Das Smartphone, bitte!

Digitalisierung von Migrationskontrolle

in Deutschland und Europa

Gesellschaft für Freiheitsrechte

Herausgeberin

Gesellschaft für Freiheitsrechte e.V.
Hessische Straße 10, D – 10115 Berlin.
https://freiheitsrechte.org/.
Telefon +49 30 549 08 10 – 0. Fax +49 30 549 08 10 – 99. info@freiheitsrechte.org.
Dezember 2019.

Die vorliegende Studie dient der Vorbereitung von Klageverfahren und wurde durch den **Digital Freedom Fund** gefördert, https://digitalfreedomfund.org/.

Satz und Gestaltung: Julia Zé, www.juliaze.com.

Die Gesellschaft für Freiheitsrechte e.V.

Die Gesellschaft für Freiheitsrechte e.V. (GFF) koordiniert und finanziert Gerichtsverfahren, um Grund- und Menschenrechte zu verteidigen. Mit ihren Verfahren setzt sich die GFF für die Stärkung von informationeller Selbstbestimmung und Datenschutz, insbesondere im Zusammenhang von Digitalisierung und technischem Wandel ein. Außerdem richten sich viele ihrer Verfahren gegen die Diskriminierung von benachteiligten Gruppen und zur Durchsetzung der Rechte auf soziale Teilhabe. Um gemeinsam gerichtlich gegen Rechtsverletzungen vorzugehen, bringt die GFF geeignete Kläger*innen, zivilgesellschaftliche Partnerorganisationen und exzellente Jurist*innen zusammen. Zu den aktuellen Projekten zählen beispielsweise Klagen gegen die massenhafte Speicherung von Fluggastdaten und Verfassungsbeschwerden gegen den ausufernden Einsatz von Spähsoftware durch Polizeibehörden, zuletzt im neuen Polizeigesetz in Hessen. Außerdem aber auch die Klage einer Journalistin auf gleiche Bezahlung wie ihre männlichen Kollegen.

Die GFF ist eine spendenfinanzierte Organisation. Unterstützen auch Sie die GFF und werden Fördermitglied. https://freiheitsrechte.org/foerdermitglied-werden/

Autorinnen

Anna Biselli ist Journalistin und Informatikerin und schreibt unter anderem für netzpolitik.org. Sie recherchiert und schreibt seit Jahren zu den Digitalisierungsprojekten des Bundesamtes für Migration und Flüchtlinge (BAMF).

Lea Beckmann ist Juristin der GFF und arbeitet schwerpunktmäßig zu Grund- und Menschenrechten, insbesondere zum Diskriminierungsverbot und zu Persönlichkeitsrechten. Sie wird die Klageverfahren der GFF bezüglich der Datenträgerauswertung von Geflüchteten durch das Bundesamt für Migration und Flüchtlinge koordinieren.

Inhalt

A. Einleitung

Für Geflüchtete sind Smartphones wichtige Begleiter vor, während und nach ihrer Flucht. Die digitalen Begleiter dienen dazu, Nachrichten über das Heimatland zu verfolgen, mit der Familie in Kontakt zu bleiben oder als Übersetzungshilfe. Oft bewahren die Geräte auch die wenigen Erinnerungen, die Schutzsuchende auf ihre Reise mitnehmen können: Fotos aus der verlassenen Heimat und von Dokumenten, Nachrichten von Freunden. Sie sind für viele ein unverzichtbares Werkzeug. In den vergangenen Jahren begannen mehrere Staaten, die Smartphones der Einreisenden und Asylsuchenden auszulesen, um Informationen über sie zu bekommen. Stammen sie tatsächlich aus dem angegebenen Land? Aber auch: Über welche Route sind die Geflüchteten ins Land gekommen? Geht von ihnen vielleicht eine Gefahr aus, weil sich Propagandamaterial terroristischer Gruppierungen auf ihrem Gerät befindet?

Smartphones werden so vom unerlässlichen Werkzeug im Alltag zum Einfallstor für eine umfassende staatliche Durchleuchtung des Privatlebens.

Wichtige Fakten in Kürze

Seit dem Jahr 2017 liest auch die zentrale deutsche Migrationsbehörde, das Bundesamt für Migration und Flüchtlinge (BAMF) zur Herkunfts- und Identitätsbestimmung routinemäßig Daten von elektronischen Geräten aus und analysiert sie. Das tut es, wenn ein Asylsuchender keinen gültigen Pass oder kein Passersatzdokument vorlegen kann – ohne konkreten Verdacht, dass die von den Registrierten gemachten Herkunftsangaben nicht der Wahrheit entsprechen könnten.

Das kann eine Vielzahl Geflüchteter betreffen: Im Jahr 2018 konnten 54,2 Prozent,[1] im ersten Quartal 2019 sogar 55,4 Prozent der Erstantragsteller*innen keinen gültigen Pass, Passersatz oder Personalausweis vorlegen.[2] Warum Geflüchtete keine Identitätsdokumente vorweisen können, kann dabei viele Gründe haben: Manche verlieren ihren Pass während der Flucht oder Schleuser*innen konfiszieren ihre Papiere. Manche kommen aus Ländern, in denen es nicht üblich ist, überhaupt einen Pass zu besitzen. Oder stammen aus Regionen, bei denen die Echtheit eines Ausweisdokuments kaum bestimmt werden kann und die deshalb vom BAMF nicht anerkannt werden.

Diese Datenträgerauslesung betrifft vor allem Smartphones. Werden Geflüchtete aufgefordert, ihre Handys herauszugeben, dann sind sie rechtlich verpflichtet, dem Folge zu leisten. Genutzt werden dürfen die Daten anschließend rechtlich nur, um gemachte Angaben zu Namen oder Herkunftsland zu plausibilisieren. Das Ergebnis der Prüfung hat keinen Beweiswert im Asylverfahren, sondern lediglich Indizwirkung.

[1] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 8.

[2] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Frage 5.

In etwa einem Viertel der Fälle scheitern die Datenträgerauslesungen bereits technisch. Von Januar 2018 bis Juni 2019 wurden insgesamt etwa 17.000 Datenträger erfolgreich ausgelesen.[3] Seit Beginn der Datenträgerauswertungen waren diese durchschnittlich nur in weniger als der Hälfte der Fälle brauchbar und nur in ein bis zwei Prozent der Fälle ergab sich aus der Auswertung ein Widerspruch zu gemachten Angaben. In allen übrigen Fällen bestätigte der Test das, was Asylsuchende vorgetragen hatten.

Dem stehen Kosten von insgesamt 11,2 Millionen Euro von der Einführung 2017 bis Ende 2019 gegenüber. Jährlich kommen für den Support der Systeme weitere Kosten in Höhe von schätzungsweise zwei Millionen Euro hinzu.[4]

Für die Datenauswertung werden zunächst die Daten vom Gerät ausgelesen, durch eine spezielle Software analysiert und das Ergebnis der Analyse dann gespeichert und gegebenenfalls später herangezogen. Gegenstand der Untersuchung sind die Ländervorwahlen von Kontakten im Adressbuch sowie von aus- und eingehenden Nachrichten und Anrufen, außerdem die Länderendungen der im Internetbrowser aufgerufenen Websites. Ebenfalls dargestellt werden Lokationsdaten aus Fotos sowie möglicherweise auch aus Apps. Im Klartext angezeigt werden zudem verwendete Login-Namen und E-Mail-Adressen von Apps, etwa der Facebook-Profilname oder der in einer Dating-App verwendete Name. Schließlich analysiert ein spezielles Programm die in Textnachrichten verwendete Sprache.

Die Geeignetheit der Auswertungen dieser genannten Daten, um Herkunft oder Identität einer Person zu überprüfen, wird von Expert*innen aus unterschiedlichen Gründen als gering eingeschätzt. Es besteht derzeit keine Möglichkeit, die zur Zuverlässigkeit gemachten Angaben des BAMF zu überprüfen, da die Behörde sich weigert, die Algorithmen und technischen Details offen zu legen. Das erschwert allen Beteiligten im Asylverfahren, die Aussagekraft der Ergebnisse sachgerecht einschätzen zu können.

Kern der verfassungs- und datenschutzrechtlichen Kritik

Die Praxis des Bundesamts verletzt nach Einschätzung der GFF damit das Grundrecht auf Integrität und Vertraulichkeit von informationstechnischen Systemen und das Recht auf informationelle Selbstbestimmung. Das migrationspolitische Ziel der gesetzlichen Regelung, die unberechtigte Gewährung von Asylanträgen zu verhindern und abgelehnte Asylsuchende schneller abschieben zu können, rechtfertigt einen anlasslosen, flächendeckenden und derart intensiven

[3] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 9; BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Frage 6 b); BT-Drs. 19/13945: Ergänzende Informationen zur Asylstatistik für das zweite Quartal 2019, Antwort auf Frage 6.

[4] BT-Drs. 19/1663: Einsatz von Spracherkennungssoftware durch das Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 13; BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 15.

Grundrechtseingriff nicht. Gleichzeitig haben die betroffenen Menschen keine wirksame Möglichkeit, sich gegen die Maßnahme zu wehren. Aufgrund des hohen Anteils unbrauchbarer Prüfberichte und einer als gering einzuschätzenden Zuverlässigkeit auch der übrigen Ergebnisse ist zu bezweifeln, ob die Handyauswertung überhaupt geeignet ist, belastbare Anhaltspunkte für die Identität und Herkunft der Schutzsuchenden zu erlangen. Die Folgen falscher Ergebnisse können demgegenüber fatal sein: Kommt es zu Fehlern bei der Auswertung oder der Interpretation der Ergebnisse, kann das zu Misstrauen gegenüber den Antragsteller*innen führen und ihre Asylanträge in Gefahr bringen.

Die Datenverarbeitung durch das BAMF steht damit auch im Widerspruch zu diversen datenschutzrechtlichen Grundsätzen, insbesondere der Datenminimierung und der Zweckangemessenheit der Maßnahmen, aber auch der Transparenz und Nachvollziehbarkeit von Datenverarbeitung.

Faktische Rechtsschutzlücke für Asylsuchende als Einfallstor

Bei kaum einer anderen gesellschaftlichen Gruppe sind verdachtsunabhängige und derartig intensive Rechtseingriffe vorstellbar, wie sie mit den Datenträgerauswertungen des BAMF verbunden sind – ohne dass die Rechts- und vor allem Verfassungsmäßigkeit durch Gerichte überprüft würde. Das hängt maßgeblich damit zusammen, dass der Zugang zu effektivem Rechtsschutz für Asylsuchende faktisch stark eingeschränkt ist. Sie kommen in einem neuen Land an, dessen Sprache sie erst erlernen und dessen Rechtssystem ihnen fremd ist. Sie sind möglicherweise traumatisiert, befinden sich in einer finanziell prekären Situation und müssen viele Schwierigkeiten im Alltag meistern. Außerdem sind sie im Asylverfahren und darüber hinaus besonders von Deutschland als ihrem Gastland abhängig und auch deshalb weniger geneigt, den Klageweg zu beschreiten. Schließlich wird eine grundsätzliche gerichtliche Klärung der Rechtmäßigkeit der Auswertung ihres Handys viele Jahre in Anspruch nehmen und damit in ihrem persönlichen Fall zu spät kommen.

Diese faktische Rechtsschutzlücke einer besonders vulnerablen Gruppe der Gesellschaft führt dazu, dass das BAMF aktuell an ihnen neue Formen staatlicher Überwachung austesten kann. Erfahrungen mit anderen invasiven staatlichen Maßnahmen in Deutschland, aber auch speziell mit der Handydatenauslesung in anderen Ländern zeigen, dass der Anwendungsbereich solcher Maßnahmen nach ihrer Einführung oftmals ausgebaut wird. In Großbritannien beispielsweise werden standardmäßig die Handys von Opfern sexueller Gewalt ausgelesen, um die Daten als Beweismittel im Strafverfahren zu verwenden.[5]

[5] Big Brother Watch UK (2019): Digital Strip Watch. The Police's Data Investigation of Victims.

Hintergrund und Ziel dieser Studie

Die Gesellschaft für Freiheitsrechte e.V. (GFF) will einen Beitrag dazu leisten, diese faktische Rechtsschutzlücke zu schließen und ähnlichen Entwicklungen vorzubeugen. Sie bereitet deshalb gemeinsam mit betroffenen Personen und engagierten Kooperationsanwält*innen rechtliche Schritte gegen die Auslesung der Datenträger von Asylsuchenden durch das BAMF vor. Über den staatlichen Zugriff auf sensible Daten ist nur wenig bekannt. Daher hat die GFF zusammen mit der Journalistin und Informatikerin Anna Biselli das Vorgehen des BAMF in einer umfassenden Recherche untersucht, deren Ergebnisse sie vorliegend veröffentlicht.

Langfristiges Ziel der geplanten Klagen ist es, die Verfassungsmäßigkeit der Rechtsgrundlage durch das Bundesverfassungsgericht überprüfen zu lassen, welches als einziges Gericht eine gesetzliche Grundlage „kassieren", also für nichtig erklären kann. Dafür muss eine Person, deren Handydatenauslesung von der Rechtsgrundlage gedeckt war, vor dem Verwaltungsgericht klagen. Wenn die Verwaltungsgerichte das Verfahren nicht selbst dem Bundesverfassungsgericht vorlegen, ist erst nach Ausschöpfung des Rechtsweges eine Beschwerde dorthin möglich. In weiteren Fallkonstellationen kann es zudem bereits kurzfristig sinnvoll sein, die Grenzen des Anwendungsbereichs der derzeit geltenden gesetzlichen Regelung zu klären und auf eine enge Auslegung zu drängen. Die GFF hofft zudem, bereits im Rahmen der instanzengerichtlichen Klageverfahren weitergehende Informationen über verwendete Algorithmen und technische Details zu erlangen.

Finanzierung

Die GFF ist eine gemeinnützige Organisation und finanziert sich in etwa gleichen Teilen aus Beiträgen ihrer Fördermitglieder, Einzelspenden und institutionellen Förderungen von unterschiedlichen Stiftungen. Diese Studie wurde durch eine Förderung des Digital Freedom Fund (DFF) ermöglicht.

Unterstützen auch Sie die GFF bei dieser Arbeit und werden Fördermitglied.

https://freiheitsrechte.org/foerdermitglied-werden/.

Methoden und Quellen

Für diese Studie hat die GFF in einer umfassenden Recherche verfügbare Quellen ausgewertet. Dazu gehören Dokumente aus dem Gesetzgebungsverfahren und Stellungnahmen von Rechtswissenschaftler*innen, Flüchtlingsorganisationen und Verbänden. Grundlage der Studie sind weiter Informationen, die durch parlamentarische Anfragen im Bundestag und Landesparlamenten öffentlich wurden. Einbezogen wurden zudem die Erkenntnisse aus vielfältigen Hintergrundgesprächen mit Geflüchteten, Anwält*innen und Rechtswissenschaftler*innen, Verfahrensberatungsstellen und Menschenrechtsorganisationen in Deutschland und anderen Ländern Europas. Diese Gespräche sowie eingesehene Auswertungsberichte und Asylakten vervollständigten das Bild von der Nutzung der Datenträgerauswertung in der Praxis. Mitarbeitende des BAMF lehnten Einladungen zu Gesprächen ab. Anschließend an vorherige Recherchen von Anna Biselli und zahlreiche Informationsfreiheitsanfragen konnten aber behördliche Dokumente des BAMF miteinbezogen werden, darunter interne Dienstanweisungen zur Dokumentenprüfung, Identitätsfeststellung und zum Auslesen mobiler Datenträger, sowie ein Benutzerhandbuch zum Auslesen mobiler Datenträger und umfangreiche Schulungsunterlagen für BAMF-Mitarbeitende.

B. Datenträgerauswertung in Deutschland

Vereinbarkeit mit Grund- und Menschenrechten

Will der Staat Datenträger Geflüchteter auslesen und auswerten, schränken insbesondere Grundrechte dieses Handeln ein: Das im Grundgesetz verbürgte Allgemeine Persönlichkeitsrecht verpflichtet den Staat, die Grundbedingungen der freien Persönlichkeitsentfaltung und Selbstbestimmung zu schützen (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Daraus folgt auch, dass der Staat das Recht des Einzelnen schützen muss, über die seine Person betreffenden Daten selbst zu bestimmen (sog. „informationelle Selbstbestimmung").[6] Weil sich in informationstechnischen Systemen eine Vielzahl persönlicher Daten aus unterschiedlichen Lebensbereichen zusammenfindet, muss der Staat die Vertraulichkeit und Integrität dieser Systeme besonders gewährleisten (sog. „Computer-Grundrecht").[7]

Die Auswertung von Smartphones, in welchen sich eine Vielzahl sensibler Daten aus unterschiedlichsten Lebensbereichen bündeln, stellt unzweifelhaft einen gravierenden Grundrechtseingriff dar. Dass die Maßnahmen flächendeckend und anlasslos, also ohne konkrete Verdachtsmomente, durchgeführt werden, wiegt zusätzlich schwer.

Das Ziel, die unberechtigte Gewährung von Asylanträgen zu verhindern und abgelehnte Asylsuchende schneller abschieben zu können, vermag einen derart intensiven Rechtseingriff nicht zu rechtfertigen. Das Bundesverfassungsgericht hat in mehreren Entscheidungen betont, dass der staatliche Zugriff auf IT-Systeme nicht zu jedem beliebigen politischen Ziel zulässig ist, sondern nur zum Schutz überragend wichtiger Rechtsgüter.[8] Die bezweckten migrationspolitischen Ziele lassen sich nicht etwa mit der Verhinderung oder Verfolgung schwerster Straftaten vergleichen.

Auch fehlen im Gesetz die grundrechtssichernden Verfahrensregelungen, die beim Zugriff auf persönliche Datenbestände nach ständiger Rechtsprechung geboten sind.[9] Die Vorgabe, dass nur Volljurist*innen innerhalb des BAMF den Ergebnisbericht zur Verwendung im Asylverfahren freigeben dürfen, bietet gerade nicht die Gewähr einer gebotenen unabhängigen Kontrolle der Rechtmäßigkeit der Maßnahmen.

Die Datenverarbeitung durch das BAMF läuft damit auch diversen datenschutzrechtlichen Grundsätzen zuwider, etwa denen der Zweckangemessenheit und Datenminimierung aber auch der Transparenz und Nachvollziehbarkeit von Datenverarbeitung.

---

[6] Grundlegend dazu das „Volkszählungsurteil" des Bundesverfassungsgerichts, BVerfG, NJW 1984, 419.

[7] Grundlegend dazu BVerfG, NJW 2008, 822 <827>.

[8] BVerfGE 141, 220 <304 f.>.

[9] BVerfGE 65, 1 <46>; 113, 29 <57 f.>; 120, 351 <361>.

Die Rechtsgrundlage: Was darf das BAMF?

Dennoch hat der Bundestag das Auslesen von Datenträgern gesetzlich ausgestaltet: Im Juli 2017 trat das „Gesetz zur besseren Durchsetzung der Ausreisepflicht" in Kraft. Durch dieses Gesetz wurden unter anderem die Bestimmungen zu Abschiebehaft und Ausreisegewahrsam ausgeweitet sowie die Befugnisse zur Datenweitergabe des BAMF an andere Behörden erweitert.

Zusätzlich wurde die Möglichkeit gesetzlich eingeführt, Datenträger von Geflüchteten auszulesen. Dafür wurde § 15 AsylG ergänzt, der die Pflichten eines Asylsuchenden regelt, bei der Ermittlung des Sachverhalts im Rahmen des Asylverfahrens mitzuwirken. Asylantragsteller*innen, die keinen gültigen Pass oder Passersatz vorweisen können, sind nunmehr verpflichtet, auf Verlangen alle Datenträger, die für die Feststellung ihrer Identität und Staatsangehörigkeit von Bedeutung sein können, vorzulegen, auszuhändigen und zu überlassen. Diese Auswertung von Datenträgern ist nur zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit erforderlich ist „und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann" (§ 15a AsylG).

Die gesetzlichen Regelungen beschränken die Maßnahme nicht auf Smartphones, der Begriff „Datenträger" ermöglicht grundsätzlich ebenso die Auswertung einer Vielzahl anderer Geräte, etwa als Featurephone bezeichnete einfachere Modelle von Mobiltelefonen, aber auch USB-Sticks, Festplatten, Laptops oder sogar Fitnessarmbänder.

Datenträger dürfen nur dann ausgewertet werden, wenn keine tatsächlichen Anhaltspunkte für die Annahme vorliegen, dass „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden". Dennoch erlangte Kenntnisse aus dieser Sphäre dürfen nicht verwertet und müssen gelöscht werden (§ 48 Abs. 3a S. 2-4 AufenthG). Die Datenträger dürfen zudem „nur von einem Bediensteten ausgewertet werden, der die Befähigung zum Richteramt hat" (§ 48 Abs. 3a S. 5 AufenthG) – eine Regelung, die an einen Richter*innenvorbehalt angelehnt ist.

Das Gesetz verpflichtet betroffene Personen, Zugangsdaten zur Verfügung zu stellen, die für die Auswertung des Datenträgers notwendig sind. Geschieht dies nicht, dürfen die jeweiligen Behörden bei den Telekommunikationsdienstleistern Auskunft über die entsprechenden Zugangsdaten verlangen, etwa PIN- und PUK-Codes für SIM-Karten oder Passwörter (§§ 48 Abs. 3a S. 3, 48a Abs. 1 AufenthG).

In der Begründung des Gesetzentwurfs der Bundesregierung wird im Rahmen des Erfüllungsaufwandes angenommen, dass eine Datenträgerauswertung bei 50 bis 60 Prozent der Antragsteller*innen angezeigt sei. Basierend auf der Anzahl von 280.000 registrierten Asylsuchenden

im Jahr 2016 ging die Bundesregierung von jährlich 150.000 Personen aus, bei denen eine Datenträgerauslesung in Betracht käme.[10]

Das BAMF, eine Behörde unter Druck

Fast eine halbe Million Geflüchtete stellte im Jahr 2015 einen Asylerstantrag in Deutschland, mehr als doppelt so viele wie im Jahr zuvor. Bis zum Ende des entsprechenden Jahres waren noch 337.331 Erstverfahren anhängig, die durchschnittliche Verfahrensdauer betrug 7,9 Monate.[11] Die unerledigten Fälle stapelten sich. Zusätzlich geriet die Behörde durch Medienberichte unter Druck, die das BAMF als überforderte Behörde darstellten: „Chaos und Überforderung bei der Annahme von Asylanträgen" – so und so ähnlich lauteten die Schlagzeilen über viele Monate hinweg.[12] Personalräte des Bundesamtes verfassten im November 2015 einen offenen Brief an die Behördenleitung, in dem sie die mangelnde Qualifizierung von durch Schnelllehrgänge geschleustem Personal und „systemische Mängel" anprangerten.[13] Hinzu kamen Fälle wie der von Franco A., einem deutschen Soldaten, der sich gegenüber dem BAMF als syrischer Asylbewerber ausgab und 2016 einen Schutzstatus zuerkannt bekam. Der Oberstleutnant der Bundeswehr soll aus einer rechtsextremen Gesinnung heraus einen Anschlag geplant haben.[14] Dass eine solche Täuschung möglich war, verursachte in einer breiten Öffentlichkeit Zweifel an der Qualität der Asylentscheidungen.[15]

Das BAMF stand unter Handlungsdruck. Die Einführung verschiedener IT-Assistenzsysteme sollte Entscheidungen beschleunigen und die Qualität der Entscheidungen erhöhen.[16] Automatischer Lichtbildabgleich, Dialekt- und Namensanalyse sowie die Datenträgerauswertung wurden eingeführt und im Juli 2017 in der Außenstelle Bamberg vorgeführt – etwa zwei Monate vor der anstehenden Bundestagswahl.[17] „Ein Fall wie Franco A. kann nicht mehr passieren", resümierte der BAMF-Vizepräsident Dr. Markus Richter im November 2018 gegenüber der Frankfurter Allgemeinen Zeitung,[18] die Behörde präsentiert sich mittlerweile als Vorreiter in der Behördendigitalisierung.[19]

[10] BT-Drs. 18/11546: Gesetzentwurf der Bundesregierung, Gesetz zur besseren Durchsetzung der Ausreisepflicht, S. 15.

[11] BAMF (2016): Das Bundesamt in Zahlen 2015.

[12] Siehe unter anderem J. Bock: Chaos und Überforderung bei der Annahme von Asylanträgen, Stuttgarter Nachrichten, 21.12.2015.

[13] Gesamt-Personalrat und Örtlicher Personalrat des BAMF (2015): Offener Brief an den Leiter des BAMF, veröffentlicht auf tagesschau.de.

[14] Generalbundesanwalt: Anklage wegen des Verdachts der Vorbereitung einer schweren staatsgefährdenden Gewalttat, 12.12.2017.

[15] Siehe unter anderem A. Reimann: Wie leicht kann man sich ins Asylverfahren einschleichen?, Spiegel, 17.5.2019.

[16] Bundesministerium des Innern: Meldung: Neue IT-Assistenzsysteme im BAMF, 6.12.2017.

[17] BAMF: Meldung. Moderne Technik in Asylverfahren, 26.07.2017.

[18] B. Beeger, T. Neuscheler: „Ein Fall wie Franco A. kann nicht mehr passieren", Frankfurter Allgemeine Zeitung, 6.11.2018.

[19] BAMF: Meldung: BAMF-IT: Am Puls der Zeit, 17.07.2019.

Die Praxis: Wie das BAMF Datenträger Geflüchteter ausliest und analysiert

Die Regelungen im Gesetz zur besseren Durchsetzung der Ausreisepflicht enthalten keine genauen Vorgaben zum Ablauf der Auslesung und Auswertung der Datenträger. Aufschluss gibt ein Blick in die internen Dienstanweisungen des BAMF zur „Identitätsfeststellung“[20] und zum „Auslesen von mobilen Datenträgern“[21] sowie in Handbücher und Schulungsunterlagen.[22]

Auch wenn das BAMF laut Gesetz Datenträger aller Art auswerten dürfte, analysiert die Behörde derzeit nur Smartphones und sogenannte Featurephones, einfachere Handys mit geringerem Funktionsumfang. Der Prozess der Datenträgerauswertung lässt sich in drei Phasen unterteilen: Die Auslesung, die automatische Analyse und die Auswertung der Analyseergebnisse.

Ob ein Datenträger ausgelesen wird, entscheidet sich in der Regel direkt bei der Registrierung der Antragsteller*innen – vor der Asylanhörung. Kann ein*e Geflüchtete*r keinen gültigen Pass oder Passersatzdokumente vorzeigen, kommt eine Auslesung in Betracht. Auch die mobilen Endgeräte von Kindern können ausgelesen werden, insbesondere wenn niemand sonst in deren Familie im Besitz eines solchen ist, so eine Dienstanweisung. „Die Extraktion mobiler Geräte hat keine Altersgrenze“, heißt es in der Bestimmung.

Die registrierte Person wird von Mitarbeitenden des Asylverfahrenssekretariats dazu aufgefordert, ihr Gerät auszuhändigen und auf ihre gesetzliche Pflicht hierzu hingewiesen. Ihre Zustimmung wird durch eine Unterschrift dokumentiert.[23] Die betroffene Person muss bei diesem Prozess mitwirken und das Gerät entsperren sowie bestimmte Geräteeinstellungen durchführen, die das Auslesen ermöglichen.

Anschließend werden die Daten in Anwesenheit des*der Betroffenen extrahiert und dafür an einen speziellen Computer angeschlossen. Ist die Auslesung erfolgreich, werden die extrahierten Daten automatisch zu einem Ergebnisreport zusammengefasst und in einem sogenannten „Datentresor“ gespeichert. Der*die BAMF-Mitarbeitende kann den Report zu diesem Zeitpunkt nicht einsehen. Die Rohdaten werden nach Erstellung des Ergebnisreports laut Angaben des BAMF umgehend gelöscht, der*die Antragsteller*in bekommt das Gerät unmittelbar nach dieser Durchführung zurück.

---

[20] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

[21] BAMF: Dienstanweisung für das AVS – Auslesen von mobilen Datenträgern.

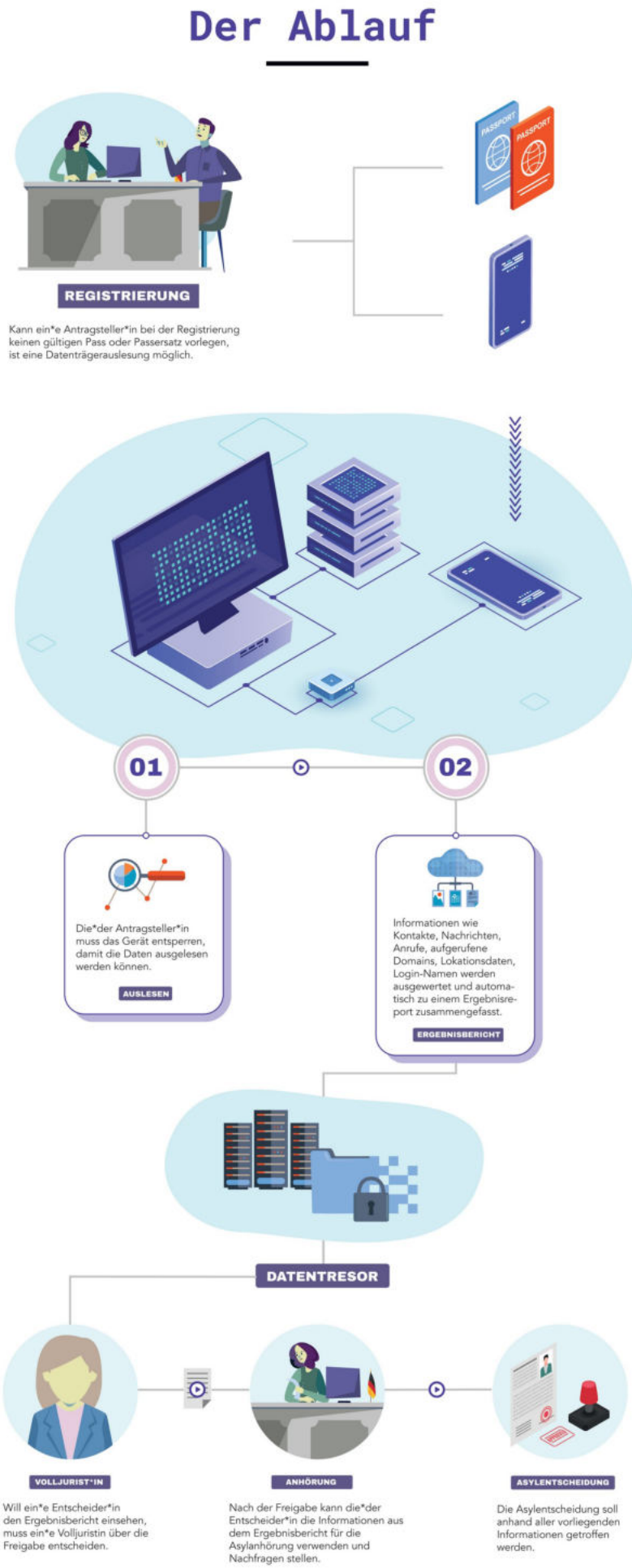
[22] BAMF: Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität, Sicherheitsaspekte. Einführung in die neuen IT-Tools, 30.08.2017.

[23] BAMF: Formular D1705.

Kommt ein*e Asylentscheider*in zum Ergebnis, dass er*sie die Ergebnisse der Analyse nicht benötigt, weil sich die Identität durch sonstige Anhaltspunkte ausreichend bestimmen lässt, veranlasst er*sie über ein Ticketsystem die Löschung des Reports. Will er*sie die Ergebnisse jedoch verwenden, muss er*sie die Freigabe des Reports beantragen.[24]

Ein*e beim BAMF beschäftigte*r Jurist*in mit Befähigung zum Richteramt – Volljurist*in – entscheidet nach einer Prüfung auf „Erforderlichkeit und Verhältnismäßigkeit" die Anfrage und gibt gegebenenfalls den Report zur Auswertung frei. Verweigert er*sie die Freigabe, müssen die Daten gelöscht werden.[25] Ist die*der Entscheider*in selbst Volljurist*in, kann er*sie eigenständig über die Freigabe entscheiden.

Das dürfte nur in Ausnahmefällen gegeben sein: Ein Abschluss in einem juristischen Studiengang ist nicht Voraussetzung für die Tätigkeit als Entscheider*in. Mindestqualifikation ist ein abgeschlossenes Bachelor-Studium, welches der Fachrichtung des gehobenen nichttechnischen Verwaltungsdienstes zuge-



[24] BAMF: Formular D1735.
[25] BAMF: Formular D1706.

ordnet werden kann.[26] Im Falle einer Freigabe wird der Report vom Datentresor in das elektronische Aktensystem MARiS (Migrations-Asyl-Reintegrationssystem) importiert, im Datentresor gelöscht und der Asylakte hinzugefügt. Der Report kann dann zur Vorbereitung der Asylanhörung genutzt werden. Je nach Aussage des Reports kann die*der Entscheider*in die Ergebnisse in eine von drei Kategorien einordnen. Erstens, der Report stützt die Angaben des*der Antragstellers*in, zweitens, der Report stützt die Angaben des*der Antragstellers*in nicht und drittens, keine verwertbaren Ergebnisse. Sobald der Report in die Asylakte eingegangen ist, wird er nicht mehr gelöscht - auch dann nicht, wenn sich die Ergebnisse als unbrauchbar erweisen. Ab dann gelten die regulären Löschfristen für Asylakten. Laut § 7 Abs. 3 AsylG sind Asylverfahrensakten spätestens zehn Jahre nach Abschluss des Asylverfahrens zu vernichten sowie in den Datenverarbeitungssystemen des Bundesamtes zu löschen. Kürzere Fristen gelten nur im Ausnahmefall, zum Beispiel wenn eine Einbürgerung erfolgt.

Der*die Anhörer*in, die nicht immer personenidentisch mit dem*der Entscheider*in ist, kann dem*der Antragsteller*in auf Basis des Ergebnisreports Fragen zu eventuellen Widersprüchen zu gemachten Identitäts- und Herkunftsangaben stellen, soll den Report aber nicht aushändigen.

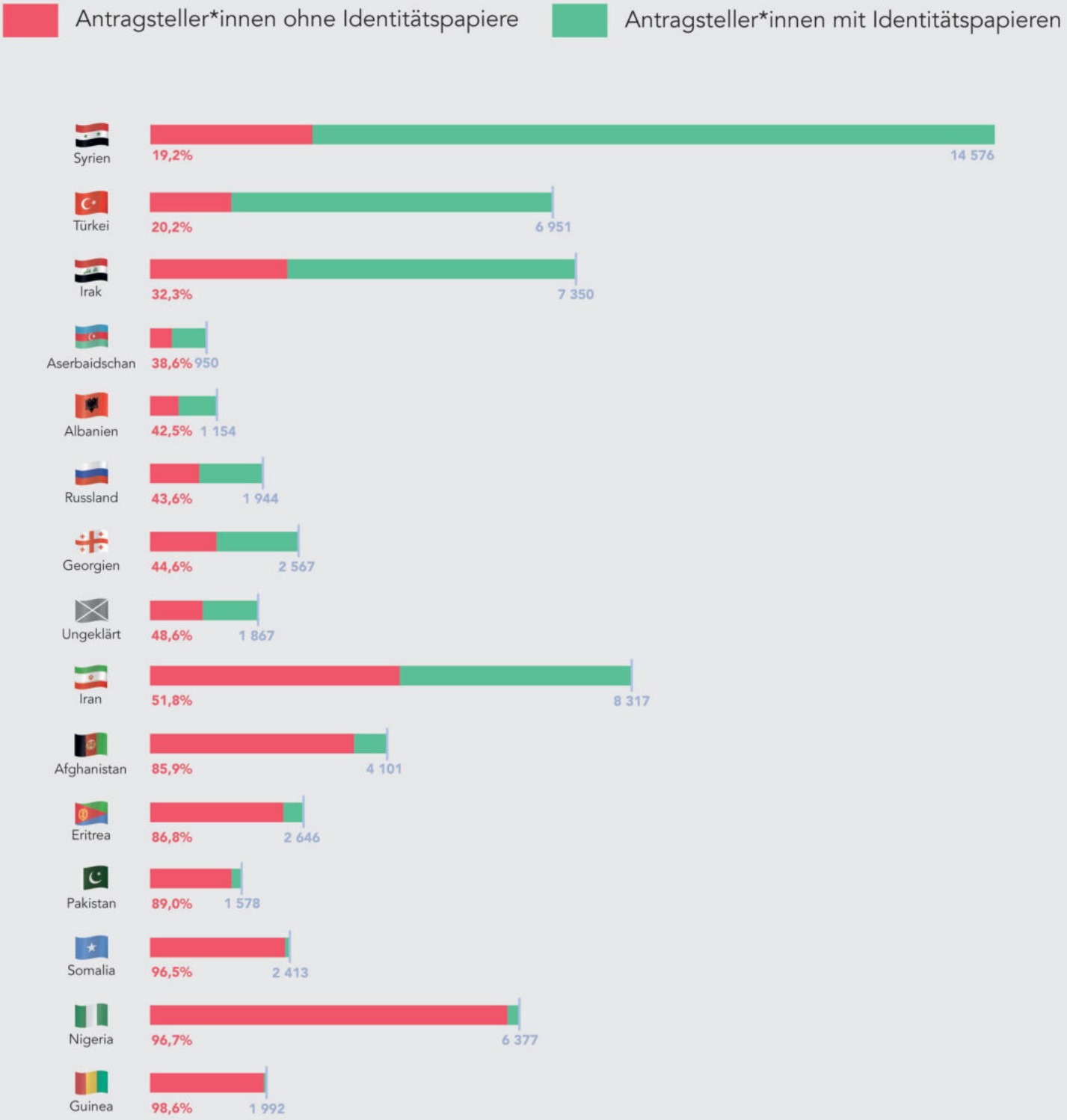
Kein Pass, kein Ausweis: Wen betrifft das?

Statistiken des Innenministeriums zufolge konnten im Jahr 2018 54,2 Prozent der Antragsteller*innen keine Identitätspapiere vorlegen;[27] im ersten Quartal 2019 waren es sogar 55,4 Prozent.[28] Diese Quote schwankt stark je nach Herkunftsland. Der Großteil aus Syrien geflüchteter Personen legte im Jahr 2018 Identitätspapiere vor, nur bei 19,2 Prozent waren diese nicht vorhanden. Bei Antragsteller*innen aus Nigeria wurden im gleichen Jahr jedoch 86,8 Prozent ohne Pass, Passersatz oder Personalausweis registriert, bei Geflüchteten aus Somalia sogar 96,5 Prozent.[29]

Legt ein*e Antragsteller*in keinen gültigen Pass oder Passersatz vor, kann sein*ihr Smartphone ausgelesen werden, wenn es keine milderen Mittel zur Bestimmung von Identität und Herkunft gibt. Als mildere Mittel kommen laut der Dienstanweisung für die Identitätsfeststellung jedoch nur Dokumente in Betracht, „die durch ein Lichtbild die Identität belegen können und vom Bundesamt auf ihre Echtheit überprüft werden können."

[26] BT-Drs. 18/10786: Befristete Beschäftigungsverhältnisse beim Bundesamt für Migration und Flüchtlinge, 30.12.2016, Antwort auf Frage 6.
[27] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 8.
[28] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Fragen 5 und 6.
[29] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 8.

Registrierte Asyl-Erstantragsteller*innen ab 18 Jahre im Zeitraum Januar-Dezember 2018



Quelle: BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 8.

Als Passersatz gelten beispielsweise Flüchtlingsausweise, Personalausweise, aber auch Personenstandsurkunden wie Geburts- oder Heiratsurkunden können eine Identität bestätigen. Doch auch manche Asylsuchende, die gültige Dokumente ihres Herkunftslandes haben, müssen ihre Geräte herausgeben. Aus internen Dienstanweisungen des BAMF geht hervor, dass es ausreicht, wenn eine andere Behörde diese Papiere aktuell einbehalten hat, um zur Identitätsfeststellung bei der Registrierung Handydaten auszulesen.

Zudem werden die Pässe mancher Staaten in Deutschland nicht anerkannt; Staatsangehörige dieser Länder müssen immer mit einer Auslesung ihrer Datenträger rechnen.[30] Welche Pässe und Ersatzdokumente in Deutschland anerkannt werden, regelt das Bundesinnenministerium im Einvernehmen mit dem Auswärtigen Amt in ständig aktualisierten Allgemeinverfügungen. Die Eignung als Identitätsnachweis beruht auch auf „einer Einschätzung zu staatlichen Strukturen und Dokumentenwesen hinsichtlich des Korruptionsindexes des jeweiligen Ausstellerlandes".[31] Aus diesen Allgemeinverfügungen ergibt sich unter anderem, dass somalische Pässe und Passersatzpapiere, die nach dem 31. Januar 1991 ausgestellt oder verlängert wurden, nicht anerkannt werden.[32] Ebenso ausgeschlossen werden durch die Verfügungen etwa Dokumente, die nach 2015 in vom IS-besetzten Gebieten des Irak, oder Pässe und Passersatzpapiere, die von Taliban-Büros in Afghanistan ausgestellt wurden.

Zudem lässt sich die Validität der Pässe mancher Länder aus technischen Gründen nicht unmittelbar vor Ort feststellen; auch in diesen Fällen liest das BAMF die Datenträger der betroffenen Personen aus: Pässe und Passersätze werden mit einer physikalisch-technischen Untersuchung (PTU) auf ihre Echtheit geprüft. Insgesamt existieren drei Prüfebenen, wie aus der der Dienstanweisung „Asylverfahren – Urkunden- und Dokumentenprüfung"[33] hervorgeht. Wenn die Gültigkeit oder Echtheit der Dokumente nicht vor Ort in der ersten Prüfebene abschließend festgestellt werden kann, zieht das BAMF eine Auslesung der Datenträger der Antragsteller*innen in Betracht. Zu den vor Ort untersuchbaren Dokumenten zählen laut der Dienstanweisung maschinenlesbare Dokumente aller Herkunftsländer, zusätzlich alle anderen Dokumente aus Syrien, dem Irak, Iran, Eritrea, der Ukraine, Afghanistan und der Russischen Föderation.

Geflüchteten mit allen anderen Arten von Identitätsdokumenten droht die unmittelbare Auslesung ihrer Datenträger. Zusätzlich werden ihre Dokumente an ein Prüfzentrum geschickt, das die zweite Prüfebene darstellt. Lässt sich auch dadurch die Echtheit der Papiere nicht bestäti-

[30] BAMF: Dienstanweisung Asylverfahren – Urkunden- und Dokumentenprüfung.

[31] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

[32] Bundesministerium des Innern, Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes vom 06.04.2016, BAnz AT 25.04.16 B1. Ausnahme sind 2013 ausgestellte Passmodelle, s. Bundesministerium des Innern, Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes vom 05.04.18, BAnz AT 13.04.18 B7.

[33] BAMF: Dienstanweisung Asylverfahren – Urkunden- und Dokumentenprüfung.

gen oder besteht Manipulationsverdacht, nimmt das PTU-Referat in Nürnberg als dritte Prüfebene die abschließende Beurteilung vor. Stellt sich ein Dokument in der zweiten oder dritten Prüfebene als echt heraus und wäre die erfolgte Datenträgerauslesung also entbehrlich gewesen, soll sich die Begründung der Asylentscheidungen nur noch auf die aus dem Identitätsdokument erwiesene Herkunftsangabe beziehen.[34] In der zentralen Asylanhörung lag der Prüfbericht jedoch möglicherweise bereits auf dem Tisch des*r Entscheiders*in. Zusammengefasst: Es kann passieren, dass ein*e Geflüchtete*r sehr wohl einen gültigen Ausweis hat oder sogar vorlegt – dieser aber schlichtweg bei der Registrierung nicht zum Tragen kommt und ein Datenträger trotzdem ausgelesen wird.

Erfahrungsbericht: Sorgen um private Fotos und Auslesungen, die nie verwendet werden

In der Außenstelle des BAMF im Ankunftszentrum Bielefeld finden Antragstellung und Anhörung häufig am selben Tag statt. Einer Verfahrensberaterin hat mit der GFF über ihre Erfahrungen gesprochen. Sie begleitete einen Geflüchteten zum BAMF, er war etwa Anfang 20 und stammt aus Nigeria. Der Mann hatte kein Passdokument dabei, lediglich einen Zeitungsausschnitt mit Bild aus seinem Herkunftsland, auf dem er abgebildet war. Zwischen der Antragstellung und der am gleichen Tag nachfolgenden Anhörung wurde sein Handy ausgelesen. Dabei saßen ihm Dolmetscher und die Person, die seinen Asylantrag aufgenommen hat, gegenüber und teilten ihm mit, dass sein Smartphone ausgelesen werden solle. Er solle sagen, seit wann er das Gerät besitze und wo er es herhabe. Ihm wurde nicht erklärt, was genau passieren würde.

Der Antragsteller habe sich Sorgen gemacht, da sich auf seinem Gerät auch private Fotos und Videos befunden hätten. Das erzählte er der Verfahrensberaterin anschließend im Warteraum. In der Situation traute er sich nicht, auch nur nachzufragen. Sein Smartphone wurde an einen Computer angeschlossen, das Auslesen dauerte etwa fünf bis zehn Minuten, dann erhielt er das Gerät zurück. Dass die Mitarbeitenden des BAMF nicht auch seine Fotos oder Inhalte von Nachrichten sehen können, war ihm nicht klar. In der Anhörung, die noch am selben Tag bei einem anderen BAMF-Mitarbeitenden stattfand, wurde nicht auf die Erkenntnisse aus seiner Handynutzung eingegangen. Unklar ist auch, ob es in dieser kurzen Zeit möglich gewesen wäre, die nötige Freigabe durch eine*n Volljurist*in einzuholen.

[34] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

Der Report: Was steht im Ergebnisbericht?

Der Ergebnisbericht enthält zusammengefasste, vor allem statistische Informationen. Es werden gespeicherte Kontakte, jeweils ein- und ausgehende Anrufe und Textnachrichten verschiedener Messenger nach Ländervorwahlen ausgewertet, außerdem wird auch die Anrufdauer nach den Ländervorwahlen ausgewertet. Als Länderhinweis werden ebenso die Top-Level-Domains aufgerufener Internetadressen statistisch aufbereitet und in Tabellen und Tortendiagrammen dargestellt.

Auf einen Blick: Was kann das BAMF auswerten?[35]

- Kontakte im Adressbuch auf Ländervorwahlen
- Ein- und ausgehende Anrufe nach Dauer und Ländervorwahlen
- Ein- und ausgehende SMS und Nachrichten nach Ländervorwahlen
- Sprache in ein- und ausgehenden SMS und Nachrichten
- Browserverlauf nach Länderendungen aufgerufener Websites
- Login-Namen und E-Mail-Adressen, die in Apps verwendet werden
- Lokationsdaten, beispielsweise aus Fotos oder Apps

Geodaten: Wo warst du?

Das BAMF nutzt neben Kontakt- und Anrufinformationen Geolokationsdaten. Die*der Entscheider*in bekommt diese Ortsangaben als Punkte ohne zeitliche Zuordnung oder Quelle auf einer Karte angezeigt. Sie*er weiß also, dass dieser Ort aus Daten auf dem Handy hervorgeht, aber nicht, woher die Information genau stammt oder von wann.

Der BAMF-Vizepräsident Dr. Markus Richter erwähnte gegenüber der FAZ, dass Geodaten von Fotodateien einbezogen würden.[36] Ein vorliegendes Auswertungsprotokoll bestätigt diese Aussage und benennt Fotos als Quelle für gefundene Ortsangaben. Ob darüber hinaus App-Informationen, gespeicherte WLAN-Netzwerke oder aufgezeichnete GPS-Daten betrachtet werden, ist nicht bekannt. Das BAMF gibt hierzu keine Informationen preis.

[35] BAMF: Schulungsunterlagen für Mitarbeitende, Stand 2017, S. 78 und 104.

[36] B. Beeger, T. Neuscheler: „Ein Fall wie Franco A. kann nicht mehr passieren", Frankfurter Allgemeine Zeitung, 06.11.2018.

Der Ergebnisbericht

01

LÄNDERCODES

Statistiken zu Länderkennungen, etwa Vorwahlen, bei Adressbuchkontakten, ein- und ausgehenden Anrufen und Textnachrichten.

02

SPRACHE DER TEXTNACHRICHTEN

Analyse der verwendeten Sprachen in ein- bzw. ausgehenden Textnachrichten. Bei arabischer Sprache erfolgt zusätzlich eine Dialekterkennung.

03

DOMAIN-ENDUNGEN

Domains, die im Browser aufgerufen wurden, werden ebenfalls nach Länderendung ausgewertet.

04

LOKATIONSDATEN

Lokationsangaben aus Apps und Fotos werden als Markierungen auf einer Landkarte dargestellt. Aus welchen Anwendungen diese Daten gewonnen werden können, ist nicht bekannt.

05

LOGIN-NAMEN UND PROFILINFOS

Als Hinweise auf die Identität werden auch Informationen wie Facebook- Profilnamen, Account-IDs oder Mailadressen dargestellt. Auch hier ist nicht bekannt, welche Apps dahingehend ausgewertet werden können.

Sprachanalyse von Textnachrichten: Welche Sprache(n) schreibst du?

Über statistische Informationen hinaus geht die Analyse von Textnachrichten. Die*der Anhörer*in sieht im Ergebnisreport die Häufigkeiten der in diesen jeweils ein- und ausgehenden Nachrichten verwendeten Sprache, bei arabischsprachigen Nachrichten werden zusätzlich ermittelte Dialekte aufgeführt.

Laut einer Antwort des Bundesinnenministeriums aus dem Dezember 2018 kann die Software derzeit zwischen 170 Sprachen und Dialekten unterscheiden.[37] Auf Auswertungsberichten, etwa aus dem Oktober 2019, ist vermerkt: „Auch wenn mehr als 90 Sprachen erkannt werden können, werden nicht alle existierenden Sprachen unterstützt. Sollte eine Sprache dem System nicht bekannt sein, wird es eine dieser am ähnlichsten erscheinende Sprache erkennen." Es lässt sich nicht beurteilen, wie zuverlässig die Erkennung des vom BAMF verwendeten Sprachmoduls ist.

Die Migrationsbehörde verweigert jegliche Auskunft darüber, auf welcher Trainingsdatenbasis und welchen Algorithmen die Spracherkennung beruht und welche Fehlerraten die Erkennung hat. Gerade aufgrund der Vielzahl arabischer Dialekte und einer großen Variation uneinheitlicher Schreibweisen insbesondere in Chatdialekten dürfte eine genaue Sprachidentifikation eine Herausforderung darstellen. Es liegt damit zumindest nahe, dass die Zuordnung mancher Sprachen mit größerer Zuverlässigkeit gelingt als die anderer Sprachen. Solche Ungleichheiten können zu Diskriminierungen führen, weil Muttersprachler*innen mancher Sprachen mit größerer Wahrscheinlichkeit von unzutreffenden Ergebnissen betroffen sind. Forschungsarbeiten zu automatischen Sprachidentifikationssystemen, die auf einer Satzebene zwischen Modernem Hocharabisch und ägyptischem Dialekt unterscheiden sollen, erreichten etwa Genauigkeiten von 85,5 Prozent.[38]

Solange Daten zur Zuverlässigkeit der Spracherkennung bei der BAMF-Handyauswertung nicht existieren, ist es für Behördenmitarbeitende, aber auch für Richter*innen nicht möglich, den Beweiswert dieser Prüfung sachgerecht einschätzen zu können. Das stellt ein rechtsstaatliches Problem dar.

[37] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 18.

[38] H. Elfardy, M. Diab (2013): Sentence Level Dialect Identification in Arabic, Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, ACL 2013.

Arabizi, Chatdialekte in der arabischen Sprache

Auch im Deutschen unterscheidet sich die Sprache, die wir in kurzen Textnachrichten verwenden, von der formalen Sprache in geschriebenen Texten oder Dokumenten, insbesondere durch häufige Verwendung von Abkürzungen. In arabischsprachigen Ländern kommt hinzu, dass in Textnachrichten die arabische Sprache häufig durch lateinische Buchstaben phonetisiert wird. Dafür gibt es unterschiedliche Möglichkeiten und es haben sich gewissermaßen verschiedene „Chatdialekte" entwickelt, die unter der Bezeichnung „Arabizi" zusammengefasst werden. Sie bestehen aus einer Kombination von lateinischen Buchstaben und Ziffern, die arabische Laute repräsentieren, die kein phonetisches Äquivalent im Englischen oder Französischen haben.[39] Für ein und dasselbe hocharabische Wort existieren vielfältige gebräuchliche Schreibweisen. So können aus dem Begriff تحرير (Freiheit) die Zeichenkombinationen ta7rir, t7rir, tahrir, ta7reer oder tahreer[40] werden. Hinzu kommen erhebliche Unterschiede zwischen arabischen Dialekten, in denen zum Teil unterschiedliche Wörter gebräuchlich sind, zum Teil Wörter aber auch nur verschieden ausgesprochen und dementsprechend abweichend phonetisiert werden. Eine Standardisierung existiert nicht, arabische Wörter mischen sich mit englischen oder französischen Ausdrücken und Abkürzungen.

Identitätshinweise: Wer bist du?

Am Ende des Ergebnisreports werden mögliche Identitätshinweise aufgelistet. Das beinhaltet Namen von Benutzer*innenprofilen aus Apps, sonstige Nutzer*innenidentitäten, gespeicherte Informationen und E-Mail-Adressen, die dem*der Gerätenutzer*in zugeordnet werden können. Diese Informationen können beispielsweise aus Google- oder Apple-Accounts stammen, aber auch aus Tinder- oder Facebook-Profilen, die mit Anwendungen verknüpft sind. Aus welchen Anwendungen das System diese Daten extrahieren kann, ist nicht bekannt.

Die Schulungsunterlagen des BAMF nennen jedoch einige Beispiele und schätzen Informationen aus beispielsweise Reisebuchungsanwendungen wie booking.com als aussagekräftiger ein als Dating-Profile. Explizit sind auch Google-Accounts und der Messenger Viber genannt, in den der GFF vorliegenden Ergebnisberichten sind auch Facebook und Whatsapp aufgeführt.

[39] M. A. Yaghan (2008): "Arabizi": A Contemporary Style of Arabic Slang. veröffentlicht in: Design Issues, Vol 24. Issue: 2.
[40] K. Darwish (2013): Arabizi Detection and Conversion to Arabic.

C. Kritik: Wo ist das Problem?

Ein tiefer Eingriff in die Privatsphäre

Elektronische Geräte, vor allem Smartphones, können große Mengen persönlicher Daten verbinden und enthalten gewissermaßen den gesamten digitalen Hausstand: Nachrichten an Familienmitglieder, Kontaktdaten inklusive Informationen über Anwält*innenkontakte, Konto- und Zahlungsdaten, Zugang zu E-Mail-Accounts, die Suchmaschinen-Historie, Aufenthaltsdaten, intime Fotos. Für Geflüchtete sind ihre Mobilgeräte oft die einzige Verbindung in ihre alte Heimat und enthalten Erinnerungen.

Aus Smartphone-Daten lassen sich Bewegungsprofile und soziale Netzwerke ableiten,[41] sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen.[42] Das betonte im Gesetzgebungsverfahren auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.[43] Das Auslesen, Analysieren und Auswerten von mobilen Datenträgern greift tief in die Privatsphäre Geflüchteter ein und verletzt das Recht auf informationelle Selbstbestimmung sowie speziell auf die Vertraulichkeit und Integrität von informationstechnischen Systemen.[44] „Mit dem systematischen Auslesen der Handydaten schafft der Gesetzentwurf den ‚gläsernen Flüchtling'", kritisierte Pro Asyl in einer Stellungnahme zum Gesetz zur besseren Durchsetzung der Ausreisepflicht.[45] Die Menschenrechtsorganisation äußerte, wie viele Datenschützer*innen und Rechtswissenschaftler*innen, erhebliche verfassungsrechtliche Bedenken während des Gesetzgebungsprozesses. Zu diesen kritischen Stimmen zählen auch der Strafrechtsexperte Nikolaos Gazeas,[46] die damalige Bundesbeauftragte für Datenschutz und die Informationsfreiheit Andrea Voßhoff und der Deutsche Anwaltverein.[47] Zentrale Kritikpunkte sind dabei der mangelnde Schutz des Kernbereichs privater Lebensgestaltung, das Fehlen wirksamer Kontroll- und Widerspruchsmechanismen sowie die Geeignetheit und sonstige Verhältnismäßigkeit. Zu beklagen ist zudem die Intransparenz des Vorgehens durch das BAMF.

---

[41] T. W. Boonstra, M. E. Larsen, H. Christensen (2015): Mapping dynamic social networks in real life using participants' own smartphones.

[42] C. Stachl, S. Hilbert, J.-Q. Au, D. Buschek, A. De Luca, B. Bischl, H. Hussmann, M. Bühner (2017): Personality Traits Predict Smartphone Usage. Eur. J. Pers., 31: 701– 722.

[43] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)831, 23.03.2017.

[44] BverfG, NJW 2008, 822.

[45] Pro Asyl: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)825 A, 22.03.2017.

[46] Siehe K. Schuler, T. Schwarze: Asylpolitik: „Mit dem Grundgesetz nicht vereinbar", Zeit Online, 20.02.2017;
T. Podolski: Sicherheitsrechtler zum Gesetzentwurf über Auslesen von Handys bei Asylsuchenden: „Kann nicht schaden, die Daten zu haben", Legal Tribune Online, 22.02.2017.

[47] Deutscher Anwaltverein: Stellungnahme SN 39/17 zum Gesetz zur besseren Durchsetzung der Ausreisepflicht, 12.05.2017.

Wer schützt die privatesten Informationen? Mangelnder Kernbereichsschutz

Das Allgemeine Persönlichkeitsrecht verpflichtet den Staat, die Grundbedingungen der freien Persönlichkeitsentfaltung und Selbstbestimmung zu schützen (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Bereits im Jahr 1957 leitete das Bundesverfassungsgericht insbesondere aus dem Verweis auf die Menschenwürde ab, dass es einen „unantastbaren Bereich menschlicher Freiheit" geben muss.[48] Später führte es dann auch begrifflich den „absolut geschützten Kernbereich privater Lebensgestaltung" ein.[49] § 48 Abs. 3a AufenthG formuliert, dass eine Auswertung von Datenträgern unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden" und dass etwaige erlangte Erkenntnisse nicht verwertbar sind und sofort gelöscht werden müssen. Fallkonstellationen, in denen „allein", also ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensführung erlangt würden, sind bei einem Handy schwer vorstellbar. Der Rechtswissenschaftler Prof. Dr. Tarik Tabbara hält den unzureichenden Kernbereichsschutz für eines der größten Probleme der Datenträgerauswertung. Er bezeichnet den Lösungsvorschlag für das Theorie-Praxis-Problem des Kernbereichsschutzes im Asyl- und Aufenthaltsgesetz als „eine geradezu zynisch anmutende Lösung".[50] Diese Ausnahme läuft damit in der Praxis leer – denn sie schützt nicht davor, dass „auch" Daten, die den Kernbereich privater Lebensführung betreffen, zunächst ausgelesen und ausgewertet werden. Auch wenn die Rohdaten nach Erstellung des Ergebnisreports gelöscht werden, hat der Eingriff durch ihre Auswertung bereits stattgefunden. Soweit im Ergebnisbericht zudem die in Apps verwendeten Login-Namen und E-Mail-Adressen gelistet werden, die etwa auch Dating-Apps betreffen können, ist auch hier ein Eingriff in den Kernbereich zumindest denkbar.

Kein wirksamer Kontrollmechanismus: Genehmigug durch BAMF-interne Jurist*innen

Für besonders eingreifende Grundrechtseingriffe, insbesondere auch Überwachungsmaßnahmen, gilt ein Richter*innenvorbehalt. Nach dem Bundesverfassungsgericht leiten sich aus den Grundrechten auch Vorgaben für das Verfahren ab, wenn ihr effektiver Schutz nur so sichergestellt werden kann. So kann ein Grundrechtseingriff nur dann zulässig sein, wenn durch eine externe Kontrollinstanz eine Rechtmäßigkeitsüberprüfung erfolgt.[51] Eine gerichtliche Genehmigung bietet besonderen Schutz, gerade weil sie von einer unabhängigen und neutralen Instanz

[48] BVerfGE 6, 32 (41).
[49] BVerfGE 80, 137 (153).
[50] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227.
[51] BVerfG, NJW 2011, 2113 <2118>.

erfolgt.[52] Viel spricht dafür, dass ein Richter*innenvorbehalt deshalb auch bei der Datenträgerauswertung Asylsuchender geboten ist. Er ist gleichwohl nicht gesetzlich ausgestaltet, die Maßnahme muss lediglich von einem*r BAMF-internen Bedienstete*n mit Befähigung zum Richter*innenamt, also einem*r Volljurist*in, genehmigt werden. Das ist offensichtlich durch den Richter*innenvorbehalt inspiriert, mit diesem aber nicht vergleichbar. Prof. Dr. Tabbara schreibt, es handele sich bei dem „'Volljuristenvorbehalt' aber eben nicht einmal um die kleine Münze des Richtervorbehalts." Die hier entscheidenden Volljurist*innen stünden vollständig in der Weisungshierarchie des BAMF, der Kontrollmechanismus könne daher „nicht ansatzweise die grundrechtssichernde Funktion erfüllen, die mit dem Richtervorbehalt verbunden ist".[53]

Was, wenn man nein sagt? Zur Freiwilligkeit der Datenträgerauswertung

Das BAMF betont, dass Bewerber*innen ihre Geräte selbst freischalten und unter Umständen auch die Systemeinstellungen eigenständig anpassen müssten, damit Daten extrahiert werden können. Außerdem müssen die Betroffenen auf einem Formular durch Unterschrift bestätigen, ihr Gerät überlassen zu haben.

Eine Datenverarbeitung kann nach Artikel 6 und 7 der Europäischen Allgemeinen Datenschutzverordnung zulässig sein, wenn die betroffene Person einwilligt. Eine solche Einwilligung muss freiwillig und informiert erfolgen (Erwägungsgrund 32 der Datenschutzgrundverordnung). Informationen darüber, welche Daten von den Datenträgern ausgelesen werden, wie sie verarbeitet werden und an wen sie gegebenenfalls weitergeleitet werden können, finden sich auf dem unterzeichneten Formular nicht. Laut Schilderungen von Betroffenen und Anwält*innen erfolgt auch keine mündliche Aufklärung darüber, was mit den Daten geschieht. Auch an einer Freiwilligkeit fehlt es: Bereits in formeller Hinsicht lässt sich bestreiten, dass die Unterschrift ein Einverständnis zum Ausdruck bringt, sie bestätigt ihrem Wortlaut nach lediglich die Überlassung des Geräts. Sie kann auch deshalb nicht als freiwillig gewertet werden, weil die Geflüchteten sich in einem Unter-Überordnungsverhältnis gegenüber der Behörde befinden. In dem auszufüllenden Vordruck werden sie zudem auf ihre gesetzliche Pflicht hingewiesen, Datenträger zur Auslesung herauszugeben.[54] Verweigern Antragsteller*innen die Herausgabe eines Geräts, kann das für sie gravierende Folgen haben. Es können Leistungen nach § 1a Abs. 5 Asylbewerberleistungsgesetz gekürzt werden. Im schlimmsten Fall kann ein Asylantrag nach § 33 Abs. 2 Asylgesetz als zurückgezogen angesehen werden; die Dienstanweisungen des BAMF sehen vor, dass Antragsteller*innen auf diesen Umstand ausdrücklich hingewiesen werden sollen, wenn sie eine Herausgabe zunächst verweigern.

---

[52] BVerfG, NJW 2018, 2619 <2623>.

[53] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227.

[54] BAMF: Formular D1705.

Mildere Mittel und Erforderlichkeit? Fehlanzeige

Das Recht auf Vertraulichkeit und Integrität von IT-Systemen darf nur eingeschränkt werden, wenn es zur Erreichung überragend wichtiger und legitimer Ziele notwendig und verhältnismäßig ist. Die Datenträgerauslesung dient rein migrationspolitischen Zielen: Sie soll verhindern helfen, dass unberechtigt Asyl gewährt wird oder abgelehnte Asylsuchende schneller abgeschoben werden können. Dass dieses Ziel überhaupt ausreichend gewichtig ist, um zu rechtfertigen, dass anlasslos und flächendeckend derart intensiv in Privatsphäre von Menschen eingegriffen wird, ist angesichts bisheriger Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich zweifelhaft. Es ist gerade nicht damit vergleichbar, wenn eine Maßnahme zur Verhinderung schwerer Straftaten und aufgrund konkreter Verdachtsmomente erfolgt.

Teil der Verhältnismäßigkeit ist dabei auch, dass intensive Rechtseingriffe nur dann durchgeführt werden, wenn es keine anderen Möglichkeiten gibt, mit denen das angestrebte Ziel erreicht werden kann. So heißt es auch in § 15a AsylG, dass die Datenträgerauswertung nur durchgeführt werden darf, wenn es keine milderen Mittel zur Bestimmung der Herkunft oder Identität von Antragsteller*innen gibt. Wenn die Tatbestandsvoraussetzungen der Eingriffsgrundlage erfüllt sind, nämlich der*die Antragsteller*in keinen gültigen Passes bzw. Passersatzdokument vorweisen kann, dann sieht das BAMF aber schlechterdings überhaupt keine anderen milderen Mittel vor. In den Schulungsunterlagen werden zwar auch Sprachbiometrie und Namenstransliteration und -analyse als mildere Mittel genannt. Abgesehen von der Frage, ob diese Mittel milder sind und also weniger in Rechte eingreifen, wendet das BAMF sie aber nicht als alternative Maßnahmen an. Ausweislich der BAMF-internen Dokumente werden diese zeitlich parallel und zusätzlich zur Datenträgerauslesung durchgeführt.[55] Eine Berücksichtigung der Ergebnisse – bevor ein Gerät ausgelesen und automatisch analysiert wird – erfolgt nicht.

Pro Asyl erklärte bereits im Gesetzgebungsverfahren, dass gerade eine Befragung in der Asylanhörung durch gut qualifizierte Mitarbeiter*innen ein geeigneteres Mittel zur Herkunfts- und Identitätsangabe sei.[56] In der Anhörung können gemachte Angaben anhand genauer Nachfragen sehr zuverlässig überprüft werden. Auch die Bundesdatenschutzbeauftragte und der Deutsche Anwaltverein bezweifelten die Verhältnismäßigkeit des Eingriffs in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen.[57]

[55] Sowohl Namenstransliteration als auch Dialektanalyse kommen laut BAMF nur bei arabischsprachigen Antragstellern in Betracht.

[56] Pro Asyl: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)825 A, 22.03.2017.

[57] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, Ausschussdrucksache 18(4)831, 23.03.2017; Deutscher Anwaltverein (2017): Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht (BT-Drs. 18/11546).

Erfahrungsbericht: Das BAMF liest Handydaten auch dann aus, wenn gewichtige Beweismittel Herkunftsangaben stützen

Im Oktober las das BAMF das Smartphone einer Frau aus Kamerun aus. Die Geflüchtete konnte dem Bundesamt keine Identitätspapiere zeigen, stattdessen aber legte sie ein ärztliches Attest vor, in dem ihre Fluchtgründe, ihre persönliche Geschichte und die daraus resultierende psychische Belastung detailliert beschrieben sind. Die Geflüchtete erlebte Zwangsprostitution und wiederholte schwere Vergewaltigungen, zu deren körperlichen Folgen auch eine durch eine Chlamydieninfektion verursachte Sterilität gehört. Die verantwortliche Psychotherapeutin attestierte ihr eine posttraumatische Belastungsstörung mit Suizidgedanken, Depression und eine dissoziative Störung.

Trotz des attestierten Abschiebehindernisses sowie der ausführlichen Beschreibungen der Herkunft, ließ das BAMF sich das Handy der betroffenen Frau aushändigen und las ihre Daten aus. Die beantragte Auswertung wurde durch eine*n Volljurist*in genehmigt. Die Angaben im Ergebnisbericht sind begrenzt aussagekräftig, doch ausgehende Anrufe zu kamerunischen Vorwahlen, Kontakte im Adressbuch der Geflüchteten und die Analyse der in den Textnachrichten verwendeten Sprache unterstützen die Angaben der Geflüchteten.

Datenübertragung: Wer bekommt die Daten sonst noch?

Das Gesetz zur besseren Durchsetzung der Ausreisepflicht führte nicht nur die Rechtsgrundlage für die Datenträgerauswertung ein, es erweiterte auch die rechtlichen Möglichkeiten, Daten an andere Stellen wie Sicherheitsbehörden oder Nachrichtendienste zu übermitteln. Für Asylbewerber*innen ist nicht mehr zu überblicken, wer auf ihre Daten zugreifen kann. Nach Angaben des Innenministeriums gibt es keine Statistiken darüber, wie oft Daten aus der Geräteanalyse an Sicherheitsbehörden weitergegeben werden.[58] Betroffene Personen erfahren davon in der Regel nicht, sodass es ihnen unmöglich ist, die datenschutzrechtliche Zulässigkeit der Weitergabe überprüfen zu lassen.

Im Allgemeinen haben die Datenübertragungen vom BAMF an andere Regierungsstellen in den letzten Jahren massiv zugenommen, ohne dass nachvollziehbar ist, ob diese aus den Datenträgerauswertungen stammen oder sonst im Rahmen des Asylverfahrens erhoben wurden. Im Jahr 2015 übermittelte das BAMF in 571 Fällen Informationen an den inländischen Geheimdienst, das Bundesamt für Verfassungsschutz.

[58] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 30.

Diese Zahl ist 2016 auf 2.418 und 2017 auf 10.597 gestiegen, während die Gesamtzahl der Asylanträge in diesem Zeitraum deutlich zurückging.[59] Nach Angaben des Innenministeriums hat der Hersteller des Auslese- und Auswertungssystems MSAB selbst keinen Zugang zu personenbezogenen Daten, weder von BAMF-Mitarbeitenden noch von Antragsteller*innen. Die Administrator*innen des BAMF haben jedoch zur Wartung oder zur Weiterleitung an Gerichte Zugriff auf den „Datentresor" und damit auf ungeprüfte Berichte der Datenauswertungen.[60]

Was meint das BAMF zur Verhältnismäßigkeit? Die geheime Datenschutzfolgenabschätzung

Nach Artikel 35 der Datenschutzgrundverordnung sind für Datenverarbeitung Verantwortliche verpflichtet, eine Datenschutzfolgenabschätzung durchzuführen, wenn die Datenverarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge" hat. Das ist insbesondere der Fall für automatisierte Verarbeitungsvorgänge, welche eine „systematische und umfassende" Bewertung „persönlicher Aspekte" von Personen beinhalten und auf deren Grundlage Entscheidungen getroffen werden sollen, welche diese Personen betreffen. Unter persönliche Aspekte fallen auch Verhalten, Aufenthaltsort oder Ortswechsel einer Person. Umfassend und systematisch sind Datenverarbeitungen, wenn dabei große Mengen personenbezogener Daten verarbeitet werden (Erwägungsgrund 91 der DSGVO). Das betrifft damit zum Beispiel Profiling-Vorgänge. Aber auch bei einer automatisierten Auswertung von Handydaten zu Anrufen und Nachrichten, Browserverhalten und Lokationsdaten, deren Ergebnis Einfluss auf die Entscheidung über einen Asylantrag haben kann, liegen diese Voraussetzungen vor.

Eine Datenschutzfolgenabschätzung muss unter anderem die geplanten Verarbeitungsvorgänge beschreiben, den damit verfolgten Zweck benennen und deren Notwendigkeit und Verhältnismäßigkeit bewerten. Eine Informationsfreiheitsanfrage zur Datenschutzfolgeabschätzung des BAMF zu den Datenträgerauswertung lehnte das Bundesamt mit einer Verzögerung von neun Monaten unter Verweis auf Sicherheitsbedenken ab.[61] Das BAMF argumentierte, dass mögliche Sicherheitslücken im System von Dritten identifiziert und genutzt werden könnten.

[59] BT-Drs. 19/3840: Datenaustausch von Polizei und Nachrichtendiensten in Deutschland, 16.08.2018, Antwort auf Frage 2.
[60] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018, Antwort auf Frage 28.
[61] Anfrage nach dem Informationsfreiheitsgesetz zu den Datenschutzfolgeabschätzungen des BAMF, Ablehnung vom 13.05.2019.

Lohnt es sich? Aussagekraft der Prüfberichte

Schon vor der Verabschiedung des Gesetzes zur besseren Durchsetzung der Ausreisepflicht bezweifelten einige Organisationen die Wirksamkeit der Datenträgeranalyse. Ziel des Gesetzes war es unter anderem, Abschiebungen zu beschleunigen: Mit den Datenträgerauswertungen sollten dazu Identität, Herkunft und Schutzgründe überprüft werden.

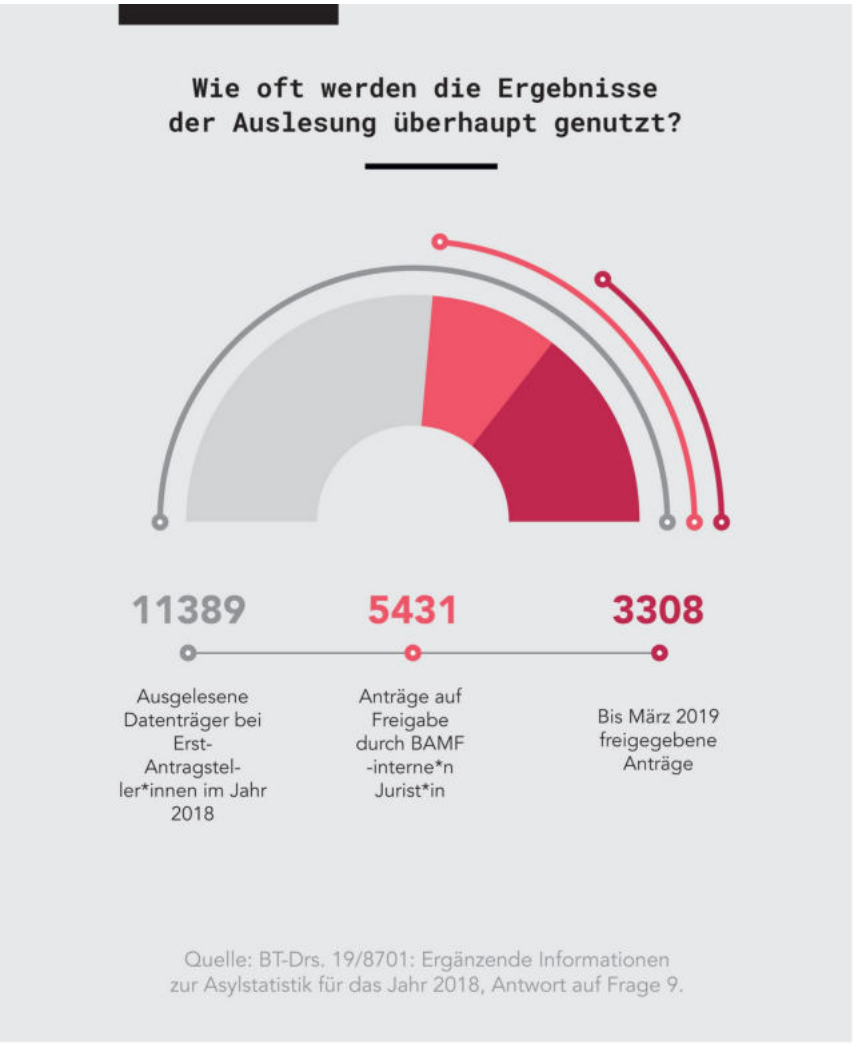
Die Statistiken bestätigen, dass sich die Handyauswertung dafür nur selten als nützlich erwiest: Sie lässt sich leicht umgehen, versagt technisch häufig und ist in den überwiegenden Fällen unbrauchbar. Die verwertbaren Ergebnisse bestätigen weit überwiegend die gemachten Angaben der Asylbewerber*innen und zeigen nur in seltenen Ausnahmefällen Widersprüche zu den gemachten Angaben auf. Wer will, kann die Maßnahme leicht umgehen, indem er*sie leugnet, ein Smartphone oder andere Datenträger zu besitzen. So ist davon auszugehen, dass sich unter Asylsuchenden herumgesprochen hat, dass das BAMF diese sonst ausliest.

In einem nennenswerten Anteil scheitern die Auslesungen zudem bereits technisch, im ersten Quartal 2019 war dies bei 23 Prozent der Fall,[62] im Jahr 2018 bei 26 Prozent.[63] Soweit die Auslesung gelingt, sind die Ergebnisse nach Angaben des BAMF überwiegend unbrauchbar: Im ersten Quartal 2019 enthielten 55 Prozent der ausgewerteten Berichte keine brauchbaren Erkenntnisse,[64] 2018 waren es ganze 64 Prozent.[65]

Unbrauchbare Ergebnisse können unterschiedlichste Gründe haben: So kann die Datenbasis zu klein sein, weil ein Handy noch nicht lange genutzt wurde. Oder es ergeben sich widersprüchliche Angaben, weil das Handy von mehreren Personen genutzt wurde, gleichzeitig oder nacheinander, ohne dass bei der Weitergabe des Geräts alle Inhalte gelöscht wurden. Hat sich ein*e Asylsuchende*r erst in Deutschland ein Smartphone besorgt, liegt es nahe, dass Geodaten für das BAMF nicht verwertbar sind, weil sich kein Aufenthaltsort außerhalb von Deutschland ermitteln lassen wird.

[62] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Fragen 5 und 6.
[63] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 9 a.
[64] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Frage 6.
[65] BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 9.

In einem der GFF vorliegenden Ergebnisreport ist unter dem Punkt Lokationsdaten zusätzlich der Hinweis vermerkt, dass „aufgrund der hochdynamischen Natur der App-Daten" nicht in jedem Fall garantiert werden kann, dass sich das Gerät auch am erkannten Ort befunden habe. Oder aber der*die Antragsteller*in benutzt hauptsächlich Apps, die die Systeme des BAMF nicht auswerten können. Außerdem nutzen Geflüchtete häufig pseudonyme Identitäten, da sie – sowohl in ihren Herkunftsländern als auch auf der Flucht – Überwachung fürchten.[66] Es ist also schon deshalb nicht sicher anzunehmen, dass der Facebook-Profilname auch dem echten Namen des*r Geflüchteten entspricht.

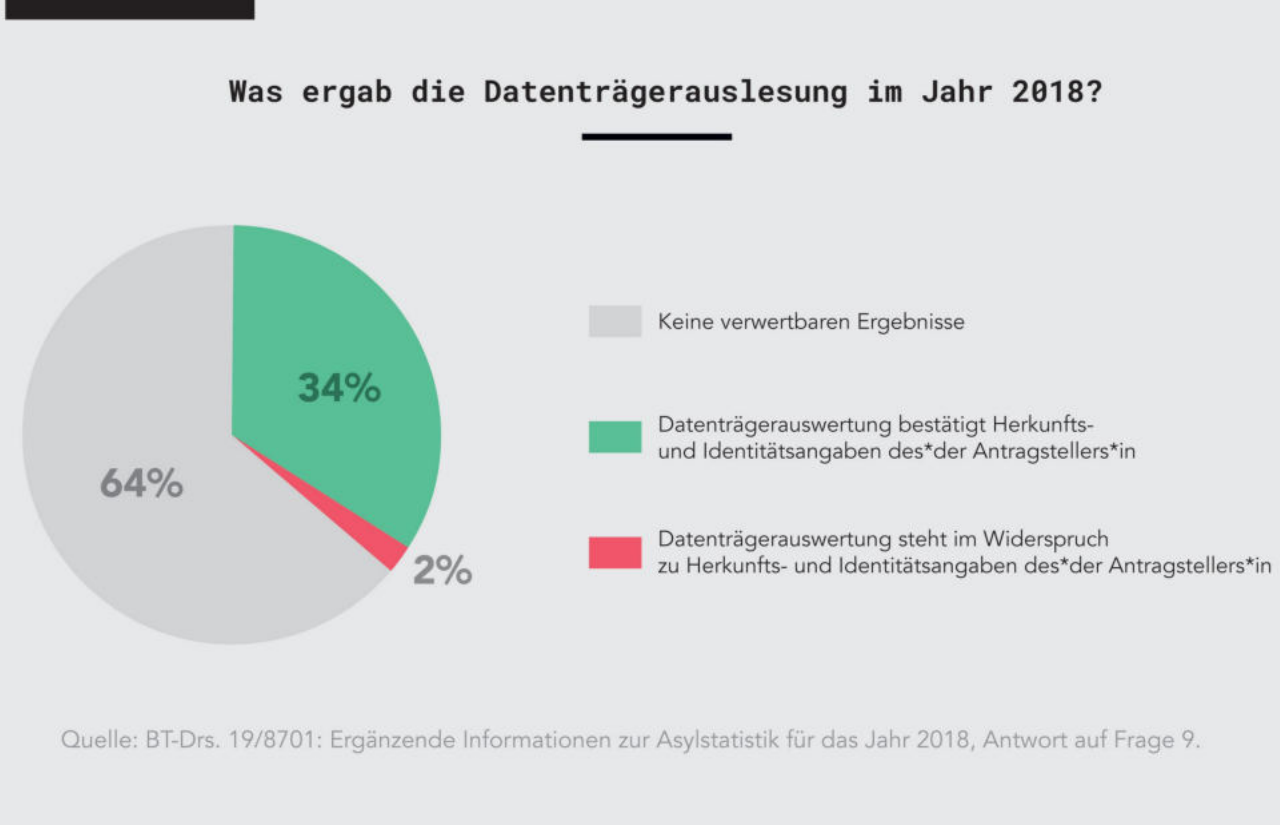


Längst nicht alle Prüfberichte verwendet das BAMF anschließend überhaupt. Von den 3.502 erfolgreich ausgelesenen Datenträgern zählte das BAMF im ersten Quartal 2019 1.538 Anträge von Entscheider*innen bei BAMF-internen Jurist*innen auf Freigabe der Ergebnisreports, in 1.236 Fällen wurden diese bis Juni 2019 freigegeben. Es ist unklar, wie viele der übrigen Anträge tatsächlich abgelehnt und wie viele bis zu diesem Zeitpunkt noch nicht bearbeitet wurden. Im Laufe von 2018 kamen auf etwa 11.400 ausgelesene Datenträger etwa 5.400 Freigabeanträge.[67]

Die Ergebnisse der Prüfberichte zeigen nur in seltensten Fällen Widersprüche zum Vorbringen der Antragsteller*innen auf. Im ersten Quartal 2019 war dies lediglich in einem Prozent der Auswertungen der Fall, damit in umgerechnet 12 Fällen. Im Verlauf des Jahres 2018 war taten sich in 2 Prozent Widersprüche auf, was bei etwa 3.300 freigegebenen Auswertungen etwa 66 Fällen entspricht. In allen übrigen Fällen bestätigten die Berichte die gemachten Angaben. Im ersten Quartal 2019 war dies

[66] M. Gillespie, L. Ampofo, M. Cheesman, B. Faith, E. Iliadou, A. Issa, S. Osseiran, D. Skleparis (2016): Mapping Refugee Media Journeys: Smartphones and Social Media Networks.

[67] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Frage 6; BT-Drs. 19/8701: Ergänzende Informationen zur Asylstatistik für das Jahr 2018, Antwort auf Frage 9.



bei 44 Prozent, 2018 war bei 34 Prozent der ausgewerteten Ergebnisberichte der Fall.[68] Der Bundesregierung sind laut eigener Aussage zumindest einzelne Fälle bekannt, in denen Antragsteller*innen manipulierte Mobilgeräte vorgelegt haben.[69]

Das Verhältnis von Eingriffen in die Grundrechte der betroffenen Asylbewerber*innen und dem Nutzen des Verfahrens befindet sich damit in einem deutlichen Ungleichgewicht.

Schließlich ist auffällig, dass Asylsuchende verschiedener Herkunftsländer sehr unterschiedlich oft von Datenträgerauslesungen betroffen sind. Die meisten der betroffenen Asylsuchenden im ersten Quartal 2019 waren afghanische Staatsbürger*innen mit 952 Fällen, gefolgt von 285 Georgier*innen. Geräte von syrischen Asylbewerber*innen, die in diesem Zeitraum mit 3.454 Personen immer noch die größte Gruppe von Asylbewerber*innen ausmachten, wurden nur 101 Mal ausgelesen.[70]

Datenträgerauslesungen dienen dem gesetzgeberischen Ziel, Asylmissbrauch zu verhindern und Abschiebungen zu beschleunigen, also nur ausgesprochen selten. Wenn Maßnahmen sehr wenig erfolgsversprechend sind, stellt sich auch die Frage, ob diese dann zulässig sind. Diese Frage wirft auch Prof. Dr. Tabbara auf und weist darauf hin, dass bei strafrechtlichen Maßnahmen wie Durchsuchungen in der Rechtsprechung des Bundesverfassungsgerichts anerkannt sei, dass ihre anzunehmende Erfolglosigkeit die Maßnahme unverhältnismäßig und damit unzu-

[68] Ebd.
[69] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 3.
[70] BT-Drs. 19/11001: Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, Antwort auf Frage 6.

lässig mache.[71] Aber auch ohne bewusste Vermeidungshandlungen durch die Antragsteller*innen können die Auswertungen unbrauchbar sein: Dr. Matthias Lehnert, Anwalt für Aufenthalts- und Asylrecht, merkt darüber hinaus an, dass die Ergebnisse der Analyse in Gerichtsverfahren keine Beweiskraft haben, wenn die Methoden nicht durch das Gericht überprüft werden können oder wenn sich herausstellt, dass die Auswertung fehleranfällig ist.

Erfahrungsbericht: Textnachrichten auf Neugriechisch, Esperanto und Finnisch? Diffuse Sprachanalyse

Im Juni 2019 las das BAMF das Smartphone eines irakischen Asylsuchenden aus. Er gab an, sein Gerät ungefähr seit März 2019 zu besitzen - was die Analyse des BAMF bestätigte. Der Informationsgewinn durch den Ergebnisreport der Smartphone-Auswertung war dementsprechend sehr gering. Bei dem Großteil der analysierten Ländercodes ausgehender (42 Prozent) und eingehender (57 Prozent) Telefonate ließ sich keine gültige Länderzuordnung ermitteln. Die meisten der zugeordneten Anrufe sollen aus Griechenland stammen, was mit den Angaben des Geflüchteten zusammenpasst, das Telefon in Griechenland erhalten zu haben. Bei den analysierten Textnachrichten sind die Ergebnisse noch weniger verwertbar. 100 Prozent der ausgehenden und 97 Prozent der eingehenden Nachrichten konnten keinem Land zugeordnet werden. Bei den Kontakten im Adressbuch des Schutzsuchenden konnten 44 Prozent nicht zugeordnet werden, die restlichen Kontaktnummern wurden zu jeweils 22 Prozent der Türkei und Griechenland und zu jeweils 6 Prozent dem Irak und Japan zugeordnet.

Die Auswertung der in den Textnachrichten verwendeten Sprache ist schließlich gänzlich unplausibel: Die meisten der ausgehenden Nachrichten sollen auf Englisch oder Italienisch verfasst worden sein, nämlich jeweils 33 Prozent. 75 Prozent der eingehenden Nachrichten waren jedoch laut Analyse auf Neugriechisch verfasst - gefolgt von Chinesisch, Japanisch, Esperanto, Finnisch und Niederländisch. Auf dem Gerät wurden laut Ergebnisreport keine brauchbaren Lokationsdaten, Browserdaten oder Identitätsinformationen gefunden. Laut der Anwältin des Betroffenen wurde weder in der Anhörung noch in der Asylentscheidung auf die Analyseergebnisse Bezug genommen.

[71] T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227.

Was heißt das eigentlich? BAMF-Mitarbeitende werden mit der Interpretation der Ergebnisse alleingelassen

Die Ergebnisse sind mehrheitlich unbrauchbar. Es liegt es an den Entscheider*innen und Anhörer*innen, das im einzelnen Fall auch zu erkennen – und Berichte zu verwerfen, bzw. Widerspruch durch gezielte Nachfragen aufzulösen. Dazu brauchen sie Informationen, die ihnen bei der Einordnung der Ergebnisse helfen. In den Schulungsunterlagen sind jedoch nur rudimentäre Orientierungspunkte dazu enthalten. Dort wird beispielsweise ausgeführt: „Je länger das Gerät verwendet worden ist, desto aussagekräftiger der Bericht." „Je mehr Daten ausgelesen werden konnten, desto valider der Bericht." Des Weiteren werden mögliche Begründungen geliefert, warum ein Gerät etwa „eine Vielzahl von Device Downtimes" aufweist, also ausgeschaltet war. Das kann darauf hindeuten, dass das Gerät von unterschiedlichen Nutzer*innen verwendet wurde oder weiterverkauft worden ist. Ab welcher Datenmenge von einem verlässlichen Ergebnis auszugehen ist, ist nicht angegeben.

Eine weitere Fehlerquelle kann darin liegen, dass trotz ausreichender Datenmenge auf einem Smartphone nur ein Ausschnitt der Daten durch das BAMF ausgewertet werden kann. Zum Beispiel, wenn die*der Antragsteller*in vor allem über Apps kommuniziert, die vom System des BAMF nicht unterstützt werden, oder wenn die Ländervorwahlen von eingehenden Nachrichten analysiert werden, ein*e Antragsteller*in aber vor allem über Messenger kommuniziert, die keine Telefonnummer als Identifikationsmerkmal nutzen und demnach auch keine Ländervorwahl enthalten. Dann wird nur ein Teil der tatsächlichen Kommunikation ausgewertet und es kann leicht eine Verzerrung der Ergebnisse entstehen.

Bei der Sprachidentifikation von Textnachrichten wird den Entscheider*innen in den Schulungsunterlagen keinerlei Informationen über die Fehlerraten der verwendeten Analysesoftware an die Hand gegeben. Die Entscheider*innen können ohne diese Information nicht einschätzen, welche Unsicherheit den Analyseergebnissen innewohnt. Wenn eine Sprache von dem System nicht bekannt ist, soll es die dieser am ähnlichsten erscheinende Sprache erkennen. Ob das dann immer auch eine Sprache ist, die in einer Region gesprochen wird, die geografisch in der Nähe des Herkunftslandes zu verorten ist, bleibt offen. Bezüglich der Qualität der Login-Daten wird in den Schulungsunterlagen darauf verwiesen, dass beispielsweise Anmeldenamen von Booking.com aussagekräftiger seien als die von Dating-Apps. Auch hier ist wiederum nicht bekannt, welche Anwendungen genutzt werden, um Profil-Informationen zu ermitteln. Ebenso ist in den Schulungsmaterialien nicht gelistet, aus welchen Quellen genau die Geo-Informationen stammen, die in die Auswertung von Ortsdaten einfließen.

Die Entscheider*innen sind verpflichtet, die Asylentscheidung in der Gesamtschau aller vorliegenden Informationen zu treffen. Computergenerierte Ergebnisse, untermauert durch statistische Angaben, vermitteln jedoch ein Gefühl von Objektivität und Exaktheit, die in die Irre leiten können. Interpretiert ein*e Entscheider*in die Ergebnisse falsch, vertraut diesen und unterstellt dem*der Antragsteller*in, unwahre Angaben zu Herkunft und Identität gemacht zu haben, kann das dazu führen, dass ein Asylantrag irrtümlich als „offensichtlich unbegründet" abgelehnt wird.

„Offensichtlich unbegründet" – eine folgenschwere Ablehnung

§ 30 AsylG regelt, wann ein Asylantrag als „offensichtlich unbegründet" abgelehnt werden kann. Dies ist unter anderen der Fall, wenn „in wesentlichen Punkten das Vorbringen des Ausländers nicht substantiiert oder in sich widersprüchlich ist, offenkundig den Tatsachen nicht entspricht oder auf gefälschte oder verfälschte Beweismittel gestützt wird", „der Ausländer im Asylverfahren über seine Identität oder Staatsangehörigkeit täuscht oder diese Angaben verweigert". Wird ein Asylantrag unter einer solchen Annahme abgelehnt, drohen unmittelbare Konsequenzen. Der*die Antragsteller*in wird aufgefordert, Deutschland innerhalb einer Woche zu verlassen (§ 36 Abs. 1 AsylG). Kommt er*sie der Ausreisepflicht nicht nach, kann er*sie abgeschoben werden.

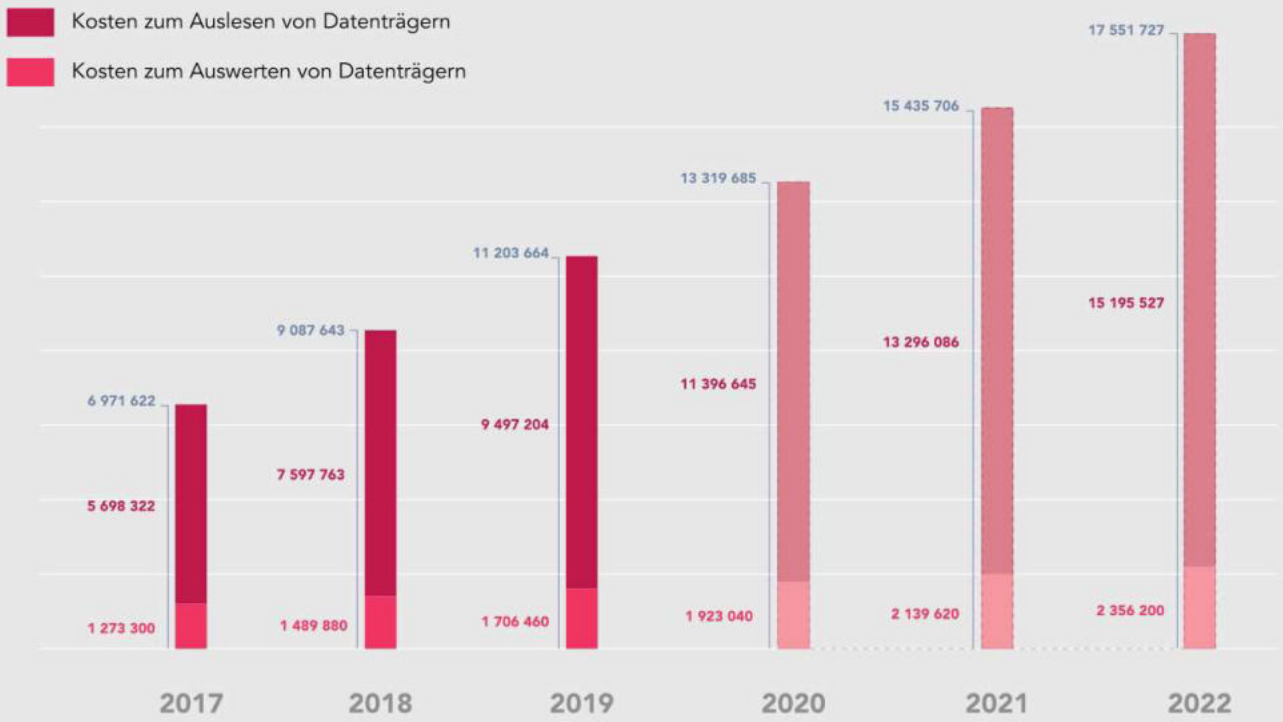
Dem*der Antragsteller*in bleibt dann lediglich eine Woche, um gegen die Ablehnung des BAMF zu klagen. Innerhalb dieser Frist muss zusätzlich ein Antrag auf gerichtlichen Eilrechtsschutz gestellt werden, weil die Abschiebeentscheidung sofort vollziehbar ist.

Zumindest im Zusammenhang mit anderen IT-Assistenzsystemen, nämlich der Dialektanalyse, sind einzelne Fälle bekannt, in denen die Ablehnung eines Asylantrags sich wesentlich auf deren Ergebnisse stützte, obwohl andere Faktoren die Angaben des*der Antragstellers*in bestätigten.[72] Wie viele Asylablehnungen vor Gerichten anhängig sind und primär auf den Ergebnissen aus den IT-Tools beruhen, ist nicht bekannt. Darüber liegen laut Bundesinnenministerium keine Erkenntnisse vor.[73]

[72] A. Biselli: Eine Software des BAMF bringt Menschen in Gefahr, Motherboard/VICE, 20.08.2018.

[73] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 23.

Gesamtkosten des BAMF für das Auslesen und Auswerten von Datenträgern in Euro



Quelle: Bei den angezeigten Kosten handelt es sich jeweils um die bisherigen Gesamtkosten für die Anschaffung von Hard- und Software und Supportkosten. Die Kosten von 2017 beinhalten Anschaffungs- sowie Supportkosten für die zur Datenträgerauslesung verwendete Hard- und Software; ab 2018 handelt es sich um Supportkosten. Die Kosten ab 2020 sind eigene Schätzungen auf der Grundlage der bisherigen Kosten. Quelle: BT-Drs. 19/6647 Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 15.

Kosten: Ist es das wert?

In Relation zum begrenzten Nutzen der Datenträgerauswertung stehen die Kosten für das System in einem Missverhältnis. Sie übersteigen die ursprünglichen Erwartungen bei seiner Einführung deutlich. Im Februar 2017 gab das Bundesinnenministerium an, es seien einmalige Einrichtungskosten für die Auslesegeräte von 3,2 Millionen Euro zu erwarten.[74] Ein Jahr später korrigierte das Ministerium seine Kalkulation: Auf 4.788.507,60 Euro für 2017 und weitere 1.596.169,20 Euro bis April 2018.[75] Diese Beträge beziehen sich lediglich auf die Hard- und Software für den Ausleseprozess.

Um die anfallenden Daten zu analysieren, wurden weitere Ausgaben fällig: 1.070.000 Euro im Jahr 2017 und weitere 182.000 Euro bis April 2018. Zusammen ergibt das rund 7,6 Millionen Euro bis Ende 2018 – und damit mehr als doppelt so viel wie ursprünglich veranschlagt.

[74] Bundesministerium des Innern: Schriftliche Frage Monat Feburar 217, Arbeitsnummer 2/223.

[75] BT-Drs. 19/1663: Einsatz von Spracherkennungssoftware durch das Bundesamt für Migration und Flüchtlinge, 16.04.2018, Antwort auf Frage 13.

Die Kostenprognose und -entwicklung setzte sich fort: Laut Angaben des Bundesinnenministerium aus dem Dezember 2018 sind für das System bis Ende des Jahres 2019 Gesamtkosten in Höhe von 11,2 Millionen Euro vorgesehen. Die Gesamtkosten werden weiter steigen, für Support ist mit jährlich etwa 2,1 Millionen Euro zu rechnen.[76] Außerdem wurden entsprechend der Gesetzesbegründung 300.000 Euro pro Jahr für Lizenzen erwartet.

Die Gesamtkosten beinhalten auch die Aufwendungen in der Testphase des Projektes mit insgesamt 585.480 Euro. Zum damaligen Zeitpunkt testete das BAMF Systeme von MSAB, T3K und Cellebrite.[77]

Black Box Smartphone-Auswertung: Intransparente Software und Algorithmen

Informationen zur Datenträgerauswertung des BAMF zu bekommen, ist ein beschwerlicher Prozess. Das BAMF gibt Informationen nur stückweise und teils mit erheblichen Verzögerungen heraus. Teilweise sind die Antworten dabei so unvollständig, dass sie kaum noch als wahrheitsgemäß eingeordnet werden können: So antwortete das BAMF auf eine Presseanfrage im April 2018 auf die Frage nach den Herstellern der Hard- und Software zum Auslesen bzw. Auswerten mobiler Geräte Geflüchteter: „Für das Auslesen und die Auswertung von Datenträgern stellt die Fa. ATOS die notwendige Soft- und Hardware."[78] Dass ATOS lediglich Lieferant des Gesamtsystems war und die einzelnen Komponenten von Herstellern wie MSAB und T3K stammen, offenbarte das BAMF nicht. Auch auf Anfragen nach dem Informationsfreiheitsgesetz antwortete die Behörde nur nach langer Wartezeit und überschreitet dabei regelmäßig alle gesetzlichen Fristen. Die gesetzliche Regelfrist von einem Monat dürfen Behörden nur in ungewöhnlichen, zum Beispiel besonders arbeitsaufwendigen Fällen abweichen. Die Zusendung der Schulungsunterlagen erfolgte erst nach fast vier Monaten, die Herausgabe der Datenschutzfolgenabschätzungen wurde nach neun Monaten vollständig abgelehnt.

Auch bei parlamentarischen Anfragen wurden Informationen verschwiegen. So antwortete das dem BAMF übergeordnete Bundesinnenministerium im Juni 2018 auf eine Schriftliche Frage aus dem Bundestag, für die Datenträgeranalyse (nur) Produkte von ATOS, MSAB und T3K getestet bzw. beschafft zu haben.[79] Erst auf eine spätere Kleine Anfrage hin ergänzte das Bundesinnenministerium im Dezember 2018, dass auch Technik der Firma Cellebrite getestet wurde.[80]

[76] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 15.

[77] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 25.

[78] A. Biselli: Handys von Asylbewerbern zu analysieren, kostet viel mehr als geplant, Motherboard/VICE, 17.04.2018.

[79] Bundesministerium des Innern: Schriftliche Frage Monat Juni 2018, Arbeitsnummer 6/225.

[80] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, Antwort auf Frage 25.

Auf welchen Algorithmen und welcher Datenbasis die Produkte basieren, welche Anwendungen sie auswerten können und mit welchen Fehlerquoten gerechnet werden müssen, ist bis heute öffentlich nicht nachvollziehbar. Anfragen dazu beantwortet das BAMF nicht, die Antworten könnten sonst Rückschlüsse auf die Arbeitsweise ermöglichen, die den Einsatz der Technik potentiell erschwerten. Selbst zur Fehlerrate der Sprachanalyse für Textnachrichten verweigert die Behörde jede Auskunft. Dabei wären viele dieser Informationen wichtig dafür, die Zuverlässigkeit des Systems zu beurteilen. So bleiben viele Fragen offen: (Wie) Verhindert das BAMF, dass beispielsweise Geodaten aus Fotos, die ein*e Geflüchtete*r von einer anderen Person zugeschickt bekam, in die Auswertung einbezogen werden? Welche Sprachen kann das Textanalysemodul überhaupt erkennen? Schreibt ein*e Geflüchtete*r Textnachrichten auf Kurmandschi, kann diese Sprache jemals erkannt werden? Werden sie dann zumindest einer anderen kurdischen Sprache zugeordnet oder völlig falsch erkannt? Wie hoch sind Fehlerquoten bei der Spracherkennung, und sind diese bei unterschiedlichen Sprachen verschieden hoch?

Die von der Bundesregierung eingesetzte Datenethikkommission erarbeitete in ihrem Abschlussgutachten Empfehlungen für den Einsatz algorithmischer Systeme durch staatliche Akteure.[81] Darin haben die Expert*innen auch Transparenzanforderungen formuliert. Dazu gehört, dass staatliche Entscheidungen, für die algorithmische Systeme genutzt wurden, transparent und begründbar bleiben müssen. Zusätzlich verweist die Datenethikkommission auf ein Positionspapier der Informationsfreiheitsbeauftragten in Deutschland. Demnach sollen öffentliche Stellen über „aussagekräftige, umfassende und allgemein verständliche Informationen bezüglich der eigenen Datenverarbeitungen verfügen" und diese auch soweit möglich veröffentlichen. Datenkategorien der verarbeiteten Daten, die enthaltene Logik samt Berechnungsformeln und die Gewichtung der Eingabedaten zählt das Positionspapier ausdrücklich dazu.[82] Diesen Transparenzkriterien genügt das BAMF nicht.

Nur der Anfang? Eine Ausweitung der Datenträgerauswertung wäre technisch kein Problem

Angesichts der Einführung dieser neuer staatlicher Befugnisse zur Datenträgeranalyse und einer entsprechenden umfangreichen und vor allem kostenintensiven technischen Aufrüstung stellt sich die Frage, ob zukünftig der Einsatz in anderen als den derzeitig durch die Rechtsgrundlage im Asylgesetz vorgesehenen Anwendungsfälle droht. Das Auslese- und Auswertesystem von MSAB kann technisch mehr als das BAMF nach der gesetzlichen Grundlage darf. Ohne großen Aufwand könnten den Geodaten Zeitstempel zugeordnet werden. Kontaktinfor-

[81] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission, 23.10.2019.

[82] 36. Konferenz der Informationsfreiheitsbeauftragten in Deutschland: Positionspapier „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar", 16. Oktober 2018.

mationen könnten auf Verbindungen zu polizeilich oder nachrichtendienstlich bekannten Personen überprüft werden. Das Unternehmen T3K, von dem das Sprachenerkennungssystem stammt, bietet auch Bilderkennungstechnologie an, die angeblich erfassen kann, ob auf Fotos Drogen, Waffen oder terroristische Propaganda abgebildet sind.[83] Die vom BAMF verwendete Software XRY kann außerdem gelöschte Daten aus iCloud-Backups wiederherstellen[84] und verfügt laut Hersteller darüber hinaus über „Android-Exploits", also die Möglichkeit, Schwachstellen in der Software von Android-Geräten auszunutzen, um Sicherheitsmechanismen zu umgehen.[85] Technisch möglich wäre auch eine Inhaltsanalyse der Textnachrichten, die etwa nach Schlagworten durchsucht werden könnten. Damit würden Geflüchtete, die sich in Deutschland registrieren, zunehmend Opfer von Maßnahmen, wie sie sonst nur bei konkreten Verdacht von Straftaten zulässig sind. Das ist kein theoretisches Szenario, sondern schlug sich bereits in konkreten Forderungen nieder. Die ehemalige Leiterin des BAMF, Jutta Cordt, teilte dem SWR schon im November 2017 mit, dass sie sich Zugriff auf die Bilder wünsche.[86] Ein Jahr später, im Dezember 2018, erklärte das Bundesinnenministerium, man prüfe derzeit die technischen und rechtlichen Möglichkeiten einer Erweiterung der Smartphone-Auswertung.[87]

Durch den Einsatz von Künstlicher Intelligenz in der Analyse von Anhörungsprotokollen versucht das BAMF zudem bereits heute in einem Pilotprojekt zur „Profilanalyse", automatisch sicherheitsrelevante Inhalte zu ermitteln. So will die Behörde „den gesetzlichen Meldeverpflichtungen des BAMF an Sicherheitsbehörden leichter und schneller nachkommen".[88]

Schließlich sind auch Rückschlüsse auf die Fluchtroute für die Behörden interessant: In Österreich ist die Bestimmung von Reiserouten ausdrückliches Ziel der gesetzlichen gesetzlich vorgesehenen Datenträgerauswertung, um Anhaltspunkte dafür zu bekommen, durch welchen Staat der Geflüchtete in die EU eingereist ist. Die Dublin-III-Verordnung legt fest, dass der EU-Staat für eine*n Geflüchtete*n zuständig ist, in dem er*sie zuerst eingereist ist. Im sogenannten „Dublin-Verfahren" können Asylbewerber*innen ausgewiesen werden, wenn nachgewiesen werden kann, dass sie durch einen anderen EU-Staaten eingereist sind.

---

[83] T3K-Forensics: Analyse von Smartphones in der Mobilforensik. http://www.t3k-forensics.com/analytics/ (zuletzt abgerufen am 7.12.2019).

[84] Darstellung auf der MSAB-Website: XRY v7.3 upgrade tackles implications of iOS 10.3 (zuletzt abgerufen am 20.12.2019).

[85] Darstellung auf MSAB-Website: XRY (zuletzt abgerufen am 7.12.2019).

[86] SWR: Interview der Woche – Jutta Cordt, Präsidentin Bundesamt für Migration und Flüchtlinge (BAMF), November 2017 (depubliziert).

[87] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 27.

[88] R. Böcker: KI-Anwendungen im Einsatz, Newsletter des Behörden Spiegel „E-Government, Informationstechnologie und Politik", Ausgabe Nr. 938, 21.03.2019; A. Biselli: Asylbehörde sucht mit Künstlicher Intelligenz nach auffälligen Geflüchteten, netzpolitik.org, 19.07.2019.

D. Mehr als Smartphone-Daten: Automatisierung bei der Migrationskontrolle in Deutschland

Parallel zur Datenträgerauswertung führte das BAMF weitere sogenannte IT-Assistenzsysteme zur Identitätsprüfung ein. Die IT-Systeme sind unter dem Namen „Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte (IDM-S)" zusammengefasst und beinhalten neben der Datenträgerauswertung auch Verfahren zur Bildbiometrie, Stimmbiometrie und zur Transliteration und Analyse arabischer Namen.[89]

Biometrische Bilder und automatischer Datenbankabgleich

Zusätzlich zu der Erfassung von Fingerabdrücken werden bei jeder Erstregistrierung biometrische Gesichtsbilder der Geflüchteten erfasst. Sie dienen dazu, bereits registrierte Asylbewerber*innen zu erkennen und Doppelregistrierungen zu vermeiden. Biometrische Gesichtsbilder und Fingerabdrücke werden außerdem genutzt, um sie mit anderen Datenbeständen zu vergleichen. So dient ein Abgleich mit der EURODAC-Datenbank der EU dazu, zu ermitteln, ob bereits eine Registrierung in einem anderen EU-Land stattfand. Die Bilder sowie Fingerabdrücke werden anschließend in einem Chip des elektronischen Aufenthaltstitels gespeichert.

TraLitA, der Transliterationsassistent

Bei der Übertragung von arabischen Namen ins lateinische Alphabet kam es im BAMF immer wieder zu Inkonsistenzen, da eine einheitliche Transliteration nicht stattfand. Ein Programm zur automatischen Transliteration soll die Eingaben der Antragsteller*innen bei der Registrierung von arabischen Schriftzeichen in das lateinische Alphabet standardisiert übertragen.

Zusätzlich dazu findet eine Analyse statt, wie häufig ein Name in bestimmten Herkunftsregionen vorkommt, um eine Plausibilitätseinschätzung der gemachten Angaben zu erhalten. Diese Herkunftslandprognose erfolgt laut Dienstanweisung zur Identitätsfeststellung beispielsweise in der folgenden Form: „Der Name kommt im angegebenen Land [Syrien] [selten/sehr selten] vor. In [den Ländern/dem Land] [Libyen/Ägypten/Marokko] kommt er hingegen häufiger vor."[90] Laut Angaben des Innenministeriums beruht das System auf einer Datengrundlage von einer Milliarde Namen weltweit, für jedes arabischsprachige Land sei das System mit 20.000 reellen Namen getestet worden. Dennoch sind die Fehlerquoten teilweise hoch. Bei syrischen oder irakischen Staatsangehörige soll das System zwar in 85 bis 90 Prozent der Fälle richtig liegen, bei Antragsteller*innen aus der Maghreb-Regionen werden jedoch nur noch Erfolgsraten von

[89] BAMF: Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität, Sicherheitsaspekte. Einführung in die neuen IT-Tools, 30.08.2017.
[90] BAMF: Dienstanweisung Asylverfahren – Identitätsfeststellung.

35 Prozent registriert, „dies könnte mit der historisch entstandenen Vermischung mit der französischen und italienischen Sprache zusammenhängen", heißt es als Begründung.[91] Bei Einschätzungen der Software dazu, ob ein Name eine Herkunft aus dem Maghreb nahelegt, ist es deshalb also ungleich wahrscheinlicher, dass diese fehlerhaft sind.

Dialekt als Herkunftsmerkmal

Bei arabischsprachigen Antragstellern kann bei ihrer Registrierung außerdem eine Dialektanalyse durchgeführt werden. Dabei müssen sie eine zweiminütige Sprachprobe abgeben, die durch ein System analysiert wird und Wahrscheinlichkeiten für mögliche Sprachen und Dialekte angibt. Auch hiermit sollen Herkunftsangaben plausibilisiert werden. Nach aktuellen Angaben liegt die Fehlerrate dieser Software laut Eigenangaben des BAMF bei 15 Prozent, diese schwankt jedoch je nach Muttersprache und Herkunftsregion. Für den arabisch-levantinischen Dialekt, der im Libanon, Jordanien, Syrien, Israel und Palästina gesprochen wird, wurde von der Bundesregierung im Dezember 2018 eine Erfolgsquote von über 90 Prozent angegeben. Die Fehlerquote ermittelt das BAMF mit validierten Sprachproben und Stichproben aus der eigenen Sprach- und Dialekterkennung, die zusätzlich „durch technische Experten und Sprachexperten" validiert wurden.[92]

Der arabisch-levantinische Dialekt sei im Sprachmodell am besten ausgebaut. Dafür erwarb das BAMF vom Linguistic Data Consortium der University of Pennsylvania ein Arabisch-Levantinisches Sprachpakets für 3.721,62 Euro.[93] Wie die Fehlerraten für die anderen Dialekte sind, beantwortet das BAMF nicht. Dafür ist auch der Umfang der Trainingsdatensätze für einen jeweiligen Dialekt entscheidend. Es ist bekannt, dass in das System bis Dezember 2018 insgesamt 8.000 validierte Sprachproben eingeflossen sind. Wie viele Sprachproben das je Dialekt und Sprache sind, wird nicht angegeben. Die Bundesregierung verweist in ihrer Antwort darauf, dass diese Informationen mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch" eingestuft seien, da sonst bewusste Täuschungshandlungen in Asylverfahren vorbereitet werden und die Spracherkennung manipuliert werden könnte.[94] Tatsächlich heißt es vor allem, dass die Fehleranfälligkeit nie durch eine fachaufsichtliche Kontrolle überprüft wurde und extern ohne Rückgriff auf verwendete Algorithmen nicht nachzuvollziehen ist. Verschiedene Sprachwissenschaftler*innen bezweifelten, dass die Sprachzuordnung zuverlässig sein kann.[95]

---

[91] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 34.

[92] BT-Drs 19/6647: Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018. Antwort auf Frage 11.

[93] Ebd., Antwort auf Frage 14.

[94] Ebd., Antwort auf Frage 16.

[95] Siehe unter anderem bei P. Hummel: Software soll Dialekt von Asylbewerbern untersuchen, 17.03.2017, Welt; A. Biselli:

Eine sachgerechte Einschätzung der Verlässlichkeit und Indizwirkung für alle Verfahrensbeteiligten, von den BAMF-Mitarbeitenden bis zu den zuständigen Richter*innen, ist damit aber unmöglich. Für eine betroffene Person ist ein unzutreffendes Ergebnis schwer angreifbar. Und in der Praxis droht damit vor allem, dass den Ergebnissen eine Zuverlässigkeit zugesprochen wird, die ihnen in der Sache nicht zukommt.

Seit 2015: Datenträgerauswertung in den Ausländerbehörden

Schon zwei Jahre vor dem BAMF konnten Ausländerbehörden auf Datenträger von Ausländer*innen zugreifen. Während das BAMF als Bundesbehörde für Geflüchtete und die Durchführung ihres Asylverfahrens zuständig ist, sind Ausländerbehörden zumeist auf Ebene des Landkreises oder einer kreisfreien Stadt angesiedelt, für alle Menschen ohne deutsche Staatsangehörigkeit zuständig und entscheiden unter anderem über Aufenthaltserlaubnisse, Niederlassungserlaubnisse oder auch die Durchführung von Abschiebungen. Durch eine Änderung des § 48 AufenthG dürfen sie seit dem 27. Juli 2015 auf Geräte von Ausländer*innen zugreifen, die sich nicht ausweisen können oder wollen, um so die Identität und Staatsangehörigkeit festzustellen und Abschiebungen durchzusetzen.

Über die genaue Praxis und die Häufigkeit der Nutzung durch die Ausländerbehörden ist flächendeckend wenig bekannt, da ihre Zuständigkeiten landesrechtlich geregelt sind. In einer Antwort auf eine Schriftliche Frage des Abgeordneten Niklas Schrader (LINKE) im Berliner Abgeordnetenhaus aus dem August 2018 antwortete die Senatsverwaltung für Inneres und Sport, dass in Berlin die Informationen ausschließlich durch eine*n bei der Ausländerbehörde beschäftigten Volljurist*in händisch gesichtet und ausgewertet würden.[96] Die gesichteten Informationen umfassen laut Senatsverwaltung Telefonnummern mit Vorwahl, die dazugehörigen Namen, gegebenenfalls Adressen, Telefonprotokoll, SMS, WhatsApp-Nachrichten und solche über vergleichbare Nachrichtendienste, E-Mails und Fotos.

Im Zeitraum von Juli 2015 bis August 2018 seien im Land Berlin insgesamt 40 Geräte ausgewertet worden. In Einzelfällen seien die Zugangsdaten bei einem Provider ermittelt worden, statistisch werde dies jedoch nicht erfasst.

Software, die an der Realität scheitern muss, 17.03.2017, Zeit Online; A. Biselli: Eine Software des BAMF bringt Menschen in Gefahr, 20.08.2018, Vice/Motherboard.

[96] Abgeordnetenhaus Berlin Drucksache 18/15903: Zugriff auf private Datenträger durch die so genannte Ausländerbehörde, 16.08.2018.

E. Über die Grenzen hinweg: Datenträgerauswertung bei Geflüchteten in Europa

Nicht nur Deutschland reagierte auf den Anstieg von Asylsuchenden ab dem Jahr 2015 mit der Einführung neuer Befugnisse und Technologien zur Auswertung von Datenträgern. Das European Migration Network der EU-Kommission berichtete im Dezember 2017,[97] dass die Auswertung von Smartphones und anderen Datenträgern neben Deutschland zum damaligen Zeitpunkt nur in den Niederlanden und Estland als Standardmaßnahme im Asylverfahren vorgesehen sei. Sogar obligatorisch soll eine Datenträgerauswertung außerdem in Lettland sein, jedoch nur auf Basis von Strafgesetzen. Dem Bericht zufolge ist die Datenträgerauswertung als mögliche Maßnahme zudem in Italien, Litauen, Norwegen und Kroatien vorgesehen. Weiter sind Befugnisse hierzu für Migrations- und Sicherheitsbehörden auch in Österreich, Dänemark und Belgien eingeführt worden.

Zwischen den Ländern unterscheidet sich dabei erheblich, zu welchem Zweck die Daten genutzt werden, wie häufig die Maßnahmen eingesetzt werden, in welchem Umfang Daten ausgelesen werden und welche Behörde für die Datenträgerauslesung zuständig ist. Häufiger als von Migrationsbehörden werden Geräte dabei von Polizeibehörden beschlagnahmt und ausgewertet. Auffällig ist jedoch, dass in allen Ländern wenig bis gar keine Informationen zu dieser Praxis öffentlich sind.

Dänemark und Norwegen

Zu den ersten Ländern, die Datenträger Geflüchteter auswerteten, gehörten Dänemark und Norwegen. Laut der dänischen Tageszeitung Dagbladet Information begann die dänische Polizei 2015, im Rahmen von Asylverfahren und ohne den Verdacht von Straftaten, Daten von Smartphones, SIM-Karten und anderen Datenträgern Geflüchteter auszulesen und zu speichern.[98] Aus der Antwort der dänischen Reichspolizei auf eine Informationsfreiheitsanfrage, die der GFF vorliegt, geht hervor, dass dies jedoch nur bei einem vergleichsweise kleinen Anteil von Geflüchteten tatsächlich durchgeführt wurde. Von Mai bis Dezember 2016 wurden demnach 383 Mobiltelefone ausgelesen wurden, im gesamten Jahr 2017 waren es 503. Die Polizei hat in diesen Fällen die Geräte beschlagnahmt, ausgelesen und dann die gewonnenen Informationen an die Einwanderungsbehörde weitergegeben. Zulässiges Ziel der Maßnahmen ist es, wie bei den BAMF-Maßnahmen in Deutschland, Informationen über Identität und Herkunft der Geflüchteten zu erhalten. Soweit die Polizei aber Verdachtsmomente für Straftaten erhält,

[97] European Migration Netzwork (2017): EMN Synthesis Report for the EMN Focussed Study 2017 – Challenges and practices for establishing the identity of third-country nationals in migration procedures.

[98] M. K. Stræde, S. Gjerding: Hundredvis af asylansøgeres mobiler kopieret af politiet, Dagbladet Information, 17.02.2016.

nutzt sie auch diese Zufallsfunde.[99] Die Datenträgerauslesung besteht laut dem Leiter des Nationalen Ausländerzentrums bei der dänischen Polizei Richard Østerlund la Cour aus einer nahezu vollständigen Kopie des Geräteinhalts, was auch Fotos und Videos umfasst. Die Tageszeitung Politiken zitiert la Cour folgendermaßen: „Wenn du ins Land kommst und sagst, du kommst aus Syrien, aber nichts als dein Gesicht hast, um es zu beweisen, ist das Handy der beste Weg, um festzustellen, ob du die Wahrheit sagst oder alle Anrufe nach Ghana gehen."[100]

Die Voraussetzungen für die Maßnahme wurden weiter abgesenkt. Während im Ausgangspunkt die Rechtsgrundlage eine Datenträgerauslesung vorsah, wenn diese für die Bestimmung von Herkunft und Identität als wichtig erachtet wurde, so ist dies seit einer Gesetzesänderung 2017 bereits dann zulässig, wenn anzunehmen ist, dass sie für das Asylverfahren von Bedeutung sein können (§ 40 Abs. 10 des dänischen Ausländergesetzes, Udlændingeloven).[101] Jesper Lund, Vorsitzender von IT-Politisk Forening, einer dänischen NGO für digitale Rechte, berichtet, dass die Rechtsgrundlage dabei breit interpretiert würde und die Auswertungen Mobiltelefone, Tablets und andere Geräte umfassen. Grundsätzlich sei die Auswertung ohne Zustimmung der betroffenen Person nur mit Richter*innenvorbehalt zulässig, darauf könne jedoch bei Gefahr in Verzug verzichtet werden (§ 806 Abs. 4 Retsplejeloven). „Die klare Absicht der dänischen Regierung war es, in mehr Fällen Mobiltelefone von Flüchtlingen zu beschlagnahmen, zweifellos um mehr Gründe für die Ablehnung von Asylanträgen zu finden", sagt Lund.

Wie das BAMF in Deutschland verwendet die dänische Polizei XRY von MSAB, um Informationen aus dem Handy zu extrahieren, was aus einer Antwort aus einer weiteren der GFF vorliegenden Informationsfreiheitsanfrage hervorgeht. Neben der Identitäts- und Herkunftsfeststellung ist die Auswertung der Daten aber auch zur Beurteilung des Asylantragsmotivs, zur Ermittlung möglicher Gründe für die Ablehnung des Asylantrags und zur Prüfung, ob der*die Asylbewerber*in eine Bedrohung für die dänische nationale Sicherheit darstellt, zulässig (§ 40 Abs. 10 Udlændingeloven).[102]

In Norwegen wurde die Praxis der Datenträgerauswertung 2016 medial diskutiert, da die Polizei die Telefone mehrerer unbegleiteter minderjähriger Geflüchteter beschlagnahmte.[103] Im Oktober 2017 berichtete die norwegische Tageszeitung Aftenposten über Pläne für neue Ankunftszentren, in denen die Einwanderungsdirektion UDI und die Polizeieinwanderungs-

[99] Ebd.

[100] F. Hvilsom, M. Gram: Politiet tager asylbørns mobiler ved ankomst, Politiken, 15.02.2016.

[101] Eigene Übersetzung. Original: „Dokumenter og genstande, der må antages at være af betydning for at fastslå en udlændings identitet eller tilknytning til andre lande, eller som må antages at være af betydning for sagens oplysning, kan tages i bevaring, hvis det skønnes fornødent."

[102] Udlændinge- og Integrationsministeriet: Forslag til Lov om ændring af udlændingeloven, 05.04.2017.

[103] NTB: Norsk politi beslaglegger asylsøker-mobiler, 16.02.2016.

behörde PU GPS-Pfade, Bilder, App-Nutzung, Internetaktivitäten, Nachrichten und Kontakte zur Überprüfung der Anträge von Asylbewerbern nutzen können.[104] Die Datenextraktion geschieht analog zur deutschen Praxis bereits während des Registrierungsprozesses. Auch Social-Media-Informationen wurden im Zusammenhang mit Asylanträgen systematisch analysiert.[105] Im Januar 2017 legte die norwegische Regierung einen Vorschlag für eine Änderung des Ausländergesetzes (Utlendingsloven) vor, die der Polizei weitere Befugnisse zur Durchsuchung von Telefonen und Geräten von Asylbewerbern geben sollte.[106] Bis dahin wurden Datenträger auf Grundlage des § 10 des Polizeigesetzes (Lov om politiet) beschlagnahmt, um Informationen zur Identität von Geflüchteten zu bekommen. Zukünftig sollten auch potentielle Informationen über Reiserouten oder ein mögliches Sicherheitsrisiko eine Datenauswertung rechtfertigen können.[107]

Belgien

Durch einer Gesetzesänderung aus dem Jahr 2017 dürfen Asylbehörden in Belgien die Herausgabe aller digitalen Medien von Geflüchteten verlangen und diese analysieren.[108] In der Praxis tun sie dies soweit noch nicht. Die Maßnahme ist laut Gesetz aber dann zulässig, wenn anzunehmen ist, dass ein*e Antragsteller*in Informationen zurückhält. Um welche digitalen Medien es dabei geht, ist nicht eingeschränkt, könnte also sogar den privaten E-Mail-Verkehr einbeziehen. Verweigern Antragsteller*innen die Herausgabe, verletzen sie ihre Mitwirkungspflichten und ihr Asylantrag kann abgelehnt werden. Der belgische Datenschutzbeauftragte kritisierte die Gesetzesinitiative und erklärte, dass die digitalen Informationen nur bei Bedarf und nicht systematisch angefordert werden dürften.[109] Er wies darauf hin, dass die Mitarbeitende der belgischen Migrationsbehörden nicht geschult sind, solche invasiven Eingriffe durchzuführen. Die Einschätzung, ob es Grund zur der Annahme gibt, dass der Asylbewerber Informationen zurückhält, sei subjektiv und schwer überprüfbar.

Er weist auch darauf hin, dass der Gesetzentwurf die Rechte des Betroffenen nicht schützt und nicht regelt, wie die Daten genau zu behandeln sind. Widerspruch kam auch von NGOs wie

[104] T. Olsen: Listhaugs nye ankomstsenter: Vil tappe mobiler og bruke avansert datainnsamling for å sjekke asylsøkere, Aftenposten, 26.10.2017.

[105] T. Olsen, L. L. Dragland: Slik kan Facebook avdekke løgn: Disse avslørte seg selv, Aftenposten, 12.07.2017; T. Olsen: Asyladvokat: – Facebook er et sted mange driver med tull og fanteri, Aftenposten, 13.07.2017.

[106] Norwegisches Justizministerium: Høringsnotat-Forslag til endring i utlendingsloven og utlendings-forskriften–visitasjon og undersøkelse av asylsøkere ved registre-ringmv, 11.01.2017.

[107] Ebd.

[108] Original: "Loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demanders d'asile et de certaines autres catégories d'étrangers", online abrufbar hier.

[109] Commission de la protection de la vie privée (2017): Avis d'initiative relatif au projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'ac

der Association pour le droit des étrangers, die kritisierte, dass die Zustimmung der Geflüchteten nicht freiwillig sei, da die Betroffenen aus Angst vor Ablehnung ihres Asylantrags unter Druck stehen.[110]

Die Befugnisse wurden seit Inkrafttreten des Gesetzes noch nicht angewendet. Im Jahr 2018 wurde gegen das Gesetz eine Beschwerde beim Belgischen Verfassungsgericht eingereicht.[111] Eine Verhandlung der Beschwerde habe bisher nicht stattgefunden, wie die zuständigen Anwälte der GFF mitgeteilt haben.

Österreich

Ebenso wie in Belgien gibt es auch in Österreich gesetzliche Befugnisse zur Datenträgerauswertung, die jedoch ebenfalls noch nicht genutzt werden. Seit September 2018 ist es Organen des öffentlichen Sicherheitsdienstes in Österreich erlaubt, Geflüchteten Datenträger abnehmen und auswerten zu können, um im Asylverfahren die Identität aufzuklären oder Fluchtrouten zu bestimmen.[112] Die Fluchtroute soll bestimmt werden, um Asylsuchende möglichst in andere EU-Staaten zu überführen: Wenn sich durch die Datenauswertung ergibt, dass die geflüchtete Person durch einen anderen EU-Mitgliedstaat nach Österreich eingereist ist, dann ist dieser Staat nach der Dublin-III-Verordnung der EU zur Aufnahme verpflichtet.[113]

Das Ergebnis der Auswertung sowie die Sicherungskopie sollen die Sicherheitsbehörden dem Bundesamt für Fremdenwesen und Asyl übermitteln können. Laut einer Anfragebeantwortung des österreichischen Innenministeriums aus dem Juli 2019 liegt es unter anderem an datenschutzrechtlichen Gründen, dass die Maßnahmen bisher nicht angewendet werden.[114] Die österreichische Regierung erklärt in der Gesetzesbegründung, dass vor allem auf Handys gespeicherte Geolokalisierungsdaten, aber auch Fotos von nicht physisch vorgelegten Dokumenten nützlich sein können. Ein Richter*innen- oder andere Genehmigungsvorbehalte sind nicht vorgesehen, ebenso existiert keine Einschränkung für die Verwertung von Daten aus dem Kernbereich der privaten Lebensgestaltung. Mildere Mittel sind im Gesetzestext nicht explizit definiert. Die österreichische NGO epicenter.works, die sich für digitale Rechte einsetzt, kritisiert, dass die Polizei von Datenträgern jeglicher Art vollständige Sicherungskopien erstellen kann,

---

[110] V. Henkinbrant: D'une curieuse idée du consentement : une plongée sans fond dans la vie privée des demandeurs d'asile, September 2017.

[111] Ciré: Un recours contre des lois liberticides et contraires à la Constitution, 12.09.2018.

[112] Das Fremdenrechtsänderungsgesetz fügte dazu dem Fremdenpolizeigesetz 2005 zwei neue Abschnitte zur Auswertung von Datenträgern hinzu; s. Bundesgesetzblatt für die Republik Österreich: 56. Bundesgesetz: Fremdenrechtsänderungsgesetz 2018 – FrÄG 2018 (NR: GP XXVI RV 189 AB 207 S. 36. BR: 9998 AB 10020 S. 883.), 14.08.2018.

[113] Bundesministerium für Inneres: Erläuterungen zur Regierungsvorlage zum Fremdenrechtsänderungsgesetz, 2018.

[114] Bundesminister für Inneres, Dr. Wolfgang Peschorn: Entscheidungen des BFA und Evaluation aktueller Maßnahmen im Bereich des Asylwesens, 3614/AB XXVI. GP, 23.07.2019.

ohne anschließend Daten wieder löschen zu müssen, die nicht den vorgesehenen gesetzlichen Zwecken dienen.[115] Die NGO bemängelt zudem eine Verletzung des Gleichheitsgrundsatzes, weil die strengeren Voraussetzungen, die sogar für strafrechtliche Ermittlungen gelten, auf Asylsuchende nicht anzuwenden sind - „und das obwohl die davon Betroffenen weder Verdächtige noch Beschuldigte sind, noch auf sonstige Weise mit Verbrechen in Verbindung stehen". Die UN-Flüchtlingsorganisation UNHCR kritisierte, dass in Österreich pauschal Sicherheitsbehörden Datenträger ausgewerten dürfen, obwohl für Asylverfahren Migrationsbehörden zuständig sind.[116]

Großbritannien

In Großbritannien enthält der „Data Protection Act" aus dem Jahr 2018 weitreichende Ausnahmen für Datenschutzgarantien nach der Datenschutzgrundverordnung, wenn Daten für die Aufrechterhaltung effektiver Einwanderungskontrolle verarbeitet werden. Die Menschenrechtsorganisation Privacy International kritisierte das. An Grenzen und darüber hinaus würden große Mengen an Daten gesammelt, um Menschen zu tracken und zu identifizieren. Die NGO Platform for International Cooperation on Undocumented Migrants hat daher eine Beschwerde bei der Europäischen Kommission eingereicht.[117] Darüber hinaus ist die Auslesung von Datenträgern allgemein durch die Polizei weit verbreitet, nicht nur bei Verdächtigen von Straftaten, auch bei Zeug*innen und Opfern.[118] Die Menschenrechtsorganisation Privacy International hat diese Praxis untersucht und festgestellt, dass dazu oftmals gesetzliche Grundlagen und grundlegende Schutzmechanismen fehlen.[119] Wie sehr Geflüchtete von solchen Auslesungen betroffen sind, beispielsweise während Polizeikontrollen an Grenzen, ist nicht bekannt.

In Großbritannien gibt es jedoch noch weitreichendere Befugnisse: Durch eine Gesetzesänderung im Polizeigesetz im Jahr 2013 erhielten neben Polizeibeamt*innen auch britische Einwanderungsbeamt*innen die Befugnis, auf Handys und andere technische Geräte von Asylbewerbern zuzugreifen.[120] Das geht über eine Handyauswertung, wie sie in Deutschland möglich ist, weit hinaus und ermöglicht es, heimliche Überwachungsmaßnahmen durchführen, Abhörgeräte zu platzieren sowie Telefone und Computer zu hacken und zu durchsuchen. Die Gesetzesände-

[115] A. Adensamer, A. Hanel, L. D. Klausner, H. R. Pecina: Stellungnahme zum Fremdenrechtsänderungsgesetz von epicenter.works, 15.05.2018.

[116] UNHCR: UNHCR-Analyse des Entwurfs für das Fremdenrechtsänderungsgesetz 2018, 09.05.2018.

[117] PICUM: PRESS RELEASE – Advocates bring first GDPR complaint to EU against UK data protection law for violating data rights of foreigners, 01.07.2019.

[118] Big Brother Watch UK (2019): Digital Strip Watch. The Police's Data Investigation of Victims.

[119] Privacy International (2018): Digital stop and search: how the UK police can secretly download everything from your mobile phone.

[120] Durch den „Crime and Courts Act 2013" wurde § 93 Abs. 5 des Polizeigesetzes (Police Act 1997) geändert und die Liste derjenigen, die befugt sind, in Eigentum und drahtlose Kommunikation einzugreifen, um Migrationbeamte erweitert.

rung und neue Praxis blieb zunächst weitgehend unbemerkt, bis The Guardian Observer 2016 darüber berichtete.[121] Einem Briefing-Dokument des Innenministeriums für Migrationsbeamt*innen zufolge soll damit Einwanderungskriminalität effektiv bekämpft werden.[122] Ein Vertreter des britischen Innenministeriums bestätigte, dass mit der Maßnahme die Verteilung gefälschter Reisedokumente unterbunden worden sei. Auf eine Anfrage der Labour Party im Unterhaus gab James Brokenshire, damaliger Minister für Sicherheit und Einwanderung im Innenministerium[123] an, dass Einwanderungsbeamt*innen die Befugnis seit 2013 ausschließlich zur Untersuchung und Verhütung schwerer Straftaten, die sich auf Einwanderungs- oder Staatsangehörigkeitsdelikte beziehen ausüben dürften - und dies seither auch täten.[124] Ob das Verfahren auch zur Überprüfung der Aussagen von Asylbewerber*innen im Asylverfahren genutzt wurde, ist bisher nicht bekannt.

Zu vermuten ist, dass die zuständigen Behörden Hard- und Software des israelischen Mobilforensikherstellers Cellebrite verwenden: Dieser belieferte die Abteilung „UK Immigration Enforcement", im Mai 2018 ist eine Zahlung des britischen Innenministeriums in Höhe von 45.000 Pfund für „laboratory and scientific equipment" im Transparenzverzeichnis des britischen Innenministeriums verzeichnet.[125]

[121] M. Townsend: Revealed: immigration officers allowed to hack phones, The Guardian, 10.04.2016.

[122] Eigene Übersetzung. Original: „to ensure that immigration officers can deploy a full range of investigative techniques to deal effectively with all immigration crime."

[123] Schriftliche Frage des Parlamentariers Andy Slaughter: Immigration Officers: Surveillance, Antwort vom 22.03.2016.

[124] Original: "Immigration officers have had the power to carry out property interference, including interference with equipment, since 2013 through an amendment to the Police Act 1997.They may only use the power to investigate and prevent serious crime which relates to an immigration or nationality offence and have done so since 2013. The Bill maintains this position whilst strengthening safeguards and oversight."

[125] UK Home Office: Transparency data – Home Office spending over £25,000: May 2018.

F. Fazit

Mit der Auswertung der Daten von Smartphones und anderen Datenträgern greift das BAMF tief in die Privatsphäre von Geflüchteten ein, die in diesem Moment besonders vulnerabel sind: Sie befürchten negative Folgen für ihr Asylverfahren, wenn sie die Herausgabe verweigern und stehen unter Druck, können die Folgen der Auswertung kaum einschätzen und wissen nicht, was genau mit ihren Daten passiert. Der Schutz im Verfahren durch BAMF-interne Kontrollen der Rechtmäßigkeit ist unzureichend und nachträglicher Rechtsschutz für Betroffene schwer zugänglich und kurzfristig wenig aussichtsreich.

Angesichts intransparenter Vorgehensweise und unbekannter verwendeter Auswertungsverfahren (Algorithmen) können weder die breitere Öffentlichkeit noch Entscheider*innen und Richter*innen die Zuverlässigkeit der Ergebnisse sachgerecht einordnen. Die Entscheidung über den Asylantrag wird damit mehr und mehr von den Ergebnissen fehleranfälliger IT-Systeme abhängig gemacht.

Im Verhältnis dazu ist der Nutzen der mehrere Millionen Euro teuren Technik gering: In weniger als der Hälfte der Fälle liefert eine Auswertung überhaupt verwertbare Informationen, Widersprüche zu den Angaben von Geflüchteten deckte die Auswertung nur in den seltensten Fällen auf: Bei etwa 20.000 ausgelesenen Geräten bis Ende 2019 geschah das hochgerechnet in weniger als 120 Fällen. Es profitieren damit in erster Linie die Hersteller von Überwachungstechnologie, die mit ihren Angeboten gut verdienen.

Das Vorgehen des BAMF muss als Teil eines nationalen wie internationalen Trends verstanden werden, neue technische Kontroll- und Überwachungstechnologien werden an geflüchteten Menschen erprobt und eingesetzt. Anschließend droht die Ausweitung des Einsatzes dieser Technologien zu weiteren Zwecken und auf weitere Teilen der Bevölkerung. Denn nicht nur Deutschland setzt auf die Datenträgerauswertung. Auch in anderen europäischen Ländern begannen Asyl- und Polizeibehörden in den vergangenen Jahren, den digitalen Hausstand Geflüchteter zu beschlagnahmen und zu analysieren. Asylverfahren werden zunehmend digitalisiert – sei es mit automatischen Abgleichen von Daten mit anwachsenden Datenbanken, Mobilforensik wie sie sonst nur in Strafverfahren eingesetzt wird oder Künstlicher Intelligenz zur Suche nach auffälligen Geflüchteten. Der Mensch mit seiner persönlichen Fluchtgeschichte tritt in den Hintergrund und wird zum reinen Datensatz.

Jede*r Geflüchtete hat das Recht auf ein faires Asylverfahren. Dazu gehört auch, dass es nicht von einer automatisierten und schwer überprüfbaren Entscheidung abhängen darf, ob Schutz gewährt wird oder nicht. Auch Geflüchtete haben ein Recht auf informationelle Selbstbestim-

mung und auf Vertraulichkeit und Integrität informationstechnischer Systeme. Für sie darf kein Datenschutz zweiter Klasse gelten. Ihre besondere Vulnerabilität und Schutzlosigkeit darf nicht ausgenutzt werden, um neue Kontroll- und Überwachungstechnologie zu testen.

Es zeigt sich damit insgesamt, dass eine umfassende, auch juristische Überprüfung und Auseinandersetzung mit der Datenträgerauswertung des BAMF notwendig ist.