]

Die Notwendigkeit einer **europäischen Harmonisierung und Standardisierung** ergab sich mit der Entwicklung des europäischen Binnenmarkts und der EU-weiten Freizügigkeit für EU-Bürger, was einheitliche Identifizierungsstandards nahelegt. Sog. Drittausländer, also Nicht-EU-Bürger, bei denen man sich nicht zwingend auf die staatlich ausgestellten Identitätsdokumente verlassen kann, werden hierüber identifiziert. Fehlen Identitätsdokumente oder scheinen die gefälscht, so wie dies bei seit den 90er Jahren verstärkt einreisenden Migranten immer wieder der Fall ist[20], so sind biometrische Merkmale der einzige Weg für eine sichere Personenzuordnung und Identifizierung.

Werden biometrische Daten zu Zugangs- oder Zutrittszwecken gespeichert, so sind sie ein potenzielles Ziel für Hacker, die diese für **unberechtigte Authentifizierungen** nutzen wollen. Deren sichere Speicherung ist wesentlich, um Datenmissbrauch zu verhindern. Welche Risiken entstehen können zeigte sich, als 2019 bekannt wurde, dass die Biometriedatenbank „Biostar 2" (Gesichtsbilder und Fingerabdrücke) der südkoreanischen IT-Firma Suprema mit 27,8 Mio. Einträgen über das Internet ohne größeren Aufwand zugänglich war.[21] Auch staatliche Einrichtungen sind nicht davor gefeit, illegal oder auch nach eigenem Recht legal beschaffte biometrische Daten zur Identitätstäuschung zu verwenden, etwa im Rahmen der Tätigkeit von Geheimdiensten.

1.4 Gesichtsbilder

Für die rein **analoge Zuordnung** durch einen Menschen finden Gesichtsbilder seit Jahrzehnten selbstverständlichen Einsatz auf Ausweisen und Berechtigungsscheinen in privaten wie im öffentlichen Bereich. So ist es üblich, auf Betriebsausweisen ein Lichtbild aufzunehmen. Die elektronische Gesundheitskarte zum Nachweis der Berechtigung für Leistungen der gesetzlichen Krankenversicherung enthält ein Lichtbild (§ 291 Abs. 2 SGB V).[22] Entsprechendes gilt z.B. für die Fahrerlaubnis für Kraftfahrzeuge – den Führerschein (§ 2 Abs. 1 S. 1 StVG).

Die datenschutzrechtliche **Problematik der Verarbeitung von Gesichtsbildern**, die per Foto- oder Videografie erfasst werden, besteht darin, dass diese jederzeit ohne Beteiligung der Betroffenen aus der Ferne erstellt werden können und dass diese oft mit einer Zuordnungsmöglichkeit zu weiteren

[18] Golembiewski/Probst, S. 9 f.; Hornung, S. 84 f. m.w.N.; zur Rechtmäßigkeit ausführlich Conrad K&R 2020, 253 ff.
[19] Hornung, S. 94 f.
[20] Gemäß dem BMI lag der Anteil der Asylantragstellenden ab 18 Jahre ohne Identitätspapiere bei 51,8% Asylanträge ohne Ausweis, SZ 24.02.2021 6.
[21] Biometrische Zugangssicherungsdaten im Netz verfügbar, DANA 4/2019, 226.
[22] Zu weiteren Einsatzmöglichkeiten im Gesundheitsbereich Bäumler u.a., S. 44

Identifizierungsdaten (Name, Adresse, Erreichbarkeitsdaten, sonstige Angaben und Merkmale) im Internet verfügbar sind. Diese Eigenschaft haben Gesichtsbilder mit anderen biometrischen Identifizierungsmethoden gemein, bei denen aus der Ferne bzw. im öffentlichen Raum eine Zuordnung über Mikrofone oder Kameras möglich ist (Sprechererkennung, Gangzuordnung, s.u. 1.6). Diese Informationen werden nicht selten von Dritten mit einer eindeutigen Zuordnung öffentlich zugänglich gemacht, etwa im Internet. Oder die Betroffenen veröffentlichen diese Informationen selbst, ohne sich dessen bewusst zu sein, dass ihre Veröffentlichung ein Schlüssel dafür ist, sie auch in anderen Kontexten zu identifizieren.[23]

Gesichtsbilder finden sich mit weiteren identifizierenden Angaben und Attributen in großem Umfang allgemein zugänglich im Internet. So hat z.B. die in den USA ansässige Fa. Clearview AI aus dem Internet verfügbare Informationen zum Aufbau einer weltweiten Gesichtsbilddatenbank mit angeblich 3 Mrd. Bildern erfasst, die sowohl privaten wie auch öffentlichen Stellen zur Nutzung zur Verfügung gestellt wird.[24] Ein vergleichbares Angebot mit 900 Mio. biometrisch analysierten Gesichtern wird als öffentlich nutzbare Suchmaschine von dem polnischen Unternehmen PimEyes betrieben.[25] Facebook praktiziert seit 2010 automatisierte Gesichtserkennung. Diese wurde in Europa 2012 wegen Datenschutzbedenken gestoppt. In den USA muss Facebook 650 Mio. Dollar im Rahmen eines Sammelklageverfahrens wegen des Einsatzes der Technologie ohne Einwilligung der Betroffenen bezahlen.[26] Seit 2018 ermöglicht das Social-Media-Portal auch in Europa wieder eine Zuordnung von Bildern, wenn die Betroffenen „zustimmen“.[27]

Im zentralen **polizeilichen Informationssystem** in Deutschland (INPOL), das vom Bundeskriminalamt (BKA) geführt wird, sind über 5,8 Millionen Lichtbilder von ca. 3,6 Millionen Personen und ca. 3,5 Millionen Personenbeschreibungen aus erkennungsdienstlichen Behandlungen gespeichert (Stand März 2020). Der damit verfolgte Zweck ist die Strafverfolgung und die Gefahrenabwehr (s.u. 6.1). Durch den direkten Zugriff auf INPOL stehen diese Lichtbilder mitsamt Personenbeschreibungen allen deutschen Polizeidienststellen sofort und aktuell abrufbar zur Verfügung. Mit dem seit 2008 im BKA betriebenen Gesichtserkennungssystem (GES) können einzelne Lichtbilder mit dem Lichtbild-Gesamtbestand automatisiert abgeglichen werden. Das GES trifft eine Vorauswahl aus dem Gesamtbestand. Die Treffer werden anschließend von Lichtbildexperten und -sachverständigen ausgewertet. Im Jahr 2019 wurden bundesweit bei ca. 54.000 Recherchen im GES über 2.100 Personen identifiziert.[28]

Die bisherige zweidimensionale Gesichtserkennung wird nach Weiterentwicklung der Mustererkennungsmethoden durch **dreidimensionale Techniken** ergänzt. Mit einem solchen multi-

[23] Conrad K&R 2020, 255.
[24] Clearview betreibt weltweite Gesichtsdatenbank mit Abgleichsangebot, DANA 1/2020, 68 f.; Nutzung von Clearviews Gesichtsdatenbank durch Private und Behörden, DANA 2/2020, 125 f.; Clearview AIs biometrische Fotodatenban in der EU illegal, aber nur begrenzte Löschungsanordnung noyb.eu 28.01.2021.
[25] Laufer/Meineck, Eine polnische Firma schafft gerade unsere Anonymität ab, www.netzpolitik.org 10.07.2020; Reda DANA 3/2020, 175 f.; Polnische Gesichtsdatenbank beunruhigt deutsche Politiker, www.zeit.de 10.07.2020.
[26] Facebook zahlt 650 Millionen, SZ 02.03.2021, 19.
[27] Gesichtserkennung bei Facebook: Das sollten Nutzer wissen, www.vzbv.de 05.07.2019.
[28] Polizeiliche Gesichtserkennung nimmt massiv zu, DANA 3/2020, 186 f.; Bundeskriminalamt (BKA), https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html;jsessionid=E702B9AF17BA335BBDAB6BF326F5F6DF.live2301#doc19616bodyText4; zur Praxis in Bayern LKA plant verstärkte automatisierte Gesichtserkennung, DANA 1/2018, 39 f.

biometrischen System besteht die Möglichkeit, Identifizierungen auch aus partiellen Gesichtsbildaufnahmen mit minderer Bildqualität vorzunehmen.[29]

Gesichtsbilder sind die biometrischen Merkmale, die sich am besten für eine **Öffentlichkeitsfahndung** eignen. Sie können über Fahndungsplakate, über Print- und Digitalmedien und insbesondere auch über das Internet verbreitet werden und ermöglichen es allen Menschen, Zuordnungen vorzunehmen und an die fahndende Stelle zu melden.[30]

Die Qualität der biometrischen Gesichtserfassung wird erhöht, indem bestimmte **Erfassungsstandards** vorgegeben werden und die Erfassung sowie Übermittlung in einer vertrauenswürdigen Umgebung stattfindet. Insofern macht z.B. nun das Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis und ausländerrechtlichen Dokumentenwesen[31] eine Vielzahl von Vorgaben. Es soll damit u.a. das „Morphing“ verhindert werden, also die digitale Verfälschung von Gesichtsbildern, die dann von mehr als einer Person genutzt werden können und deren Verfälschung im automatisierten Verfahren nicht so leicht erkannt werden kann.

Die Verfügbarkeit staatlich qualitätsgesicherter, automatisiert lesbarer Lichtbilder aus Pässen und Personalausweisen sowie von privaten oder hoheitlichen **Zuordnungsdatenbanken** (z.B. GES des BKA) erhöht das Risiko, dass Menschen anhand ihres Gesichts automatisiert oder konventionell identifiziert werden, ohne dass die Betroffenen hiervon Kenntnis erlangen. Zugleich erhöht eine solche Verfügbarkeit auch das Risiko, über Tatortbilder in strafrechtliche Ermittlungsverfahren einbezogen zu werden. Diesem Risiko muss mit Hilfe von geeigneten Garantien entgegengewirkt werden (Art. 10 DSRl-JI).

Bisher spielten Gesichtsbildabgleiche außerhalb der Strafverfolgung in Deutschland eine untergeordnete Rolle. Einzig als geeignetes Mittel zur Überführung von Straßenverkehrsverstößen, insbesondere Rotlichtverstößen und Geschwindigkeitsüberschreitungen, wird die Methode durch den analogen Vergleich von Verkehrssünderfotos mit den Bildern in den kommunalen Pass- bzw. Ausweisregister auf Massenbasis genutzt, wenn der Kfz-Halter bestreitet, der regelverletzende Fahrer zu sein. Die Praxis in China zeigt, dass die Methode zur **Sanktionierung von jeder Art von Regelverstößen** geeignet ist, etwa zur Anprangerung von Rotlichtverstößen auf öffentlichen Displays (s.u. 2).

In den Jahren 2017/2018 wurde vom Bundesinnenministerium auf dem Bahnhof Berlin-Südkreuz ein Feldversuch zur **automatisierten Gesichtserkennung im öffentlichen Bereich** durchgeführt, der auf starke, auch rechtlich begründete öffentliche Kritik stieß.[32] In Deutschland forderte ein Bündnis von Bürgerrechtsorganisationen „Gesichtserkennung stoppen“ ein generelles Verbot automatisierter

[29] Multi-Biometrische Gesichtserkennung (GES-3D), Monroy, Gesichtserkennung: BKA will auf verbessertes System umstellen, netzpolitk.org 31.01.2018; Mehr Gesichtserkennung beim BKA, Bürgerrechte&Polizei/CILIP 115 (April 2018), S. 93; zum Datenschutz Körffer/Opel/Nouak, DuD 2013, 347 ff.
[30] Große Öffentlichkeitsfahndung nach G-20-Gewaltverdächtigen, DANA 1/2018, 41 ff.
[31] Fußnote 1.
[32] Dachwitz, Überwachungstest am Südkreuz: Geschönte Ergebnisse und vage Zukunftspläne, netzpolitik,org 16.10.2018.

Gesichtserkennung.[33] In anderen Staaten ist dagegen der automatisierte Gesichtsabgleich für viele Anwendungsfälle schon über das Teststadium hinaus alltägliche Praxis.

1.5 Fingerabdrücke

Die in **Personalausweisen und Reisepässen** gespeicherten Fingerabdrücke dienen der schnellen Identitätsfeststellung, wenn Zweifel an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person bestehen.[34] Bisher war die Aufnahme von Fingerabdrücken im Personalausweis freiwillig (§ 9 Abs. 3 S. 1-4 PAuswGaF), was nun mit dem § 3 Abs. 5 S. 1 PAuswG vom 02.08.2021 obligatorisch gemacht wurde. Im Reisepass ist die Aufnahme von zwei Fingerabdrücken nach § 4 Abs. 3 S. 1 PassG schon (basierend auf Art. 1 Abs. 2 ‚Pass-VO mit Gesetz vom 20.07.2007[35] obligatorisch.

Der Fingerabdruck ist die Wiedergabe der **Papillarlinien an der Fingerkuppe** eines Menschen. Diese Linien sind in Bezug auf jeden Menschen einzigartig. Es ist bisher nicht bekannt, dass identische Fingerabdrücke von zwei Menschen gefunden worden sind. Ein Vergleich erfolgt insbesondere über die Poren- und Linienstruktur (Minutien). Zur Extrahierung der Minutien werden diese mit Hilfe von speziellen Algorithmen in eine mathematische Form gebracht.[36]

Anders als Gesichtsbilder sind Fingerabdrücke nicht so leicht zu erlangen. Um auf einfache Weise qualitativ hochwertige Fingerabdrücke zu erhalten, bedarf es einer gewissen Kooperation des Betroffenen. Fingerabdrücke lassen sich aber mit etwas höherem Aufwand auch ohne Beteiligung der Betroffenen erheben, z.B. indem angefasste Objekte (Gläser, Türklinken) auf Fingerabdruckspuren hin ausgewertet werden.[37] Da solche **Spuren fast überall im täglichen Leben** eines Menschen anfallen, ist ein Erlangen von Fingerabdrücken und deren Zuordnung zu einer Person ohne deren Wissen möglich.

Die Erfassung von Fingerabdrücken hat eine lange Tradition in der polizeilichen Praxis zwecks Zuordnung von Tatortspuren.[38] Inzwischen wird das Erfassen und Abgleichen als Identifizierungsmethode auch von anderen Behörden und von privaten Stellen genutzt. Anders als die Gesichtserkennung, bei der die Zuordnungsqualität von der Bildperspektive, der Beleuchtung und dem Fehlen von störenden Einflüssen (Haare, Brille, Gesichtsbedeckung) abhängt, kann wegen der Einzigartigkeit der Fingerabdrücke allein mit einem Fingerabdruck in der Regel eine **sichere Zuordnung** vorgenommen werden.[39]

Das BKA führt seit 1951 eine zentrale Fingerabdrucksammlung. 1993 wurde dort ein **automatisiertes Fingerabdruck-Identifizierungs-System** (AFIS), eingeführt, das auf der Codierung der anatomischen Merkmale (Minutien) basiert (vgl. 5.3).[40] Die Einführung der „Livescan“-Technologie im Jahr 2004

[33] DANA 1/2020, 38 f.
[34] BT-Drs. 19/22133, S. 10.
[35] BGBl. I 2007 S. 1566.
[36] DSK, Positionspapier, S. 8 f.
[37] Chaos Computer Club konkretisiert Biometrie-Debatte an Schäubles Fingerabdruck, 29.03.2008, www.ccc.de/de/updates/2008/schaubles-finger.
[38] Weichert, CR 1997, 369 ff.
[39] Generell zur Zuordnungswahrscheinlichkeit Weichert in Kühling/Buchner, Art. 4 Nr. 14 Rn. 7 f.; Gundermann/Probet S. 1972 ff.; zur Technik Burger DANA 1/2004, 6.
[40] DSK, Positionspapier, S. 13; Weichert, DuD 1999, 167.

ermöglicht es, die Fingerabdrücke (ebenso wie die der Handflächen) digital aufzunehmen und im zentralen AFIS des BKA zu speichern. Im Rahmen des sog. Fast-ID-Verfahrens können seit 2006 digital aufgenommene Fingerabdrücke ohne Zeitverzug im AFIS recherchiert werden. So sind z.B. im polizeilichen Streifendienst, bei Großveranstaltungen (Fußballspiele, Konzerte etc.) und bei Grenzkontrollen rund um die Uhr innerhalb von wenigen Augenblicken zuverlässige, biometrisch basierte Personenidentifizierungen oder Zuordnungen möglich. Das BKA verarbeitet monatlich ca. 60.000 eingehende digitale Fingerabdruckblätter, die gespeichert, ausgewertet und qualitätsüberprüft werden. Dabei wurden 2019 monatlich rund 19.300 Identifizierungen durch Abgleich von Fingerabdrücken erzielt. Bei Fast-ID ist das Vorgangsaufkommen bisher ähnlich hoch: Hier führt ca. ein Drittel der Anfragen zu einem Treffer im Bestand. Zudem wurden im Jahr 2019 monatlich ca. 30.000 Tatortspuren recherchiert, die im AFIS gespeichert sind, was im Durchschnitt zu ca. 2.200 Treffern führte.[41]

1.6 Sonstige biometrische Identifizierungsverfahren

Biometrische Identifizierung mit Mitteln der automatisierten Mustererkennung beschränkt sich nicht auf das Gesicht und die Finger. Grundsätzlich eignen sich viele **physiologische und verhaltenstypische Merkmale** zu Identifizierungszwecken, soweit ihnen eine individuelle Eigenheit zukommt. Die Merkmalserfassung kann optisch, akustisch, mit sonstiger Sensorik, etwa mit chemischen und biotechnischen Verfahren, erfolgen. Beispiele sind die Iris- und die Retinaerkennung, der Abgleich von Handabdrücken, der Scan der Handvenen, die Stimmerkennung (Sprechererkennung),[42] die Zuordnung über den Geruch oder das Mikrobiom, also der bei einem Menschen festgestellten Mikroben.[43]. Inzwischen gibt es auch immer mehr Verfahren, mit denen über eine Verhaltensanalyse eine (relativ) sichere individuelle Zuordnung ermöglicht wird, etwa die Analyse der Unterschriftsdynamik, des Tastaturanschlags oder der Mausbewegung am Computer, des Gangs eines Menschen.[44] Auch genetische Daten aus biotechnischen Analysen, die juristisch als besondere Datenkategorie eigenständig einem besonderen Schutz unterliegen (Art. 4 Nr. 13 DSGVO, Art. 3 Nr. 12 DSRl-JI), eignen sich als biometrische Identifizierungsdaten.[45]

2 Staatliche biometrische Identifizierung anderswo

In **Europa** konzentriert sich die staatliche biometrische Identifizierung auf die Bereiche der Sicherheit, der Grenzkontrolle und des Ausländerwesens. Doch bestehen darüber hinausgehende Begehrlichkeiten. So wurde z.B. in Schweden ein Schulprojekt mit einem Bußgeld von ca. 18.000 € sanktioniert, bei dem mittels Gesichtserkennung die Anwesenheit der Schüler kontrolliert werden sollte.[46] In Italien machte man entsprechende Anwesenheitskontrollversuche bei Schülern mit Fingerabdrücken.[47] Rechtlich unbeanstandet blieb bisher offenbar das „Loi relative á la protection de l´identité“ in Frankreich, das nicht nur die Speicherung von Fingerabdrücken in Personalausweisen und

[41] BKA (Fn. 24).
[42] Tillenburg DuD 2011, 197 f.; DSK, Positionspapier, S. 8 ff.
[43] Mikroben identifizieren Personen und Umgebungen, DANA 2015, 188 f.
[44] Conrad K&R 2020, 254 f.¸ Golembiewski/Probst, S. 12 f.; Hornung, S. 76 f.
[45] Weichert in Däubler u.a., Art. 4 Rn. 131.
[46] Bußgeld gegen Schule wegen automatischer Gesichtserkennung, DANA 4/2019, 228.
[47] Schulische Anwesenheitsüberwachung per Fingerabdruck, DANA 3/2016, 145 f

Reisepässen vorsieht, sondern auch deren Speicherung in einem Zentralregister, auf das u.a. die Strafverfolgungsbehörden zugreifen können.[48]

In den **USA** ist automatisierte Gesichtserkennung weit verbreitet und wird schon von privaten Unternehmen für Sicherheitszwecke bei Großveranstaltungen eingesetzt.[49] Strafverfolgungsbehörden nutzen die Gesichtserkennungsdatenbank von Clearview AI (s.o. 1.4). Hiergegen regt sich Widerstand, der u.a. damit begründet wird, dass die Gesichtserkennung vorrangig mit Gesichtern weißer Männer trainiert wurde. Dies führt dazu, dass bei Frauen und nicht-weißen Personen eine sehr viel höhere Fehlerrate vorliegt, was zu einer Diskriminierung der Betroffenen führen kann. Die Kritik erfolgt aber nicht nur aus Gründen der Diskriminierung, sondern auch wegen der Überwachungseignung. Der Widerstand führte dazu, dass Gesichtserkennung in einigen Städten, u.a. San Francisco und Oakland, verboten ist. Amazon untersagte für ein Jahr der US-Polizei die Nutzung seiner Erkennungssoftware „AWS Recognition“ wegen der Fehlerrisiken. Microsoft erklärte, mit seinen Produkten Polizeibehörden nicht mehr zu unterstützen zu wollen.[50] Im Januar 2020 startete die US-Regierung mit einer zentralen Speicherung von DNA-Identifizierungsdaten von Flüchtlingen.[51]

In **Brasilien** wurden im Jahr 2019 erstmals Kameras mit Gesichtserkennung eingesetzt, um große Menschenmassen zu kontrollieren. Dies erfolgte z.B. während des Karnevals in Rio mit Hilfe des britischen Facewatch-Systems, wobei die Gesichtsdaten von 1.100 gesuchten Straftätern zum Abgleich hinterlegt wurden. Anwendung findet die Technik auch in Flughäfen. Zum Einsatz kommt dabei auch chinesische Software.[52]

In **Russland** wird in größeren Städten biometrische Gesichtserkennung umfangreich angewendet. 2017 waren in der Hauptstadt Moskau 170.000 Überwachungskameras im Einsatz, die mit der Gesichtserkennung der Fa. N-Tech.Lab ausgestattet wurden.[53]

In **Indien** wird im Rahmen des sog. Aadhar-Projektes die größte biometrische Datenbank der Welt aufgebaut. Dabei sollen alle 1,3 Mrd. Inder mit Iris-Scan und Fingerabdruck erfasst werden.[54]

Besonders weit entwickelt ist die biometrische Identifizierung in **China**. Im Wirtschaftsbereich ist Gesichtserkennung etabliert, etwa beim elektronischen Bezahlen über den Messenger-Dienst WeChat.[55] Gesichtserkennung wird genutzt, um Straßenverkehrsverstöße zuzuordnen und die Betroffenen umgehend öffentlich an den Pranger zu stellen. Selbst die Papiernutzung auf Toiletten kann dort per Gesichtsscanning kontrolliert werden.[56] Seit Dezember 2019 bekommt man in China nur noch einen Internet-Anschluss oder eine Mobilfunknummer, wenn zuvor zur Überprüfung der Identität

[48] Zentrale Fingerabdruckdatei beschlossen, DANA 2/2012, 88.
[49] Gesichtserkennungs-Abgleich bei Tylor-Swift-Konzert, DANA 1/2019, 47.
[50] Reda DANA 3/2020, 176; Graff, Gesichtsverlust, SZ 07.07.2020, 9; Gierlinger, Bits und Vorurteil, SZ 13./14.07.2020, 21.
[51] US-Regierung speichert DNA-Proben von Flüchtlingen, DANA 1/2020, 63 f.
[52] Gesichtserkennung im Karneval, DANA 2/2019, 106.
[53] Videoüberwachung in Moskau mit Gesichtserkennung, DANA 4/2017, 214.
[54] Kritik an Aadhar-Projekt, DANA 4/2017, 215; Supreme Court erkennt Grundrecht auf Privatsphäre an, DANA 3/2017, 172; Biometrische Bevölkerungserfassung fast abgeschlossen, DANA 3/2016, 150 f.; Volkszählung mit Iris-Scan und Fingerabdrücken, DANA 1/2011, 29 f.
[55] Bezahlen mit Gesichts-Biometrie bei WeChat, DANA 4/2019, 232 f.
[56] Gesichtsscanner kontrolliert Klopapiernutzung auf Toiletten, DANA 2/2017, 108 f.

das Gesicht gescannt wurde.[57] November 2019 wurde das National Information Security Standardization Technical Committee gebildet, mit dem Standards für die Identifizierung, zunächst im Bereich der Gesichtserkennung, festgelegt werden. Die Standards sollen alle Bereiche erfassen, auch die regionale und die lokale Verwaltung, die Industrie und die Wirtschaft.[58] Zur erleichterten Kontrolle und Unterdrückung der uigurischen Bevölkerung der westchinesischen Provinz Xinjiang wurde eine umfassende DNA-Bevölkerungsdatenbank etabliert.[59]

3 Internationale Kooperation: Interpol

Die Internationale kriminalpolizeiliche Organisation – Interpol – (englisch International Criminal Police Organization, ICPO) ist ein privatrechtlich organisierter Verein zur Stärkung der Zusammenarbeit nationaler Polizeibehörden. Sie wurde 1923 als Internationale kriminalpolizeiliche Kommission in Wien gegründet und hat seit langem ihren Sitz in Lyon/Frankreich. Derzeit hat Interpol 194 Mitgliedstaaten. Interpol betreibt **Datenbanken zur forensischen Identifizierung** mit Hilfe von Biometrie. Ziel ist der grenzüberschreitende globale Austausch zwecks Bekämpfung von internationalen Verbrechen, aber auch zwecks Identifizierung von Katastrophenopfern. Alle drei Jahre führt Interpol ein International Fingerprint and Face Symposium durch, das einen weltweiten Austausch über moderne biometrische Identifizierungsmethoden zum Ziel hat.

Die Identifizierung von Katstrophenopfern erfolgt seit 1984 über **Disaster Victim Identification** (DVI), wobei eine Kombination von Abgleichen zu Gesichtsbildern, sonstigen Körpereigenschaften (Tatoos, Implantate, Narben), Finger-, Hand- und Fußabdrücken, Gebissdokumentationen und Genproben genutzt wird. Das deutsche BKA hat hierfür ein unterstützendes DVI Germany Team im Einsatz.

Im Bereich der internationalen Kriminalitätsbekämpfung kommen bei Interpol Verfahren der automatisierten Gesichtserkennung, des Fingerabdruck- und des DNA-Abgleichs zum Einsatz. Das **Interpol Face Recognition System** (IFRIS) wurde 2016 eingeführt und hat mit einer Kombination von automatisierter Suche und analoger Verifizierung seitdem über 1.000 Personen identifiziert. Zum Einsatz kommt bei einigen Mitgliedstaaten zudem eine vollständig automatisierte Treffer-Rückmeldung.

Das von Interpol betriebene **Automatic Fingerprint Identification System** (AFIS) enthält mehr als 220.000 personalisierte Datensätze sowie mehr als 17.000 Tatortspuren. Die Speicherung und der Abgleich erfolgt auf der Grundlage des NIST-Standards (National Institute of Standards and Technology, Version 6.0 von 2020), mit dem JPG-Datensätze einheitlich konvertiert werden können. 2019 konnten so mehr als 1.600 Zuordnungen vorgenommen werden.

2002 wurde bei Interpol eine **DNA-Datenbank** eingerichtet, die mit Stand 2019 von 89 Mitgliedstaaten bestückt wird und 242.000 Datensätze enthält. Gespeichert sind ausschließlich die DNA-Marker in

[57] Handynummer künftig nur noch nach Gesichtsscan, DANA 4/2019, 231 f.
[58] Standardisierung bei der Gesichtserkennung, DANA 1/2020, 66 f.
[59] Xinjiang erstellt unter falschem Vorwand Bevölkerungs-DNA-Datenbank DANA 1/2018, 53.

Form eines alphanumerischen Codes; die dazu gehörenden Informationen werden von den Mitgliedsstaaten vorgehalten und auf Einzelanfrage hin übermittelt.[60]

4 Europäische Biometrie-Kooperationen

Folgende **Einrichtungen der EU** sammeln systematisch biometrische Daten für Identifizierungszwecke: Das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS), Eurodac sowie Europol. 2012 wurde EU-LISA gegründet als Agentur für das Betriebsmanagement der drei großen IT-Systeme für Sicherheit und Migrationskontrolle (SIS, VIS, Eurodac).[61] Für die Speicherung von eingescannten Fingerabdruckbildern verwenden alle in der EU eingesetzten Systeme das gleiche Format. Für die Fingerabdruck-Templates zur Erfassung der Minutien werden hingegen unterschiedliche Formate verwendet.

EU-LISA stellte in einem Bericht vom Juli 2020 sog. **künstliche Intelligenz** (KI) als eine der „vorrangig zu entwickelnden Technologien“ vor und betonte die Vorteile von KI bei der Migrationskontrolle, v.a. dank der Gesichtserkennungstechnologie. EU-LISA, aber auch die Grenzschutzagentur Frontex sind besonders aktiv bei der Erprobung dieser Technologien, wobei die Unterscheidung zwischen Erprobung und Anwendung nicht genau genommen wird.[62]

4.1 Europol

Europäisches Polizeiamt, kurz Europol, ist der Name der EU-Polizeibehörde mit Sitz in Den Haag. Sie soll die Arbeit der nationalen Polizeibehörden Europas im Bereich der grenzüberschreitenden organisierten Kriminalität koordinieren und den Informationsaustausch zwischen den nationalen Polizeibehörden fördern. Seit dem 01.01.2010 ist Europol, das zunächst auf der Grundlage eines völkerrechtlichen Vertrags gegründet wurde, eine Agentur der Europäischen Union. Aktuell gültige Rechtsgrundlage ist die Verordnung (EU) 2016/794 (Europol-VO).[63] Im Anhang II dieser Verordnung werden die personenbezogenen Daten aufgeführt, die gemäß Art. 18 Abs. 2 lit. a Europol-VO erhoben und abgeglichen werden dürfen. Dort sind unter B. lit. c v aufgeführt: *Informationen für die forensische Identifizierung wie Fingerabdrücke, (dem nicht codierenden Teil der DNA entnommene) DNA-Profile, Stimmprofil, Blutgruppe, Gebiss*.

Die Datenspeicherung erfolgt im Europol Informations System (EIS). 2018 waren bei Europol 8.000 Datensätze mit vollständigen **Zehnfingerabdrücken** gespeichert sowie 1.000 einzelne Fingerabdrücke aus Tatortspuren. Es wird Hardware von Hewlett-Packard verwendet mit dem personalisierten automatisierten biometrischen Identifizierungssystem (ABIS) von SopraSteria.[64]

[60] www.interpol.int/How-we-work/Forensics/; BT-Drs. 19/22897 v. 29.09.2020, 9.
[61] Töpfer, Bürgerrechte&Polizei/CILIP 109 (Januar 2016, 33 ff.
[62] Data et nouvelles technologies, la face cachée du controle des mobilités, www.migroup.org 20.01.2021.
[63] Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) v. 11.05.2016, ABl. EU v. 25.06.2016, L 135/53.
[64] Antwort Avramopoulos/EU-Kommission v. 20.06.2018, E-001595/2018.

Europol soll künftig (ebenso wie die europäische Grenzschutzbehörde Frontex[65]) einfacheren Zugang zu SIS, Eurodac und VIS erhalten als bisher zur Verfolgung und Prävention terroristischer und anderer schwerer Straftaten.[66]

4.2 Schengener Informationssystem

Das Schengener Informationssystem (SIS) wurde 1995 als Kompensations- und Sicherungsmaßnahme nach Abschaffung von Grenzkontrollen zwischen EG-Mitgliederstaaten eingerichtet. Es ist inzwischen die größte hoheitliche Datenbank in Europa und wird als Fahndungsdatenbank von Grenz-, Polizei-, Zollbehörden sowie auch von Geheimdiensten genutzt. Unter der Verantwortung der Europäischen Kommission wurde eine erweitere Version des SIS (SIS II) entwickelt, in dem seit 2013 (geplant war 2007) auch erstmals **biometrische Daten zu Fahndungszwecken** gespeichert werden. Derzeit sind an dem System 25 EU-Mitgliedstaaten (alle außer Irland und Zypern) sowie Island, Norwegen, Liechtenstein und die Schweiz beteiligt. Zum Stichtag 01.01.2020 waren 90 Mio. Datensätze (Personen und Gegenstände) gespeichert.

Die aktuell gültigen **Rechtsgrundlagen** sind für den ausländerrechtlichen Teil die Verordnung (EG) Nr. 1987/2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der Zweiten Generation (SIS II-VO)[67] sowie in Bezug auf die Sicherheitsbehörden der Beschluss 2007/533/JI (SIS-II-B).[68] In Art. 1 Abs 2 SIS-II-VO/SIS-II-B wird der Zweck von SIS II denkbar weit definiert als der Informationsaustausch, um *ein hohes Maß an Sicherheit in dem Raum der Freiheit, der Sicherheit und des Rechts der Europäischen Union, einschließlich der Wahrung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der Sicherheit im Hoheitsgebiet der Mitgliedstaaten, zu gewährleisten*. Eine Ausschreibungskategorie sind Einreise- und Aufenthaltsverweigerungen, wozu Lichtbilder und Fingerabdrücke ausgetauscht werden können (Art. 20 Abs. 2 lit. e, f SIS-II-VO/SIS-II-B). Insofern besteht eine enge Zweckbegrenzung auf die Identitätsbestätigung und (für Fingerabdrücke) die Identitätsfeststellung (Art. 21 Abs. 2, 3 SIS-II-VO, Art. 22 Abs. 2, 3 SIS-II-B). Ein weiterer Zweck besteht in polizeilichen Fahndungsausschreibungen (Art. 20 i.V.m. Art. 26, 32, 34, 36, 38 SIS-II-B: Auslieferungshaft, Vermisste, Durchführung eines Gerichtsverfahrens, Strafverfolgung, Gefahrenabwehr, verdeckte/gezielte Kontrolle). Einen direkten Zugriff auf die Daten haben Grenzkontrollbehörden, der Zoll, die Polizei, Justizbehörden sowie Stellen, die für die Visumerteilung sowie für die Erteilung von Aufenthaltstiteln zuständig sind (Art. 27 SIS-II-VO, Art. 40 SIS-II-B). Auf Daten zur Gefahrenabwehr und Strafverfolgung dürfen auch Europol und Eurojust zugreifen (Art. 41, 42 SIS-II-B). Die SIS-II-Daten können in nationalen Dateien gespeichert werden (Art. 32 SIS-III-VO, Art. 47 SIS-II-B). Erlaubt ist auch die Speicherung von Fingerabdrücken und Lichtbildern sowie sonstiger Identifizierungsdaten zur Missbrauchsverhinderung in Bezug Personen, deren Identität missbraucht werden könnte, wenn der Betroffene seine Genehmigung hierzu erteilt (Art. 36 SIS-II-VO/Art. 51 SIS-II-B).

[65] Zu Frontex Verordnung (EU) Nr. 1168/2011 v. 25.10.2011, ABl. EU L 304 v. 22.11.2011, Wagner/Monroy, Bürgerrechte&Polizei/CILIP 109 (Januar 2016), 45 ff.
[66] Busch, Biometrie: Vom Ende des «Identitätsbetrugs» in Europa, www.cilip.de 29.06.2017.
[67] VO (EG) Nr. 1987/2006 v. 20.12.2006, ABl. EU v. 28.12.2006, L 381/4.
[68] Beschluss 2007/533/JI v. 12.06.2007, ABl. EU v. 07.08.2007, L 205/63.

2018 lagen im SIS ca. 121.000 **Fingerabdruckdatensätze** vor, inzwischen sind es über 273.000. 2020 gab es zudem einen Bestand von ca. 63.500 Lichtbilder. Allein die deutschen Behörden konnten 2019 ca. 9.000 Treffer bei biometrischen Suchläufen vorweisen und damit das Vierfache des Vorjahres.[69] Die Hardware des automatisierten Fingerabdruck-Informationssystems stammt von Hewlett-Packard. Darauf laufen folgende Software-Komponenten: Safari (AFIS), Accenture (Middleware) Oracle (Datenbank) und Linux.[70]

Mit den Verordnungen (EU) 2018/1860, 2018/1861 und 2018/1862[71] erfolgt eine **Erweiterung** des Anwendungsbereichs von SIS II in Bezug auf für die Registrierung von Drittstaatsangehörigen sowie für Bescheinigungen zuständigen Behörden, Verkehrsbehörden oder Stellen, die für Schusswaffen zuständig sind. Angeschlossen wird zudem die europäische Grenzagentur Frontex. Die Zugriffsrechte schon berechtigter Stellen werden ausgeweitet. Zur Speicherung zugelassen werden Licht- und Gesichtsbilder sowie daktyloskopische Daten. Letztere bestehen aus *ein bis zehn flache Fingerabdrücken und ein bis zehn abgerollten Fingerabdrücken* oder *bei denen die Erfassung von Fingerabdrücken nicht möglich ist, aus bis zu zwei Handabdrücken*. Die nationale Umsetzung der SIS-Neufassung (SIS 3.0) sollte bis Ende 2021 abgeschlossen sein. Die Federführung für die Umsetzung in Deutschland liegt beim BKA, wobei es drei Teilprojekte (Fachlichkeiten) gibt: Polizei (BKA), Rückkehrentscheidungen (BAMF) und Technik (BKA).[72]

4.3 Eurodac

Mit dem europäischen daktyloskopischen System Eurodac werden **alle zehn Fingerabdrücke von Asylbewerbern und Geflüchteten** EU-weit sowie von Island, Liechtenstein, die Schweiz und Norwegen gespeichert und für Abgleichzwecke bereitgehalten. Das Eurodac-System wurde am 15.01.2003 zunächst in den Mitgliedstaaten der Europäischen Union in Betrieb genommen.[73] Rechtsgrundlage ist heute eine Verordnung der Europäischen Union von 2013, die in den teilnehmenden Mitgliedstaaten unmittelbar gilt (Eurodac-VO).[74] Diese Verordnung löst die ursprüngliche Verordnung von 2000 ab.[75] Um eine länderübergreifende Vergleichsmöglichkeit der Fingerabdrücke zu ermöglichen, werden die Fingerabdrücke in Eurodac nicht als Template, sondern als digitale Bilddaten abgelegt und verglichen.

Die beteiligten Staaten erfassen von den mindestens 14 Jahre (künftig 6 Jahre) alten Asylbewerbern nach Antragstellung oder von ausländischen Personen, die an der Außengrenze oder im grenznahen Raum angetroffen werden, deren jeweilige Fingerabdrücke und übermitteln diese in digitalisierter Form an eine zentrale nationale Stelle (Zentraleinheit), die über die technische Ausstattung zur Speicherung und zum Abgleich verfügt. Erfasst werden die „**Fingerabdruckdaten**“, die in Art. 2 Abs. 1

[69] Monroy, Bürgerrechte & Polizei/CILIP 121 (April 2020), 69.
[70] Antwort Avramopoulos/EU-Kommission v. 20.06.2018, E-001595/2018.
[71] VO (EU) 2018/1860, 2018/1861 und 2018/1862 v. 28.11.2018, ABl. EU v. 07.12.2018, L 312/1, L 312/14, L 312/56.
[72] Antwort der BReg. auf Kleine Anfrage Fraktion Die Linke, BT-Drs. 19.23614 v. 23.10.2020; Mehr deutsche Behörden erhalten Zugriff auf SIS, DANA 4/2020, 240.
[73] Golembiewski/Probst, S. 11 f.
[74] Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26.06.2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013, ABl. EU v. 29.06.2013, L 180/1; dazu Polizei erhält Zugriff auf Eurodac, DANA 1/2013, 25; Kuster/Tsianos, Bürgerrechte&Polizei/CILIP 105 (Mai 2014), 61 ff.
[75] Verordnung (EG) Nr. 2725/2000 des Rates v. 11.12.2000, ABl. EG v. 15.12.2000, L 316/1.

lit. l Eurodac-VO definiert werden: *Fingerabdruckdaten für sämtliche Finger, mindestens aber für die Zeigefinger, oder sollten diese fehlen, für alle anderen Finger einer Person oder eine Fingerabdruckspur*.

Die Datenverarbeitung erfolgt bei Eurodac **im Auftrag** der jeweils verantwortlichen Mitgliedstaaten (Art. 3 Abs. 3 Eurodac-VO). Die von Eurodac verwendete Hardware stammt von Dell; die Datenbank stammt von Oracle und als Programm genutzt werden Linux und „GAFIS“ von Gemalto.[76] 2018 waren 5,18 Mio. Datensätze in Eurodac gespeichert.

Die Datenanlieferung zur Zentraleinheit und die Abfrage von dort erfolgt über eine „**nationale Zugangsstelle**“. In Deutschland ist dies das Bundesamt für Migration und Flüchtlinge (BAMF). Der zentrale Zugang für die deutschen Polizei- und Strafverfolgungsbehörden erfolgt über das BKA.[77] Die Fingerabdruckdaten werden gemeinsam mit einer von dem einspeichernden Mitgliedstaat vergebenen Referenznummer und wenigen Verfahrensdaten an Eurodac übermittelt (Art. 9, 11 Eurodac-VO). Als Ergebnis des elektronischen Abgleichs wird dem anfragenden Mitgliedstaat nur mitgeteilt, ob in der Zentraleinheit bereits übereinstimmende Fingerabdruckdaten vorhanden sind oder nicht (hit/no-hit-System). Im Trefferfall werden zusätzlich die genannten Verfahrensdaten übermittelt. Anhand dieser Angaben kann festgestellt werden, ob die betreffende Person bereits vorher in einem oder mehreren anderen Mitgliedstaaten einen Asylantrag gestellt hat. Die endgültige Identifizierung kann danach von dem anfragenden Mitgliedstaat nach Artikel 15 des Dubliner Übereinkommens in bilateraler Zusammenarbeit mit den betroffenen Mitgliedstaaten vorgenommen werden.

Seit 2015 ist nach Neufassung der Eurodac-VO die Nutzung der Eurodac-Daten auch für den Abgleich zu Zwecken der **Gefahrenabwehr und Strafverfolgung** erlaubt. Hierfür müssen bestimmte Voraussetzungen erfüllt sein, z.B. muss der Datenabgleich im Einzelfall erforderlich sein zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat und ein vorheriger Abgleich mit nationalen Fingerabdruckdateien muss erfolglos geblieben sein.

Inzwischen ist eine **Neufassung der Eurodac-VO** von der EU-Kommission auf den Weg gebracht worden.[78] Darin ist die Herabsetzung des Alters der von einer Fingerabdruckerfassung Betroffenen von 14 auf 6 Jahre vorgesehen. Geplant ist weiterhin eine Änderung in der Speicherpraxis. Geplant sein soll zudem eine Erfassung des Gesichtsfelds.[79]

4.4 Visa-Informationssystem

Eine Parallele zu Eurodac besteht mit dem europäischen Visa-Informationssystem (VIS), das eine europaweite Koordination der Visa-Erteilung zum Ziel hat und 2011 in Betrieb ging.[80] Rechtliche Grundlage ist die **VIS-Verordnung** (VIS-VO).[81] Gemäß Art. 9 Nr. 6, 6 VIS-VO gibt die Visumbehörde u.a. in das System ein: *5. ein Foto des Antragstellers entsprechend der Verordnung (EG) Nr. 1683/95; 6.*

[76] Antwort Avramopoulos/EU-Kommission v. 20.06.2018, E-001595/2018.
[77] Eurodac Supervision Coordination Group, Activity Report 2018-2019, 4 November 2020, S. 13
[78] COM (2016) 272 final, 2016/0132 (COD); vgl. COM (2016) 270 final, 2016/0133 (COD).
[79] So tilmann-schott-mehrings.de/Asylrecht/Eurodac, Stand 15.03.2020.
[80] Visa-Informationssystem nimmt Betrieb auf, DANA 4/2011, 174.
[81] Verordnung (EG) Nr. 767/2008 v. 09.07.2008, ABl. EU v. 15.08.2008, L 218/60.

Fingerabdrücke des Antragstellers gemäß den maßgeblichen Bestimmungen der Gemeinsamen Konsularischen Instruktion.

Die Erfassung biometrischer Daten für Visazwecke ist im **Visakodex** geregelt.[82] Art. 13 Abs. 1 Visakodex enthält folgende Regelung: *Die Mitgliedstaaten erfassen im Einklang mit den in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten des Europarates, in der Charta der Grundrechte der Europäischen Union und im VN-Übereinkommen über die Rechte des Kindes verankerten Garantien biometrische Identifikatoren des Antragstellers, nämlich sein Lichtbild und seine zehn Fingerabdrücke.* Die Aufbewahrungsfrist im VIS beträgt nach Art. 23 Abs. 1 VIS-VO höchstens 5 Jahre.

Gemäß Art. 15 Abs. 2 lit. e VIS-VO können die Fingerabdrücke zur **Prüfung der Visumsanträge** abgerufen werden. Art. 18 Abs. 1, Abs. 4 lit. b VIS-VO erlaubt die Abfrage der Fingerabdrücke sowie im Zweifelsfall von Fotos an Außengrenzübergangsstellen *zur Verifizierung der Identität des Visuminhabers und/oder der Echtheit des Visums*. Entsprechendes gilt für die Verifizierung nach Art. 19, 20 VIS-VO innerhalb des Hoheitsgebiets der EU-Mitgliedstaaten, zur Bestimmung der Zuständigkeit für Asylanträge (Art. 21 VIS-VO) sowie zur Prüfung eines Asylantrags (Art. 22 VIS-VO). Eine Löschung erfolgt grds. nach 5 Jahren (Art. 23 VIS-VO).

2018 hat die EU-Kommission eine Überarbeitung der Verordnung sowie damit in Verbindung stehender Verordnungen beschlossen, wodurch der **Zugang von Strafverfolgungsbehörden** zum VIS erleichtert werden soll.[83] Den Zugang deutscher Sicherheitsbehörden zu VIS regelt das VIS-Zugangsgesetz.[84]

Die Hardware für den biometrischen Abgleich im Visa-Informationssystem stammt von Hewlett-Packard. Als Software werden genutzt Morpho Biometric Search Services (MBSS, IDEMIA), Linux und RabbitMQ. Die Workflow-Integration erfolgt durch ein Programm von Accenture und die Datenbank stammt von Oracle. 2018 waren knapp 48 Mio. Fingerabdruckdatensätze im VIS gespeichert.[85] Künftig soll das VIS mit einer **Gesichtserkennungssoftware** ausgestattet werden. Zudem ist geplant, den automatisierten **Abgleich der Fingerabdrücke** im SIS, im europäischen Einreise-/Ausreisesystem (EES) und im Europäischen Reisegenehmigungssystem (ETIAS) „mit einem einzigen Klick“ zu ermöglichen.[86]

4.5 Prümer Vertrag

Der **Prümer Vertrag** ist ein zwischenstaatliches, ins EU-Recht inkorporiertes Abkommen, das die grenzüberschreitende Zusammenarbeit und insbesondere den Informationsaustausch zwischen den Vertragsparteien zum Zweck der Verhinderung und Verfolgung von Straftaten und der illegalen Migration verbessern soll. Das Abkommen mit der amtlichen Bezeichnung „Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration“ wurde am 27.05.2005 im rheinland-pfälzischen Prüm geschlossen. Signatarstaaten sind Belgien, Deutschland, Spanien, Frankreich,

[82] Verordnung (EG) Nr. 810/2009 v. 13.07.2009, ABl. EU v. 15.09.2009, L 243/1.
[83] COM(2018) 302 final, näheren Angaben in EU-Kommission v. 24.6.2020, COM(2020) 262 final, S. 4 f.
[84] VISZG v. 6.5.2009, BGBl. I S. 1034; zuletzt geändert mit G. v. 19.6.2020, BGBl. I S. 1328, 1332.
[85] Antwort Avramopoulos/EU-Kommission v. 20.06.2018, E-001595/2018.
[86] Biometrie-Superdatenbank beschlossen, DANA 2/2019, 99; Busch, Biometrie: Vom Ende des «Identitätsbetrugs» in Europa, www.cilip.de 29.06.2017.

Luxemburg, die Niederlande und Österreich. 2008 wurde der Prümer Vertrag in das Regelwerk der EU inkorporiert.[87] Dem Abkommen beigetreten Bulgarien, Estland, Finnland, Rumänien, die Slowakei und Ungarn.

Der Prümer Vertrag sieht vor, dass Polizei- und Strafverfolgungsbehörden direkt auf bestimmte Datenbanken zugreifen können, die von den Behörden der anderen Vertragsstaaten geführt werden. Die Zugriffsberechtigung erstreckt sich u.a. auch auf **elektronisch gespeicherte Fingerabdrücke**, in Deutschland also auf die in AFIS gespeicherten Daten (Art. 12-14 PrümV).[88] Seit Februar 2008 tauschen Deutschland, Luxemburg und Österreich als weltweit erste Staaten im automatisierten Verfahren Fingerabdruckdaten aus. Weiterhin erlaubt der Vertrag zu Zwecken einer eindeutigen biometrischen Identifizierung den Zugriff auf DNA-Analyse-Dateien (Art. 7-11 PrümV), in Deutschland also auf die DNA-Datenbank des Bundeskriminalamts (BKA).

Derzeit errichten die Firmen IDEMIA und Sopra Steria für die EU ein biometrisches Erkennungssystem, wozu Fingerabdrücke und Gesichtsbilder aus fünf nationalen Datenbanken in einer Datei zusammengeführt werden und damit eine **europaweite Interoperabilität biometrischer Datenbanken** erreicht werden soll.[89]

4.6 Einreise-/Ausreisesystem

Die EU realisiert zudem ein Ein-/Ausreisesystem (EES), womit sämtliche Ein- und Ausreisen von Drittstaatsangehörigen an den Schengener Außengrenzen erfasst werden – und zwar nicht beschränkt auf die visumspflichtigen Drittausländer, deren Visa bereits im VIS gespeichert sind. Beim Grenzübertritt werden dann die in den Reisedokumenten enthaltenen **Gesichtsbilder und Fingerabdrücke ausgelesen** und zusammen mit den Personalien sowie den Angaben über frühere Aufenthalte für fünf Jahre gespeichert.

Mit dem Ein-/Ausreisesystem gekoppelt werden soll zudem das **Reiseinformations- und -genehmigungssystem** (Etias). Dieses soll eine „Vorabinformation“ über die geplante Einreise visumsbefreiter Drittstaatsangehöriger möglich machen, die ihre Reise neu auf einem Internetformular ankündigen müssen. Vorab würden die entsprechenden Daten von den zuständigen Grenzbehörden mit nationalen und internationalen Informationssystemen abgeglichen. Europol soll hierfür eine „Watchlist“ erstellen, um die Einreise von unerwünschten Ausländern zu verhindern.[90]

[87] Beschluss 2008/615/JI des Rates v. 23.06.2008, ABl. EU v. 06.08.2008, L 210/12; dazu PrümG v. 10.07.2006, BGBl. I S. 1456 i.d.F. v. 31.07.2009, BGBl. I S. 2507.
[88] Weichert, DANA 1/2006, 12-15.
[89] Monroy, EU zahlt 300 Millionen Euro für Erkennung von Gesichtern und Fingerabdrücken, netzpolitik.org 05.06.2020.
[90] Busch, Biometrie: Vom Ende des «Identitätsbetrugs» in Europa, www.cilip.de 29.06.2017; Entry/Exit System kommt, DANA 2/2019, 99; Monroy DANA 2/2015, 76 ff; „Smart Borders“ – elektronische Grenzüberwachung, DANA 2/2013, 69.

5 Erfassung von Ausländern nach deutschem Recht

Parallel zur biometrischen Identifizierung nach europaweiten Vorgaben erfolgt der Einsatz der Methode auf der Grundlage des deutschen Ausländerrechts. Dieser Einsatz ist dadurch gekennzeichnet, dass **keine strengen Erforderlichkeits- und Zweckprüfungen** stattfinden.

5.1 Ausländerzentralregister

Seit 1953 besteht in der Bundesrepublik Deutschland ein Ausländerzentralregister (AZR), das seit 1967 automatisiert geführt wird. Darin erfasst sind **alle Nichtdeutschen**, die sich nicht nur vorübergehend in der Bundesrepublik aufhalten. Das ursprünglich von Bundesverwaltungsamt (BVA) betriebene AZR steht seit 2004 in der rechtlichen Verantwortung des Bundesamtes für Migration und Flüchtlinge (BAMF). Die Identifizierung der Betroffenen erfolgte ursprünglich auf der Grundlage der von diesen zur Verfügung gestellten Dokumente. Erfasst wurden die sog. Grundpersonalien (Namen, Schreibweisen der Namen, Geburtsangaben, Geschlecht, Staatsangehörigkeit) sowie „weitere Personalien“ (u.a. abweichende Schreibweisen, andere, frühere und Aliasnamen, Familienstand, Angaben zum Ausweispapier).[91] Biometrische Daten wurden zunächst nicht im AZR gespeichert.

Das **Lichtbild** wird seit 2002 in der Visa-Datei des AZR, in der Visaanträge vermerkt werden, gespeichert (§ 29 Abs. 1 Nr. 4 AZRG).[92] In den allgemeinen Datenbestand des AZR wurde das Lichtbild mit Gesetz vom 19.08.2007 in § 3 Abs. 1 Nr. 5a AZRG 2007 aufgenommen.[93] Damit soll die Identitätsfeststellung bei abfragenden Stellen, die einen direkten Kontakt zum Ausländer haben, erleichtert werden. Voraussetzung für die Erteilung eines Aufenthaltstitels ist die eindeutige Identifizierung (§ 5 Abs. 1 Nr. 1a AufenthG). Das Lichtbild wurde vom Gesetzgeber als ein zuverlässiges, weil wenig veränderliches Datum eingestuft.[94]

Die Lichtbildangaben von **EU-Bürgern**, die innerhalb der EU Freizügigkeit genießen, wurden mit Gesetz vom 27.12.2012 wieder aus dem AZR-Datenbestand herausgenommen (§ 3 Abs. 4 AZRG).[95] Hintergrund dieser Änderung war, dass der Europäische Gerichtshof 2008 festgestellt hatte, dass diese und weitere Speicherungen sowie insbesondere Datennutzungen für Zwecke der Kriminalitätsbekämpfung in Bezug auf EU-Bürger zu einer Diskriminierung im Vergleich zu deutschen Staatsangehörigen führten.[96]

Mit Gesetz vom 02.02.2016[97] wurde die Speicherung von **Fingerabdruckdaten** im AZR eingeführt. Diese werden aber nicht von allen Ausländern erfasst, sondern nur von Flüchtlingen und unzulässig aufhältigen Ausländern. Betroffen ist nach § 3 Abs. 2 Nr. 1 AZRG ein Ausländer, der *1. ein Asylgesuch geäußert hat, 2. unerlaubt eingereist ist oder 3. sich unerlaubt im Geltungsbereich dieses Gesetzes aufhält* (§ 2 Abs. 1a AZRG). Derart erfasst werden zudem Ausländer, *die einen Asylantrag gestellt haben oder über deren Übernahme nach den Rechtsvorschriften der Europäischen Gemeinschaft oder*

[91] § 3 (Abs. 1) Nr. 4, 5 AZRG.
[92] Kritisch zur zentralen Speicherung Golembiewski/Probst, S. 58 ff.
[93] BGBl. I 2007 S. 1970.
[94] Streit ZAR 2002, 239 f.
[95] BGBl. I 2012 S. 2745.
[96] EuGH 16.12.2008 – C-524/06, NVwZ 2009, 378 = DVBl 2009, 171.
[97] BGBl. I 2016 S. 130.

eines völkerrechtlichen Vertrages zur Durchführung eines Asylverfahrens entschieden ist (§ 2 Abs. 2 Nr. 1 AZRG). Im AZR werden zusätzlich zu den Fingerabdruckdaten die dazu gehörigen Referenznummern gespeichert (§ 3 Abs. 2 Nr. 1 AZRG). Mit diesen sog. D-Nummern soll eine Zuordnung der Daten im AZR zu den Beständen im polizeilichen INPOL-System vorgenommen werden können.

2019 wurde mit § 3 Abs. 3a AZRG der Kreis der Personen, von denen im AZR Fingerabdrücke (und Referenzdaten) gespeichert werden, erweitert um Ausländer, *für oder gegen die aufenthaltsrechtliche Entscheidungen getroffen worden sind oder die Antrag auf einen Aufenthaltstitel oder passrechtliche Maßnahme gestellt haben, ausgenommen Entscheidungen und Anträge im Visaverfahren* (§ 2 Abs. 2 Nr. 3 AZRG). Es handelt sich um Ausländer, die aus dem Ausland aufgenommen werden sollen (Resettlement-, Relocation-, sonstige humanitäre Aufnahmeverfahren und Dublin-Übernahmeersuchen). Die **zusätzliche Speicherung** wurde wieder mit der besseren Identifizierbarkeit, diesmal im Rahmen des Abgleichverfahrens, begründet.

In § 10 Abs. 2 S. 2 AZRG ist vorgesehen, dass bei Zweifel an der Identität eines Nicht-EU-Bürgers allen berechtigten Stellen eine **AZR-Abfrage** allein auf der Grundlage von Lichtbildern oder Fingerabdruckdaten erlaubt ist. Ob bei dieser Abfrage ein automatisierter Abgleich mit den AZR-Daten erfolgt und ob ein solcher erlaubt sein soll, ergibt sich aus der Regelung nicht.

Ein Hauptzweck der Einführung einer Spezialregelung für Flüchtlinge im AZRG bestand darin, einen gesetzlichen Rahmen für einen frühzeitigen Informationsaustausch über diese zwischen verschiedenen öffentlichen Stellen nach einer **qualifizierten Identitätsprüfung** vornehmen zu können. Hierfür nutzt das BAMF weitere neue automatisierte Instrumente. Dazu gehört ein Transliterationsassistent (TraLiTa), mit dem bei arabischsprachigen Antragstellern arabische Schriftzeichen einheitlich in lateinische Buchstaben übertragen werden, ein automatisiertes sprachbiometrisches Analysesystem, mit dem Sprachproben einer Dialektanalyse unterworfen werden, um Herkunftsregionen festzustellen, und die Auswertung von Handydaten, um Rückschlüsse auf Kontakte und Fluchtwege ziehen zu können.[98]

5.2 Aufenthalts- und Asylgesetz

Vor der zentralen AZR-Speicherung fanden sich biometrische Daten schon in den Akten und Dateien der **Ausländer- und Asylbehörden**. § 49 Abs. 1 AufenthG hat heute folgenden Wortlaut:

Die mit dem Vollzug dieses Gesetzes betrauten Behörden dürfen unter den Voraussetzungen des § 48 Abs. 1 die auf dem elektronischen Speicher- und Verarbeitungsmedium eines Dokuments nach § 48 Abs. 1 Nr. 1 und 2 gespeicherten biometrischen und sonstigen Daten auslesen, die benötigten biometrischen Daten beim Inhaber des Dokuments erheben und die biometrischen Daten miteinander vergleichen. Darüber hinaus sind auch alle anderen Behörden, an die Daten aus dem Ausländerzentralregister nach den §§ 15 bis 20 des AZR-Gesetzes übermittelt werden, und die Meldebehörden befugt, Maßnahmen nach Satz 1 zu treffen, soweit sie die Echtheit des Dokuments oder die Identität des Inhabers überprüfen dürfen. Biometrische Daten nach Satz 1 sind nur die Fingerabdrücke und das Lichtbild.

[98] Tangermann, Identitätssicherung und -feststellung im Migrationsprozess, EMN-Studie, 2017; kritisch dazu Biselli, Bürgerrechte&Polizei/CILIP 118/119 (6/2019), S. 87 ff.; 16 TB LfD NRW 2003, Kap. 15, S. 148 f.

Vorübergehend war geregelt, dass zur Identifizierung von Ausländern auch Irisbilder zugelassen sind. Da sich dieses Verfahren in der Praxis aber nicht etabliert hat, wurde dieses Merkmal wieder aus dem Gesetz gestrichen.

§ 49 Abs. 1 AufenthG nimmt Bezug auf § 48 Abs. 1 Nr. 1 u. 2 AufenthG, der die **ausweisrechtlichen Pflichten von Ausländern** regelt:

Ein Ausländer *ist verpflichtet,*
1. seinen Pass, seinen Passersatz oder seinen Ausweisersatz und
2. seinen Aufenthaltstitel oder eine Bescheinigung über die Aussetzung der Abschiebung
auf Verlangen den mit dem Vollzug des Ausländerrechts betrauten Behörden vorzulegen, auszuhändigen und vorübergehend zu überlassen, soweit dies zur Durchführung oder Sicherung von Maßnahmen nach diesem Gesetz erforderlich ist.

§ 49 Abs. 7 AufenthG erlaubt ein weiteres biometrisches Verfahren zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers: Das **gesprochene Wort** des Ausländers darf auf Ton- oder Datenträgern aufgezeichnet werden, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde.

Mit dem Terrorismusbekämpfungsgesetz[99] wurde 2002 das damalige Ausländergesetz dahingehend geändert, dass in die Dokumente über den jeweiligen **Aufenthaltstitel** biometrische Merkmale aufgenommen werden. Gemäß § 48 Abs. 2 AufenthG genügt *ein Ausländer, der einen Pass oder Passersatz weder besitzt noch in zumutbarer Weise erlangen kann, … der Ausweispflicht mit der Bescheinigung über einen Aufenthaltstitel oder die Aussetzung der Abschiebung, wenn sie mit den Angaben zur Person und einem Lichtbild versehen und als Ausweisersatz bezeichnet ist*. So ist über diesen „Ausweisersatz“ gewährleistet, dass mit dem Lichtbild eine biometrische Identifizierung erfolgen kann.

Gemäß § 49 Abs. 6, 6a AufenthG sind die typischen Verfahren zur **Feststellung der Identität** *das Aufnehmen von Lichtbildern und das Abnehmen von Fingerabdrücken*.

Bisher war die Durchführung dieser Maßnahmen auf Ausländer ab dem 14. Lebensjahr beschränkt (§ 49 Abs. 6 S. 2 AufenthG, ebenso § 16 Abs. 1 S. 2 AsylG). Am 01.04.2021 trat eine Neuregelung in Kraft, wonach die Erfassung von Fingerabdrücken schon **ab dem 6. Lebensjahr** zulässig ist.[100] Hintergrund dieser Ausweitung ist, dass auf EU-Ebene eine Änderung der Eurodac-VO und der Verordnung über das Visa-Informationssystems anstand, die eine Erfassung der Fingerabdrücke schon ab dem 6. Lebensjahr vorsieht.[101] Es wird damit in Kauf genommen, dass wegen des Wachsens der Kinder Qualitätsdefizite bei den Abdrücken auftreten, da diese noch Wachstumsprozessen und Änderungen ausgesetzt sind.[102]

[99] G. v. 09.01.2002, BGBl. I S- 361, hier Art. 11, 12; dazu Golembiewski/Probst, S. 43 ff..
[100] Zweites Datenaustauschverbesserungsgesetz (2. DVAG) v. 04.08.2019, BGBl. I S. 1131, Art. 3 Nr. 2 cb, c, Art. 5 Nr. 2.
[101] BT-Drs. 19/8752, 68.
[102] Kritisch dazu European Union Agency for Fundamental Rights, FRA Opinion 3 3/2018 (Security features ID) Fundamental rights implications of storing biometric data in identity documents and residence cards, 05.09.2018, S. 22 f.; Netzwerk Datenschutzexpertise v. 08.11.2020 Verbändeanhörung zum Referentenentwurf, https://b-umf.de/src/wp-content/uploads/2018/11/stn_netzwerk_datenschutzexpertise.pdf; .

Das **Verfahren der ausländerrechtlichen Identitätsprüfung** ist in § 89 AufenthG geregelt:

(1) Das Bundeskriminalamt leistet Amtshilfe bei der Auswertung der nach § 49 von den mit der Ausführung dieses Gesetzes betrauten Behörden erhobenen und nach § 73 übermittelten Daten. Es darf hierfür auch von ihm zur Erfüllung seiner Aufgaben gespeicherte erkennungsdienstliche Daten verwenden. Die nach § 49 Abs. 3 bis 5 sowie 8 und 9 erhobenen Daten werden getrennt von anderen erkennungsdienstlichen Daten gespeichert. Die Daten nach § 49 Abs. 7 werden bei der aufzeichnenden Behörde gespeichert.
(1a) Im Rahmen seiner Amtshilfe nach Absatz 1 Satz 1 darf das Bundeskriminalamt die erkennungsdienstlichen Daten nach Absatz 1 Satz 1 zum Zwecke der Identitätsfeststellung auch an die für die Überprüfung der Identität von Personen zuständigen öffentlichen Stellen von Drittstaaten mit Ausnahme des Herkunftsstaates der betroffenen Person sowie von Drittstaaten, in denen die betroffene Person eine Verfolgung oder einen ernsthaften Schaden zu befürchten hat, übermitteln. Die Verantwortung für die Zulässigkeit der Übermittlung trägt das Bundeskriminalamt. Das Bundeskriminalamt hat die Übermittlung und ihren Anlass aufzuzeichnen. Die empfangende Stelle personenbezogener Daten ist darauf hinzuweisen, dass sie nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt worden sind. Ferner ist ihr der beim Bundeskriminalamt vorgesehene Löschungszeitpunkt mitzuteilen. Die Übermittlung unterbleibt, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass
1. unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person, insbesondere ihr Interesse, Schutz vor Verfolgung zu erhalten, das Allgemeininteresse an der Übermittlung überwiegen oder
2. die Übermittlung der Daten zu den Grundrechten, dem Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge sowie der Konvention zum Schutz der Menschenrechte und Grundfreiheiten in Widerspruch stünde, insbesondere dadurch, dass durch die Verarbeitung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen.
(2) Die Verarbeitung der nach § 49 Absatz 3 bis 5 oder Absatz 7 bis 9 erhobenen Daten ist auch zulässig zur Feststellung der Identität oder der Zuordnung von Beweismitteln im Rahmen der Strafverfolgung oder zur polizeilichen Gefahrenabwehr. Sie dürfen, soweit und solange es erforderlich ist, den für diese Maßnahmen zuständigen Behörden übermittelt oder bereitgestellt werden.
(3) Die nach § 49 Abs. 1 erhobenen Daten sind von allen Behörden unmittelbar nach Beendigung der Prüfung der Echtheit des Dokuments oder der Identität des Inhabers zu löschen. Die nach § 49 Abs. 3 bis 5, 7, 8 oder 9 erhobenen Daten sind von allen Behörden, die sie speichern, zu löschen, wenn
1. dem Ausländer ein gültiger Pass oder Passersatz ausgestellt und von der Ausländerbehörde ein Aufenthaltstitel erteilt worden ist,
2. seit der letzten Ausreise, der versuchten unerlaubten Einreise oder der Beendigung des unerlaubten Aufenthalts zehn Jahre vergangen sind,
3. in den Fällen des § 49 Abs. 5 Nr. 3 und 4 seit der Zurückweisung oder Zurückschiebung drei Jahre vergangen sind oder
4. im Falle des § 49 Abs. 5 Nr. 5 seit der Beantragung des Visums sowie im Falle des § 49 Abs. 7 seit der Sprachaufzeichnung zehn Jahre vergangen sind.
Die Löschung ist zu protokollieren.
(4) Absatz 3 gilt nicht, soweit und solange die Daten im Rahmen eines Strafverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung benötigt werden.

Die Funktion der Identifizierungsdaten von Ausländern hat sich mit der Zeit ausgeweitet. Der Grundsatz ist, dass die erkennungsdienstlichen Unterlagen zu vernichten sind, nachdem *dem Ausländer ein gültiger Pass oder Passersatz ausgestellt und von der Ausländerbehörde eine Aufenthaltsgenehmigung erteilt worden ist* (so § 78 Abs. 4 S. 1 Nr. 1 AuslG, vgl. jetzt § 89 Abs. 3 S. 2 Nr. 1 AufenthG). Nach § 89 AufenthG kommt den ED-Unterlagen nun der zusätzliche Zweck der Datenbevorratung für eine **künftige Identifizierung in Zweifelsfällen** zu: Der Ausländer könnte später unter einer anderen Identität versuchen, einen Aufenthaltstitel zu erlangen.[103]

Während im Aufenthaltsgesetz die biometrische Identifizierung davon abhängt, dass diese erforderlich ist, verpflichtet § 16 Abs. 1, 2 AsylG **in jedem Fall eines Asylgesuchs** zu dieser Maßnahme:

(1) Die Identität eines Ausländers, der um Asyl nachsucht, ist durch erkennungsdienstliche Maßnahmen zu sichern. Nach Satz 1 dürfen nur Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden; soweit ein Ausländer noch nicht das 14. Lebensjahr vollendet hat, dürfen nach Satz 1 nur Lichtbilder aufgenommen werden. Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers kann das gesprochene Wort außerhalb der förmlichen Anhörung des Ausländers auf Ton- oder Datenträger aufgezeichnet werden. Diese Erhebung darf nur erfolgen, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde. Die Sprachaufzeichnungen werden beim Bundesamt gespeichert.
(1a) Zur Prüfung der Echtheit des Dokumentes oder der Identität des Ausländers dürfen die auf dem elektronischen Speichermedium eines Passes, anerkannten Passersatzes oder sonstigen Identitätspapiers gespeicherten biometrischen und sonstigen Daten ausgelesen, die benötigten biometrischen Daten erhoben und die biometrischen Daten miteinander verglichen werden. Biometrische Daten nach Satz 1 sind nur die Fingerabdrücke, das Lichtbild und die Irisbilder.

5.3 AFIS beim BKA

Die zentrale **Fingerabdrucksammlung des Bundeskriminalamtes** (BKA) wurde seit dessen Gründung im Jahr 1951 kontinuierlich ausgebaut. Im Jahr 1976 nahm das erste halbautomatische Datenverarbeitungssystem zur Auswertung von Fingerabdrücken den Wirkbetrieb auf. Ein verbessertes, automatisiertes Fingerabdruck-Identifizierungs-System (AFIS) wurde im Jahr 1993 eingeführt.[104] Es basiert auf der Codierung der anatomischen Merkmale (Minutien), die im Finger- und Handflächenabdruck abgebildet sind. Das System kann die Minutien automatisch erkennen und mit dem Code der abgespeicherten Fingerabdrücke und -spuren vergleichen. Seit 2003 werden im AFIS auch Handflächenabdrücke systematisch ausgewertet.

BKA-Präsident Holger Münch kündigte 2017 an, dass Deutschland als erstes europäisches Land seine Fingerabdruck-Datenbank AFIS an das Schengener Informationssystem SIS II anschließt (s.o. 4.2). Während dort bisher nur nach Personennamen gefahndet werden konnte, ist dies nun auch mittels Fingerabdruck möglich. Deutschland arbeitet unter der Federführung Frankreichs an einem neuen

[103] Weichert in Huber, AufenthG, 2010, § 89 Rn. 2 f.
[104] Weichert DuD 1999, 167; Golembiewski/Probst, S. 10 f.

Abfragesystem, das den Abruf von Fingerabdrücken und weiteren Biometrie-Daten nach dem Prümer Vertrag **über ganz Europa hinweg** vereinfacht (s.o. 4.5).[105]

Bei AFIS wird unterschieden zwischen einem Bestand AFIS-P, den das BKA auf Grund seiner originären Zuständigkeit im Bereich der Gefahrenabwehr und der Strafverfolgung speichert (s.u. 6.1), sowie dem sich auf Ausländer beziehenden Bestand AFIS-A. Insofern ist das BKA gemäß § 1 Abs. 3 AZRG **in Amtshilfe** tätig bei der Verarbeitung der Daten nach § 16 Abs. 1 S. 1 AsylG und § 49 AufenthG. In § 1 Abs. 3 S. 2 AZRG heißt es: *Sie werden dort getrennt von anderen erkennungsdienstlichen Daten gespeichert.* Entsprechende Amtshilfevorschriften gibt es in § 16 Abs. 3, 3a, 4 AsylG und § 89 Abs. 1 AufenthG. Die Amtshilfeverpflichtung des BKA besteht im Asylverfahren bereits seit 1993 und wurde 2007 auf die Daten nach § 49 AufenthG erweitert.

Die Fingerabdrücke werden in der **Fingerabdruckdatei AFIS-A** mit einer recherchierbaren Referenznummer gespeichert, die auf die Identitätsprüfungen nach § 16 AsylG durch Aufnahmeeinrichtungen, Mobile Teams und Außenstellen des BAMF verweisen. Seit dem 25.10.2017 besteht insofern eine sog. AsylOnline-Schnittstelle bzw. zur Personengruppe nach § 49 AufenthG eine sog. AZR-Erstregistrierungsschnittstelle (AZR-ER-SST).

Die Amtshilferegelungen erklären sich traditionell damit, dass die Auswertung von ED-Unterlagen und insbesondere von Fingerabdrücken für die Kriminalitätsbekämpfung entwickelt worden ist und insofern das BKA die nötige Expertise vorweisen konnte. Inzwischen ist die Technik so weiterentwickelt, dass es anderen Stellen problemlos möglich wäre, diese Aufgaben selbst wahrzunehmen. Durch die weiterhin erfolgende Einschaltung ist es dem BKA als Polizeibehörde leicht, die bei sich aus „Amtshilfegründen“ gespeicherten Daten **auch für eigene Zwecke** zu nutzen.[106]

Der Begriff der Amtshilfe ist dem Datenschutzrecht fremd. Insofern wird nur zwischen Verantwortlichem (Art. 4 Nr. 7, 24, 26 DSGVO) und Auftragsverarbeiter (Art. 4 Nr. 8, 28 DSGVO) unterschieden. Die Verarbeitung durch das BKA erfolgt vorrangig als **Auftragsverarbeitung**; Verantwortlicher ist i.d.R. das BAMF als für das AZR und für die Verarbeitung im Asylverfahren verantwortliche Stelle. Verantwortlich kann bei einer Erhebung nach § 48 AufenthG aber auch jede tätig werdende Ausländerbehörde sein.

Die vorgesehene **Trennung** der ausländerrechtlichen AFIS-Daten von anderen erkennungsdienstlichen Daten hat keine erkennbare räumliche, organisatorische oder funktionale Bedeutung. Es erfolgt zwischen AFIS-A (Ausländer) und AFIS-P (Polizei) lediglich eine spezifische technische Markierung.[107] Die gesetzlich vorgesehene Trennung gewährleistet nicht, dass das BKA für die Daten keine Nutzungsbefugnis für die eigenen Zwecke der Gefahrenabwehr und der Strafverfolgung hat. Diese Eigennutzung ist ausdrücklich gesetzlich erlaubt (§ 15 Abs. 1 S. 1 Nr. 5 AZRG, § 89 Abs. 2 AufenthG, § 16 Abs. 5 AsylG). Die Trennung ist damit keine von der DSGVO geforderte wirksame Garantie bzw. technisch-organisatorische Sicherungsmaßnahme.

[105] Borchers, BKA-Chef: Deutsche Fingerabdrücke kommen nach Schengen, www.heise.de 16.11.2017, Kurzlink: https://heise.de/-3891722.
[106] Weichert in Huber, AufenthG, 2010, § 89 Rn. 5.
[107] Weichert in Huber, AufenthG, 2010, § 89 Rn. 7.

6 Sicherheitsbehörden

Fingerabdrücke und Lichtbilder sind **klassische Informationsgrundlagen** für Sicherheitsbehörden. In jüngerer Zeit werden weitere biometrische Verfahren zur Identifizierung von Personen, seien es Täter, Opfer oder Dritte, eingesetzt.

6.1 Strafverfolgung und Gefahrenabwehr

Der primäre Zweck biometrischer Identifizierung durch Sicherheitsbehörden ist die Strafverfolgung. Damit werden tatrelevante Spuren Personen zugeordnet, um Beteiligte, Zeugen und insbesondere Täter zu identifizieren. Die Methode wird „**Erkennungsdienst**“ (ED) bezeichnet. Die gesetzliche Grundlage hierfür findet sich in § 81b StPO mit folgendem Wortlaut[108]:

Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden.

Eine ED-Untersuchung von anderen Personen als Beschuldigten ist unter bestimmten Voraussetzungen nach § 81c StPO möglich. Erkennungsdienstliche (ED-) Maßnahmen sind auch nach § 24 Abs. 3 BPolG nach § 20e BKAG oder gemäß **polizeirechtlichen Regelungen** der Bundesländer zulässig.[109]

Die Fingerabdrücke von Beschuldigten eines Ermittlungsverfahrens werden bei Vorliegen der rechtlichen Voraussetzungen dem BKA zwecks Speicherung im zentralen **Fingerabdruckidentifizierungssystem** (AFIS-P) übermittelt. Eine weitere Übermittlung durch das BKA erfolgt an Eurodac, wenn Art. 14 i.V.m. Art. 17 Eurodac-VO (illegaler Grenzübertritt/illegaler Aufenthalt) zum Tragen kommt und die erkennungsdienstlich behandelte Person älter als 14 Jahre ist, oder zum Zwecke der Gefahrenabwehr und Strafverfolgung (bei Vorliegen terroristischer oder sonstiger schwerer Straftaten), und wenn vorher die Abfragen aller anderen nationalen und internationalen Dateien zu keiner Identifizierung geführt haben.

Die Identifizierung mit dem „genetischen Fingerabdruck“ fand in den 90er Jahren Eingang ins Strafverfahren und wurde seitdem immer mehr ausgeweitet (§§ 81e-81 h StPO). Beim BKA wird eine DNA-Datenbank geführt. Mit dem bayerischen Polizeiaufgabengesetz von 2018 schaffte die **DNA-Analyse** zur Feststellung biologischer Merkmale (Farbe von Haar, Haut und Augen), des Alters sowie der biogeografischen Herkunft ihre erste gesetzliche Anerkennung im Bereich der Gefahrenabwehr.[110] 2019 wurde die Methode zur Feststellung von Merkmalen und Alter auch in § 81e Abs. 2 der Strafprozessordnung zu strafrechtlichen Ermittlungen zugelassen.

[108] Dazu Weichert DANA 1/2004, 11
[109] Ausführlich Bäumler u.a., S. 38 ff.
[110] Netzwerk Datenschutzexpertise, DANA 1/2018, 19 ff.

Im **Strafvollzugsrecht** ist ebenso die Vornahme von ED-Maßnahmen vorgesehen und umfasst u.a. Finger- und Handflächenabdrücke, Lichtbilder sowie weitere äußere Merkmale und Messungen.[111]

6.2 Geheimdienste

Die deutschen Geheimdienste, der Auslandsdienst BND (Bundesnachrichtendienst), der MAD (Militärischer Abschirmdienst), das Bundesamt für Verfassungsschutz (BfV) sowie die Landesbehörden für Verfassungsschutz, betreiben das zunächst als analoge Datensammlung geführte und später digitalisierte **Nachrichtendienstliche Informationssystem** (NADIS). Es handelt sich um eine Hinweisdatei, die der Identifizierung einer Person, Organisation oder eines Sachverhaltes und dem Auffinden von Aktenfundstellen dient. Eine Speicherung im NADIS darf nur aufgrund der in den Verfassungsschutzgesetzen definierten gesetzlichen Regelungen erfolgen. Diese Regelungen enthalten keine speziellen Aussagen zur Speicherung biometrischer Identifizierungsdaten. Dies schließt aber die Personenidentifizierung mit derartigen Merkmalen nicht aus. Bei der nachrichtendienstlichen Tätigkeit spielt die biometrische Identifikation wohl eine geringere Rolle als bei der Gefahrenabwehr und Strafverfolgung durch die Polizei.

Die Nachrichtendienste können sich die **Sammlung von Identifizierungsdaten** anderer Behörden nutzbar machen. Dies gilt für Lichtbilder und Fingerabdrücke des Ausländerzentralregisters, die automatisiert abgerufen werden dürfen (§ 20, 22 Abs. 1 S. 1 Nr. 9 AZRG). Sie haben ebenso den automatisierten Zugriff auf die Lichtbilder der Pass- und das Personalausweisregister der Kommunen (§ 22a Abs. 2 S. 4 PassG u. § 25 Abs. 2 S. 4 PAuswG). Direkten Zugriff nehmen können die Nachrichtendienste auch auf gemeinsame mit der Polizei geführten Datenbanken wie z.B. seit 2007 die Anti-Terror-Datei (ATD) oder seit 2012 die Rechtsextremismusdatei (RED). Gespeichert sind dort zu Personen aus den Bereichen Terrorismus oder Gewaltextremismus keine Fingerabdrücke, wohl aber biometrisch „besondere körperliche Merkmale“, Lichtbilder und Angaben zu Identitätspapieren (§§ 2, 3 Abs. 1 Nr. 1a ATDG, §§ 2, 3 Abs. 1 Nr. 1a RED-G). Gemäß § 17 BKAG kann das Bundeskriminalamt für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Verfassungsschutzbehörden des Bundes und der Länder, dem MAD und dem BND (ebenso wie mit den Polizeibehörden des Bundes und der Länder und dem Zollkriminalamt) unter bestimmten Voraussetzungen gemeinsame Dateien errichten. Eine Einschränkung auf bestimmte Daten erfolgt auf gesetzlicher Basis nicht. Regelungen zu Erhebung und Verarbeitung biometrischer Identifizierungsdaten gibt es auch in den einschlägigen Geheimdienstgesetzen nicht; die Befugnis hierzu ist durch die Generalklauseln zur Datenverarbeitung abgedeckt (§ 6 BNDG, § 4 Abs. 1 MADG, § 10 BVerfSchG).

Regelungen, die den **Datenaustausch zwischen Polizei- und sonstigen Exekutivbehörden und Nachrichtendiensten** ermöglichen, müssen den Anforderungen der „hypothetischen Datenneuerhebung“ genügen. Eine Abwägung zwischen dem Verarbeitungszwecke und der Eingriffstiefe für den Betroffenen muss in jedem Fall erfolgen.[112]

[111] Weichert DANA 1/2004, 12; Bäumler u.a., S. 42; Goerdeler in Ostendorf, Jugendstrafvollzugsrecht, 2. Aufl. 2012, § 8 Rn. 119 ff.
[112] BVerfG 10.11.2020 – 1 BvR 324/15, Leitsätze 1 und 3a-c.

7 Anlasslose Erfassung (auch) von Deutschen

Während die biometrische Identifizierung von Ausländern und insbesondere von Flüchtlingen weitgehend etabliert ist, ist die generelle **anlassunabhängige Erfassung** bei Deutschen bzw. der Bevölkerung allgemein erst in jüngerer Zeit eingeführt worden.

7.1 Registrierung der Bevölkerung

Die Identitätssicherung der Bevölkerung generell und damit also auch der deutschen Staatsangehörigen erfolgt über die **kommunalen Melde-, Personalausweis- und Passbehörden**. Die Meldebehörden haben die in ihrem Zuständigkeitsbereich Wohnenden zu registrieren, um deren Identität und Wohnung feststellen und nachweisen zu können. Sie wirken bei der Durchführung von Aufgaben anderer Behörden oder sonstiger Stellen mit und übermitteln Daten. Zu diesem Zweck führen sie Melderegister (§ 2 BMG).[113] In den dezentralen Melderegistern sind keine biometrischen Daten gespeichert. Gespeichert sind aber – neben anderen Identifizierungsdaten – u.a. nach § 3 Abs. 1 BMG

17. Ausstellungsbehörde, Ausstellungsdatum, letzter Tag der Gültigkeitsdauer und Seriennummer des Personalausweises, vorläufigen Personalausweises oder Ersatz-Personalausweises, des anerkannten Passes oder Passersatzpapiers sowie Sperrkennwort und Sperrsumme des Personalausweises,
17a. die AZR-Nummer in den Fällen und nach Maßgabe des § 10 Absatz 4 Satz 2 Nummer 4 des AZR-Gesetzes.

Damit wird eine Verbindung zur biometrischen Registrierung geschaffen: Innerhalb der **Verwaltungseinheit, der die Meldebehörde angehört**, dürfen alle in § 3 Abs. 1 BMG aufgeführten Daten und Hinweise weitergegeben werden, soweit dies zur Aufgabenerfüllung der jeweiligen Stellen erforderlich ist (§ 37 BMG). Zur gleichen Verwaltungseinheit gehören die Personalausweis- und die Passbehörde sowie die dort geführten Personalausweis- und Passregister.

Mit dem Registermodernisierungsgesetz ist geplant, registerübergreifend die bisherige Steuer-Identifizierungsnummer gemäß § 139b der Abgabenordnung (Steuer-ID) als **nationales Kennzeichen** einzuführen.[114] Die Steuer-ID soll danach ins Melderegister aufgenommen werden (Art. 4, § 3 Abs. 1 Nr. 8 BMG-E), ebenso wie in das Passregister (Art. 7, § 21 Abs. 2 Nr. 9a PassG), in das Personalausweisregister (Art. 8, § 23 Abs. 3 Nr. 9a PAuswG-E) sowie in das Ausländerzentralregister (Art. 6, § 3 Abs. 5 AZRG-E in Bezug auf Flüchtlinge).[115]

[113] Zilkens, Datenschutz in der Kommunalverwaltung, 3. Aufl. 2011, Rn. 263.
[114] BT-Drs. 19/24226.
[115] Zu Recht kritisch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens, 28.08.2020; Deutscher Bundestag Wissenschaftlicher Dienst, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 16.09.2020.

7.2 Pass- und Personalausweisgesetz

Das Lichtbild und Fingerabdrücke werden im Pass und im Personalausweis, die Lichtbilder auch im **Passregister** und im **Personalausweisregister** gespeichert. Eine Speicherung der Fingerabdrücke von deutschen Staatsangehörigen findet in diesen **Datenbanken** nicht statt.[116]

Die EU-Mitgliedstaaten stellen auf Basis der Verordnung (EG) 2252/2004 des Rates vom 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten **Pässen und Reisedokumenten**, geändert durch Verordnung (EG) 444/2009 vom 28.05.2009 (Pass-VO), reguläre Reisepässe mit Chip aus, welche das Lichtbild und zwei Fingerabdrücke enthalten. Die europäische Regelung im Jahr 2004 erfolgte auf politischen Druck der Regierung der USA, die mit dem Wegfall der Visumfreiheit für europäische Reisende drohte.[117] Damit werden zwei konkrete Ziele verfolgt: 1. der Schutz vor Fälschung von Pässen und 2. die Verhinderung der betrügerischen Verwendung von Pässen, d.h. deren Verwendung durch andere Personen als ihren rechtmäßigen Inhaber.[118] Deutschland hat den elektronischen Reisepass zum 01.11.2005 und die Speicherung von Fingerabdrücken in Pässen zum 01.11.2007 eingeführt.[119]

Die Verordnung (EU) Nr. 2019/1157 zur Erhöhung der Sicherheit der **Personalausweise** von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (Perso-VO)[120], schafft zudem europaweit eine einheitliche Rechtsgrundlage für nationale Personalausweise. Gespeichert werden zwei Fingerabdrücke der antragstellenden Person in Form des flachen Abdrucks des linken und rechten Zeigefingers im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises.

Personalausweise werden mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält. Bei der Erfassung der biometrischen Identifikatoren wenden die Mitgliedstaaten die technischen Spezifikationen gemäß dem Durchführungsbeschluss der Kommission C(2018)7767 an (Art. 3 Abs. 5 Perso-VO). Gemäß Art. 3 Abs. 7 Perso-VO waren Kinder unter 6 Jahren sowie Personen, bei denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist, von der Abgabepflicht befreit, Kinder unter 12 Jahren konnten bisher befreit werden.

Das Personalausweisgesetz (PAuswG) regelt die Pflicht zum **Mitführen des Ausweises** und dessen Vorlage bei unterschiedlichen Behörden und sonstigen Stellen (§ 1 Abs. 1 S. 1 PAuswG):

Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen gültigen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen und es ihr ermöglichen, ihr Gesicht mit dem Lichtbild des Ausweises abzugleichen.

[116] BT-Drs. 19/22133, S. 6.
[117] Antwort Vitorino im Namen der Kommission v. 11.06.2002, ABl. EU v. 08.05.2003, C110 E/10.
[118] EuGH 17.10.2013 – C-291/12 Rn. 36, 45, NVwZ 2014, 437 f.
[119] BT-Drs. 19/22133, S. 12 f.
[120] ABl. EU v. 12.7.2019, L 188/67.

Bzgl. der **Ein- und Ausreise ins bzw. aus dem Bundesgebiet** besteht in § 1 Abs. 1 PassG eine entsprechende Ausweispflicht durch Vorlage eines Passes.

Die im Chip gespeicherten biometrischen Daten sind nur mit einem hoheitlichen Berechtigungszertifikat **auslesbar**, welches an explizit berechtigte Stellen ausgegeben wird. Die Daten sind durch kryptographische Maßnahmen (Extended Access Control) entsprechend den Vorgaben in der Technischen Richtlinie TR-03110 „Advanced Security Mechanisms for Machine Readable Travel Documents" gegen unberechtigten Zugriff geschützt.[121] Die EU-Kommission veröffentlicht eine Liste der von den Mitgliedstaaten übermittelten Behörden, die eine Leseberechtigung auf den Ausweisen haben (Art. 11 Abs. 7 Perso-VO). Gemäß Art. 11 Abs. 5 Perso-VO dürfen maschinenlesbare Informationen nur gemäß dieser Verordnung oder dem nationalen Recht des ausstellenden Mitgliedsstaats aufgenommen werden. Erlaubt sind gemäß Art. 11 Abs. 6 Perso-VO nur die Echtheitsprüfung des Dokuments und die Identitätsprüfung.

Die Aufnahme des Lichtbilds im Personalausweis ist in § 5 Abs. 2 Nr. 5 PAuswG im Pass in § 4 Abs. 1 S. 1 PassG vorgesehen. Die **Fingerabdrücke** werden gemäß § 4 Abs. 4 PassG bzw. § 5 Abs. 9 S. 2-4 PAuswG gespeichert:

Die Fingerabdrücke werden in Form des flachen Abdrucks des linken und rechten Zeigefingers des Passbewerbers im elektronischen Speichermedium des Passes gespeichert. Bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe wird ersatzweise der flache Abdruck entweder des Daumens, des Mittelfingers oder des Ringfingers gespeichert. Fingerabdrücke sind nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist.

§ 26 Abs. 1 PAuswG sieht vor, dass die Datenerhebung zwecks Ausstellung der Pass- bzw. Ausweisdokumente incl. der biometrischen Merkmale nicht zum Anlass für die Speicherung für weitere Zwecke genommen werden darf. In § 26 Abs. 2 PAuswG bzw. § 16 Abs. 2 S. 3 PassG ist geregelt, dass die bei der Ausweis- oder Passbehörde gespeicherten Fingerabdrücke spätestens nach Aushändigung des Personalausweises bzw. des Passes **gelöscht** werden müssen.

Es bestehen Regelungen zur **Datensicherheit** in § 4 Abs. 3 S. 2 PassG bzw. § 5 Abs. 6 PAuswG: *Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern.* Eine **Zentralisierung** der biometrischen Daten wird in § 4 Abs. 3 S. 3 PassG bzw. § 26 Abs. 4 PAuswG ausgeschlossen: *Eine bundesweite Datenbank der biometrischen Daten … wird nicht errichtet*.

In § 16a PassG (inhaltsidentisch § 17 PAuswG) wird die **Zweckbindung** der biometrischen Daten im Dokument geregelt: *Die im Chip des Passes gespeicherten Daten dürfen nur zum Zweck der Überprüfung der Echtheit des Dokumentes oder der Identität des Passinhabers und nur nach Maßgabe der Sätze 2 und 3 ausgelesen und verwendet werden. Soweit die Polizeivollzugsbehörden, die Zollverwaltung sowie die Pass-, Personalausweis- und Meldebehörden die Echtheit des Passes oder die Identität des Inhabers überprüfen dürfen, sind sie befugt, die auf dem elektronischen Speichermedium des Passes gespeicherten biometrischen und sonstigen Daten auszulesen, die benötigten biometrischen Daten beim Passinhaber zu erheben und die biometrischen Daten miteinander zu vergleichen. Die nach*

[121] BT-Drs. 19/22133, S. 6.

Satz 2 erhobenen Daten sind unverzüglich nach Beendigung der Prüfung der Echtheit des Passes oder der Identität des Inhabers zu löschen.

Das **Passregister und das Personalausweisregister** ist in den §§ 21 ff. PassG und den §§ 23 ff. PAuswG geregelt. In § 21 Abs. 2 PassG sowie § 23 Abs. 3 PAuswG ist vorgesehen, dass neben textlichen Angaben das Passregister sowie das Personalausweisregister ein Lichtbild enthalten darf.

Gemäß § 22a Abs. 2 S. 1-5 PassG u. § 25 Abs. 2 S. 1-4 PAuswG haben die Berechtigung für den automatisierten Abruf des Lichtbildes aus dem Pass- bzw. dem Personalausweisregister Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten sowie generell zur Aufgabenerfüllung: *die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter*.

Die **Zugriffsmöglichkeit von Geheimdiensten** auf die Lichtbilddaten wurde 2017 eingeführt.[122]

8 Rechtliche Bewertung

Die Frage nach der Verfassungsverträglichkeit der staatlichen Nutzung von biometrischen Merkmalen für Identifizierungszwecke ist insbesondere am Maßstab des Grundrechts auf Datenschutz nach Art. 8 GRCh bzw. des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen sowie an den grundrechtlichen Konkretisierungen durch die DSGVO. Es ist unbestritten, dass das Lichtbild und Fingerabdrücke zur Identifizierung von natürlichen Personen geeignet sind. Ebenso klar ist, dass für eine Vielzahl von staatlichen Maßnahmen eine eindeutige Identifizierung der Personen erforderlich ist. Fraglich ist aber, wie bei dieser Datenkategorie die Zweckbindung eingehalten werden kann und ob nicht auch geringere Eingriffe zu einer sicheren Identifizierung führen können und mit welchen Vorkehrungen ein Schutz der Betroffenen bewirkt werden kann. Letztlich steht immer die Frage im Raum, ob die jeweils gesetzlich vorgesehenen Maßnahmen angemessen sind (Art. 52 Abs. 1 GRCh). Dabei ist relevant, ob die bestehenden Regelungen **angemessene Garantien** und spezifische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen vorsehen, so wie dies in Art. 9 Abs. 2 lit. g, Art. 87 DSGVO sowie Art. 10 DSRl-JI gefordert wird (s.o. 1.1).

Inzwischen ist es nicht mehr bestritten, dass die staatliche biometrische Identifizierung einem **Gesetzesvorbehalt** unterliegt. Wegen deren Grundrechtsrelevanz sind die Art, das Ausmaß sowie die Grenzen normenklar gesetzlich zu regeln.[123]

8.1 Zweckbindung

Gemäß Art. 8 Abs. 2 S. 1 GRCh dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden. Der **Grundsatz der Zweckbindung** wird in Art. 5 Abs. 1 lit. b DSGVO und Art. 4 Abs. 1 lit. b DSRl-JI konkretisiert, wonach die Zwecke schon bei der Erhebung

[122] Gesetz zur Förderung des elektronischen Identitätsnachweises, G. v. 07.07.2017, BGBl. I S. 2310; Automatisierter Zugriff der Geheimdienste auf Passbilder? DANA 2/2017.
[123] Hornung, S. 153 ff.; Gundermann/Probst, Kap. 9.6 Rn. 66; Golembiewski/Probst, 2003, S. 20 ff.

festgelegt, eindeutig und legitim sein müssen. Der Zweck von biometrischen Identifizierungsdaten besteht darin, eine Person eindeutig zu identifizieren.

Dieser Identifizierungszweck ist bei einer Verarbeitung biometrischer Identifizierungsdaten zumeist nur ein **Zwischenziel**, mit dem ein administrativer Vorgang zu der identifizierten Person ermöglicht werden soll. Vergleichbar mit der Verarbeitung sonstiger identifizierender Stammdaten ist die Identitätsfeststellung ein Teilschritt bei der Verwirklichung eines darüber hinausgehenden Zwecks, etwa der Gewährung einer Leistung oder der Erlaubnis zu einer bestimmten Tätigkeit.

Identifizierungsdaten können als Schlüssel für die Totalüberwachung eines Menschen oder für die Erstellung eines umfassenden Persönlichkeitsprofils, aber auch für die Kontrolle einer gesamten Gesellschaft genutzt werden. Auf diese Gefahren wurde im deutschen Rechtssystem vom Bundesverfassungsgericht immer wieder hingewiesen.[124] Die DSGVO macht nun Vorgaben zur Eingrenzung dieser Gefahren: Mit der materiell-rechtlichen **Verpflichtung zur weitestgehenden Pseudonymisierung** wird zweckbezogen insbesondere bezüglich der Identifizierungsdaten zur Datensparsamkeit verpflichtet (Art. 5 Abs. 1 lit. c, 32 Abs. 1 lit. a i.V.m. Art. 4 Nr. 5 DSGVO). Art. 11 DSGVO flankiert diese Vorgabe dadurch, dass dem Verantwortlichen keine nachträgliche Verpflichtung zur Reidentifizierung auferlegt wird. Lässt sich die staatliche Verarbeitung der Identifizierungsdaten angesichts der verfolgten Zwecke nicht verhindern, so bedarf es mindestens geeigneter Garantien zur Wahrung der Rechte und Freiheiten der Betroffenen (Art. 87 DSGVO). Dies gilt in besonderem Maße, wenn es sich bei den Identifizierungsdaten um biometrische Identifikatoren handelt (Art. 9 Abs. 1, Abs. 2 lit. g DSGVO).

Im Ergebnis wird durch die DSGVO bei Identifizierungsdaten einerseits die Verarbeitung für sekundär verfolgte Zwecke erleichtert, zugleich aber wird versucht, den Primärzweck „Identifizierung“ von dem Sekundarzweck zu separieren. Bzgl. der verfolgten Sekundärzwecke ist eine strenge Angemessenheitsprüfung durchzuführen. Dabei steht im Vordergrund, inwieweit diese **Sekundärzwecke kompatibel**, also mit einander vereinbar sind, welche Folgen für die Betroffenen zu befürchten sind, und dass geeignete Garantien für die Betroffenen vorhanden sind (vgl. Art. 6 Abs. 4 DSGVO).[125]

Art. 11 Abs. 6 Perso-VO definiert eine enge Zweckbindung bzgl. der Verwendung der biometrischen **Daten auf Personalausweisen**:[126]

Auf dem Speichermedium von Personalausweisen und Aufenthaltsdokumenten gespeicherte biometrische Daten dürfen nur gemäß dem Unionsrecht und dem nationalen Recht von ordnungsgemäß befugten Mitarbeitern der zuständigen nationalen Behörden und Agenturen der Union verwendet werden, um
a) den Personalausweis oder das Aufenthaltsdokument auf seine Echtheit zu überprüfen,
b) die Identität des Inhabers anhand direkt verfügbarer abgleichbarer Merkmale zu überprüfen, wenn die Vorlage des Personalausweises oder Aufenthaltsdokuments gesetzlich vorgeschrieben ist.

[124] BVerfG 15.12.1983 – 1 BvR 209/83 u.a. Rn. 94, NJW 1984, 419 ff., 422; BVerfG 02.03.2010 – 1 BvR 256/08 u.a. Rn. 216-218, NJW 833 ff, 839; dazu Roßnagel NJW 2010, 1240 ff..
[125] Golembiewski/Probst, S. 22 f.
[126] Erwägungsgrund 21 VO (EU) 2019/1157; entsprechend EuGH 17.10.2013 – C-291/12 Rn. 56; NVwZ 2014, 438.

Diese europarechtlich vorgegebene **strenge Zweckbeschränkung** wird bei der nationalen Umsetzung in § 17 PAuswG (und auch in § 16a PassG) übernommen.

8.2 „Sicherheit“ als Sekundärzweck

Angesichts der grundrechtlichen Vorgaben bzw. dem rechtlichen Rahmen von DSGVO und DSRl-JI ist es irritierend, mit welcher Nonchalance die Zweckbindungsanforderungen bei der Verarbeitung biometrischer Identifizierungsdaten im Ausländer- und insbesondere **im Flüchtlingsrecht ignoriert** werden. Dies lässt sich rechtshistorisch damit erklären, dass die Verarbeitungsregeln älter sind als die Vorgaben der GRCh und der DSGVO. Ausländerrecht wurde ursprünglich als besonderes Sicherheitsrecht wahrgenommen. Rechtspolitisch erklärt sich der Umstand damit, dass es für diese Betroffenengruppen keine wirksame Betroffenenlobby gibt. Verfassungsrechtlich gab und gibt es aber keine Legitimation für die Verschmelzung von Aufenthalts- und Sicherheitsrecht:

Die Zeiten, in denen die fremde Staatsangehörigkeit per se als ein Indiz für ein **Sicherheitsrisiko** angesehen wurde, sollten angesichts der Globalisierung der personalen Mobilität und den damit gesammelten Erfahrungen überwunden sein. Tatsächlich werden aber über die umfassende Verfügbarkeit der biometrischen Identifizierungsdaten für Sicherheitszwecke im AZR sowie in AFIS-A keine materiell-rechtlichen oder prozeduralen Schranken zwischen den beiden Zwecken etabliert.

Dies gilt insbesondere für die generelle **Verfügbarkeit von Fingerabdrücken** aus dem AZR, AFIS-A und subsidiär aus VIS und Eurodac in Bezug auf Nicht-EU-Bürger. Die unabdingbare aufenthaltsrechtliche Identifizierbarkeit mag deren weitgehende Erfassung insbesondere bei Flüchtlingen legitimieren, auch wenn bei vielen Flüchtlingen auf der Grundlage von Dokumenten eine unzweifelhafte Identifizierung möglich sein dürfte. Wenn gut die Hälfte der erwachsenen Asylsuchenden keine Dokumente vorlegen können, die zweifelsfrei Herkunft, Namen und Geburtsdatum belegen können, so spricht dies dafür, dass regelmäßig eine zusätzliche biometrische Identitätssicherungsmaßnahme ergriffen wird.[127]

Diesen biometrischen „Datenschatz“ ungehindert der Polizei für **Zwecke der Strafverfolgung und der Gefahrenabwehr** oder gar den Geheimdiensten zur Verfügung zu stellen, kann definitiv nicht mehr als angemessen gerechtfertigt werden, zumindest solange keine Untersuchungen vorliegen, die die besondere Kriminalität oder Staatsgefährdung nachgewiesen ist, die von dieser Gruppe potenziell ausgeht, sowie, dass diese Gefahren mit Hilfe der Fingerabdrücke wirksam bekämpft werden können.

Einschränkungen erfolgten in Bezug auf **Staatsangehörige anderer EU-Mitgliedstaaten** erst durch eine Entscheidung des EuGH, wobei hierbei dessen Verdikt weniger auf der Zweckunvereinbarkeit, als auf die Ungleichbehandlung der anderen EU-Bürger gegenüber Deutschen basiert.[128]

Das Verbot der **Diskriminierung wegen der Staatsangehörigkeit** gilt nicht nur für EU-Staatsangehörige sondern gemäß Art. 21 Abs. 2 GRCh generell: *Im Anwendungsbereich der Verfassung ist unbeschadet ihrer einzelnen Bestimmungen jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten*. Damit wird nicht jegliche Ungleichbehandlung wegen der Staatsangehörigkeit untersagt. Wohl aber bedarf die Ungleichbehandlung einer plausiblen Begründung; sie muss objektiv gerechtfertigt sein.[129]

[127] Siehe Fn. 20: Asylanträge ohne Ausweis, SZ 24.02.2021 6.
[128] EuGH 16.12.2008 – C-524/06, NVwZ 2009, 378.
[129] Grasser/Reiser in Schwarze, EU-Kommentar, 4. Aufl. 2018, Art. 21 Rn. 12.

Voraussetzung ist also, dass die Verarbeitung der biometrischen Daten von Nicht-EU-Bürgern aus allgemeinen Sicherheitsgründen legitimiert werden kann. Dies setzt voraus, dass Sicherheitsrisiken, die von Nicht-EU-Bürgern ausgehen, gegenüber denen von EU-Bürgern signifikant höher sind, es hierfür eine plausible Erklärung gibt und mit Hilfe der biometrischen Daten diese Risiken signifikant reduziert werden können. Entsprechende empirische Erkenntnisse sind nicht bekannt. Eine pauschale Behauptung, dass gegenüber EU-Bürgern von Nicht-EU-Bürgern ein höheres Sicherheitsrisiko ausgeht, hat keine Grundlage. Daher ist die Ungleichbehandlung in Bezug auf die Sekundärnutzung biometrischer Identifizierungsdaten von Nicht-EU-Bürgern eine unzulässige Diskriminierung.

§ 15 Abs. 1 PAuswG und § 17 PassG enthalten in Bezug auf **Deutsche** für Sicherheitsbehörden – die strenge Zweckbindung der biometrischen Daten auf den Ausweisdokumenten aufhebend – eine generelle automatisierte Abruf- und Speicherbefugnis „im Rahmen ihrer Aufgaben und Befugnisse“. Diese Aufweichung der ursprünglichen Zweckbindung (Identitätsprüfung) kann angesichts der spezifischen Funktion von Grenzkontrollen als angemessen bewertet werden.[130] Ein Abgleich für Fahndungszwecke ist jedoch nur akzeptabel, wenn hinreichende materielle und prozedurale Anforderungen für die Ausschreibung bestehen, mit denen die Angemessenheit sichergestellt wird. Eine generelle Nutzungsbefugnis für Sicherheitszwecke wäre nicht verhältnismäßig.

Die Frage, inwieweit die generelle **Verfügbarkeit des Lichtbilds** im AZR, aber auch im Pass- und im Personalausweisregister für Sicherheitszwecke als angemessen bewertet werden kann, ist bisher nicht befriedigend beantwortet.

8.3 Erforderlichkeit

Gemäß Art. 5 Abs. 1 lit. c DSGVO müssen personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (´Datenminimierung´)“. Der Grundsatz der Datenminimierung bezieht sich auf **sämtliche Umstände der Datenverarbeitung**: auf die Art der Daten und die Art der Verarbeitung, die Personenbeziehbarkeit, den technisch-organisatorischen Schutz.[131]

Die Pflicht zur Datenminimierung verbietet eine bestimmte Verarbeitung, wenn mit einer **weniger invasiven Form der Datenverarbeitung** der gleiche Zweck erreicht werden kann. Können die Zwecke der Identifizierung mit nicht sensitiven Daten erreicht werden, etwa allein mit einem Ausweis und dort gespeicherten Angaben zu Name und Wohnort, so ist auf eine Nutzung von biometrischen Identifizierungsdaten zu verzichten.[132] Genügt zum Identifizierungszweck ein nicht automatisiert auswertbares Lichtbild, so ist ein automatisiert auswertbares Bild und dessen automatisierte Auswertung unzulässig. Ein analoger Datenabgleich ist grds. einem automatisierten Abgleich vorzuziehen.

Bei der **Wahl des genutzten biometrischen Merkmals** und des Verfahrens ist darauf zu achten, dass diesem eine möglichst geringe invasive Wirkung zukommt. Die Irisidentifikation ist wegen der geringeren Missbrauchsgefahr als milderes Mittel der Identifikation über Gesichtsbild oder Fingerabdrücke grds. vorzuziehen. Entsprechendes gilt für die Nutzung von Templates gegenüber

[130] EuGH 17.10.2013 – C-291/12 Rn. 61; NVwZ 2014, 438
[131] Weichert in Däubler u.a., Art. 5 Rn. 45.
[132] LAG Berlin Brandenburg 04.06.2020 – 10 Sa 2130/19, DANA 4/2020, 268.

biometrischen Rohdaten.[133] Genügt ein Lichtbild, so ist auf ein weiteres biometrisches Merkmal, etwa Fingerabdrücke, zu verzichten. Genügt eine Ein-Faktor-Identifizierung, so ist die Nutzung von weiteren Merkmalen unzulässig. Genügt eine lokale Verarbeitung auf einem Ausweis, so ist die Speicherung in einem Hintergrundsystem unzulässig; eine dezentrale Speicherung ist weniger eingriffsintensiv als eine zentrale Speicherung.[134]

8.4 Erforderlichkeit von mehr als einem Finger

Art. 3 Abs. 5 Perso-VO sowie Art. 1 Abs. 2 Pass-VO verpflichten sämtliche EU-Bürger, in ihren Personalausweisen und in ihren Reisepässen die **Erfassung von zwei Fingerabdrücken** zu dulden und dadurch im Fall einer behördlichen Kontrolle auch einen Abgleich der Fingerabdrücke mit den gespeicherten Daten vornehmen zu lassen. Diese Regelungen müssen gemäß Art. 52 Abs. 1 S. 2 GRCh dem Grundsatz der Verhältnismäßigkeit entsprechen. In Erwägungsgrund 18 der Perso-VO wird ausgeführt:

Die Speicherung eines Gesichtsbilds und zweier Fingerabdrücke (im Folgenden „biometrische Daten“) auf Personalausweisen und Aufenthaltskarten, die in Bezug auf biometrische Pässe und Aufenthaltstitel für Drittstaatsangehörige bereits vorgesehen ist, stellt eine geeignete Kombination einer zuverlässigen Identifizierung und Echtheitsprüfung im Hinblick auf eine Verringerung des Betrugsrisikos dar, um die Sicherheit von Personalausweisen und Aufenthaltskarten zu verbessern.

Die Bundesregierung hatte wegen der verpflichtenden Fingerabdruckspeicherung im Gesetzgebungsverfahren zunächst einen Prüfvorbehalt geltend gemacht. Als Argument für die **Erforderlichkeit** erklärte sie später – unter Aufgabe ihres Vorbehalts: „Die Speicherung des Fingerabdruckes in Identitätsdokumenten dient dem Zweck, bei Zweifeln an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person die Identität dennoch unmittelbar feststellen zu können. Die derzeit in Zweifelsfällen noch teilweise notwendigen und zeitaufwändigen Nachfragen bei anderen Behörden können damit künftig entfallen.“[135]

Dass derartige Zweifel an der Identität bei Ausweisprüfungen entstanden sind und wie oft dies der Fall war, ist nicht bekannt. Es gibt bisher keinerlei Belege für die behauptete Erforderlichkeit.[136] Die Erforderlichkeit der Speicherung von Fingerabdrücken auf Ausweispapieren wird u.a. mit der **Bewahrung von Sicherheit** „insbesondere im Zusammenhang mit Terrorismus und grenzüberschreitender Kriminalität“ begründet.[137] Dem steht die Aussage der Bundesregierung entgegen: „Es sind keine Fälle von als terroristisch eingestufter Straftaten bekannt, in denen das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Auseisdokumenten mutmaßlich dazu geführt hätten, dass die Taten nicht verhindert bzw. nicht aufgeklärt und die Täter ermittelt werden konnten.“[138]

[133] VG Gelsenkirchen 15.05.2012 – 17 K 3382/07 Rn. 25, NVwZ 2012, 984.
[134] EuGH 16.12.2008 – C-524/06, Rn. 62, MMR 2009, 174.
[135] BT-Drs. 19/22133, S. 5 f.
[136] Ebenso FRA (Fn. 102) S. 20; Digitalcourage Stellungnahme v. 22.10.2020, Deutscher Bundestag Innenausschuss A-Drs. 19(4)613 B, S. 3 ff.
[137] ErwGr 6 VO (EU) 2019, 1157.
[138] Antwort Bundesregierung auf Kleine Anfrage Fraktion die Linke, BT-Drs. 19/22133, S. 9.

Der **Abdruck eines Fingers** würde genügen, um in den wenigen Fällen eines Identitätszweifels eine Ausräumung des Zweifels zu ermöglichen. Durch die Speicherung nur eines Fingerabdrucks würde die Eingriffsintensität reduziert, da das mit zwei Abdrücken bestehende Missbrauchsrisiko angesichts der Verdoppelung der Zahl der potenziellen Abgleichsfingerabdrücke höher ist.[139]

Angesichts einer geringen Zahl von Fällen, bei denen mit Hilfe des Fingerabdrucks eine schnelle Beseitigung von Identitätszweifeln möglich ist, ist es **nicht angemessen**, eine Verpflichtung für über 300 Mio. EU-Bürger auszusprechen, zwei sensitive digital erfasste Fingerabdrücke auf dem Ausweis oder Pass speichern zu lassen.

Die Eingriffsintensität erhöht sich bei Drittausländern und insbesondere Flüchtlingen, bei denen zur eindeutigen Identifizierung nicht nur zwei Fingerabdrücke, sondern die **Abdrücke aller zehn Finger** erhoben und u.a. in Eurodac, im AFIS-A, im VIS und im AZR gespeichert werden. Weshalb alle Finger für Identifizierungszwecke erhoben werden müssen, wurde bisher – soweit ersichtlich – offiziell nirgends begründet. Angesichts des Umstands, dass für die eindeutige Identifikation ein Fingerabdruck genügt, erfolgt ein übermäßiger, d.h. unverhältnismäßiger informationeller Eingriff. Die Nutzungsmöglichkeit aller zehn Fingerabdrücke für Zwecke der Sicherheitsbehörden kann die Erforderlichkeit der Erfassung nicht begründen. Es gibt keine wissenschaftlichen Nachweise für die Notwendigkeit aller 10 Fingerabdrücke der Drittausländer, bei denen niemals ein Tatverdacht bestanden hat, für solche Sicherheitszwecke.[140]

8.5 Welcher Finger?

Bei der Umsetzung der europäischen Vorgabe im Personalausweisgesetz oder im Passgesetz wurde der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und damit der Erforderlichkeitsgrundsatz in einer weiteren Hinsicht missachtet: Die in § 5 Abs. 9 PAuswG und § 4 Abs. 4 PassG vorgesehene Speicherung der **Fingerabdrücke der Zeigefinger** betrifft für jede Hand diejenigen Finger, mit denen am meisten Spuren hinterlassen werden. Statt Fingerabdrücke des Zeigefingers zu verwenden, wären solche des Ringfingers und des kleinen Fingers weniger missbrauchsanfällig, für Identifizierungszwecke aber ebenso geeignet. Wegen des Fehlens europarechtlicher Vorgaben hätte der Gesetzgeber den Spielraum gehabt, insofern eine weniger eingreifende Maßnahme vorzusehen.

Die der Fingerspeicherpflicht bei Personalausweisen zugrunde liegende EU-Verordnung 2019/1157 (Perso-VO) sieht keine Festlegung auf einen bestimmten Finger vor. Als Rechtfertigung für die Wahl der Zeigefinger wird vorgetragen, dass damit die **Datenstruktur von ICAO 9303** gewählt wurde, wie sie auch in den Reisepässen gemäß Art. 2 lit. c EU-Verordnung 2252/2004 (PassVO) für Reisepässe Verwendung findet.[141] Tatsächlich enthält der ICAO-Standard 9303 Part 9 detaillierte Vorgaben für die Gestaltung biometrisch automatisiert lesbarer Lichtbilder. Fingerabdrücke werden dagegen nur als zusätzliches Merkmal aufgeführt, ohne dass spezifische Finger vorgegeben werden.[142] Zudem kann ein

[139] Mit der Frage, ob in Fingerabdruck ausreichend wäre, hat sich der EuGH 17.10.2013 – C-291/12, Rn. 48, NVwZ 2014, 438, nicht befasst.
[140] BVerfG 16.05.2002 – 1 BvR 2257/01, Rn. 13-15, NJW 2002, 3231 f.
[141] Busch, Athene, Stellungnahme zum Gesetzentwurf BT-Drs. 19/21986 u. 19/22783, Bundestag Innenausschuss A-Drs. 19(A)613 D v. 23.10.2020, 7.
[142] ICAO Doc 9303 Machine Readable Travel Documents, Seventh Edition, 2015, Part 9, S. 10 f.; Hornung, S. 94 f

internationaler Standard keine eigenständige Verbindlichkeit entwickeln, mit dem Grundrechtseingriffe legitimiert werden.[143]

Vorgetragen wird zudem, dass die Wahl eines anderen Fingers wegen der abweichenden internationalen Standards die Identitätsfeststellung im Ausland zumindest behindern würde. Hinzu käme, dass die Fingerabdruckfläche z.B. des kleinen Fingers kleiner ist und weniger Minutien liefert und die Erfassung der Zeigfinger durch die **anatomischen Gegebenheiten** einfacher sei als etwa bei einem kleinen Finger.[144] Diese Erwägung mag für den kleinen Finger zutreffen, gilt aber nicht für den Ringfinger, der in Bezug auf Ausmaß und Qualität keinen Unterschied zum Zeigefinger aufweist.

8.6 Lokale Speicherung und Datenabgleich

Die europäischen rechtlichen Vorgaben sehen vor, dass bei der Verpflichtung zur biometrischen Identifizierung geeignete Garantien für Freiheiten und Rechte der Betroffenen bestehen müssen (s.o. 1.1 und 8.1). So werden von Deutschen die biometrischen Referenzdaten nur in den Ausweisdokumenten gespeichert und nicht staatlich hinterlegt. Damit befinden sich diese Daten weitgehend unter der Kontrolle des Bürgers selbst.[145] Eine **Hinterlegung in einer Datenbank** führt zu einer verstärkten Nutzung dieser Daten und zu einer reduzierten Kontrollierbarkeit für die Betroffenen.

Eine Garantie i.S.d. DSGVO kann darin bestehen, dass die für Identifizierungszwecke erhobenen biometrischen Daten in einer **Datenbank nicht abgespeichert** werden dürfen. Ein solches Verbot enthalten bzgl. der abgeglichenen Fingerabdruckdaten § 15 Abs. 2 PAuswG und § 16 Abs. 3 S. 3 PassG.

Nicht gesetzlich ausgeschlossen sind aber Fahndungsabgleiche (s.o. 8.2). Ein solches Abgleichsverbot enthält Art. 11 Abs. 6 Perso-VO, der die Nutzung der biometrischen Daten aus Personalausweisen ausschließlich auf die Echtheitsprüfung des Ausweises und die Identitätsprüfung des Inhabers beschränkt. Abgleiche mit den Identitätsstammdaten sind danach zwar nicht ausgeschlossen, wohl aber die Verwendung von Gesichtsbild- und Fingerabdruckdaten. Das Fehlen einer strengen nationalen Zweckbeschränkung kann dazu führen, dass Fingerabdruckdaten aus den Ausweisen nicht nur zur Identitätsfeststellung verwendet werden, sondern auch zu **Zwecken des Fahndungsabgleichs** z.B. mit AFIS-P und die Abspeicherung der dabei erlangten Treffer. Derartige Datenerhebungen mit dem Zweck des Abgleichs in eigenen und sogar externen Datenbanken werden in den deutschen Sicherheitsgesetzen erlaubt (z.B. §§ 81b, 163, 483 StPO, §§ 38 f., 42 f., 49 BKAG, §§ 21, 23, 29, 34 BPolG sowie entsprechende Landesregelungen).

Den Beamten in Sicherheitsbehörden dürfte angesichts ihrer weitgehenden sicherheitsgesetzlichen Befugnisse nicht hinreichend bewusst sein, dass europarechtlich der Abruf biometrischer Daten aus einem Personalausweis **für andere Zwecke als den der Identitätsfeststellung** verboten ist. Ein Abgleich mit biometrischen Fahndungsdatenbanken wie z.B. AFIS ist daher europarechtlich unzulässig.

[143] Golembiewski/Probst, S. 37.
[144] Busch, Athene, Stellungnahme zum Gesetzentwurf BT-Drs. 19/21986 u. 19/22783, Bundestag Innenausschuss A-Drs. 19(A)613 D v. 23.10.2020, 7.
[145] Busch, Athene, Stellungnahme zum Gesetzentwurf BT-Drs. 19/21986 u. 19/22783, Bundestag Innenausschuss A-Drs. 19(A)613 D v. 23.10.2020, 7.

Eine solche Klarstellung im nationalen Recht wurde im Rahmen der Regelung der verpflichtenden Aufnahme von Fingerabdrücken im Ausweis unterlassen.[146]

Entsprechendes gilt für den automatisierten **Abgleich der Lichtbilddaten** im Personalausweis oder im Pass mit externen Dateien, etwa dem GES des BKA. Welche Risiken insofern bestehen, haben die polizeilichen Ermittlungen zu den im Rahmen des G-20-Gipfels im Jahr 2017 begangenen Straftaten gezeigt, wo Gesichtsbilder von vermeintlichen Straftätern mit Hilfe von automatisierter Gesichtserkennung analysiert und zur Öffentlichkeitsfahndung verwendet wurden.[147] Angesichts eines fehlenden expliziten Abgleichsverbots besteht das Risiko, dass im Rahmen von Ausweiskontrollen biometrische Abgleiche mit Fahndungsregistern vorgenommen werden. Angesichts der technisch bedingten Fehlerquote gerade in diesem Bereich würden solche Fahndungsabgleiche dazu führen, dass zunächst viele unschuldige Personen in sicherheitsbehördliche Fahndungen einbezogen würden.

Eine beschränkte Schutzregelung kann darin bestehen, dass biometrische Daten nicht in einem zentralen, z.B. nationalen Register gespeichert werden, sondern vielmehr **dezentral auf kommunaler Ebene**, wenn hierdurch der Zugriff auf die biometrischen Daten eingeschränkt wird.[148]

Keine Einschränkungen bzgl. Abspeicherung und Fahndungsabgleich gibt es in Bezug auf biometrische Daten von **Flüchtlingen**. Derartige Speicherungen und Abgleiche sind vielmehr für Sicherheitszwecke explizit vorgesehen (s.o. 5). Auch sonstige geeignete Garantien zum Schutz von deren Rechten und Freiheiten fehlen auf einfachgesetzlicher Ebene. Dies führt dazu, dass die erlaubten Speicherungen und Abgleiche auf europa- bzw. verfassungsrechtlicher Ebene hinterfragt und verworfen werden müssen.

8.7 Angemessenheit

Im Rahmen der **Verhältnismäßigkeitsprüfung** ist nicht nur die Geeignetheit und die Erforderlichkeit biometrischer Identifizierungsmethoden festzustellen, sondern auch deren Angemessenheit. Grundrechtseinschränkungen dürfen danach nur vorgenommen werden, wenn sie *den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen* (Art. 52 Abs 1 S. GRCh).

Dabei sind die administrativen Möglichkeiten mit den Risiken für die Betroffenen abzuwägen. Die Risiken werden erhöht, wenn Identitätsdatenabgleiche im Geheimen bzw. ohne Wissen der Betroffenen erfolgen, wenn dadurch kein oder nur eingeschränkter Rechtsschutz besteht, wenn ein hohes Fehlerrisiko anzunehmen ist oder wenn besonders schwerwiegende Eingriffe bei den Betroffenen als Folgemaßnahmen zu befürchten sind. Grundlage für eine Bewertung von Möglichkeiten und Risiken sollten objektive Daten über die Datennutzung und deren Nutzen sein. Tatsächlich sind keine empirischen Untersuchungen hierzu bekannt; ebenso wenig wie nachvollziehbar **dokumentierte Abwägungen**. Die massive Expansion staatlicher automatisierter biometrischer

[146] Stellungnahme Netzwerk Datenschutzexpertise v. 12.10.2020 zum Gesetzentwurf der Bundesregierung, BT-Drs. 19/21986, Deutscher Bundestag, Innenausschuss A-Drs. 19(4)605, 7f.
[147] Große Öffentlichkeitsfahndung nach G-20-Gewaltverdächtigen, DANA 1/2018, 41 ff.; Datenschutzbeauftragter beanstandet polizeiliche Gesichtserkennung, DANA 4/2018, 199 f.
[148] So § 4 Abs. 4 S. 2 PassG, § 1 Abs. 5 S. 2 PAuswG i.d.F. des Terrorismusbekämpfungsgesetz von 2002; dazu Golembiewski/Probst, S. 58 ff., 68.

Identifizierung in den letzten Jahren, ohne dass dem eine sichtbare Gefährdungserhöhung entsprach, begründet generell Zweifel an der Verhältnismäßigkeit/Angemessenheit der Maßnahmen. So liegen z.B. keine Erkenntnisse vor, wie die Möglichkeit des Direktzugriffs von Geheimdiensten auf die Bilddaten des Pass- bzw. Personalausweisregisters genutzt wird und welche Effekte bzgl. Sicherheit einerseits bzw. Gefährdung von Betroffenen ausgelöst wurden.

Die Verarbeitung sensitiver Identifizierungsdaten ist nur erlaubt, wenn „der Gesetzgeber für **spezifische Garantien** im Hinblick auf einen wirksamen Schutz dieser Daten vor falschen und missbräuchlichen Verarbeitungen“ sorgt. Solche Garantien liegen u.a. in engen Zweckbegrenzungen (Identitätsprüfung) und Sicherungen vor dem Zugriff durch Nichtberechtigte.[149]

Eine besondere Gefahr von auf Ausweisdokumenten gespeicherten biometrischen Ausweisen liegt darin, dass anlässlich von **Ausweiskontrollen im Drittausland** dortige Behörden die Biometriedaten abspeichern – was innerhalb der EU verboten ist – und dann zur behördlichen oder gar geheimdienstlichen Zwecken gebrauchen bzw. missbrauchen.[150] Vorkehrungen hiergegen sind nicht vorgesehen.

Angesichts Fehlerrisiken der automatisierten **Gesichtserkennung**, der Streubreite der Technik und dem massiven Grundrechtseingriff kann deren Einsatz im öffentlichen Raum derzeit nicht als verhältnismäßig angesehen werden.[151] Die geheimdienstliche Zugriffsbefugnis auf Bilddaten aus dem Pass- und Personalausweisregister in den Kommunen ist, insbesondere auch wegen ihrer bisherigen Unkontrollierbarkeit, unverhältnismäßig.

Das gleiche Verdikt liegt nahe bei dem undifferenzierten Zugriff von deutscher Sicherheitsbehörden aus sämtliche Fingerabdruckdaten von **Flüchtlingen**. Besonders gravierend ist die Verletzung des Verhältnismäßigkeitsgrundsatzes bei der geheimdienstlichen automatisierte und weitgehend unkontrollierte Zugriffsmöglichkeit auf die biometrischen Daten des AZR (§§ 20, 22 AZRG).[152]

8.8 Transparenz

Dieser Befund wird durch Transparenzdefizite bekräftigt. Zwar enthält die DSGVO umfangreiche Regelungen, mit denen für die Betroffenen Transparenz hergestellt werden soll, insbesondere in den Art. 12 ff. DSGVO. Diese Regelungen finden aber z.B. auf die Verarbeitung von Geheimdiensten keine Anwendung. Bei sonstigen Sicherheitsbehörden sind die Transparenzpflichten stark eingeschränkt (Art. 12-15 DSRl-JI). Doch selbst die DSGVO-Regelungen laufen in der praktischen Umsetzung weitgehend ins Leere. Staatliche Identifizierung erfolgt in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO). Ihr liegt regelmäßig eine gesetzliche Regelung als Rechtsgrundlage zugrunde. Die Nennung dieser Rechtsgrundlagen (Art. 13, 14, jeweils Abs. 1 lit. c DSGVO) ist für die Betroffenen wenig hilfreich,

[149] EuGH 17.10.2013 – C-291/12, Rn. 55 ff, NJW 2014, 438; zu Maßnahmen gemäß dem Standard-Datenschutzmodell DSK, Positionspapier, S. 35.
[150] Dies war ein zentrales Argument in der – aus anderen Gründen – abgewiesenen Verfassungsbeschwerde BVerfG 30.12.2012 – 1 BvR 502/09, Rn. 4.
[151] FDP-Fraktion BT-Drs. 19/16862 v. 29.01.2020, Fraktion Bündnis 90/Die Grünen BT-Drs. 19/16885 v. 29.01.2020, vgl. Deutscher Bundestags Plenarprotokoll v. 30.01.2020, S. 17860 ff.
[152] Weichert, AZRG, 1998, § 22 Rn. 5.

da deren **Zugänglichkeit, Komplexität und Struktur** für den durchschnittlichen Betroffenen nicht erfasst werden können.

Es bedarf daher eigenständiger Mechanismen, mit denen die fehlende Transparenz hergestellt wird, so dass für die Betroffenen die relevanten Informationen in einem verständlichen Format zugänglich gemacht werden. Einen Ansatz hierfür enthält der Entwurf eines Registermodernisierungsgesetzes, bei dem die Einrichtung eines **Datencockpits** geplant ist, eine Informationsquelle in einem Internetportal, die den Einsatz von Identifikatoren (hier der Steuer-ID) für den Betroffenen nachvollziehbar und verständlich macht.[153]

8.9 Ergebnis

Die rechtliche Untersuchung der Regelungen zur Verarbeitung biometrischer Identifizierungsdaten kommt zu dem Ergebnis, dass in vieler Hinsicht gegen die **Vorgaben des nationalen Verfassungsrechts und des Europarechts** verstoßen wird. Dies kann in folgenden Aussagen zusammengefasst werden:

1. Für die eindeutige Identifizierung mit Hilfe von Fingerabdruckdaten genügt der Abdruck eines Fingers. Aus Gründen der Datenminimierung ist daher grds. nur die Speicherung der Minutien eines Ringfingers oder kleinen Fingers zulässig.
2. Das Fehlen einer einschränkenden Abgleichsregelung für biometrische Pass- und Ausweisdaten auf nationaler Regelungsebene mit Sicherheitsdatenbanken außerhalb von Grenzkontrollen verstößt gegen den Zweckbindungsgrundsatz und gegen höherrangiges europäisches Recht.
3. Die generelle Erlaubnis zur Datennutzung für Sicherheitszwecke bei Daten von Flüchtlingen verstößt gegen den Zweckbindungsgrundsatz und gegen das Diskriminierungsverbot wegen Staatsangehörigkeit.
4. Das in der Praxis bestehende unbegrenzte Zugriffsrecht für Geheimdienste auf Lichtbilder von Deutschen im Pass- und Personalausweisregister und auf biometrische Daten von Flüchtlingen im AZR ist unverhältnismäßig.
5. Die automatisierte Gesichtserkennung im öffentlichen Raum muss auch künftig unterbleiben.
6. Die Transparenz der Nutzung biometrischer Identifizierungsdaten muss verbessert werden.

9 Abschließende Bemerkungen

Die staatliche biometrische Identifizierung hat sich in den letzten zwanzig Jahren immer weiter durchgesetzt. Die vorrangigen Motivationen waren die Regulierung des Aufenthaltes sowie die Gewährleistung der Sicherheit. Es ist absehbar, dass der **Siegeszug der biometrischen Identifizierung**, der auch im privaten Bereich stattfindet[154], sich auch in weiteren staatlichen Anwendungen fortsetzen wird.

Diese technische Entwicklung und deren rechtliche Legitimation wurden bisher nur eingeschränkt durch **rechtliche Schutzmaßnahmen** flankiert. Zwar ist in Deutschland noch eine gewisse Hemmung zu

[153] BT-Drs. 19/24226 v. 11.11.2020, dort Art. 2 § 10 OZG-E.
[154] Sieh schon Bäumler u.a., S. 48 ff.

erkennen, wenn es um zentrale zweckübergreifende Datenverarbeitungen geht, die über eindeutige Identifikatoren erschlossen werden. Dass insofern bezüglich biometrischen Identifikatoren eine besondere Zurückhaltung geboten ist, spiegelt sich bisher in der Gesetzgebung jedoch nur begrenzt ab.

Besonders eklatant ist die Missachtung der europa- und verfassungsrechtlichen Vorgaben bei **Drittausländern**, also bei Nicht-EU-Bürgern.[155] Bestehende rechtliche Differenzierungen sind vorrangig von Praktikabilitätserwägungen getrieben und kaum vom Grundrechtsschutz. Dies führt dazu, dass die überkommene Vorstellung vom (Dritt-)Ausländer als Sicherheitsrisiko[156] auch darin einen Ausdruck findet, dass dieser unverhältnismäßig biometrisch erfasst wird.

Es bedarf einer umfassenden Bestandsaufnahme, in welchem Umfang biometrische Identifizierungsdaten in welcher Art und Weise genutzt werden und welche Wirkungen dies für die Sicherheit wie für die Rechte der Betroffenen zur Folge hat. Dabei sind insbesondere Sicherheitszwecke in den Blick zu nehmen. Auf der Basis einer umfassenden **Evaluation der Regelungen** und deren Anwendung bedarf es einer Überarbeitung der geltenden Bestimmungen unter Berücksichtigung der Grundsätze der Zweckbindung, der Transparenz und der Verhältnismäßigkeit.

Welche praktischen Auswirkungen sich aus einer normativ nicht eingehegten Nutzung biometrischer Identifizierungsdaten ergeben können, demonstrieren uns Überwachungsstaaten wie z.B. China, in denen biometrische Identifizierung als zentrales Werkzeug zur Unterdrückung und zur Diskriminierung genutzt wird. Wollen wir Zustände wie solche in China vermeiden, so muss der **demokratische Diskussionsprozess** über die Nutzung biometrischer Identifizierung generell wie insbesondere für staatliche Zwecke intensiviert werden.

[155] So schon Golembiewski/Probst, S. 7
[156] Weichert in Huber, AufenthG, 2010, Vorb §§ 86-91e Rn. 9.

Literatur

Bäumler, Helmut/Gundermann, Lukas/Probst, Thomas, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, 2001, https://www.datenschutzzentrum.de/download/tabga.pdf.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke (Däubler u.a.), EU-Datenschutz-Grundverordnung und BDSG-neu, 2018.

Datenschutzkonferenz (DSK), Positionspapier zur biometrischen Analyse, Version 1, 03.04.2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_positionspapier-biometrie.pdf.

Golembiewski, Claudia/Probst, Thomas (Golembiewski/Probst), Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, 2003, https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf.

Gundermann, Lukas/Probst, Thomas (Gundermann/Probst), Biometrie, in Roßnagel, Alexander, Handbuch Datenschutzrecht, 2003, S. 1967-2016.

Kühling, Jürgen/Buchner, Benedikt (Kühling/Buchner), DS-GVO BDSG, 3. Aufl. 2020.

Hornung, Gerrit, Die digitale Identität, 2005.

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
A-Drs.	Ausschuss-Drucksache
aF	alte Fassung
AFIS	Automatisiertes Fingerabdruck-Identifikationssystem
Art.	Artikel
AsylG	Asylgesetz
ATD/G	Anti-Terror-Datei/-Gesetz
AufenthG	Aufenthaltsgesetz
AZR/G	Ausländerzentralregister/gesetz
BAMF	Bundesamt für Migration und Flüchtlinge
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BKA/G	Bundeskriminalamt/sgesetz
BMG	Bundesmeldegesetz
BND/G	Bundesnachrichtendienst/gesetz
BPolG	Bundespolizeigesetz
BReg.	Bundesregierung
BT-Drs.	Bundestags-Drucksache
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
ca.	circa
CILIP	Civil Liberties and Police (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
DANA	DatenschutzNachrichten (Zeitschrift)
DDR	Deutsche Demokratische Republik
DNA	Desoxyribonukleinsäure
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DSRl-JI	Europäische Datenschutzrichtlinie für Polizei und Justiz
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt
-E	Entwurf (eines Gesetzes)
ED-	erkennungsdienstlich/e
EG	Europäische Gemeinschaften
EL	Estland
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
eu-LISA	European Agency for the operational management of large-scale IT Systems in the area of freedom, security and justice
Fa.	Firma
f/f.	fort-/folgende
Fn.	Fußnote
FRA	European Union Agency for Fundamental Rights
G.	Gesetz
GES	Gesichtserkennungssystem
GRCh	Europäische Grundrechte-Charta

grds.	grundsätzlich
ICAO	International Civil Aviation Organization
ID	Identifikation
i.d.F.	in der Fassung
INPOL	Informationssystem der Polizei
i.S.d.	im Sinne der
IT	Informationstechnik
i.V.m.	in Verbindung mit
JPG	Joint Photographic Experts Group (digitales Bildformat)
Kap.	Kapitel
K&R	Kommunikation und Recht (Zeitschrift)
LAG	Landesarbeitsgericht
LfD	Landesbeauftragter für Datenschutz
lit.	Buchstabe
MAD/G	Militärischer Abschirmdienst/-Gesetz
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarden
m.w.N.	mit weiteren Nachweisen
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NRW	Nordrhein-Westfalen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
PassG	Passgesetz
PAuswG	Personalausweisgesetz
Perso-VO	Personalausweis-Verordnung
RED/-G	Rechtsextremismusdatei/-Gesetz
Rn.	Randnummer
Ro	Rumänien
S.	Seite oder Satz
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SIS-II-B/VO	Verordnung/Beschluss zu SIS II
s.o.	siehe oben
sog.	so genannte/r
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
s.u.	siehe unten
SZ	Süddeutsche Zeitung
TB	Tätigkeitsbericht
u.a.	und Andere, unter anderem
UK	United Kingdom (Großbritannien)
US/A	United States/of America
v.	von
VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Visa-Informationssystem
VO	Verordnung
ZAR	Zeitschrift für Ausländerrecht
z.B.	zum Beispiel