DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht

zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht (BT-Drs. 18/11546)

Stellungnahme Nr.: 39/2017 Berlin, im Mai 2017

Mitglieder des Ausschusses

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwältin Dr. Annika Dießner, Berlin
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln (Berichterstatter)
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg
- Rechtsanwältin Lea Voigt, Bremen

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Deutschland

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag – Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer
Deutscher Richterbund
Bundesverband der Freien Berufe
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Deutsches Institut für Menschenrechte

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Presse

Redaktion der Frankfurter Allgemeinen Zeitung
Redaktion der Süddeutschen Zeitung
Redaktion der Berliner Zeitung
Redaktion des Juris Newsletter
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Mit der vorliegenden Stellungnahme wird nur zu einem Teil des Entwurfs eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht (BT-Drs. 18/11546) Stellung genommen. Die Stellungnahme beschränkt sich auf die in dem Gesetzesentwurf vorgesehene Regelung zur Auswertung von Datenträgern (Art. 2 des Gesetzesentwurfs).

Zusammenfassung

Die vorgesehenen Regelungen zur Auswertung von Datenträgern (§ 15 Abs. 2 Nr. 6 AsylG-E, § 15 Abs. 4 Satz 1 AsylG-E und § 15a AsylG) begegnen tiefgreifenden verfassungsrechtlichen Bedenken. Sie sind in der vorgesehenen Form abzulehnen. Der Grundsatz der Verhältnismäßigkeit ist nicht mehr gewahrt. Die vorgesehene Mitwirkungspflicht und die Befugnis zur Auswertung von Datenträgern sind mit dem allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht mehr vereinbar. Entsprechend ist auch die vorgesehene Durchsuchungsbefugnis nicht verhältnismäßig. Es dürfte zudem an einer verfassungsrechtlich ausreichenden Regelung zum Schutz des Kernbereichs privater Lebensgestaltung fehlen. Schließlich fehlen ausreichende verfahrensrechtliche Schutzvorkehrungen, namentlich Regelungen zu Auskunftsrechten des Betroffenen, individuellem Rechtschutz sowie zur aufsichtlichen Kontrolle.

Die vorgesehene Mitwirkungspflicht des Asylbewerbers, die daran anknüpfende Durchsuchungsbefugnis und die Auswertungsbefugnis gehen zu weit. Sie erfassen nämlich sämtliche Datenträger – neben Mobiltelefonen und Smartphones z. B. Tablets, Notebooks, sonstige Computer, externe Festplatten und USB-Sticks) und vor allem sämtliche darauf enthaltene Daten des Betroffenen – von Daten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, einmal abgesehen. Dies geht im Hinblick auf die Verhältnismäßigkeit des Eingriffs zu weit. Auch in tatsächlicher Hinsicht besteht kein Bedarf an einer Speicherung und Verwendung dieses Datenumfangs zur

Feststellung von Identität und/oder Staatsangehörigkeit des Betroffenen. Es dürfen viel mehr Daten gespeichert und durchgesehen werden, als es für den verfolgten Zweck der Feststellung von Identität und/oder Staatsangehörigkeit erforderlich ist. Hierin liegt das verfassungsrechtliche Kernproblem der geplanten Neuregelungen. Zur Feststellung der Identität werden weitaus weniger Daten benötigt. Zur Feststellung der Staatsangehörigkeit werden noch weniger Daten tatsächlich benötigt.

Der Zugriff auf Datenträger zur Feststellung der Identität und/oder Staatsangehörigkeit des Betroffenen, ist nicht per se verfassungsrechtlich unzulässig. Eine verfassungskonforme Ausgestaltung ist möglich.

Der aktuelle Fall des Bundeswehr-Offiziers Franco A. ändert an dieser Bewertung nichts.

A. Vorgesehene Regelungen

Mit Artikel 2 des Gesetzesentwurfs soll für das Bundesamt für Migration und Flüchtlinge (BAMF) die Möglichkeit geschaffen werden, Datenträger zur Feststellung der Identität des Asylbewerbers zu erlangen und auszuwerten.

Vorgesehen ist nach § 15 Abs. 2 Nr. 6 AsylG-E eine neue Regelung, wonach der Asylbewerber im Falle des Nichtbesitzes eines gültigen Passes oder Passersatzes verpflichtet wird, an der Beschaffung eines Identitätspapiers mitzuwirken und auf Verlangen alle Datenträger, die für die Feststellung seiner Identität und Staatsangehörigkeit von Bedeutung sein können und in deren Besitz er ist, den für die Ausführung des Asylgesetzes zuständigen Behörden vorzulegen, auszuhändigen und zu überlassen.

Die in § 15 Abs. 4 Satz 1 AsylG bereits jetzt bestehende Durchsuchungsbefugnis soll auf Datenträger erweitert werden.

Mit § 15a AsylG-E soll eine Neuregelung zur Auswertung der so erlangten Datenträger geschaffen werden. Die Auswertung von Datenträgern soll danach nur zulässig sein, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Abs. 2 Nummer 6 erforderlich ist und der Zweck der Maßnahme nicht durch

mildere Mittel erreicht werden kann. Die vorgesehene Regelung verweist auf § 48 Abs. 3a Satz 2 bis 8 und § 48a des AufenthG, die entsprechend gelten sollen. Danach ist die Maßnahme unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass für die Auswertung von Datenträgern allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. (§ 48 Abs. 3a Satz 2 AufentG). Der Asylbewerber hat die Zugangsdaten für eine zulässige Auswertung von Datenträgern zur Verfügung zu stellen (Satz 3). Die Auswertung darf nur von Bediensteten vorgenommen werden, die die Befähigung zum Richteramt haben (Satz 4). Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch die Auswertung von Datenträgern erlangt werden, dürfen nicht verwertet werden (Satz 5). Aufzeichnungen hierüber sind unverzüglich zu löschen (Satz 6). Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen (Satz 7). Sind die durch die Auswertung der Datenträger erlangten personenbezogenen Daten für die Zwecke der Identitätsfeststellung nicht mehr erforderlich, sind sie unverzüglich zu löschen (Satz 8). Durch den Verweis auf § 48a AufenthG soll wie dort eine Befugnis geschaffen werden, die Zugangsdaten beim Anbieter von Telekommunikationsdiensten in Erfahrung zu bringen, wenn der Asylbewerber sie nicht von sich aus zur Verfügung stellt.

Zuständig für diese Maßnahmen soll das BAMF sein (§ 15a Abs. 2 AsylG-E). Ausweislich der Gesetzesbegründung soll die Auswertung dezentral und damit auch in den fast 100 Außenstellen des BAMF erfolgen.[1]

B. Stellungnahme

Der Entwurf begegnet tiefgreifenden verfassungsrechtlichen Bedenken im Hinblick auf seine Vereinbarkeit mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[2]

I. Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Die geplante Neuregelung zur Mitwirkungspflicht und die Befugnis zur Auswertung von Datenträgern greifen in das aus dem allgemeinen Persönlichkeitsrecht

[1] BT-Drs. 18/11546, S. 15.
[2] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in ihrer Stellungnahme vom 23.03.2017 (Ausschussdrucksache 18(4)831) auf diese Bedenken bereits zutreffend hingewiesen. Diesen Bedenken schließt sich der DAV vollumfänglich an.

abgeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein, das einen spezifischen Grundrechtschutz gewährt:[3]

"Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen 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."[4]

„Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können".[5]

Die vorgesehene Befugnis zum Zugriff auf Datenträger und damit auch zur Auswertung und Speicherung sämtlicher Daten des Betroffenen unterfällt zweifellos dem Schutzbereich dieses Grundrechts.

[3] S. dazu grundlegend BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 ff.
[4] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 203.
[5] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 204.

Die Befugnis zur Durchsuchung des Betroffenen mit dem Ziel des Auffindens von Datenträgern stellt einen vorgelagerten Eingriff in die allgemeine Handlungsfreiheit dar.

II. Verfassungsrechtliche Rechtfertigung - Verhältnismäßigkeit des Eingriffs

1. Die beabsichtigte Ermächtigungsgrundlage in § 15a Abs. 1 AsylG-E wahrt nicht den Grundsatz der Verhältnismäßigkeit. Dasselbe gilt für die in § 15 Abs. 2 Nr. 6 AsylG-E vorgesehene Mitwirkungspflicht und entsprechend in § 15 Abs. 4 Satz 1 AsylG-E vorgesehene Durchsuchungsbefugnis. Da alle drei beabsichtigten Regelungen inhaltlich zusammenhängen und im Kern am selben verfassungsrechtlichen Maßstab[6] zu messen sind, werden sie nachstehend gemeinsam erörtert.

Der Grundsatz der Verhältnismäßigkeit verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist.[7]

a) Zweck der Normen. Die Normen dienen der Überprüfung der Angaben eines Asylbewerbers im Hinblick auf seine Identität und Staatsangehörigkeit bzw. deren Vorbereitung. Dies sind zweifellos legitime Zwecke. Mittelbar soll auf diesem Wege sichergestellt werden, dass behördlicherseits bekannt ist, wer sich in der Bundesrepublik Deutschland aufhält und wer tatsächlich Asyl beantragt hat. Es soll umgekehrt verhindert werden, dass Asylbewerber unter falscher Identität Asylanträge stellen, sich möglicherweise mehrfach registrieren und so auch auf betrügerische Weise mehrfach Leistungen des BAMF in Anspruch nehmen.

In erster Linie geht es folglich nicht um Terrorismusbekämpfung. Zweck der geplanten Norm ist ausweislich seines Wortlauts auch „nur“ die Feststellung der Identität und Staatsangehörigkeit des Asylbewerbers, nicht hingegen das

[6] Für die Durchsuchungsbefugnis in § 15 Abs. 4 Satz 1 AsylG-E dürfte insoweit der Maßstab von Art. 2 Abs. 1 GG einschlägig sein.
[7] St. Rspr. des BVerfG, s. nur BVerfGE 109, 279, 335 ff.; 115, 320, 345; BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 218.

Sammeln von Informationen über ihn und das Überprüfen seiner über seine Identität und Staatsangehörigkeit hinausgehenden Angaben.[8]

b) Erforderlichkeit.

aa) Die Einhaltung des Grundsatzes der Erforderlichkeit könnte im Hinblick auf den verfolgten Zweck und die bestehende Einschätzungsprärogative des Gesetzgebers bei § 15a Abs. 1 AsylG-E als gewährt bewertet werden.

bb) Dies gilt hingegen nicht für die geplante Norm in § 15 Abs. 2 Nr. 6 AsylG-E. Diese enthält insoweit keine Klausel, dass der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann. Die dort beabsichtigte Mitwirkungspflicht des Asylbewerbers dahingehend, auf Verlangen alle Datenträger, die für die Feststellung seiner Identität und Staatsangehörigkeit von Bedeutung sein können, und in deren Besitz er ist, für den Fall, dass er – einerlei ob verschuldet oder unverschuldet – keinen gültigen Pass oder Passersatz besitzt, greift unabhängig davon, ob dieser Zweck durch mildere Mittel erreicht werden kann. Letztlich soll der Betroffene immer, wenn er keinen gültigen Pass oder Passersatz besitzt, auf Verlangen alle Datenträger vorlegen, aushändigen und überlassen müssen. Die Entscheidung darüber, wann der Betroffene dies zu tun hat, soll mangels besonderer Regelung letztlich jeder einfache Sachbearbeiter im BAMF treffen können. Bestimmte Vorgaben an ihn stellt das Gesetz nicht. Damit verstößt die vorgesehene Mitwirkungspflicht nach § 15 Abs. 2 Nr. 6 AsylG-E gegen den Grundsatz der Erforderlichkeit.[9] Entsprechendes gilt für die daran anknüpfende Durchsuchungsbefugnis in § 15 Abs. 4 Satz 1 AsylG-E.

cc) Empfehlung. Es wird empfohlen, durch eine Änderung des Gesetzeswortlauts sicherzustellen, dass die Mitwirkungspflicht nur dann greift, wenn die Feststellung der Identität und/oder Staatsangehörigkeit nicht durch mildere Mittel erreicht werden kann. Es sollte – auch durch entsprechende Formulierungen im Bericht und in der Beschlussempfehlung des Innenausschusses – sichergestellt werden, dass die Mitwirkungspflicht

[8] Vgl. auch BT-Drs. 18/11546, S. 23.
[9] Vgl. auch Stellungnahme der BfDI (o. Fn. 2), S. 5.

im Hinblick auf die Vorlage, Aushändigung und Überlassung von Datenträgern nur dann greift, wenn zunächst alle ansonsten üblichen Maßnahmen ausgeschöpft worden sind und weiterhin erhebliche und begründete Zweifel an den Angaben des Asylbewerbers bestehen.[10]

c) Verhältnismäßigkeit im engeren Sinne. § 15 Abs. 2 Nr. 6, der daran anknüpfende § 15 Abs. 4 Satz 1 sowie § 15a Abs. 1 AsylG-E wahren nicht das Gebot der Verhältnismäßigkeit im engeren Sinne.

aa) Dieses Gebot verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf.[11] Der Gesetzgeber hat das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann dazu führen, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange.[12]

Weder § 15 Abs. 2 Nr. 6 und § 15 Abs. 4 Satz 1 AsylG-E, noch § 15a Abs. 1 AsylG-E genügen diesen Anforderungen. Da der Grund insoweit derselbe ist, soll die Begründung im Folgenden gemeinsam erfolgen.

Die in allen drei Normen vorgesehenen Maßnahmen bewirken derart intensive Grundrechtseingriffe in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, dass sie zu dem verfolgten Zweck außer Verhältnis stehen. Zudem bedarf es strengerer verfahrensrechtlicher Vorgaben, als sie in § 15a Abs. 1 Satz 2 AsylG-E i. V. m.§ 48 Abs. 3a Satz 2 bis 8 AufenthG vorgesehen sind.

bb) Eine Mitwirkungspflicht, eine Durchsuchungsbefugnis und eine Ermächtigungsgrundlage zur Auswertung von Datenträgern zur Feststellung

[10] So bereits der Vorschlag der BfDI, (o. Fn. 2), S. 5.
[11] St. Rpr. des BVerfG, s. nur BVerfGE 90, 145, 173; 109, 279, 349 ff.; 113, 348, 382.
[12] S. nur BVerfGE 115, 320, 345 f.; BVerfG, Beschl. v. 13.06.2007 – 1 BvR 1550/03 u.a.; BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 227.

der Identität und/oder Staatsangehörigkeit des Betroffenen, ist nicht per se unverhältnismäßig. Die Unverhältnismäßigkeit im vorliegenden Fall ergibt sich vielmehr aus dem Umfang der Ermächtigungsgrundlage und der Weite der Mitwirkungspflicht und der daran anknüpfenden Durchsuchungsbefugnis. Eine verfassungskonforme Ausgestaltung aller drei Normen ist möglich.

cc) Die geplante Neuregelung wird medial und weitgehend auch in der politischen Diskussion als Befugnis zum *Zugriff auf Handys* bezeichnet und diskutiert.[13] Damit wird der Umfang der geplanten Befugnis verharmlost. Denn sie geht weit darüber hinaus.

(1) Der Begriff „Datenträger“ geht sehr weit[14] und erfasst neben Mobiltelefonen und Smartphones beispielsweise auch sämtliche Notebooks, Tablets, Festplatten und USB-Sticks. § 15a AsylG soll folglich alle denkbaren Speichermedien, mithin den gesamten digitalen Hausstand eines Asylbewerbers, erfassen. Auch die Gesetzesbegründung verweist ausdrücklich darauf, dass auch andere Datenträge, die die Betreffenden mit sich führen, relevant sein können.[15]

(2) Die Ermächtigungsgrundlage sieht nicht nur vor, dass diese durchgesehen werden. Der Begriff des „Auswertens“ erfasst neben der Durchsicht der auf den Datenträgern enthaltenen Daten deren Speicherung auf einem Datenträger des BAMF sowie deren nachträgliche Sicherung.[16] Sie erlaubt das vollständig Kopieren (sog. Spiegeln) sämtlicher Datenträger des Asylbewerbers auf Server des BAMF, damit diese Datenbestände im Nachgang ausgewertet werden können. Das Auswerten dürfte auch die

[13] S. nur „Bamf soll Identität von Asylbewerbern durch Blick ins Handy überprüfen“, http://www.sueddeutsche.de/politik/abschiebepraxis-bamf-soll-identitaet-von-asylbewerbern-durch-blick-ins-handy-ueberpruefen-1.3385870; „Handys von einreisenden Asylbewerbern sollen überprüft werden“, http://www.zeit.de/politik/deutschland/2017-02/asylpolitik-bamf-einreise-ueberpruefung-handys-fluechtlinge.
[14] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rn. 26.
[15] BT-Drs. 18/11546, S. 23.
[16] Vgl. nur zur Parallelregelung in § 48 Abs. 3a AufenthG *Weichert/Stoppa*, in: Huber, AufenthG, 2. Aufl. 2016, § 48 Rn. 20.

Sichtbarmachung und Wiederherstellung von etwaig gelöschten Daten umfassen.[17]

(3) Die vorgesehenen Neuregelungen betreffen unter den Ausländern in erster Linie Flüchtlinge. Es liegt in der Natur der Sache, dass diese alles, was ihnen wichtig ist und was sie aus ihrem Herkunftsland haben mitnehmen können, bei sich führen. Hierzu zählen insbesondere Datenträger. Diese Menschen befinden sich regelmäßig über Wochen, wenn nicht über Monate auf der Flucht bzw. auf Reisen. In dieser Zeit sind digitale Medien das wesentliche Mittel der Kommunikation mit der Außenwelt, aber auch des Festhaltens von persönlichen Eindrücken in dieser besonderen Lebensphase. Nicht selten sind Ehepartner oder Kinder alleine unterwegs. Man wird regelmäßig davon ausgehen können, dass Mobiltelefone und Smartphones das zentrale Sprachrohr zum Ehepartner, den Eltern, Verwandten und anderen nahe stehenden Personen ist. Kommuniziert wird auf allen möglichen Kanälen (insb. Telefon, SMS, WhatsApp und andere Messanger-Dienste, E-Mail). Auf den digitalen Medien und damit Datenträgern, die ein Flüchtling bei sich führt, dürften sich regelmäßig auch Fotos und Videos – möglicherweise auch intime – sowie tagebuchartige Aufzeichnungen befinden. Die beabsichtigte Norm in § 15a Abs. 1 AsylG-E soll eine Speicherung und anschließende Durchsicht sämtlicher E-Mail-, Chat-, und SMS-Verläufe, sämtlicher Fotos und Videos sowie sonstiger Aufzeichnungen des Betroffenen erlauben. Anhand von Geodaten – etwa auf Fotos – werden Bewegungsprofile erstellt werden können. Von der Speicherung und Durchsicht werden all diese z. T. sensible personenbezogene Daten erfasst.

dd) Mitwirkungspflicht, daran anknüpfende Durchsuchungsbefugnis und Auswertungsbefugnis gehen damit zu weit. Sie erfassen nämlich sämtliche Datenträger und vor allem sämtliche Daten des Betroffenen darauf – von Daten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, einmal abgesehen. Mit anderen Worten: Es dürfen viel mehr Daten gespeichert und durchgesehen werden, als dies für den verfolgten Zweck der

[17] Vgl. zur Parallelregelung in § 48 Abs. 3 AufenthG *Weichert/Stoppa*, in: Huber, AufenthG, 2. Aufl. 2016, § 48 Rn. 20.

Feststellung von Identität und/oder Staatsangehörigkeit erforderlich ist. Genau hierin liegt das verfassungsrechtliche Kernproblem der geplanten Neuregelungen. Verfassungsrechtlich kann insoweit an dieser Stelle die Frage erhoben werden, ob dies nicht schon einen Verstoß gegen den Grundsatz der Erforderlichkeit darstellt.[18] Dies kann jedoch dahinstehen, da jedenfalls ein Verstoß gegen die Verhältnismäßigkeit im engeren Sinne hierin zu sehen ist. Denn sowohl die beabsichtige Ermächtigungsgrundlage in § 15a AslG-E als auch die vorgesehene Praxis sehen eine vollständige Spiegelung der Datenträger des Betroffenen auf Server des BAMF vor. Dadurch, dass der Betroffene alle Datenträger aushändigen muss und sämtliche Datenträger vollständig gespeichert und durchgesehen werden sollen, verschafft sich das BAMF als staatliche Stelle Zugriff auf den gesamten digitalen Hausstand des Betroffenen. Dies sind viel mehr Daten, als es notwendig ist, um Identität und/oder Staatsangehörigkeit des Betroffenen festzustellen. Insoweit ist die Situation parallel gelagert mit der der Online-Durchsuchung, die das Bundesverfassungsgericht mit Urteil vom 27.02.2008 für unverhältnismäßig und verfassungswidrig erklärt hat.[19] Das Bundesverfassungsgericht hat in seinem Urteil zur *Online-Durchsuchung* im Jahr 2008 hervorgehoben, dass nach den seinerzeitigen Nutzungsgewohnheiten typischerweise informationstechnische Systeme, insbesondere Computer,

„bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt [werden]. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen.“[20]

Ein Zugriff in diesem Umfang ist zudem mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende

[18] S. dazu allgemein nur *Grzeszick*, in: Maunz/Dürig, GG, 78. EL September 2016, Rn. 113 ff. m.w.N.
[19] Vgl. dazu BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 229 ff.
[20] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 231.

Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen, ermöglichen.[21] Jedenfalls sind durch die Auswertung eines derart großen Datenbestandes, wie er sich auf einem Mobiltelefon, Smartphone oder Computer befindet, Rückschlüsse auf die Persönlichkeit des Betroffenen möglich, die potentiell ausgeforscht werden kann.

ee) Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht:[22]

„Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann. Zudem weisen solche Datenerhebungen insoweit eine beträchtliche, das Gewicht des Eingriffs erhöhende Streubreite auf, als mit den Kommunikationspartnern der Zielperson notwendigerweise Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348, 382 f.; ferner BVerfGE 34, 238, 247; 107, 299, 321“.[23]

Dies gilt insbesondere im Hinblick darauf, dass auf den betroffenen Datenträgern auch Kommunikation der Betroffenen mit Verteidigern und Rechtsanwälten vorhanden sein kann, die ebenfalls gespeichert und durchgesehen werden können soll. Dies ist für den verfolgten Zweck der Feststellung der Identität und/oder Staatsangehörigkeit nicht erforderlich. Die Kommunikation des Betroffenen mit einem Verteidiger und einem Rechtsanwalt ist – ebenso wie die mit anderen Berufsangehörigen wie Ärzten, Geistlichen, Abgeordneten – verfassungsrechtlich besonders geschützt. Dieser Schutz wird durch die geplante Neuregelung missachtet.

[21] Vgl. BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, Rn. 232.
[22] Vgl. vgl. zur Erhebung von Verbindungsdaten BVerfGE 115, 166, 187 ff.; zur Online-Durchsuchung BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 233.
[23] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 233.

Der vorgesehene Kernbereichsschutz (§ 15a Abs. 1 Satz 2 AsylG-E i. V. m. § 48 Abs. 3a Satz 2, 5, 6 und 7 AufenthG) fängt dies nicht auf, da die Kommunikation mit Verteidigern und Rechtsanwälten – ebenso wie jene mit anderen Berufsangehörigen, bei denen das Vertrauensverhältnis verfassungsrechtlich besonders geschützt ist, nicht immer, sondern eher selten dem Kernbereich privater Lebensgestaltung unterfällt.

ff) Die geplante Mitwirkungspflicht in § 15 Abs. 2 Nr. 6 AsylG-E, die Durchsuchungsbefugnis in § 15 Abs. 4 Satz 1 AsylG-E und die Ermächtigungsgrundlage in § 15a Abs. 1 AsylG-E stellen eine Fortsetzung der Idee einer Online-Durchsuchung des gesamten Datenbestands eines Betroffenen dar; nur mit dem Unterschied, dass dies offline und in Kenntnis des Betroffenen geschehen soll und somit ohne die technischen Hürden, die bei einer Online-Durchsuchung zunächst zu überwinden sind.

gg) Auch wenn die beabsichtigte Speicherung und Durchsicht – anders als bei der Online-Durchsuchung – nicht heimlich erfolgt, ist darin ein besonders schwerer Grundrechtseingriff zu sehen. Dass er nicht heimlich erfolgt, ändert an der Intensität des Eingriffs kaum etwas. Denn § 15 Abs. 2 Nr. 6 AsylG-E soll dem Asylbewerber insoweit einen Zwang auferlegen, sämtliche Datenträger (vollständig mit sämtlichen darauf gespeicherten Daten) herauszugeben; notfalls soll die Behörde im Wege einer Durchsuchung ihrer habhaft werden. Damit unterscheidet sich die Maßnahme nur unwesentlich von der einer heimlichen Überwachung qua Online-Durchsuchung, die grundsätzlich ebenfalls den gesamten Datenbestand erfassen kann.[24] Die BfDI spricht in ihrer Stellungnahme insoweit zutreffend von einem „massiven Eingriff“ in das betroffene Grundrecht.[25] Das Bundesverfassungsgericht hat in seinem Urteil zur *Online-Durchsuchung* hervorgehoben, dass der Zugriff auf einen potentiell äußerst großen und aussagekräftigen Datenbestand besonderes Gewicht hat:

[24] Vgl. auch Stellungnahme BfDI (o. Fn. 2), S. 6.
[25] Stellungnahme BfDI v. 23.03.2017, S. 6.

„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.“[26]

hh) Ein derart schwerwiegender Eingriff ist im Ergebnis nur dann verfassungsrechtlich gerechtfertigt, wenn der Schwere des Eingriffs ein entsprechend gewichtiger Zweck gegenübersteht. Dem ist vorliegend nicht so.

(1) Die Feststellung von Identität und Staatsangehörigkeit dienen keinen derart herausragenden Zwecken, dass sie einen so massiven Grundrechtseingriff rechtfertigen. Sie dienen unmittelbar weder dem Schutz von Leib, Leben oder Freiheit einer Person, noch der Abwehr von Gefahren für den Bestand des Staates und die Grundlage der Existenz von Menschen.

(2) Auch im Hinblick auf das legitime Interesse an einer Feststellung von Identität und Staatsangehörigkeit des Asylbewerbers genügt in tatsächlicher Hinsicht nur ein Bruchteil der Daten auf den Datenträgern.

(3) Die Pflicht zur Herausgabe aller Datenträger soll in § 15 Abs. 2 Nr. 6 AsylG-E wird völlig unabhängig von irgendeinem Verschulden oder einer Weigerung zur Kooperation des Betroffenen begründet werden. Auch wird nicht gefordert, dass zumindest tatsächliche Anhaltspunkte für etwaige Zweifel an den Angaben des Betroffenen vorliegen müssen. Angeknüpft wird lediglich an den objektiven Zustand des Nichtbesitzes eines Passes oder eines Passersatzes. Anders als etwa im repressiven Bereich, wo zumindest der Anfangsverdacht einer Straftat vorliegt, werden hier de jure noch nicht einmal Zweifel an den Angaben des Betroffenen verlangt. Auf diesem Wege werden alle Betroffenen gleichsam unter Generalverdacht gestellt, bewusst falsche Angaben zu machen.

[26] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 200.

(4) Damit bekommt die geplante Maßnahme gleichsam durch die Hintertür den Charakter einer Standardmaßnahme. Getreu dem Motto, „sicher ist sicher“, dürfte davon auszugehen sein, dass die Frage der Erforderlichkeit der Datenauswertung zur Feststellung von Identität und/oder Staatsangehörigkeit im Zweifel angenommen und die Datenauswertung vorgenommen wird. Dies gilt einmal mehr vor dem Hintergrund der aktuellen Geschehnisse um den Bundeswehr-Offizier *Franco A*. Es besteht damit die begründete Sorge, dass die Auswertung von Datenträgern keine Maßnahme für Einzelfälle bleibt, die als *ultima ratio* eingesetzt wird, sondern regelrecht zur Standard-Maßnahme mutiert. Das Bundesministerium des Innern hat insoweit Zahlen über den erwarteten Umfang der geplanten Maßnahme präsentiert, die – lediglich etwas zurückhaltender begrifflich verpackt – auch Eingang in die Darstellung des Erfüllungsaufwands in der Gesetzesbegründung[27] genommen haben. Danach sollen für diese Maßnahme 50-60 % der Asylbewerber aus dem Jahr 2016 in Betracht gekommen sein. Ausgehend von den Asylzahlen im Jahr 2016 wären dies ca. 150.000 Menschen.[28] Es wird mit täglich bis zu 2.400 Datenauswertungen gerechnet. Dass diese Zahlen – entgegen ihrer Bezeichnung in der Gesetzesbegründung – nicht rein theoretischer Natur sind, zeigt schon das erhebliche Investitionsvolumen in die erforderlichen IT-Systeme. Die einmaligen Kosten werden auf 3.200.000 € geschätzt. Weiter sollen jährlich 300.000 € Lizenzkosten für die forensische Software in den Folgejahren anfallen.[29]

(5) Für die Feststellung der Staatsangehörigkeit können weitaus weniger Daten genügen. Eine Speicherung und Auswertung des gesamten Datenbestands ist nicht notwendig. So kann die Durchsicht der Anruferlisten auf einem Mobiltelefon anhand der Auslandsvorwahlen schon ein wesentliches Indiz dafür liefern, aus welchem Staat ein Betroffener kommt.[30] Zwar kann daraus nicht per se auf seine Staatsangehörigkeit geschlossen werden, jedoch kann diese schlichte,

[27] BT-Drs. 18/11546, S. 15.
[28] BT-Drs. 18/11546, S. 15.
[29] BT-Drs. 18/11546, S. 16.
[30] So auch die Gesetzesbegründung, s. BT-Drs. 18/11546, S. 23.

weitaus weniger eingriffsintensive Maßnahme Indizien dazu liefern. Dasselbe gilt für etwaige bei einem Foto hinterlegten Geodaten. Was die Identität des Betroffenen anbelangt, kann es genügen, einzelne E-Mails und dort insbesondere die Absender-Adresse sowie den dort hinterlegten Namen durchzusehen. Dies könnte auch in den Einstellungen des entsprechenden E-Mail-Programms erfolgen. Daneben kann die vereinzelte Einsichtnahme in E-Mails genügen. Regelmäßig werden E-Mails mit dem eigenen Namen abgeschlossen. Dasselbe gilt in weiten Teilen für SMS und sonstige Chatverläufe. Dort findet sich der Name oft in der Anrede des Kommunikationspartners. Diese wenigen Datenbestände können ohne weiteres vor Ort bei einer Befragung des Asylbewerbers gemeinsam mit diesem durchgesehen werden. Einer Speicherung des gesamten Datenbestands auf die Server des BAMF ist dafür nicht erforderlich. Kurzum: Zur Feststellung der Identität werden weitaus weniger Daten benötigt, als die geplanten Neuregelungen den Behörden verschaffen wollen. Zur Feststellung der Staatsangehörigkeit werden noch weniger Daten tatsächlich benötigt. Obwohl nur ein Bruchteil der Daten auf den Datenträgern des Betroffenen für die Erreichung des verfolgten Zwecks tatsächlich erforderlich ist, soll sich die Auswertung – und damit auch die Speicherung – auf den gesamten Datenbestand erstrecken. Das ist unverhältnismäßig

(6) Zu berücksichtigen ist auch, dass die Auswertung der Datenträger regelmäßig allenfalls Indizien für die Feststellung der Identität und Staatsangehörigkeit werden liefern können.[31]

(7) An der Schwere des Grundrechtseingriffs ändert auch die vorgesehene Regelung in § 15a Abs. 2 AsylG-E i. V. m. § 48 Abs. 3a Satz 8 AufenthG nichts, die eine Pflicht zur unverzüglichen Löschung der personenbezogenen Daten vorsieht, sobald die Daten nicht mehr zur Feststellung von Identität und/oder Staatsangehörigkeit benötigt werden. Denn der massive Grundrechtseingriff erfolgt bereits durch die

[31] So auch Stellungnahme BfDI (o. Fn. 2), S. 5, 6.

Speicherung der Daten sowie anschließend erneut durch die Durchsicht der Daten als Verarbeitungsform.

(8) Zwar existiert eine insoweit inhaltsgleiche Regelung im selben – weiten – Umfang bereits in § 48 Abs. 3a AufenthG. Richtig ist auch, dass die Einführung dieser Befugnis seinerzeit 2015 weitgehend kritiklos erfolgte. Beides ist jedoch kein Argument dafür, dass das „Kopieren“ dieser Befugnis ins Asylrecht rechtlich unbedenklich ist. Der Bundesrat hat als einer von wenigen schon damals zutreffend Bedenken im Hinblick auf die Verhältnismäßigkeit der Norm geäußert, datenschutzrechtliche Nachjustierungen gefordert und einen Richtervorbehalt verlangt.[32] Die Bundesregierung hat diese Kritik zurückgewiesen.[33]

(9) Die vorgesehene Mitwirkungspflicht in § 15 Abs. 2 Nr. 6 AsylG-E, die daran anknüpfende Durchsuchungsbefugnis in § 15 Abs. 4 Satz 1 AsylG-E sowie die geplante Ermächtigungsgrundlage in § 15a Abs. 1 AsylG-E sind somit unverhältnismäßig und verstoßen gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

2. Kein ausreichender Kernbereichsschutz. Die geplante Ermächtigungsgrundlage enthält keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Zwar sieht § 15a Abs. 1 AsylG-E einen Kernbereichsschutz vor. Dieser genügt jedoch den verfassungsrechtlichen Anforderungen nicht.

a) Soll auf das informationstechnische System des Betroffenen zugegriffen werden, bedarf es besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen.[34] Dies gilt wegen des vergleichbaren Effekts und der Absolutheit des Schutzes von Daten, die dem Kernbereich zuzuordnen sind, unabhängig davon, ob diese heimlich erhoben werden oder nicht. Der Schutz des Kernbereichs ist sowohl der Ebene der Datenerhebung

[32] BR-Drs. 642/1/14, S. 25 ff.
[33] BT-Drs. 18/4199, S. 5 f.
[34] Vgl. BVerfG Rn. 273 ff.

als auch auf Ebene der Auswertung und Verwertung durch geeignete Maßnahmen sicherzustellen. Verfassungsrechtlich erforderlich ist primär, bereits die Erhebung von Kernbereichsdaten nach Möglichkeit zu verhindern. Erst wenn dies nicht möglich ist, ist durch geeignete Maßnahmen sicherzustellen, dass nachgelagert eine Sichtung durch eine unabhängige Stelle erfolgt, eine Löschung unverzüglich erfolgt und eine Verwertung dieser Daten ausgeschlossen wird.[35]

b) § 15a Abs. 1 Satz 2 AsylG-E i.V.m. § 48 Abs. 3a Satz 2 AufenthG sieht vor, dass die Datenauswertung (und damit auch Speicherung) nur dann unzulässig ist, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass „durch die Auswertung von Datenträgern *allein* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden“ (Hervorh. diesseits). Dies wird in praxi nie der Fall sein, weil in kaum einer denkbaren Konstellation auf einem Datenträger nur (= allein) Daten enthalten sein werden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind. Schon eine E-Mail, die lediglich der Sozialsphäre zuzuordnen wäre, lässt das Erhebungsverbot entfallen, auch wenn 99% der sonstigen Daten der Intimsphäre zuzuordnen wären. Die Regelung zur vorgelagerten Prüfung läuft damit vollständig leer und bietet im Ergebnis überhaupt keinen Schutz. Damit fehlt es an einer verfassungsrechtlich erforderlichen Regelung zur vorgelagerten Prüfung.[36]

c) Es fehlt auch an einer verfassungsrechtlich ausreichenden Regelung zur nachgelagerten Sicherstellung eines ausreichenden Kernbereichsschutzes. § 15a Abs. 1 Satz 2 AsylG-E i. V. m. § 48 Abs. 3a Satz 4 AufenthG sieht lediglich eine Durchsicht durch Bedienstete des BAMF vor, die die Befähigung zum Richteramt haben. Dies genügt nicht den Anforderungen an eine unabhängige Stelle. Die Volljuristen des BAMF stellen mangels Unabhängigkeit – sie sind der klassischen Behördenhierarchie unterworfen und weisungsabhängig – keine ausreichend unabhängige Stelle dar.[37]

[35] Vgl. nur BVerfGE 109, 279, 318; 113, 348, 391 f.; BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 Rn. 263, 270 ff.
[36] Ebenso die BfDI (o. Fn. 2), S. 7.
[37] Ebenso die BfDI (o. Fn. 2), S. 7.

3. Schließlich fehlt es an ausreichenden verfahrensrechtlichen Schutzvorkehrungen, namentlich an Regelungen zu Auskunftsrechten des Betroffenen, individuellem Rechtschutz sowie zur aufsichtsrechtlichen Kontrolle.[38]

a) Auskunftsrechte des Betroffenen sind überhaupt nicht vorgesehen. Verfassungsrechtlich ist ein solches Recht jedoch erforderlich.[39]

b) Aufgrund der erzwungenen Auswertung von Datenträgern ist eine nachgelagerte Möglichkeit, diese Maßnahme gerichtlich auf ihre Rechtmäßigkeit überprüfen zu lassen, erforderlich. Einfachgesetzlich ist eine solche Möglichkeit zur Rechtmäßigkeitsprüfung weder im AsylG noch andernorts vorgesehen.

c) Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt zunächst eine mit wirksamen Befugnissen ausgestattete Stelle – wie nach geltendem Recht die Bundesdatenschutzbeauftragte – voraus. Dazu ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten der Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält.[40] An einer solchen Protokollierungspflicht im Hinblick auf die Datenerhebung fehlt es vorliegend. Vorgesehen ist lediglich eine Regelung zur Erlangung und Löschung von Kernbereichsdaten vorgesehen.

III. Verfassungsrechtlich zulässige Ausgestaltung möglich

Der Zugriff auf Datenträger zur Feststellung der Identität und/oder Staatsangehörigkeit des Betroffenen, ist nicht per se verfassungsrechtlich unzulässig. Eine verfassungskonforme Ausgestaltung ist möglich.

[38] So auch die BfDI (o. Fn. 2), S. 8.
[39] Vgl. nur BVerfGE 65, 1, 46; BVerfG, Beschl. v. 12.04.2005 – 2 BvR 1027/02 Rn. 123.
[40] Vgl. nur BVerfGE 65, 1 , 46; 133, 277, 370; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 Rn. 141.

Sofern eine solche Regelung geschaffen werden soll, sollte sie an einen Verdacht in Form bestimmter Tatsachen anknüpfen, dass durch den Betroffenen unzutreffende Angaben zu Identität und/oder Staatsangehörigkeit gemacht werden. Sie sollte einen Zugriff nur auf Daten in dem tatsächlich erforderlichen Umfang vorsehen. Etwa in Form von Regelbeispielen könnte angeführt werden, um welche Daten es sich hierbei handelt. Dies wären primär die Landesvorwahlen in Anruferlisten und gespeicherten Rufnummern auf einem Mobiltelefon oder Smartphone. Ferner wäre dies etwa die hinterlegte E-Mail-Adresse in einem E-Mail-Programm. Die Ermächtigungsgrundlage sollte keine vollständige Speicherung aller Datenträger vorsehen, sondern nur die Befugnis zur Durchsicht des Mobiltelefons oder Smartphones des Betroffenen, bestenfalls in Anwesenheit des Betroffenen und hier auch nur in dem Umfang, in dem es erforderlich ist, um Angaben zu Identität und/oder Staatsangehörigkeit zu finden. Sofern Auffindungsergebnisse für eine weitere Verwertung, auch in einem Gerichtsverfahren, dokumentiert werden sollten, könnte eine dahingehende Befugnis vorgesehen werden.

Der Gesetzgeber wird dringend aufgerufen, den vorgelegten Gesetzesentwurf zu überarbeiten.

Der aktuelle Fall des Bundeswehr-Offiziers *Franco A*. ändert an dieser Bewertung nichts. Nach den bisherigen Erkenntnissen zu diesem Fall hätte selbst eine umfassende Befugnis, wie mit dem Gesetzesentwurf vorgesehen, nicht zur Aufdeckung der Pläne von *Franco A.* geführt. Denn, soweit ersichtlich, sind in diesem Fall schlicht keine Zweifel an der Identität und Staatsangehörigkeit erhoben worden. In diesem Fall wäre die geplante Befugnis auch in ihrer bislang vorgesehenen Form de jure nicht zur Anwendung gekommen.