

Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Vorab per FAX an 0721/9101382

Berlin, den 14.07.2018 / pst
Unser Zeichen _____
Bitte stets angeben!

Verfassungsbeschwerde

der Rechtsanwältin Halina Wawzyniak,

– Beschwerdeführerin zu 1 –,

des Journalisten Andre Meister,

– Beschwerdeführer zu 2 –,

des Journalisten Markus Beckedahl,

– Beschwerdeführer zu 3 –,

des Rechtsanwalts Sven Adam,

– Beschwerdeführer zu 4 –,

Bevollmächtigte:
dka Rechtsanwälte Fachanwälte
Rechtsanwalt Dr. Peer Stolle
Immanuelkirchstraße 3-4
10405 Berlin,

wegen: Gesetz zur Förderung des elektronischen Identitätsnachweises

Namens und gem. anliegender Vollmachten der Beschwerdeführer erhebe ich Verfassungsbeschwerde gegen § 25 Abs. 2 S. 4, 5, 7 und 9 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) sowie gegen § 22a Abs. 2 S. 5, 6, 8 und 10 des Passgesetzes, jeweils in der Fassung des Gesetzes zur Förderung des elektronischen Identitätsnachweises vom 7. Juli 2017 (BGBl. I, S. 2310), und beantrage,

1. § 25 Abs. 2 S. 4, 5, 7 und 9 des Personalausweisgesetzes und § 22a Abs. 2 S. 5, 6, 8 und 10 des Passgesetzes für mit dem Grundgesetz unvereinbar und nichtig zu erklären,

2. den Beschwerdeführern die notwendigen Auslagen zu erstatten.

Die Beschwerdeführer rügen die Verletzung ihrer Grundrechte aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 sowie Art. 19 Abs. 4 GG durch die genannten Vorschriften.

Gliederung

A. Sachverhalt und Situation der Beschwerdeführer	5
I. Sachverhalt.....	5
1. Hintergrund	5
2. Gesetzgebungsverfahren	9
a) Gesetzesbegründung	9
b) Gutachterliche Stellungnahmen	9
c) Verlauf und Inkrafttreten.....	11
3. Die gerügten Vorschriften.....	12
4. Bedeutung der Vorschriften	13
II. Beschwerdeführer	14
1. Beschwerdeführerin zu 1.....	14
2. Beschwerdeführer zu 2.....	15
3. Beschwerdeführer zu 3.....	16
4. Beschwerdeführer zu 4.....	17
B. Rechtsschutzbegehren	19
C. Zulässigkeit	20
I. Beschwerdebefugnis.....	20
1. Selbstbetroffenheit.....	20
2. Unmittelbare Betroffenheit	22
3. Gegenwärtige Betroffenheit	23
II. Subsidiarität.....	24
III. Frist.....	24
D. Begründetheit	26
I. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.....	26
1. Maßstäblicher Schutzbereich	26
2. Intensiver Grundrechtseingriff durch automatisierten Lichtbildabruf.....	26

a) Lichtbildabruf als Erhebung personenbezogener Daten	26
b) Intensität des Grundrechtseingriffs.....	27
aa) Umfang und Art der abgerufenen Daten	27
bb) Art und Weise des Datenabrufs	28
cc) Baustein staatlicher Dateninfrastruktur	29
3. Gebot der Normenbestimmtheit und Normenklarheit	30
a) Anzuwendender Maßstab	30
b) Mangelnde Bestimmtheit von Abrufzweck und Aufgabenbereichen.....	31
4. Verhältnismäßigkeit.....	36
a) Erforderlichkeit.....	36
b) Verhältnismäßigkeit im engeren Sinne.....	38
aa) Anzuwendender Maßstab	38
bb) Niedrige Eingriffsschwelle durch weiten Aufgabenkreis	41
cc) Unbeschränkter Kreis zugriffsberechtigter Personen.....	43
dd) Verschiedenartigkeit von Erhebungs- und Verwendungsbehörden	43
ee) Anlasslose und vorsorgliche Totalerhebung.....	44
ff) Fehlende Nutzungsregelungen.....	45
gg) Fehlende Subsidiarität des automatisierten Verfahrens.....	46
hh) Mangelnde Gewährleistung von Transparenz, Rechtsschutz und Kontrolle	46
II. Art. 19 Abs. 4 GG	49

A. Sachverhalt und Situation der Beschwerdeführer

Die Verfassungsbeschwerde richtet sich gegen Befugnisse zum automatisierten Abruf von Lichtbildern aus Datenbanken der Personalausweis- und Passbehörden durch eine Vielzahl von Strafverfolgungs- und Sicherheitsbehörden, insbesondere auch die Nachrichtendienste, im Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie im Passgesetz.

I. Sachverhalt

1. Hintergrund

Die Personalausweis- und Passbehörden speichern biometrische Lichtbilder von allen Ausweis- oder Passinhabern. Nach der allgemeinen Ausweis- bzw. Passpflicht gem. § 1 Abs. 1 und 2 PAuswG und § 1 Abs. 1 S. 1 PassG sind alle Deutschen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten, bzw. alle Deutschen, die aus der Bundesrepublik aus- oder einreisen, verpflichtet, einen gültigen Ausweis bzw. Pass zu besitzen. Damit erfolgt die Erhebung der biometrischen Daten flächendeckend von nahezu allen Deutschen.

Zwingender Bestandteil des Personalausweises bzw. des Passes ist gem. §§ 1 Abs. 1 S. 2, 5 Abs. 2 Nr. 5 PAuswG in Verbindung mit § 7 Abs. 3 PAuswV und deren Anhang 3 Abschnitt 2 bzw. § 4 Abs. 1 S. 2 PassG in Verbindung mit § 5 PassV und deren Anlage 8 ein biometrisches Lichtbild. Unter Biometrie ist die automatisierte Identifizierung von Personen anhand körperlicher Merkmale zu verstehen.¹ Die hierfür zu erhebenden physiologischen Charakteristika erlauben eine hochakkurate, automatisierte Erkennung und sind aufgrund der vielfältigen in ihnen enthaltenen Informationen als besonders sensibel zu bewerten – vergleichbar mit genetischen Informationen oder Gesundheitsdaten.²

Verdeutlicht wird die Sensibilität etwa durch die sich rasant entwickelnde Technik zur automatisierten Gesichtserkennung in der Videoüberwachung, die mittels intelligenter Kamerasysteme anhand biometrischer Daten zur Identifizierung und automatischen Nachverfolgung (sog. Tracking) Einzelner auch in Menschenmengen befähigt³ und anhand von Algorithmen individuelle Eigenschaften wie Alter oder Geschlecht ableitet.⁴ Die in einem biometrischen Lichtbild enthaltenen Daten bieten vielfältige weitere potentielle

¹ Ernst, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 4 DS-GVO Rn. 99.

² Vgl. zur Bewertung im Rahmen der DS-GVO dort Erwägungsgrund 51.

³ Vgl. Bayerischer Landtag, Drs. 17/20425, S. 52 ff.

⁴ Vgl. Jandt, ZRP 2018, 16.

Verwendungsmöglichkeiten mit tiefgreifendem Persönlichkeitsbezug. So dienen Gesichtsfeldmuster bereits heute der individuellen Authentifizierung (beispielsweise zur Freischaltung von Smartphones), Gesichtsanalyseverfahren erzielen hohe Trefferquoten bei der Erkennung der sexuellen Orientierung⁵ und Gesichtserkennungssoftware wird in der Medizin eingesetzt, um genetische Krankheiten zu identifizieren⁶.

Dieser umfassende Datenbestand ist jedoch nicht zentralisiert, sondern bei den einzelnen Personalausweis- und Passbehörden gespeichert (dies sind die gem. § 7 Abs. 1 PAuswG bzw. § 19 Abs. 1 PassG in Verbindung mit dem einschlägigen Landesrecht bestimmten Behörden und im Ausland zudem nach § 7 Abs. 2 PAuswG bzw. § 19 Abs. 2 PassG das Auswärtige Amt mit den von ihm bestimmten Auslandsvertretungen).

§ 24 PAuswG und § 22 PassG regeln die herkömmliche Übermittlung von Daten durch die Personalausweis- oder Passbehörden an andere Stellen. Die andere Stelle kann dazu ein Ersuchen an die Personalausweis- oder Passbehörde stellen, dass diese gem. § 24 Abs. 2 Nr. 1 bis 3 PAuswG bzw. § 22 Abs. 2 Nr. 1 bis 3 PassG erfüllen darf, wenn hierfür eine Rechtsgrundlage besteht und die Daten zur Aufgabenerfüllung erforderlich sind, wobei der Weg über die Behörde subsidiär zur Erhebung beim Betroffenen ist. Ein solches Ersuchen darf nur von bestimmten, hierzu besonders ermächtigten Bediensteten gestellt werden. Der Anlass des Ersuchens ist dort zu dokumentieren.

Nur in bestimmten Ausnahmefällen war bislang ein Abruf im automatisierten Verfahren zulässig. Nach § 25 Abs. 2 PAuswG und § 22a Abs. 2 PassG a.F. durften ausschließlich die Polizei- und Ordnungsbehörden, die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung das Lichtbild im automatisierten Verfahren abrufen. Dies setzte zudem voraus, dass dies dem Zweck der Verfolgung von Straftaten oder Verkehrsordnungswidrigkeiten dient, die Behörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Alle Abrufe waren von beiden beteiligten Seiten zu protokollieren. Ein Online-Abruf durch andere Stellen, insbesondere die Nachrichtendienste, war nicht zulässig.

⁵ Vgl. Wang/Kosinski, *Journal of Personality and Social Psychology* 2018, 246.

⁶ Vgl. Kruszka u.a., *American Journal of Medical Genetics Part A* 2017, 2323.

Die hier verfahrensgegenständlichen Normen lauten in ihrer alten Fassung wie folgt:

§ 25 Personalausweisgesetz: Datenübertragung und automatisierter Abruf von Lichtbildern

(1) In den Fällen des § 24 Abs. 2 dürfen personenbezogene Daten auch durch Datenübertragung übermittelt werden. § 12 Abs. 1 Satz 3 gilt entsprechend.

(2) Die Polizei- und Ordnungsbehörden, die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung dürfen das Lichtbild zum Zweck der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten im automatisierten Verfahren abrufen, wenn die Personalausweisbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 1 vorliegen. Alle Abrufe sind von den beteiligten Behörden so zu protokollieren, dass eine Kontrolle der Zulässigkeit der Abrufe möglich ist. Die Protokolle enthalten:

1. Familienname, Vornamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,
4. die Angabe der abrufenden und der den Abruf anordnenden Person sowie
5. das Aktenzeichen.

§ 24 Abs. 3 Satz 5 gilt entsprechend.

§ 22a Passgesetz: Datenübertragung und automatisierter Abruf von Lichtbildern

(1) In den Fällen des § 22 Abs. 2 kann die Übermittlung auch durch Datenübertragung erfolgen. § 6a Abs. 1 Satz 3 gilt entsprechend.

(2) Im Fall der Übermittlung von Lichtbildern durch Passbehörden gemäß § 19 Abs. 1 Satz 1 an die Polizei- und Ordnungsbehörden im Rahmen der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten sowie an die Steuerfahndungsstellen der Länder und an die Behörden der Zollverwaltung im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten kann der Abruf des Lichtbildes im automatisierten Verfahren erfolgen. Der Abruf ist nur zulässig, wenn die Passbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 2 vorliegen. Über alle Abrufe sind von den beteiligten Behörden Aufzeichnungen zu fertigen, die eine Kontrolle der Zulässigkeit der Abrufe ermöglichen. Die Aufzeichnungen enthalten:

1. Vor- und Familiennamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,
4. die Angabe der abrufenden und verantwortlichen Person sowie
5. das Aktenzeichen.

§ 22 Abs. 3 Satz 5 gilt entsprechend.

Die hier gegenständlichen Änderungen von § 25 Abs. 2 PAuswG bzw. § 22a Abs. 2 PassG in Form der Ermächtigung zum automatisierten Lichtbildabruf auch durch Nachrichtendienste sind eingebettet in das Gesetz zur Förderung des elektronischen Identitätsnachweises. Dieses verfolgt in erster Linie ein anderes Ziel, namentlich die Ausweitung der Nutzung der sog. eID-Funktion in Personalausweisen. Art. 1 Nr. 15 und Art. 3 Nr. 4 des Änderungsgesetzes betreffen demgegenüber an wenig prominenter Stelle Änderungen zum automatisierten Abruf von Lichtbildern aus den Datenbanken der Personalausweis- und Passbehörden.

Danach besteht die Befugnis zum automatisierten Lichtbildabruf nunmehr für alle Polizeibehörden des Bundes und der Länder, den Militärischen Abschirmdienst, den Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, die Steuerfahndungsdienststellen der Länder, den Zollfahndungsdienst und die Hauptzollämter. Insbesondere die Ermächtigung der Nachrichtendienste stellt eine grundlegende Neuorientierung im Vergleich zur vorherigen Gesetzeslage dar. Für alle Behörden – außer den Ordnungsbehörden – wird der automatisierte Abruf zudem vom Zweck der Verfolgung einer Straftat oder sonstigen konkreten Zwecken entkoppelt und lediglich an die Erfüllung der eigenen Aufgaben gebunden. Dass die Behörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet, ist künftig keine Voraussetzung mehr. An die Stelle der beidseitigen Protokollierungspflicht tritt die Protokollierung allein durch die abrufende Stelle.

Die Änderungen finden statt vor dem Hintergrund einer grundlegenden gesellschaftlichen Debatte über den staatlichen Umgang mit persönlichen Daten. Im Zuge der fortschreitenden Digitalisierung entstehen rasant zunehmende Datenbestände und gleichzeitig immer leistungsfähigere technische Möglichkeiten zu ihrer Auswertung und Verknüpfung. Das einzelne Datum existiert nicht mehr isoliert, sondern ist stets ein Datenpunkt unter vielen und damit Baustein eines Datenmosaiks, das zur Erstellung eines umfassenden Persönlichkeitsprofils der betroffenen Person herangezogen werden kann. Für den Bürger spielt sich diese Entwicklung auf zwei Ebenen ab: einerseits der Erhebung immer umfassenderer Datensätze, andererseits der für ihn unüberschaubaren Entwicklung neuer Verwertungsmöglichkeiten und der Zusammenführung bestehender Datenbestände in neuen, sie verknüpfenden Datenbanken. Insbesondere die zunehmende Erhebung, Speicherung und Verwendung biometrischer Daten (wie etwa von Fingerabdrücken und biometrischen Lichtbildern) wirkt im Zusammenspiel mit der Erweiterung von nationalen wie internationalen Zugriffsbefugnissen und Dateisystemen sowie entsprechenden Auswertungstechnologien (etwa der automatisierten Gesichtserkennung) unkontrollierbar und bedrohlich. Dies gilt umso

mehr, wo mit den Nachrichtendiensten Behörden der Zugriff gewährt wird, die aufgrund ihrer Aufgaben und der spezifischen Art der Aufgabenwahrnehmung nur geringe Transparenz und subjektiven Rechtsschutz gewährleisten können.

2. Gesetzgebungsverfahren

a) Gesetzesbegründung

Der Gesetzgeber hat die Einführung der Befugnisse zum automatisierten Lichtbildabruf im Wesentlichen mit eilbedürftigen Situationen und Geheimschutzinteressen begründet.⁷ So sei die Ermittlung der zuständigen Personalausweis- oder Passbehörde mitunter zeitaufwändig. In zeitkritischen Situationen, in denen beispielsweise eine konkrete Tat unmittelbar bevorstehe und das Lichtbild zur einwandfreien Identifizierung erforderlich sei, scheidet ein manuelles Ersuchen aus. Gleiches gelte, wenn die zuständige Behörde geschlossen habe oder das Lichtbild auf herkömmlichem Wege nicht zum erforderlichen Zeitpunkt verfügbar sei. Dies komme bei Maßnahmen am Wochenende oder an Feiertagen in Betracht. Zudem berge ein manuelles Ersuchen das Risiko der Enttarnung von Vertrauenspersonen oder der Vereitelung von Maßnahmen. Kenne ein Mitarbeiter der ersuchten Behörde die abgefragte Person, bestehe die Gefahr der Mitteilung des Ersuchens an Dritte.

Die bisherige Regelung, wonach ein automatisierter Abruf nur zulässig war, wenn die zuständige Behörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde, sei nicht ausreichend, da die Überprüfung von Personen durch die Sicherheitsbehörden zumeist zeitkritisch und aus Gründen der Gefahrenabwehr rund um die Uhr an allen Tagen der Woche erforderlich sei. Die Zeit für eine herkömmliche Abfrage zu den üblichen Geschäftszeiten der Pass- und Ausweisbehörden stehe grundsätzlich nicht zur Verfügung. Für alle beteiligten Behörden bringe das automatisierte Verfahren eine Reduzierung des Verwaltungsaufwands mit sich, es handle sich zugleich um die schnellere Form der Kommunikation. Dem Datenschutz werde durch eine automatisierte Protokollierung seitens der abfragenden Behörde Rechnung getragen.

b) Gutachterliche Stellungnahmen

Die am 24. April 2017 im Innenausschuss des Deutschen Bundestages angehörten Sachverständigen haben in ihren Stellungnahmen zu unterschiedlichen Aspekten des Gesetzes zur Förderung des elektronischen Identitätsnachweises Position bezogen. Soweit die Stellungnahmen die hier gegenständlichen Ermächtigungen zum automatisierten

⁷ BR-Drs. 787/16, S. 32 f.; BT-Drs. 18/11279, S. 32; 18/12417, S. 8 f.

Lichtbildabruf betrafen, haben alle Sachverständigen die Vorschriften in der gegenwärtigen Ausgestaltung abgelehnt.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit lehnte die Befugnisse des automatisierten Lichtbildabrufs – da nahezu voraussetzungslos – in der Form des § 25 Abs. 2 PAuswG und § 22a Abs. 2 PassG aus datenschutzrechtlicher Sicht ab.⁸ Die bisherige Rechtslage sei völlig ausreichend. Sie regte an, den automatisierten Zugriff auf die Polizei- und Ordnungsbehörden, die Steuerfahndungsstellen der Länder sowie die Behörden der Zollverwaltung und auf den Zweck der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten zu beschränken. Als Voraussetzung sei beizubehalten, dass die Personalausweis- bzw. Passbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Die Abrufe sollten von beiden beteiligten Stellen protokolliert werden.

Prof. Dr. Bernd Holznagel (LL.M.) und Dr. Marius Stracke vom Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster hielten den automatisierten Abruf durch die genannten Behörden in Fällen der Eilbedürftigkeit oder einer bestehenden Gefahr für den Untersuchungszweck für erforderlich.⁹ Sie kritisierten jedoch den Anknüpfungspunkt der Aufgabenerfüllung als zu weit. Das automatisierte Verfahren werde so zum Standardverfahren erhoben. Angesichts der heute sehr weit vorangeschrittenen Vernetzung der Behörden untereinander werde damit funktional eine bundesweite Datenbank für biometrische Merkmale errichtet, was das Verbot der Errichtung solcher Datenbanken in seinem Sinngehalt unterlaufe. Die Subsidiarität des automatisierten Abrufs gegenüber dem herkömmlichen Ersuchen sollte deshalb für alle Stellen beibehalten und an die besondere Interessenlage der Nachrichtendienste und Sicherheitsbehörden durch Normierung bestimmter Ausnahmen (etwa bei der Gefahr der Enttarnung) angepasst werden. Solche Subsidiaritätsklauseln seien beispielsweise aus § 10 Abs. 7 BKAG a.F.¹⁰ bekannt. Die automatisierte Abfrage sei daran zu knüpfen, dass gerade diese Form der Datenermittlung erforderlich sei. Weiter sei durch Rechtsverordnung oder Verwaltungsvorschrift ein in der jeweiligen Behörde zur Abfrage berechtigter Personenkreis zu definieren, für den im Gesetz aber Leitlinien vorzugeben seien. In der mündlichen Anhörung am 24. April 2017 hat der Sachverständige Prof. Dr. Holznagel darüber hinaus verfassungsrechtliche Bedenken

⁸ Die Beauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 24. April 2017 zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises, Ausschuss-Drs. 18(4)868 A, S. 12 f., 15 f.

⁹ Holznagel/Stracke, Stellungnahme zur öffentlichen Anhörung zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises, Ausschuss-Drs. 18(4)868 C, S. 4 ff.

¹⁰ Vgl. § 25 Abs. 7 S. 1 BKAG n.F.

hinsichtlich des Bestimmtheitsgebots und des Rechts auf informationelle Selbstbestimmung geltend gemacht und auf die innere Widersprüchlichkeit des Gesetzes bezüglich des Verbots bundesweiter biometrischer Datenbanken hingewiesen.¹¹

Dr. Constanze Kurz hat für den Chaos Computer Club die Ermächtigungen zum automatisierten Lichtbildabruf als Schritt in die umfassende Überwachung kritisiert.¹² Der Datenzugriff weite die Nutzung in kaum überschaubarem Maße aus und habe zu unterbleiben, mindestens aber müsse jede dauerhafte Speicherung und Weitergabe der so erlangten Daten untersagt werden. Der automatisierte Zugriff müsse im Kontext des Ausbaus der Videoüberwachung öffentlicher Räume und der automatischen Gesichtserkennung gesehen werden. Die einfache Abfrage großer Mengen an Gesichtsbildern erlaube den Aufbau von Systemen, die durch Eingabe eines Namens das zugehörige Passbild und umgekehrt als Inverssuche durch Einspeisung eines Bildes die zugehörigen persönlichen Daten lieferten. Hinzu komme der weitgehend unkontrollierte Datenaustausch der Geheimdienste mit ausländischen Partnerdiensten. In der mündlichen Anhörung am 24. April 2017 hat die Sachverständige Dr. Kurz zudem eine Aushöhlung des Verbots zentraler biometrischer Datenbanken gem. § 26 Abs. 4 PAuswG moniert und für automatisierte Abfragen eine beidseitige Protokollierungspflicht gefordert.¹³

c) Verlauf und Inkrafttreten

Der ursprüngliche Gesetzentwurf war am 30. Dezember 2016 von der Bundesregierung in den Bundesrat eingebracht worden. Hierzu empfahl der federführende Ausschuss für Innere Angelegenheiten am 31. Januar 2017, u.a. die Abrufbefugnis auf die zunächst nicht einbezogenen Steuerfahndungsdienststellen der Länder, den Zollfahndungsdienst und die Hauptzollämter auszuweiten und die Pflicht zur Protokollierung des Abrufs auf die abrufende Behörde zu beschränken. Darüber hinaus empfahl der Ausschuss, das im ursprünglichen Gesetzentwurf vorgesehene Inkrafttreten der Abrufvorschriften zum 1. Mai 2021 durch das sofortige Inkrafttreten am Tag nach der Verkündung zu ersetzen. Dies wurde damit begründet, dass eine Vielzahl von Personalausweis- und Passbehörden schon heute in der Lage sei, den örtlich zuständigen Polizeibehörden den automatisierten Abruf zu ermöglichen. Diese Empfehlungen machte sich der Bundesrat zu eigen. Die Bundesregierung schloss sich dem in ihrer Gegenäußerung an. Nach der öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages empfahl der Ausschuss die Annahme in dieser Fassung ohne weitere Änderungen.

¹¹ Deutscher Bundestag – Innenausschuss, Prot.-Nr. 18/113, S. 25.

¹² Kurz/Krissler/Neumann/Rieger, Stellungnahme eID, Ausschuss-Drs. 18(4)868 D, S. 8 f.

¹³ Deutscher Bundestag – Innenausschuss, Prot.-Nr. 18/113, S. 24.

Die Änderungen sind als Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 7. Juli 2017 mit Zustimmung des Bundesrats beschlossen und am 14. Juli 2017 (Bundesgesetzblatt 2017 Teil I Nr. 46, S. 2310 ff.) verkündet worden. Die Regelungen sind gem. Art. 6 Abs. 1 des Gesetzes am 15. Juli 2017 in Kraft getreten.

3. Die gerügten Vorschriften

Die gerügten Vorschriften lauten in der vollständigen Wiedergabe folgendermaßen:

§ 25 Personalausweisgesetz: Datenübertragung und automatisierter Abruf von Lichtbildern

(1) In den Fällen des § 24 Abs. 2 dürfen personenbezogene Daten auch durch Datenübertragung übermittelt werden. § 12 Abs. 1 Satz 3 gilt entsprechend.

*(2) Die Ordnungsbehörden dürfen das Lichtbild zum Zweck der Verfolgung von Verkehrsordnungswidrigkeiten im automatisierten Verfahren abrufen, wenn die Personalausweisbehörde auf andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 1 vorliegen. **Die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter dürfen das Lichtbild zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Absatzes 1 vorliegen.** Alle Abrufe sind von den beteiligten Behörden so zu protokollieren, dass eine Kontrolle der Zulässigkeit der Abrufe möglich ist. **Abrufe nach Satz 4 werden nur von der abrufenden Behörde protokolliert.** Die Protokolle enthalten:*

- 1. Familienname, Vornamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,*
- 2. Tag und Uhrzeit des Abrufs,*
- 3. die Bezeichnung der am Abruf beteiligten Stellen,*
- 4. die Angabe der abrufenden und der den Abruf anordnenden Person sowie*
- 5. das Aktenzeichen.*

§ 24 Abs. 3 Satz 5 gilt entsprechend.

§ 22a Passgesetz: Datenübertragung und automatisierter Abruf von Lichtbildern

(1) In den Fällen des § 22 Abs. 2 kann die Übermittlung auch durch Datenübertragung erfolgen. § 6a Abs. 1 Satz 3 gilt entsprechend.

(2) Im Fall der Übermittlung von Lichtbildern durch Passbehörden nach § 19 Absatz 1 Satz 1 an die Ordnungsbehörden im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten kann der Abruf des Lichtbildes im automatisierten Verfahren erfolgen. Der Abruf ist nur zulässig, wenn die Passbehörde nicht erreichbar ist und ein weiteres

Abwarten den Ermittlungszweck gefährden würde. Zuständig für den Abruf sind die Polizeivollzugsbehörden auf Ebene der Landkreise und kreisfreien Städte, die durch Landesrecht bestimmt werden. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen der Absätze 1 und 2 Satz 2 vorliegen. **Die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter dürfen das Lichtbild zur Erfüllung ihrer Aufgaben im automatisierten Verfahren abrufen. Die abrufende Behörde trägt die Verantwortung dafür, dass die Voraussetzungen des Absatzes 1 vorliegen. Über alle Abrufe sind von den beteiligten Behörden Aufzeichnungen zu fertigen, die eine Kontrolle der Zulässigkeit der Abrufe ermöglichen. Abrufe nach Satz 5 werden nur von der abrufenden Behörde protokolliert. Die Aufzeichnungen enthalten:**

1. Vor- und Familiennamen sowie Tag und Ort der Geburt der Person, deren Lichtbild abgerufen wurde,
2. Tag und Uhrzeit des Abrufs,
3. die Bezeichnung der am Abruf beteiligten Stellen,
4. die Angabe der abrufenden und verantwortlichen Person sowie
5. das Aktenzeichen.

§ 22 Abs. 3 Satz 5 gilt entsprechend.

4. Bedeutung der Vorschriften

Es wird vorliegend davon ausgegangen, dass § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG im Bild des Doppeltürenmodells¹⁴ den Personalausweis- und Passbehörden die Tür der Übermittlung öffnen, ohne eine selbstständige Rechtsgrundlage für die abrufenden Behörden zu liefern. Zur Regelung einer solchen Rechtsgrundlage fehlt dem Bund jedenfalls für die Verfassungsschutz- und Polizeibehörden der Länder schon die Gesetzgebungskompetenz; sie ergeben sich vielmehr aus dem jeweils geltenden Fachrecht. Das verfassungsrechtliche Vorgehen gegen die Vorschriften ist jedoch hiervon weitgehend unabhängig zu ermöglichen. Zum einen regeln die neu eingeführten Normen ihrerseits den Zweck, das Verfahren und die möglichen Adressaten der durch sie konstituierten Übermittlungspflicht und stellen insofern eigenständige Grundrechtseingriffe dar. Der Gesetzgeber geht dabei erkennbar davon aus, dass sich im Verhältnis zur bisherigen Möglichkeit, die zuständige Personalausweis- oder Passbehörde um Übermittlung zu ersuchen, keine weiteren qualifizierenden Hürden auf Seiten der abrufenden Behörden ergeben.

Zum anderen würde es den verfassungsrechtlichen Rechtsschutz unzumutbar erschweren, wenn die einzelnen Elemente des datenschutzrechtlichen Doppeltürenmodells nicht losgelöst

¹⁴ Vgl. BVerfGE 131, 151 (184).

von ihren Entsprechungen im Fachrecht in ihrer Verfassungskonformität gerügt werden könnten. Die ursprünglich den Schutz der Daten der Betroffenen gewährleistende Konzeption der doppelten Türe würde gleichsam zur Drehtür, die den Beschwerdeführern das Durchstoßen zum Kern des von ihnen gerügten Eingriffshandelns verwehrt.

II. Beschwerdeführer

1. Beschwerdeführerin zu 1

Die Beschwerdeführerin zu 1 ist Rechtsanwältin, Aktivistin und ehemalige Politikerin der Partei Die Linke. Sie ist deutsche Staatsangehörige und Inhaberin eines deutschen Personalausweises und Reisepasses. Von 1990 bis 2006 war sie Mitglied der PDS bzw. Linkspartei.PDS und hatte dort diverse Ämter inne, darunter als Mitglied im Parteivorstand und stellvertretende Landesvorsitzende für Berlin. Für die Partei Die Linke war sie hernach unter anderem als Mitglied im Bundesvorstand, stellvertretende Bundesvorsitzende und Vorsitzende des Bezirksverbandes Friedrichshain-Kreuzberg in Berlin tätig. Von 2009 bis 2017 war sie Abgeordnete im Deutschen Bundestag.

Schwerpunkte ihrer Arbeit sind Themen der sozialen Gerechtigkeit und der Umverteilung materiellen Wohlstandes, der Globalisierung und Klimapolitik, der Demokratisierung und Reform von Recht und Parlamentarismus, der Opposition zu Krieg und Rüstungsexporten, des Abbaus der Kompetenzen der Geheimdienste (so etwa mit dem Entwurf eines Gesetzes zur Aufhebung des Artikel 10-Gesetzes) und der Begegnung rechtspopulistischer Tendenzen. Durch auf eine datenschutzrechtliche Eingabe erfolgten Bescheid des Bundesamtes für Verfassungsschutz vom 31. Juli 2012 wurde bekannt, dass die Beschwerdeführerin zu 1 vom Bundesamt für Verfassungsschutz beobachtet wird, ohne dass das Ende der Beobachtung bzw. das Unterlassen der Wiederaufnahme feststünde.

Die Verfassungsschutzbehörden stufen bis heute Teile der Partei Die Linke als „extremistisch“ ein. Zu den nachrichtendienstlich beobachteten Parteiteilen gehören alleine dem Jahresbericht des Bundesamtes für Verfassungsschutz für 2016 zufolge die parteiinternen Zusammenschlüsse „Kommunistische Plattform“, „Sozialistische Linke“, „Arbeitsgemeinschaft Cuba Si“, „Antikapitalistische Linke“, „Marxistisches Forum“, „Geraer Dialog“ und das Netzwerk „marx21“ mit insgesamt mehreren Tausend Personen.¹⁵ Wiederholt ist in der Vergangenheit die Beobachtung größerer Zahlen individueller Parteimitglieder durch Verfassungsschutzbehörden öffentlich geworden, so etwa 2012 und 2013 für 27 bzw. 25 und

¹⁵ Bundesministerium des Innern, Verfassungsschutzbericht 2016, S. 144 ff.

damit fast die Hälfte der Bundestagsabgeordneten. Auch in verschiedenen Bundesländern ist die Beobachtung durch Landesverfassungsschutzbehörden bekannt.¹⁶

Die gegenwärtige Aktivität der Beschwerdeführerin umfasst regelmäßige Zusammentreffen und Diskussionen mit Parteimitgliedern und anderen Personen aus dem politischen Umfeld der Partei sowie die Teilnahme an Veranstaltungen und Versammlungen wie etwa Parteitagen. Im Rahmen ihrer politischen Tätigkeit ist sie weiterhin Mitglied der Partei Die Linke, pflegt dort nach wie vor vielfältige Kontakte und publiziert in Zeitungsbeiträgen und Blogbeiträgen zu politischen Themen.

2. Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 ist Journalist und Bürgerrechtsaktivist, deutscher Staatsangehöriger und Inhaber eines deutschen Personalausweises und Reisepasses. Er ist langjähriger Redakteur des mit zahlreichen Preisen ausgezeichneten Blogs netzpolitik.org, Mitgründer der Vereine Digitale Gesellschaft e. V. und Gesellschaft für Freiheitsrechte e.V. und Mitglied im Chaos Computer Club. Er ist zudem als Beobachter bei European Digital Rights tätig, einer internationalen Vereinigung von Bürgerrechtsorganisationen. Er beschäftigt sich schwerpunktmäßig mit digitaler Sicherheit und staatlicher Überwachung, Datenschutz sowie Informations- und Pressefreiheit.

Hierbei kommt es häufig zu Umgang mit und Publikation von Dokumenten, die durch sog. Whistleblower oder andere Quellen zugänglich gemacht wurden und die Tätigkeit deutscher oder ausländischer Sicherheitsbehörden und Nachrichtendienste betreffen. So hat der Beschwerdeführer zu 2 für den Blog netzpolitik.org unter anderem im September 2017 interne Kommunikation des Bundesnachrichtendienstes zur Entwicklung von Online-Überwachungstechnologie und diesbezüglicher Kooperation mit der US-amerikanischen National Security Agency ausgewertet und öffentlich gemacht, im Juli 2017 einen eingestuften Bericht des Innenministeriums zum Stand der Quellen-TKÜ-Software des Bundeskriminalamts, im Juni 2017 das zu diesem Zeitpunkt nicht freigegebene Sondervotum der Opposition im Abschlussbericht des Ersten parlamentarischen Untersuchungsausschusses des 18. Bundestages (NSA-Untersuchungsausschuss), im Februar 2017 geheime Dokumente des Bundesnachrichtendienstes zur Erweiterung der satellitengestützten Überwachung und im Mai 2015 ursprünglich teils vertrauliche

¹⁶ Vgl. beispielsweise Bayerisches Staatsministerium des Innern und für Integration, Verfassungsschutzbericht 2017, S. 216 ff.; Ministerium für Inneres, Digitalisierung und Migration des Landes Baden-Württemberg, Verfassungsschutzbericht 2017, S. 223 ff.; Ministerium des Innern des Landes Nordrhein-Westfalen, Verfassungsschutzbericht des Landes Nordrhein-Westfalen, S. 130 ff.

Kommunikation des Militärischen Abschirmdienstes zum Umgang mit kritischer medialer Berichterstattung.

Als Teil seiner journalistischen Arbeit pflegt der Beschwerdeführer zu 2 auch Kontakte zu anderen in diesem Bereich tätigen Journalisten und potentiellen Quellen. Er gerät dabei häufig mit Personen in Kontakt, die entweder selbst als Journalisten mit sicherheitsrelevanten Informationen oder geheimen Dokumenten umgehen oder als potentielle Quellen Zugang zu solchen Informationen und Dokumenten haben. Dies beinhaltet auch Treffen mit diesen Personen. In diesem Zusammenhang finden auch Treffen mit ausländischen Staatsangehörigen im Ausland statt.

Bei einer Sitzung des NSA-Untersuchungsausschusses im Oktober 2014 ist der Beschwerdeführer zu 2, der als Zuschauer anwesend war, von der Bundestagspolizei überwacht worden. Im Rahmen der Veröffentlichung von Ausschnitten aus als vertraulich eingestuften Berichten des Bundesamtes für Verfassungsschutz auf netzpolitik.org und auf eine Anzeige des Präsidenten des Bundesamtes für Verfassungsschutz hin führte der Generalbundesanwalt im Jahr 2015 ein Ermittlungsverfahren wegen des Verdachts auf Landesverrat unter anderem gegen den Beschwerdeführer zu 2. Soweit ersichtlich, ist die mögliche Quelle der im dortigen Verfahren gegenständlichen Informationen nach wie vor nicht bekannt.

3. Beschwerdeführer zu 3

Der Beschwerdeführer zu 3 ist deutscher Journalist und netzpolitischer Aktivist. Er ist Inhaber eines deutschen Personalausweises und Reisepasses. Seit 2002 ist er Chefredakteur des von ihm begründeten Blogs netzpolitik.org; zudem ist er Mitglied des Medienrats der Medienanstalt Berlin-Brandenburg und des Vereins Digitale Gesellschaft e.V. Er hat außerdem die jährliche Konferenz re:publica mitbegründet und organisiert sie bis heute. Die Konferenz bietet auch zahlreichen Dissidenten aus dem Ausland, zuletzt u.a. aus dem Iran, dem Libanon, Pakistan oder den Vereinigten Staaten, eine Bühne. Die diesbezüglichen Organisationstätigkeiten umfassen dabei auch Treffen im Ausland.

Seine Arbeit konzentriert sich inhaltlich auf die Themen Datenschutz, Pressefreiheit, Digitalisierung, Automatisierung und Künstliche Intelligenz. Auf dem sich kritisch mit staatlicher Überwachung, Sicherheitspolitik und Geheimdiensten auseinandersetzenden Blog netzpolitik.org werden regelmäßig Dokumente veröffentlicht, die durch sog. Whistleblower oder andere Quellen zugänglich gemacht wurden und die Tätigkeit deutscher oder ausländischer Sicherheitsbehörden und Nachrichtendienste betreffen. Im Rahmen seiner

diesbezüglichen Tätigkeit kommt der Beschwerdeführer zu 3 mit anderen Journalisten und Aktivisten in Kontakt, die zu sicherheitsrelevanten Themen recherchieren und hierzu mit als geheim eingestuften Dokumenten und den entsprechenden Quellen umgehen. Insbesondere die für das Blog netzpolitik.org angestellten oder publizierenden Journalisten berichten ihm als Chefredakteur regelmäßig über Erkenntnisse und Recherchen. Darüber hinaus knüpft er auch selbst Kontakte zu potentiellen Quellen, von denen er aufgrund seiner Wahrnehmung in der Öffentlichkeit häufig kontaktiert wird. Da es sich bei diesen Kontakten teilweise um ausländische Staatsangehörige handelt, finden die Treffen gegebenenfalls im Ausland statt. Nach der auf netzpolitik.org erfolgten Veröffentlichung von Ausschnitten aus als vertraulich eingestuften Berichten des Bundesamtes für Verfassungsschutz und auf eine Anzeige des Präsidenten des Bundesamtes für Verfassungsschutz hin führte der Generalbundesanwalt im Jahr 2015 ein Ermittlungsverfahren wegen des Verdachts auf Landesverrat unter anderem gegen den Beschwerdeführer zu 3. Soweit ersichtlich, ist die mögliche Quelle der im dortigen Verfahren gegenständlichen Informationen nach wie vor nicht bekannt.

4. Beschwerdeführer zu 4

Der Beschwerdeführer zu 4 ist überregional tätiger Rechtsanwalt in Göttingen und insbesondere auf den Gebieten des Strafrechts, des Sozialrechts, des Polizei- und Ordnungsrechts sowie des Versammlungsrechts tätig. Er ist deutscher Staatsangehöriger und Inhaber eines deutschen Personalausweises sowie Reisepasses.

Im Rahmen seiner anwaltlichen Tätigkeit berät er unter anderem Mandanten, die von den Strafverfolgungs- und Sicherheitsbehörden der „linksextremen“ Szene zugerechnet oder durch den polizeilichen Staatsschutz oder Verfassungsschutzbehörden in entsprechenden Dateien geführt werden. Dabei kommt er mit einer Vielzahl von Personen in Kontakt, die selbst als „linksextremistisch“ eingestuft werden oder von den Behörden in Zusammenhang mit als „linksextremistisch“ eingestuften Organisationen, Versammlungen oder Personen gebracht worden sind. Hier besteht entweder Kenntnis oder eine hohe Wahrscheinlichkeit einer Beobachtung oder Überwachung durch Verfassungsschutzbehörden.

Er vertritt derzeit einen Mandanten im Zusammenhang mit dem Verbot der Internetplattform „linksunten.indymedia.org“. Das Verbot basierte auch auf Erkenntnissen der Verfassungsschutzbehörden und wurde unter anderem damit begründet, die Plattform richte sich gegen die verfassungsmäßige Ordnung. Das Bundesamt für Verfassungsschutz und mehrere Landesverfassungsschutzbehörden beobachten das deutsche Indymedia-Netzwerk und insbesondere „linksunten.indymedia.org“ und das zugehörige Umfeld bereits seit Jahrzehnten, stufen sie als „linksextremistisch“ ein und messen ihnen eine große Bedeutung

für die linke Szene bei.¹⁷ Des Weiteren betrifft die versammlungsrechtliche Arbeit des Beschwerdeführers zu 4 häufig kurdische Aktivisten im Zusammenhang mit politischen Demonstrationen, die er teilweise auch begleitet. Diesen werden von den Sicherheits- und Strafverfolgungsbehörden regelmäßig Verbindungen zur Arbeiterpartei Kurdistans (PKK) vorgeworfen, weshalb eine Überprüfung, Beobachtung oder Überwachung durch Verfassungsschutzbehörden nahe liegt. Nicht zuletzt, weil der Beschwerdeführer zu 4 überregional anwaltlich tätig ist, sind seine anwaltlichen Kontakte mit diesen Personen örtlich nicht beschränkt.

Für den Beschwerdeführer zu 4 ist durch entsprechende Bescheide im Rahmen eines Auskunftersuchens bekannt geworden, dass über ihn selbst zwischen 2009 und 2013 im Zusammenhang mit seiner anwaltlichen Tätigkeit zu Protesten gegen rechte Demonstrationen Informationen durch den Polizeilichen Staatsschutz der Polizeiinspektion Göttingen gesammelt und an die niedersächsische Verfassungsschutzbehörde weitergeleitet und dort gespeichert wurden. Die behördliche Auskunft über den genauen Umfang der gespeicherten Daten ist unter Hinweis auf Sperrvermerke verweigert worden. Diese Daten sind mittlerweile gelöscht worden und nicht mehr nachvollziehbar.

¹⁷ Vgl. Bundesministerium des Innern, Verfassungsschutzbericht 2016, S. 115 ff.

B. Rechtsschutzbegehren

Die Beschwerdeführer wenden sich gegen die Vorschriften zum automatisierten Abruf von Lichtbildern aus Datenbanken der Personalausweis- und Passbehörden des § 25 Abs. 2 S. 4, 5, 7 und 9 des Personalausweisgesetzes und § 22a Abs. 2 S. 5, 6, 8 und 10 des Passgesetzes. Die Beschwerdeführer rügen die Verletzung ihres Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie der Garantie effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG durch die angegriffenen Vorschriften.

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig. Die Beschwerdeführer sind beschwerdebefugt, der Grundsatz der Subsidiarität ist gewahrt und die Beschwerdefrist wird eingehalten.

I. Beschwerdebefugnis

Die Beschwerdeführer sind hinsichtlich der angegriffenen Regelungen beschwerdebefugt. Sie sind durch diese Regelungen mit einiger Wahrscheinlichkeit selbst, unmittelbar und gegenwärtig in ihren Grundrechten betroffen. Dabei ist zu berücksichtigen, dass die Anforderungen an die Darlegung der Wahrscheinlichkeit eigener Betroffenheit an die tatsächlichen, bei heimlichen Eingriffsmaßnahmen regelmäßig reduzierten Möglichkeiten einer solchen Darlegung anzupassen sind.¹⁸

1. Selbstbetroffenheit

Die in § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG geregelten Befugnisse zum automatisierten Abruf von Lichtbildern durch die dort genannten Stellen verletzen die Beschwerdeführer in eigenen Grundrechten. Die Beschwerdeführer sind nicht Adressaten der Vorschriften. Es handelt sich aber um Befugnisse, die Eingriffe bei Vorliegen der Voraussetzungen grundsätzlich gegen jedermann erlauben. Es ist aufgrund der dargelegten Tätigkeiten mit einiger Wahrscheinlichkeit anzunehmen, dass die Beschwerdeführer von den Abrufermächtigungen betroffen sind.

Die angegriffenen Ermächtigungen erlauben den Polizeibehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, den Verfassungsschutzbehörden des Bundes und der Länder, den Steuerfahndungsdienststellen der Länder, dem Zollfahndungsdienst und den Hauptzollämtern den automatisierten Lichtbildabruf zur Erfüllung ihrer Aufgaben. Der Bildabruf ist ein Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen. Weitere materielle Voraussetzungen für den Abruf bestehen nicht; insbesondere ist keine spezifischere Eingriffsschwelle vorgesehen. Der Abruf im automatisierten Verfahren ist damit bei Beachtung der formellen Voraussetzungen zulässig, sobald eine der genannten Stellen das Lichtbild einer Person als zur Erfüllung ihrer Aufgaben erforderlich erachtet. Dies kann – nicht zuletzt aufgrund der Vielfältigkeit der in Bezug genommenen Aufgaben und der mitunter weiten Fassung ihrer Umschreibung – für eine Vielzahl von Sachverhalten gegeben sein. Ein Lichtbildabruf kommt bei zu bestimmten Personen geführten Beobachtungen, Ermittlungen oder Verfahren stets hinsichtlich dieser Person selbst in Betracht. Regelmäßig wird ein solcher Bildabruf aber –

¹⁸ Vgl. BVerfGE 100, 313 (354 f.); 113, 348 (363); 133, 277 (312 f.); 143, 1 (21).

insbesondere bei den mit der Erkenntnissammlung weit im Vorfeld der konkreten Gefahrenabwehr oder Strafverfolgung betrauten Nachrichtendiensten – auch zur Identifizierung von Personen eingesetzt werden, die sich etwa aus beruflichen Gründen im Umfeld einer beobachteten Zielperson, Organisation oder Szene bewegen.

Die Beschwerdeführer standen aufgrund ihrer eingangs erläuterten Tätigkeiten bereits im Fokus nachrichtendienstlicher Erkenntnisgewinnung. Sie sind entweder selbst (Beschwerdeführer zu 1 und 4) regelmäßig im Umfeld von Beobachtungsobjekten der Verfassungsschutzbehörden tätig oder stehen bei ihrer journalistischen und publizistischen Tätigkeit (Beschwerdeführer zu 2 und 3) regelmäßig im persönlichen, auch direkten Austausch mit Personen und Quellen, welche ihrerseits Gefahr laufen, von Ermittlungen der Verfassungsschutzbehörden, des Militärischen Abschirmdienstes oder des Bundesnachrichtendienstes betroffen zu sein. Dass diese dabei von den angegriffenen Ermächtigungsvorschriften Gebrauch machen, ist mit einiger Wahrscheinlichkeit anzunehmen. Somit besteht eine hinreichend enge Beziehung zwischen der Grundrechtsposition der Beschwerdeführer und den angegriffenen Vorschriften.

Im Einzelnen ist davon auszugehen, dass die Beschwerdeführerin zu 1 im Rahmen ihrer vielfältigen Kontakte mit der Partei Die Linke weiterhin zumindest peripher in das Interesse der Verfassungsschutzbehörden gerät.

Die Tätigkeit der Beschwerdeführer zu 2 und 3 wurde durch das Bundesamt für Verfassungsschutz offensichtlich bereits als geeignet bewertet, die Gefahr eines schweren Nachteils für die Sicherheit der Bundesrepublik Deutschland im Sinne des § 94 StGB herbeizuführen, weshalb mit einiger Wahrscheinlichkeit von einer Beobachtung durch Verfassungsschutzbehörden ausgegangen werden muss. Nicht zuletzt die Tatsache, dass die Quelle der dem Landesverratsverfahren zugrunde liegenden Informationen soweit ersichtlich noch immer nicht bekannt ist, lässt auf ein fortbestehendes Interesse am Umfeld der Beschwerdeführer zu 2 und 3 schließen. Dass andere Nachrichtendienste hinsichtlich der sie jeweils betreffenden Veröffentlichungen zu vergleichbaren Einschätzungen kommen können, liegt nahe. Die Auswertung und Veröffentlichung zugespielter geheimer oder behördeninterner Dokumente durch die Beschwerdeführer zu 2 und 3 betrifft auch weiterhin regelmäßig Bereiche, die sowohl für die Verfassungsschutzbehörden als auch für den Bundesnachrichtendienst und den Militärischen Abschirmdienst von Relevanz sind. Es ist mit einiger Wahrscheinlichkeit anzunehmen, dass unter den potentiellen Quellen auch Personen sind, die unter Beobachtung oder Überwachung eines Nachrichtendienstes stehen und dann

durch den betreffenden Nachrichtendienst bezüglich der Beschwerdeführer ein automatisierter Lichtbildabruf nach den angegriffenen Vorschriften durchgeführt wird.

Für den Beschwerdeführer zu 4 ist mit einiger Wahrscheinlichkeit anzunehmen, dass bei den mit seiner anwaltlichen Tätigkeit einhergehenden Treffen mit Personen, die selbst unter Beobachtung oder Überwachung durch Verfassungsschutzbehörden stehen, oder bei Begleitung entsprechender Demonstrationen der betreffende Dienst auch einen Lichtbildabruf nach den angegriffenen Vorschriften etwa zur zweifelsfreien Identifizierung des Beschwerdeführers zu 4 durchführt.

2. Unmittelbare Betroffenheit

Die Beschwerdeführer sind durch die angegriffenen Vorschriften unmittelbar betroffen. Die Verfassungsbeschwerde wendet sich gegen gesetzliche Ermächtigungen und nicht gegen einen sie umsetzenden Vollzugsakt. Eine unmittelbare Betroffenheit durch ein Gesetz ist jedoch gegeben, wenn der Rechtsweg gegen die darauf beruhenden Vollzugsakte mangels Kenntnis der Vollzugsmaßnahmen nicht oder nicht effektiv beschritten werden kann.¹⁹

Der automatisierte Lichtbildabruf nach den hier angegriffenen Vorschriften erfolgt heimlich. Die verbesserte Möglichkeit der Geheimhaltung des Eingriffs ist sogar ausdrücklicher Bestandteil der Gesetzesbegründung für die Ausweitung des automatisierten Verfahrens.²⁰ Der Betroffene hat keine Kenntnis davon, dass ein solcher in seine Rechte eingreifender Abruf durchgeführt worden ist.

Nachträgliche Benachrichtigungspflichten, die dies aufzufangen in der Lage wären, bestehen nicht. Personalausweis- und Passgesetz enthalten keine eigenen Benachrichtigungsvorschriften für den Fall des automatisierten Datenabrufs. Die Nutzung des Abrufverfahrens unterliegt allein der Verantwortung der abrufenden Behörde. Aus den gesetzlichen Vorschriften der abrufenden Behörden ergeben sich für die Nachrichtendienste keine Benachrichtigungspflichten für den automatisierten Lichtbildabruf. Das Gesetz über den Bundesnachrichtendienst, das Gesetz über den militärischen Abschirmdienst, das Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz sowie die Landesverfassungsschutzgesetze sehen bei Datenerhebungen eine Benachrichtigung des Betroffenen entweder gar nicht vor oder nur für besondere Erhebungsmethoden, etwa beim verdeckten Einsatz technischer Mittel. Darüber hinaus bestehen erhebliche

¹⁹ Vgl. BVerfGE 109, 279 (306 f.); 100, 313 (354); 113, 348 (362 f.); 133, 277 (311); 141, 220 (261).

²⁰ BT-Drs. 18/11279, S. 32; 18/12417, S. 8 f.

Ausschlusstatbestände; darunter stets die Voraussetzung, dass keine Gefährdung des Erhebungszwecks vorliegen darf.

Soweit sich aus diesen Gesetzen Auskunftsrechte ergeben (etwa aus § 15 BVerfSchG und in Verbindung damit § 22 BNDG und § 9 MADG), beziehen sich diese lediglich auf die zu einem gegebenen Zeitpunkt gespeicherten Daten und nicht auf die Herkunft der Daten oder die Art ihrer Erlangung. Ob und wann ein automatisierter Lichtbildabruf durchgeführt worden ist, erschließt sich dem Betroffenen dabei nicht. Eine Erhebung und Speicherung bleibt nach einer Auskunftserteilung weiter jederzeit möglich. Die Auskunftserteilung steht zudem unter dem Vorbehalt der Nennung eines konkreten Sachverhalts und kann aus vielfältigen Gründen unterbleiben (vgl. § 15 Abs. 2 BVerfSchG), wobei die Ablehnung keiner Begründung bedarf und deshalb nur schwer überprüfbar ist (vgl. § 15 Abs. 4 BVerfSchG). Es ist davon auszugehen, dass diesen Ausnahmen erhebliche Bedeutung zukommt und sie den Auskunftsanspruch deutlich einschränken können. Das Auskunftersuchen ermöglicht somit keinen umfassenden Rechtsschutz und verschafft den Beschwerdeführern jedenfalls keine Kenntnis davon, ob eine Maßnahme nach den angegriffenen Vorschriften durchgeführt worden ist. Sie können deshalb nicht darauf verwiesen werden, einzelne Vollzugsakte und deren Bekanntwerden abzuwarten.

3. Gegenwärtige Betroffenheit

Die Beschwerdeführer sind durch die angegriffenen Ermächtigungen gegenwärtig betroffen. Die Vorschriften sind am 15. Juli 2017 in Kraft getreten. Aufgrund der bereits aufgeführten Tätigkeiten der Beschwerdeführer, die in der Vergangenheit bereits die Aufmerksamkeit verschiedener Nachrichtendienste auf sich gezogen haben, ist mit einiger Wahrscheinlichkeit anzunehmen, dass ihre Lichtbilder im Wege des § 25 Abs. 2 S. 4 PAuswG oder des § 22a Abs. 2 S. 5 PassG abgerufen werden. Die Maßnahmen sind nicht auf einen bestimmten Personenkreis begrenzt und können leicht auch Dritte erfassen, die selbst unverdächtig sind, aber mit beobachteten oder überwachten Personen verkehren. Angesichts des heimlichen Charakters der Maßnahme dürfen auch hier an die Darlegungslast nur begrenzte Anforderungen gestellt werden.

Dem steht nicht entgegen, dass die angegriffenen Befugnisse möglicherweise eine technische Anpassung der entsprechenden Fachverfahren mit sich bringen werden. Der automatisierte Abruf nach diesen Vorschriften ist bereits in vollem Umfang zulässig. Bezugspunkt für den Grundrechtsschutz der Beschwerdeführer ist das Wirksamwerden der Befugnisse unabhängig von etwaigen technischen Problemen bei der Anwendung. Ob und inwieweit die technischen Voraussetzungen für den automatisierten Abruf – der zumindest von einigen Behörden bereits

seit langem praktiziert wird – bestehen, ist für die Beschwerdeführer nicht nachvollziehbar und auch nicht entscheidend. Die Funktionsfähigkeit besteht zum Teil bereits und kann andernfalls jederzeit eintreten. Auf eine zunächst vorgesehene gesetzliche Übergangsphase ist im Übrigen bewusst verzichtet worden, da insbesondere angesichts der bereits bestehenden Möglichkeiten des automatisierten Abrufs keine Schwierigkeiten bei der sofortigen Umsetzung erwartet werden.²¹ Insofern kommt es auch nicht darauf an, ob jede Behörde verpflichtet ist, sofort ein automatisiertes Abrufverfahren zu ermöglichen, sondern darauf, dass jede Behörde hierzu befugt ist.

II. Subsidiarität

Die Verfassungsbeschwerde wahrt auch den Grundsatz der Subsidiarität. Den Beschwerdeführern ist nicht zuzumuten, einzelne Vollzugsakte und eine etwaige Kenntniserlangung hierüber abzuwarten, um dann gegen diese gerichtlich vorzugehen. Da die gegenständlichen Maßnahmen ohne Wissen der Betroffenen erfolgen, haben die Beschwerdeführer regelmäßig keine Kenntnis von einem vorgenommenen Eingriff.

Dies gilt auch im Hinblick auf Auskunftsansprüche gegenüber den Nachrichtendiensten, wie sie in § 15 BVerfSchG und – in Verbindung damit – § 22 BNDG oder § 9 MADG geregelt sind. Solche Ansprüche bestehen nur in engen Grenzen und unter besonderen Voraussetzungen, wie der Benennung eines konkreten Sachverhaltes und der Darlegung eines besonderen Interesses. Zudem kann eine Auskunftserteilung aus vielfältigen Gründen abgelehnt werden, ohne dass es einer Begründung bedarf (vgl. § 15 Abs. 2 und 4 BVerfSchG, § 22 BNDG, § 9 MADG), was eine rechtliche Überprüfung noch erheblich erschwert.

Die Eingriffe gehen in der gegenwärtigen Fassung der Vorschriften mit erheblichen Grundrechtsverletzungen einher, die Rechtsschutz auf dem verfassungsgerichtlichen Wege erforderlich machen.

III. Frist

Die Verfassungsbeschwerde ist fristgerecht erhoben. Es gilt die Jahresfrist des § 93 Abs. 3 BVerfGG. Die angegriffenen Vorschriften sind gem. Art. 6 Abs. 1 des Gesetzes zur Förderung des elektronischen Identitätsnachweises (BGBl. I, S. 2310) am 15. Juli 2017 in Kraft getreten. Soweit sich die Beschwerde gegen § 25 Abs. 2 S. 9 PAuswG und § 22a Abs. 2 S. 10 PassG wendet, steht ihrer Zulässigkeit nicht entgegen, dass diese Normbestandteile durch das Gesetz zur Förderung des elektronischen Identitätsnachweises nicht verändert worden sind.

²¹ BR-Drs. 787/1/16, S. 6 f.; BT-Drs. 18/12417, S. 10.

Durch die Gesetzesänderung erstrecken sich die Aufbewahrungsfristen, auf die darin verwiesen wird, auch auf die neu geregelten Maßnahmen und erhalten einen neuen Anwendungsbereich und Regelungsgehalt. Die Einbettung von Vorschriften in ein neues gesetzliches Umfeld mit der Folge neuer belastender Wirkungen setzt die Beschwerdefrist des § 93 Abs. 3 BVerfGG neu in Gang.²²

²² BVerfGE 78, 350 (356); 100, 313 (356); 141, 220 (242).

D. Begründetheit

Die angegriffenen Vorschriften verletzen die Beschwerdeführer in ihrem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und auf effektiven Rechtsschutz aus Art. 19 Abs. 4 GG.

I. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG

1. Maßstäblicher Schutzbereich

Das Recht auf informationelle Selbstbestimmung gewährleistet als Ausprägung des allgemeinen Persönlichkeitsrechts die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, und trägt damit insbesondere den diesbezüglichen Gefahren Rechnung, die sich aus informationsbezogenen Maßnahmen unter den Bedingungen moderner Datenverarbeitung ergeben.²³ Der Schutzbereich beginnt bereits dort, wo personenbezogene Daten in einer Weise genutzt oder verknüpft werden, die der Betroffene nicht überschauen oder beherrschen kann.²⁴ Diesem Grundrecht kommt – ganz seiner ursprünglichen Konzeption der Eingrenzung neuartiger, mit dem technologischen Fortschritt einhergehender Gefährdungen entsprechend²⁵ – eine stets zunehmende Bedeutung zu.

2. Intensiver Grundrechtseingriff durch automatisierten Lichtbildabruf

Die mit den angegriffenen Vorschriften gestatteten Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein.

a) Lichtbildabruf als Erhebung personenbezogener Daten

Der automatisierte Abruf betrifft das in den Datenbanken der Personalausweis- und Passbehörden gespeicherte Lichtbild und damit personenbezogene, sich auf eine identifizierte oder identifizierbare natürliche Person beziehende Daten²⁶ der Beschwerdeführer. Jeder abrufende Zugriff auf die Lichtbilddaten durch die in § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG angeführten Behörden stellt ebenso wie die Verwendung, Verarbeitung und Speicherung in deren Dateien einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dabei ist unerheblich, dass die Daten bereits anderweitig erhoben worden sind, denn sie werden anderen Behörden als denen, die sie erhoben haben, zu deren

²³ Vgl. BVerfGE 65, 1 (42); 115, 320 (341); 118, 168 (184).

²⁴ BVerfGE 118, 168 (184).

²⁵ Vgl. BVerfGE 54, 158 (153); 65, 1 (41).

²⁶ Vgl. BVerfGE 65, 1 (42).

Zwecken zur Verfügung gestellt und dort nach deren Kriterien aufbereitet.²⁷ Damit ist für den Betroffenen, der sein Lichtbild der Personalausweis- oder Passbehörde zur Verfügung stellen sollte, nicht länger überschaubar, welche Stelle zu welcher Zeit über seine Daten verfügt und welche Konsequenzen sich daraus für ihn ergeben. Die Kenntnis des Bürgers davon, wer wann und bei welcher Gelegenheit über ihn weiß, ist jedoch zentrales Element der informationellen Selbstbestimmung.²⁸

b) Intensität des Grundrechtseingriffs

Der mit den angegriffenen Vorschriften gestattete automatisierte Lichtbildabruf stellt einen Grundrechtseingriff von erheblicher Intensität dar. Dies ergibt sich nicht nur aus Umfang und Art der erhobenen Daten (aa) und der Art und Weise ihrer Erhebung (bb), sondern auch aus der Gesamtschau bestehender Datensammlungen und Verwendungsmöglichkeiten (cc).

aa) Umfang und Art der abgerufenen Daten

Bei dem nach § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG abgerufenen Lichtbild handelt es sich jeweils um ein die Anwendung der Gesichtsbioometrie, also die biometrische Erkennung der Person ermöglichendes Bild. Biometrische Lichtbilder stellen personenbezogene Daten dar, die – wie bereits ausgeführt – wie genetische oder Gesundheitsdaten von besonderer Sensibilität sind (vgl. oben A. I. 1.). Dies ergibt sich sowohl aus den Rückschlüssen, die sich aus biometrischen Daten ziehen lassen (etwa auf Alter, Geschlecht, Herkunft, Gesundheitszustand oder sexuelle Orientierung), als auch aus den vielfältigen und sich ständig weiterentwickelnden potentiellen Verwendungsmöglichkeiten (beispielsweise zur Authentifizierung, für intelligente Kamerasysteme oder den automatisierten Abgleich mit anderen Datenbanken). In Anerkennung der mit der Sammlung biometrischer Daten einhergehenden Gefahren ist die Errichtung bundesweiter biometrischer Datenbanken durch den Gesetzgeber ausdrücklich ausgeschlossen worden (vgl. § 26 Abs. 4 PAuswG und § 4 Abs. 3 S. 3 PassG).

Ausgangspunkt des Abrufs ist die flächendeckende verpflichtende Erhebung der biometrischen Daten von nahezu allen Deutschen. Diese Erhebung ist unabhängig vom Vorliegen eines Straftatverdachts oder einer Gefahrenlage und dient rein vorsorglich der Feststellung der Identität. Es handelt sich dabei um eine anlasslose vorsorgliche

²⁷ Vgl. BVerfGE 133, 277 (317).

²⁸ Vgl. BVerfGE 65, 1 (43).

Totalerhebung. An die zweckändernde Verwendung von Daten aus vorsorglichen anlasslosen Erhebungen sind grundsätzlich besonders hohe Anforderungen zu stellen.²⁹

Zu berücksichtigen sind weiter die möglichen belastenden Folgen des Lichtbildabrufs für den Betroffenen.³⁰ Die Schwere eines Informationseingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe zu.³¹ Die Aufnahme des Lichtbildes in die Dateien der abrufberechtigten Stellen kann zum Ansatz weiterer Untersuchungen gemacht werden und erhöht die Wahrscheinlichkeit solcher Maßnahmen. Die Speicherung in geheimdienstlichen Datenbanken kann für Betroffene schwerwiegende Konsequenzen haben, ohne dass sie um eine solche Speicherung wissen.³²

bb) Art und Weise des Datenabrufs

Besonders schwer wiegt der Eingriff aufgrund der Heimlichkeit der Maßnahme.³³

Dem Betroffenen eines heimlichen Eingriffs wird aufgrund seines Nichtwissens vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erheblich erschwert.³⁴ Heimliche staatliche Informationseingriffe wirken sich zudem aufgrund ihres Verunsicherungs- und Störungspotentials hinsichtlich der Ausübung von Grundrechten nicht nur auf die einzelnen Grundrechtsträger, sondern auf die Gesellschaft insgesamt aus.³⁵ Eine besondere Belastungswirkung liegt vorliegend darin, dass nicht nur der jeweilige Eingriff als solcher verdeckt geschieht, sondern die gesamten Aktivitäten der Nachrichtendienste geheim erfolgen. Befugnisse dieser Dienste zur Verwendung von vorsorglich und flächendeckend gespeicherten Daten verstärken deshalb das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise.³⁶

Hinzu tritt erschwerend die Erhebung im automatisierten Verfahren. Die besondere Eingriffsintensität entsteht dabei sowohl durch die in der Gesetzesbegründung ausdrücklich in Bezug genommene Vereinfachung des Abrufs und der damit einhergehenden Vervielfachung der Zahl der möglichen Erfassungsvorgänge als auch durch die verbesserten Bedingungen für eine heimliche Datenerfassung und -verarbeitung.³⁷

²⁹ Vgl. BVerfGE 125, 260 (335).

³⁰ Vgl. BVerfGE 100, 313 (376); 113, 348 (382); 115, 320 (347 f.); 118, 168 (197); 120, 378 (403).

³¹ BVerfGE 120, 378 (403).

³² Vgl. BVerfGE 133, 277 (331 f.).

³³ Vgl. BVerfGE 107, 299 (321); 113, 348 (383 f.); 115, 320 (353); 120, 274 (347 f.); 120, 378 (403).

³⁴ Vgl. BVerfGE 113, 348 (383 f.); 118, 168 (197 f.); 120, 378 (403).

³⁵ Vgl. BVerfGE 65, 1 (43); 93, 181 (188); 100, 313 (381); 109, 279 (354 f.); 120, 378 (403).

³⁶ Vgl. BVerfGE 125, 260 (332).

³⁷ Vgl. BVerfGE 115, 320 (357); 120, 378 (407).

cc) Baustein staatlicher Dateninfrastruktur

Die gegenständlichen Ermächtigungsnormen sind Bestandteil des schrittweisen Aufbaus der staatlichen Datenarchitektur und eines fortschreitenden Abbaus von Informationsgrenzen unter Sicherheitsbehörden und Nachrichtendiensten sowie zwischen ihnen und anderen staatlichen Stellen. Maßnahmen der großflächigen Datenerhebung und -speicherung können nicht isoliert betrachtet werden, sie sind vielmehr in den Kontext der Gesamtheit vorhandener Datensammlungen und Verarbeitungsmöglichkeiten zu stellen.³⁸

Zusätzliche Gefahren für die Grundrechte der Beschwerdeführer liegen in den weitläufigen Möglichkeiten der Verknüpfung biometrischer Daten mit anderweitigen Datenbeständen. Für die Beurteilung des Gewichts eines Grundrechtseingriffs sind auch die Informationen relevant, die durch eine weitergehende Verarbeitung und Verknüpfung der erfassten Daten gewonnen werden sollen.³⁹ Der Mehrwert des Lichtbildabrufs liegt gerade in der Zuordnung zu und Verbindung mit weiteren personenbezogenen Daten – oder, noch schwerwiegender – in den Erkenntnissen, die sich mittels entsprechender Analysetechnologien ggf. ableiten lassen. Der automatisierte Abgleich mit eigenen Bilddatenbanken der Nachrichtendienste kann beispielsweise anhand der biometrischen Merkmale (und wohl im Rahmen von Nutzungsbefugnissen nach § 10 Abs. 1 BVerfSchG, § 19 Abs. 1 BNDG, § 6 Abs. 1 MADG) nicht nur leicht Aufschluss darüber geben, ob der Betroffene dort bereits abgebildet ist, sondern auch über etwaige Verwandtschaftsverhältnisse mit anderen Abgebildeten.

Unter diesem Gesichtspunkt sind die umfassenden Befugnisse der Nachrichtendienste zur weiteren Verwendung der abgerufenen biometrischen Daten zu berücksichtigen. Da die angegriffenen Vorschriften keine eigenständigen Löschungspflichten für einmal abgerufene Daten vorsehen, können diese in der Regel solange gespeichert werden, wie sie für die Aufgabenerfüllung als erforderlich erachtet werden. Hierbei gelten lange Prüffristen von fünf bzw. zehn Jahren (§ 12 Abs. 2 und 3 bzw. § 13 Abs. 3 BVerfSchG, § 20 Abs. 1 BNDG, § 6 Abs. 2 MADG). Gleichzeitig bestehen weitreichende Ermächtigungen und Verpflichtungen zum Austausch personenbezogener Daten unter den Nachrichtendiensten, die teilweise wiederum automatisierte Abrufverfahren erlauben (vgl. §§ 3 Abs. 3, 11 Abs. 2 MADG, § 20 Abs. 1 S. 3, Abs. 2 S. 2 BVerfSchG, § 24 Abs. 1 und 3 BNDG). Die Vervielfachung und Vereinfachung der möglichen Datenabrufe durch das hier angegriffene automatisierte Abrufverfahren begünstigt so die Entstehung extensiver Datenbanken biometrischer Lichtbilder.⁴⁰

³⁸ Vgl. BVerfGE 125, 260 (324).

³⁹ BVerfGE 120, 378 (402).

⁴⁰ Vgl. zur darin liegenden Gefahr der parallelen Datenbanken Schaar, ZD 2017, 301 (302).

3. Gebot der Normenbestimmtheit und Normenklarheit

Die angegriffenen Vorschriften sind mit dem Bestimmtheitsgebot unvereinbar, da sie nicht mit der hinreichenden Klarheit umgrenzen, unter welchen Voraussetzungen der Lichtbildabdruck erfolgen darf.

a) Anzuwendender Maßstab

Das Bestimmtheitsgebot soll der Verwaltung hinreichende begrenzende Maßstäbe setzen, um im Hinblick auf den Gesetzesvorbehalt sicherzustellen, dass Grundrechtseingriffe durch die Legislative definiert und nicht einseitig ins behördliche Ermessen gestellt werden und darüber hinaus eine wirksame gerichtliche Rechtskontrolle ermöglichen. Zugleich erlauben es erst Bestimmtheit und Klarheit der Normen den Bürgern, sich auf belastende Maßnahmen einzustellen und ihr Verhalten danach auszurichten.⁴¹ Die Grenzen eines Eingriffs müssen deshalb stets bereichsspezifisch, präzise und normenklar aufgezeigt werden.⁴²

Welche Anforderungen an die Bestimmtheit gesetzlicher Vorschriften im Einzelnen zu stellen sind, richtet sich auch nach Art und Intensität der mit ihnen verbundenen Grundrechtseingriffe.⁴³

Ermächtigt eine Norm zu einem Eingriff in die informationelle Selbstbestimmung, tritt dazu die spezifische Funktion des Gebots von Bestimmtheit und Klarheit, den Erhebungsanlass und die möglichen Verwendungszwecke der betroffenen Informationen festzulegen.⁴⁴ Mit abnehmender Bestimmtheit einer solchen Regelung intensiviert sich der auf ihr beruhende Grundrechtseingriff, denn gerade durch die Vielfalt möglicher Verwendungszwecke und zugriffsberechtigter Stellen sowie die damit entstehenden Verknüpfungsmöglichkeiten geht die Überschaubarkeit und Beherrschbarkeit der eigenen Daten für den Betroffenen verloren.⁴⁵

Wo die praktische Umsetzung einer Norm vom Zusammenwirken der Vorschriften unterschiedlicher Rechtsgebiete abhängt, muss die Voraussehbarkeit der Ergebnisse für den Betroffenen auch im Hinblick auf dieses Zusammenwirken noch gewährleistet sein.⁴⁶

⁴¹ BVerfGE 113, 348 (375 ff.); 133, 277 (336).

⁴² BVerfGE 110, 33 (53); 113, 348 (375); 120, 378 (407 f.).

⁴³ Vgl. BVerfGE 133, 277 (336 f.).

⁴⁴ BVerfGE 120, 378 (408).

⁴⁵ Vgl. BVerfGE 118, 168 (187).

⁴⁶ BVerfGE 110, 33 (53 f.).

Befugnisnormen, die eine Überwachung von Bürgern ermöglichen, müssen zudem erkennen lassen, welche Verhaltensweisen das Risiko einer Anwendung von Überwachungsmaßnahmen bergen.⁴⁷

Besonders hohe Ansprüche ergeben sich aus dem Gebot von Normenbestimmtheit und Normenklarheit für heimliche Eingriffe. Denn der Betroffene, der keine Kenntnis einer ihn belastenden Maßnahme hat, ist umso mehr auf die gesetzliche Bindung der Exekutive und eine Verfahrensgestaltung, welche die Einhaltung dieser gesetzlichen Bindung sicherstellt, angewiesen.

Diesen Anforderungen werden die angegriffenen Vorschriften nicht gerecht.

b) Mangelnde Bestimmtheit von Abrufzweck und Aufgabenbereichen

Unter Anwendung des erörterten Maßstabs und angesichts des erheblichen Gewichts des mit dem automatisierten Lichtbildabruf verbundenen heimlichen Eingriffs in das Recht auf informationelle Selbstbestimmung sind vorliegend erhöhte Anforderungen an die Umgrenzung des Abrufanlasses und des Nutzungszwecks zu stellen. Um die Beurteilung der Rechtmäßigkeit eines Abrufs zu ermöglichen, sind der behördlichen Praxis die erforderlichen Kontrollmaßstäbe in Form einer aufgabenspezifischen Beschreibung der Ziele, die einen Abruf rechtfertigen können, bereitzustellen. Das bloße Anknüpfen an der Erforderlichkeit zur Aufgabenerfüllung stellt noch keine aufgaben- und bereichsspezifische Voraussetzung dar.⁴⁸ Es muss ersichtlich werden, unter welchen Umständen ein hinreichender Anlass für den Eingriff bestehen soll, welchem Zweck die Erhebung dient und inwieweit sich die weitere Verwendung auf diesen Zweck zu beschränken hat.

In den angegriffenen Vorschriften fehlt es hingegen an näheren Voraussetzungen für die Maßnahme – insbesondere an einer hinreichend bereichsspezifischen und normenklaren Bestimmung des Erhebungsanlasses und des Verwendungszwecks. § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG berechtigen mit den Polizeibehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, den Verfassungsschutzbehörden des Bundes und der Länder, den Steuerfahndungsdienststellen der Länder, dem Zollfahndungsdienst und den Hauptzollämtern eine sehr große Anzahl von Stellen zum automatisierten Datenabruf. Mit jeder beteiligten Stelle vervielfachen sich die Verknüpfungs- und Verwendungsmöglichkeiten. Die befugten Behörden verfolgen vielfältige unterschiedliche Ziele auf verschiedenen Rechtsgebieten. Anknüpfungspunkt für die

⁴⁷ BVerfGE 110, 33 (54).

⁴⁸ Vgl. BVerfGK 10, 330 = NVwZ 2007, 688 (691).

Berechtigung zum automatisierten Abruf ist dabei lediglich die Erfüllung der eigenen Aufgaben. Den unterschiedlichen berechtigten Stellen sind jeweils vielfältige Aufgaben zugeteilt, die im Einzelnen mitunter sehr offen gefasst sind. Die Befugnisse dieser Behörden sind teilweise in mehreren Gesetzen geregelt. Aufgabenzuweisungen finden sich zudem nicht nur in dem Gesetz oder den Gesetzen, welche die Befugnisse der einzelnen Behörden regeln, sondern auch in anderen Vorschriften, auf die mittels zahlreicher Verweise Bezug genommen wird. Hiermit wird die Voraussehbarkeit der Ergebnisse der Normanwendung weiter reduziert.

Besonders problematisch ist die unbeschränkte und lediglich verweisende Bezugnahme auf die Aufgabenbeschreibungen der Nachrichtendienste, die aufgrund ihrer vorwiegend erkenntnissammelnden und nicht operativ gefahrenabwehrenden oder strafverfolgenden Funktion⁴⁹ sehr weit gefasst sind. Maßnahmen werden regelmäßig unabhängig vom Vorliegen einer konkreten Gefahr durchgeführt. So verfügen die Nachrichtendienste über weitreichende Befugnisse zur Datensammlung, die weder hinsichtlich der konkreten Tätigkeitsfelder spezifisch ausdefiniert noch hinsichtlich der einzusetzenden Mittel detailscharf ausgestaltet sind.⁵⁰

Die Aufgaben des Bundesnachrichtendienstes ergeben sich aus § 1 Abs. 2 S. 1 BNDG:

Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus.

Die Aufgaben des Militärischen Abschirmdienstes sind in § 1 Abs. 1 bis 3 MADG geregelt:

(1) Aufgabe des Militärischen Abschirmdienstes des Bundesministeriums der Verteidigung ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über
1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,
wenn sich diese Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten und von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind. Darüber hinaus obliegt dem Militärischen Abschirmdienst die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über die Beteiligung von Angehörigen des Geschäftsbereiches des Bundesministeriums der

⁴⁹ Vgl. BVerfGE 133, 277 (327).

⁵⁰ BVerfGE 133, 277 (325).

Verteidigung sowie von Personen, die in ihm tätig sind oder in ihm tätig sein sollen, an Bestrebungen, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind. § 4 des Bundesverfassungsschutzgesetzes findet Anwendung.

(2) Darüber hinaus obliegt dem Militärischen Abschirmdienst zur Beurteilung der Sicherheitslage

1. von Dienststellen und Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung und

2. von Dienststellen und Einrichtungen der verbündeten Streitkräfte und der internationalen militärischen Hauptquartiere, wenn die Bundesrepublik Deutschland in internationalen Vereinbarungen Verpflichtungen zur Sicherheit dieser Dienststellen und Einrichtungen übernommen hat und die Beurteilung der Sicherheitslage im Einvernehmen zwischen dem Bundesministerium der Verteidigung und den zuständigen obersten Landesbehörden dem Militärischen Abschirmdienst übertragen worden ist,

die Auswertung von Informationen über die in Absatz 1 genannten Bestrebungen und Tätigkeiten gegen diese Dienststellen und Einrichtungen, auch soweit sie von Personen ausgehen oder ausgehen sollen, die nicht dem Geschäftsbereich des Bundesministeriums der Verteidigung angehören oder in ihm tätig sind.

(3) Der Militärische Abschirmdienst wirkt mit

1. bei der Sicherheitsüberprüfung von Personen, die dem Geschäftsbereich des Bundesministeriums der Verteidigung angehören, in ihm tätig sind oder werden sollen und

a) denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können

b) die an sicherheitsempfindlichen Stellen des Geschäftsbereichs des Bundesministeriums der Verteidigung eingesetzt sind oder werden sollen oder

c) die in sonstigen gesetzlich bestimmten Fällen einer Sicherheitsüberprüfung unterliegen,

2. bei technischen Sicherheitsmaßnahmen im Geschäftsbereich des Bundesministeriums der Verteidigung zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte.

[...]

Die Aufgaben des Bundesverfassungsschutzes sind insbesondere in § 3 Abs. 1 und 2 BVerfSchG aufgeführt:

(1) Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

3. Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,

4. Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind.

(2) Die Verfassungsschutzbehörden des Bundes und der Länder wirken mit

1. bei der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können,

2. bei der Sicherheitsüberprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen,

3. bei technischen Sicherheitsmaßnahmen zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte,

4. bei der Überprüfung von Personen in sonstigen gesetzlich bestimmten Fällen,

5. bei der Geheimschutzbetreuung von nichtöffentlichen Stellen durch den Bund oder durch ein Land.

[...]

Die Aufgaben der Landesbehörden für Verfassungsschutz ergeben sich zum Teil aus dem BVerfSchG, werden aber auch ergänzt durch landesrechtliche Normen, die mitunter erheblich weitere Aufgabenumschreibungen erhalten. So gehört zu den Aufgaben des Landesamtes für Verfassungsschutz in Baden-Württemberg, die hier beispielhaft aufgeführt werden, gem. § 3 Abs. 3 des baden-württembergischen Landesverfassungsschutzgesetzes die Mitwirkung

1. bei der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können,

2. bei der Sicherheitsüberprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen,

3. bei technischen oder organisatorischen Sicherheitsmaßnahmen zum Schutze von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte sowie bei Maßnahmen des vorbeugenden Sabotageschutzes,

4. auf Anforderungen der Einstellungsbehörde bei der Überprüfung von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben, sowie auf Anforderung der Beschäftigungsbehörde bei der

Überprüfung von Beschäftigten im öffentlichen Dienst, bei denen der auf Tatsachen beruhende Verdacht besteht, dass sie gegen die Pflicht zur Verfassungstreue verstoßen,

5. *bei der sicherheitsmäßigen Überprüfung von Einbürgerungsbewerbern,*

6. *bei der sicherheitsmäßigen Überprüfung von Ausländern im Rahmen der Bestimmungen des Ausländerrechts,*

7. *bei der Überprüfung der Zuverlässigkeit von Personen nach dem Waffen-, Sprengstoff- und Jagdrecht,*

8. *bei der Überprüfung der Zuverlässigkeit von Personen nach § 12b des Atomgesetzes,*

9. *bei der sicherheitsmäßigen Überprüfung von Personen nach § 7 des Luftsicherheitsgesetzes,*

10. *bei der Überprüfung der Zuverlässigkeit von Personen nach der Gewerbeordnung und den auf ihr beruhenden Rechtsverordnungen,*

11. *bei der Überprüfung der Zuverlässigkeit von Personen, denen bei Großveranstaltungen auf Grund ihrer Tätigkeit Zugang zu nicht allgemein zugänglichen Bereichen gewährt werden soll,*

12. *bei sonstigen Überprüfungen, soweit dies im Einzelfall zum Schutz der freiheitlichen demokratischen Grundordnung oder für Zwecke der öffentlichen Sicherheit erforderlich ist. [...]*

Diese Aufgabenzuweisungen beinhalten ersichtlich zugleich verschiedenartige und weit gefasste Ziele wie das Sammeln von außen- und sicherheitspolitisch relevanten Informationen, den Schutz vor verfassungsfeindlichen Bestrebungen im Inland und vor innerstaatlichen Tätigkeiten ausländischer Geheimdienste, den Schutz vor gewaltbereiten Bestrebungen, den Schutz vor Bestrebungen, die gegen den Gedanken der Völkerverständigung oder das friedliche Zusammenleben der Völker gerichtet sind sowie die allgemeine Beurteilung von Sicherheitslagen.⁵¹

Das Ausmaß der zum Zugriff berechtigenden Sachverhalte erfährt – im Gegensatz zur früheren Fassung und zur Regelung für herkömmliche Ersuchen – keine weitere Umgrenzung. So setzt der einzelne Abruf keinen konkreten Ermittlungsanlass, kein zu dem Betroffenen geführtes Ermittlungsverfahren und keine konkrete Gefahr voraus. Eine solche Voraussetzung ergibt sich weder aus den angegriffenen Vorschriften noch aus den die Aufgabenerfüllung der Nachrichtendienste regelnden Normen. Inwieweit ein bestimmter Sachverhalt für den Aufgabenbereich der Nachrichtendienste relevant ist, ist diesen selbst anheimgestellt und kaum justitiabel. Insofern knüpft diese Voraussetzung grundsätzlich nicht am Verhalten des Betroffenen an, sondern an internen Strukturen und Abläufen.

Auch steht die Befugnis zum automatisierten Abruf nicht unter einem übergeordneten, gemeinsamen Zweck wie etwa der Strafverfolgung oder der Bekämpfung des internationalen Terrorismus, anhand dessen sich der Anwendungsbereich eingrenzen ließe. Nicht weiter

⁵¹ Vgl. BVerfGE 133, 277 (325).

erhellend wirkt in dieser Hinsicht der in der Gesetzesbegründung in Bezug genommene Zweck, der sich – wie eingangs dargestellt – neben der erhofften Kosten- und Aufwandsersparnis weitgehend in der Nennung weniger Szenarien erschöpft, in denen der automatisierte Abruf erforderlich sein könnte. Die dort genannten Sachverhalte sind weder für alle befugten Behörden relevant, noch decken sie die Breite ihrer Aufgabenbereiche ab. Sie geben keinen Aufschluss darüber, zu welchen konkreten Zwecken der automatisierte Lichtbildabruf eingesetzt werden soll und welches Gewicht der Gesetzgeber ihm beimisst. Vielmehr verdeutlicht die an dieser Stelle unpräzise bleibende Gesetzesbegründung die mangelnde Begrenztheit und Bestimmtheit der auf ihr beruhenden Gesetzesänderung.

Dem stehen keinerlei Nutzungsregelungen für die abrufende Stelle, etwa in Form einer Beschränkung auf die Identifizierung ermittlungsrelevanter Personen, eines Ausschlusses der Weiterverwendung oder Speicherung oder eines Verbots der Weitergabe gegenüber. Solchen Nutzungsregelungen kommt aber wesentliche Bedeutung in der Umgrenzung des Eingriffs zu.⁵² Nicht weiter begrenzt ist auch der Kreis zugriffsberechtigter Personen.

Für die Beschwerdeführer ist daher nicht erkennbar, bei welchen Anlässen und unter welchen Voraussetzungen ihre Lichtbilder von welchen Personen abgerufen werden können, wann sie mit einer solchen Weiterverwertung ihrer Daten zu rechnen oder wie sie ihr Verhalten auszurichten haben, wenn sie dies vermeiden möchten. In welcher Form und zu welchen Zwecken das Lichtbild von der abrufenden Behörde verwendet werden wird, erschließt sich eben so wenig. Für den Bürger ergibt sich aus den angegriffenen Rechtsgrundlagen nicht, unter welchen Voraussetzungen in seine Grundrechte eingegriffen werden kann, sondern nur die Tatsache, dass solche Eingriffe gestattet sind. Das exekutive Eingriffshandeln bleibt für ihn unvorhersehbar, er muss es schlicht hinnehmen.

4. Verhältnismäßigkeit

Die angegriffenen Vorschriften verfehlen die sich aus dem verfassungsrechtlichen Verhältnismäßigkeitsprinzip ergebenden Anforderungen. Die mit den Befugnissen einhergehenden Eingriffe sind weder erforderlich (a) noch angemessen (b).

a) Erforderlichkeit

Der in den angegriffenen Vorschriften geregelte automatisierte Lichtbildabruf als Regelfall ist nicht im verfassungsrechtlichen Sinne erforderlich.

⁵² Vgl. BVerfGE 133, 277 (361 f.).

Grundsätzlich wiegt der automatisierte Abruf von Daten aufgrund seiner reduzierten Transparenz, seiner geringeren Justitiabilität und der niedrigeren praktischen Anwendungshürden schwerer als das von beiden Seiten protokollierte Ersuchen, welches im Vergleich das mildere Mittel darstellt. Eine flächendeckende, vorbehaltlose automatisierte Abfrage stünde zudem – wie erläutert – dem Verbot der Errichtung bundesweiter biometrischer Datenbanken gem. § 26 Abs. 4 PAuswG und § 4 Abs. 3 S. 3 PassG entgegen. Dem Grundsatz der Offenheit der Erhebung und Nutzung personenbezogener Daten entsprechend ist die Verwendung von Daten ohne Wissen des Betroffenen verfassungsrechtlich auch nur dann zulässig, wenn andernfalls der Zweck, dem der Datenabruf dient, vereitelt wird.⁵³

Folgerichtig war der automatisierte Abruf bis zur Änderung durch das Gesetz zur Förderung des elektronischen Identitätsnachweises an das Vorliegen besonderer Umstände gekoppelt und ist es für die Ordnungsbehörden noch heute. So erlauben § 25 Abs. 2 S. 1 PAuswG bzw. § 22a Abs. 2 S. 1 und 2 PassG einen automatisierten Abruf nur, wenn die zuständige Behörde „nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde“. Im Gesetzgebungsverfahren sind verschiedene Gründe angeführt worden, die eine unmittelbare Abfrage erforderlich machen können.⁵⁴ Dazu gehören insbesondere die Eilbedürftigkeit und die Gefährdung des Untersuchungszwecks durch Kenntniserlangung des Betroffenen oder Dritter von der Abfrage. Auch nach Ansicht des Gesetzgebers ist der automatisierte Abruf demnach nur bei Vorliegen besonderer Umstände erforderlich.

Solche besonderen Umstände machen die angegriffenen Vorschriften aber gerade nicht zur Voraussetzung eines automatisierten Abrufs. Ziel der erfolgten Änderung der angegriffenen Vorschriften war es stattdessen, den automatisierten Abruf zum Regelfall zu machen, also selbst dann für anwendbar zu erklären, wenn er nicht erforderlich ist und einem herkömmlichen Ersuchen keine Gründe entgegenstehen. Ein zwingendes grundsätzliches Erfordernis des automatisierten Abrufs jenseits des Vorliegens besonderer Umstände im Einzelfall ist nicht ersichtlich. Der Gesetzgeber hat es versäumt, verallgemeinerbare Beispiele zu nennen, die eine solche Einschätzung tragen würden, oder Angaben zum Ausmaß der behaupteten praktischen Vollzugsprobleme zu machen.⁵⁵ Die Folgen für den Betroffenen sind durch den automatisierten Abruf auch nicht geringer als durch das Ersuchen bei der zuständigen Behörde. Die dennoch vorgenommene Umkehr von Regel und Ausnahme missachtet den verfassungsrechtlichen Verhältnismäßigkeitsmaßstab.

⁵³ BVerfGE 125, 260 (335 f.).

⁵⁴ BT-Drs. 18/11279, S. 32; 18/12417, S. 8 f.; Deutscher Bundestag – Innenausschuss, Prot.-Nr. 18/113, S. 13.

⁵⁵ So auch der Sachverständige MDg Müller (für die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) in der öffentlichen Anhörung, Deutscher Bundestag – Innenausschuss, Prot.-Nr. 18/113, S. 21.

b) Verhältnismäßigkeit im engeren Sinne

Die mit den angegriffenen Ermächtigungen verbundenen Nachteile stehen außer Verhältnis zu den damit verfolgten Zielen. Dies ergibt sich im Hinblick auf die verfassungsrechtlichen Anforderungen (aa), insbesondere aus der zu niedrigen Eingriffsschwelle (bb), dem unbeschränkten Kreis der zugriffsberechtigten Personen (cc), der Verschiedenartigkeit der erhebenden und verwendenden Behörden (dd), der Herkunft der Daten aus einer anlasslosen und vorsorglichen Totalerhebung (ee), dem Fehlen von Nutzungsregelungen (ff), der Nichtsubsidiarität des automatisierten Verfahrens (gg) und der mangelnden Gewährleistung von Transparenz, Rechtsschutz und Kontrolle (hh).

aa) Anzuwendender Maßstab

Das Gebot der Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere eines Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht.

(1) Die Neufassung der angegriffenen Vorschriften verfolgt das Ziel, den zum automatisierten Abruf berechtigten Behörden die Erfüllung ihrer Aufgaben zu erleichtern. Zu diesen gehören wie oben ausgeführt teilweise gewichtige Bereiche wie die Außen- und Sicherheitspolitik der Bundesrepublik, der Schutz der freiheitlich demokratischen Grundordnung oder das friedliche Zusammenleben der Völker. Die Konkretisierungen der Aufgabenzuweisungen überantworten hingegen sogar dem Wirkungsbereich der Nachrichtendienste ausdrücklich auch deutlich weniger schwerwiegende Tätigkeiten. So wirkt das baden-württembergische Landesamt für Verfassungsschutz beispielsweise bei der Überprüfung der Zuverlässigkeit von Personen nach der Gewerbeordnung mit (§ 3 Abs. 3 Nr. 10 LVSG-BW). Des Weiteren werden auch die Polizeibehörden des Bundes und der Länder, die Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter zum automatisierten Abruf befugt, deren Aufgaben auch die Verfolgung von Straftaten geringen Gewichts, die Regelung des Verkehrs und allgemein niedrigschwellige Eingriffe umfassen.

Bei der verfassungsrechtlichen Bewertung der Vorschriften sind die in Bezug genommenen Aufgabenzuweisungen grundsätzlich weit zu verstehen. Ist eine Ermächtigung nicht eindeutig, weil sie eine spezifische Auslegung nicht hinreichend deutlich ausschließt, ist für die Prüfung der Verhältnismäßigkeit das dadurch ermöglichte weite Verständnis ihrer Zwecksetzung und Reichweite zugrunde zu legen.⁵⁶ Die Vielfältigkeit der Aufgaben, deren Erfüllung die

⁵⁶ BVerfGE 120, 378 (427).

angegriffenen Eingriffsbefugnisse erleichtern sollen, verwässert vorliegend gleichsam das Gesamtgewicht der den Eingriff rechtfertigenden Ziele.

(2) Der mit den angegriffenen Vorschriften verbundene Grundrechtseingriff ist – wie bereits ausgeführt (vgl. oben D. I. 2. lit. b) – von erheblichem Gewicht. Dies ergibt sich nicht nur aus Umfang und Art der erhobenen biometrischen Daten und ihrer Nutzungsmöglichkeiten, sondern auch aus der Art und Weise ihrer Erhebung ohne Wissen des Betroffenen im automatisierten Verfahren und dem Kontext der bestehenden Dateninfrastruktur. Bei heimlichen Eingriffen – insbesondere unter dem Einsatz moderner Technologien und Verfahren – ist im Hinblick auf die additive Wirkung von Grundrechtseingriffen zudem das Gesamtausmaß der bezüglich des Betroffenen ermöglichten Datenerhebung und -speicherung als Maßstab zu nehmen.⁵⁷

Erschwerend wirkt sich die geringe Bestimmtheit der angegriffenen Normen aus (vgl. oben D. I. 3.). Bestimmtheitsmängel können die Beachtung des verfassungsrechtlichen Übermaßverbots beeinträchtigen, weil sie die Beurteilung einer Maßnahme erschweren und das Risiko unangemessener Eingriffe erhöhen.⁵⁸ Insbesondere bei Eingriffen in das Recht auf informationelle Selbstbestimmung wird das Gewicht des Eingriffs durch eine wie vorliegend offene Gestaltung der Erhebungs- und Verwendungszwecke erhöht.⁵⁹

(3) Eine Spezifizierung der Anforderungen ergibt sich aus den Grundsätzen der Zweckbindung und Zweckänderung.

Der automatisierte Abruf der Lichtbilder durch die in den angegriffenen Vorschriften befugten Behörden stellt im Verhältnis zu ihrem ursprünglichen Erhebungszweck eine Zweckänderung dar. Eine Nutzung noch innerhalb der ursprünglichen Zwecksetzung läge nur vor, wenn sie seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter wie die Datenerhebung erfolgte.⁶⁰ Die Erhebung der Lichtbilder erfolgt durch die Personalausweis- und Passbehörden zur Erfüllung ordnungsrechtlicher Aufgaben auf dem Gebiet des Melde-, Pass- und Ausweisrechts. Der Abruf durch die in § 25 Abs. 2 S. 4 PAuswG und § 22a Abs. 2 S. 5 PassG angeführten Behörden zur Erfüllung der dort angeführten Aufgaben ermöglicht die Verwendung durch andere als die ursprünglich erhebende Behörde und erlaubt diesen – wie bereits ausgeführt – den Abruf im Rahmen gänzlich anderer Aufgabenbereiche für den Schutz eines weiten Kreises an Rechtsgütern.

⁵⁷ Vgl. BVerfGE 112, 304 (319 f.); 141, 220 (280).

⁵⁸ Vgl. BVerfGE 120, 378 (427).

⁵⁹ Vgl. BVerfGE 118, 168 (187).

⁶⁰ Vgl. BVerfGE 141, 220 (325).

Der Gesetzgeber ist nicht grundsätzlich daran gehindert, solche Zweckänderungen zuzulassen. Er hat dann jedoch sicherzustellen, dass dieser erneute Grundrechtseingriff auch unter Berücksichtigung der ursprünglichen Erhebung verhältnismäßig bleibt. Bei der Verwendung von Daten für die Aufgabenerfüllung der Nachrichtendienste gilt grundsätzlich dieselbe Bindung an die verfassungsrechtlichen Vorgaben des Verhältnismäßigkeitsprinzips wie für andere präventive Eingriffsermächtigungen.⁶¹ Die Ermächtigung zu einer Zweckänderung ist insofern einerseits an Art, Zweck und Gewicht der ursprünglichen Datenerhebung zu messen.⁶² Eine zweckändernde Verwendung kann demnach nur zulässig sein, wenn zu diesem Zweck eine hypothetische Neuerhebung der Daten mit diesen Mitteln zulässig wäre.⁶³ An die zweckändernde Verwendung von Daten aus vorsorglichen anlasslosen Erhebungen sind grundsätzlich besonders strenge Anforderungen zu stellen.⁶⁴ Für die Beurteilung der Verhältnismäßigkeit eines Informationsaustauschs zwischen verschiedenen Behörden kommt es darüber hinaus insbesondere auf die Vergleichbarkeit der verschiedenen Informationszusammenhänge an. Je verschiedenartiger Aufgaben, Befugnisse und Art der Aufgabenwahrnehmung sind, desto größeres Gewicht hat der Austausch entsprechender Daten.⁶⁵

(4) Aus dem Verhältnismäßigkeitsprinzip ergeben sich zudem bestimmte, in der verfassungsgerichtlichen Rechtsprechung herausgearbeitete Anforderungen an Transparenz, Rechtsschutz und Kontrolle für die in das Recht auf informationelle Selbstbestimmung eingreifende Datenerhebung und -verarbeitung in Form verfahrensrechtlicher Sicherungen. Bei heimlichen Grundrechtseingriffen ist grundsätzlich eine nachträgliche Kenntnisnahme durch die Betroffenen zu gewährleisten, die diesen einen effektiven Rechtsschutz ermöglicht.⁶⁶ Dies geschieht durch das System gesetzlicher Auskunftsrechte und Benachrichtigungspflichten. Wo die Vornahme von Eingriffen aufgrund ihrer verdeckten Durchführung von den Betroffenen nicht sicher abgeschätzt werden kann, sind wirksame Auskunftsrechte vorzusehen.⁶⁷ Der ausnahmsweise Ausschluss oder die Beschränkung solcher Rechte ist tatbestandlich und überprüfbar unter Abwägung der gegenüberstehenden Interessen zu rechtfertigen.⁶⁸

Sind bei heimlichen, in die informationelle Selbstbestimmung eingreifenden Datenerhebungen keine Auskunftsansprüche eingeräumt oder tragen diese den Rechten des Betroffenen nicht

⁶¹ BVerfGE 125, 260 (331 f.).

⁶² BVerfGE 141, 220 (327).

⁶³ Vgl. BVerfGE 141, 220 (327 f.).

⁶⁴ Vgl. BVerfGE 125, 260 (335).

⁶⁵ BVerfGE 133, 277 (323 f.).

⁶⁶ Vgl. BVerfGE 141, 220 (282 f.).

⁶⁷ Vgl. BVerfGE 133, 277 (367); 141, 220 (283).

⁶⁸ Vgl. BVerfGE 120, 351 (365); 141, 220 (283).

angemessen Rechnung, ist eine Benachrichtigung zwingend erforderlich.⁶⁹ Insofern kommt der gesetzlichen Anordnung von Benachrichtigungspflichten große Bedeutung für eine verhältnismäßige Ausgestaltung der Eingriffsermächtigungen zu.⁷⁰ Soweit in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter⁷¹ Ausnahmen von einer erforderlichen Pflicht zur nachträglichen Benachrichtigung gemacht werden, haben diese sich auf das unbedingt Erforderliche zu beschränken.⁷² Einer dementsprechenden Ausgestaltung von Benachrichtigungspflichten bedarf es dabei nicht nur in der Strafverfolgung und der Gefahrenabwehr, sondern auch hinsichtlich der Verwendung der Daten für Aufgaben der Nachrichtendienste.⁷³

Großer Bedeutung kommt daneben der Gewährleistung aufsichtlicher Kontrolle zu.⁷⁴ Die Verfügbarkeit der für eine solche Kontrolle erforderlichen Daten ist durch technische Vorkehrungen sicherzustellen, insbesondere in Gestalt hinreichender Protokollierung.⁷⁵ In Hinblick auf den dort nur schwach ausgestalteten subjektiven Rechtsschutz kommt bei heimlichen Maßnahmen der regelmäßigen Aufsichtsübung erhöhte Bedeutung zu und sind gegebenenfalls entsprechende Kontrollen in angemessenen Abständen vorzusehen.⁷⁶ Werden Daten von vielen unterschiedlichen Behörden auf Bundes- und Landesebene genutzt, ist dies bei der Gewährleistung wirksamer Aufsicht entsprechend zu berücksichtigen. Wo der Gesetzgeber eine informationelle Kooperation von Behörden ermöglicht, ist er gehalten, auch die kontrollierende Kooperation zugunsten des Datenschutzes zu realisieren.⁷⁷

bb) Niedrige Eingriffsschwelle durch weiten Aufgabenkreis

Die angegriffenen Befugnisse setzen mit dem uneingeschränkten Bezug auf einen weiten Aufgabenkreis eine unzureichende Eingriffsschwelle für den automatisierten Lichtbildabruf. Die Ermächtigungen gestatten den Abruf zur Erfüllung von Aufgaben durch eine Vielzahl von Behörden, denen wiederum vielfältige verschiedene Aufgaben zukommen. Wie bereits ausgeführt umfasst das vor allem im Bereich der Nachrichtendienste breite und weitgefaste Aufgabenspektrum Aufgaben von unterschiedlicher Bedeutung. Die Aufgabenerfüllung setzt sich zudem stets aus einzelnen konkreten Tätigkeiten zusammen, denen jeweils eine unterschiedliche Relevanz für das übergeordnete Ziel zukommen kann. Es ist deshalb möglich – und angesichts der weiten Fassung der Eingriffsermächtigungen ist die weitgehendste

⁶⁹ Vgl. BVerfGE 118, 168 (208).

⁷⁰ Vgl. BVerfGE 125, 260 (336); 133, 277 (369); 141, 220 (282 f.).

⁷¹ Vgl. BVerfGE 125, 260 (344); 141, 220 (283).

⁷² Vgl. BVerfGE 109, 279 (364); 125, 260 (336); 141, 220 (283).

⁷³ Vgl. BVerfGE 125, 260 (337).

⁷⁴ Vgl. BVerfGE 65, 1 (46); 133, 277 (369 f.); 141, 220 (284 f.).

⁷⁵ Vgl. BVerfGE 141, 220 (285).

⁷⁶ Vgl. BVerfGE 133, 277 (370); 141, 220 (285).

⁷⁷ Vgl. BVerfGE 133, 277 (370).

Auslegungsmöglichkeit maßstäblich für die Beurteilung ihrer Angemessenheit –, dass ein Lichtbildabruf im Rahmen der Aufgabenerfüllung für die Verfolgung von im Einzelnen weniger gewichtigen Zielen erfolgt.

Eine übergeordnete Zwecksetzung wie etwa die Bekämpfung terroristischer Straftaten, aus der Anhaltspunkte für eine grundsätzlich schwerwiegende Bedeutung der im Einzelnen verfolgten Zwecke zu ziehen wären, besteht nicht. Für die Abwägung im Einzelfall bieten die angegriffenen Vorschriften keine Handhabe in Form einer Beschränkung auf näher bestimmte Aufgabenspektren oder konkrete Verfahren, das Vorliegen besonderer Umstände oder eine vorzunehmende Abwägung unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen. Eine konkrete Gefahr wird nicht vorausgesetzt. Die Verhältnismäßigkeit des Eingriffs ist somit nicht durch eine konkretisierte oder qualifizierte Eingriffshürde gesichert. Eine derart niedrige, verdachtsunabhängige Eingriffsschwelle kann zwar unter bestimmten Voraussetzungen gerechtfertigt sein, etwa zur Verfolgung besonderer, außerordentlich gewichtiger Zwecke durch einzelne, in gerade diesen Fällen auf eine solche Vorgehensweise angewiesene Behörden und im Rahmen bestimmter materieller Kriterien.⁷⁸ So liegt es hier aber nicht. Weder sind besondere, im Einzelnen außerordentlich gewichtige Zwecke benannt, noch wird eine Verbindung hergestellt zwischen einer bestimmten Behörde und ihrer spezifischen Zielsetzung, die für sie den automatisierten Lichtbildabruf unter solch geringen Eingriffsvoraussetzungen unentbehrlich machen würde. Materielle Kriterien sind nicht festgelegt.

Eine behördliche Prüfung, ob unter Gesichtspunkten der Zweckänderung eine hypothetische Datenneuerhebung im konkreten Fall zulässig wäre, findet nicht statt. Nicht zuletzt an dieser Stelle zeigt sich deutlich, dass der automatisierte Zugriff auf die biometrischen Lichtbilddatenbanken nicht wie erforderlich in seinem Gesamtgewicht einer Abwägung unterzogen worden ist. Der automatisierte und verdeckte Abruf anlasslos, vorsorglich und großflächig gespeicherter biometrischer Daten durch die dem Transparenzgebot nur in geringem Maße unterliegenden Nachrichtendienste und eine Vielzahl von Strafverfolgungs- und anderen Sicherheitsbehörden ist kein Eingriff von so geringem Gewicht, dass er zu jedem mit der Aufgabenerfüllung dieser Behörden in Verbindung stehenden Zweck gerechtfertigt wäre.

Damit ist die Eingriffsschwelle insgesamt als zu niedrig zu bewerten. Sie genügt in dieser Form angesichts der erheblichen Eingriffsintensität nicht den oben genannten verfassungsrechtlichen Anforderungen an die Verhältnismäßigkeit.

⁷⁸ Vgl. BVerfGE 100, 313 (383); 120, 274 (330); 125, 260 (331).

cc) Unbeschränkter Kreis zugriffsberechtigter Personen

Im Sinne der Datenminimierung kommt auch dem Kreis der zugriffsberechtigten Personen Bedeutung zu. Eine Beschränkung dieses Kreises kann die Unübersichtlichkeit der Datenverwendung für den Betroffenen reduzieren. Sie findet sich etwa in § 24 Abs. 3 S. 2 PAuswG und § 22 Abs. 3 S. 2 PassG für das herkömmliche Ersuchen. Solche Begrenzungen fehlen in den angegriffenen Vorschriften und ergeben sich auch nicht aus den anzuwendenden gesetzlichen Bestimmungen der abrufenden Behörden. Die Hürde für den Datenabruf wird damit weiter reduziert, während sich die Anzahl der potentiell über die Daten verfügenden Personen erhöht. Unter Berücksichtigung des Grundsatzes des Vorbehalts des Gesetzes und des Wesentlichkeitsgrundsatzes wäre eine diesbezügliche gesetzliche Regelung erforderlich gewesen.

dd) Verschiedenartigkeit von Erhebungs- und Verwendungsbehörden

Wie erläutert wird die Angemessenheit des Datenaustausches zwischen Behörden durch die Vergleichbarkeit der Informationszusammenhänge beeinflusst.

Die angegriffenen Vorschriften zeichnen sich durch die automatisierte Verknüpfung von Personalausweis- und Passbehörden nicht nur mit den Polizei-, Zoll- und Steuerfahndungsbehörden, sondern auch und insbesondere mit den Nachrichtendiensten aus. Während die datenerhebenden Behörden in Form der Personalausweis- und Passbehörden im Wesentlichen ordnungsrechtliche Aufgaben auf dem Gebiet des Melde-, Pass- und Personalausweisrechts erfüllen, kommen vor allem den Nachrichtendiensten verschiedenartige und weitreichende Aufgaben zu, die vom Sammeln von außen- und sicherheitspolitisch relevanten Informationen über den Schutz vor verfassungsfeindlichen Bestrebungen im Inland und vor innerstaatlichen Tätigkeiten ausländischer Geheimdienste bis hin zum Schutz vor gewaltbereiten oder gegen den Gedanken der Völkerverständigung oder das friedliche Zusammenleben der Völker gerichteten Bestrebungen reichen. Die von den abrufenden Behörden zu erfüllenden Aufgaben unterscheiden sich damit ganz erheblich von denen der erhebenden Behörde. Hinzu kommt, dass die nachrichtendienstlichen Aufgabenbeschreibungen – der spezifischen und wiederum maßgeblich von der der erhebenden Behörden divergierenden Art der Aufgabenwahrnehmung entsprechend – grundsätzlich weit gefasst und wenig umgrenzt sind. Auch die Ausgestaltung der damit einhergehenden Befugnisse verdeutlicht die Verschiedenartigkeit der beteiligten Behörden. So sind die Nachrichtendienste im Gegensatz zu den Personalausweis- und Passbehörden mit weitreichenden und eingriffsintensiven Befugnissen ausgestattet. Diese sind regelmäßig mit

schwerwiegenden Konsequenzen für die Betroffenen verbunden, etwa durch die Speicherung in bestimmten nachrichtendienstlichen Dateien, die Weitergabe an ausländische Dienste oder die mittelbare Einleitung operativer Maßnahmen der Gefahrenabwehr oder Strafverfolgung durch die hierfür zuständigen Behörden.

Angesichts der grundlegenden und tiefgreifenden Verschiedenartigkeit der Aufgaben, Befugnisse und Aufgabenwahrnehmung der erhebenden und der abrufenden Behörden und dem sich daraus ergebenden Gewicht des Datenaustauschs stellt sich der nahezu vorbehaltlose automatisierte Abruf nicht mehr als angemessen dar. Das umfassende Erheben und Sammeln der Lichtbilder durch die Personalausweis- und Passbehörden ist gerade aufgrund der spezifischen, begrenzten und kontrollierbaren Aufgabenausgestaltung und geringen Eingriffsbefugnisse dieser Behörden verfassungsrechtlich zu rechtfertigen, während umgekehrt den Nachrichtendiensten eine solche Totalerhebung aufgrund ihrer weitreichenden und weit gefassten Befugnisse und Verwertungsoptionen nicht gestattet ist. Mit den durch die angegriffenen Vorschriften geschaffenen Möglichkeiten des Datenaustauschs werden diese bereichsspezifischen Aufgabenaufteilungen in unzulässiger Weise aufgehoben und die damit beabsichtigten und notwendigen Begrenzungen umgangen.

ee) Anlasslose und vorsorgliche Totalerhebung

Das Erheben und Sammeln der biometrischen Lichtbilder durch die Personalausweis- und Passbehörden stellt eine anlasslose und vorsorgliche Totalerhebung besonders sensibler personenbezogener Daten dar, deren Weiterverwendung in der vorgesehenen Form des automatisierten Abrufs mit dem Übermaßverbot unvereinbar ist.

Den sich hieraus ergebenden, besonders strengen Anforderungen an eine zweckändernde Verwendung der Daten werden die Vorschriften zum automatisierten Abruf nicht gerecht. Sie erlauben den Zugriff auf diese verdachtsunabhängig erhobenen biometrischen Daten für einen nahezu unbeschränkten Anwendungsbereich zur Erfüllung einer Vielzahl von Aufgaben durch unterschiedlichste Behörden aus unterschiedlichen Rechtsgebieten zu nicht näher bestimmten Zwecken und ohne den Vorbehalt der spezifischen Erforderlichkeit des automatisierten Abrufverfahrens. Die unmittelbare und in das eigene Ermessen gestellte Anbindung der Nachrichtendienste an den nahezu die gesamte Bevölkerung umfassenden biometrischen Datenbestand der erhebenden Behörden steht in der gegenwärtigen Ausgestaltung der angegriffenen Vorschriften außer Verhältnis zu den diese Grundrechtseingriffe rechtfertigenden Gründen. Eine solch umfassende Erhebung wäre den Nachrichtendiensten unter dem Gesichtspunkt der Neuerhebung gerade nicht gestattet. Der

einzelne Abruf kann – erst recht im automatisierten Verfahren – nicht von der Herkunft des Ausgangsdatensatzes isoliert bewertet werden.

ff) Fehlende Nutzungsregelungen

Entscheidende Bedeutung für die Bewertung der Verhältnismäßigkeit kommt – insbesondere bei datenbezogenen Ermächtigungen mit weiten Abrufmöglichkeiten und ohne begrenzende Eingriffsschwellen – dem Vorliegen konkreter Nutzungsregelungen zu.⁷⁹ Die angegriffenen Vorschriften enthalten keine solchen Regelungen. Weder wird der Abruf auf bestimmte konkretisierte Anlässe beschränkt, noch ist die Weiterverwendung durch für den Lichtbildabruf spezifische Regelungen eingeehgt.

Durch die nicht subsidiär gestaltete Befugnis des automatisierten Abrufs entsteht faktisch eine bundesweit verfügbare (und im Widerspruch zu der gesetzgeberischen Wertung aus § 26 Abs. 4 PAuswG und § 4 Abs. 3 S. 3 PassG stehende) Datenbank biometrischer Merkmale. Die gegenwärtige Ausgestaltung der angegriffenen Vorschriften schafft einen unmittelbaren Zugriff auch der Nachrichtendienste auf die biometrischen Lichtbilddatenbanken der Personalausweis- und Passbehörden. Die Entscheidung über den Abruf und die Verantwortung für das Vorliegen der Voraussetzungen liegt allein bei den abrufenden Behörden; eine Protokollierung erfolgt nur bei diesen. Ein Vorrang des Ersuchens um Übermittlung besteht nicht. Dies entspricht in der Funktionalität einer bundesweiten Datenbank. Deren Umfang richtet sich nach dem Fachrecht der Nachrichtendienste, das weitreichende Befugnisse zur Speicherung und Weiterverwertung vorsieht und dessen Löschungspflichten wiederum weitgehend an die eigene Aufgabenwahrnehmung anknüpfen (vgl. oben D. I. 2. lit. b cc).

Die Nachrichtendienste sind nach dem Fachrecht etwa dazu befugt, die abgerufenen Daten in neuem Zusammenhang in eigenen Dateien zu speichern, mittels geeigneter Technologien wie der Gesichtsanalyse und -erkennung auszuwerten, mit anderen Datenbanken (etwa Videoüberwachungssystemen) abzugleichen oder an andere Stellen oder an ausländische Dienste weiterzugeben. Der in den nicht vorhandenen Nutzungsregelungen liegende Verzicht auf ein wesentliches Mittel zur Reduzierung der Eingriffsschwere führt dazu, dass die Intensität der Eingriffe an keiner Stelle gesetzlich abgefedert wird. Genau dies verlangt aber das Übermaßverbot. Angesichts der geringen Bestimmtheit der Ermächtigung und des erheblichen Gewichts der darin vorgesehenen Grundrechtseingriffe, das wiederum maßgeblich aus den vielfältigen potentiellen Verwendungs- und Verknüpfungsmöglichkeiten der erlangten Daten

⁷⁹ Vgl. BVerfGE 133, 277 (361 f.).

resultiert, war eine zumindest ansatzweise Umgrenzung durch Nutzungsregelungen im Sinne der Angemessenheit unerlässlich.

Die Unüberschaubarkeit der möglichen Anwendungsfälle ist zusammen mit dem allgemeinen Bewusstsein davon, dass die biometrischen Daten aller Bürger in den entsprechenden Datenbanken der Personalausweis- und Passbehörden gespeichert und abrufbar sind, geeignet, eben jenes diffuse Gefühl des Beobachtetseins hervorzurufen, dass die unbefangene Wahrnehmung der Grundrechte zu beeinträchtigen droht.⁸⁰

gg) Fehlende Subsidiarität des automatisierten Verfahrens

Im Sinne des Übermaßverbotes und dem Prinzip der Datenminimierung setzen informationsbezogene Maßnahmen voraus, dass die behördliche Datennutzung allzeit auf das zur Zielerreichung erforderliche Minimum reduziert wird.⁸¹ Wie bereits ausgeführt, erlauben die angegriffenen Vorschriften den automatisierten Datenabruf unabhängig davon, ob ein herkömmliches nichtautomatisiertes Ersuchen als milderer Mittel in Betracht kommt. Damit erfüllen die Vorschriften die sich aus dem Recht auf informationelle Selbstbestimmung ergebende Pflicht, die behördliche Datennutzung auf ein Minimum zu reduzieren, auch unter dem Gesichtspunkt der Angemessenheit nicht. Gegen eine solche Beschränkung sprechen keine gewichtigen Gründe. Es wäre ohne Weiteres möglich gewesen, den automatisierten Abruf unter den Vorbehalt der Erforderlichkeit dieses spezifischen Übertragungsweges zu stellen. Auch die Gesetzesbegründung erkennt insofern an, dass der automatisierte Abruf insbesondere durch besondere Umstände erforderlich gemacht wird und benennt diese ausdrücklich. Stattdessen wird durch die in dieser Hinsicht vorbehaltlose Befugnis zu automatisierten Abrufen diese Eingriffsweise zur Routine des behördlichen Datenaustauschs.

hh) Mangelnde Gewährleistung von Transparenz, Rechtsschutz und Kontrolle

Die angegriffenen Vorschriften werden auch den Anforderungen an Transparenz, Rechtsschutz und Kontrolle nicht gerecht.

(1) Es bestehen keine Auskunftsrechte, die einen wirksamen Rechtsschutz ermöglichen und damit den Rechten der Beschwerdeführer hinreichend Rechnung tragen. Die angegriffenen Regelungen enthalten keine eigenständigen Auskunftsrechte. Soweit sich aus dem Fachrecht Auskunftsrechte ergeben (etwa § 15 BVerfSchG, § 22 BNDG, § 9 MADG und entsprechende Gesetze für die Landesverfassungsschutzbehörden), beziehen sich diese lediglich auf die zu

⁸⁰ Vgl. BVerfGE 125, 260 (320).

⁸¹ Vgl. BVerfGE 65, 1 (46).

einem gegebenen Zeitpunkt gespeicherten Daten und nicht auf die Herkunft der Daten oder die Art ihrer Erlangung. Ob und wann ein automatisierter Lichtbildabruf durchgeführt worden ist, erschließt sich den Beschwerdeführern dabei nicht. Die Auskunftserteilung steht zudem unter dem Vorbehalt der Nennung eines konkreten Sachverhalts und kann aus vielfältigen Gründen unterbleiben (§ 15 Abs. 2 BVerfSchG), wobei die Ablehnung keiner Begründung bedarf und deshalb nur schwer überprüfbar ist (§ 15 Abs. 4 BVerfSchG).

Das Auskunftersuchen verschafft den Beschwerdeführern keine Kenntnis davon, ob eine Maßnahme nach den angegriffenen Vorschriften durchgeführt worden ist, und ermöglicht auch keinen tatsächlich wirkungsvollen Rechtsschutz. Die Betroffenen erlangen auf diesem Wege nicht die Fähigkeit, die Unrechtmäßigkeit des Eingriffs geltend zu machen. Zu berücksichtigen ist diesbezüglich noch, dass eine Datenerfassung durch die Nachrichtendienste zwar vielfältige Nachteile für den Betroffenen mit sich bringen kann, aber nicht notwendigerweise in für ihn sichtbaren Schritten wie einer Beschuldigtenvernehmung gipfelt. Er hat deshalb meist keinen faktischen Anlass, von seinen Auskunftsrechten Gebrauch zu machen, weshalb ein erfolgter Eingriff auf unbestimmte Zeit unentdeckt bleiben kann. Dass Auskunftsgesuche zu jedem denkbaren Sachverhalt bei vielen verschiedenen Behörden separat gestellt werden müssten, erschwert die Kenntniserlangung zusätzlich.

(2) Unverhältnismäßig ist angesichts dessen der Verzicht auf entsprechende Benachrichtigungspflichten. Die angegriffenen Vorschriften ordnen selbst keine Benachrichtigungspflichten für den automatisierten Lichtbildabruf an und solche Pflichten ergeben sich auch nicht aus dem Recht der Nachrichtendienste. Eine Benachrichtigung des Betroffenen von Datenerhebungen ist dort nur in besonderen Fällen vorgesehen, etwa bei Erhebungen aus Wohnungen, mittels besonderer Methoden oder durch Eingriffe in das Brief-, Post- und Fernmeldegeheimnis (vgl. § 9 Abs. 3 Nr. 1 BVerfSchG und die darauf verweisenden § 5 S. 2 BNDG und § 5 S. 2 MADG sowie § 12 Abs. 1 S. 1, Abs. 2 S. 1 G10). Darüber hinaus bestehen erhebliche Ausschlussstatbestände.

Es liegen keine Umstände vor, die das Fehlen von Benachrichtigungspflichten unter verfassungsrechtlichen Gesichtspunkten rechtfertigen. Im Hinblick auf den weit gefassten Anwendungsbereich und die niedrige Eingriffsschwelle der Befugnisse kann nicht ohne Weiteres davon ausgegangen werden, dass bei einer Benachrichtigung stets der Untersuchungszweck oder Rechtsgüter Dritter gefährdet würden. Auch ergibt sich aus der Funktionsweise des Lichtbildabrufs keine grundsätzlich substantielle Beeinträchtigung durch eine Benachrichtigungspflicht. Allein die Tatsache, dass der Abruf zur Aufgabenerfüllung durch die Nachrichtendienste erfolgt, vermag keine Abkehr vom Gebot der Transparenz unter

Entbindung von jeglichen Pflichten zur nachträglichen Benachrichtigung zu begründen.⁸² Soweit durchaus Umstände denkbar sind, die einer Benachrichtigung im Einzelfall entgegenstehen können, handelt es sich dabei um eben jene Ausnahmetatbestände, die für eine Eingriffsermächtigung solcher Breite gesetzlich zu normieren gewesen wären. Die geringe Transparenz und die damit einhergehenden äußerst eingeschränkten Möglichkeiten subjektiven Rechtsschutzes im Bereich nachrichtendienstlicher Maßnahmen sind auf deren Feld zugeschnitten und dürfen beim Zugriff auf Datensammlungen anderer Behörden nicht ohne entsprechende Anpassungen übertragen werden.

(3) Auch die Anforderungen an die Gewährleistung aufsichtlicher Kontrolle sind nicht erfüllt. Abrufe im automatisierten Verfahren werden gem. § 25 Abs. 2 S. 7 PAuswG bzw. § 22a Abs. 2 S. 8 PassG nur von der abrufenden Behörde protokolliert, was die faktischen Überprüfungsmöglichkeiten wesentlich einschränkt. Die standardmäßig und unabhängig von besonderen Umständen bloß einseitige Protokollierung greift insbesondere unter Berücksichtigung der Herkunft der Lichtbilddaten aus einer anlasslosen vorsorglichen Erhebung zu kurz. Mangels Protokollierung oder Kennzeichnung seitens der Erhebungsbehörde bleibt dieser Umstand nach dem zweckändernden Abruf nicht erkennbar. Die für solche Datenbestände geltende besondere Zweckbindung lässt sich in der Folge nicht gewährleisten.⁸³

Die Protokolle enthalten nach § 25 Abs. 2 S. 8 PAuswG bzw. § 22a Abs. 2 S. 9 PassG – und im Gegensatz zum herkömmlichen Ersuchen nach § 24 Abs. 3 S. 4 PAuswG bzw. § 22 Abs. 3 S. 4 PassG – keine Angaben zu Anlass oder Zweck des Zugriffs. Damit wird eine spätere Überprüfung erheblich erschwert.

Nicht angemessen sind weiter die Aufbewahrungsfristen für die Abrufprotokolle. Gem. § 24 Abs. 3 S. 5 in Verbindung mit § 25 Abs. 2 S. 9 PAuswG bzw. § 22 Abs. 3 S. 5 in Verbindung mit § 22a Abs. 2 S. 10 PassG sind die Protokolle am Ende des Kalenderjahres, das dem Jahr des Abrufs folgt, zu vernichten. Diese Frist ist zu kurz, um die bezüglich des automatisierten Verfahrens besonders bedeutsame aufsichtliche Kontrolle wirksam sicherzustellen. In dieser Zeit kann weder von einer Überprüfung durch die Datenschutzbeauftragte noch durch den Betroffenen ausgegangen werden.⁸⁴

Mindestabstände, in denen die datenschutzrechtliche Kontrolle durchzuführen ist, legen die angegriffenen Regelungen nicht fest. Damit ist eine effektive aufsichtliche Kontrolle –

⁸² Vgl. BVerfGE 125, 260 (337).

⁸³ Vgl. BVerfGE 125, 260 (333).

⁸⁴ Vgl. zur entsprechend kurzen Frist in § 20h Abs. 5 S. 10 BKAG a.F. BVerfGE 141, 220 (302 f.).

insbesondere angesichts der kurzen Aufbewahrungsfristen – nicht hinreichend gewährleistet.⁸⁵

II. Art. 19 Abs. 4 GG

Die angegriffenen Vorschriften verstoßen gegen Art. 19 Abs. 4 GG und die Garantie effektiven Rechtsschutzes.

Art. 19 Abs. 4 GG vermittelt einen Anspruch auf effektiven Schutz der grundrechtlich gewährleisteten subjektiven Rechte, vorliegend aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Zu gewährleisten ist eine tatsächlich wirksame gerichtliche Kontrolle. Die Rechtsschutzgarantie ist nicht erst zu einem spezifischen gerichtlichen Verfahren in Bezug zu setzen, sondern wirkt in das behördliche Verfahren hinein, um dort gleichsam im Vorfeld die praktischen Voraussetzungen für die Inanspruchnahme des Rechtswegs zu sichern.⁸⁶ Sofern die Effektivität des Rechtsschutzes die Offenlegung bestimmter Maßnahmen und Entscheidungen erfordert, ist der Anspruch auf diese Offenlegung von Art. 19 Abs. 4 GG umfasst.⁸⁷

Effektiver Rechtsschutz gegen heimliche Eingriffe in das Recht auf informationelle Selbstbestimmung setzt voraus, dass der Betroffene hiervon überhaupt Kenntnis erlangt.⁸⁸ Insofern ergibt sich aus Art. 19 Abs. 4 GG ein eigenständiger Anspruch der Beschwerdeführer, von den mit den angegriffenen Vorschriften einhergehenden Grundrechtseingriffen dergestalt Kenntnis zu erlangen, dass ihnen tatsächlicher gerichtlicher Rechtsschutz dagegen ermöglicht wird.

Die für eine wirksame Inanspruchnahme gerichtlichen Rechtsschutzes notwendigen Mindestanforderungen an Transparenz in Form von Auskunftsrechten und Benachrichtigungspflichten sind im Hinblick auf die Verhältnismäßigkeit der Ermächtigungen bereits ausgeführt worden (vgl. oben D. I. 4. lit. b hh). Die angegriffenen Vorschriften verfehlen diese Anforderungen auch unter den Gesichtspunkten der Garantie effektiven Rechtsschutzes. Es bestehen keine hinreichenden Auskunftsrechte und Benachrichtigungspflichten, die es den Beschwerdeführern ermöglichen würden, sich gegen die Maßnahmen wirksam zur Wehr zu setzen. Angesichts der niedrigen Eingriffsschwelle und des erheblichen, durch die vielfältigen Verwendungsmöglichkeiten und das einfache

⁸⁵ Vgl. BVerfGE 133, 277 (370); 141, 220 (321).

⁸⁶ BVerfGE 118, 168 (207).

⁸⁷ BVerfGE 101, 106 (123); BVerfGE 118, 168 (208).

⁸⁸ BVerfGE 118, 168 (207).

automatisierte Verfahren noch intensivierten Eingriffs sind ein solcher Verzicht auf rechtsschutzgewährende Vorkehrungen und der daraus resultierende insgesamt nur schwach ausgestaltete subjektive Rechtsschutz nicht mit den verfassungsrechtlichen Vorgaben in Einklang zu bringen.

Dr. Stolle
Rechtsanwalt