**Kanzlei**
**Für Aufenthaltsrecht**

Jentsch Rechtsanwälte

Kanzlei für Aufenthaltsrecht, Jentsch Rechtsanwälte, Gohliser Str. 20, 04105 Leipzig

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

**Bitte beachten Sie die neuen Bürozeiten:**
Mo, Di und Do: 10:00 - 12:00 Uhr
Mo und Do: 15:00 - 17:00 Uhr
Mi und Fr geschlossen

**Zweigstelle Leipzig:**
Gohliser Str. 20
04105 Leipzig
Telefon: (0341) 978 543 12

Verwaltungsgericht Stuttgart
Augustenstraße 5
70178 Stuttgart

**per beA**

20.12.2024 (...)

Unser Zeichen:
**(...)**

**K l a g e**

**u n d**

**A n t r a g a u f W i e d e r h e r s t e l l u n g u n d A n o r d n u n g d e r a u f s c h i e b e n d e n W i r k u n g**

des … –

Kläger und Antragsteller,

- Prozess- und Verfahrensbevollmächtigte: Jentsch Rechtsanwälte, Eichendorffstraße 13, 10115 Berlin -

gegen

das Land Baden-Württemberg, vertreten durch das Regierungspräsidium Karlsruhe, Durchlacher Allee 100, 76137 Karlsruhe –

Beklagter und Antragsgegner,

wegen: Einzug von Datenträger und Zurverfügungstellung der Zugangsdaten zwecks Auslesung und Auswertung, § 48 Abs. 3, 3a, 3b, § 48a AufenthG.

Namens und in Vollmacht des Klägers, Vollmacht anbei (**Anlage 1**), erheben wir Klage, und beantragen,

**1.**
**den Bescheid des Beklagten vom … (Az. …) hinsichtlich der Ziffern 1, 2, 4 und 5 aufzuheben.**

**2.**
**dem Kläger Prozesskostenhilfe unter Beiordnung des unterzeichnenden Rechtsanwalts zu bewilligen.**

Ebenfalls begehren wir einstweiligen Rechtsschutz und beantragen namens und in Vollmacht des Antragstellers,

**1.**

**die aufschiebende Wirkung der Klage gegen die Ziff. 1 und 2. des Bescheides des Antragsgegners vom … (Az. …) wiederherzustellen,**

**2.**

**den Antragsgegner zu verpflichten, dem Antragsteller sein Mobiltelefon, seine SIM-Karte und seine externe Speicherkarte herauszugeben,**

**3.**

**die aufschiebende Wirkung der Klage gegen die Ziff. 5. des Bescheids vom … anzuordnen.**

**4.**

**dem Antragsgegner aufzugeben, bis zur Entscheidung im einstweiligen Rechtsschutzverfahren von der Auslesung und Auswertung des vom Kläger überlassenen Mobiltelefons mitsamt Sim-Karte und externer Speicherkarte abzusehen.**

**5.**

**dem Antragsteller Prozesskostenhilfe unter Beiordnung des unterzeichnenden Rechtsanwalts zu bewilligen.**

Es wird zugleich angeregt,

**das Verfahren in der Hauptsache gem. Art. 100 Abs. 1 GG i.Vm. § 80 Abs. 1 BVerfGG auszusetzen und dem Bundesverfassungsgericht mit der Frage vorzulegen, ob § 48 Abs. 3, 3a, 3b und § 48a AufenthG 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 des Beklagten und bitten um Übersendung.

**Zusammenfassung**

Vor der ausführlichen Begründung fassen wir die maßgeblichen Punkte des Rechtsstreits wie folgt zusammen:

Der angegriffene Bescheid weist zahlreiche formelle und materielle Mängel auf. Vor allem sind die Rechtsnormen, auf die er sich stützt, verfassungswidrig: Die Verfassungsmäßigkeit der Befugnis nach § 48 Abs. 3, 3a, 3b AufenthG scheitert bereits an einer abstrakten Abwägung des staatlichen Interesses an der Förderung einer Abschiebung mit dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, weil die Auslesung und Auswertung u.a. von Smartphones und allen darauf befindlichen Inhalten extrem tiefe Einblicke in die Persönlichkeit bietet, was deutlich außer Verhältnis zum erhofften Ziel steht. Aber auch die konkrete Ausgestaltung der Norm genügt nicht verfassungsrechtlichen Anforderungen, weil die Befugnis zum Auslesen von Datenträgern weder auf verhältnismäßige Fälle begrenzt ist noch Anlass und Reichweite hinreichend begrenzt, weil sie den Kernbereich privater Lebensgestaltung nicht hinreichend schützt und weil sie verfahrensrechtliche Anforderungen zum Schutz der Grundrechte der Betroffenen nicht einhält. § 48 Abs. 3, 3a, 3b AufenthG verletzt zudem die Maßgaben des Unionsrechts.

**Gliederung**

## A. Sachverhalt

Der Kläger wendet sich gegen den Einzug und die Einbehaltung seines Mobiltelefons inkl. SIM-Karte und externer Speicherkarte durch das Regierungspräsidium Karlsruhe und die entsprechende Überlassungsanordnung, welche sich auch auf weitere Datenträger bezieht, sowie gegen die Anordnung, die Zugangsdaten des Mobiltelefons und weiterer Datenträger zur Verfügung zu stellen, und die Androhung des Zwangsmittels. Mittelbar rügt er die Verfassungswidrigkeit der Rechtsgrundlagen des § 48 Abs. 3, 3a, 3b AufenthG.

Der Kläger reiste im … in das Bundesgebiet ein und stellte anschließend einen Asylantrag in …. Dabei gab er an, gambischer Staatsangehöriger zu sein. Er durchlief das Asylverfahren erfolglos. Seine Klage gegen den ablehnenden Bescheid des BAMF bezüglich seines Asylantrags wurde mit Urteil des Verwaltungsgerichts … vom … abgewiesen. Das Urteil ist seit dem … rechtskräftig (vgl. **Anlage 2**). Seitdem ist sein Aufenthalt im Bundesgebiet geduldet. Aktuell ist der Kläger er im Besitz einer Duldung nach § 60b AufenthG. In dieser ist als Staatsangehörigkeit „gambisch“ angegeben. Er hat keinen Reisepass oder sonstige Identitätsdokumente aus Gambia.

Am … fand er sich um … aufgrund der Verfügung vom … (**Anlage 3**) zu einer persönlichen Vorsprache zwecks Identitätsklärung unter Zuhilfenahme einer Delegation aus Gambia in den Räumen des Regierungspräsidiums Karlsruhe, …, ein. Als er ankam, wurde er von den anwesenden Polizist*innen durchsucht und ihm wurden sein Mobiltelefon (…), sein Portmonnaie und weitere Sachen, die er bei sich trug, mit der Begründung abgenommen, dass er diese Sachen nicht mit in den Befragungsraum nehmen dürfe. Die Gegenstände wurden in einen Karton gelegt. Anschließend begab er sich in einen anderen Raum, in dem er von zwei vermummten Personen, einem Mann und eine Frau, gefragt wurde, ob er aus Gambia komme. Der Kläger beschränkte seine Angaben auf den Hinweis, dass er bereits … bei seiner Ankunft in Deutschland während einer Befragung in … seine Nationalität bekannt gegeben habe und sie dies in den damaligen Aufzeichnungen nachschauen könnten. Danach sollte der Kläger den Raum verlassen. Einer der anwesenden Polizist*innen wollte ihm seine Sachen zurückgeben. Ein anderer Polizist hielt ihn jedoch davon ab und gab dem Kläger auf, zu warten. Kurze Zeit später kam eine Mitarbeiterin des Regierungspräsidiums Karlsruhe zu ihnen, wobei sie das Mobiltelefon des Klägers bei sich hatte. Sie steckte es in eine Tüte und ließ ihn wissen, dass sie sein Mobiltelefon an sich genommen habe, da er bei der Befragung keine Antwort gegeben habe. Sie überreichte ihm den Bescheid vom …, Az. … (**Anlage 4**), und forderte ihn auf, die Empfangsbekenntnis auf der letzten Seite zu unterschreiben.

Der Kläger weigerte sich, zu unterschreiben. Die Mitarbeiterin des Regierungspräsidiums entfernte sich daraufhin kurz. Als sie wiederkam, forderte sie den Kläger auf, ihr den

Handycode zu nennen. Seine Nachfrage, weshalb sie sein Mobiltelefon einbehalten würde und aus welchem Grund sie seinen Handycode benötige, beantwortete sie nicht und stellte nur klar, dass er dazu verpflichtet sei. Ansonsten würden sie sein Handy für eine längere Zeit einbehalten. Als der Kläger sich weiterhin weigerte, den Code zu nennen, wurden seinMobiltelefon, in dem sich eine SIM-Karte und eine Speicherkarte befanden, einbehalten.

## B. Rechtliche Würdigung

### I. Klage

#### 1. Zulässigkeit bzgl. Ziffern 1, 2, 4 und 5 des Bescheids

Die Klage ist bezüglich der Ziffern 1, 2, 4 und 5 des Bescheides als Anfechtungsklage zulässig.

#### a) Statthafte Klageart

#### (1) Ziffer 1 des Bescheids

Der Antrag ist hinsichtlich Ziffer 1 des Bescheids als Anfechtungsklage statthaft, da der Kläger die Aufhebung der Anordnung des Regierungspäsidiums Karlsruhe begehrt, die im Tenor beschriebenen Datenträger unverzüglich vorzulegen, auszuhändigen und zur Auslesung und Auswertung zu überlassen. Diese behördliche Aktualisierung der kraft Gesetzes nach § 48 Abs. 3 S. 1 AufenthG bestehenden Pflicht ist ein den Kläger belastender Verwaltungsakt.

Dieser hat sich nicht erledigt. Eine vollständige Erledigung der Anordnung in Ziffer 1 kommt von vornherein deshalb nicht in Betracht, weil diese sich nicht nur auf das bereits überlassene Mobiltelefon des Klägers bezieht, sondern auf alle in seinem Besitz befindlichen Datenträger mitsamt Zubehör, die für die Feststellung der Identität und Staatsangehörigkeit des Klägers von Bedeutung sein können. Lediglich exemplarisch werden im Tenor Mobiltelefone, SIM-Karten, Tablets, Festplatten, Kameras, USB-Sticks, SD-Karten, CD-ROMS genannt.

Auch insoweit, als sich die Anordnung auf das bereits überlassene Mobiltelefeon des Klägers inklusive der SIM-Karte und Speicherkarte bezieht, hat sich der Verwaltungsakt nicht erledigt, da das Regierungspräsidium weiterhin im Besitz der betroffenen Datenträger ist und die weitere Einbehaltung auf die angegriffene Verfügung stützt, bis es die Daten ausgelesen hat.

**(2) Ziffer 2 des Bescheids**

Der Antrag ist hinsichtlich Ziffer 2 des Bescheids als Anfechtungsklage statthaft, da der Kläger die Aufhebung der Anordnung des Regierungspäsidiums Karlsruhe begehrt, ihm die Zugangsdaten und den Sperrcode für eine Auslesung der unter Ziffer 1 des Bescheids genannten Datenträger zwecks Auslesung der Daten zur Verfügung zu stellen.

**(3) Ziffer 4 des Bescheids**

Der Antrag ist hinsichtlich Ziffer 4 des Bescheids als Anfechtungsklage statthaft, da der Kläger die Aufhebung der Androhung der Wegnahme der unter Ziffer 1 genannten Datenträger mit unnmittelbaren Zwang begehrt. Die Androhung von Zwangsmitteln stellt einen eigenständigen, den Kläger belastenden Verwaltungsakt dar. Dieser hat sich nicht durch das Einbehalten des Mobiltelefons des Klägers erledigt, da sich die Androhung auf alle unter Ziffer 1 genannten Datenträger bezieht.

**(4) Ziffer 5 des Bescheids**

Der Antrag ist auch hinsichtlich Ziffer 5 des Bescheids als Anfechtungsklage statthaft, da der Kläger die Aufhebung der Androhung der Entsperrung des Geräts in Ersatzvornahme als einen ihn belastenden Verwaltungsakt begehrt.

**b) Sachentscheidungsvoraussetzungen**

Der Kläger ist als Adressat des Bescheids klagebefugt gemäß § 42 Abs. 2 VwGO, da jeweils jedenfalls eine Verletzung der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG möglich erscheint.

Darüber hinaus erscheint hinsichtlich der Anordnung nach Ziffer 1, 4 und 5 des Bescheides eine Verletzung des Grundrechts des Klägers aus Art. 14 Abs. 1 S. 1 GG zumindest als möglich, da ihm durch die Anordnung der Überlassung der Datenträger, insbesondere des überlassenen Mobiltelefons, die Nutzung seines Eigentums für die Dauer der Überlassung vollständig unmöglich gemacht wird.

Hinsichtlich der Ziffern 1, 2 und 3 des Bescheides liegt zudem eine Verletzung des Klägers in seinem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, hilfsweise in seinem Grundrecht auf informationelle Selbstbestimmung, vor.

Eines Widerspruchsverfahrens bedarf es gem. § 15 Abs. 1 S. 1 Fall 1 Ausführungsgesetz VwGO Baden-Württemberg nicht.

**2. Begründetheit hinsichtlich Ziffern 1 und 2 des Bescheids**

Die Anfechtungsklage ist begründet. Das Regierungspräsidium Karlsruhe war zu den angegriffenen Maßnahmen nicht berechtigt und der Kläger ist dadurch in seinen Rechten verletzt.

**a) Auswahl der Ermächtigungsgrundlage**

Es ist schon zweifelhaft, ob sich das Regierungspräsidium Karlsruhe mit seinen Anordnungen in Ziffer 1 und 2 des Bescheids vom … auf die richtige Ermächtigungsgrundlage gestützt hat. Es ist sehr umstritten, ob Anordnungen der Herausgabe von Datenträgern und ihren Zugangsdaten zwecks Datenauslesung und -auswertung gegen abgelehnte Asylbewerber*innen auf § 48 Abs. 3, 3a, 3b AufenthG gestützt werden können oder die § 15 Abs. 2 Nr. 6, §15a AsylG lex specialis sind,

> dafür: OVG Greifswald BeckRS 2013, 49502; OVG Koblenz BeckRS 2007, 20838; VG Freiburg BeckRS 2020, 25752 Rn. 4 ff.; dagegen OVG Magdeburg BeckRS 2011, 50644; OVG Weimar Beschl. V. 17.2.2005 – 3 EO 1424/04; VG Stade BeckRS 2021, 22221 Rn. 26 ff.; offenlassend VGH München BeckRS 2021, 15855 Rn. 5; VGH Mannheim BeckRS 2022, 36497 Rn. 9 ff.

Dem VG Karlsruhe sowie dem VGH Mannheim zufolge wirft die Frage, welche Ermächtigungsgrundlage heranzuziehen ist, wenn die Ausländerbehörde gegenüber abgelehnte Asylbewerber*innen die Herausgabe von Datenträgern und Zugangsdaten anordnen will, schwierige und bislang ungeklärte Auslegungsfragen auf,

> VGH Mannheim, Beschluss vom 23.11.2022 – 12 S 3213/21, BeckRS 2022, 36497, Rn. 15; VG Karlsruhe, Beschluss vom 09.08.2023 – A 19 K 1797/23, BeckRS 2023, 20923, Rn. 24.

Hinsichtlich der Argumente gegen eine Anwendbarkeit des § 48 Abs. 3, 3a, 3b AufenthG auf abgelehnte Asylbewerber*innen wird auf die genannten Beschlüsse Bezug genommen.

Diesen kann nicht entgegengehalten werden, dass die Rechtsfrage bereits durch den Gesetzgeber geklärt worden sei. Zwar enthält der Entwurf des

Rückkehrverbesserungsgesetzes, mit welchem § 48 Abs. 3, 3a, 3b AufenthG zuletzt geändert wurde, Ausführungen dazu, dass nach bestandskräftigem Abschluss des Asylverfahrens § 48 Abs. 3, 3a, 3b AufenthG richtige Ermächtigungsgrundlage für die in Rede stehenden Maßnahmen sei,

vgl. BT-Drs. 20/9463, S. 38.

Indes handelt es sich dabei nicht um eine Klärung durch gesetzliche Regelung, sondern lediglich um eine nachträgliche Interpretation des vorangegangenen gesetzgeberischen Willens durch die Bundesregierung.

Ein Wahlrecht der Ausländerbehörden, welche Ermächtigungsgrundlage sie für die Anordnung der Herausgabe von Datenträgern und Zugangsdaten im Falle von abgelehnten Asylbewerbern heranziehen, besteht jedenfalls nicht,

vgl. VGH Mannheim, Beschluss vom 23.11.2022 – 12 S 3213/21, BeckRS 2022, 36497, Rn. 13 f.

**b) Formelle Rechtswidrigkeit**

Die Anordnung in Ziffer 2 des Bescheids vom … ist formell rechtswidrig, da zweifelhaft ist, ob die zuständige Behörde gehandelt hat, und weil es keine Anhörung gab.

Die Anordnung in Ziffer 5 ist formell rechtswidrig, da die Formerfordernisse des § 20 Abs. 1 S. 2 VwVG BW nicht eingehalten sind.

**(1) Zuständigkeit**

Es ist zweifelhaft, ob das Regierungspräsidium Karlsruhe für die Anordnung nach Ziff. 2 des Bescheids vom …, ihm die Zugangsdaten und Sperrcodes für die Datenträger zur Verfügung zu stellen, zuständig ist. Sollte § 15a Abs. 1 S. 2 AsylG die richtige Ermächtigungsgrundlage sein, ist allein das Bundesamt für Migration und Flüchtlinge (BAMF) für eine solche Anordnung zuständig, vgl. § 15a Abs. 4 AsylG. Eine Erweiterung dieser Befugnisse auf Ausländerbehörden wie das Regierungspräsidium Karlsruhe wirft die Frage auf, ob sie mit dem verfassungsrechtlichen Gebot der hinreichenden Bestimmtheit und Begrenzung einer Norm vereinbar wäre,

vgl. VGH Mannheim, Beschluss vom 23.11.2022 – 12 S 3213/21, BeckRS 2022, 36497, Rn. 20.

**(2) Verfahren**

Die Anordnung in Ziffer 2 des Bescheids vom … ist formell rechtswidrig, da keine Anhörung nach § 28 Abs. 1 VwVfG erfolgt ist. Als die Mitarbeiterin des Regierungspräsidiums Karlsruhe zu dem Kläger kam, hatte sie sein Mobiltelefon schon in der Hand und ihm lediglich mitgeteilt, dass sie sein Handy einbehalten würde, da er bei der Befragung keine Antworten gegeben habe. Anschließend hat sie ihn dazu aufgefordert ihr seinen Handycode zur Verfügung zu stellen. Auf seine Nachfrage, wozu sie den Code brauche, hat sie nicht geantwortet und lediglich erwidert, dass er dazu verpflichtet sei, ihr den Code zu offenbaren. Damit hatte er keine ausreichende Gelegenheit, sich zu äußern.

Auch war die Anhörung nicht nach § 28 Abs. 2 VwVfG entbehrlich. Insbesondere lag keine Gefahr im Verzug vor, die eine sofortige Entcheidung notwendig erscheinen ließe. Es gibt keine Anhaltspunkte dafür, dass der Erhalt des Handycodes so dringlich war, dass es nicht erst nach einer Anhörung geschehen könnte. Das Regierungspräsidium hatte zum Zeitpunkt der möglichen Anhörung das Handy bereits in Besitz genommen.

Die Begründung der Entbehrlichkeit der Anhörung im Bescheid bezieht sich lediglich auf Ziffer 1. Die Begründung ist inhaltlich aber nicht nachvollziehbar. Unter Berücksichtigung des Umstands, dass das Regierungspräsidium zur Zeit des Erlasses des Bescheides bereits im Besitz des Mobiltelefones war und der Kläger sich zudem unter Polizeibewachung in ihren Räumlichkeiten aufhielt, ist eine Gefahr der Vernichtung des Datenträgers nicht erkennbar. Hinsichtlich der übrigen von Ziffer 1 des Bescheides erfassten Datenträger ist ebenfalls nicht erkennbar, wie eine Anhörung die Gefahr der Vernichtung im Vergleich zur Situation nach Bescheiderlass und vor Vollziehung hätte erhöhen sollen.

**c) Materielle Rechtswidrigkeit**

Der Bescheid vom … ist bezüglich der Ziff. 1 und 2 auch materiell rechtswidrig.

**(1) Unbestimmtheit des Bescheides in Ziff. 1 und 2**

Der Bescheid entspricht hinsichtlich der Ziffern 1 und 2 nicht den Anforderungen des § 37 Abs. 1 LVwVfG BW, da er inhaltlich nicht hinreichend bestimmt ist.

Das Bestimmtheitsgebot verlangt zum einen, dass der Adressat in die Lage versetzt werden muss, zu erkennen, was von ihm gefordert wird. Zum anderen muss der Verwaltungsakt geeignete Grundlage für Maßnahmen zu seiner zwangsweisen Durchsetzung sein können,

BVerwG, Urteil vom 15. Februar 1990 – 4 C 41/87 –, BVerwGE 84, 335-353, Rn. 29.

Erforderlich ist, dass die Behörde zumindest die allgemeine Art der vorzulegenden Urkunden, Unterlagen und Datenträger bezeichnet, die der Ausländer vorzulegen hat, z.B. Mobiltelefone, PC etc.,

vgl. Hailbronner, § 48 AufenthG, Rn. 72.

Diesen Anforderungen wird der Bescheid in Ziffer 1 und 2 nicht gerecht, da eine Konkretisierung eines bestimmten Datenträgers, auf welchen sich die Handlungspflichten in Ziffer 1 und 2 des Bescheids beziehen, fehlt. Der Tenor enthält zur Beschreibung der erfassten Datenträger lediglich eine Wiedergabe des Gesetzeswortlauts in § 48 Abs. 3 S. 1 AufenthG. Darüber hinaus werden Beispiele genannt, die erkennbar nicht abschließend sind („insbesondere…etc.“).

Für den Kläger ist damit nicht erkennbar, was genau von ihm gefordert wird. So soll zwar das bereits eingezogene Mobiltelefon – das der Beklagte bereits in seinem Besitz hatte und deshalb ohne Weiteres hätte spezifizieren können – erkennbar von Ziffer 1 des Bescheides erfasst sein, jedoch erstreckt sich der Tenor potentiell auf eine unbestimmte Vielzahl weiterer Datenträger. Dem Kläger wird das Risiko der Beurteilung auferlegt, welche in seinem Besitz befindlichen Datenträger für die Feststellung seiner Identität und Staatsangehörigkeit von Bedeutung sein können. Mangels Benennung der erfassten Gegenstände wird die notwendige Subsumtion damit unzulässigerweise auf die Ebene der Vollziehung verlagert, für die der Verwaltungsakt keine geeignete Grundlage darstellt. Dies gilt insbesondere vor dem Hintergrund, dass es sich bei der Überlassung von Datenträgern zur Aushändigung und Auswertung um einen intensiven Grundrechtseingriff handelt, der zu erhöhten Bestimmtheitsanforderungen führt.

**(2) Unverhältnismäßigkeit des Bescheides in Ziffer 1 und 2**

Aus der fehlenden Bestimmtheit des Bescheides folgt zudem ein Ermessensfehler in Form einer Ermessensüberschreitung. Wie die Formulierung „auf Verlangen“ in § 48 Abs. 3 S. 1 AufenthG zeigt, handelt es sich dabei um eine Ermächtigungsgrundlage, die der zuständigen

Behörde Ermessen einräumt. Es obliegt der Behörde, unter Wahrung des Verhältnismäßigkeitsgrundsatzes die zu überlassenden Datenträger so auszuwählen, dass die Zwecke des § 48 Abs. 3 S. 1 AufenthG auf möglichst grundrechtsschonende Weise erreicht werden. Dies verlangt zwingend die Auswahl eines bestimmten Datenträgers, der vorzulegen, auszuhändigen oder zu überlassen ist.

Da das Regierungspräsidium eine solche Auswahl (etwa auf das Mobiltelefon des Klägers) nicht getroffen hat, sondern die Anordnung auf alle Datenträger erstreckt hat, die für die Feststellung der Identität und Staatsangehörigkeit des Klägers von Bedeutung sein können, liegt eine Ermessensüberschreitung vor, da die Maßnahme nicht erforderlich bzw. jedenfalls nicht angemessen ist.

**(3) Verfassungswidrigkeit der Ermächtigungsgrundlagen in § 48 Abs. 3, 3a, 3b AufenthG**

Darüber hinaus ist der Bescheid bezüglich Ziffer 1 und 2 materiell rechtswidrig, weil die Regelungen in § 48 Abs. 3, 3a, 3b AufenthG verfassungswidrig sind. 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 sowie in seinem Eigentumsgrundrecht aus Art. 14 Abs. 1 GG.

Die Herausgabeanordnung gem. § 48 Abs. 3 S. 1 AufenthG ist rechtswidrig, da es an einer Rechtsgrundlage für die Auswertung der Datenträger mangelt; es besteht dann an der Überlassung der Datenträger kein rechtliches Interesse, mangels Auswertungsmöglichkeit können sie nicht für die in der Vorschrift genannten Feststellungen von Bedeutung sein,

> vgl. VG Karlsruhe, Beschluss vom 09.08.2023 – A 19 K 1797/23, BeckRS 2023, 20923, Rn. 25.

Auch eine Anordnung nach § 48 Abs. 3a S. 2 AufenthG sowie die Androhung von Zwangsmitteln zur Durchsetzung sind rechtswidrig, da die davon betroffene Person nicht zur Offenbarung seiner Zugangsdaten verpflichtet ist, wenn die damit bezweckte Auswertung von Datenträgern unzulässig ist. Dies ergibt sich dem Bundesverwaltungsgericht zufolge bereits aus dem klaren Wortlaut der Norm. Schon bei der darauf gerichteten Anordnung müssen die Voraussetzungen für eine rechtmäßige Auswertung vorliegen,

> vgl. BVerwG, Urteil vom 16.2.2023 – 1 C 19.21 (VG Berlin), ZD 2023, 707, Rn. 23, 27.

Der Prüfung des § 48 Abs. 3, 3a, 3b AufenthG am Maßstab des Grundgesetzes steht der Anwendungsvorrang des Unionsrechts nicht entgegen. Da die Maßnahmen erst nach Abschluss des Asylverfahrens ergriffen werden, fallen sie nicht unter Richtlinie 2013/32/EU (Asylverfahrensrichtlinie). Zwar fallen sie mit Blick 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 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.

### (3.1.) Eingriff des § 48 Abs. 3, 3a, 3b AufenthG in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

#### i. Maßgebliches Grundrecht

Das Recht auf Gewährleistung der 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 Persönlichkeitsrechts 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 Gewährleistung der 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).*

§ 48 Abs. 3a, 3b AufenthG 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 zur Einführung des fast wortgleichen § 15a AsylG, an das § 48 AufenthG angepasst wurde, werden neben Mobiltelefonen auch Tablets und Laptops genannt,

> BT-Drs. 18/11546, S. 23, abrufbar unter: https://dip21.bundestag.de/dip21/btd/18/115/1811546.pdf.

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 Gewährleistung der 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, 46. Edition, Stand: 01.11.2024, 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.

**ii. Eingriffsqualität der einzelnen Schritte der Datenträgerauslesung und -auswertung**

Bereits die Anordnung der Vorlage, Aushändigung und Überlassung von Datenträgern als Vorbereitungshandlung zur Ermöglichung der Auslesung und Auswertung stellt einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, jedenfalls aber in das Eigentumsgrundrecht aus Art. 14 Abs. 1 S. 1 GG dar.

Den zweiten Grundrechtseingriff begründet der technische Vorgang der Auslesung sämtlicher Daten des Datenträgers, bei dem also der Rohdatensatz kopiert wird und in einem behördlichen Datenspeicher abgelegt wird. In diesem Zusammenhang erlangt noch kein Mensch Kenntnis von persönlichen Daten der Betroffenen, bei der Extrahierung werden die auf den Datenträgern vorhanden Datentypen nur kategorisiert und nach Art und Menge angezeigt. Mögliche Kategorien sind Anrufprotokolle, Geräteorte, Kontakte, Sprache, Bilder, Videos und Texte von installierten Anwendungen wie E-Mail- oder Messenger-Diensten, Sprachrekorder oder sonstige Applikationen,

> vgl. Heimann/Bodenbenner: Datenträgerauswertung in der ausländerbehördlichen Praxis, ZAR 2020, 284 (285).

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 von der Maßnahme Betroffenen von den Ausländerbehörden vollständig kopiert und kurzfristig gespeichert, um für die Feststellung der Identität und der Staatsangehörigkeit und für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit möglicherweise bedeutsame Daten zu erheben.

Dem Vorliegen eines Grundrechtseingriffs kann nicht entgegengehalten werden, dass die Betroffenen ihre Datenträger den Ausländerbehörden freiwillig übergäben und ihre Daten damit freiwillig preisgäben, mithin auf ihr Grundrecht verzichteten. Die Vorlage, Aushändigung und Überlassung der Datenträger sowie die Zurverfügungstellung der notwendigen Zugangsdaten können durch Zwangsmittel nach dem Bundes- bzw. der Landesverwaltungsvollzugsgesetze durchgesetzt werden. Ersteres kann auch mit einer Durchsuchung gem. § 48 Abs. 3 S. 2 – 4 AufenthG durchgesetzt werden.

Vgl. Hruschka, in BeckOK Ausländerrecht, Kluth/Heusch, 42. Edition, Stand: 01.07.2024, § 53 m.w.N.

Aus denselben Gründen scheidet auch eine Rechtfertigung des Eingriffs auf Grundlage einer Einwilligung aus.

Eigenständige Eingriffsqualität kommt sodann der Prüfung und Auswertung der ausgelesenen Daten durch eine*n Volljurist*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.

Werden die Ergebnisse der Datenauswertung freigegeben, erfolgt schließlich ein weiterer, vertiefter Grundrechtseingriff dadurch, dass der*die Entscheider*in den Report der Entscheidung über Folgemaßnahmen zur Geltendmachung oder Erleichterung einer Rückführungsmöglichkeit zugrunde legt und Dritten wie z.B. Konsulatsverterter*innen von potentiellen Herkunftstaaten des Betroffenen über die Daten in Kenntnis setzt. Die Ausländerbehörde 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.

**iii. Intensität des Eingriffs**

Werten staatliche Stellen ein informationstechnisches System aus, auf dem sich eine Vielzahl von Daten befinden, die erhebliche Rückschlüsse auf das Leben der Betroffenen zulassen, liegt darin ein intensiver Grundrechtseingriff. § 48 Abs. 3a, 3b AufenthG ermöglichen der Ausländerbehörde den Zugriff auf einen immensen Datenbestand, welchen sie sowohl automatisiert als auch durch Lesen der einzelnen auf dem Datenträger gespeicherten Kommunikationsinhalte auswerten können. Insbesondere Smartphones verbinden große Mengen persönlicher Daten und enthalten gewissermaßen den gesamten digitalen Hausstand: Nachrichten an Familienmitglieder und Partner*innen, Kontaktdaten inklusive Informationen über Anwält*innenkontakte, Konto-und Zahlungsdaten, Zugang zu E-Mail-Accounts, die Suchmaschinen-Historie, Aufenthaltsdaten, intime und persönliche Fotos. Die Eingriffsintensität wird dadurch weiter erhöht, dass die Regelung sich auf Ausländer*innen mit unsicherem Aufenthaltsstatus, in einer Vielzahl der Fälle abgelehnte Asylbewerber*innen, bezieht. Für diese Personengruppe sind ihre Mobilgeräte oft die einzige kommunikative Verbindung zu engen Angehörigen in ihrer alten Heimat und enthalten wichtige Erinnerungen.

Fotos, Videos, Textnachrichten und sonstige gespeicherte Aufzeichnungen geben dem Smartphone im Zusammenspiel regelmäßig die Funktion eines Tagebuchs. Aus Smartphone-Daten lassen sich Bewegungsprofile und soziale Netzwerke ableiten, sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen.

> T. W. Boonstra, M. E. Larsen, H. Christensen (2015): Mapping dynamic social networks in real life using participants' own smartphones, abrufbar unter: https://www.cell.com/action/showPdf?pii=S2405-8440%2815%2930056-6; 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, abrufbar unter: https://www.researchgate.net/publication/318879569_Personality_Traits_Predict_Smartphone_Usage.

Dabei ist insbesondere zu berücksichtigen, dass digitale Medien in einer unsicheren Lebensphase oftmals das wesentliche Mittel der Kommunikation mit engen Angehörigen sind.

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. Betroffen sind mangels darüber hinausgehender tatbestandlicher Einschränkung prinzipiell alle Ausländer*innen ohne gültigen Pass, Passersatz oder sonstigen Identitätsnachweis. Auch wird tatbestandlich kein Verschulden der betroffenen Person hinsichtlich der fehlenden Identitätsklärung vorausgesetzt. Erfasst werden somit die Daten einer Vielzahl von Personen ohne zwingende Anknüpfung an ein zurechenbar vorwerfbares Verhalten oder einen individuell begründeten Verdacht,

> vgl. BVerfGE 125, 260 (318).

Die Erhebung von Telekommunikationsverbindungsdaten und -inhalten hat zudem immer auch zur Folge, dass persönliche Daten Dritter miterhoben werden. Gerade bei abgelehnten Asylbewerber*innen besteht dabei eine hohe Wahrscheinlichkeit, dass neben engen Angehörigen auch Sozial- oder Rechtsberater*innen und Rechtsanwält*innen betroffen sind. Auch die Kommunikation mit anderen Berufsgruppen, bei denen das Vertrauensverhältnis verfassungsrechtlich besonders geschützt ist, etwa Ärzt*innen, Geistliche, Journalist*innen

oder Abgeordnete, kann betroffen sein. Hierdurch wird einerseits die Streubreite des Eingriffs erhöht und andererseits die – auch im Allgemeinwohl liegende – Möglichkeit der Bürger*innen beschränkt, an einer unbeobachteten und damit unbefangenen Fernkommunikation teilzunehmen, sodass die Eingriffsintensität insgesamt weiter erhöht wird,

BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07,1 BvR 595/07, Rn. 233 – juris.

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 Fitnessarmbänder und Smart Watches.

Zudem sind nunmehr auch Cloud-Dienste ausdrücklich erfasst. Der Gesetzgeber verfolgt damit erkennbar das Ziel, auf jede Form der Datenspeicherung von Ausländer:innen zugreifen zu können,

vgl. BT-Drs. 20/9463, S. 37, abrufbar unter: https://dserver.bundestag.de/btd/20/094/2009463.pdf.

### (3.2.) Keine hinreichende Rechtfertigung

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 §§ 48 Abs. 3a, 3b AufenthG nicht gerecht.

#### (3.2.1.) Unverhältnismäßigkeit der Datenträgerauswertung zu migrationspolitischen Zwecken

Das Auslesen des Datenträgers und die Auswertung der ausgelesenen Daten dient der Feststellung der Identität und Staatsangehörigkeit der ausländischen Person und der Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat. Gegenüber dieser migrationspolitischen Zielsetzung erweisen sich die von §§ 48 Abs. 3a, 3b AufenthG ermöglichten Grundrechtseingriffe als unverhältnismäßig.

**i. Datenträgerauswertung ist zur Feststellung von Identität, Staatsangehörigkeit und Rückführungsmöglichkeit 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.

Ausweislich der Gesetzesbegründung ist das „wesentliche tatsächliche Hindernis für die Rückführung ausreisepflichtiger Ausländer […] in vielen Fällen die ungeklärte Identität, die die Beschaffung für die Rückführung erforderlicher Reisedokumente unmöglich macht. Dabei fehlt es bei vielen ausreisepflichtigen Ausländern schon an einem hinreichenden Anknüpfungspunkt für die mögliche Staatsangehörigkeit und mithin einem Anlass für weitere Ermittlungen in Zusammenarbeit mit den Behörden eines möglichen Herkunftsstaates."

> BT-Drs. 18/4097, S.47, abrufbar unter: https://dserver.bundestag.de/btd/18/040/1804097.pdf.

Die Datenträgerauswertung nach § 48 Abs. 3b) AufenthG ist bereits nicht geeignet, in diesem Sinne einen hinreichenden Anknüpfungspunkt für weitere Ermittlungen in Zusammenarbeit mit den Behörden eines möglichen Herkunftsstaates zu schaffen.

So führt die hinsichtlich der Zweckrichtung vergleichbare Auswertung von Datenträgern von Asylsuchenden durch das BAMF lediglich in 1 bis 2 Prozent der Fälle zu Ansätzen, die die Angaben von Asylsuchenden widerlegen. Dies 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 Aussagekraft der gespeicherten Datenkategorien**

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 Migrant*innen ist es wahrscheinlich, dass ihr 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 dem Reiseweg oder im neuen Gastland kennengelernt haben.

Die auf einer Karte dargestellten Geolokationsdaten geben ebenfalls keine sicheren Hinweise auf die Staatsangehörigkeit der betroffenen Person. Sie könnten auch lediglich auf Aufenthalte in einem Land hinweisen. Auch längere Aufenthalte in einer bestimmten Region begründen nicht die entsprechende Zuordnung zu einer bestimmten Staatsangehörigkeit.

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 Migrant*innen auch Sprachen bzw. Dialekte sprechen, die in dem Land ihrer Staatsangehörigkeit nicht verbreitet sind. Das ist beispielsweise der Fall, wenn Migrant*innen für längere Zeit im Ausland gelebt haben oder in einer Familie aufgewachsen sind, die nicht aus ihrem Heimatland kommt.

Auch eine Auswertung von Film- und Fotoaufnahmen in den Speichermedien ermöglicht keine Bestimmung der Identität oder Staatsangehörigkeit einer Person. Die Wiedergabe von Fotos und Filmen steht in der Bedeutung allein für sich selbst. Auf den Aufnahmen zu erkennende dritte Personen, deren Verhältnis zur betroffenen Person allein durch die Aufnahme nicht erkennbar ist, erlauben keine Rückschlüsse auf die Identität der betroffenen Person. Hinsichtlich der ggf. in der Filmaufnahme gesprochenen Sprache gelten die genannten Unsicherheiten bei der Auswertung von Dialekten.

Auch die Identität von Migrant*innen 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 Migrant*innen ein erst vor kurzem erworbenes Mobiltelefon ohne ausreichend große und damit aussagekräftige Datenbestände besitzen können.

**(b) Erhebliche Risiken der automatisierten Erzeugung unrichtiger Daten**

Unrichtige Daten sind zur Erreichung des Zwecks des Verfahrens von vornherein nicht geeignet. Gerade der je nach genutzter Software automatisiert erfolgende Erzeugungsvorgang birgt aber erhebliche Fehlerquellen. Im Rahmen der dem Kläger zugänglichen Informationen ist davon auszugehen, dass diese technisch vergleichbar zur Handydatenauswertung durch das BAMF erfolgt, sodass erhebliche Risiken der Erzeugung unrichtiger Daten bestehen.

So ist bei durch 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.

Bei der Anwendung von 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 Personen 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. 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, abrufbar unter: https://aclanthology.org/P13-2081.pdf.

Eine weitere Fehlerquelle kann darin liegen, dass trotz ausreichender Datenmenge auf einem Smartphone nur ein Ausschnitt der Daten ausgewertet werden kann. Dies ist etwa der Fall, wenn die von der Maßnahme betroffene Person vor allem über Apps kommuniziert, die vom System der Ausländerbehörde nicht unterstützt werden, oder wenn die Ländervorwahlen von eingehenden Nachrichten analysiert werden, die*der Betroffene 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 Personen 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 dem BAMF „manipulierte“ Mobilgeräte vorgelegt haben,

> BT-Drs. 19/6647, Antwort auf Frage 3, abrufbar unter: https://dserver.bundestag.de/btd/19/066/1906647.pdf.

Ob im Falle der automatisierten Erzeugung von Ergebnissen zutreffende Daten dargestellt werden, ist für die Bediensteten der Ausländerbehörde nicht erkennbar. Sie kennen die Algorithmen nicht und haben keinen technischen Sachverstand, um die Zuverlässigkeit der automatisierten Erhebung einzuschätzen. Handreichungen zur Feststellung, dass Datenträger nur unvollständig ausgewertet worden sind und dass keine von Dritten erzeugten Daten erhoben worden sind, finden sich nicht.

**ii. 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 §§ 48 Abs. 3a, 3b AufenthG nicht gerecht.

Die oben dargelegte 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.

§ 48 Abs. 3 S. 1, 3a, 3b AufenthG verfolgt das Ziel der Identitätsfeststellung zur Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat und dienen damit der Vereinfachung und Effektivierung staatlicher Verwaltungstätigkeit. Dies ist zwar als solches legitim. Der gravierende Grundrechtseingriff der verschuldensunabhängigen

Auswertung von Datenträgern lässt sich damit aber nicht rechtfertigen. Diese mangels Anknüpfung an zusätzliche Tatbestandsvoraussetzungen rein migrationspolitische Zielsetzung ist weder mit der Verhinderung gewichtiger Straftaten (insbesondere Terroranschlägen), für die hinreichend konkrete Anhaltspunkte bestehen, noch mit deren Aufklärung zu repressiven Zwecken zu vergleichen. Das bloße Ziel, die Abschiebung von Menschen zu erleichtern, die auf dem Staatsgebiet nicht erwünscht sind, bei denen aber keine Anhaltspunkte dafür bestehen, dass sie hochrangige Rechtsgüter durch Straftaten beeinträchtigen werden, rechtfertigt eine derart eingriffsintensive Maßnahme nicht,

> so auch Möller, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 58 und Lehnert, in: Huber/Mantel, Aufenthaltsgesetz/Asylgesetz, 4. Auflage 2025, § 48 Rn. 21.

Das gilt umso mehr, als die erhobenen und ausgewerteten Daten zur Feststellung der Staatsangehörigkeit weitgehend ungeeignet sind und im Übrigen lediglich Indizien abgeben und keinen Beweis erbringen (siehe dazu bereits ausführlich unter I. 3. c) (3.2.1.) i.).

Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat im Zuge der kürzlich erfolgten Überarbeitung der §§ 48 Abs. 3, 3a, 3b AufenthG festgestellt, dass die Ermächtigungsgrundlagen zur Herausgabe der Zugangsdaten sowie zum Auslesen und Auswerten der Datenträger in Ermangelung einer konkreten Gefahr für ein überragend wichtiges Rechtsgut nicht mit dem Verhältnismäßigkeitsgrundsatz im engeren Sinne vereinbar sind

> Vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Verbesserung der Rückführung, 08.12.2023, S. 2 f., BT-Ausschuss-Drs. 20(4)354, abrufbar: https://www.bundestag.de/resource/blob/982448/9d5c55eb4b99abf8d08f3c75212dff23/20-4-354.pdf.

**(3.2.2.) Verfassungswidrigkeit der konkreten Ausgestaltung**

Auch die konkrete Ausgestaltung des § 48 Abs. 3 S. 1, 3a, 4b AufenthG ist verfassungswidrig.

Die Regelungen enthalten weder eine Begrenzung der Pflicht zur Vorlage, Aushändigung und Überlassung sowie der Befugnis zum Auslesen von Datenträgern auf verhältnismäßige Fälle noch Einschränkungen der Auswertung, insbesondere bezüglich Anlass und Reichweite (unter i. und ii.). Der Kernbereich privater Lebensgestaltung wird nicht hinreichend geschützt (unter iii.) und es fehlen verfahrensrechtliche Anforderungen zum Schutz der Grundrechte der Betroffenen (unter iv.).

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 vor dem Hintergrund der entsprechenden gesetzgeberischen Intention auch nicht Aufgabe der Gerichte –, diese strengeren Vorgaben im Wege einer verfassungskonformen Auslegung zu etablieren.

**i. Verletzung des Bestimmtheitsgebots**

Zunächst erfüllen die Ermächtigungsgrundlagen des § 48 Abs. 3, 3a, 3b AufenthG nicht die verfassungsrechtlichen Anforderungen des Bestimmtheitsgebots.

Dieses stellt 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).

Entsprechend der Wesentlichkeitslehre sind wegen der hohen Eingriffsintensität auch hohe Anforderungen an die Bestimmtheit zu stellen,

BVerfG, Beschluß vom 8. 8. 1978 - 2 BvL 8/77, NJW 1979, 359 (360).

Diesen werden die angegriffenen Normen mangels hinreichender Konkretisierung der erfassten Datenträger und der erfassten Daten nicht gerecht.

Die von der Vorlage-, Aushändigungs- und Überlassungspflicht nach § 48 Abs. 3 S. 1 AufenthG erfassten Datenträger werden nicht hinreichend bestimmt festgelegt. Ausländer*innen können danach zur Herausgabe aller Urkunden, sonstigen Unterlagen und Datenträger, die für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat von Bedeutung sein können und in deren Besitz sie sind, verpflichtet werden.

Das Tatbestandsmerkmal „von Bedeutung sein können“ ist zu weit und unbestimmt. Nach dem BVerwG setzt dieses lediglich voraus, dass der Datenträger für die zu treffende Feststellung nicht schlechthin ungeeignet sein darf, was sich bereits aus der Vielzahl der auf einem Datenträger gespeicherten Inhalte ergeben könne,

BVerwG, Urteil vom 16. Februar 2023 – 1 C 19/21 –, BVerwGE 178, 8-17, Rn. 30.

Dieses Tatbestandsmerkmal erfüllen damit prinzipiell alle erdenklichen Datenträger. Konkrete Anhaltspunkte für die Eignung setzt die Norm nicht voraus. Auch fehlt jede Eingrenzung auf bestimmte Arten von Datenträgern.

Auch die §§ 48a, 48b AufenthG enthalten keine weitere Eingrenzung der erfassten Datenträger und sind daher zu unbestimmt.

Darüber hinaus enthalten die Ermächtigungsgrundlagen in § 48 Abs. 3a, 4b AufenthG keine Bestimmung zur Reichweite der Datenverarbeitungsbefugnisse, insbesondere wird Art und Ausmaß der auszulesenden und auszuwertenden Daten nicht näher spezifiziert und es wird nicht zwischen Verkehsdaten und Inhaltsdaten unterschieden, was ebenfalls gegen die grundrechtlichen Anforderungen an die Normenbestimmtheit und Normenklarheit verstößt.

**ii. Fehlende Verhältnismäßigkeit**

Die Ermächtigungsgrundlagen in § 48 Abs. 3, 3a, 3b AufenthG sind darüber hinaus unverhältnismäßig, da sie keine hinreichenden tatbestandlichen Begrenzungen auf geeignete, erforderliche und angemessene Fälle vorsehen.

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

§§ 48 Abs. 3a, 3b AufenthG begrenzen die Art der auszulesenden und auszuwertenden Daten lediglich durch den Zweck, Identität und Staatsangehörigkeit festzustellen und eine Rückführungsmöglichkeit festzustellen und geltend zu machen. Dazu können auf dem Datenträger gespeicherte Daten sehr unterschiedlicher Art ausgewertet werden. § 48 Abs. 3c AufenthG enthält keinerlei begrenzende Regelungen hinsichtlich der Art der auszuwertenden Daten. So wird zunächst die Auswertung nicht auf Daten, die für die zu treffenden Feststellungen voraussichtlich geeignet sind, beschränkt. Die Ermächtigungsgrundlage schließt weder aus, dass neben Metadaten auch gespeicherte Kommunikationsinhalte ausgewertet werden dürfen, noch enthält sie entsprechend differenzierte Eingriffsschwellen. Darüber hinaus ist der Schutz des Kernbereichs privater Lebensgestaltung unzureichend.

**(b) Fehlende Erforderlichkeit**

Die Ermächtigungsgrundlagen in § 48, 48a, 48b AufenthG stellen in ihrer derzeitigen Ausgestaltung nicht sicher, dass die erlaubten Eingriffe stets das relativ mildeste Mittel bei gleicher Eignung sind.

**(i.) Fehlende Erforderlichkeit der Überlassung und des Auslesens von Datenträgern**

Die Ermächtigungsgrundlagen in § 48 Abs. 3, 3a AufenthG verstoßen gegen den Erforderlichkeitsgrundsatz. Die tatbestandlichen Voraussetzungen der Norm in § 48 Abs. 3 S. 1, 3a, 3b AufenthG sind uneinheitlich ausgestaltet, wodurch nicht erforderliche Maßnahmen erlaubt werden. Die Normen erlauben in § 48 Abs. 3 S. 1 AufenthG einerseits die Anordnung der Aushändigung und Überlassung von Daternträgern in Fällen, in denen das Auslesen ausgeschlossen ist und andererseits in § 48 Abs. 3a AufenthG das Auslesen von Datenträgern in Fällen, in denen die Auswertung ausgeschlossen ist und erfassen damit Fälle, in denen es an der Eignung bzw. Erforderlichkeit fehlt.

Die Anordnung der Überlassung eines Datenträgers kann zur Identitäts- und Staatsangehörigkeitsfeststellung von vornherein nur dann geeignet sein, wenn auch das Auslesen des Datenträgers zulässig ist. Das Auslesen eines Datenträgers kann zur Identitäts- und Staatsangehörigkeitsfeststellung von vornherein nur dann geeignet sein, wenn auch das Auswerten des Datenträgers zulässig ist. Steht demgegenüber zur Zeit der Anordnung des Überlassens bzw. zur Zeit des Auslesens nicht fest, dass das Auswerten des Datenträgers zulässig ist, sind diese Maßnahmen von vornherein ungeeignet.

Jedenfalls würde es sich in solchen Fällen um ein Überlassen oder Auslesen auf „Vorrat“ und damit um eine „Vorratsdatenspeicherung“ handeln, welche einen Verstoß gegen den Erforderlichkeitsgrundsatz begründet.

Diesen Anforderungen wird die derzeitige Ausgestaltung der §§ 48 Abs. 3 S. 1, 3a, 3b AufenthG nicht gerecht. § 48 Abs. 3 S. 1 AufenthG verlangt für die Überlassungsanordnung lediglich den Nichtbesitz eines Passes oder Passersatzes. Demgegenüber ist das Auslesen gemäß § 48 Abs. 3a S. 1 AufenthG unzulässig, wenn der*die Ausländer*in einen sonstigen geeigneten Identitätsnachweis besitzt. Ist die betroffene Person im Besitz eines solchen Identitätsnachweises, ist die Herausgabe eines Datenträgers, obwohl von § 48 Abs. 3 S. 1 AufenthG zugelassen, kein geeignetes Mittel zur Identitäts- und Staatsangehörigkeitsklärung, da dieser nicht ausgelesen werden darf.

Darüber hinaus fehlt in den Regelungen zur Überlassungsanordnung nach § 48 Abs. 3 S. 1 AufenthG sowie zur Befugnis zum Auslesen nach § 48 Abs. 3a S. 1 AufenthG anders als in der Regelung der Befugnis zur Auswertung nach § 48 Abs. 3b S. 1 AufenthG eine tatbestandliche Normierung des Erforderlichkeitsgrundsatzes dergestalt, dass der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann. Somit ist nicht sichergestellt, dass die Datenträgerüberlassung und -auswertung letztes Mittel und (zeitlich) nachrangig gegenüber milderen Mittel wie einer Befragung zur Herkunft und Identität ist,

> vgl. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23.03.2017, BT-Ausschuss-Drs. 18 (4) 831, S. 4 f.; abrufbar: https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf.

Bemerkenswert ist insofern, dass die jetzige, durch das „Rückführungsverbesserungsgesetz“ geänderte Fassung der §§ 48 Abs. 3, 3a, 3b AufenthG im Vergleich zur alten Fassung somit zu einer weiteren Abschwächung des Grundrechtsschutzes in Form einer Aufweichung des Erforderlichkeitsgrundsatzes führt. Vor der Änderung differenzierte die Norm nicht zwischen dem Auslesen und Auswerten, sondern enthielt eine einheitliche Regelung zur Datenauswertung, die nur zulässig war, wenn der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden konnte.

Nach der Rechtsprechung des Bundesverwaltungsgerichts zur Parallelnorm des § 15a Abs. 1 S. 1 AsylG aF umfasste der Begriff der Datenauswertung auch das Auslesen des Datenträgers, sodass auch dieses nur zulässig war, wenn der Zweck der Maßnahme nicht durch mildere Mittel wie der Vorlage sonstiger Unterlagen, dem Abgleich von Registern oder der Befragung des Sprachmittlers erreicht werden konnte.

> Vgl. BVerwG, Urteil vom 16. Februar 2023 – 1 C 19/21 –, BVerwGE 178, 8-17, Rn. 25, 37 – 38.

Demgegenüber setzt das Auslesen nach § 48 Abs. 3a S. 1 AufenthG nunmehr keine solche Erforderlichkeitsprüfung voraus. Dies folgt aus dem Wortlaut „erforderlich ist, da der Ausländer keinen gültigen Pass, Passersatz oder sonstigen geeigneten Identitätsnachweis besitzt“, sowie einem Umkehrschluss zu § 48 Abs. 3b S. 1 AufenthG, der ausdrücklich vorsieht, dass „der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann“. Das Ergebnis wird bestätigt durch die Gesetzesbegründung, die davon spricht, dass das „frühzeitige Auslesen der Datenträger somit zu einem Zeitpunkt [erfolgen soll], bei dem die größtmögliche Wahrscheinlichkeit eines Vorhandenseins von relevanten Daten besteht“ und ausdrücklich

zwischen den Voraussetzungen des Auslesens und des Auswertens differenziert wird. „Dieser schwerwiegendere Eingriff soll deshalb nur unter der Voraussetzung erfolgen, dass der Eingriff erforderlich ist und keine milderen Mittel zur Verfügung stehen."

> BT-Drs. 20/9463, S. 37, 55, abrufbar unter: https://dserver.bundestag.de/btd/20/094/2009463.pdf.

Durch diesen Verzicht auf die Erforderlichkeitsprüfung werden wiederum die Überlassungsanordnung und die Datenträgerauslesung „auf Vorrat" erlaubt in Fällen, in denen eine Auswertung wegen bestehender milderer Mittel unzulässig ist.

> Vgl. DAV, Stellungnahme zum Referentenentwurf eines Gesetzes zur Verbesserung der Rückführung, Oktober 2023, S. 5 f.; abrufbar: https://anwaltverein.de/de/newsroom/sn-75-23-rueckfuehrungsverbesserungsgesetz?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2023/dav-sn-75-23-gesetz-zur-verbesserung-der-rueckfuehrung-docx.pdf

**(ii.) Fehlende Erforderlichkeit der Auswertung mangels Ausschluss oder Begrenzung der Auswertung von Kommunikationsinhalten**

Die von §§ 48 Abs. 3a, 3b AufenthG erlaubten Eingriffe sind darüber hinaus insoweit nicht erforderlich, als sie unterschiedslos den Zugriff auf alle auf dem Datenträger – oder in über ihn zugänglichen Clouddiensten – gespeicherten Daten erlauben, ohne den Zugriff auf Meta- bzw. Verkehrsdaten zu beschränken oder zumindest gesteigerte Eingriffsvoraussetzungen für den Zugriff auf Kommunikationsinhalte vorzusehen.

Eine Auswertung nur von Metadaten stellt ein milderes Mittel im Vergleich zur Auswertung von Kommunikationsinhalten dar, welcher eine wesentlich erhöhte Eingriffsintensität zukommt. Vor diesem Hintergrund gebietet der Grundsatz der Erforderlichkeit einen Ausschluss der Auswertung von Kommunikationsinhalten. Hilfsweise ist zumindest ein gestuftes Vorgehen dergestalt vorzugeben, dass die Auswertung von Kommunikationshinhalten nur unter der Voraussetzung zulässig ist, dass die zu treffenden Feststellungen durch eine Auswertung allein von Metadaten aussichtslos oder wesentlich erschwert würden.

Falls die Auswertung von Metadaten im Vergleich zur Auswertung von Kommunikationsinhalten nicht als gleich geeignet erachtet wird, ergeben sich identische Anforderungen auf der Ebene der Angemessenheit.

Eine vergleichbare Differenzierung sieht die StPO vor: So dürfen Verkehrsdaten gemäß § 100g Abs. 1 Nr. 1 StPO bereits beim Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Eine Online-Durchsuchung setzt dagegen den Verdacht einer auch im Einzelfall besonders schweren Straftat voraus, deren Erforschung auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Eine solche tatbestandliche Differenzierung zwischen Metadaten und Kommunikationsinhalten sehen §§ 48 Abs. 3a, 3b AufenthG nicht vor. Bereits der Wortlaut spricht nur vom „Auslesen von Datenträgern“ und vom „Auswerten der ausgelesenen Daten“. Nach § 48 Abs. 3b S. 3, 4 AufenthG dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch das Auswerten von Datenträgern erlangt werden, nicht verwertet werden und sind unverzüglich zu löschen. Damit setzt die Norm voraus, dass auch Kommunikationsinhalte und nicht lediglich Metadaten, die kaum zu einer Berührung des Kernbereichs führen können, ausgelesen und ausgewertet werden können. Auch die Gesetzesbegründung geht neben der Auswertung von Metadaten von der Auswertung gespeicherter Inhalte aus: *„So können etwa die Adressdaten in dem Mobiltelefon eines ausreisepflichtigen Ausländers […] wesentliche Hinweise auf eine mögliche Staatsangehörigkeit geben. Erfasst sind zum Beispiel auch in elektronischer Form in (Klein-)Computern gespeicherte Reiseunterlagen.“*

> BT-Drs. 18/4097, S. 47, abrufbar unter: https://dserver.bundestag.de/btd/18/040/1804097.pdf.

Auch hinsichtlich des 2024 ergänzten Zugriffs auf Cloud-Dienste stellt die Gesetzesbegründung auf die in der Cloud selbst gespeicherten Inhalte ab: *„Es besteht funktional kein Unterschied, ob man die Daten lokal auf einem Speicher im Mobiltelefon oder via Internet auf der serverbasierten Cloud speichert. […] Das Bedürfnis für die Klarstellung ergibt sich aus der zunehmenden Bedeutung dieser Form der Datenspeicherung bei Personen aus vielen Herkunftsländern.“*

BT-Drs. 20/9463, S. 37, abrufbar unter: https://dserver.bundestag.de/btd/20/094/2009463.pdf.

In der Praxis unterliegt es damit letztlich der freien Entscheidung des*der zuständigen Sachbearbeiter*in, welche Datentypen ausgelesen und ausgewertet werden sollen:

*„Bei diesen Datentypen handelt es sich beispielsweise um Anrufprotokolle, Geräteorte, Kontakte, Sprache, Bilder, Videos und Texte von installierten Anwendungen wie E-Mail- oder Messenger-Diensten, Sprachrekordern oder sonstigen Applikationen. Das bedeutet, dass die auf dem Gerät existierenden Datentypen nach Art und Menge angezeigt werden und der Anwender entscheiden kann, z. B. nur die Telefonverbindungsdaten zu extrahieren. […] Die […] Inhalte werden anschließend dem zuständigen Sachbearbeiter freigegeben. Dieser nimmt eine vergleichende Analyse mit den Inhalten der Ausländerakte vor, um Hinweise auf die bislang unbekannte Identität oder Staatsangehörigkeit zu erlangen. Für nicht-native Textinhalte ist für über 70 Sprachen eine Übersetzungsunterstützung gegeben. Die eingesetzte Software ermöglicht dabei die rasche Analyse von Massendaten, womit die Einsichtnahme in jedes einzelne Datum nicht mehr erforderlich ist. So werden beispielsweise prozentuale Verteilungen von gewählten Telefonverbindungen in die jeweiligen Zielländer aufgezeigt, Zeiträume hochfrequenter Nutzung oder Geolokationen samt Zeitpunkten“,*

Heimann/Bodenbenner, ZAR 2020, 284 (285 f.).

**(c) Fehlende Angemessenheit**

Die Ermächtigungsgrundlagen in § 48, 48a, 48b AufenthG werden den oben dargelegten Anforderungen für die Angemessenheit von Eingriffen in das Grundrecht auf Vertraulichkeit und Integrität computertechnischer Systeme (I. 3. c) (3.2.1.) ii.) unter verschiedenen Gesichtspunkten nicht gerecht.

**(i.) Fehlende tatbestandliche Begrenzung der betroffenen Personengruppe auf Personen mit Duldung nach § 60b AufenthG**

Die Ermächtigungsgrundlagen in § 48 Abs. 3, 3a, 3b AufenthG zur Anordnung der Vorlage, Aushändigung und Überlassung von Datenträgern sowie zum Auslesen und Auswerten von Datenträgern sind mangels tatbestandlicher Begrenzung der betroffenen Personengruppe unangemessen.

Wie oben dargelegt, setzt die Angemessenheit einer staatlichen Datenträgerauswertung „tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend

wichtiges Rechtsgut“ voraus. Erforderlich ist damit eine tatbestandliche Ausgestaltung des §48 Abs. 3a, b AufenthG, die eine Datenträgerauslesung und -auswertung nur in solchen Fällen erlaubt. Vergleichbar erscheint insofern die Regelung des § 100b StPO, die den auf bestimmte Tatsachen begründeten Verdacht der Täterschaft oder Teilnahme an einer besonders schweren Straftat, welche auch im Einzelfall besonders schwer wiegt, verlangt.

In entsprechender Weise dürfte eine konkrete Gefahr für ein überragend wichtiges Rechtsgut nicht in jedem Fall einer vollziehbaren Ausreiseplicht, sondern nur bei Bestehen eines besonderen Interesses an der Abschiebung, zB im Falle eines besonderen Ausweisungsinteresse iSv §§ 53 Abs. 1, 54 AufenthG, vorliegen.

Jedenfalls kann die Datenträgerauswertung zur Abwehr einer solchen konkreten Gefahr für ein überragend wichtiges Rechtsgut im Einzelfall nur dann angemessen sein, wenn es sich um einen vollziehbar ausreisepflichten Ausländer handelt, dessen Abschiebung aus von ihm selbst zu vertretenden Gründen in Form der fehlenden Mitwirkung bei der Identitäts- und Staatsangehörigkeitsklärung nicht vollzogen werden kann.

Denn Zweck der Norm ist die Ermöglichung einer Abschiebung. Eine relevante, den intensiven Grundrechtseingriff rechtfertigende Förderung dieses Zwecks kann die Identitäts- und Staatsangehörigkeitsklärung mittels Datenträgerauswertung von vornherein nur dann darstellen, wenn die betroffene Person vollziehbar ausreisepflichtig ist. Darüber hinaus ermöglicht die Identitätsklärung auch dann keine Abschiebung, wenn die betroffene Person zwar vollziehbar ausreisepflichtig ist, aber neben der Passlosigkeit zusätzliche Abschiebungshindernisse rechtlicher oder tatsächlicher Art iSv § 60a Abs. 2 S. 1 AufenthG bestehen. In diesen Fällen kann eine Maßnahme nach §§ 48 Abs. 3 S. 1. 3a, 3b AufenthG damit von vornherein aufgrund der äußerst geringen Eignung nicht verhältnismäßig sein.

Damit kämen als Adressatenkreis der Ermächtigungsgrundlagen in §§ 48 Abs. 3 S. 1, 3a, 3b AufenthG bei verhältnismäßiger Ausgestaltung von vornherein nur vollziehbar aureisepflichtige Personen mit einer Duldung nach § 60b AufenthG (für Personen mit ungeklärter Identität aus selbst zu vertretenden Gründen) in Betracht, in deren Person ein besonderes Interesse an der Abschiebung, zB im Falle eines besonderen Ausweisungsinteresses iSv §§ 53 Abs. 1, 54 AufenthG besteht.

Eine entsprechende Begrenzung der erfassten Personengruppen enthalten die Ermächtigungsgrundlagen in § 48 Abs. 3, 3a, 3b AufenthG nicht. Alleinige adressatenbezogene Tatbestandsvoraussetzung des § 48 Abs. 3 S. 1 AufenthG ist der Nichtbesitz eines gültigen Passes oder Passersatzes. Für das Auslesen und Auswerten von Datenträgern nach § 48 Abs. 3a, 3b AufenthG ist darüber hinaus der Nichtbesitz sonstiger

geeigneter Identitätsnachweise erforderlich. Die Normen setzen damit lediglich das Fehlen eines Passes bzw. Identitätsnachweises voraus, knüpfen aber im Übrigen nicht ausdrücklich an die aufenthaltsrechtliche Situation der betroffenen Person an.

Eine tatbestandliche Begrenzung des erfassten Personenkreises ergibt sich auch nicht aus dem Erfordernis, dass die Maßnahmen „für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat von Bedeutung sein können“ bzw. „erforderlich“ sind. Denn bei der Feststellung und Geltendmachung einer Rückführungsmöglichkeit handelt es sich nicht um ein Tatbestandsmerkmal, sondern lediglich um eine Zweckbestimmung. So könnten Anordnungen nach § 48 Abs. 3, 3a, 3b AufenthG nach dem Wortlaut darauf gestützt werden, dass die Identitätsklärung für die künftige Geltendmachung einer Rückführungsmöglichkeit im Fall einer künftig entstehenden vollziehbaren Ausreisepflicht erforderlich sei. Für dieses Verständnis spricht auch die systematische Stellung der Norm innerhalb der allgemeinen, für alle Ausländer*innen geltenden ausweisrechtlichen Pflichten nach § 48 AufenthG in Abgrenzung zu den besonderen Mitwirkungspflichten vollziehbar ausreisepflichtiger Personen nach § 60b AufenthG.

§ 48 Abs. 3 S. 1, 3a, 3b AufenthG setzt somit kein besonderes Interesse an der Abschiebung bzw. ein Ausweisungsinteresse voraus und erfasst auch Personen, deren Abschiebung aus anderen rechtlichen oder tatsächlichen Gründen unmöglich ist, etwa wegen Krankheit, Schwangerschaft (§ 60a Abs. 2 AufenthG) oder Ausbildung (§ 60c AufenthG). Darüber hinaus setzt die Norm tatbestandlich nicht einmal das Bestehen einer vollziehbaren Ausreisepflicht voraus. Demnach könnte sogar gegenüber Personen mit gültiger Aufenthaltserlaubnis die Herausgabe von Datenträgern angeordnet werden. Dies betrifft insbesondere Inhaber*innen des Chancen-Aufenthaltsrechts nach § 104c Abs. 1 AufenthG, welches gerade keinen Passbesitz und keine Identitätsklärung voraussetzt.

Da die Auswahl der Fälle, in denen ein solches besonderes Interesse an der Abschiebung bestehen könnte, dem originären gestalterischen Aufgabenbereich des Gesetzgebers unterfällt, kommt eine verfassungskonforme Auslegung der Ermächtigungsgrundlagen nicht in Betracht.

**(ii.) Fehlende tatbestandliche Begrenzung der Überlassung von Datenträgern**

Darüber hinaus fehlt eine Differenzierung zwischen der Eingriffsschwelle für Urkunden und Unterlagen einerseits sowie Datenträgern andererseits. Die Verhältnismäßigkeit im engeren Sinne kann nur gewahrt werden, wenn die Befugnisnorm die Anordnung der Herausgabe von Datenträgern nur im Falle der Aussichtslosigkeit der Identitätsfeststellung durch Urkunden und

sonstige Unterlagen erlaubt, weil es sich im Vergleich zu Urkunden bzw. Unterlagen um einen Eingriff mit wesentlich höherer Intensität handelt.

Bei Urkunden und Unterlagen handelt es sich um Einzelobjekte mit von vornherein begrenztem Datenumfang. Urkunden beweisen regelmäßig eine bestimmte Tatsache oder ein bestimmtes Ereignis, erlauben aber keinen umfassenden Einblick in das Leben der betroffenen Person. Auch sind einschlägige Urkunden regelmäßig gut zur Identitätsfeststellung geeignet. Wird etwa die Herausgabe einer Geburts- oder Eheurkunde oder eines Schulzeugnisses angeordnet, besteht die begründete Erwartung, hieraus Erkenntnisse über die Identität und Staatsangehörigkeit der betroffenen Person zu erhalten, da diese Urkunden hierüber regelmäßig Angaben enthalten. Demgegenüber enthalten Datenträger – insbesondere Smartphones oder Laptops – eine unüberschaubare Vielzahl an Daten, die einen tiefgehenden Einblick in das Leben der betroffenen Person erlauben und gleichzeitig größtenteils ungeeignet sind für Zwecke der Identitätsfeststellung (s.o. I. 3. c) (3.2.1.) i.). Bei der Anordnung der Herausgabe von Smartphones oder Laptops besteht regelmäßig gerade keine Erwartung, eine bestimmte Information zu erhalten, vielmehr handelt es sich um Ermittlungen ins Blaue hinein.

**(iii.) Keine Begrenzung der Auswertung auf voraussichtlich geeignete Daten**

Die Regelung zur Auswertung der ausgelesenen Daten in § 48 Abs. 3c AufenthG ist auch insofern unangemessen, als sie die auszuwertenden Daten von vornherein nicht auf solche Daten beschränkt, die voraussichtlich geeignet sind für die zu treffenden Feststellungen. Wie oben dargelegt, weist ein erheblicher Teil der auf einem Smartphone gespeicherten Daten eine allenfalls begrenzte Aussagekraft auf. Vor diesem Hintergrund ist die Regelung nur dann angemessen, wenn sie Art und Umfang der auszuwertenden Daten möglichst grundrechtsschonend auf das Mindestmaß beschränkt. Dies gilt insbesondere vor dem Hintergrund, dass es sich beim Auslesen und Auswerten eines Datenträgers um einen Eingriff ins Blaue hinein handelt, der nach der Gesetzesbegründung dazu dient, einen *„hinreichenden Anknüpfungspunkt für die mögliche Staatsangehörigkeit und mithin einem Anlass für weitere Ermittlungen“* zu finden,

> BT-Drs. 18/4097, S. 47, abrufbar unter: https://dserver.bundestag.de/btd/18/040/1804097.pdf.

Die zur Wahrung der Angemessenheit erforderliche Begrenzung kann positiv durch eine Beschränkung der zulässigerweise auszuwertenden Daten ihrer Art nach (zB ausschließlich

die Ländervorwahlen von Anrufern, Geodaten von Fotos, Anrede und Grußformel bei E-Mails) oder zumindest negativ durch einen Ausschluss der Auswertung von Daten mit hoher Persönlichkeitsrelevanz (zB keine Einsichtnahme in Inhalte von E-Mails und Chats) erfolgen,

vgl. Bruckermann, SRa 2018, 133 (135 f.).

Dies wird durch den Wortlaut des § 48 Abs. 3b AufenthG, der die Datenauswertung zulässt, „soweit“ dies für die zu treffenden Feststellungen erforderlich ist, nicht sichergestellt. Der hierin verankerte Erforderlichkeitsgrundsatz schließt nur die Auswertung solcher Daten aus, hinsichtlich derer eine Förderung des Zwecks mit Sicherheit ausgeschlossen ist.

**iii. Unzureichender Schutz des Kernbereichs privater Lebensgestaltung**

Die Ermächtigungsgrundlagen in § 48 Abs. 3a, 3b AufenthG erlauben Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung ein und verletzen dadurch Art. 1 Abs. 1 GG.

Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen,

BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1786 Rn. 121).

Wie bereits oben umfassend ausgeführt, erlaubt § 48 Abs. 3a, 3b die Auslesung und Auswertung aller Daten, die auf den eingezogenen Datenträgern vorhanden sind (I. 3. c) (3.1.) iii.). Insbesondere enthalten Mobiltelefone typischerweise Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind (Kommunikationsinhalte, intime Bilder und Videos etc.).

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden,

vgl. BVerfGE 109, 279 [314] = NJW 2004, 999; BVerfGE 120, 274 [339] = NJW 2008, 822; stRspr.

**(a) Unzureichender vorgelagerter Schutz des Kernbereichs privater Lebensgestaltung**

Der vorgelagerte Schutz des Kernbereichs privater Lebensgestaltung ist unzureichend. Nach der verfassungsrechtlichen Rechtsprechung zu Überwachungsmaßnahmen ist die Art der Datenerhebung so auszugestalten, dass die Erfassung von Kernbereichsdaten gar nicht erst erfolgt,

BVerfGE 120, 274 (338) = NJW 2008, 822.

Auf der Ebene der Datenerhebung ist bei verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt,

BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1787 Rn. 128 m.w.N.).

Können staatliche Maßnahmen typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten,

vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1787 Rn. 123) m.w.N.

Für die nachträgliche Erhebung von auf einem Datenträger gespeicherte Kommunikationsinhalte und sonstige Daten, die dem Kernbereich zugeordnet sind, können keine geringeren Anforderungen gelten,

so auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60

Insoweit ist der vorgelagerte Schutz des Kernbereichs privater Lebensgestaltung in § 48 Abs. 3a, 3b AufenthG unzureichend. Ausdrücklich unzulässig ist es lediglich nach § 48 Abs. 3b S. 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. Hinsichtlich der Befugnis zum Auslesen von Datenträgern in § 48 Abs. 3a S. 1 AufenthG findet sich keinerlei Begrenzung zum Schutz des Kernbereichs privater Lebensgestaltung.

Lediglich die Auswertung von Datenträgern ist nach § 48 Abs. 3b Satz 1 AufenthG unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch das Auswerten von Datenträgern allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Diese Regelung ist aber praktisch bedeutungslos, da von der Auswertung der Datenträger von Asylsuchenden nie „allein“ Erkenntnisse aus dem Kernbereich zu erwarten sind. Vielmehr handelt es sich bei den betroffenen Datenträgern regelmäßig um Mischdatenbestände, sodass der angestrebte Kernbereichsschutz vollständig leer läuft und im Ergebnis keinen Schutz bietet,

> so auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60 und *Lehnert*, in: Huber/Mantel, Aufenthaltsgesetz/Asylgesetz, 4. Auflage 2025, § 48 Rn. 21 sowie GK-AslylG/Funke-Kaiser AsylG § 15a Rn. 12; vgl. *Vasel/Heck*, NVwZ 2024, 540 (546); Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23.03.2017, S. 7; abrufbar: https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf.

Zwingend erforderlich und ohne Weiteres möglich wäre eine Regelung entsprechend § 100d Abs. 3 S. 1 StPO, welche einen wirksamen Kernbereichsschutz sicherstellt, indem soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

**(b) Unzureichender nachgelagerter Schutz des Kernbereichs privater Lebensgestaltung mangels Richtervorbehalts**

Auch der nachgelagerte Kernbereichsschutz ist unzureichend. Auf der Ebene der Auswertung und Verwertung ist dessen Einhaltung durch eine unabhängige Prüfung sicherzustellen. Es fehlt aber an institutionalisierten Mechanismen, die eine solche unabhängige Kontrolle gewährleisten. Die Regelung des § 48 Abs. 3a Satz 6 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.

Nach der Rechtsprechung des Bundesverfassungsgerichts hat der Gesetzgeber auf der Ebene der Auswertung für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor der anschließenden Verwendung der Daten herausfiltert. Die Erforderlichkeit einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab. Dabei kann auf die Sichtung durch eine unabhängige Stelle umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt,

> vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 NJW 2016, 1781 (1787 Rn. 129 m.w.N.).

Wie bereits oben ausgeführt, sieht § 48 Abs. 3a, 3b AufenthG unzureichende Vorkehrungen vor, den Schutz des Kernbereichs schon im Vorfeld zu gewährleisten. Daher ist die Sichtung durch eine unabhängige Stelle unverzichtbar.

Ungeachtet ihrer juristischen Qualifikation fehlt es bei Behördenmitarbeiter*innen, die aufgrund beamtenrechtlicher oder arbeitsvertraglicher Treuepflichten den Weisungen ihres Dienstherrn bzw. ihres Arbeitgebers unterstehen und bei denen aufgrund ihrer Aufgabenstellung und den damit verbundenen Zielsetzungen eine interessensgeleitete Entscheidung nicht auszuschließen ist, an der für einen Richtervorbehalt typischen Unabhängigkeit und Unparteilichkeit,

> vgl. *Vasel/Heck*, NVwZ 2024, 540 (547); Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, a.a.O.; *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 53.

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).

**iv. Keine effektiven verfahrensrechtlichen Sicherungen mangels Transparenz für Betroffene**

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).

Zwar gelten für die Datenverarbeitung durch die Ausländerbehörde 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 die Ausländerbehörde 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).

**(4) Europarechtswidrigkeit der Ermächtigungsgrundlagen**

Schließlich verstößt § 48 Abs. 3a, 3b AufenthG aus den dargelegten Gründen gegen Europarecht, weil die durch Auslesung und Auswertung erfolgende Datenverarbeitung in unverhältnismäßiger Weise in die von Art. 7 und 8 der Charta verbürgten Rechte auf Achtung des Privat- und Familienlebens und auf Schutz personenbezogener Daten der von der Maßnahme Betroffenen eingreift.

Nach der Rechtsprechung des EuGH ist es für die Verhältnismäßigkeit einer staatlichen Regelung, die den Zugriff der zuständigen nationalen Behörden auf personenbezogene Daten gewährt, wenn er die Gefahr eines schwerwiegenden oder sogar besonders schwerwiegenden

Eingriffs in die Grundrechte der betroffenen Person mit sich bringt, von wesentlicher Bedeutung, dass der Datenzugang von einer vorherigen Kontrolle durch ein Gericht oder eine von der die Daten verarbeitende Stelle unabhängige Verwaltungsstelle abhängig gemacht wird,

> EuGH (Große Kammer), Urteil vom 04.10.2024 – C-548/21, BeckRS 2024, 26054 Rn. 102.

So hat der EuGH festgestellt, dass der Zugriff auf die in einem Mobiltelefon gespeicherten Daten durch polizeiliche Ermittlungsmaßnahmen zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen aufgrund der Vielfalt und Sensibilität der Daten, sehr genaue Schlüsse auf das Privatleben der betroffenen Person zulassen, als ein schwerwiegender oder sogar besonders schwerwiegender Eingriff in die in den Art. 7 und 8 der Charta verbürgten Grundrechte darstellt.

> EuGH (Große Kammer), Urteil vom 04.10.2024 – C-548/21, BeckRS 2024, 26054, Rn. 92 ff.

Aufgrund der fehlenden Gewährleistung einer angemessenen Kontrolle durch eine unabhängige Stelle im Vorfeld der Auslesung und Auswertung nach § 48 Abs. 3a, 3b AufenthG (s.o.) genügen die Ermächtigungsgrundlagen nicht den Verhältnismäßigkeitsanforderungen des EuGH und verletzen die Rechte der Betroffenen aus Art. 7 und 8 Charta der Grundrechte der Europäischen Union. Das Unionsrecht ist grundsätzlich anwendbar über Art. 6 Abs. 1 UAbs. 1 lit. 2, Abs. 3 DSGVO und die Grundrechte bilden den Maßstab für die Anforderungen des Art. 6 Abs. 3 Satz 2 und 4 DSGVO an das nationale Recht, wodurch die jüngst entwickelten Maßgaben auch auf die hiesige Konstellation übertragbar sind.

**3. Begründetheit hinsichtlich Ziffern 4 und 5 des Bescheids.**

Die Klage ist auch bezüglich der Ziffern 4 und 5 des Bescheids begründet. Die Androhung des unmittelbaren Zwangs sowie die Androhung der Ersatzvornahme sind rechtswidrig und der Kläger ist dadurch in seinen Rechten verletzt.

Die Androhung in Ziffer 4 des Bescheids vom … ist materiell rechtswidrig, da die ihr zugrundeliegende Überlassungsanordnung in Ziff. 1 des Bescheids materiell rechtswidrig ist (s.o. B. II. 3. c)). Darüber hinaus war die Androhung der Vollstreckung durch unmittelbaren Zwang, nicht geeignet, die Überlassung der Datenträger zu veranlassen. Zum Zeitpunkt der

Bekanntgabe der Androhung hatte die Mitarbeiterin des Regierungspräsidiums das Mobiltelefon bereits an sich genommen und sie somit dem Zugriff des Antragsteller entzogen.

Die Androhung der Ersatzvornahme in Ziffer 5 des Bescheids vom … ist bereits formell rechtswidrig, da sie entgegen § 20 Abs. 1 S. 2 VwVG Baden-Württemberg keine angemessene Frist enthält. Ziffer 5 selbst enthält keine Frist. Auch wenn sie Bezug zur Frist in Ziffer 2 nehmen sollte, liegt keine angemessene Frist vor. Ziffer 2 des Bescheids ordnet an, dass der Kläger die Zugangsdaten und Sperrcodes „unverzüglich“ zur Verfügung stellen soll. Eine Aufforderung zu „unverzüglichem“ Handeln ist jedoch nicht hinreichend bestimmt genug und damit keine angemessene Frist. Denn bei einer von Verschuldenserwägungen, in der Person des Pflichtigen abhängigen Frist, vgl. § 121Abs. 1 S. 1 BGB, kann der Fristablauf weder zuverlässig noch eindeutig festgestellt werden,

> vgl. VGH Mannheim NVwZ-RR 1995, 506; OVG Weimar DÖV 2008, 881 = BeckRS 2008, 38373; OVG Greifswald NVwZ-RR 1997, 762; OVG Münster NVwZ-RR 1993, 59.

Die Unbestimmtheit wird auch nicht dadurch geheilt, dass die Vollstreckungsbehörde bis zur Festsetzung des Zwangsmittels eine längere Zeit verstreichen lässt; denn für den Pflichtigen ergibt sich die Zeitdauer dabei erst nachträglich, so dass er sein Verhalten nicht daran orientieren kann,

> vgl. VGH Mannheim NVwZ-RR 1995, 506 (508).

Auch bezieht sich die Zwangsmittelandrohung in Ziffer 5 fälschlicherweise auf Ziffer 3 des Bescheids, der die sofortige Vollziehung der Ziffer 1 und 2 anordnet. Sie ist dadurch zu unbestimmt.

Die Androhung der Ersatzvornahme in Ziffer 5 des Bescheids ist ebenfalls materiell rechtswidrig, da die ihr zugrundeliegende Anordnung in Ziffer 2 des Bescheids materiell rechtswidrig ist.

**III. Ergebnis: Vorlage an das Bundesverfassungsgericht oder den Gerichtshof der Europäischen Union**

Die §§ 48 Abs. 3, 3a, 3b AufenthG 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. Auch kommt ein Vorabentscheidungsersuchen an den EuGH in Betracht.

## C. Eilanträge

### I. Antrag auf Wiederherstellung der aufschiebenden Wirkung

#### 1. Zulässigkeit

Der Antrag zu 1. auf Wiederherstellung der aufschiebenden Wirkung der Klage gegen die Anordnungen aus Ziffer 1 und 2 des Bescheids vom … (Az. …) ist zulässig.

##### a) Statthafte Antragsart

Die statthafte Antragsart ist gem. § 80 Abs. 5 S. 1 Fall 2 VwGO der Antrag auf Wiederherstellung der aufschiebenden Wirkung, da die sofortige Vollziehung der Ziffer 1 und 2 in Ziffer 3 des Bescheids angeordnet wurde.

##### b) Antragsbefugnis

Der Antragssteller ist antragsbefugt, da er durch Ziffer 1 und 2 des Bescheids in seinem Grundrecht auf Eigentum aus Art. 14 Abs. 1 S. 1 GG bzw. in seinem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, hilfsweise in seinem Grundrecht auf informationelle Selbstbestimmung, beides aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, verletzt wird. Die Antragsbefugnis für einen Aussetzungsantrag nach § 80 Abs. 5 S. 1 folgt der Klagebefugnis für eine Anfechtungsklage. Für weitere Ausführungen verweise ich auf die Klage (s.o. A. I. 1. b))

##### c) Rechtsschutzbedürfnis

Der Antragssteller hat ein Rechtsschutzbedürfnis, insbesondere hat er die Klage zeitgleich und fristgemäß eingereicht (s.o. A. I. 1. b))

#### 2. Begründetheit

Der Eilantrag zu 1. auf Wiederherstellung der aufschiebenden Wirkung der Klage gegen die Anordnungen auf Ziffer 1 und 2 des Bescheids ist begründet.

**a) Formelle Rechtswidrigkeit der Anordnung der sofortigen Vollziehung**

**(1) Bezüglich der Überlassung der Datenträger**

Die Anordnung der sofortigen Vollziehung der Ziff. 1 des Bescheides vom … ist formell rechtswidrig, da das besondere Interesse an der sofortigen Vollziehung vor der Abnahme des Mobiltelefons durch Mitarbeitende des Regierungspräsidiums nicht gem. § 80 Abs. 3 S. 1 VwGO schriftlich begründet wurde.

Nachdem der Antragsteller den Mitwirkungsaufforderungen zur Identifizierung seines Herkunftslandes nicht nachgekommen ist, hat die Mitarbeiterin des Regierungspräsidiums ihm sein Mobiltelefon abgenommen, indem sie es eigenhändig ohne sein Wissen und gegen seinen Willen aus dem Karton geholt hat, in den es zuvor die Polizei gelegt hatte. Erst nach Einzug des Mobiltelefons hat sie ihm den Bescheid vom … übergeben, der eine schriftliche Begründung für das besondere Interesse der sofortigen Vollziehung enthielt.

Eine nachträgliche schriftliche Begründung ist aber nicht ausreichend und kann die fehlende Begründung nicht heilen,

> VGH Mannheim NJW 1977, 165; VGH München BayVBl. 1989, 117 (118); OVG Hamburg InfAuslR 1984, 72 (74); OVG Lüneburg RdL 1987, 335; Gersdorf, in: BeckOK VwGO, Posser/Wolff/Decker, 71. Edition, Stand: 01.01.2024, § 80 Rn. 91 m.w.N.

Auch war die besondere Begründung nicht nach § 80 Abs. 3 S. 2 VwGO entbehrlich, da das Regierungspräsidium keine als solche bezeichnete Notstandsmaßnahme getroffen hat.

**(2) Bezüglich der Zurverfügungstellung der Zugangsdaten**

Die Anordnung der sofortigen Vollziehung der Ziffer 2 (Zurverfügungstellung des Handycodes) ist formell rechtswidrig, da das Regierungspräsidium Karlsruhe diesbezüglich keine gesonderte Begründung für das Bestehen eines besonderen Interesses an der sofortigen Vollziehung liefert.

Sie führt im Bescheid vom … auf S. … nur Gründe an, die sich auf einen möglichen Datenverlust beziehen, wenn das Handy nicht unverzüglich eingezogen wird. Dies wird insbesondere am letzten Satz des ersten Absatzes auf S. … des Bescheids deutlich, da das Regierungspräsidium dort aufführt, dass „aus den [oben] genannten Gründen Gefahr im Verzug besteht, dass die zur Identitätsklärung notwendigen Daten verloren gehen, wenn ihr Mobiltelefon nicht unverzüglich eingezogen wird.“ Damit wird deutlich, dass sich die gesamte Begründung des Absatzes nur auf die Anordnung des Einzugs des Mobiltelefons aus Ziff. 1 des Bescheids beziehen soll. Zum besonderen Interesse bzw. der Dringlichkeit am sofortigen Vollzug der Ziffer 2 nichts angeführt.

Auch genügen die Ausführungen auf S. … des Bescheids nicht den Anforderungen an eine schriftliche Begründung i.S.d. § 80 Abs. 3 S. 1 VwGO. Das Regierungspräsidium führt dort nur im Allgemeinen an, dass ein besonderes öffentliches Interesse an der zügigen Aufenthaltsbeendigung abgelehnter Asylbewerbenden besteht und die Ausländerbehörden all diejenigen Maßnahmen zu treffen haben, die geeignet und erforderlich sind, um die Aufenthaltsbeendigung schnellstmöglich durchzuführen. Die Behörde muss aber bezogen auf die Umstände im konkreten Fall das besondere Interesse an der sofortigen Vollziehung sowie die Ermessenserwägungen, die sie zur Anordnung der sofortigen Vollziehung bewogen haben, darlegen. Formelhafte, also für beliebige Fallgestaltungen passende Wendungen, formblattmäßige oder pauschale Argumentationsmuster sowie die bloße Wiederholung des Gesetzestextes reichen nicht aus,

> VGH Mannheim VBlBW 1990, 386; NVwZ-RR 1990, 561; 1994, 625 f.; 1995, 17 (19); NVwZ 1995, 292 (293); NVwZ-RR 1995, 174 (175); NVwZ 1996, 281 (282); VGH München BayVBl. 1994, 722 f.; OVG Berlin ZUM 1993, 495 (496); Gersdorf, in: BeckOK VwGO, Posser/Wolff/Decker, 71. Edition, Stand: 01.01.2024, § 80 Rn. 87 m.w.N.

**b) Materielle Rechtswidrigkeit der Anordnung der sofortigen Vollziehung**

Die Anordnung der sofortigen Vollziehung der Ziffer 2 des Bescheides vom … ist auch materiell rechtswidrig, da kein besonderes Interesse am Sofortvollzug besteht. Im Zeitpunkt der Anordnung hat das Regierungspräsidium bereits das Mobiltelefon des Antragstellers nach § 48 Abs. 3 S. 1 AufenthG eingezogen. Damit kann es das Mobiltelefon so lange einbehalten, bis es die Daten nach § 48 Abs. 3a AufenthG ausgelesen hat,

vgl. Hruschka, in BeckOK Ausländerrecht, Kluth/Heusch, 42. Edition, Stand: 01.07.2024, § 48 Rn. 9 f..; Möller, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 7, 65.

Der Antragsteller hat keinen Zugriff mehr auf das Mobiltelefon sowie auf die Daten, die sich darauf befinden. Damit hat er auch keine Möglichkeit, die betroffenen Daten zu löschen oder auf sonstiger Weise zu entfernen, solange das Regierungspräsidium im Besitz des Mobiltelefons ist. Andere Gründe, die ein besonderes Interesse an einem Sofortvollzug begründen würden, sind nicht ersichtlich.

**c) Aussetzungsinteresse überwiegt Vollzugsinteresse**

Bezüglich des Antrags zu 1. überwiegt das Aussetzungsinteresse des Antragstellers das öffentliche Interesse an der sofortigen Vollziehung (Vollzugsinteresse), da ernstliche Zweifel an der Rechtmäßigkeit des zugrundeliegenden Verwaltungsakts aus Ziffer 1 und Ziffer 2 des Bescheids vom … bestehen. An einem rechtswidrigen Verwaltungsakt besteht kein öffentliches Interesse an der sofortigen Vollziehbarkeit, da die Behörde aufgrund Art. 20 Abs. 3 GG keine rechtswidrigen Maßnahmen ergreifen darf.

Für die Ausführungen zur Rechtswidrigkeit der Verwaltungsakte, insbesondere zur Verfassungswidrigkeit der Ermächtigungsgrundlagen in § 48 Abs. 3, 3a, 3b AufenthG verweise ich nach oben auf die Klagebegründung (B. I. 3. c))

Das Gericht ist an der Gewährung vorläufigen Rechtsschutzes auch nicht dann gehindert, wenn es die einem Verwaltungsakt zu Grunde liegende Gesetzesvorschrift für verfassungswidrig erachten würde, sofern dies im Interesse eines wirksamen Rechtsschutzes geboten ist und die Hauptsache dadurch nicht vorweggenommen wird.

BVerfGE 86, 382 (389) = NJW 1992, 2749 (2750); BVerfG-K NVwZ-RR 2014, 369 Rn. 17.

Schließlich überwiegt in jedem Fall unter Berücksichtigung der mit der Anordnung oder Wiederherstellung der aufschiebenden Wirkung einerseits und deren Ablehnung andererseits verbundenen Folgen aufgrund der Schwere und der Irreversibilität des Eingriffs in das Allgemeine Persönlichkeitsrecht des Antragstellers dessen Aussetzungsinteresse das Vollzugsinteresse, auch wenn das Gericht zum Ergebnis kommen sollte, dass die Erfolgsaussichten offen sind.

Bei der Prüfung ist der Rechtsschutzanspruch des Betroffenen umso stärker zu gewichten, je schwerer die ihm auferlegte Belastung wiegt und je mehr die Maßnahmen der Verwaltung Unabänderliches bewirken können.

> BVerfGE 35, 382 (402); 67, 42 (59); s. auch BVerfG NVwZ 2004, 93 (94); NK-VwGO/Puttler Rn. 136).

Unsicherheiten in tatsächlicher oder rechtlicher Hinsicht sind daher entsprechend der Schwere der für den Antragsteller drohenden Nachteile zu seinen Gunsten zu berücksichtigen.

> Burkholz, Der Untersuchungsgrundsatz 1988, 108 f.; NK-VwGO/Puttler Rn. 136.

Im vorliegenden Fall ist den Interessen des Antragstellers insoweit Vorrang einzuräumen. Der mit einer Aushändigung zum Zwecke der Auswertung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Antragstellers gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG wiegt besonders schwer und wäre im Falle der Rechtswidrigkeit der Anordnung irreversibel. Dem Antragsteller wird durch den Entzug seines Mobiltelefons einerseits die Teilnahme am gesellschaftlichen Leben wesentlich erschwert, welche unter den heutigen Bedingungen vielfach die Nutzung eines Mobiltelefons voraussetzt. Darüber wird ihm die persönliche Kommunikation zu nahestehenden Personen wesentlich erschwert oder, sofern diese nicht in der näheren Umgebung des Antragstellers, sondern etwa in seinem Heimatland leben, praktisch unmmöglich gemacht. Auch würde die Behörde eine Vielzahl an vertraulichen Kommunikationsinhalten, etwa mit engen Vertrauenspersonen und Beratungseinrichtungen, sowie intime Bilder und Videos einsehen können. Die Gefahr der Datenvernichtung wiegt dagegen weniger schwer,

> so auch VG Karlsruhe (19. Kammer), Beschluss vom 09.08.2023 – A 19 K 1797/23, BeckRS 2023, 20923, Rn. 27 und VG Sigmaringen (1. Kammer), Beschluss vom 07.10.2021 – VG 1 K 2165/21, BeckRS 2021, 59399, Rn. 13, bestätigt von VGH Mannheim, Beschluss vom 23.11.2022 – 12 S 3213/21, BeckRS 2022, 36497, Rn. 22.

**II. Antrag auf Herausgabe der Datenträger**

Der Antrag zu 2. auf Anordnung der Herausgabe des Mobiltelefons, der SIM-Karte und der externen Speicherkarte an den Antragsteller ist zulässig und begründet.

Gem. § 80 Abs. 5 S. 3 VwGO kann das Gericht die Aufhebung der Vollziehung anordnen, wenn der Verwaltungsakt im Zeitpunkt der Entscheidung schon vollzogen ist.

Da der Antrag zu 1. auf Wiederherstellung der aufschiebenden Wirkung der Überlassungsanordnung in Ziffer 1 des Bescheids vom … zulässig und begründet ist (s.o. B. I.) sind dem Antragsteller seine Datenträger herauszugeben.

### III. Antrag auf Anordnung der aufschiebenden Wirkung

#### 1. Zulässigkeit

Der Eilantrag zu 3. auf Anordnung der aufschiebenden Wirkung der Klage gegen die Zwangsmittelandrohung aus Ziff. 5 des Bescheids vom … ist zulässig.

#### a) Statthafte Antragsart

Die statthafte Antragsart ist gem. § 80 Abs. 5 S. 1 Fall 1 VwGO der Antrag auf Anordnung der aufschiebenden Wirkung, da die Anfechtungsklage keine aufschiebende Wirkung hat, soweit sie sich gegen Maßnahmen richtet, die in der Verwaltungsvollstreckung getroffen wird, § 12 VwVG BW.

#### b) Antragsbefugnis

Der Antragsteller ist antragsbefugt, da er durch Ziffer 5 des Bescheids jedenfalls in seiner allgemeinen Handlungsfreiheit verletzt ist. Für weitere Ausführungen verweise ich auf die Klage (B. I. 1. b))

#### c) Rechtsschutzbedürfnis

Der Antragsteller hat ein Rechtsschutzbedürfnis, insbesondere hat er die Klage zeitgleich und fristgemäß eingereicht (s.o. B. I. 1. b))

#### 2. Begründetheit

Der Antrag zu 3. auf Anordnung der aufschiebenden Wirkung der Klage gegen die Zwangsmittelandrohung aus Ziffer 5 des Bescheids vom … ist begründet. Das Aussetzungsinteresse des Antragstellers überwiegt das öffentliche Interesse an der sofortigen

Vollziehung (Vollzugsinteresse), da ernstliche Zweifel an der Rechtmäßigkeit des zugrundeliegenden Verwaltungsakts aus Ziffer 5 des Bescheids vom … bestehen. Für die Ausführungen zur Rechtswidrigkeit der Zwangsmittelandrohung, insbesondere zum Fehlen der Vollstreckungsvoraussetzungen nach § 2 VwVG BaWü und zur formellen Rechtswidrigkeit aufgrund fehlender angemessener Frist, verweise ich nach oben auf die Klagebegründung (B. I. 3. c))

**IV. Antrag auf Erlass einer prozessualen Zwischenverfügung**

Es droht die Entsperrung des Mobiltelefons im Wege der Ersatzvornahme sowie der SIM-Karte nach Auskunft durch den Telekommunikationsdiensteanbieter nach § 48a Abs. 3 S. 1 AufenthG und die anschließende Auslesung und Auswertung der sich darauf befindenden Daten bevor das Gericht im Eilverfahren entschieden hat. Dasselbe gilt für die Daten auf der externen Speicherkarte, die durch keine Zugangsbeschränkungen geschützt ist. Durch die Datenauslesung und -auswertung würde sehr tiefgreifend und irreversibel in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme des Antragsstellers eingegriffen werden. Der Erlass einer prozessualen Zwischenverfügung bzw. eines Hängebeschlusses ist daher geboten.

Mit freundlichen Grüßen

Dr. Lehnert, Rechtsanwalt

**E. Anlagenverzeichnis**

| | |
|---|---|
| Anlage 1 | Vollmacht |
| Anlage 2 | Schreiben des Verwaltungsgerichts … vom …, Az. …, Bestätigung der Rechtskraft des Urteils des Verwaltungsgerichts … vom … in der Verwaltungsrechtssache … wegen Anerkennung als Asylberechtigter, Zuerkennung der Flüchtlingseigenschaft, subsidiärer Schutz, Feststellung von Abschiebungsverboten sowie Abschiebungsandrohung seit dem … |
| Anlage 3 | Bescheid des Regierungspräsidiums Karlsruhe vom …, Az. … wegen Durchführung des Asylgesetzes (AsylG); Begleitete Vorsprache bei Vertretern Ihres Heimatlandes |
| Anlage 4 | Bescheid des Regierungspräsidiums Karlsruhe vom …, Az. … wegen Durchführung des Aufenthaltsgesetzes (AufenthG); hier: Auslesung und Auswertung von Datenträgern |