Kanzlei
Für Aufenthaltsrecht

Jentsch Rechtsanwälte

Kanzlei für Aufenthaltsrecht, Jentsch Rechtsanwälte, Eichendorffstr. 13, 10115 Berlin

Eichendorffstraße 13
10115 Berlin
Telefon (030) 252 987 77 /-78
Telefax (030) 252 987 85
E-Mail kontakt@aufenthaltsrecht.net

Bürozeiten:
Mo, Di, Do, Fr.: 10:00 - 12:00 Uhr
Mo, Do: 15:00 - 17:00 Uhr
Mittwoch geschlossen

Verwaltungsgericht Hannover
Leonhardtstraße 15

30175 Hannover

per beA

04.05.2020 (…)

Unser Zeichen:
(…)

Die auslagenfreie Übersendung einer weiteren Abschrift jedes gerichtlichen Schreibens, jeder gerichtlichen Entscheidung, jedes Verhandlungsprotokolls und jedes vor Gericht abgeschlossenen Vergleichs für jede(n) von uns vertretene(n) Beteiligte(n) wird hiermit ebenso beantragt, wie die Übersendung entsprechender Doppelstücke der Schriftsätze der weiteren Beteiligten.

K l a g e

des (…),

Kläger,

- Bevollmächtigte: Jentsch Rechtsanwälte, Eichendorffstraße 13, 10115 Berlin -

gegen

die Bundesrepublik Deutschland, diese vertreten durch den Bundesminister des Innern, dieser vertreten durch den Leiter des Bundesamtes für Migration und Flüchtlinge, Frankenstr. 210, 90461 Nürnberg,

Beklagte,

wegen Auswertung von Datenträger, § 15a AsylG.

Namens und in Vollmacht des Klägers, Vollmacht anbei, erheben wir Klage und beantragen,

1.
festzustellen, dass die Anordnung der Beklagten an den Kläger (Gz. Beim BAMF: ...), sein Mobiltelefon herauszugeben und seine Zugangsdaten für eine Auswertung zur Verfügung zu stellen, rechtswidrig war.

2.
festzustellen, dass die Beklagte nicht berechtigt war,

a. die Daten des Klägers von seinem Mobiltelefon auszulesen und mittels einer Software auszuwerten,

b. den aus der Auswertung des Mobiltelefons des Klägers generierten Ergebnisreport zu speichern,

c. den Ergebnisreport für das Asylverfahren des Klägers freizugeben und der Entscheidung über seinen Asylantrag zugrundezulegen.

3.
Die Beklagte zu verpflichten, den aus dem Mobiltelefon des Klägers generierten Ergebnisreport zu löschen.

4.
dem Kläger Prozesskostenhilfe unter Beiordnung des unterzeichnenden Rechtsanwaltes zu bewilligen.

Prozesskostenhilfeunterlagen werden alsbald nachgereicht.

Es wird zugleich angeregt,

das Verfahren gem. Art. 100 Abs. 1 GG i.Vm. § 80 Abs. 1 BVerfGG auszusetzen und dem Bundesverfassungsgericht mit der Frage vorzulegen, ob § 15 Abs. 2 Nr. 6 und § 15a AsylG mit Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG vereinbar ist.

Weiterhin beantragen wir

Akteneinsicht und Aktenmitnahme

bezüglich der beizuziehenden Verwaltungsvorgänge der Beklagten. Wegen der räumlichen Entfernung unserer Kanzlei vom Gerichtsort bitten wir um Übersendung der Akten in unser Büro, hilfsweise an das Verwaltungsgericht Berlin, Kirchstraße 7, 10557 Berlin, um dort Einsicht nehmen zu können.

Gliederung

A. Sachverhalt

Mit der gegenständlichen Klage wendet sich der Kläger gegen die Auslesung und Auswertung seines Mobiltelefons durch das Bundesamt für Migration und Flüchtlinge (BAMF) sowie die dieser zeitlich vorausgegangene Herausgabeanordnung und die nachfolgende Verwendung der generierten Datensätze für sein Asylverfahren. Mittelbar rügt er die Verfassungswidrigkeit der Rechtsgrundlagen der §§ 15 Abs. 2 Nr. 6, 15a AsylG.

I. Rechtsgrundlagen

Durch das Gesetz zur besseren Durchsetzung der Ausreisepflicht vom 20. Juli 2017 wurde § 15 Abs. 2 Nr. 6 AsylG neugefasst und § 15a AsylG eingeführt. Nach § 15 Abs. 2 Nr. 6 AsylG ist „der Ausländer“ nun verpflichtet,

> *im Falle des Nichtbesitzes eines gültigen Passes oder Passersatzes (…) auf Verlangen alle Datenträger, die für die Feststellung seiner Identität und Staatsangehörigkeit von Bedeutung sein können und in deren Besitz er ist, den für die Ausführung des Gesetzes zuständigen Behörden vorzulegen, auszuhändigen und zu überlassen.*

§ 15 Abs. 4 AsylG ermöglicht eine Durchsuchung von Asylsuchenden und ihren Sachen, wenn sie der Aufforderung zur Herausgabe nicht nachkommen.

§ 15a Satz 1 AsylG erklärt die Auswertung der herausgegebenen Datenträger für zulässig,

> *soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Absatz 2 Nummer 6 erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann.*

Im Übrigen verweist § 15a AsylG auf die bereits durch Gesetz vom 27. Juli 2015 eingeführten §§ 48 Abs. 3a und 48a AufenthG. Nach § 48 Abs. 3a Satz 3 AufenthG hat „der Ausländer“ die notwendigen Zugangsdaten für eine zuverlässige Auswertung zur Verfügung zu stellen; kommt er dem nicht nach, können die Zugangsdaten nach § 48a AufenthG von den Telekommunikationsdienstleistern erhoben werden. Im Übrigen begrenzt § 48 Abs. 3a AufenthG die Auswertungsbefugnis. Eine Auswertung ist ausgeschlossen, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden (Satz 2); Erkenntnisse aus dem Kernbereich dürfen nicht verwertet werden und sind unverzüglich zu löschen (Satz 5 und 6). Die Auswertung darf nur von Bediensteten mit Befähigung zum Richteramt erfolgen (Satz 4).

II. Praktische Durchführung der Datenträgerauswertung

Die Rechtsgrundlage erlaubt das Auslesen und Auswerten im Asylverfahren.

> Zum ganzen Biselli/Beckmann (2019), Das Smartphone, bitte – Digitalisierung von Migrationskontrolle in Deutschland und Europa, https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf., **Anlage 1**.

Die Rechtsgrundlage erlaubt dies ohne den Zeitpunkt zu präzisieren. Ausweislich der Dienstanweisungen „Identitätsfeststellung" sowie „AVS Auslesen von mobilen Datenträgern" des BAMF sollen Datenträger regelmäßig bereits bei der Registrierung der Asylsuchenden ausgelesen werden. Zum Teil geschieht dies aber auch zu anderen Zeitpunkten im Asylverfahren, etwa im Rahmen eines Widerrufs- oder Rücknahmeverfahrens nach den §§ 73 ff. AsylG.

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 fünf Phasen unterteilen: 1. Der Asylsuchende wird mündlich und schriftlich auf seine Pflicht zur Überlassung von Datenträgern hingewiesen und aufgefordert, diese herauszugeben und zu entsperren. 2. Alle auf dem Gerät befindlichen Daten werden ausgelesen, dieser Gesamtdatensatzes wird automatisch nach bestimmten Kategorien analysiert und ein digitaler Prüfbericht erstellt. 3. Anschließend wird dieser Prüfbericht in einem Datentresor des BAMF gespeichert. 4. Auf Antrag der*des Entscheiders*in prüft eine*n BAMF-interne*n Volljurist*in die Freigabe des Prüfberichts. 5. Der freigegebene Prüfberichts wird in die Asylakte überführt.

Ausgelesen werden Datenträger, wenn die geflüchtete Person keinen gültigen Pass oder Passersatz vorlegen kann.

> vgl. Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Identitätsfeststellung, **Anlage 2**, Ziff. 3.1.1.; Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, Ziff. 1.

Wann ein Pass oder Passersatz ungültig ist, ist in § 11 PassG festgelegt. Danach ist ein Dokument insbesondere ungültig, wenn es eine einwandfreie Feststellung der Identität nicht zulässt, verändert worden ist oder die Gültigkeitsdauer abgelaufen ist (§ 11 Abs. 1 Nr. Nr. 1-3 PassG).

Die Validität der Pässe mancher Länder lässt sich aus technischen Gründen nicht unmittelbar vor Ort feststellen; auch in diesen Fällen liest das BAMF die Datenträger der betroffenen Personen aus. Insgesamt existieren drei Prüfebenen der physikalisch-technischen Untersuchung (PTU). Nur die erste Prüfebene findet vor Ort beim BAMF statt. Wenn die Gültigkeit oder Echtheit der Dokumente nicht vor Ort in der ersten Prüfebene abschließend festgestellt werden kann, findet die Auslesung der Datenträger statt; die zweite und die dritte Prüfebene werden nicht abgewartet,

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, S. 2.

Zu den vor Ort untersuchbaren Dokumenten zählen laut der Dienstanweisung „Asylverfahren – Urkundenprüfung" maschinenlesbare Dokumente aller Herkunftsländer, zusätzlich alle anderen Dokumente aus Syrien, dem Irak, Iran, Eritrea, der Ukraine, Afghanistan und der Russischen Föderation,

> Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Urkundenprüfung, Stand 06/18, **Anlage 4**

Legen Asylsuchende keinen Pass oder Passersatz vor, der vom BAMF nach einer Überprüfung vor Ort als gültig anerkannt wird, werden Datenträger ausgelesen. Die Anhörung sei nicht als vorab einzubeziehendes milderes Mittel zu klassifizieren. Auch sonstige Dokumente wie ID-Karten, Führerscheine, Flüchtlingsausweise und Militärausweise werden laut Dienstanweisung Identitätsfeststellung erst vor der Auswertung als mildere Mittel in Betracht gezogen, gelten aber jeweils und nach allgemeinen Grundsätzen nicht als Passersatzvorlage, der die Anwendbarkeit der Vorschrift sperrt,

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3,** Ziff. 3.1., Ziff. 3.1.1. und Ziff. 3.1.2.

Die Asylsuchenden, deren Datenträger ausgelesen werden sollen, werden bei der Registrierung unter Hinweis auf ihre gesetzlichen Mitwirkungspflichten aufgefordert, ihre Datenträger herauszugeben und zu entsperren. Für das weitere Vorgehen bestimmt die Dienstanweisung:

> *Mit dem Dokument D1705 (Datenträger_Erklärung), das dem MARiS-Aktenbestand zugefügt wird, wird festgehalten, ob der Antragsteller einen Datenträger aushändigt, die Aushändigung verweigert oder nicht besitzt. Wird die Herausgabe des Datenträgers verweigert, wird der Antragsteller erneut auf*

> *seine Mitwirkungspflicht hingewiesen. Außerdem wird er darauf hingewiesen, dass bei Nichtmitwirkung das Verfahren gem. der vom Antragsteller unterschriebenen Erstbelehrung nach § 33 Abs. 1 AsylG als zurückgenommen angesehen werden kann und das Verfahren eingestellt wird.* (Anlage 3, Ziff. 3.1.1.)

Die ausgehändigten Datenträger werden über ein USB-Verlängerungskabel an einem speziell dafür erworbenen Gerät des schwedischen Herstellers MSAB, dem „MSAB Kiosk" angeschlossen und dort ausgelesen. In der Folge wird zunächst ein kompletter Rohdatensatz ausgelesen und daraus automatisch ein elektronischer Ergebnisreport generiert. Dieser wird in einem Datentresor gespeichert. Nach Abschluss des Vorgangs wird der Datenträger der asylsuchenden Person zurückgegeben, die Kopie des kompletten Rohdatensatzes wird automatisch gelöscht,

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, Ziff. 3.1.1. und Anlage 4, Ziff. 1.

Der mithilfe der Software XRY des Herstellers MSAB erstellte Ergebnisreport enthält in Form von Tortendiagrammen Informationen zu den Ländervorwahlen der im Adressbuch gespeicherten Kontakte, der ein- und ausgehenden Anrufe und der Textnachrichten verschiedener Messenger. In Form von Tabellen werden die Gesamt-Anrufdauer und die Zahl der Textnachrichten zu und von Nummern mit den jeweiligen Ländervorwahlen dargestellt. In einer weiteren Tabelle werden die Anzahl und Häufigkeit der Top-Level-Domains aufgerufener Internetadressen aufbereitet. Darüber hinaus werden Geolokationsdaten auf einer Karte angezeigt, wofür Fotos sowie möglicherweise Apps ausgewertet werden. Ob darüber hinaus App-Informationen, gespeicherte WLAN-Netzwerke oder aufgezeichnete GPS-Daten betrachtet werden, ist nicht bekannt. Das BAMF gibt hierzu keine Informationen preis. Zusätzlich wird mithilfe einer zusätzlich erworbenen Software des Herstellers T3K die Sprache von Textnachrichten analysiert und in Tabellen das Ergebnis nach Zahl und Häufigkeit der in den Nachrichten verwendeten Sprachen dargestellt. Im Fall des Arabischen wird auch der verwendete Dialekt angegeben. Als Hinweis auf die Identität werden aus verschiedenen, im Einzelnen benannten Apps ermittelte Namen, Account-Namen, IDs, Geburtstage und E-Mail-Adressen dargestellt. Einzelheiten lassen sich Schulungsunterlagen des BAMF entnehmen,

> Bundesministerium für Migration und Flüchtlinge, Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte, Einführung in die neuen IT-Tools, Schulung AVS-Mitarbeiter, Entscheider und Volljuristen, 30.08.2017, **Anlage 5**, S. 104 ff.

Nach der „Dienstanweisung Asylverfahren Identitätsfeststellung“ wird der Ergebnisreport nur dann verwendet, wenn der*die Entscheider*in ihn anfordert und ein*e beim BAMF angestellte Volljurist*in ihn für das Asylverfahren freigibt. Eine Anforderung soll erfolgen, wenn basierend auf einer Gesamtschau der verfügbaren Informationen die Identität und Staatsangehörigkeit nicht eindeutig geklärt erscheint und auch nicht mit milderen Mitteln geklärt werden kann. Als mildere Mittel kommen laut Dienstanweisung Asylverfahren Identitätsfeststellung nur Dokumente in Betracht, „die durch ein Lichtbild die Identität belegen können und vom Bundesamt auf ihre Echtheit überprüft werden können“. Dies seien etwa ID-Karten, Führerscheine, Flüchtlingsausweise und Militärausweise.

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, Ziff. 3.1. und Ziff. 3.1.2.

Hält der*die Entscheider*in den Ergebnisreport nicht für verfahrensrelevant, hat er*sie die Löschung zu veranlassen,

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, Ziff. 3.1.2.; Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Urkundenprüfung, Stand 06/18, **Anlage 4**, Ziff. 2.

Der*die zuständige Volljurist*in überprüft, ob der Ergebnisreport für das Verfahren freizugeben ist. Bejahendenfalls wird er 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. Andernfalls wird die Löschung veranlasst,

> Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung, **Anlage 3**, Ziff. 3.1.3.

Die elektronische Akte, deren Teil der Ergebnisreport nach der Freigabe wird, darf gem. § 7 Abs. 3 AsylG für zehn Jahre nach unanfechtbarem Abschluss des Asylverfahrens gespeichert bleiben. § 8 Abs. 3 AsylG ermöglicht die Weitergabe der im Asylverfahren erhobenen Daten an zahlreiche andere Behörden, etwa zur Abwehr erheblicher Gefahren für Leib und Leben von Asylsuchenden und Dritten, zur Verfolgung von Straftaten und Ordnungswidrigkeiten sowie zur Aufdeckung und Verfolgung von zu Unrecht erbrachten Sozialleistungen.

III. Aussagekraft und Zuverlässigkeit der Datenträgerauswertung

Die Bundesregierung hat auf mehrere Kleine Anfragen der Fraktion Die Linke im Deutschen Bundestag Zahlen zur Häufigkeit des Auslesens und Auswertens der Datenträger von Asylsuchenden sowie zu den daraus ermittelten Ergebnissen vorgelegt,

> BT-Drs. 19/8701, 25.03.2019, **Anlage 6**, Antwort auf Fragen 9, 9a, 9b und 9c, S. 28 f.;
>
> BT-Drs. 19/11001, 19.06.2019, **Anlage 7**, Antwort auf Fragen 6, 6a, 6b und 6c, S. 17 ff.;
>
> BT-Drs. 19/13945, 09.10.2019, **Anlage 8**, Antwort auf Fragen 6, 6a, 6b und 6c, S. 19 ff.

Aus diesen Zahlen ist ersichtlich, dass nur etwas über ein Drittel der Erstantragsteller*innen über 14 Jahren ohne Pass bzw. Passersatz angibt, im Besitz eines Datenträgers zu sein. Bei etwa einem Viertel der herausgegebenen Datenträger gelingt die Auslesung bereits technisch nicht. Nur bei weniger als der Hälfte der ausgelesenen Datenträger beantragt die über den Asylantrag entscheidende Person die Auswertung, bei einem erheblichen Teil dieser Fälle verweigert der*die zuständige Volljurist*in die Freigabe. Die durchgeführten Datenträgerauswertungen liefern überwiegend keine aussagekräftigen Daten, sie widerlegen die Angaben der Asylsuchenden nur in ganz wenigen Fällen. Einzelheiten sind der folgenden Tabelle zu entnehmen:

	2018	1. Quartal 2019	2. Quartal 2019
Erstantragsteller*innen > 14 J. ohne Pass/ Passersatz im Besitz von Datenträgern	35 %	41 %	40 %
Anteil technisch auslesbarer Datenträger	74 %	77%	74 %
Erstellte Rohdatensätze	11.389	3.502	2.435
Datenträger-Erstauswertungsanträge	5.431	1.538	1.009
Zur Auswertung freigegebene Datenträger	3.308	1.236	789
davon keine aussagekräftigen Daten	64 %	55 %	56 %
Bestätigung der Angaben	34 %	44 %	42 %
Widerlegung der Angaben	2 %	1 %	2 %

Die Gründe dafür, dass aus der Datenträgerauswertung vielfach keine aussagekräftigen Daten gewonnen werden, sind struktureller Art. Zum einen analysiert die Software nicht die Staatsangehörigkeit selbst, sondern Datenkategorien wie die Ländervorwahlen bei den

Telekommunikationsverbindungsdaten. Diese Daten können für die Staatsangehörigkeit allenfalls Indizwirkung haben. Da heute viele Menschen Kontakte in zahlreiche Länder haben, lässt sich die Herkunft aus einem bestimmten Staat so nicht sicher ermitteln. Die Ermittlung der Identität aus E-Mail-Adressen und Login-Daten ist ebenfalls mit Unsicherheiten behaftet, geben doch viele Menschen bei Online-Applikationen nicht ihren bürgerlichen Namen an. Hinzu kommt, dass erhebliche Risiken einer Erfassung unrichtiger Daten bestehen. So können die auf dem Mobiltelefon einer asylsuchenden Person gespeicherten Daten auch von Vorbesitzer*innen herrühren. Bei der Ermittlung von Geolokationsdaten aus Fotos ist zu beachten, dass diese extrem fehleranfällig sind. Die softwaregestützte Spracherkennung in Textnachrichten ist mit dem erheblichen Risiko einer fehlerhaften Zuordnung verbunden. Das gilt in besonderer Weise für die Zuordnung arabischer Dialekte, für die zunächst arabische Schriftzeichen in lateinische transkribiert werden müssen und bei denen sich deshalb eine große Vielfalt von unterschiedlichen, phonetisierenden Schreibweisen entwickelt hat.

IV. Asylverfahren des Klägers

Der Kläger ist syrischer Staatsangehöriger (…). Er reiste am (…) in das Bundesgebiet ein und stellte am (…) einen Asylantrag (Gz. Beim BAMF: …). Mit Bescheid vom (…) wurde ihm die Flüchtlingseigenschaft zuerkannt.

Mit Schreiben vom (…) wurde dem Kläger mitgeteilt, dass ein Widerrufsverfahren (Gz. Beim BAMF: …) bezüglich der Zuerkennung der Flüchtlingseigenschaft eingeleitet wird.

Abgesehen von einer Kopie eines Familienbuches aus Syrien verfügt der Kläger über keine Identitätsdokumente aus Syrien.

Im Rahmen der Befragung über das Widerrufsverfahren am (…) wurde der Kläger von der Beklagten aufgefordert, sein Mobiltelefon zur Auslesung zu überlassen (Bl. ...). Die Aufforderung wurde damit begründet, dass der Kläger keine gültigen Identitätspapiere vorlegen kann. Im Zusammenhang mit der Befragung wurde zugleich verfügt, dass der Kläger eine Sprachprobe abgeben muss (Bl. ...). Auch fand eine Befragung zu seiner Herkunft statt (Bl. ...). Dem Kläger wurde in der Befragung nicht mitgeteilt, welche Daten aus seinem Mobiltelefon ausgelesen, analysiert oder in der Folge abgespeichert und kenntlich sein würden.

Am selben Tag wurde das Mobiltelefon des Klägers ausgelesen und es wurde ein Ergebnisreport angefordert. Aus dem sodann erstellten Ergebnisreport (Bl. ...) geht hervor, (…).

In einem abschließenden Vermerk vom (…)wurde festgestellt, dass nach Aktenlage keine Anhaltspunkte beständen, die an der behaupteten Herkunft des Klägers zweifeln lassen. Mit

Schreiben vom (…) teilte die Beklagte dem Kläger mit, dass das Widerrufsverfahren eingestellt und an der getroffenen Entscheidung festgehalten wird.

Zu dem vorgelegten Mobiltelefon des Klägers und dessen Nutzung kann ergänzend wie folgt vorgetragen werden: (…)

B. Feststellungsanträge

I. Zulässigkeit

Die Klage ist bezüglich des Antrags zu 1. als Fortsetzungsfeststellungsklage, bezüglich der Anträge zu 2. als Feststellungsklage zulässig.

1. Statthafte Klageart

Der Klageantrag zu 1. betrifft die Anordnung des BAMF an den Kläger, sein Mobiltelefon herauszugeben und die Zugangsdaten zur Verfügung zu stellen. Die behördliche Aktualisierung der kraft Gesetzes nach § 15 Abs. 2 Nr. 6 AsylG und § 15a Satz 2 AsylG i.V.m. § 48 Abs. 3a Satz 3 AufenthG bestehenden Pflicht ist ein Verwaltungsakt. Zwar handelt es sich um einen Vorgang innerhalb eines Verwaltungsverfahrens. Diesem kommt hier jedoch ein über die bloße Vorbereitung der Sachentscheidung hinausgehender eigenständiger Regelungsgehalt zu. Verwaltungsaktqualität hat eine Anordnung zur Mitwirkung immer dann, wenn dem Betroffenen nicht (wie etwa bei der Anforderung eines Gutachtens) lediglich andere Nachteile entstehen, wenn er ihr nicht nachkommt, sondern sie selbstständig vollstreckt werden kann,

> Stelkens in Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35 Rn. 148, 153.

Die Herausgabeanordnung ist derart gesondert vollstreckbar, und zwar regeln § 15 Abs. 4 und § 15a Satz 2 AsylG i.V.m. § 48a Abs. 1 AufenthG spezielle Vollstreckungsmöglichkeiten für die BAMF-Mitarbeitenden. Die Möglichkeit einer Durchsuchung nach § 15 Abs. 4 AsylG beinhaltet eine Vollstreckung der Pflicht zur Herausgabe des Datenträgers. Im allgemeinen Polizeirecht ist anerkannt, dass die dort als Standardmaßnahme vorgesehene Durchsuchung als Realakt ihre eigene Durchführung in sich trägt. Dadurch wird ein Rückgriff auf das VwVG entbehrlich,

> Mosbacher in Engelhardt/App/Schlatmann, VwVG, 11. Aufl. 2017, Vor § 6 Rn. 1a.

Das ist auf die Durchsuchung durch Mitarbeitende des BAMF übertragbar. Für den Fall, dass Asylsuchende ihre Zugangsdaten nicht zur Verfügung stellen, ermöglicht § 15a Satz 2 AsylG i.V.m. § 48a Abs. 1 AufenthG, diese von den Telekommunikationsdiensteanbietern zu erheben. Auch das

beinhaltet eine Vollstreckung der Anordnung, und ist insofern der Vollstreckung der Anordnung im Wege der Ersatzvornahme vergleichbar.

Die Anordnung an den Kläger hat sich erledigt, nachdem dieser ihr nachgekommen ist. Ob das BAMF dazu berechtigt war, die geforderten Mitwirkungshandlungen vom Kläger zu verlangen, kann mit einer Fortsetzungsfeststellungsklage analog § 113 Abs. 1 Satz 4 einer gerichtlichen Überprüfung zugeführt werden.

Die Klageanträge zu 2. betreffend den Vorgang der automatisierten Auslesung und Auswertung des Mobiltelefons, die Speicherung des Ergebnisreports und dessen Übernahme in die elektronische Asylakte beziehen sich auf Verwaltungsrealhandeln. Insoweit ist die Feststellungsklage gem. § 43 VwGO einschlägig. Einem feststellungsfähigen Rechtsverhältnis steht nicht entgegen, dass die Maßnahme verwaltungsintern erfolgte. Ein streitiges Rechtsverhältnis im Sinne einer rechtlichen Beziehung zwischen den Beteiligten besteht insofern, als zu klären ist, ob das BAMF zur Verarbeitung personenbezogener Daten des Klägers – mit potentiellen Folgen für dessen Asylverfahren – berechtigt war.

2. Sachentscheidungsvoraussetzungen

Die bei Feststellungs- und Fortsetzungsfeststellungsklagen analog § 42 Abs. 2 VwGO darzulegende Klagebefugnis ergibt sich aus dem Umstand, dass das BAMF personenbezogene Daten des Klägers erhoben, gespeichert und verarbeitet hat. Der Kläger macht, wie unten näher aufgeführt, geltend, dass das Auslesen und die Auswertung seines Mobiltelefons sowie die Verwendung des dabei erzeugten Datensatzes (Ergebnisreports) in seinem Asylverfahren gegen sein Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, hilfsweise gegen sein Grundrecht auf informationelle Selbstbestimmung verstößt. Auch die zur Ermöglichung dieser Maßnahmen ergangene Herausgabeanordnung verstößt jedenfalls gegen die allgemeine Handlungsfreiheit.

Der Kläger hat ein berechtigtes Interesse an der Feststellung der Rechtswidrigkeit der angegriffenen Maßnahmen. Die Verarbeitung der Daten des bei der Auswertung des Mobiltelefons des Klägers generierten Ergebnisreports wirkt gegenwärtig noch fort. Der Report ist Teil der elektronischen Asylakte, die nach Abschluss des Asylverfahrens gem. § 7 Abs. 3 AsylG für zehn Jahre gespeichert bleibt. Aber auch bezüglich der erledigten Anordnung zur Herausgabe des Datenträgers und des Kopierens und Auswertens des mittlerweile gelöschten Rohdatensatzes hat der Kläger ein berechtigtes Interesse an der Feststellung, dass das BAMF hierzu nicht befugt war. Dem Bundesverwaltungsgericht zufolge ist ein Fortsetzungsfeststellungsinteresse mit Blick auf Art. 19 Abs. 4 GG bei erledigten Eingriffsmaßnahmen unabhängig von deren Schwere stets zu

bejahen, wenn andernfalls kein wirksamer Rechtsschutz zu erlangen wäre. Davon ist bei Maßnahmen auszugehen, die sich typischerweise so kurzfristig erledigen, dass sie ohne die Annahme eines Fortsetzungsfeststellungsinteresses regelmäßig keiner Überprüfung im gerichtlichen Hauptsacheverfahren zugeführt werden könnten,

> BVerwGE 146, 303 = NVwZ 2013, 1481 Rn. 30 ff.

Die Herausgabeanordnung nach § 15 Abs. 2 Nr. 6 AsylG ist darauf angelegt, dass ihr die Betroffenen umgehend nachkommen. Die Auslesung des Datenträgers und die softwaregestützte Erzeugung des Ergebnisreports aus dem Rohdatensatz ist ein Vorgang von Minuten oder allenfalls Stunden. Rechtsschutz gegen diese Eingriffsmaßnahmen ist allein durch eine nachträgliche gerichtliche Feststellung der Rechtswidrigkeit zu erlangen.

Ein Vorverfahren ist bei Erledigung des Verwaltungsaktes vor Ablauf der Widerspruchsfrist nicht notwendig, bei Verwaltungsrealhandeln ohnehin nicht vorgesehen.

Die Klage ist im Übrigen in Bezug auf alle Anträge auch fristgerecht erhoben worden: (…)

3. Keine Unzulässigkeit nach § 44a VwGO

§ 44a VwGO steht der Zulässigkeit der Klage nicht entgegen. Gemäß § 44a VwGO können Rechtsbehelfe gegen behördliche Verfahrenshandlungen nur gleichzeitig mit den gegen die Sachentscheidung zulässigen Rechtsbehelfen geltend gemacht werden. Zwar werden mit den Feststellungsanträgen Maßnahmen im Rahmen des Asylverfahrens isoliert angegriffen. Der Ausschlussgrund des § 44a Satz 1 VwGO ist hier jedoch nicht anwendbar.

Bezüglich des Klageantrags zu 1. betreffend die Herausgabeanordnung ist der Ausnahmetatbestand der vollstreckbaren Maßnahme nach § 44a Satz 2 VwGO einschlägig.

Hinsichtlich der Klageanträge zu 2. ist hier eine ungeschriebene Ausnahme von § 44a Satz 1 VwGO anzuerkennen. Eine einschränkende Auslegung ist mit Blick auf Art. 19 Abs. 4 GG geboten, wenn die Verfahrenshandlung eine gegenüber der Sachentscheidung selbstständige Beschwer enthält. Insofern kann es für die gerichtliche Überprüfbarkeit der Rechtmäßigkeit nicht darauf ankommen, ob auch in der Sachentscheidung selbst eine Beschwer liegt und sie deshalb inzident bei der Anfechtung einer Sachentscheidung überprüft werden kann. Wie das BVerwG ausgeführt hat, gebietet Art. 19 Abs. 4 GG

> eine einschränkende Auslegung des § 44a S. 1 VwGO in den Fällen, in denen bei einer Abwägung zwischen dem von § 44a S. 1 VwGO verfolgten Zweck der

> Gewährleistung eines effektiven Verwaltungsverfahrens und den Belangen des Betroffenen Letzteren eindeutig der Vorrang einzuräumen ist, insbesondere deshalb, weil die negativen Folgen für diesen besonders schwer wiegen (…). So können etwa Verfahrenshandlungen, die in materielle Rechtspositionen des Betroffenen eingreifen und dadurch eine selbstständige, im Verhältnis zur abschließenden Sachentscheidung andersartige Beschwer enthalten, selbstständig angefochten werden.
>
> BVerwGE 141, 196 = NJW 2012, 792 Rn. 32.

Das BVerfG hat betont, dass die Fachgerichte bei der Anwendung von § 44a VwGO das Grundrecht aus Art. 19 Abs. 4 GG im Blick behalten müssen. Der Ausschluss einer gerichtlichen Überprüfung von Verfahrenshandlungen dürfe für den Rechtssuchenden nicht zu unzumutbaren Nachteilen führen, die in einem späteren Prozess nicht mehr vollständig zu beseitigen sind,

> BVerfG, NJW 1991, 415 (416).

Da das Widerrufsverfahren des Klägers eingestellt wurde, ist er durch die Sachentscheidung nicht beschwert. Das ändert aber nichts daran, dass die Auswertung seines Mobiltelefons in seine Grundrechte eingreift. Nach Art. 19 Abs. 4 GG muss eine gerichtliche Überprüfung deshalb möglich sein. Aus demselben Grund ist Rechtsschutz gegen strafprozessuale Zwangsmaßnahmen nicht nur inzident im Rahmen von Rechtsmitteln gegen eine Verurteilung, sondern unabhängig vom Ausgang des Strafverfahrens unmittelbar in analoger Anwendung des § 98 Abs. 2 Satz 2 StPO anerkannt. Die Strafgerichte kommen damit einer Verpflichtung aus Art. 19 Abs. 4 GG nach,

> BVerfG NJW 1997, 2165.

Der vorliegende Fall unterscheidet sich von anderen Konstellationen wie der Verpflichtung zur Beibringung eines medizinisch-psychologischen Gutachtens im Verfahren zur Wiedererlangung der Fahrerlaubnis, für die die Rechtsprechung eine Ausnahme zu § 44a Satz 1 VwGO abgelehnt hat. In diesen Fällen betont die Rechtsprechung, dass mit dem Ausschluss einer isolierten Anfechtung die Anordnung der Begutachtung nicht der gerichtlichen Kontrolle entzogen werde. Wenn das Gutachten für den Betroffenen günstig ausfalle, habe er die Möglichkeit, die Rechtmäßigkeit der Anordnung im Rahmen einer Klage auf Erstattung der Untersuchungskosten geltend zu machen,

> BVerwG, Beschl. v. 17.05.1994, 11 B 157.93 = BeckRS 1994, 30435808.

Im vorliegenden Fall ist eine alternative Rechtsschutzmöglichkeit nicht ersichtlich.

II. Begründetheit

Die Klage ist begründet. Das BAMF war zu den angegriffenen Maßnahmen nicht berechtigt.

Zwar lagen die Voraussetzungen der Ermächtigungsgrundlagen der §§ 15 Abs. 2 Nr. 6, 15a AsylG i.V.m. § 48 Abs. 3a AufenthG vor. Der Kläger konnte keinen gültigen Pass oder Passersatz vorweisen. Auch wurde die Auslesung in Person des Einzelentscheiders (…) durch einen Volljuristen vorgenommen.

Die Regelungen sind jedoch verfassungswidrig. Sie verletzen den Kläger in seinem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG in der Ausprägung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme.

Der Prüfung der §§ 15 Abs. 2 Nr. 6, 15a AsylG am Maßstab des Grundgesetzes steht der Anwendungsvorrang des Unionsrechts nicht entgegen. Zwar fallen die Maßnahmen mit Blick auf die Richtlinie 2013/32/EU (Asylverfahrensrichtlinie) und auf die Datenschutz-Grundverordnung (DSGVO) in den Anwendungsbereich des Unionsrechts. Jedoch handelt es sich hier nicht um einen vollharmonisierten Bereich, der allein am Maßstab der Unionsgrundrechte zu prüfen ist. Die Asylverfahrensrichtlinie verpflichtet die Mitgliedsstaaten nicht zur Datenträgerauswertung. Die DSGVO regelt die Zulässigkeit der Verarbeitung personenbezogener Daten grundsätzlich abschließend, enthält aber in Art. 6 Abs. 1 UAbs. 1 lit. e i.V.m. Abs. 3 Satz 1 lit. b eine Öffnungsklausel, die die Datenerhebung im öffentlichen Interesse auf einer mitgliedsstaatlichen Rechtsgrundlage ermöglicht. Als Prüfungsmaßstab sind daher hier die Grundrechte des Grundgesetzes heranzuziehen,

> vgl. BVerfG, Beschl. v. 6.11.2019, 1 BvR 16/13, Rn. 41 ff. – Recht auf Vergessen I.

1. Eingriff der §§ 15 Abs. 2 Nr. 6, 15a AsylG in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

a) Maßgebliches Grundrecht

Das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist seit der Leitentscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts anerkannt. Damit wird es der lückenfüllenden Funktion des allgemeinen Persönlichkeitsrecht gerecht, denn das Recht auf informationelle Selbstbestimmung trägt

> *den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus. (BVerfGE 120, 274 (312f.)).*

Das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist jedoch nicht beim Zugriff auf solche informationstechnischen Systemen anwendbar, die nach ihrer technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten (BVerfGE 120, 274 (313). Es ist als Maßstab aber anzuwenden, wenn

> *die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.*
>
> *BVerfGE 120, 274 (314).*

§ 15 Abs. 2 Nr. 6, 15a AsylG ermächtigt zur Auslesung und Auswertung von Datenträgern. Auch wenn in der derzeitigen Praxis nur Mobiltelefone mit großem Funktionsumfang (Smartphones) und Mobiltelefone mit geringerem Funktionsumfang (Featurephones) ausgelesen und ausgewertet werden, sind von der Ermächtigungsgrundlage auch andere informationstechnische

Systeme umfasst. In der Begründung des Regierungsentwurfs werden neben Mobiltelefonen auch Tablets und Laptops genannt.

> BT-Drs. 18/11546, **Anlage 9**, S. 23.

Das Gesetz erfasst damit Systeme, die eine Vielzahl von personenbezogenen Daten enthalten, insbesondere die vom Bundesverfassungsgericht angesprochenen Personalcomputer und Mobiltelefone mit großem Funktionsumfang.

Das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme schützt „insbesondere vor einem heimlichen Zugriff, durch den auf dem System vorhandene Daten (…) ausgespäht werden“,

> BVerfGE 120, 274 (314).

„Insbesondere“ bedeutet nicht „ausschließlich“. Auch offene Zugriffe auf Datenträger wie ein Mobiltelefon, auf denen eine große Menge personenbezogener Daten gespeichert ist (hier wird auch vom „digitalen Hausstand“ gesprochen), unterscheiden sich qualitativ von Zugriffen auf Einzeldaten, vor denen das Recht auf informationelle Selbstbestimmung Schutz bietet: Hier gewinnen staatliche Stellen mit einer einzigen Maßnahme einen Einblick in wesentliche Teile der Lebensgestaltung einer Person. Insoweit ist zwar anders als bei einer heimlichen Infiltration nicht der grundrechtliche Schutz der *Integrität* informationstechnischer Systeme gegenüber externer Ausspähung, Überwachung und Manipulation betroffen. Wohl aber wird in die selbstständige grundrechtliche Teilgewährleistung der *Vertraulichkeit* der vom System erzeugten, verarbeiteten und gespeicherten Daten eingegriffen,

> vgl. BVerfGE 120, 274 (314); zum zweigliedrigen Schutzbereich des Grundrechts auch Gersdorf in Gersdorf/Paal, BeckOK-Informations- und Medienrecht, Stand 01.08.2019, Art. 2 GG Rn. 27; Böckenförde, JZ 2009, 925 (928).

Insofern macht es keinen Unterschied, ob der Staat durch eine Online-Durchsuchung oder durch die physische Beschlagnahme des Datenträgers Einblicke in die Lebensgestaltung einer Person gewinnt. Auch offene Zugriffe auf informationstechnische Systeme im Rahmen einer lokalen Durchsuchung können Eingriffstatbestände in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme begründen,

Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 167; Hornung, CR 2008, 299 (303); Michalke, StraFo 2008, 287 (291); Polenz in Kilian/Heussen, Computerrechts-Handbuch, EL 29 Feb. 2011, Teil 13 Rn. 32.

Geht man demgegenüber davon aus, dass das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme allein vor heimlichen Zugriffen schützt, ist das allgemeine Persönlichkeitsrecht in der Ausprägung des Rechts auf informationelle Selbstbestimmung betroffen.

b) Eingriffsqualität der einzelnen Schritte der Datenträgerauslesung und -auswertung

Den ersten Grundrechtseingriff stellt der technische Vorgang der Auslesung sämtlicher Daten des Datenträgers, bei dem also der Rohdatensatz kopiert wird, sowie dessen anschließende Auswertung und die Generierung des elektronischen Ergebnisreports mithilfe des „MSAB Kiosk“ dar, bei dem noch kein Mensch Kenntnis von persönlichen Daten der Asylsuchenden erlangt. An einem Eingriff fehlt es im Rahmen von elektronischen Datenverarbeitungsprozessen lediglich dann, wenn Daten nur zufällig am Rande miterfasst und unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden gelöscht werden,

BVerfG, NJW 2019, 827 Rn. 48.

Demgegenüber werden die Datenträger der Asylsuchenden ohne anerkannte Ausweispapiere vom BAMF vollständig kopiert und kurzfristig gespeichert, um für das Verfahren möglicherweise bedeutsame Daten zu erheben.

Dem Grundrechtseingriff kann nicht entgegengehalten werden, dass die Asylsuchenden ihre Datenträger dem BAMF freiwillig übergäben und ihre Daten damit freiwillig preisgäben, mithin auf ihr Grundrecht verzichteten. Zwar scheinen die Asylsuchenden nach den Alternativen zum Ankreuzen die Wahl zu haben, der Herausgabe des Datenträgers zuzustimmen oder sie zu verweigern. Doch ist die Mitwirkung nicht als bloße Obliegenheit, sondern als gesetzliche Pflicht ausgestaltet, die mit einer Durchsuchung gem. § 15 Abs. 4 AsylG durchgesetzt werden kann. Zudem wertet das BAMF den Asylantrag von Personen, die ihre Datenträger nicht herausgeben, wegen Nichtbetreiben des Verfahrens gem. § 33 Abs. 1 AsylG als zurückgenommen.

Ein weiterer technischer Grundrechtseingriff ist die längerfristige Speicherung des von der Software bei der Auswertung des Rohdatensatzes erstellten Ergebnisreports in einem Datentresor.

Eigenständige Eingriffsqualität kommt sodann der Prüfung des Ergebnisreports durch eine*n Volljurist*in auf einen Auswertungsantrag des*der Entscheider*in zu. Hier erhält erstmals ein Mensch Kenntnis von den auf dem Datenträger gespeicherten Daten, selbst wenn der Datenträger für das weitere Verfahren nicht freigegeben wird.

Wird der Ergebnisreport freigegeben, erfolgt schließlich ein weiterer, vertiefter Grundrechtseingriff dadurch, dass der*die Entscheider*in den Report der Entscheidung über den Asylantrag zugrunde legt und unter Umständen in der Anhörung Fragen zu im Report dargestellten Daten stellt. Er*sie kann diese Daten dann als Grundlage seiner Befragung in der Anhörung im Asylverfahren sowie zur Entscheidung über den Asylantrag heranziehen. Er*sie kann zudem die in der Tabelle über die Identität vermerkten Daten, etwa den Namen eines Facebook-Profils zum Anlass für weitere eigenständige Recherchen nehmen. Zudem können entliche weitere Behörden unter besonderen Voraussetzungen auf die Asylakte zugreifen und das Ergebnis der Handydatenauswertung damit ebenfalls zur Kenntnis nehmen.

2. Verstoß gegen verfassungsrechtliche Rechtfertigungsanforderungen

Gesetzliche Ermächtigungen zu Eingriffen in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme sowie in das Recht auf informationelle Selbstbestimmung sind nur unter strengen verfassungsrechtlichen Rechtfertigungsanforderungen zulässig, insbesondere sind die Grundsätze der Bestimmtheit und Verhältnismäßigkeit zu beachten. Diesen Anforderungen werden die §§ 15 Abs. 2 Nr. 6, 15a AsylG i.V.m. § 48 Abs. 3a AufenthG nicht gerecht.

a) Unverhältnismäßigkeit der Datenträgerauswertung zu migrationspolitischen Zwecken

Die Datenträgerauswertung dient der Klärung der Identität und Staatsangehörigkeit von Asylsuchenden, um unberechtigte Asylanträge ablehnen und die Betroffenen leichter abschieben zu können. Gegenüber dieser migrationspolitischen Zielsetzung erweist sich der von §§ 15 Abs. 2 Nr. 6, 15a AsylG ermöglichte Grundrechtseingriff als unverhältnismäßig.

(1) Datenträgerauswertung ist zur Klärung von Staatsangehörigkeit und Identität ungeeignet

Die Verhältnismäßigkeit einer Ermächtigungsgrundlage setzt voraus, dass die Maßnahmen überhaupt geeignet sind, den Zweck des Gesetzes zu erreichen. Im Bereich der Datenverarbeitung bedeutet dies (wie es in Art. 5 Abs. 1 lit. c DSGVO ausdrücklich normiert ist), dass nur solche Daten

erhoben und weiterverarbeitet werden dürfen, die für den jeweiligen Zweck überhaupt erheblich sein können. Schon gar nicht dürfen sachlich unrichtige Daten verarbeitet werden.

Die Art und Weise, wie das BAMF mithilfe einer Software aus Datenträgern der Asylsuchenden einen Datensatz generiert, ist zu der beabsichtigten Klärung der Staatsangehörigkeit und Identität nicht geeignet. Der mit 1 bis 2 Prozent sehr geringe Anteil der Fälle, in denen die Auswertung zu Ansätzen geführt hat, die die Angaben von Asylsuchenden widerlegen, erklärt sich daraus, dass die Software Datenkategorien erfasst, die lediglich Hinweise auf die Staatsangehörigkeit und die Identität ermöglichen und zudem ein erhebliches Risiko der Erzeugung unrichtiger und möglicherweise fehlleitender Daten besteht.

(a) Mangelnde Beweiskraft der gespeicherten Datenkategorien

In einem verwaltungsgerichtlichen Verfahren könnte das BAMF mit dem Ergebnisreport die Behauptung, die Person habe eine andere als die bei der Anhörung angegebene Staatsangehörigkeit, nicht nachweisen. Maßgeblich sind gem. § 98 VwGO die Vorschriften der ZPO über das Beweisverfahren. Bei dem Ergebnisreport handelt es sich um ein elektronisches Dokument einer öffentlichen Stelle, dass nach § 371a Abs. 3 i.V.m. § 418 ZPO vollen Beweis der darin bezeugten Tatsachen begründet. Bezeugt werden im Ergebnisreport aber nur die dort erfassten Merkmale, nicht die Staatsangehörigkeit selbst. Hierfür stellen sie lediglich ein Indiz dar, das die asylsuchende Person durch den Vortrag alternativer Erklärungsansätze widerlegen kann.

So kann die Auswertung der Verbindungsdaten zwar zeigen, dass die betroffene Person häufig in ein bestimmtes Land telefoniert bzw. Textnachrichten dorthin gesendet und von dort empfangen hat. Daraus ist jedoch nicht zwingend zu schließen, dass sie die Staatsangehörigkeit dieses Landes hat. Regelmäßige Kontakte in ein Land können auch daraus resultieren, dass jemand dort eine Zeit lang gelebt hat oder sich gegenwärtig Angehörige oder Freunde dort aufhalten. Gerade bei Menschen auf der Flucht ist es wahrscheinlich, dass ihre Familien- und Bekanntenkreis aus dem Heimatland sich ebenfalls nicht mehr dort sondern in unterschiedlichen Ländern befindet oder aber, dass sie mit Menschen im Kontakt stehen, die sie auf der Flucht oder im neuen Gastland kennengelernt haben.

Die auf einer Karte dargestellten Geolokationsdaten geben ebenfalls keine sicheren Hinweise auf die Staatsangehörigkeit der asylsuchenden Person. Sie könnten auch lediglich auf Aufenthalte in einem Land hinweisen.

Daten über die in Textnachrichten verwendete Sprachen geben in vielen Fällen nicht einmal einen Hinweis auf ein bestimmtes Land, werden viele Sprachen – namentlich diejenigen früher

europäischer Kolonialmächte – doch in zahlreichen Ländern gesprochen. Auch die Verbreitung der von der Software erhobenen arabischen Dialekte deckt sich nicht mit den Staatsgrenzen. So wird Tschadisch-Arabisch (Schuwa) im Tschad, Südsudan, Sudan, Kamerun, Niger, Nigeria und der Zentralafrikanischen Republik gesprochen. Golf-Arabisch (Chalidschi) ist in Barain, Irak, Kuwait, Katar, den Vereinigten Arabischen Emiraten, Saudi-Arabien, Iran und im Oman verbreitet. Und levantinisches Arabisch wird in Jordanien, Syrien, den palästinensischen Autonomiegebieten und Israel sowie in Syrien gesprochen. Abgesehen davon können Asylsuchende auch Sprachen bzw. Dialekte sprechen, die in dem Land ihrer Staatsangehörigkeit nicht verbreitet sind. Das ist beispielsweise der Fall, wenn Flüchtlinge (z.B. während der Flucht) für längere Zeit im Ausland gelebt haben oder in einer Familie aufgewachsen sind, die nicht aus ihrem Heimatland kommt.

Auch die Identität von Asylsuchenden lässt sich mit den von der Software gespeicherten Daten nicht zuverlässig ermitteln. Viele Menschen geben in E-Mail-Adressen und als Login-Daten bei Apps nicht ihren bürgerlichen Namen, sondern einen Spitz- oder Fantasienamen an.

Zu beachten ist schließlich, dass Asylsuchende ein erst vor kurzem erworbenes Mobiltelefon ohne ausreichend große und damit aussagekräftige Datenbestände besitzen können.

Sowohl den BAMF-Mitarbeiter*innen als auch den Gerichten fehlt es an der Kompetenz, die Aussagekraft der Daten einschätzen zu können. In den Schulungsunterlagen des BAMF sind 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." Ab welcher Datenmenge von einem verlässlichen Ergebnis auszugehen ist, ist nicht angegeben,

> Bundesministerium für Migration und Flüchtlinge, Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte, Einführung in die neuen IT-Tools, Schulung AVS-Mitarbeiter, Entscheider und Volljuristen, 30.08.2017, **Anlage 5**, S. 110 ff.

(b) Erhebliche Risiken der automatisierten Erzeugung unrichtiger Daten

Unrichtige Daten sind zur Erreichung des Zwecks des Verfahrens von vornherein nicht geeignet. Gerade der automatisierte Erzeugungsvorgang birgt aber erhebliche Fehlerquellen.

So ist bei den von der Software erfassten Geolokationsdaten nicht klar, ob sich die betroffene Person selbst an dem auf der Karte im Ergebnisreport verzeichneten Ort aufgehalten hat. Viele Menschen haben auf ihren Smartphones eine Vielzahl von mit Ortsangaben (Geotag) versehenen Fotos gespeichert, die ihnen zugesendet worden sind. Geotags sind zudem sehr fehleranfällig. In

diesem Sinne wird auch im Ergebnisreport des Klägers ausgeführt „aufgrund der hochdynamischen Natur der App-Daten" nicht in jedem Fall garantiert werden kann, dass sich das Gerät auch am erkannten Ort befunden habe (Bl. …).

Bei der Spracherkennungssoftware bestehen Zweifel, ob sie Sprachen und insbesondere arabische Dialekte zutreffend zuordnet. Gerade die Tatsache, dass es bei der Transkription arabischsprachiger Nachrichten in lateinische Zeichen mehrere Umsetzungsmöglichkeiten gibt, kann leicht zu Zuordnungsfehlern führen. Da Zuordnungsfehler bei arabischen Dialekten sehr viel wahrscheinlicher sind als bei mit lateinischem Alphabet geschriebenen Sprachen, werden zudem arabischsprechende Asylsuchende benachteiligt, weil sie höchstwahrscheinlich mit einem höheren Risiko der Falschzuordnung konfrontiert sind. Forschungsarbeiten zu automatischen Sprachidentifikationssystemen, die auf einer Satzebene zwischen Modernem Hocharabisch und ägyptischem Dialekt unterscheiden sollen, erreichten etwa Genauigkeiten von 85,5 Prozent.

> Vgl. **Anlage 10**: H. Elfardy, M. Diab (2013): Sentence Level Dialect Identification in Arabic, Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, ACL 201.

Eine weitere Fehlerquelle kann darin liegen, dass trotz ausreichender Datenmenge auf einem Smartphone nur ein Ausschnitt der Daten durch das BAMF ausgewertet werden kann. Dies ist etwa der Fall, 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. Das ist zum Beispiel bei dem populären Messengerdienst Telegram so. Schließlich ist zu beachten, dass Daten von Datenträgern erhoben werden können, die gar nicht von deren Besitzer*in stammen. Neben der Tatsache, dass auf einem Datenträger Daten gespeichert sein können, die der ihn nutzenden Person zugesendet worden sind, ist auch denkbar, dass jemand einen Datenträger von einer anderen Person übernommen hat, ohne dass deren Benutzerprofil zuvor vollständig gelöscht wurde. Zudem kann es vorkommen, dass Datenträger durch mehrere Personen genutzt werden, sich z.B. eine Person dort für eine App angemeldet hat. Schließlich erscheint es nicht völlig ausgeschlossen, dass einzelne Asylsuchende in Kenntnis der Untersuchungen (bestimmte) Daten von ihren Telefonen löschen und dadurch das Ergebnis verfälschen. Der Bundesregierung sind laut eigener Aussage zumindest einzelne Fälle bekannt, in denen Antragsteller*innen „manipulierte" Mobilgeräte vorgelegt haben,

BT-Drs. 19/6647, Antwort auf Frage 3, **Anlage 11**.

Ob bei der Erzeugung des Ergebnisreports zutreffende Daten dargestellt werden, ist für die Bediensteten des BAMF nicht erkennbar. Sie kennen die Algorithmen nicht und haben keinen technischen Sachverstand, um die Zuverlässigkeit der automatisierten Erhebung einzuschätzen. Handreichungen des BAMF für seine Bediensteten, wie sie feststellen können, dass Datenträger nur unvollständig ausgewertet worden sind und dass keine von Dritten erzeugten Daten erhoben worden sind, finden sich nicht.

Auch die Verwaltungsgerichte haben in etwaigen Rechtsstreitigkeiten in aller Regel keine Möglichkeit, die sachliche Richtigkeit und den Beweiswert der vom BAMF ermittelten Daten und durch die Software des BAMF gezogenen Schlüsse im Ergebnisreports einzuschätzen. Anders als sonstige Beweismittel in Gerichtsverfahren kann die Qualität und Zuverlässigkeit der Datenträgerauswertung überhaupt nicht überprüft oder in Zweifel gezogen werden. Denn dazu wäre es notwendig, dass das BAMF die zugrunde liegenden Algorithmen offenlegt oder extern überprüfen ließe, um beispielsweise Fehlerquoten klar zu machen. Besonders bei der Spracherkennung wäre zwingend notwendig, dass das BAMF offenlegt, welchen „Trainingsdatensatz“ das BAMF verwendet, also wie viele Sprachproben welcher Sprache der Software als Lerndatensatz zugrunde gelegt wurde. Eine externe Überprüfung dieser Software ist aber weder individuell im Verfahren möglich noch behördlicherseits erfolgt. Angesichts der Schwere der möglichen Folgen einer falschen Entscheidung im Asylverfahren widerspricht dies dem Rechtsstaatsgebot (Art. 20 Abs. 3 GG).

(2) Unangemessenheit der Datenträgerauswertung zu migrationspolitischen Zwecken

Die Schwere des Grundrechtseingriffs darf bei einer Gesamtabwägung nicht außer Verhältnis zum Gewicht der ihn rechtfertigenden Zwecke stehen. Dieser Anforderung werden die §§ 15 Abs. 2 Nr. 6, 15a AsylG nicht gerecht.

Werten staatliche Stellen ein informationstechnisches System aus, auf dem sich eine Vielzahl von Daten befinden, die erhebliche Rückschlüsse über das Leben der Betroffenen zulassen, liegt darin ein intensiver Grundrechtseingriff. Zwar erfolgt in der derzeitigen Praxis im Wesentlichen nur eine automatisierte Auswertung von Metadaten, während Bedienstete des BAMF keine auf dem Datenträger gespeicherten Kommunikationsinhalte lesen. Doch greift die automatisierte Auswertung auf einen immensen Datenbestand zu. So verbinden insbesondere Smartphones große Mengen persönlicher Daten 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 und persönliche 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, sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen.

> **Anlage 12**: T. W. Boonstra, M. E. Larsen, H. Christensen (2015): Mapping dynamic social networks in real life using participants' own smartphones; 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.

Auch die Aussagekraft von Telekommunikationsverbindungsdaten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten gewinnen.

> BVerfGE 125, 260 (319).

Der Eingriff hat zudem eine erheblich Streubreite. Nach Angaben des Bundesministeriums des Innern wurden im Jahr 2018 insgesamt 11.389 Datenträger ausgelesen. Die gesetzlichen Voraussetzungen erfüllen indes deutlich mehr Personen. So konnten laut Innenministerium im Jahr 2018 45.322 Antragsteller*innen keine Identitätspapiere vorlegen, das entspricht 54,2 Prozent. Im ersten Quartal 2019 waren es sogar 55,4 Prozent (11.666 Antragsteller*innen).

> BT-Drs. 19/8701, 25.03.2019, **Anlage 6**, Antwort auf die Fragen 8 und 9; BT-Drs. 19/11001, **Anlage 7**, 19.06.2019, Antwort auf die Fragen 5 und 6.

Dies entspricht den Schätzungen der Bundesregierung im Vorfeld der Gesetzesänderung. In der Begründung des Gesetzentwurfs wurde 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.

> BT-Drs. 18/11546, **Anlage 9**, S.15.

Erfasst werden somit die Daten einer Vielzahl von Personen ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten oder einen individuell begründeten Verdacht,

> vgl. BVerfGE 125, 260 (318).

Die Erhebung von Telekommunikationsverbindungsdaten hat zudem immer auch zur Folge, dass persönliche Daten Dritter miterhoben werden.

Der Eingriff wird dadurch vertieft, dass das Gesetz zur Auslesung und Auswertung einer Vielzahl von Geräten ermächtigt. Die gesetzlichen Regelungen beschränken die Maßnahme nicht auf Smartphones, der Begriff „Datenträger“ ermöglicht grundsätzlich ebenso die Auswertung anderer Geräte, etwa als Featurephone bezeichnete einfachere Modelle von Mobiltelefonen, aber auch USB-Sticks, Festplatten, Tablets, Laptops oder sogar Fitnessarmbänder.

Die Datenträgerauswertung ist auch deshalb ein schwerwiegender Grundrechtseingriff, weil die Betroffenen im Vorfeld der Anhörung eingeschüchtert werden. Da ihnen nicht mitgeteilt wird, in welcher Weise ihr Datenträger ausgewertet wird, müssen sie davon ausgehen, dass den Personen, die die Anhörung durchführen und die über den Asylantrag entscheiden, alle darauf gespeicherten Informationen bekannt sind oder dass der Datenträger zumindest zur Nachprüfung ihrer Angaben bei der Anhörung umfassend durchsucht werden könnte. Die Asylsuchenden wissen nicht, was das BAMF über sie weiß, wissen aber, dass es vieles, auch Höchstpersönliches über sie wissen kann. Dadurch kann bei ihnen ein diffuses Bedrohungsgefühl entstehen, vor dem die Grundrechte auf informationelle Selbstbestimmung und auf Vertraulichkeit und Integrität informationstechnischer Systeme gerade auch und allgemein schützen,

BVerfGE 113, 29 (46); 125, 260 (320).

Dieses weist, erstens, aufgrund der existenziellen Bedeutung des grundrechtlich geschützten Asylverfahrens eine nochmals besondere Intensität auf, trifft, zweitens, mit Asylsuchenden eine besonders vulnerable Bevölkerungsgruppe trifft, und, drittens, aufgrund der Anwendung in nur bestimmten Fallkonstellationen hinsichtlich einzelner Länder ein diskriminierendes Momentum hat.

Die hohe Eingriffsintensität der staatlichen Datenträgerauswertung wirkt sich dahingehend aus, dass sie nur zum Schutz hochrangiger Rechtsgüter erfolgen darf. Das Bundesverfassungsgericht hat im Urteil zum BKA-Gesetz ausgeführt, dass Eingriffe in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme unter strengen Bedingungen stehen. Daher müssten „die Maßnahmen davon abhängig sein, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen“,

BVerfGE 141, 220 (Rn. 212).

Für § 20k BKAG a.F. konnte das Bundesverfassungsgericht dieses Kriterium bejahen. Diese Norm ermöglichte verdeckte Eingriffe in informationstechnische Systeme nur, wenn bestimmte

Tatsachen die Annahme rechtfertigten, dass eine Gefahr für Leib, Leben oder Freiheit einer Person oder „solche Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt," besteht.

Dass Eingriffe in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme nur zum Schutz hochrangiger Rechtsgüter erfolgen dürfen, gilt nicht nur bei verdeckten Eingriffen. Wie oben dargelegt, sind die Unterschiede zwischen einem offenen Zugriff auf Datenträger infolge einer Anordnung zur Herausgabe und einem verdeckten Eingriff gering. Wenn sich staatliche Stellen Zugang zu großen Datenmengen auf einem informationstechnischen System verschaffen, die Rückschlüsse auf wesentliche Teile des Lebens einer Person zulassen, und damit dessen Vertraulichkeit aufheben, ist dies unabhängig von der Art des Zugriffs stets ein intensiver Eingriff in die grundrechtlich geschützte Privatsphäre, der nicht zu beliebigen Gemeinwohlzielen erfolgen darf.

Wird der offene Zugriff auf einen Datenträger am Recht auf informationelle Selbstbestimmung gemessen, ergibt sich nichts anderes. Vor der Etablierung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme hat das Bundesverfassungsgericht im Beschluss zur Beschlagnahme und Sichtung von Datenträgern aus Anwaltskanzleien am Maßstab des Rechts auf informationelle Selbstbestimmung strenge Verhältnismäßigkeitsanforderungen für derartige Maßnahmen aufgestellt. Der eingriffsintensive Zugriff auf Datenträger bedürfe im jeweiligen Einzelfall in besonderer Weise einer regulierenden Beschränkung. Im Strafverfahren dürfe der Eingriff aufgrund von §§ 98, 110 StPO nur erfolgen, wenn er in angemessenem Verhältnis zur Schwere der Straftat und zur Stärke des Tatverdachts stehe,

BVerfGE 113, 29 (53).

Aus der verfassungsgerichtlichen Rechtsprechung wird damit deutlich, dass die Auswertung von Datenträgern – unabhängig davon, an welcher Ausprägung des allgemeinen Persönlichkeitsrechts sie zu messen ist – angesichts ihrer hohen Eingriffsintensität nicht zu beliebigen Gemeinwohlzielen erfolgen darf. Politische Zielsetzungen jenseits des Schutzes hochrangiger Rechtsgüter vor bereits hinreichend konkret absehbaren Gefahren und der Aufklärung gewichtiger Straftaten vermögen den Eingriff nicht zu rechtfertigen.

Das mit §§ 15 Abs. 2 Nr. 6, 15a AsylG verfolgte Ziel der Zuwanderungsbegrenzung und der erleichterten Abschiebung von Personen, deren Asylantrag abgelehnt wurde, ist zwar als solches verfassungslegitim. Der gravierende Grundrechtseingriff der verdachtsunabhängigen Auswertung von Datenträgern lässt sich damit aber nicht rechtfertigen. Die migrationspolitische Zielsetzung ist weder mit der Verhinderung gewichtiger Straftaten (insbesondere

Terroranschlägen), für die hinreichend konkrete Anhaltspunkte bestehen, noch mit deren repressiver Aufklärung zu vergleichen. Das bloße Ziel, Menschen abzuschieben, die aufgrund einer restriktiven Zuwanderungspolitik auf dem Staatsgebiet nicht erwünscht sind, bei denen aber keine Anhaltspunkte bestehen, dass sie hochrangige Rechtsgüter durch Straftaten beeinträchtigen werden, rechtfertigt eine derart eingriffsintensive Maßnahme nicht. Das gilt umso mehr, als die Daten des Ergebnisreports zur Feststellung der Staatsangehörigkeit lediglich Indizien abgeben und keinen Beweis erbringen.

b) Hilfsweise: Verfassungswidrigkeit der konkreten Ausgestaltung

Sollte das Gericht offene Zugriffe auf Datenträger zu migrationspolitischen Zielen trotz der genannten Einwände nicht per se für unzulässig erachten, sind die §§ 15 Abs. 2 Nr. 6, 15a AsylG jedenfalls in ihrer konkreten Ausgestaltung verfassungswidrig. Die Regelungen enthalten weder Begrenzungen, aus welchem Anlass und wie weitgehend Datenträger von Asylsuchenden ausgewertet werden dürfen, noch verfahrensrechtliche Anforderungen zum Schutz der Grundrechte der Betroffenen. Solche Begrenzungen wären zur Wahrung der Verhältnismäßigkeit und Bestimmtheit der Eingriffsermächtigung jedoch geboten gewesen. Es ist angesichts der weiten Formulierung der Rechtsgrundlage und der möglichen massiven Grundrechtseingriffe nicht möglich, und wohl auch nicht Aufgabe der Gerichte, diese strengeren Vorgaben im Wege einer verfassungskonformen Auslegung zu etablieren.

(1) Unverhältnismäßigkeit jedenfalls der Auswertung der Datenträger aller Asylsuchenden ohne anerkannte Ausweispapiere zum Zeitpunkt der Registrierung

Die Verhältnismäßigkeit einer gesetzlichen Eingriffsermächtigung setzt voraus, dass der Zweck nicht ebenso gut durch mildere Mittel zu erreichen ist. Dies ist im Bereich der staatlichen Datenverarbeitung von besonderer Bedeutung (was sich auch an der ausdrücklichen Normierung in Art. 5 Abs. 1 lit. c DSGVO zeigt): Persönliche Daten dürfen nur dann erhoben und ausgewertet werden, wenn dies für den Zweck des Verwaltungsverfahrens zwingend notwendig ist.

Nach der „Dienstanweisung Asylverfahren Identitätsfeststellung“ des BAMF, Ziff. 3.1., werden Datenträger bereits bei der Registrierung von Asylsuchenden als Routinemaßnahme bei all denjenigen ausgelesen, die keinen Pass oder Passersatz vorweisen können, der vor Ort auf seine Gültigkeit überprüft werden kann. Gestützt wird dieses Vorgehen auf die Begründung des Regierungsentwurfs des § 15a AsylG, nach der die Auslesung regelmäßig bei der Registrierung als Asylsuchender erfolgen soll,

> BT-Drs. 18/11546, **Anlage 9**, S. 15.

Zu diesem Zeitpunkt, vor der Anhörung, haben die Asylsuchenden selbst noch nicht die Möglichkeit gehabt, sich zu äußern. In der Dienstanweisung des BAMF wird unter Verweis auf die Gesetzesbegründung ausgeführt, die Anhörung sei kein milderes Mittel. Ein nach § 15a AsylG vorrangig heranzuziehendes milderes Mittel zur Klärung von Identität und Staatsangehörigkeit sei lediglich gegeben, wenn Asylsuchende andere Dokumente vorlegten, die das BAMF auf ihre Echtheit überprüfen könne.

Diese Einschätzung trifft nicht zu. Die Befragung in der Asylanhörung durch gut qualifizierte Mitarbeiter*innen ist ein geeignetes, und auch neben den Datenträgerauswertungen nach wie vor das einzig belastbare Mittel zur Überprüfung der Herkunfts- und Identitätsangabe. In der Anhörung können gemachte Angaben anhand genauer Nachfragen sehr zuverlässig überprüft werden. Ein Klärungsbedürfnis hinsichtlich Identität und Staatsangehörigkeit, das eine Datenerhebung erforderlich machen könnte, entsteht erst, wenn die diesbezüglichen Angaben bei der Anhörung Anlass zu Zweifeln geben. Könnte eine Datenträgerauswertung nur in solchen Fällen stattfinden, wäre sowohl die Zahl als auch die Intensität der Grundrechtseingriffe wesentlich geringer. Auf diese Weise würden nicht sämtliche Asylsuchende unter Generalverdacht gestellt, bevor sie bei der Anhörung umfassende und wahrheitsgemäße Angaben machen können.

Das gilt besonders für die Asylsuchenden, die einen Pass oder Passersatz herausgeben, der von dem jeweiligen Staat amtlich ausgestellt wurde und noch gültig ist, aber vom BAMF wegen einer Allgemeinverfügung nach § 71 Abs. 6 AufenthG nicht anerkannt wird oder vor Ort nicht auf seine Echtheit geprüft werden kann. Auch Asylsuchenden, die keine Ausweispapiere vorlegen können, kann nicht pauschal unterstellt werden, dass sie diese selbst beseitigt hätten. Pässe und Passersatzpapiere können etwa auf der Flucht verloren gehen, in ihrer Gültigkeit ablaufen oder von Schleuser*innen einbehalten worden sein; in manchen Ländern ist der Besitz von Pässen schlicht nicht üblich. Somit ist eine Vielzahl Asylsuchender von der Maßnahme betroffen, ohne dass sie durch ihr Verhalten dazu Anlass gegeben haben. Das lässt den Eingriff ihnen gegenüber als besonders gravierend erscheinen,

vgl. BVerfGE 115, 320 (347); 120, 378 (402).

Dass die Auslesung der Datenträger aller Asylsuchenden, die über keine vom BAMF anerkannten Ausweispapiere verfügen, nicht erforderlich ist, ergibt sich schon daraus, dass der Ergebnisreport nicht in jedem Fall von dem*der Entscheider*in angefordert wird, sondern nur, wenn basierend auf den sonst verfügbaren Informationen Identität und Staatsangehörigkeit nicht als geklärt gelten. Insbesondere sind, wenn sich ein vorgelegtes Ausweisdokument bei einer Prüfung in den speziellen Prüfzentren als echt erweist, allein die daraus ersichtlichen Angaben der Entscheidung

über den Asylantrag zugrundezulegen. Die eigenständigen Grundrechtseingriffe der Auslesung von Datenträgern und der Speicherung des Ergebnisreports erfolgen also auf Vorrat; ausweislich der von der Bundesregierung genannten Zahlen (oben A III.) werden sie in über der Hälfte der Fälle letztlich auch nach Einschätzung der Entscheider*innen nicht benötigt. Eine Auslesung und Auswertung zu einem späteren Zeitpunkt, wenn Zweifel aufgekommen sind, würde für die Zwecke des Verfahrens genügen. In diesem Sinne hat auch die damalige Bundesdatenschutzbeauftragte die Erforderlichkeit der Regelung verneint,

BT-Drs. 18(4)831, **Anlage 13**, S. 5.

Hält man eine Herausgabepflicht erst nach der Anhörung, wenn sich dabei konkrete Zweifel an den Angaben zu Identität und Staatsangehörigkeit ergeben haben, nicht für gleich effektiv zur Zielerreichung, muss sich der Gesetzgeber zumindest auf der Stufe der Verhältnismäßigkeit im engeren Sinne auf sie verweisen lassen. Eine geringfügige Effektivitätseinbuße ist zugunsten der damit zu erreichenden Abmilderung des Grundrechtseingriffs hinzunehmen. Sollte das BAMF bezwecken, durch die Auswertung überhaupt erst einen Verdacht zu gewinnen („Verdachtsgewinnungseingriff"), könnte das migrationspolitische Ziel jedenfalls eine derart weite Absenkung der Eingriffsschwelle nicht rechtfertigen.

(2) Fehlende Eingrenzung der Art der zu erhebenden Daten als Verstoß gegen Bestimmtheit und Verhältnismäßigkeit

§ 15a AsylG begrenzt die Art der bei der Auswertung zu erhebenden Daten lediglich durch den Zweck, Identität und Staatsangehörigkeit zu klären. Dazu könnten auf dem Datenträger gespeicherte Daten sehr unterschiedlicher Art ausgewertet werden. § 15a AsylG schließt weder aus, dass neben Metadaten auch gespeicherte Kommunikationsinhalte ausgewertet werden dürfen, noch enthält er Regelungen zur Verarbeitung von automatisiert erhobenen besonders sensiblen persönlichen Daten.

(a) Kein Ausschluss der Speicherung von Kommunikationsinhalten

Nach der derzeitigen Praxis wird zunächst der gesamte Inhalt des Datenträgers vom BAMF kopiert. Die gespeicherten Textnachrichten werden aber nur bezüglich der Metadaten und verwendeten Sprachen automatisiert ausgewertet, während Bedienstete des BAMF keine Kenntnis von Kommunikationsinhalten erlangen. Diese Praxis ist in Verwaltungsvorschriften des BAMF geregelt. Demgegenüber schließt § 15a AsylG nicht aus, dass auch von Bediensteten des BAMF persönlich ausgewertete Kommunikationsinhalte gespeichert und für das Asylverfahren verwendet werden. Damit ermöglicht die Regelung Grundrechtseingriffe, die noch wesentlich weiter reichen als die derzeitige Praxis. Ausdrücklich unzulässig ist es lediglich nach § 15a AsylG i.V.m. § 48 Abs. 3a Satz 5 AufenthG, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung

zu verwerten. Dies verhindert aber nicht, dass Daten aus dem Kernbereich erhoben werden und die für die Auswertung zuständige Person davon Kenntnis erlangt. Denn das Erhebungsverbot des § 15a AsylG i.V.m. § 48 Abs. 3a Satz 1 AufenthG ist praktisch bedeutungslos, da von der Auswertung der Datenträger von Asylsuchenden nie „allein“, Erkenntnisse aus dem Kernbereich zu erwarten sind,

> vgl. **Anlage 14**: T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227, S. 123, 127; Funke-Kaiser, in: GK-AsylG, EL 115 März 2018, § 15a Rn. 12.

Vor allem gilt der Kernbereichsschutz nur für einen kleinen Kreis intimer Äußerungen, während Kommunikationsinhalte mit sozialem Bezug erfasst werden dürfen.

Dass § 15a AsylG die Reichweite der Datenverarbeitungsbefugnisse im Unklaren lässt, verstößt zunächst gegen die grundrechtlichen Anforderungen an die Normenbestimmtheit und Normenklarheit. Sie stellen sicher, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und ihre Reichweite selbst trifft, die Verwaltung steuernde und begrenzende Handlungsmaßstäbe vorfindet und die Gerichte eine wirksame Kontrolle durchführen können,

> BVerfGE 113, 348 (375 ff.); 120, 378 (407).

Zu einer Auswertung der auf den Datenträgern von Asylsuchenden gespeicherten Telekommunikationsinhalte dürfte freilich auch der Gesetzgeber – selbst für Fälle, in denen ein hinreichender Verdacht falscher Angaben zu Staatsangehörigkeit und Identität besteht – nicht ermächtigen: Jedenfalls dieser Eingriff kommt in seiner Intensität der Überwachung laufender Telekommunikation gleich, die nur zur Abwehr von Gefahren für hochrangige Rechtsgüter und zur Aufklärung gewichtiger Straftaten, nicht aber aus migrationspolitischen Gründen zulässig ist.

(b) Unzureichende Regelung zur Verarbeitung von mittels der Software erhobenen besonders sensiblen persönlichen Daten

Bereits nach der aktuellen Praxis des BAMF erweisen sich einige der Auswertungskriterien selbst dann als unverhältnismäßig, wenn die Auswertung von Datenträgern zu migrationspolitischen Zielen nicht schon grundsätzlich für unzulässig erachtet sollte. Die neben den Statistiken im Ergebnisreport erscheinenden Tabellen über verwendete Apps und zugehörige Account-Namen sowie über E-Mail-Adressen können Rückschlüsse auf besonders sensible persönliche Daten zulassen. So können installierte Dating-Apps Hinweise auf die sexuelle Orientierung ermöglichen; aus den Domains von E-Mail-Adressen ergeben sich unter Umständen Hinweise auf die politische

Meinung und eine Religions- oder Gewerkschaftszugehörigkeit. Die Speicherung derart sensibler Daten ist auch nach dem europäischen Datenschutzrecht nur ausnahmsweise zur Wahrung erheblicher öffentlicher Interessen zulässig (Art. 9 Abs. 2 lit. g DSGVO) und kann mit migrationspolitischen Zielen nicht gerechtfertigt werden.

Insofern hätte die Regelung zumindest eine Verpflichtung vorsehen müssen, sensible Einzeldaten aus dem Ergebnisreport zu entfernen.

(3) Keine effektiven verfahrensrechtlichen Sicherungen

Zur Wahrung der Verhältnismäßigkeit einer gesetzlichen Ermächtigung zur Datenverarbeitung bedarf es auch verfahrensrechtlicher Sicherungen, die die Transparenz der Datenverwendung, einen effektiven Rechtsschutz und effektive Sanktionen gewährleisten,

BVerfGE 65, 1 (46); 113, 29 (57 f.); 120, 351 (361).

(a) Fehlende Transparenz gegenüber den Betroffenen

Zwar gelten für die Datenverarbeitung durch das BAMF die allgemeinen Betroffenenrechte der DSGVO. So sind nach Art. 17 Abs. 1 lit. a DSGVO Daten unverzüglich zu löschen, wenn sie für die Zwecke der Erhebung oder Weiterverarbeitung nicht mehr benötigt werden. Ein Auskunftsanspruch der Betroffenen ergibt sich aus Art. 15 DSGVO. Allerdings dürften die Betroffenen diese Regelungen meist nicht kennen.

Umso wichtiger wären zur Wahrung der Verhältnismäßigkeit Regelungen, die das BAMF verpflichten, von sich aus gegenüber den Betroffenen transparent zu machen, Daten welcher Art und welchen Umfangs von ihnen erhoben werden. Da es sich gerade nicht um eine heimliche Maßnahme handelt, ist auch nicht ersichtlich, warum Transparenzanforderungen der Effektivität der Maßnahme entgegenstehen sollten. Würde den Betroffenen bekanntgegeben, welche Daten von ihnen erhoben werden, milderte dies die diffuse Bedrohlichkeit der Datenspeicherung ab,

vgl. BVerfGE 125, 260 (335).

(b) Fehlen institutioneller Sicherungen

Es fehlt zudem an institutionalisierten Mechanismen, die für eine unabhängige Kontrolle sorgen. Die Regelung des § 15a AsylG i.V.m. § 48 Abs. 3a Satz 4 AufenthG, wonach der Datenträger nur durch Bedienstete mit Befähigung zum Richteramt ausgewertet werden darf, ist keine geeignete Verfahrensgarantie. Erforderlich wäre ein Richtervorbehalt, der auf eine vorbeugende Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz abzielt. Das Grundgesetz geht davon aus, dass Richter*innen aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer

strikten Unterwerfung unter das Gesetz (Art. 97 GG) die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren können,

> vgl. BVerfG NJW 2018, 2619 Rn. 96; Wildhagen, Persönlichkeitsschutz durch präventive Kontrolle, 2011, S. 184 f.

Ungeachtet ihrer juristischen Qualifikation fehlt es bei Behördenmitarbeiter*innen, die aufgrund beamtenrechtlicher oder arbeitsvertraglicher Treuepflichten den Weisungen ihres Dienstherrn bzw. ihres Arbeitgebers unterstehen, an der für einen Richtervorbehalt typischen Unabhängigkeit und Unparteilichkeit,

> vgl. T. Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227, **Anlage 14**, S. 123, 128 f.

Im Übrigen ist der „Volljuristenvorbehalt“ nicht geeignet, die materiellen Bedenken gegen die Eingriffsermächtigung auszuräumen. Richtervorbehalte oder vergleichbare Regelungen sind nur dann grundrechtlich sinnvoll, wenn die Gerichte prüfen können, ob grundrechtsschützende materielle Eingriffsvoraussetzungen vorliegen. Dagegen sind sie nicht dazu geeignet, die Mängel einer zu niedrig angesetzten Eingriffsschwelle auszugleichen,

> BVerfGE 120, 274 (331).

Eine Verfahrensgarantie besteht in der Überwachung der Datenverarbeitung des BAMF durch den Bundesbeauftragen für Datenschutz und Informationsfreiheit als Aufsichtsbehörde im Sinne des Art. 51 DSGVO. Das BAMF untersteht wie alle Bundesbehörden gem. § 9 Abs. 1 BDSG seiner Kontrolle. Effektiver Grundrechtsschutz würde aber voraussetzen, dass § 15a AsylG das BAMF zu einer umfassenden Dokumentation verpflichtet, die der Bundesdatenschutzbeauftragte zum Gegenstand seiner Überprüfung machen kann,

> vgl. BVerfG NJW 2019, 827 Rn. 156 ff.

Das Fehlen einer solchen Regelung in § 15a AsylG hat bereits vor Inkrafttreten die damalige Bundesdatenschutzbeauftragte als verfassungsrechtliches Defizit bemängelt,

> BT-Drs. 18 (4) 831, **Anlage 13**, S. 8.

C. Löschungsantrag

I. Zulässigkeit

Der Anspruch auf Löschung rechtswidrig gespeicherter persönlicher Daten ist nach überwiegender Auffassung mit Blick auf die dem tatsächlichen Vorgang der Löschung vorgelagerte Entscheidung, dass Daten nicht gespeichert werden sollen, im Wege der Verpflichtungsklage geltend zu machen.

Die Klagebefugnis ergibt sich aus dem vom Kläger geltend gemachten Löschungsanspruch gem. Art. 17 DSGVO.

Eines Vorverfahrens gem. § 68 Abs. 2 VwGO in Form eines Antrags beim BAMF bedurfte es hier nicht. Zum einen gilt für den auf Art. 17 DSGVO gestützten Löschungsanspruch die Garantie gerichtlichen Rechtsschutzes in Art. 79 DSGVO, die „unbeschadet anderer verwaltungsrechtlicher und außergerichtlicher Rechtsbehelfe“ besteht. Damit ist das Erfordernis eines Vorverfahrens unvereinbar. § 68 VwGO ist wegen des Unionsrechtsverstoßes hier unanwendbar,

> Bergt in Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 79 Rn. 12, 20.

Zudem ist das Vorverfahren im Bereich des Asylrechts gem. § 11 AsylG ausgeschlossen. Rechtsgrundlage des Löschungsanspruchs ist hier zwar nicht das AsylG, sondern die DSGVO. Für die Anwendbarkeit des § 11 AsylG genügt es jedoch, wenn der angefochtene oder begehrte Verwaltungsakt in einem inneren Zusammenhang zum Asylverfahren steht,

> Preisner in Kluth/Heusch, BeckOK-Ausländerrecht, 23. Ed. 01.08.2019, § 11 Rn. 8.

Schließlich ist ein Vorverfahren entbehrlich, weil es nicht zielführend wäre. Der Kläger macht die Rechtswidrigkeit der Datenverarbeitung durch das BAMF allein unter dem Aspekt geltend, dass die Rechtsgrundlage, § 15a AsylG, verfassungswidrig ist. Einem so begründeten Löschungsantrag könnte das BAMF nicht entsprechen. Denn die Behörden haben die geltenden Gesetze ungeachtet ihrer Verfassungsmäßigkeit anzuwenden; ein Normverwerfungsrecht kommt ihnen nicht zu,

> BGH NVwZ 2015, 1309 Rn. 15; BFHE 225, 299 (301); Huster/Rux in BeckOK-GG, 41. Ed. 15.02.2019, Art. 20 Rn. 168; Sommermann in MKS, 6. Aufl. 2018, Art. 20 Rn. 257; *Gärditz,* in: Friauf/Höfling, Art. 20 (6. Teil) (2011) Rn. 108 ff.

II. Begründetheit

Gem. Art. 17 Abs. 1 lit. d DSGVO besteht ein Löschungsanspruch, wenn personenbezogene Daten zu Unrecht verarbeitet wurden. Die Rechtswidrigkeit kann sich dabei nicht nur aus einem Verstoß gegen das materielle Datenschutzrecht der DSGVO ergeben, sondern auch aus einem Verstoß gegen nationales Datenschutzrecht im Bereich der Öffnungsklauseln,

> Worms in Wolff/Brink, BeckOK-Datenschutzrecht, 29. Ed. 01.08.2019, Art. 17 DSGVO Rn. 43.

Mitgliedsstaatliche Ermächtigungen zur Datenerhebung im öffentlichen Interesse, die Art. 6 Abs. 3 Satz 1 lit. b DSGVO zulässt, müssen dem nationalen Verfassungsrecht genügen. Die Verfassungswidrigkeit des § 15a AsylG führt daher zu einem Löschungsanspruch der auf dessen Grundlage erhobenen Daten gem. Art. 17 Abs. 1 lit. d DSGVO.

D. Ergebnis: Vorlage an das Bundesverfassungsgericht

Die §§ 15 Abs. 2 Nr. 6 und 15a AsylG sind verfassungswidrig. Stellt das Bundesverfassungsgericht dies fest, ist den geltend gemachten Anträgen in vollem Umfang stattzugeben. Es wird daher angeregt, dass das Verwaltungsgericht das Verfahren aussetzt und die Regelungen dem Bundesverfassungsgericht nach Art. 100 Abs. 1 GG vorlegt.

Hochachtungsvoll

Dr. Lehnert, Rechtsanwalt

E. Anlagenverzeichnis

Anlage 1	L. Beckmann, A. Biselli (2019), Das Smartphone, bitte - Digitalisierung von Migrationskontrolle in Deutschland und Europa, Herausgeberin Gesellschaft für Freiheitsrechte e.V., (abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von-Migrationskontrolle.pdf)
Anlage 2	Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Identitätsfeststellung
Anlage 3	Bundesamt für Migration und Flüchtlinge, Dienstweisung für das AVS, Auslesen von mobilen Datenträgern, Verfahrensweise bei persönlicher Erstantragstellung
Anlage 4	Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Urkundenprüfung, Stand 06/18
Anlage 5	Bundesministerium für Migration und Flüchtlinge, Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte, Einführung in die neuen IT-Tools, Schulung AVS-Mitarbeiter, Entscheider und Volljuristen, 30.08.2017
Anlage 6	Deutscher Bundestag, Drucksache 19/8701, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/7338 – Ergänzende Informationen zur Asylstatistik für das Jahr 2018, 25.03.2019 (abrufbar unter: http://dipbt.bundestag.de/doc/btd/19/008/1900870.pdf)
Anlage 7	Deutscher Bundestag, Drucksache 19/11001, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/9911 – Ergänzende Informationen zur Asylstatistik für das erste Quartal 2019, 19.06.2019 (abrufbar unter: http://dip21.bundestag.de/dip21/btd/19/110/1911001.pdf)
Anlage 8	Deutscher Bundestag, Drucksache 19/13945, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/12797 – Ergänzende Informationen zur Asylstatistik für das zweite Quartal 2019, 11.10.2019

(abrufbar unter:
http://dip21.bundestag.de/dip21/btd/19/139/1913945.pdf)

Anlage 9 Deutscher Bundestag,
Drucksache 18/11546, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 16.03.2017
(abrufbar unter:
https://dip21.bundestag.de/dip21/btd/18/115/1811546.pdf)

Anlage 10 H. Elfardy, M Diab (2013),
Sentence Level Dialect Identification in Arabic, Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, Sofia, Bulgaria, August 2013
(abrufbar unter: https://www.aclweb.org/anthology/P13-2081.pdf)

Anlage 11 Deutscher Bundestag,
Drucksache 19/6647, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/5691 – Einsatz von IT-Assistenzsystemen im Bundesamt für Migration und Flüchtlinge, 19.12.2018
(abrufbar unter:
http://dip21.bundestag.de/dip21/btd/19/066/1906647.pdf)

Anlage 12 T. W. Boonstra, M. E. Larsen, H. Christensen (2015),
Mapping dynamic social networks in real life using participants' own smartphones, Heliyon 1(3), e00037
(abrufbar unter:
https://www.sciencedirect.com/science/article/pii/S2405844015300566)

Anlage 13 Deutscher Bundestag, Innenausschuss,
Ausschussdrucksache 18(4)831,
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23.03.2017
(abrufbar unter: https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf)

Anlage 14 T. Tabbara (2019),
Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227, S. 123