

Pressemitteilungen

Bundesverfassungsgericht - Pressestelle -**Pressemitteilung Nr. 31/2013 vom 24. April 2013**

Urteil vom 24. April 2013

[1 BvR 1215/07](#)

Antiterrordatei ist in ihren Grundstrukturen mit dem Grundgesetz vereinbar, nicht jedoch in ihrer Ausgestaltung im Einzelnen

Die Antiterrordatei ist in ihren Grundstrukturen verfassungsgemäß. Jedoch genügt sie hinsichtlich ihrer Ausgestaltung im Einzelnen den verfassungsrechtlichen Anforderungen nicht. Dies hat der Erste Senat des Bundesverfassungsgerichts in einem heute verkündeten Urteil entschieden. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, dürfen die verfassungswidrigen Vorschriften unter Maßgaben weiter angewendet werden.

Der Entscheidung liegen im Wesentlichen die folgenden Erwägungen zugrunde:

1. Der Beschwerdeführer wendet sich gegen das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz ATDG).

2. Die Verfassungsbeschwerde gibt keinen Anlass für ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof. Unzweifelhaft stellen das Antiterrordateigesetz und die Tätigkeit auf dessen Grundlage keine Durchführung des Rechts der Union im Sinne des Art. 51 Abs. 1 Satz 1 der Grundrechtecharta der Europäischen Union dar. Das Antiterrordateigesetz verfolgt innerstaatlich bestimmte Ziele, die das Funktionieren der unionsrechtlich geordneten Rechtsbeziehungen nur mittelbar beeinflussen können. Die europäischen Grundrechte sind daher von vornherein nicht anwendbar, und der Europäische Gerichtshof ist insoweit nicht gesetzlicher Richter im Sinne des Art. 101 Abs. 1 Satz 2 GG. Nichts anderes kann sich aus der Entscheidung des Europäischen Gerichtshofs in der Rechtssache Åkerberg Fransson (Urteil vom 26. Februar 2013, C-617/10) ergeben. Im Sinne eines kooperativen Miteinanders darf dieser Entscheidung keine Lesart unterlegt werden, nach der diese offensichtlich als Ultra-vires-Akt zu beurteilen wäre oder Schutz und Durchsetzung der mitgliedstaatlichen Grundrechte in einer Weise gefährdete, dass dies die Identität der durch das Grundgesetz errichteten Verfassungsordnung in Frage stellte. Der Senat geht davon aus, dass die in der EuGH-Entscheidung enthaltenen Aussagen auf Besonderheiten des Umsatzsteuerrechts beruhen, aber keine grundsätzliche Auffassung äußern. Die Entscheidung über diese Frage ist im Senat einstimmig ergangen.

3. Die Verfassungsbeschwerde ist teilweise begründet.

a) Die Antiterrordatei ist in ihren Grundstrukturen mit dem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG vereinbar.

aa) Der durch die angegriffenen Vorschriften geschaffene

Informationsaustausch ist von erheblichem Gewicht. Für die Betroffenen kann die Aufnahme in eine solche Datei erheblich belastende Wirkung haben.

Das Eingriffsgewicht wird dadurch erhöht, dass die Datei auch den Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden ermöglicht. Die Rechtsordnung unterscheidet zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung ausgerichtet und von detaillierten Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten, die auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt für den Datenaustausch zwischen diesen ein informationelles Trennungsprinzip. Soweit Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein operatives Tätigwerden ausgetauscht werden, handelt es sich um einen besonders schweren Eingriff. Dieser ist nur ausnahmsweise zulässig und muss einem herausragenden öffentlichen Interesse dienen. Hierbei dürfen die jeweiligen Eingriffsschwellen für die Erlangung der Daten nicht unterlaufen werden.

Das Eingriffsgewicht der Antiterrordatei wird jedoch dadurch gemindert, dass sie als Verbunddatei ausgestaltet ist, die sich in ihrem Kern auf die Informationsanbahnung durch bereits erhobene Daten beschränkt. Für die Übermittlung der Daten zur operativen Aufgabenwahrnehmung ist das einschlägige Fachrecht maßgeblich, das seinerseits den verfassungsrechtlichen Anforderungen und dem informationellen Trennungsprinzip genügen muss. Das Antiterrordateigesetz selbst berechtigt zu einem Austausch zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen.

bb) Straftaten mit dem Gepräge des Terrorismus, wie sie das Antiterrordateigesetz zum Bezugspunkt hat, richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Es ist Gebot unserer verfassungsrechtlichen Ordnung, solche Angriffe nicht als Krieg oder als Ausnahmezustand aufzufassen, der von der Beachtung rechtsstaatlicher Anforderungen dispensiert, sondern sie als Straftaten mit den Mitteln des Rechtsstaats zu bekämpfen. Dem entspricht umgekehrt, dass der Terrorismusbekämpfung im Rahmen der Verhältnismäßigkeitsabwägung ein erhebliches Gewicht beizumessen ist.

cc) Angesichts der sich gegenüberstehenden Interessen bestehen gegen die Grundstrukturen der Antiterrordatei keine verfassungsrechtlichen Bedenken. Allerdings entspricht die Regelung der Datei dem Verhältnismäßigkeitsgrundsatz im engeren Sinne nur, wenn sie hinsichtlich der zu erfassenden Daten sowie deren Nutzungsmöglichkeiten normenklar und in der Sache hinreichend begrenzt ausgestaltet ist sowie hierbei qualifizierte Anforderungen an die Kontrolle gestellt und beachtet werden.

b) Das Antiterrordateigesetz genügt diesen Maßstäben nicht vollständig.

aa) § 1 Abs. 2 ATDG, der die Beteiligung weiterer Polizeivollzugsbehörden an der Antiterrordatei nur nach weiten und wertungsoffenen Kriterien regelt, ist mit dem Bestimmtheitsgebot unvereinbar. Will der Gesetzgeber die Entscheidung über die beteiligten Behörden in die Hände der Exekutive legen, ist er vorliegend auf die Form der Rechtsverordnung verwiesen. Eine bloße Verwaltungsvorschrift reicht insoweit nicht.

bb) Nicht in jeder Hinsicht mit den verfassungsrechtlichen Anforderungen vereinbar sind die Vorschriften, die den von der Datei erfassten Personenkreis festlegen.

(1) Die Vorschrift des § 2 Satz 1 Nr. 1 ATDG erfasst zunächst Angehörige, Unterstützer und unterstützende Gruppierungen von terroristischen Vereinigungen. Sie erweitert diesen Kreis aber auf Personen, die eine unterstützende Gruppierung lediglich unterstützen, ohne klarzustellen, dass es sich um eine willentliche Unterstützung der den Terrorismus unterstützenden Aktivitäten handeln muss. Daher können Personen erfasst werden, die im Vorfeld und ohne Wissen von einem Terrorismusbezug eine in ihren Augen unverdächtige Vereinigung unterstützen. Dies verstößt gegen den Grundsatz der Normenklarheit und ist mit dem Übermaßverbot nicht vereinbar. Eine verfassungskonforme Auslegung scheidet hier aus.

(2) Nicht vollständig mit der Verfassung vereinbar ist auch § 2 Satz 1 Nr. 2 ATDG. Die Vorschrift, die Einzelpersonen erfassen soll, die möglicherweise in einer Nähe zum Terrorismus stehen, verbindet eine Reihe von mehrdeutigen und potenziell weiten Rechtsbegriffen.

Hinsichtlich der Begriffe der „rechtswidrigen Gewalt“ und des „vorsätzlichen Hervorrufens solcher Gewalt“ lässt sich eine Verfassungswidrigkeit wegen Stimmgleichheit im Senat nicht feststellen. Nach Auffassung der vier Mitglieder des Senats, die die Entscheidung insoweit tragen, ist die Verwendung dieser Merkmale mit dem Grundgesetz vereinbar, sofern ihnen keine übermäßig weite Bedeutung beigelegt wird und insbesondere unter Gewalt nur solche Gewalt verstanden wird, die unmittelbar gegen Leib und Leben gerichtet oder durch den Einsatz gemeingefährlicher Mittel geprägt ist. Nach der Auffassung der anderen vier Mitglieder des Senats müsste die Vorschrift wegen fehlender Bestimmtheit und übermäßiger Reichweite insgesamt für verfassungswidrig erklärt werden; eine verfassungskonforme Auslegung komme nicht in Betracht.

Das bloße „Befürworten von Gewalt“ im Sinne dieser Vorschrift reicht nach der einhelligen Auffassung des Senats für die Erfassung von Personen in der Antiterrordatei nicht. Die Vorschrift verstößt insoweit gegen das Übermaßverbot. Das Gesetz macht hier die subjektive Überzeugung als solche zum Maßstab und legt damit Kriterien zugrunde, die vom Einzelnen nur begrenzt beherrscht und durch rechtstreu Verhalten nicht beeinflusst werden können.

(3) Verfassungswidrig ist § 2 Satz 1 Nr. 3 ATDG. Nach dieser Regelung sind die einfachen Grunddaten in die Datei einzustellen, soweit Kontaktpersonen von einem Terrorismusbezug der Hauptperson nichts wissen, bei Kenntnis vom Terrorismusbezug auch die erweiterten Grunddaten. Infolgedessen erstreckt sich der Austausch von Klarinformationen zwischen den beteiligten Behörden auch auf Daten zu den Kontaktpersonen.

Die Regelung ist weder mit dem Bestimmtheitsgrundsatz noch mit dem Übermaßverbot vereinbar. Allerdings ist es verfassungsrechtlich nicht prinzipiell ausgeschlossen, Daten von Kontaktpersonen in der Antiterrordatei bereitzustellen. In der Regel sind solche Personen nur insoweit von Interesse, als sie Aufschluss über die als terrorismusnah geltende Hauptperson vermitteln können. Hieran muss sich auch die gesetzliche Ausgestaltung orientieren. Möglich wäre es insoweit, Kontaktpersonen mit wenigen Elementardaten zu erfassen und diese – als Information zu der terrorismusnahen Hauptperson – nur verdeckt recherchierbar zu speichern.

cc) Verfassungsrechtlich nicht zu beanstanden ist der in § 3 Abs. 1 Nr. 1 a und b ATDG geregelte Umfang der erfassten Daten. Hinsichtlich einiger dieser Daten ist es jedoch erforderlich, die administrativen Zwischenschritte für deren Konkretisierung zu dokumentieren und zu veröffentlichen.

Diese Dokumentations- und Veröffentlichungspflicht gilt für die sehr offen formulierten Merkmale in § 3 Abs. 1 Nr. 1 b gg, hh, ii, kk, nn ATDG (beispielsweise zur Erfassung terrorismusrelevanter Fähigkeiten). Auch sie genügen allerdings dem Bestimmtheitsgebot, da eine nähere Konkretisierung nur durch die Sicherheitsbehörden erfolgen kann. Der Gesetzgeber hat jedoch sicherzustellen, dass sie dokumentiert und veröffentlicht wird. Nach gegenwärtiger Praxis werden die in Frage stehenden unbestimmten Rechtsbegriffe durch einen – in das Computerprogramm eingebundenen – Katalog der zu speichernden Merkmale konkretisiert und standardisiert; die Bundesregierung hat dem Senat diesbezüglich ein „Katalog-Manual“ vorgelegt. Dessen Veröffentlichung ist im Antiterrordateigesetz aber nicht vorgeschrieben. Damit genügt die derzeitige Rechtslage den Anforderungen an eine rechtsstaatliche Ausgestaltung nicht.

Mit dem Übermaßverbot vereinbar ist das Freitextfeld (§ 3 Abs. 1 Nr. 1 b rr ATDG). Es handelt sich hierbei nicht um eine Blankovollmacht zur Ergänzung der Datei um beliebige weitere Informationen, sondern um eine Öffnung für Hinweise und Bewertungen, die durch die Standardisierung und Katalogisierung der Eingaben sonst nicht abgebildet werden.

dd) Nicht in jeder Hinsicht mit dem Übermaßverbot vereinbar sind die Regelungen zur Verwendung der Daten.

(1) Verfassungsrechtlich unbedenklich sind Abfrage und Nutzung in Bezug auf die einfachen Grunddaten geregelt. Gleiches gilt für Abfragen zu den erweiterten Grunddaten, soweit diese namensbezogen durchgeführt werden (§ 5 Abs. 1 Satz 1 und 3 in Verbindung mit § 3 Abs. 1 Nr. 1 b ATDG). Hierbei erhält die Behörde nicht Zugang auf die erweiterten Grunddaten selbst, sondern nur eine Treffermeldung verbunden mit dem Nachweis, bei welcher Behörde und unter welchem Aktenzeichen entsprechende Informationen geführt werden. Der Zugriff unmittelbar auf die erweiterten Grunddaten wird erst auf Einzellersuchen nach Maßgabe des Fachrechts durch Freischaltung seitens der informationsführenden Behörde ermöglicht.

(2) Mit dem Übermaßverbot nicht vereinbar ist die Regelung zur sogenannten Inverssuche (§ 5 Abs. 1 Satz 2 Nr. 1 a ATDG). Hierbei handelt es sich um merkmalsbezogene Recherchen in den erweiterten Grunddaten, die der abfragenden Behörde im Trefferfall nicht nur eine Fundstelle zu weiterführenden Informationen vermitteln, sondern unmittelbar Zugang zu den entsprechenden einfachen Grunddaten verschaffen. So kann eine Behörde zum Beispiel nach Personen mit einer bestimmten Religionszugehörigkeit und Ausbildung, die einen bestimmten Treffpunkt frequentieren, suchen und erhält im Trefferfall nicht nur die Angabe, welche Behörde darüber Informationen besitzt, sondern auch die Namen, Adressen sowie weitere Grundinformationen von allen Personen, auf die die abgefragten Merkmale zutreffen. Eine solch weitgehende Nutzung trägt der inhaltlichen Reichweite der erweiterten Grunddaten nicht hinreichend Rechnung. Wenn sich eine Recherche auch auf erweiterte Grunddaten erstreckt, dürfen nur das Aktenzeichen und die informationsführende Behörde angezeigt werden, nicht aber auch die korrespondierenden einfachen Grunddaten.

(3) Keinen verfassungsrechtlichen Bedenken, auch nicht für den Fall einer Inverssuche, unterliegt die Nutzung der erweiterten Grunddaten im Eilfall (§ 5 Abs. 2 in Verbindung mit § 6 Abs. 2 ATDG). Die Voraussetzungen, unter denen eine solche Nutzung erlaubt ist, sind hinreichend eng gefasst, um den Eingriff zu rechtfertigen. Die Vorschrift genügt dem Übermaßverbot und hat auch Bestand vor dem informationellen Trennungsprinzip.

ee) Das Antiterrordateigesetz gewährleistet eine Transparenz

hinsichtlich des Informationsaustauschs – bedingt durch Zweck und Funktionsweise der Datei – nur in begrenztem Umfang. Damit sind den Betroffenen nur eingeschränkte Rechtsschutzmöglichkeiten eröffnet. Dies ist mit der Verfassung vereinbar, wenn für die effektive Ausgestaltung der Aufsicht verfassungsrechtliche Maßgaben beachtet werden. So müssen die Aufsichtsinstanzen auf Bundes- wie auf Landesebene – wie nach geltendem Recht die Datenschutzbeauftragten – mit wirksamen Befugnissen ausgestattet sein. Zugriffe und Änderungen im Datenbestand müssen vollständig protokolliert und den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung gestellt werden. Kontrollen sind in angemessenen Abständen durchzuführen, deren Dauer ein gewisses Höchstmaß – etwa zwei Jahre – nicht überschreiten darf. Hinsichtlich des Erfordernisses turnusmäßig festgelegter Pflichtkontrollen fehlt es an einer hinreichenden gesetzlichen Vorgabe; den Gesetzgeber trifft insoweit eine Nachbesserungspflicht. Im Übrigen sind die Vorschriften verfassungskonform auszulegen. Der Gesetzgeber hat im Übrigen zu beobachten, ob Konflikte auftreten, die gesetzlicher Klarstellungen oder der Einführung etwa von Streitlösungsmechanismen wie dem Ausbau von Klagebefugnissen bedürfen.

ff) Zur Gewährleistung von Transparenz und Kontrolle bedarf es schließlich einer gesetzlichen Regelung von Berichtspflichten. Regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit über Datenbestand und Nutzung der Antiterrordatei sind sicherzustellen.

c) Die gesetzlich vorgesehene vollständige und uneingeschränkte Einbeziehung aller auch durch Eingriff in Art. 10 Abs. 1 (Telekommunikationsgeheimnis) und in Art. 13 Abs. 1 GG (Unverletzlichkeit der Wohnung) erhobenen Daten in die Antiterrordatei ist mit der Verfassung nicht vereinbar. Angesichts des besonderen Schutzgehalts gelten für Datenerhebungen, die in diese Grundrechte eingreifen, in der Regel besonders strenge Anforderungen. Durch die uneingeschränkte Einstellung auch solcher Daten in die Antiterrordatei werden die Informationen unabhängig von bereits geschehenen oder bevorstehenden Terrorakten für Ermittlungsmaßnahmen noch im Vorfeld greifbarer Gefahrenlagen zur Verfügung gestellt, obwohl hierfür eine Datenerhebung unter Eingriffen in das Telekommunikationsgeheimnis oder die Unverletzlichkeit der Wohnung nicht gerechtfertigt werden könnte. Dies unterläuft die entsprechenden Datenerhebungsanforderungen.

Demgegenüber wäre eine Regelung, die für solche Daten stets eine verdeckte Speicherung gemäß § 4 ATDG vorsieht, unter Verhältnismäßigkeitsgesichtspunkten mit der Verfassung vereinbar. Die entsprechenden Informationen würden bei einer solchen Regelung nur nach Maßgabe der fachrechtlichen Übermittlungsvorschriften zugänglich gemacht, die dann ihrerseits verfassungsrechtlich gebotene qualifizierte Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz sicherstellen könnten.

4. Die teilweise Verfassungswidrigkeit der angegriffenen Vorschriften führt nicht zu deren Nichtigkeitserklärung, sondern nur zur Feststellung ihrer Unvereinbarkeit mit dem Grundgesetz. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, dürfen die Vorschriften weiter angewendet werden. Vor deren weiteren Anwendbarkeit ist allerdings zunächst die Beachtung bestimmter Maßgaben sicherzustellen.

Zum [ANFANG](#) des Dokuments

Entscheidungen

Zitierung: BVerfG, 1 BvR 1215/07 vom 24.4.2013, Absatz-Nr. (1 - 233), http://www.bverfg.de/entscheidungen/rs20130424_1bvr121507.html
Frei für den nicht gewerblichen Gebrauch. Kommerzielle Nutzung nur mit Zustimmung des Gerichts.

Leitsätze

zum Urteil des Ersten Senats vom 24. April 2013

1 BvR 1215/07

1. Die Errichtung der Antiterrordatei als Verbunddatei verschiedener Sicherheitsbehörden zur Bekämpfung des internationalen Terrorismus, die im Kern auf die Informationsanbahnung beschränkt ist und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsieht, ist in ihren Grundstrukturen mit der Verfassung vereinbar.
2. Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendienste ermöglichen, unterliegen hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderungen. Aus den Grundrechten folgt ein informationelles Trennungsprinzip, das diesen Austausch nur ausnahmsweise zulässt.
3. Eine Verbunddatei zwischen Sicherheitsbehörden wie die Antiterrordatei bedarf hinsichtlich der zu erfassenden Daten und ihrer Nutzungsmöglichkeiten einer hinreichend bestimmten und dem Übermaßverbot entsprechenden gesetzlichen Ausgestaltung. Das Antiterrordateigesetz genügt dem nicht vollständig, nämlich hinsichtlich der Bestimmung der beteiligten Behörden, der Reichweite der als terrorismusnah erfassten Personen, der Einbeziehung von Kontaktpersonen, der Nutzung von verdeckt bereitgestellten erweiterten Grunddaten, der Konkretisierungsbefugnis der Sicherheitsbehörden für die zu speichernden Daten und der Gewährleistung einer wirksamen Aufsicht.
4. Die uneingeschränkte Einbeziehung von Daten in die Antiterrordatei, die durch Eingriffe in das Brief- und Fernmeldegeheimnis und das Recht auf Unverletzlichkeit der Wohnung erhoben wurden, verletzt Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 1215/07 -



Verkündet
am 24. April 2013
Sommer
Regierungshauptsekretärin
als Urkundsbeamtin
der Geschäftsstelle

Im Namen des Volkes

**In dem Verfahren
über
die Verfassungsbeschwerde**

des Herrn S...,

- Bevollmächtigter:
Rechtsanwalt Maximilian Suermann,
Braunschweiger Straße 57, 12055 Berlin -

gegen das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von
Polizeibehörden und Nachrichtendiensten von Bund und Ländern
(Antiterrordateigesetz - ATDG) vom 22. Dezember 2006 (BGBl I S. 3409)

hat das Bundesverfassungsgericht - Erster Senat - unter Mitwirkung der Richterinnen und Richter

Vizepräsident Kirchhof,
Gaier,
Eichberger,

Schluckebier,
Masing,
Paulus,
Baer,
Britz

aufgrund der mündlichen Verhandlung vom 6. November 2012 durch

Urteil

für Recht erkannt:

1. a) § 1 Absatz 2 und § 2 Satz 1 Nummer 3 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22. Dezember 2006 (Bundesgesetzblatt I Seite 3409) sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.
b) § 2 Satz 1 Nummer 1 Buchstabe b hinsichtlich des Unterstützens einer unterstützenden Gruppierung und § 2 Satz 1 Nummer 2 des Antiterrordateigesetzes hinsichtlich des Merkmals „Befürworten“ sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.
c) § 5 Absatz 1 Satz 2 Nummer 1 a des Antiterrordateigesetzes ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes insoweit unvereinbar, als bei Recherchen in den erweiterten Grunddaten im Trefferfall Zugriff auf Informationen gemäß § 3 Absatz 1 Nummer 1 a des Antiterrordateigesetzes eröffnet wird.
d) § 3 Absatz 1 Satz 1 Nummer 1 b und § 10 Absatz 1 des Antiterrordateigesetzes sind, soweit es an ergänzenden Regelungen nach Maßgabe der Gründe fehlt, mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar.
e) § 2 Satz 1 Nummer 2 und § 10 Absatz 1 des Antiterrordateigesetzes sind im Übrigen nach Maßgabe der Gründe verfassungskonform auszulegen.
2. § 2 Satz 1 Nummern 1 bis 3, § 3 Absatz 1 Nummer 1, § 5 Absatz 1 und 2 sowie § 6 Absatz 1 und 2 des Antiterrordateigesetzes sind mit Artikel 10 Absatz 1 und Artikel 13 Absatz 1 des Grundgesetzes unvereinbar, soweit sie sich auf nicht gemäß § 4 des Antiterrordateigesetzes verdeckt gespeicherte Daten erstrecken, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren.
3. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014 gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass außerhalb des Eilfalls gemäß § 5 Absatz 2 des Antiterrordateigesetzes eine Nutzung der Antiterrordatei nur zulässig ist, sofern der Zugriff auf die Daten von Kontaktpersonen (§ 2 Satz 1 Nummer 3 des Antiterrordateigesetzes) und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen und gewährleistet ist, dass bei Recherchen in den erweiterten Grunddaten im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Absatz 1 Nummer 3 des Antiterrordateigesetzes gewährt wird; sobald danach die Möglichkeit des Zugriffs auf die Daten von Kontaktpersonen und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen ist, dürfen diese auch für die Nutzung der Datei im Eilfall gemäß § 5 Absatz 2 des Antiterrordateigesetzes nicht mehr genutzt werden.
4. Im Übrigen wird die Verfassungsbeschwerde zurückgewiesen.
5. Die Bundesrepublik Deutschland hat dem Beschwerdeführer seine notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

Gründe:

A.

Gegenstand der Verfassungsbeschwerde ist die Verfassungsmäßigkeit des Antiterrordateigesetzes.

1

I.

2

Der Beschwerdeführer wendet sich gegen das als Art. 1 des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) vom 22. Dezember 2006 (BGBl I S. 3409) erlassene Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG). Das Antiterrordateigesetz wurde seit seinem Inkrafttreten am 31. Dezember 2006 nicht substantiell geändert. Bei sachgerechtem Verständnis des Beschwerdevorbringens wendet sich der Beschwerdeführer unmittelbar gegen die §§ 1 bis 6 ATDG über die Speicherung und Verwendung von Daten; ausgenommen ist insoweit allerdings § 2 Satz 1 Nr. 4 ATDG. Mittelbar richtet sich die Verfassungsbeschwerde auch gegen die diese Vorschriften flankierenden §§ 8 bis 12 ATDG, die insbesondere die datenschutzrechtliche Verantwortung und Kontrolle betreffen.

3

1. Durch das Antiterrordateigesetz wurde die Rechtsgrundlage für die Antiterrordatei, eine der Bekämpfung des internationalen Terrorismus dienende Verbunddatei von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder, geschaffen. Die Datei erleichtert und beschleunigt den Informationsaustausch zwischen den beteiligten Polizeibehörden und Nachrichtendiensten, indem bestimmte Erkenntnisse aus dem Zusammenhang der Bekämpfung des internationalen Terrorismus, über die einzelne Behörden verfügen, für alle beteiligten Behörden schneller auffindbar und leichter zugänglich werden.

4

a) § 1 ATDG legt zum einen fest, dass die Antiterrordatei als gemeinsame standardisierte zentrale Datei beim Bundeskriminalamt geführt wird, und bestimmt zugleich die an ihr beteiligten Behörden. Nach § 1 Abs. 1 ATDG sind das Bundeskriminalamt, in Verbindung mit § 58 Abs. 1 BPolG, § 1 Abs. 3 Nr. 1 d BPolZV das Bundespolizeipräsidium, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt beteiligte Behörden. Neben diesen von Gesetzes wegen beteiligten Behörden können nach § 1 Abs. 2 ATDG in Verbindung mit § 12 Nr. 2 ATDG durch Errichtungsanordnung unter bestimmten Voraussetzungen weitere Polizeivollzugsbehörden an der Antiterrordatei beteiligt werden. Nach der Gesetzesbegründung sollen dies in erster Linie die Dienststellen des polizeilichen Staatsschutzes der Länder sein (BTDrucks 16/2950, S. 14). Ausweislich der Errichtungsanordnung mit Stand vom 4. Juni 2010 haben in drei Bundesländern polizeiliche Dienststellen unterhalb der Ebene der Landeskriminalämter Zugriff auf die Antiterrordatei.

5

b) In § 2 ATDG wird bestimmt, dass und in Bezug auf welche Personen oder Objekte Behörden verpflichtet sind, bereits erhobene Daten in der Antiterrordatei zu speichern. Voraussetzung einer Speicherung ist zunächst, dass polizeiliche oder nachrichtendienstliche Erkenntnisse vorliegen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass sich die Daten auf die in § 2 Satz 1 Nr. 1 bis 4 ATDG genannten Personen oder Objekte beziehen und dass die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zu Deutschland erforderlich ist. Von der Speicherung betroffen sind nach Nr. 1 zunächst Personen, die Vereinigungen oder Gruppierungen des internationalen Terrorismus angehören oder in einer besonderen Nähe dazu stehen. Darüber hinaus sind nach Nr. 2 auch Einzelpersonen von der Speicherung betroffen, sofern sie rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteteter politischer oder religiöser Belange anwenden, unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen. Nr. 3 sieht schließlich auch die Speicherung der Daten von Kontaktpersonen zu den in Nr. 1 und 2 genannten Personen vor, sofern der Kontakt nicht nur flüchtiger oder zufälliger Art ist und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind.

6

c) Welche Daten über die in § 2 Satz 1 Nr. 1 bis 4 ATDG genannten Personen und Objekte zu speichern sind, ergibt sich aus § 3 Abs. 1 ATDG. Die Regelung differenziert dabei zwischen den in § 3 Abs. 1 Nr. 1 a ATDG aufgeführten Grunddaten (im Folgenden zur Verdeutlichung auch als einfache Grunddaten bezeichnet) und den in § 3 Abs. 1 Nr. 1 b ATDG aufgeführten erweiterten Grunddaten.

7

Die einfachen Grunddaten sind zu allen in § 2 Satz 1 Nr. 1 bis 3 ATDG genannten Personengruppen zu speichern. Als solche Grunddaten definiert die Vorschrift verschiedene allgemeine Angaben zur Person, wie Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder sowie die Bezeichnung der Fallgruppe nach § 2 ATDG. Demgegenüber verlangt § 3 Abs. 1 Nr. 1 b ATDG eine Speicherung der erweiterten Grunddaten nur zu den in § 2 Satz 1 Nr. 1 und 2 ATDG genannten Personen sowie zu Kontaktpersonen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie von terrorismusbezogenen Aktivitäten Kenntnis haben. Die erweiterten Grunddaten werden im Einzelnen in § 3 Abs. 1 Nr. 1 b aa bis rr

ATDG aufgezählt. Dazu zählen unter anderem Angaben wie Telekommunikationsanschlüsse und Telekommunikationsendgeräte (aa), Bankverbindungen (bb), Volkszugehörigkeit (gg), Angaben zur Religionszugehörigkeit (hh), terrorismusrelevante Fähigkeiten (ii), Angaben zur Ausbildung (jj), Angaben zu Tätigkeiten in wichtigen Infrastruktureinrichtungen (kk), Angaben zu Gewaltbereitschaft (ll) oder zu besuchten Orten und Gebieten, die als Treffpunkt terrorismusverdächtiger Personen dienen (nn).

8

Nach der Gesetzesbegründung sollen die Daten, soweit der Art der Daten nach möglich, standardisiert gespeichert werden. Die Daten sollen also nicht freihändig, sondern durch Auswahl bestimmter systemseitig vorgegebener Angaben eingestellt werden. Diese Standardisierung soll die Recherchefähigkeit der Datei sichern und der Vereinheitlichung der Verwaltungspraxis dienen (BTDrucks 16/2950, S. 17). Ein Korrektiv zur weitgehenden Standardisierung der gespeicherten Angaben bietet die durch § 3 Abs. 1 Nr. 1 b rr ATDG ermöglichte Eingabe besonderer Bemerkungen, ergänzender Hinweise und Bewertungen als Freitext.

9

Neben den Grunddaten und erweiterten Grunddaten sieht § 3 Abs. 1 Nr. 3 ATDG Angaben zur einspeichernden Behörde und zu deren Aktenzeichen vor, wodurch die Kontaktaufnahme für den weiteren Informationsaustausch erleichtert werden soll.

10

Soweit besondere Geheimhaltungsinteressen oder schutzwürdige Interessen des Betroffenen dies erfordern, ermöglicht § 4 ATDG die beschränkte oder verdeckte Speicherung von Daten. Bei der verdeckten Speicherung werden die Daten so eingegeben, dass die anderen beteiligten Behörden das Vorhandensein der Daten bei Abfragen nicht erkennen und unmittelbar keinen Zugriff auf die gespeicherten Daten erhalten. Die Abfrage wird dann automatisiert an die informationsführende Behörde weitergeleitet, damit diese nach Maßgabe der gesetzlichen Vorschriften aus eigenem Entschluss mit der abfragenden Behörde Kontakt aufnimmt und über die Übermittlung der Daten entscheidet. Dies sollte zunächst dem Quellenschutz der jeweiligen Ermittlungsbehörden dienen, insbesondere der Geheimdienste bei ihrer Zusammenarbeit mit ausländischen Geheimdiensten. Im Lauf des Gesetzgebungsverfahrens ist der Schutz der Betroffenen als eigener Zweck hinzugekommen (vgl. BTDrucks 16/3642, S. 6).

11

d) In § 5 Abs. 1 ATDG ist der Zugriff auf die gespeicherten Daten im Regelfall normiert. § 5 Abs. 1 Satz 1 ATDG erlaubt den beteiligten Behörden Abfragen im automatisierten Verfahren, wenn dies im Rahmen ihrer Aufgaben zur Bekämpfung oder Aufklärung des internationalen Terrorismus erforderlich ist. Durch diese Zugriffsbefugnis, die nicht auf eine Suche nach einem bestimmten Namen begrenzt ist, wird den abfragenden Behörden eine Recherche in allen offen und verdeckt gespeicherten Datensätzen sowohl der Grunddaten als auch der erweiterten Grunddaten einschließlich des Freitextfeldes ermöglicht. Im Falle eines Treffers erhält die abfragende Behörde bei einer Abfrage zu Personen Zugriff auf die Grunddaten sowie die Angaben zur einspeichernden Behörde. Zugriff auf die erweiterten Grunddaten erhält die abfragende Behörde im Falle eines Treffers gemäß § 5 Abs. 1 Satz 3 und 4 ATDG nur, wenn die Behörde, die die Daten eingegeben hat, den Zugriff im Einzelfall auf Ersuchen nach den jeweils geltenden Übermittlungsvorschriften gewährt. Auch bei Recherchen in den erweiterten Grunddaten werden im Trefferfall aber hiervon unabhängig ohne weiteres die korrespondierenden einfachen Grunddaten übermittelt.

12

Nach § 6 Abs. 1 Satz 1 ATDG darf die abfragende Behörde die Daten, auf die sie gemäß § 5 Abs. 1 ATDG Zugriff erhalten hat, nur zur Prüfung, ob der Treffer der gesuchten Person zuzuordnen ist, sowie zur Vorbereitung und Substantiierung eines Einzelübermittlungersuchens verwenden.

13

e) § 5 Abs. 2 Satz 1 ATDG ermöglicht der abfragenden Behörde, im Eilfall unmittelbar auf die erweiterten Grunddaten eines Treffers Zugriff zu nehmen. Ein Eilfall im Sinne dieser Vorschrift setzt voraus, dass ein solcher Zugriff zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann. Die Entscheidung hierüber trifft der Leiter oder ein besonders beauftragter Beamter des höheren Dienstes der abfragenden Behörde. Der Zugriff bedarf im Übrigen der nachträglichen Zustimmung der Behörde, die die Daten eingegeben hat; diese entscheidet zugleich über die weitere Verwendbarkeit der Daten.

14

Hat die abfragende Behörde im Eilfall Zugriff auf Daten erhalten, erlaubt § 6 Abs. 2 ATDG die Verwendung dieser Daten nur, soweit dies zur Abwehr einer gegenwärtigen Gefahr im Zusammenhang mit der Bekämpfung des internationalen Terrorismus unerlässlich ist. Haben das Bundeskriminalamt oder ein Landeskriminalamt auf Ersuchen oder im Auftrag des Generalbundesanwalts die Antiterrordatei genutzt, übermitteln sie nach § 6 Abs. 4 Satz 1 und 2 ATDG die Daten dem Generalbundesanwalt für die Zwecke

der Strafverfolgung; der Generalbundesanwalt darf die Daten für ein Ersuchen um die Übermittlung von Erkenntnissen zur Aufklärung oder Bekämpfung des internationalen Terrorismus nach § 6 Abs. 1 Satz 1 ATDG verwenden.

15

In § 7 ATDG ist festgelegt, dass sich die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 ATDG nach den jeweils geltenden Übermittlungsvorschriften richtet.

16

f) § 8 ATDG teilt die datenschutzrechtliche Verantwortung zwischen einspeichernder und abfragender Behörde auf. Letztere trägt die Verantwortung für die Zulässigkeit der Abfrage, erstere die Verantwortung für die Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten. § 9 ATDG sieht eine Protokollierung aller Zugriffe auf die Daten zum Zweck der Datenschutzkontrolle vor. Diese ist gemäß § 10 Abs. 1 ATDG in die Hände der Datenschutzbeauftragten des Bundes und - nach Maßgabe des Landesrechts - der Länder gelegt.

17

In § 10 Abs. 2 ATDG ist die Auskunftserteilung an Betroffene geregelt. Die Regelung differenziert zwischen den offen und den verdeckt gespeicherten Daten. Gemäß § 10 Abs. 2 Satz 1 ATDG erteilt über die offen gespeicherten Daten das Bundeskriminalamt die Auskunft nach § 19 BDSG, wobei es das Einvernehmen der jeweils datenverantwortlichen Behörde einholt. Dagegen richtet sich die Auskunft zu verdeckt gespeicherten Daten gemäß § 10 Abs. 2 Satz 2 ATDG nach den Rechtsvorschriften für die Behörde, die die Daten eingegeben hat. Das bedeutet, dass die Betroffenen Auskunft zu einer etwaigen verdeckten Speicherung nicht zentral beim Bundeskriminalamt erhalten können, sondern nur jeweils bei der Behörde, die die Daten verdeckt gespeichert hat.

18

In § 11 ATDG sind schließlich Vorgaben zur Berichtigung, Löschung und Sperrung von Daten enthalten, während § 12 ATDG regelt, welche Einzelheiten das Bundeskriminalamt in einer Errichtungsanordnung festzulegen hat, wobei diese der Zustimmung des Bundesministeriums des Innern, des Bundeskanzleramts, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen und der für die beteiligten Behörden zuständigen obersten Landesbehörden bedarf. Hierzu gehören die Bestimmung der weiteren beteiligten Polizeivollzugsbehörden nach § 1 Abs. 2 ATDG, Einzelheiten zur Art der nach § 3 Abs. 1 ATDG zu speichernden Daten und zu den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden.

19

g) Das Antiterrordateigesetz ist gemäß Art. 5 Abs. 2 Halbsatz 1 Gemeinsame-Dateien-Gesetz befristet und tritt mit Ablauf des 30. Dezember 2017 außer Kraft. Es ist nach Art. 5 Abs. 2 Halbsatz 2 Gemeinsame-Dateien-Gesetz fünf Jahre nach seinem Inkrafttreten zu evaluieren.

20

2. Die Vorschriften des Antiterrordateigesetzes vom 22. Dezember 2006 (BGBl I S. 3409), das durch Artikel 5 des Gesetzes vom 26. Februar 2008 (BGBl I S. 215) geändert worden ist, lauten - soweit hier von Interesse - wie folgt:

21

§ 1 Antiterrordatei

(1) Das Bundeskriminalamt, die in der Rechtsverordnung nach § 58 Abs. 1 des Bundespolizeigesetzes bestimmte Bundespolizeibehörde, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt (beteiligte Behörden) führen beim Bundeskriminalamt zur Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland eine gemeinsame standardisierte zentrale Antiterrordatei (Antiterrordatei).

(2) Zur Teilnahme an der Antiterrordatei sind als beteiligte Behörden im Benehmen mit dem Bundesministerium des Innern weitere Polizeivollzugsbehörden berechtigt, soweit

1. diesen Aufgaben zur Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland nicht nur im Einzelfall besonders zugewiesen sind,

2. ihr Zugriff auf die Antiterrordatei für die Wahrnehmung der Aufgaben nach Nummer 1 erforderlich und dies unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Sicherheitsinteressen der beteiligten Behörden angemessen ist.

22

§ 2 Inhalt der Antiterrordatei und Speicherungspflicht

Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Abs. 1 in der Antiterrordatei zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich beziehen auf

1. Personen, die

a) einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, die einen internationalen Bezug aufweist, oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Abs. 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland oder

b) einer Gruppierung, die eine Vereinigung nach Buchstabe a unterstützt, angehören oder diese unterstützen,

2. Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen,

3. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in Nummer 1 Buchstabe a oder in Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (Kontaktpersonen), oder

4. (...)

und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland erforderlich ist. Satz 1 gilt nur für Daten, die die beteiligten Behörden nach den für sie geltenden Rechtsvorschriften automatisiert verarbeiten dürfen.

23

§ 3 Zu speichernde Datenarten

(1) In der Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. zu Personen

a) nach § 2 Satz 1 Nr. 1 bis 3: der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),

b) nach § 2 Satz 1 Nr. 1 und 2 sowie zu Kontaktpersonen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie von der Planung oder Begehung einer in § 2 Satz 1 Nr. 1 Buchstabe a genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne von § 2 Satz 1 Nr. 2 Kenntnis haben, folgende weiteren Datenarten (erweiterte Grunddaten):

aa) eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,

bb) Adressen für elektronische Post,

cc) Bankverbindungen,

dd) Schließfächer,

ee) auf die Person zugelassene oder von ihr genutzte Fahrzeuge,

ff) Familienstand,

gg) Volkszugehörigkeit,

hh) Angaben zur Religionszugehörigkeit, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind,

- ii) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und Durchführung terroristischer Straftaten nach § 129a Abs. 1 und 2 des Strafgesetzbuchs dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,
- jj) Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf,
- kk) Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Abs. 5 des Sicherheitsüberprüfungsgesetzes oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude,
- ll) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zur Gewaltbereitschaft der Person,
- mm) Fahr- und Flugerlaubnisse,
- nn) besuchte Orte oder Gebiete, an oder in denen sich in § 2 Satz 1 Nr. 1 und 2 genannte Personen treffen,
- oo) Kontaktpersonen nach § 2 Satz 1 Nr. 3 zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2,
- pp) die Bezeichnung der konkreten Vereinigung oder Gruppierung nach § 2 Satz 1 Nr. 1 Buchstabe a oder b,
- qq) der Tag, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet, und
- rr) auf tatsächlichen Anhaltspunkten beruhende zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen zu Grunddaten und erweiterten Grunddaten, die bereits in Dateien der beteiligten Behörden gespeichert sind, sofern dies im Einzelfall nach pflichtgemäßem Ermessen geboten und zur Aufklärung oder Bekämpfung des internationalen Terrorismus unerlässlich ist,

2. (...)

3. zu den jeweiligen Daten nach den Nummern 1 und 2 die Angabe der Behörde, die über die Erkenntnisse verfügt, sowie das zugehörige Aktenzeichen oder sonstige Geschäftszeichen und, soweit vorhanden, die jeweilige Einstufung als Verschlusssache.

(2) Soweit zu speichernde Daten aufgrund einer anderen Rechtsvorschrift zu kennzeichnen sind, ist diese Kennzeichnung bei der Speicherung der Daten in der Antiterrordatei aufrechtzuerhalten.

24

§ 4 Beschränkte und verdeckte Speicherung

(1) Soweit besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen des Betroffenen dies ausnahmsweise erfordern, darf eine beteiligte Behörde entweder von einer Speicherung der in § 3 Abs. 1 Nr. 1 Buchstabe b genannten erweiterten Grunddaten ganz oder teilweise absehen (beschränkte Speicherung) oder alle jeweiligen Daten zu in § 2 genannten Personen, Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post in der Weise eingeben, dass die anderen beteiligten Behörden im Falle einer Abfrage die Speicherung der Daten nicht erkennen und keinen Zugriff auf die gespeicherten Daten erhalten (verdeckte Speicherung). Über beschränkte und verdeckte Speicherungen entscheidet der jeweilige Behördenleiter oder ein von ihm besonders beauftragter Beamter des höheren Dienstes.

(2) Sind Daten, auf die sich eine Abfrage bezieht, verdeckt gespeichert, wird die Behörde, die die Daten eingegeben hat, automatisiert durch Übermittlung aller Anfragedaten über die Abfrage unterrichtet und hat unverzüglich mit der abfragenden Behörde Kontakt aufzunehmen, um zu klären, ob Erkenntnisse nach § 7 übermittelt werden können. Die Behörde, die die Daten eingegeben hat, sieht von einer Kontaktaufnahme nur ab, wenn Geheimhaltungsinteressen auch nach den Umständen des Einzelfalls überwiegen. Die wesentlichen Gründe für die Entscheidung nach Satz 2 sind zu dokumentieren. Die übermittelten Anfragedaten

sowie die Dokumentation nach Satz 3 sind spätestens zu löschen oder zu vernichten, wenn die verdeckt gespeicherten Daten zu löschen sind.

25

§ 5 Zugriff auf die Daten

(1) Die beteiligten Behörden dürfen die in der Antiterrordatei gespeicherten Daten im automatisierten Verfahren nutzen, soweit dies zur Erfüllung der jeweiligen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich ist. Im Falle eines Treffers erhält die abfragende Behörde Zugriff

1. a) bei einer Abfrage zu Personen auf die zu ihnen gespeicherten Grunddaten oder
- b) bei einer Abfrage zu Vereinigungen, Gruppierungen, Stiftungen, Unternehmen, Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüssen, Telekommunikationsendgeräten, Internetseiten oder Adressen für elektronische Post nach § 2 Satz 1 Nr. 4 auf die dazu gespeicherten Daten, und
2. auf die Daten nach § 3 Abs. 1 Nr. 3.

Auf die zu Personen gespeicherten erweiterten Grunddaten kann die abfragende Behörde im Falle eines Treffers Zugriff erhalten, wenn die Behörde, die die Daten eingegeben hat, dies im Einzelfall auf Ersuchen gewährt. Die Entscheidung hierüber richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

(2) Die abfragende Behörde darf im Falle eines Treffers unmittelbar auf die erweiterten Grunddaten zugreifen, wenn dies aufgrund bestimmter Tatsachen zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann (Eilfall). Ob ein Eilfall vorliegt, entscheidet der Behördenleiter oder ein von ihm besonders beauftragter Beamter des höheren Dienstes. Die Entscheidung und ihre Gründe sind zu dokumentieren. Der Zugriff ist unter Hinweis auf die Entscheidung nach Satz 3 zu protokollieren. Die Behörde, die die Daten eingegeben hat, muss unverzüglich um nachträgliche Zustimmung ersucht werden. Wird die nachträgliche Zustimmung verweigert, ist die weitere Verwendung dieser Daten unzulässig. Die abfragende Behörde hat die Daten unverzüglich zu löschen oder nach § 11 Abs. 3 zu sperren. Sind die Daten einem Dritten übermittelt worden, ist dieser unverzüglich darauf hinzuweisen, dass die weitere Verwendung der Daten unzulässig ist.

(3) Innerhalb der beteiligten Behörden erhalten ausschließlich hierzu ermächtigte Personen Zugriff auf die Antiterrordatei.

(4) Bei jeder Abfrage müssen der Zweck und die Dringlichkeit angegeben und dokumentiert werden und erkennbar sein.

26

§ 6 Weitere Verwendung der Daten

(1) Die abfragende Behörde darf die Daten, auf die sie Zugriff erhalten hat, nur zur Prüfung, ob der Treffer der gesuchten Person oder der gesuchten Angabe nach § 2 Satz 1 Nr. 4 zuzuordnen ist, und für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus verwenden. Eine Verwendung zu einem anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus ist nur zulässig, soweit

1. dies zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person erforderlich ist, und
2. die Behörde, die die Daten eingegeben hat, der Verwendung zustimmt.

(2) Im Eilfall darf die abfragende Behörde die Daten, auf die sie Zugriff erhalten hat, nur verwenden, soweit dies zur Abwehr der gegenwärtigen Gefahr nach § 5 Abs. 2 Satz 1 im Zusammenhang mit der Bekämpfung des internationalen Terrorismus unerlässlich ist.

(3) Im Falle einer Verwendung nach Absatz 1 Satz 2 oder Absatz 2 sind die Daten zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten; Gleiches gilt für Kennzeichnungen nach § 3 Abs. 2.

(4) Soweit das Bundeskriminalamt und die Landeskriminalämter auf Ersuchen oder im Auftrag des Generalbundesanwalts die Antiterrordatei nutzen, übermitteln sie die Daten, auf die sie Zugriff erhalten haben, dem Generalbundesanwalt für die Zwecke der Strafverfolgung. Der Generalbundesanwalt darf die Daten für Ersuchen nach Absatz 1 Satz 1 verwenden. § 487 Abs. 3 der Strafprozessordnung gilt entsprechend.

27

§ 7 Übermittlung von Erkenntnissen

Die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 zwischen den beteiligten Behörden richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

28

§ 8 Datenschutzrechtliche Verantwortung

(1) Die datenschutzrechtliche Verantwortung für die in der Antiterrordatei gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten trägt die Behörde, die die Daten eingegeben hat. Die Behörde, die die Daten eingegeben hat, muss erkennbar sein. Die Verantwortung für die Zulässigkeit der Abfrage trägt die abfragende Behörde.

(2) Nur die Behörde, die die Daten eingegeben hat, darf diese Daten ändern, berichtigen, sperren oder löschen.

(3) Hat eine Behörde Anhaltspunkte dafür, dass Daten, die eine andere Behörde eingegeben hat, unrichtig sind, teilt sie dies umgehend der Behörde, die die Daten eingegeben hat, mit, die diese Mitteilung unverzüglich prüft und erforderlichenfalls die Daten unverzüglich berichtigt.

29

§ 9 Protokollierung, technische und organisatorische Maßnahmen

(1) Das Bundeskriminalamt hat bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Behörde und den Zugriffszweck nach § 5 Abs. 4 zu protokollieren. Die Protokolldaten dürfen nur verwendet werden, soweit ihre Kenntnis für Zwecke der Datenschutzkontrolle, der Datensicherung, zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage oder zum Nachweis der Kenntnisnahme bei Verschlusssachen erforderlich ist. Die ausschließlich für Zwecke nach Satz 1 gespeicherten Protokolldaten sind nach 18 Monaten zu löschen.

(2) Das Bundeskriminalamt hat die nach § 9 des Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen zu treffen.

30

§ 10 Datenschutzrechtliche Kontrolle, Auskunft an den Betroffenen

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 24 Abs. 1 des Bundesdatenschutzgesetzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die datenschutzrechtliche Kontrolle der Eingabe und der Abfrage von Daten durch eine Landesbehörde richtet sich nach dem Datenschutzgesetz des Landes.

(2) Über die nicht verdeckt gespeicherten Daten erteilt das Bundeskriminalamt die Auskunft nach § 19 des Bundesdatenschutzgesetzes im Einvernehmen mit der Behörde, die die datenschutzrechtliche Verantwortung nach § 8 Abs. 1 Satz 1 trägt und die Zulässigkeit der Auskunftserteilung nach den für sie geltenden Rechtsvorschriften prüft. Die Auskunft zu verdeckt gespeicherten Daten richtet sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften.

31

§ 11 Berichtigung, Löschung und Sperrung von Daten

(1) Unrichtige Daten sind zu berichtigen.

(2) Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist. Sie sind spätestens zu löschen, wenn die

zugehörigen Erkenntnisse nach den für die beteiligten Behörden jeweils geltenden Rechtsvorschriften zu löschen sind.

(3) An die Stelle einer Löschung tritt eine Sperrung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen eines Betroffenen beeinträchtigt würden. Gesperrte Daten dürfen nur für den Zweck abgerufen und genutzt werden, für den die Löschung unterblieben ist; sie dürfen auch abgerufen und genutzt werden, soweit dies zum Schutz besonders hochwertiger Rechtsgüter unerlässlich ist und die Aufklärung des Sachverhalts ansonsten aussichtslos oder wesentlich erschwert wäre oder der Betroffene einwilligt.

(4) Die eingebenden Behörden prüfen nach den Fristen, die für die Erkenntnisdaten gelten, und bei der Einzelfallbearbeitung, ob personenbezogene Daten zu berichtigen oder zu löschen sind.

32

§ 12 Errichtungsanordnung

Das Bundeskriminalamt hat für die gemeinsame Datei in einer Errichtungsanordnung im Einvernehmen mit den beteiligten Behörden Einzelheiten festzulegen zu:

1. den Bereichen des erfassten internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland,
2. den weiteren beteiligten Polizeivollzugsbehörden nach § 1 Abs. 2,
3. der Art der zu speichernden Daten nach § 3 Abs. 1,
4. der Eingabe der zu speichernden Daten,
5. den zugriffsberechtigten Organisationseinheiten der beteiligten Behörden,
6. den Einteilungen der Zwecke und der Dringlichkeit einer Abfrage und
7. der Protokollierung.

Die Errichtungsanordnung bedarf der Zustimmung des Bundesministeriums des Innern, des Bundeskanzleramts, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen und der für die beteiligten Behörden der Länder zuständigen obersten Landesbehörden. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass der Errichtungsanordnung anzuhören.

33

§ 13 Einschränkung von Grundrechten

Die Grundrechte des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.

34

3. Erste Überlegungen zur Schaffung einer Antiterrordatei gehen auf die 15. Wahlperiode des Bundestags zurück. Damals legte der Bundesrat auf Initiative der Länder Niedersachsen, Bayern, Saarland und Thüringen einen „Entwurf eines Gesetzes zur Errichtung einer gemeinsamen Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus (Anti-Terror-Datei-Gesetz)“ vor (BTDrucks 15/4413). In diese gemeinsame Datei sollten nach den Vorstellungen des Entwurfs die teilnehmenden Polizeibehörden und Nachrichtendienste alle Daten über Personen oder Vorgänge einstellen, die im Zusammenhang mit dem islamistischen Extremismus und Terrorismus stünden (BTDrucks 15/4413, S. 8). Die damalige Bundesregierung favorisierte dagegen die Schaffung einer Indexdatei, also lediglich eines elektronischen Fundstellennachweises für die zum Auffinden weiterer Erkenntnisse erforderlichen Daten (BTDrucks 15/4413, S. 9). Keiner der beiden Vorschläge wurde in der 15. Wahlperiode realisiert.

35

Nach fehlgeschlagenen Anschlagversuchen auf Eisenbahnzüge in Koblenz und Dortmund im August 2006 brachte die Bundesregierung den „Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz)“ ein, der in seinem Art. 1 auch den Entwurf für das „Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG)“ enthielt (BTDrucks 16/2950, S. 5) und mit nur geringfügigen Änderungen nach einer Anhörung von Sachverständigen im Innenausschuss (Innenausschussprotokoll Nr. 16/24) verabschiedet wurde. Nach der Begründung des Entwurfs soll das Gesetz eine Rechtsgrundlage für eine gemeinsame Datei schaffen, die den Informationsaustausch zwischen Polizeibehörden und Nachrichtendiensten effektiver gestalten, bewährte Formen der Zusammenarbeit ergänzen und Übermittlungsfehler verringern solle (BTDrucks

16/2950, S. 12). Nach § 1 Abs. 1 ATDG soll die Antiterrordatei dazu dienen, die beteiligten Behörden bei der Erfüllung ihrer Aufgaben bei der Aufklärung und Bekämpfung des internationalen Terrorismus zu unterstützen, wobei mit dem Begriff der „Aufklärung“ die nachrichtendienstlichen Aufgaben und mit dem Begriff der „Bekämpfung“ die polizeilichen Aufgaben umschrieben würden. § 2 ATDG regelt den Inhalt der Antiterrordatei. In der Datei dürften nur Daten zu Kenntnissen gespeichert werden, über die die beteiligten Behörden auf der Grundlage der für sie geltenden Rechtsvorschriften bereits verfügten; es werde keine zusätzliche Rechtsgrundlage für die Datenerhebung durch die beteiligten Behörden geschaffen (BTDrucks 16/2950, S. 15). Durch § 2 Satz 1 Nr. 2 ATDG sollten auch gewalttätige und gewaltbereite Einzeltäter, insbesondere auch als solche bezeichnete „Hassprediger“, erfasst werden (vgl. BTDrucks 16/2950, S. 15).

36

§ 3 Abs. 1 ATDG lege fest, welche Datenarten zu den in § 2 genannten Personen und Objekten zu speichern seien. Die Grunddaten nach § 3 Abs. 1 Nr. 1 a ATDG sollten der Identifizierung der abgefragten Personen dienen. Die erweiterten Grunddaten sollten neben der Identifizierung einer gesuchten Person auch eine zuverlässige Gefährdungseinschätzung als fachliche Erstbewertung ermöglichen. Im Gegensatz zu den Grunddaten seien die erweiterten Grunddaten grundsätzlich nur recherchierbar, würden der abfragenden Behörde aber im Trefferfall erst auf Nachfrage nach Maßgabe des Fachrechts angezeigt. Die einzugebenden Daten sollten - soweit möglich - nach systemseitigen Vorgaben in standardisierter Form erfasst werden. Die durch das Freitextfeld eröffnete Möglichkeit, daneben individuelle Bemerkungen, Hinweise und Bewertungen eingeben zu können, diene dazu, auch terrorismusrelevante Angaben zu erfassen, die sich nicht über einen Katalog standardisiert erfassen ließen. Die grundsätzliche Pflicht zur Standardisierung dürfe hierdurch jedoch nicht umgangen werden (BTDrucks 16/2950, S. 17).

37

Das Antiterrordateigesetz ist gemäß Art. 5 Abs. 1 Gemeinsame-Dateien-Gesetz am 31. Dezember 2006 in Kraft getreten.

38

4. In der Praxis der teilnehmenden Behörden ist die Handhabung und Nutzung der Antiterrordatei von ihrem Charakter als standardisierte Datei geprägt. Standardisierung bedeutet, dass nicht alle der gemäß § 3 Abs. 1 ATDG zu speichernden Angaben freihändig in die Datei eingegeben werden, sondern in einem Katalog eine bestimmte Auswahl von Angaben, sogenannte Katalogwerte, angeboten wird, aus denen die eingebende Behörde auswählt. Nach Angaben der Bundesregierung wurden Freitexteingabemöglichkeiten auf solche Angaben nach § 3 Abs. 1 ATDG begrenzt, bei denen eine Standardisierung auf feste Katalogwerte nicht möglich ist. Dies betrifft im Rahmen der Grunddaten die Angaben zu Straße, Hausnummer, Postleitzahl und Ort, sowie im Rahmen der erweiterten Grunddaten beispielsweise die Rufnummer und Gerätenummer eines Telekommunikationsendgeräts oder die Fahrzeugident-Nummer, Kennzeichen und Zulassungsort eines Kraftfahrzeugs sowie naturgemäß auch das Freitextfeld des § 3 Abs. 1 Nr. 1 b rr ATDG. Die Standardisierung erfolgt innerhalb der Eingabemaske in Form sogenannter „Pull-Down Menüs“ durch eine Liste von Katalogwerten, die zur Auswahl angeboten werden. Zu welchen Datenarten des § 3 Abs. 1 ATDG Kataloge angeboten werden und welche als Katalogwerte bezeichneten Angaben in den jeweiligen Katalogen ausgewählt werden können, wird grundsätzlich von einer beim Bundeskriminalamt angesiedelten Katalogredaktion aufgrund der Vorgaben des § 3 Abs. 1 ATDG und der weiteren gemäß § 12 Satz 1 Nr. 3 ATDG in der Errichtungsanordnung enthaltenen Konkretisierungen bestimmt und in einem Katalogmanual festgehalten, das ebenso wie die Errichtungsanordnung selbst als „VS – Nur für den Dienstgebrauch“ klassifiziert ist. Zu unterscheiden sind dabei „geschlossene“ und „lernende“ Kataloge. Bei „geschlossenen“ Katalogen sind die möglichen Katalogwerte abschließend festgelegt. So ist beispielsweise im Rahmen der Angaben des § 3 Abs. 1 Nr. 1 b ee ATDG zu den von einer Person genutzten Fahrzeugen im Katalog „Fahrzeugart“ aus der abschließenden Liste „PKW; LKW; Bus; Boot; Flugzeug; Motorrad; Bahn; Sonderfahrzeug; Fahrrad; Quad“ auszuwählen. Andere Einträge sind nicht möglich. Eine Veränderung des Katalogs kann nur die Katalogredaktion beim Bundeskriminalamt vornehmen. „Lernende“ Kataloge sind den geschlossenen Katalogen insofern ähnlich, als eine vorgegebene Auswahl von Katalogwerten den Nutzern von der Katalogredaktion zur Auswahl vorgeschlagen ist. Darüber hinaus kann ein Nutzer den Katalog aber um weitere Einträge ergänzen. Diese stehen anschließend auch allen anderen Nutzern als Katalogwerte zur Auswahl zur Verfügung. Für diese zusätzlichen Einträge ist keine Zustimmung des Bundeskriminalamtes erforderlich. So kann beispielsweise bei den Angaben zu Telekommunikationsendgeräten nach § 3 Abs. 1 Nr. 1 b aa ATDG ein neuer Typ von Telekommunikationsendgerät durch die Nutzer in den Katalog aufgenommen werden, sollte dies erforderlich werden, weil die zu speichernde Person einen neuartigen Typ von Telekommunikationsendgerät benutzt, der bislang nicht im Katalog aufgeführt ist.

39

Die Befüllung der Antiterrordatei mit Datenbeständen aus den Quelldateien der teilnehmenden Behörden erfolgt oftmals in einem teilautomatisierten Verfahren. Zunächst werden dabei die in den Quelldateien vorhandenen Datensätze im Wege einer manuellen fachlichen Prüfung von der jeweiligen teilnehmenden Behörde auf ihre Relevanz für die Antiterrordatei überprüft und gegebenenfalls als geeignet markiert. Anschließend wird aus den markierten Datensätzen eine sogenannte Exportdatei erzeugt, in die nur

diesjenigen Datenarten aus der Quelldatei aufgenommen werden, für die in der Antiterrordatei Entsprechungen vorhanden sind. Datenarten der Antiterrordatei, die in der Quelldatei nicht vorhanden oder beim konkreten Datensatz nicht belegt sind, bleiben auch in der Antiterrordatei unbelegt. Dabei findet im Hinblick auf die standardisierten Kataloge auch eine Prüfung statt, ob jeder Katalogwert aus der Quelldatei mit den vorgegebenen Katalogwerten der Antiterrordatei übereinstimmt. Im Fall unterschiedlicher Terminologie findet eine Übersetzung statt, beispielsweise von „Fernsprecher“ zu „Telefon“. Anschließend wird die Exportdatei an das Bundeskriminalamt übermittelt und dort in die Antiterrordatei importiert.

40

5. Im Hinblick auf die Antiterrordatei führten verschiedene Datenschutzbeauftragte Kontrollen bei teilnehmenden Behörden durch. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrollierte die Datenverarbeitung beim Bundeskriminalamt, beim Bundesamt für Verfassungsschutz und beim Bundesnachrichtendienst. Er äußerte im Hinblick auf die Speicherung von erweiterten Grunddaten von Kontaktpersonen grundsätzliche Bedenken und kritisierte, dass beim Bundeskriminalamt Daten einer Quelldatei ohne Einzelfallprüfung in das Freitextfeld nach § 3 Abs. 1 Nr. 1 b rr ATDG übertragen wurden. Daraufhin änderte das Bundeskriminalamt das Verfahren der Befüllung des Freitextfeldes (BTDrucks 16/12600, S. 51 f.). Beim Bundesamt für Verfassungsschutz wurden neben Problemen bei der Befüllung der Antiterrordatei, insbesondere des Freitextfeldes, Mängel bei der Kennzeichnung von Daten festgestellt, die aus heimlichen Telekommunikationsüberwachungen stammen. Eine förmliche Beanstandung unterblieb im Hinblick auf die Zusage sofortiger Behebung der festgestellten Mängel (BTDrucks 17/5200, S. 83 f.). Auch Landesbehörden wurden im Hinblick auf die Antiterrordatei überprüft, so etwa in Baden-Württemberg in Form mehrtägiger Kontrollbesuche beim Landeskriminalamt Baden-Württemberg (Abteilung Staatsschutz) und beim Landesamt für Verfassungsschutz. Mängel bezüglich einiger Datensätze führten auf die Beanstandung des Landesbeauftragten hin zu einer Löschung oder Korrektur dieser Datensätze (Landtag von Baden-Württemberg, LTDrucks 14/2050, S. 12, 14 ff.). Weitere Kontrollen wurden durch die Landesbeauftragten für den Datenschutz durchgeführt.

II.

41

Der Beschwerdeführer sieht sich durch die angegriffenen Vorschriften in seinem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie seinen Grundrechten aus Art. 10, Art. 13 und Art. 19 Abs. 4 GG verletzt.

42

1. Er sei durch die Vorschriften unmittelbar betroffen. Zwar bedürften die Vorschriften des Antiterrordateigesetzes noch eines faktischen Vollzugsaktes, nämlich der Einstellung seiner Daten in die Antiterrordatei. Da er hiervon aber nicht benachrichtigt werde, könne er eine effektive gerichtliche Kontrolle nicht herbeiführen. Allerdings könne er nach § 10 Abs. 2 ATDG um Auskunft ersuchen und gegebenenfalls dann den Rechtsweg beschreiten. Diese Rechtsschutzmöglichkeit greife aber zu kurz. Selbst wenn ihm an einem Tag mitgeteilt werde, nicht in die Antiterrordatei aufgenommen zu sein, könne schon am nächsten Tag das Gegenteil zutreffen. Zudem seien diese Ersuchen in Bezug auf die verdeckt gespeicherten Daten bei mehr als 30 verschiedenen Behörden zu stellen.

43

Wegen der Pflicht der Verfassungsschutzbehörden, erhobene Daten in der Antiterrordatei zu speichern, befürchtet der Beschwerdeführer, dass ihn betreffende Daten in die Antiterrordatei aufgenommen würden, ohne dass er davon Kenntnis erlangen könne. Angesichts der Befugnis der Verfassungsschutzbehörden zu heimlicher Informationsbeschaffung mit nachrichtendienstlichen Mitteln sei es möglich, als unbescholtener Bürger bei legalem Verhalten – beispielsweise aufgrund eines anonymen Hinweises – Objekt einer intensiven nachrichtendienstlichen Ausspähung zu werden. Möglich sei auch, dass von ihm als Kontaktperson zu Personen, deren Verstrickung in den Terrorismus er nicht kenne, weiterführende Hinweise für die Aufklärung des internationalen Terrorismus erwartet würden.

44

2. Durch die Antiterrordatei erhielten alle beteiligten Behörden Zugriff auf die von den Verfassungsschutzbehörden gespeicherten Daten, insbesondere auch die Polizeibehörden, die diese Informationen selbst nicht hätten erheben dürfen und ohne die Antiterrordatei nicht davon Kenntnis bekommen würden. Durch das Antiterrordateigesetz werde so das Gebot der Trennung von Polizei und Nachrichtendiensten teilweise aufgehoben. Der Verfassungsrang dieses Trennungsgebots folge aus Art. 87 Abs. 1 Satz 2 GG; es sei Ausprägung des Rechtsstaatsprinzips und des Grundrechtsschutzes. Es ziele darauf zu verhindern, dass die gesetzlichen Bestimmungen für Eingriffsbefugnisse der Polizei dadurch ausgehöhlt würden, dass die Polizei Informationen erhalte, die sie aufgrund der für sie geltenden Bestimmungen nicht selbst gewinnen könne.

45

3. Die Regelungen des Antiterrordateigesetzes verletzen das informationelle Selbstbestimmungsrecht des Beschwerdeführers. Sie seien zu unbestimmt und unverhältnismäßig. Nach ihnen seien Daten auch über Personen einzustellen, die – unter Umständen aufgrund nur ungesicherter Anhaltspunkte – als Befürworter rechtswidriger Gewalt gälten, wobei hierfür nicht nur typisch terroristische, sondern jedwede minimale Gewalt genüge; was ein „Befürworten“ darstelle, bleibe offen. Für die Speicherung könnten „Anhaltspunkte“ für eine innere Gesinnung ausreichen. Daher werde § 2 Satz 1 Nr. 2 ATDG dem Bestimmtheitsgebot nicht gerecht.

46

Die Kontaktpersonenregelung des § 2 Satz 1 Nr. 3 ATDG sei zu unbestimmt. Durch die Aufnahme von Kontaktpersonen ohne eigene Kenntnis terroristischer Aktivitäten werde der Kreis der Betroffenen auf der Grundlage einer „doppelten Mutmaßung“ unverhältnismäßig ausgedehnt. Es würden nämlich auch Daten unbescholtener Personen erfasst, soweit nur – auch ungesicherte – „Anhaltspunkte“ für einen Kontakt zu Personen bestünden, bei denen – eventuell ebenfalls ungesicherte – „Anhaltspunkte“ für terroristische Handlungsweisen oder für ein „Gewaltbefürworten“ vorlägen. Die erforderliche Erwartung, von den Kontaktpersonen „weiterführende Hinweise“ gewinnen zu können, schränke den betroffenen Personenkreis faktisch nicht ein.

47

Unverhältnismäßig und zu unbestimmt sei die Regelung der Grunddaten in § 3 Abs. 1 Nr. 1 a ATDG. Die Grundrechtsbeeinträchtigung verstärke sich, wenn nach § 3 Abs. 1 Nr. 1 b ATDG „erweiterte Grunddaten“ in die Antiterrordatei eingestellt würden. Diese Daten stellten ein weitgehendes Persönlichkeitsprofil dar. Die Regelung des § 5 Abs. 2 ATDG, der im Eilfall allen beteiligten Behörden Zugriff auch auf diese Daten gestatte, sei unverhältnismäßig, da sie der Bedeutung dieser Daten nicht gerecht werde und schon eine Gefahr für die Gesundheit einer Person den Zugriff auf die erweiterten Grunddaten rechtfertige.

48

Ferner sei die Aufnahme von nur auf „Anhaltspunkten“ beruhenden Bemerkungen, Zusammenfassungen, Bewertungen und Hinweisen als zusätzlicher Freitext gemäß § 3 Abs. 1 Nr. 1 b rr ATDG unverhältnismäßig und zu unbestimmt. Mangels sachhaltiger Beschränkung könnten in unbegrenztem Umfang weitere Informationen aller Art in die Datei eingestellt werden; die Speicherung von Freitexten sei nicht im Voraus abschätzbar.

49

Das Bestimmtheitsgebot werde auch verletzt, weil das Antiterrordateigesetz keine eigenständige Regelung zur Löschung der Daten enthalte, sondern nur auf die Vorschriften der die Daten eingebenden Behörden verweise. Diese fänden sich in einer Vielzahl von Gesetzen, die das Antiterrordateigesetz nicht mitteile. Auch bleibe unklar, was mit den von den beteiligten Behörden zur Kenntnis genommenen und ihrerseits gespeicherten Daten im Sperr- oder Löschungsfall zu geschehen habe.

50

4. Gegen Art. 13 GG verstoße, dass in die Antiterrordatei auch Daten aufgenommen werden könnten, die aus in Wohnungen durchgeführten „großen Lauschangriffen“ herrührten. § 3 Abs. 2 ATDG ermögliche dies, ohne dass die grundrechtlich gebotenen Hürden eingehalten werden müssten. Das Brief- und Fernmeldegeheimnis des Art. 10 GG werde verletzt, weil die den Verfassungsschutzbehörden und Nachrichtendiensten eingeräumten, weitgehenden Eingriffsmöglichkeiten durch die Datenübermittlung mittels Antiterrordatei zu einer unverhältnismäßigen Kenntnisnahme des privaten Kommunikationsverhaltens des Beschwerdeführers und seiner Kommunikationsinhalte durch andere Behörden führten.

51

5. Auch das Grundrecht des Beschwerdeführers auf Beschreiten des Rechtswegs gegen Akte der öffentlichen Gewalt nach Art. 19 Abs. 4 GG sei verletzt. Die durchgängige Verheimlichung der Maßnahmen nehme dem Beschwerdeführer jede Chance einer gerichtlichen Überprüfung. Es fehle auch an einer anderen, den Rechtsweg ersetzenden Nachprüfung.

III.

52

Zu der Verfassungsbeschwerde haben die Bundesregierung, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, der Berliner Beauftragte für Datenschutz und Informationsfreiheit und der Landesbeauftragte für den Datenschutz Baden-Württemberg Stellung genommen.

53

1. Die Bundesregierung hält die Verfassungsbeschwerde für unzulässig, jedenfalls aber für unbegründet.

54

a) Die Verfassungsbeschwerde sei bereits unzulässig, da der Beschwerdeführer nicht unmittelbar, selbst und gegenwärtig durch das Antiterrordateigesetz beschwert sei. Er trage keinen Sachverhalt vor, der eine Speicherung in der Antiterrordatei nahelege. Der Beschwerdeführer habe unterlassen, vor Erhebung der Verfassungsbeschwerde gemäß § 10 Abs. 2 ATDG beim Bundeskriminalamt und gegebenenfalls bei weiteren teilnehmenden Behörden um Auskunft über eine Speicherung in der Antiterrordatei zu ersuchen, um nachzuweisen, von einer Speicherung betroffen zu sein. Der Aufwand, erforderlichenfalls bei den 38 beteiligten Behörden eine Auskunft einzuholen, sei zumutbar. Auch sei der Vortrag des Beschwerdeführers zu vage, als dass er zur Darlegung der Beschwerdebefugnis genügen könne, ohne deren eine „Populärverfassungsbeschwerde“ ausschließende Funktion aufzugeben. Es fehle zugleich an einer hinreichenden Bestimmung des Beschwerdegegenstandes, weil unklar sei, welche Bestimmungen konkret angegriffen seien.

55

b) Die Verfassungsbeschwerde sei jedenfalls unbegründet.

56

aa) Die Gesetzgebungskompetenz des Bundes für den Erlass des Antiterrordateigesetzes ergebe sich grundsätzlich aus Art. 73 Abs. 1 Nr. 10 a bis c GG; soweit der Bundesnachrichtendienst und der Militärische Abschirmdienst betroffen seien, folge sie aus Art. 73 Abs. 1 Nr. 1 GG sowie hinsichtlich des Zollkriminalamtes und der Bundespolizei aus Art. 73 Abs. 1 Nr. 5 GG. Die Schaffung einer zentralen Datei beim Bundeskriminalamt lasse sich auch der in Art. 87 Abs. 1 Satz 2 GG angesiedelten Befugnis zur Errichtung von Zentralstellen zuordnen.

57

bb) Ob sich dem Grundgesetz ein organisatorisches und befugnisbezogenes Trennungsgebot zwischen Polizei und Verfassungsschutzbehörden entnehmen lasse, könne dahinstehen, da es nicht zu einer Vermischung der Aufgaben- und Tätigkeitsfelder von Verfassungsschutz- und Polizeibehörden komme. Dem Grundgesetz könne ein strenges Verbot der Informationshilfe zwischen Nachrichtendiensten und Polizeibehörden nicht entnommen werden. Das Antiterrordateigesetz bewirke keinen unkontrollierten Datenfluss. Es ermögliche lediglich die Kontaktaufnahme zwischen den Behörden und einen Informationsfluss, der sich nach anderen Normen richte. Die relevanten Informationsweitergabenormen erhielten keine neue Dimension.

58

cc) Das Antiterrordateigesetz verletze das Grundrecht auf informationelle Selbstbestimmung nicht. Die Speicherung und der Abruf der Daten sowie ihre weitere Verwendung seien gerechtfertigt.

59

Die Speicherung von Daten in der Antiterrordatei stelle allenfalls einen geringfügigen Grundrechtseingriff beziehungsweise eine geringfügige Vertiefung des Grundrechtseingriffs der ursprünglichen Datenerhebung und -verwendung dar. In der Antiterrordatei dürften nur bereits nach den jeweiligen Fachgesetzen erhobene Daten gespeichert werden. Die Befüllung selbst bewirke noch keine Zweckänderung. Der Verwendungszusammenhang der in der Antiterrordatei gespeicherten Daten sei auf einen sehr spezifischen Gefahrensektor des internationalen Terrorismus beschränkt. Auch die Standardisierung der gespeicherten Angaben wirke beschränkend. Die einfachen Grunddaten enthielten im Wesentlichen Angaben zur Person mit dem Ziel einer Erleichterung des Informationsaustauschs, die erweiterten Grunddaten dienten darüber hinaus im Eilfall dazu, einen ersten Eindruck von einer Person und ihrer Gefährlichkeit zu vermitteln.

60

Bedenken gegen die Bestimmtheit der umfassten Personengruppen griffen nicht durch. Der Begriff der Gewalt in § 2 Satz 1 Nr. 2 ATDG erfordere enger als nach dem Strafgesetzbuch physische Kraftentfaltung mit Zwangswirkung. Die Variante des Befürwortens von Gewalt zielen auf sogenannte Hassprediger und verlange ein nach außen erkennbares Gutheißens von Gewaltanwendung. Für die nach § 2 Satz 1 Nr. 3 ATDG zu speichernden Kontaktpersonen müssten andere Maßstäbe als beispielsweise bei der präventiven Telefonüberwachung gelten, da die Vorschrift nur die Einstellung bereits anderweitig rechtmäßig gespeicherter Personen und keine neue Informationserhebung betreffe. Die erforderlichen tatsächlichen Anhaltspunkte erforderten immer eine Tatsachenbasis für einen Verdacht. Die Speicherung von Daten im Freitextfeld des § 3 Abs. 1 Nr. 1 b rr ATDG sei ein Korrektiv zur Standardisierung der Dateneingabe und dadurch eingegrenzt, dass die Daten einen unmittelbaren inhaltlichen Bezug zu den gesetzlich definierten Daten aufweisen müssten. Auch das umfasste Informationsvolumen sei begrenzt.

61

Die Eingriffstiefe einer Recherche in der Antiterrordatei werde dadurch begrenzt, dass sie nur erfolgen dürfe, wenn sie zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sei. Die Antiterrordatei könne nicht zum automatischen Abgleich mit anderen Datenbanken genutzt werden. Ein Treffer eröffne grundsätzlich nur den Zugriff auf die einfachen Grunddaten zur Identifizierung einer Person und die Nutzung dieser Daten sei auf den Trefferabgleich und das Stellen eines Ermittlungsersuchens

begrenzt. Das Antiterrordateigesetz diene allein dazu, im Hinblick auf Personen, gegen die schon ermittelt werde, den Kontakt zwischen den beteiligten Behörden zu ermöglichen; es gestatte nicht, „Verdächtige“ erst zu finden. Die Freigabe der erweiterten Grunddaten aufgrund eines Ermittlungersuchens richte sich nach den maßgeblichen fachrechtlichen Übermittlungsvorschriften.

62

Ein schwerer, dem Antiterrordateigesetz zurechenbarer Eingriff ergebe sich aus der Möglichkeit zum Zugriff auch auf die erweiterten Grunddaten im Eilfall und deren Verwendung zur Abwehr der in § 5 Abs. 2 ATDG genannten Gefahren. Allerdings sei auch der Informationsgehalt der erweiterten Grunddaten beschränkt. Der Zugriff sei nur in außerordentlichen Notsituationen vorgesehen. Soweit die Vorschrift auf Sachen von erheblichem Wert abstelle, würden diese nicht nur durch ihren finanziellen, sondern ihren gemeinschaftlichen Wert bestimmt: Dies zielen auf den Schutz von öffentlichen Sachen wie Brücken, Behörden und Infrastruktureinrichtungen. Auch sei der Zugriff im Eilfall mit besonderen verfahrensrechtlichen Sicherungen verbunden. Tatsächlich habe man bislang nur einmal auf die Vorschrift zurückgegriffen.

63

Die dem Antiterrordateigesetz zuzurechnenden Grundrechtseingriffe seien gerechtfertigt. Die Bekämpfung des Terrorismus sei eine Verfassungsaufgabe von höchstem Rang. Die Errichtung der Antiterrordatei sei geeignet, dieses Ziel zu verfolgen, da sie den beteiligten Behörden durch die Verbesserung des Informationsaustauschs die Aufklärung und Bekämpfung des internationalen Terrorismus erleichtere. Das Antiterrordateigesetz sei für eine effektive Aufklärung und Bekämpfung der weit verzweigten Netzwerke des internationalen Terrorismus auch unverzichtbar, um Erkenntnisse aus dem Bereich des internationalen Terrorismus und seiner Unterstützer bei der Polizei und den Nachrichtendiensten rasch auffindbar zu machen. Das Antiterrordateigesetz sei auch verhältnismäßig im engeren Sinn. Bei einer Gesamtabwägung stehe die Schwere des Eingriffs nicht außer Verhältnis zum Gewicht der ihn rechtfertigenden Gründe.

64

dd) Die in der Antiterrordatei gespeicherten Daten könnten auch aus Eingriffen in Art. 10 und Art. 13 GG herrühren, weshalb § 13 ATDG ausdrücklich die Einschränkung dieser Grundrechte benenne. Die Befüllung mit solchen Daten wiege wesentlich schwerer, sei gleichwohl nicht unverhältnismäßig. Der neue Verwendungszweck sei hinreichend eingegrenzt und die Kennzeichnungspflicht in § 3 Abs. 2 ATDG stelle sicher, dass der Verwendungszusammenhang nicht verloren gehe. Zwar beschränke § 5 Abs. 1 ATDG die Suche nicht auf Fälle, in denen die Übermittlung der auf Eingriffen in Art. 10 und Art. 13 GG beruhenden Daten nach den Datenübermittlungsvorschriften möglich wäre. Doch würden der suchenden Behörde als Treffer nur die einfachen Grunddaten übermittelt. Dass von Art. 10 oder Art. 13 GG besonders geschützte Daten selbst als Treffer ausgeworfen würden, werde im Übrigen dadurch verhindert, dass die Behörde nach verfassungskonformer Auslegung des § 4 Abs. 1 ATDG verpflichtet sei, Grunddaten, die aus Eingriffen in Art. 10 oder Art. 13 GG herrührten, verdeckt zu speichern.

65

Die Möglichkeit des Zugriffs auf besonders geschützte Daten im Rahmen des Eilfalls nach § 5 Abs. 2 ATDG sei im Ergebnis mit dem Verhältnismäßigkeitsgrundsatz zu vereinbaren, da sie einen konkreten polizeilichen Gefahrenabwehrein satz erleichtere, nicht aber dazu diene, weitergehende Persönlichkeitsprofile zu erstellen.

66

ee) Das Antiterrordateigesetz sei auch mit der Rechtsschutzgarantie des Art. 19 Abs. 4 GG vereinbar, da der von einer Eintragung in die Antiterrordatei Betroffene nicht rechtsschutzlos gestellt sei. Zwar erhalte er keine Mitteilung von Amts wegen, doch könne er - verwaltungsgerichtlich durchsetzbar - nach § 10 Abs. 2 ATDG Auskunft verlangen. Diese Ausgestaltung der Rechtsschutzmöglichkeiten sei durch die Art der Verwaltungsaufgabe und die geringe Eingriffsqualität des Eintrags in der Antiterrordatei gerechtfertigt.

67

ff) Art. 10 Abs. 1 ATDG übertrage die datenschutzrechtliche Kontrolle der Antiterrordatei im Rahmen ihrer jeweiligen Zuständigkeiten auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und auf die Landesdatenschutzbeauftragten. Die Kontrolle der Datenschutzbeauftragten werde nicht dadurch unvollständig, dass die Kontrollbefugnisse auf ihre jeweilige Körperschaft beschränkt seien. Durch eine Kontrollbefugnis des Bundesbeauftragten für alle Nutzungsvorgänge würde eine verfassungsrechtlich problematische Kontrolle des Bundesbeauftragten für Landesbehörden entstehen. Zugriff auf die Protokolldaten erhielten die Landesdatenschutzbeauftragten beim Bundeskriminalamt in Wiesbaden.

68

gg) In tatsächlicher Hinsicht macht die Bundesregierung folgende Angaben: Von der Speicherung seien überwiegend im Ausland lebende Personen betroffen, bei denen die Schreibweise des Namens nicht immer eindeutig sei. Im August 2012 seien in der Antiterrordatei 17.101 Datensätze zu Personen gespeichert gewesen, davon ca. 920 Doppelnennungen beziehungsweise Doppelspeicherungen, so dass

etwa 16.180 unterschiedliche Personen von einer Speicherung betroffen seien. 2.888 dieser Personen hätten ihren Wohnsitz im Inland, 14.213 Personen im Ausland. Die Vielzahl von Personen mit Wohnsitz im Ausland erkläre sich aus der Teilnahme des Bundesnachrichtendienstes. Verdeckt im Sinne von § 4 Abs. 1 Satz 1 ATDG seien 2.833 Personen gespeichert. Die beteiligten Behörden übten größte Zurückhaltung, Kontaktpersonen ohne Kenntnis terroristischer Aktivitäten in die Antiterrordatei einzustellen. Sie habe im August 2012 nur 141 überwiegend von Landespolizeibehörden eingestellte Datensätze von undolosen Kontaktpersonen enthalten.

69

Die vorhandenen Datensätze enthielten kaum Eintragungen in den erweiterten Grunddaten. Nur 44 % der Datensätze seien überhaupt mit erweiterten Grunddaten befüllt. Kaum ein Datensatz enthalte einen annähernd vollständigen erweiterten Grunddatensatz. Über 94 % der Eintragungen enthielten keine Angaben im Freitextfeld, was auch daran liege, dass die Quelldatei des Bundesnachrichtendienstes kein vergleichbares Feld enthalte. Das Freitextfeld sei auf eine Anzahl von 2.000 Zeichen, also Text von weniger als einer DIN A 4-Seite, beschränkt. Die Eintragungen seien in der Regel sehr kurz, sie umfassten oft nur ein Wort, überwiegend zwischen 15 und 55 Zeichen. Nur bei einem Drittel der Personendatensätze fänden sich im Freitextfeld des § 3 Abs. 1 Nr. 1 b rr ATDG mehr als 100 Zeichen.

70

Von März 2007 bis Herbst 2012 seien relativ konstant 1.200 Suchanfragen pro Woche, insgesamt ca. 350.000 Suchanfragen, protokolliert worden. Daran zeige sich, dass die Antiterrordatei eher als „spezielles Telefonbuch“ und nicht für einen gesamten Quellenabgleich genutzt werde. In diesem Zeitraum sei in weniger als 1 % der Fälle eine Anfrage nach den erweiterten Grunddaten gestellt worden. In der Regel sei es für die Behörden sinnvoller, direkt Kontakt mit der speichernden Behörde aufzunehmen, als um die erweiterten Grunddaten zu ersuchen, die nur in besonderen Situationen als erste und schnelle Gefährlichkeitseinschätzung weiterführend seien. Bei den Anfragen zu erweiterten Grunddaten sei überschlägig in einem von drei oder vier Fällen der Zugriff verweigert worden.

71

Um eine vernünftige Eingrenzung der Ergebnisse zu ermöglichen, stelle das System derzeit sicher, dass bei einer Abfrage mit mehr als 200 Treffern technisch die Ausgabe verweigert werde. Die Zahl der bei einer Suche ausgeworfenen Treffer liege im Mittel bei vier bis fünf. Im Rahmen der Eilfallregelung des § 5 Abs. 2 ATDG habe bis August 2012 lediglich ein Zugriff auf die erweiterten Grunddaten stattgefunden. Dabei habe es sich um einen Zugriff eines Landeskriminalamts auf einen Datensatz des Bundesamts für Verfassungsschutz gehandelt.

72

Auf dem Protokolldatenserver seien insgesamt ca. 7,7 Millionen Datensätze gespeichert; jeder Datensatz spiegele jeweils die durch eine Aktion in der Antiterrordatei ausgelösten Datenbanktransaktionen wider.

73

2. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erhebt Bedenken gegen das Antiterrordateigesetz. Die informationelle Zusammenarbeit von Polizei und Nachrichtendiensten stehe unter dem Vorbehalt des Trennungsgebots. Damit sei nicht zu vereinbaren, wenn im Eilfall die beteiligten Polizeibehörden unmittelbar auf die von den Nachrichtendiensten gespeicherten erweiterten Grunddaten zugreifen könnten. Bedenken hinsichtlich des Gebots der Normenklarheit bestünden insbesondere in Blick auf § 1 Abs. 2 ATDG, das Tatbestandsmerkmal „Befürworten“ in § 2 Satz 1 Nr. 2 ATDG, die Kontaktpersonenregelung des § 2 Satz 1 Nr. 3 ATDG, bei der die Abgrenzung zwischen den von der Speicherung umfassten Kontaktpersonen und den nichtbetroffenen flüchtigen oder zufälligen Alltagskontakten unklar sei, sowie das Freitextfeld des § 3 Abs. 1 Nr. 1 b rr ATDG. Die Speicherung von Freitexten ermögliche in Zusammenschau mit den übrigen erfassten Daten die Erstellung weitreichender Persönlichkeitsprofile. § 10 Abs. 2 Satz 2 ATDG, der den Betroffenen unter Umständen zumute, Auskunftersuchen an alle an der Antiterrordatei teilnehmenden Behörden zu richten und gegen diese gegebenenfalls zu klagen, gewähre keinen effektiven Rechtsschutz; geboten sei eine Benachrichtigungspflicht.

74

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit verweist weiter darauf, dass die Aufteilung der Zuständigkeiten zwischen ihm und den Landesdatenschutzbeauftragten zu kontrollfreien Räumen führen könne. Da die Datei bei einer Bundesbehörde geführt werde, müsse er auf alle Protokolldaten Zugriff haben - auch auf diejenigen, die Datenzugriffe der Landesbehörden beträfen. Lücken der Kontrolle seien auch im Hinblick auf Daten, die durch Maßnahmen nach dem Artikel-10-Gesetz gewonnen worden seien, zu befürchten. Schwierigkeiten ergäben sich zudem daraus, dass auf den Protokolldatenserver nur an dessen Standort zugegriffen werden könne.

75

3. Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und der Berliner Beauftragte für Datenschutz und Informationsfreiheit haben gemeinsam Stellung genommen. Sie halten die

Verfassungsbeschwerde für zulässig und begründet. Das Antiterrordateigesetz werde weder dem Grundsatz der Normenklarheit und -bestimmtheit noch dem Verhältnismäßigkeitsgrundsatz gerecht und verletze sowohl das Grundrecht auf informationelle Selbstbestimmung als auch Art. 10 Abs. 1 und Art. 13 Abs. 1 GG. Ebenso sei zweifelhaft, ob das Antiterrordateigesetz dem Trennungsgebot gerecht werde.

76

§ 2 Satz 1 Nr. 1 bis 3 ATDG fasse den betroffenen Personenkreis zu weit. Es fehle für die Aufnahme von Personen an einem hinreichenden Verdachtsgrad, in Nr. 2 sei der Begriff der Gewalt nicht hinreichend auf terroristische Formen der Gewalt begrenzt, und in Nr. 3 würden die Kontaktpersonen angesichts der hohen Sensibilität der zu erfassenden Daten in vielerlei Hinsicht nicht hinreichend eingeschränkt. Es drohe die Errichtung einer bloßen Gesinnungsdatei. Die Speicherung der Religionszugehörigkeit nach § 3 Abs. 1 Nr. 1 b hh ATDG sei wegen der Gefahr einer Stigmatisierung besonders eingriffsintensiv und im Hinblick auf Art. 4 Abs. 1 GG problematisch. Auch die Zugriffsregelungen unterlägen nur unzureichenden Bindungen an den ursprünglichen Zweck der Datenerhebung. Alle beteiligten Behörden könnten ohne Eingriffsschwelle auf die einfachen Grunddaten zugreifen. Die tatbestandlichen Hürden für einen Zugriff im Eilfall seien gleichfalls nicht sehr hoch; Bedenken bestünden auch gegen § 6 Abs. 1 ATDG. Weiterhin genügten die verfahrensrechtlichen Sicherungen durch Lösch- und Aussonderungsprüffristen, Sperrung und Änderung sowie Auskunft nicht den verfassungsrechtlichen Erfordernissen. Es fehlten Vorgaben für ein gemeinsames Auskunftsverfahren im Falle der verdeckten Speicherung. Die Landesdatenschutzbeauftragten seien schließlich bei der Durchführung ihrer Kontrollen, namentlich im Hinblick auf den Zugriff auf die Protokolldaten, auf ähnliche Schwierigkeiten wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gestoßen.

77

4. Der Landesbeauftragte für den Datenschutz Baden-Württemberg berichtet von Kontrollbesuchen beim Landeskriminalamt und beim Landesamt für Verfassungsschutz in den Jahren 2007 (vgl. hierzu Landtag von Baden-Württemberg, LTDrucks 14/2050, S. 12 ff.) und 2012. Probleme hätten sich hinsichtlich des Gewaltbegriffs und der Bestimmung der Grenze zwischen verwerflichem „Befürworten“ und grundrechtlich geschützter Meinungsäußerung ergeben. Die Kontaktpersonenregelung habe sich bei den Kontrollen als zu unbestimmt erwiesen. Für die Behörde sei es schwierig, die Intensität bestehender Kontakte zu bewerten und die für eine Speicherung erforderliche Voraussetzung zu prüfen, ob von einer Kontaktperson weiterführende Hinweise für die Aufklärung und Bekämpfung des Terrorismus zu erwarten seien. Kontrollen würden dadurch erschwert, dass für die Landesdatenschutzbeauftragten kein elektronischer Zugriff auf die Protokolldaten möglich sei. Im Übrigen sei die Speicherung der Daten durch die beteiligten Stellen in Baden-Württemberg nicht zu beanstanden gewesen.

IV.

78

Das Bundesverfassungsgericht hat am 6. November 2012 eine mündliche Verhandlung durchgeführt, in der die Rechtsstandpunkte erläutert und vertieft wurden. Geäußert haben sich der Beschwerdeführer, als Mitglied des Deutschen Bundestages der Abgeordnete Clemens Binner, die Bundesregierung, das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Landesbeauftragte für den Datenschutz Baden-Württemberg, der Bayerische Landesbeauftragte für den Datenschutz, der Berliner Beauftragte für Datenschutz und Informationsfreiheit und das Landeskriminalamt Baden-Württemberg. Als Sachkundige wurden das Deutsche Institut für Menschenrechte, die Humanistische Union und der Chaos Computer Club angehört.

B.

79

Die Verfassungsbeschwerde ist zulässig.

I.

80

Der Beschwerdeführer rügt eine Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, des Brief- und Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG, der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG sowie in Verbindung mit diesen Grundrechten der Rechtsschutzgarantie aus Art. 19 Abs. 4 GG.

81

Der Beschwerdeführer legt die Möglichkeit einer Verletzung seines Grundrechts auf informationelle Selbstbestimmung dar, indem er geltend macht, dass die von ihm angegriffenen Vorschriften mit einiger Wahrscheinlichkeit eine Speicherung und Verwendung ihn betreffender personenbezogener Daten

regelten und dabei zu unbestimmt sowie unverhältnismäßig weit gefasst seien. Da es sich bei den betreffenden Daten auch um Daten handeln kann, die durch Eingriffe in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG erhoben wurden, kann der Beschwerdeführer auch eine Verletzung dieser Grundrechte geltend machen. Soweit der Beschwerdeführer bemängelt, dass die Speicherung und Verwendung der Daten nur unzureichend durch Informationsrechte zur Erlangung von Rechtsschutz flankiert werde, rügt er zugleich hinreichend substantiiert eine Verletzung dieser Grundrechte in Verbindung mit Art. 19 Abs. 4 GG.

II.

82

Der Beschwerdeführer ist durch die angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen.

83

1. Dem Beschwerdeführer fehlt es nicht an der erforderlichen unmittelbaren Betroffenheit. Zwar ist ein Beschwerdeführer nur dann von einer gesetzlichen Regelung unmittelbar betroffen, wenn diese, ohne dass es eines weiteren Vollzugsaktes bedürfte, in seinen Rechtskreis eingreift. Erfordert das Gesetz zu seiner Durchführung rechtsnotwendig oder auch nur nach der tatsächlichen staatlichen Praxis einen besonderen, vom Willen der vollziehenden Stelle beeinflussten Vollzugsakt, muss der Beschwerdeführer grundsätzlich zunächst diesen Akt angreifen und den gegen ihn eröffneten Rechtsweg erschöpfen, bevor er die Verfassungsbeschwerde erhebt (BVerfGE 1, 97 <101 ff.>; 109, 279 <306>; stRspr). Von einer unmittelbaren Betroffenheit ist jedoch dann auszugehen, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhält. In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zu wie in den Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz eintritt (vgl. BVerfGE 30, 1 <16 f.>; 113, 348 <362 f.>; 120, 378 <394>; stRspr). So liegt es hier. Grundsätzlich kann der Beschwerdeführer weder von der Speicherung noch von der Verwendung seiner Daten nach den angegriffenen Vorschriften verlässlich Kenntnis erhalten.

84

Dass der Beschwerdeführer gemäß § 10 Abs. 2 ATDG auf Antrag die Möglichkeit hat, Auskunft über die Speicherung der Daten zu erhalten und anschließend gegen die Speicherung die Gerichte anzurufen, ändert hieran nichts. Denn auf diesem Weg kann er lediglich dagegen vorgehen, dass zu einem bestimmten Zeitpunkt Daten über ihn tatsächlich gespeichert sind, nicht aber - wie es seinem Rechtsschutzanliegen entspricht - dagegen, dass eine solche Speicherung, ohne dass er hierauf Einfluss hat oder hiervon Kenntnis erlangt, jederzeit möglich ist. Die Möglichkeit, eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz zu erheben, das zu heimlichen Maßnahmen berechtigt, entfällt deshalb unter dem Gesichtspunkt der Unmittelbarkeit jedenfalls in der Regel nur, wenn die spätere Kenntniserlangung des Betroffenen durch eine aktive Informationspflicht des Staates rechtlich gesichert ist (so in BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 25. April 2001 - 1 BvR 1104/92 -, NVwZ 2001, S. 1261 <1262 f.>). Eine solche Informationspflicht sieht das Antiterrordateigesetz indes nicht vor.

85

2. Der Beschwerdeführer ist selbst und gegenwärtig betroffen.

86

Erfolgt die konkrete Beeinträchtigung erst durch die Vollziehung des angegriffenen Gesetzes, erlangt der Betroffene jedoch in der Regel keine Kenntnis von den Vollzugsakten, reicht es für die Möglichkeit der eigenen und gegenwärtigen Betroffenheit aus, wenn der Beschwerdeführer darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird (vgl. BVerfGE 122, 63 <81 f.>; 125, 260 <305>; stRspr). Der geforderte Grad der Wahrscheinlichkeit wird davon beeinflusst, welche Möglichkeit der Beschwerdeführer hat, seine Betroffenheit darzulegen. So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Beschwerdeführer selbst einer Straftat oder als möglicher Verursacher einer Gefahr für die öffentliche Sicherheit bezichtigen müsste, dürfen zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden (vgl. BVerfGE 109, 279 <308>; 113, 348 <363>; 120, 378 <396>).

87

Die Darlegungen des Beschwerdeführers genügen diesen Anforderungen. Zwar kann der Beschwerdeführer eine spezifische Wahrscheinlichkeit, von der Speicherung betroffen zu werden, nur begrenzt aufzeigen. Er verweist im Wesentlichen lediglich auf Kontakte zu möglicherweise dem Terrorismus nahestehenden Personen. Angesichts der großen Streubreite der von der Speicherung in der Antiterrordatei möglicherweise erfassten Personen sind seine Ausführungen jedoch noch ausreichend. Nach § 2 Satz 1 ATDG werden Daten nicht nur von Terrorismusverdächtigen und deren Unterstützern, sondern in weitem Umfang auch von nur dem Umkreis des Terrorismus zugerechneten Personen bis hin

zu bloßen Kontaktpersonen - und zwar einschließlich solcher, die von einem Terrorismusbezug ihres Kontaktes nichts wissen - erfasst.

C.

88

Die Verfassungsbeschwerde gibt keinen Anlass für ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof gemäß Art. 267 AEUV zur Klärung der Reichweite des unionsrechtlichen Grundrechtsschutzes in Bezug auf einen Datenaustausch von verschiedenen Sicherheitsbehörden im Rahmen einer Verbunddatei, wie ihn das Antiterrordateigesetz regelt. Dies gilt auch im Hinblick auf das Grundrecht auf Schutz personenbezogener Daten gemäß Art. 8 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta – EuGRCh). Denn die europäischen Grundrechte der Grundrechtecharta sind auf den zu entscheidenden Fall nicht anwendbar. Die angegriffenen Vorschriften sind schon deshalb an den Grundrechten des Grundgesetzes zu messen, weil sie nicht durch Unionsrecht determiniert sind (vgl. BVerfGE 118, 79 <95>; 121, 1 <15>; 125, 260 <306 f.>; 129, 78 <90 f.>). Demzufolge liegt auch kein Fall der Durchführung des Rechts der Europäischen Union vor, die allein die Bindung der Mitgliedstaaten an die Grundrechtecharta nach sich ziehen könnte (Art. 51 Abs. 1 Satz 1 EuGRCh).

89

Allerdings betreffen die angegriffenen Vorschriften die Ermöglichung eines Datenaustauschs zur Bekämpfung des internationalen Terrorismus und damit Fragen, die zum Teil auch Regelungsbereiche des Unionsrechts berühren. So verfügt die Europäische Union für Regelungen zum Datenschutz in Art. 16 AEUV über eigene Kompetenzen. Dabei legt etwa die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23. November 1995, S. 31 ff. – Datenschutz-Richtlinie) wesentliche Anforderungen an die Datenverarbeitung fest, die grundsätzlich sowohl für Private als auch für öffentliche Behörden gelten. Entsprechend kennt das Unionsrecht diverse Kompetenz- und Rechtsgrundlagen im Zusammenhang mit der Terrorismusabwehr. Insbesondere sieht Art. 2 des Beschlusses 2005/671/JI des Rates vom 20. September 2005 über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten (ABl. L 253 vom 29. September 2005, S. 22 ff.) vor, dass die Mitgliedstaaten nach Maßgabe der innerstaatlichen Vorschriften alle einschlägigen Informationen über die von ihren Strafverfolgungsbehörden durchgeführten strafrechtlichen Ermittlungsergebnisse zu terroristischen Straftaten an Eurojust, Europol und die anderen Mitgliedstaaten weiterzuleiten haben. Das Antiterrordateigesetz und die hierdurch erstrebte Effektivierung der Zusammenarbeit der Sicherheitsbehörden steht somit auch in unionsrechtlichen Bezügen und wirkt sich, wenn im Wege des durch das Antiterrordateigesetz angestoßenen Informationsaustauschs weitergehende Ergebnisse gewonnen werden, mittelbar auch auf den Umfang der unionsrechtlichen Berichtspflichten aus. Ebenso bestehen Anknüpfungspunkte zum Unionsrecht in Bezug auf die Pflichten zum Erlass von restriktiven Maßnahmen gegen bestimmte Personen und Organisationen zur Bekämpfung des Terrorismus nach der Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001 (ABl. L 344 vom 28. Dezember 2001, S. 70 ff.). Auch sonst können und müssen gegebenenfalls die Ergebnisse der durch die Antiterrordatei effektivierten Zusammenarbeit in die zahlreichen unionsrechtlich geregelten Rechtsbeziehungen im Rahmen der justiziellen Zusammenarbeit einfließen.

90

Gleichwohl ist unzweifelhaft und – im Übrigen auch nach den Maßstäben der Acte-claire-Rechtsprechung des Europäischen Gerichtshofs (EuGH, Urteil vom 6. Oktober 1982, Rs. C-283/81, C.I.L.F.I.T., Slg. 1982, S. 3415 Rn. 16 ff.) – keiner weiteren Klärung bedürftig, dass das Antiterrordateigesetz und die auf seiner Grundlage erfolgende Tätigkeit der Sicherheitsbehörden und Nachrichtendienste keine Durchführung des Rechts der Union im Sinne des Art. 51 Abs. 1 Satz 1 EuGRCh darstellen. Für die Datenschutzrichtlinie ergibt sich dies schon aus Art. 3 Abs. 2 der Richtlinie 95/46/EG, die die Datenverarbeitung betreffend die öffentliche Sicherheit, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich ausdrücklich aus ihrem Anwendungsbereich ausnimmt. Auch sonst ist die Einrichtung und Ausgestaltung der Antiterrordatei nicht durch Unionsrecht determiniert. Insbesondere gibt es keine unionsrechtliche Bestimmung, die die Bundesrepublik Deutschland zur Einrichtung einer solchen Datei verpflichtet, sie daran hindert oder ihr diesbezüglich inhaltliche Vorgaben macht. Das Antiterrordateigesetz verfolgt vielmehr innerstaatlich bestimmte Ziele, die das Funktionieren unionsrechtlich geordneter Rechtsbeziehungen nur mittelbar beeinflussen können, was für eine Prüfung am Maßstab unionsrechtlicher Grundrechtsverbürgungen nicht genügt (vgl. EuGH, Urteil vom 18. Dezember 1997, C-309/96, Annibaldi, Slg. 1997, S. I-7493 Rn. 22). Eine Anwendbarkeit der Unionsgrundrechte scheidet damit von vornherein aus. Es ergibt sich unmittelbar aus dem Wortlaut des Art. 51 Abs. 2 EuGRCh wie auch aus Art. 6 Abs. 1 des Vertrags über die Europäische Union, dass die Charta den Geltungsbereich des Unionsrechts nicht über die Zuständigkeiten der Union hinaus ausdehnt und weder neue Zuständigkeiten noch neue Aufgaben für die Union begründet noch die in den Verträgen festgelegten Zuständigkeiten und Aufgaben ändert (vgl. auch EuGH, Urteil vom 15. November 2011, C-256/11, Dereci u.a., Rn. 71; EuGH,

Urteil vom 8. November 2012, C-40/11, Iida, Rn. 78; EuGH, Urteil vom 27. November 2012, C-370/12, Pringle, Rn. 179 f.).

91

Der Europäische Gerichtshof ist danach für die aufgeworfenen – ausschließlich die deutschen Grundrechte betreffenden – Fragen nicht gesetzlicher Richter im Sinne des Art. 101 Abs. 1 GG. Nichts anderes kann sich aus der Entscheidung des EuGH in der Rechtssache Åkerberg Fransson (EuGH, Urteil vom 26. Februar 2013, C-617/10) ergeben. Im Sinne eines kooperativen Miteinanders zwischen dem Bundesverfassungsgericht und dem Europäischen Gerichtshof (vgl. BVerfGE 126, 286 <307>) darf dieser Entscheidung keine Lesart unterlegt werden, nach der diese offensichtlich als Ultra-vires-Akt zu beurteilen wäre oder Schutz und Durchsetzung der mitgliedstaatlichen Grundrechte in einer Weise gefährdete (Art. 23 Abs. 1 Satz 1 GG), dass dies die Identität der durch das Grundgesetz errichteten Verfassungsordnung in Frage stellte (vgl. BVerfGE 89, 155 <188>; 123, 267 <353 f.>; 125, 260 <324>; 126, 286 <302 ff.>; 129, 78 <100>). Insofern darf die Entscheidung nicht in einer Weise verstanden und angewendet werden, nach der für eine Bindung der Mitgliedstaaten durch die in der Grundrechtecharta niedergelegten Grundrechte der Europäischen Union jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrecht oder rein tatsächliche Auswirkungen auf dieses ausreiche. Vielmehr führt der Europäische Gerichtshof auch in dieser Entscheidung ausdrücklich aus, dass die Europäischen Grundrechte der Charta nur in „unionsrechtlich geregelten Fallgestaltungen, aber nicht außerhalb derselben Anwendung finden“ (EuGH, Urteil vom 26. Februar 2013, C-617/10, Rn. 19).

D.

92

Die Verfassungsbeschwerde ist teilweise begründet.

I.

93

Die angegriffenen Vorschriften greifen in den Schutzbereich des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), des Brief- und Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) und des Rechts auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) ein.

94

1. Die §§ 1 bis 6 ATDG regeln die Speicherung und Verwendung personenbezogener Daten und berühren damit den Schutzbereich des Rechts auf informationelle Selbstbestimmung. Soweit die von der Speicherung und Verwendung betroffenen Daten durch Eingriff in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG erhoben wurden, ist auch deren Folgeverwendung an diesen Grundrechten zu messen (vgl. BVerfGE 125, 260 <313>; stRspr).

95

2. Die Vorschriften greifen in diese Grundrechte ein. Ein Eingriff liegt dabei zunächst in der Verknüpfung der Daten aus verschiedenen Quellen durch die Anordnung einer Speicherungspflicht gemäß §§ 1 bis 4 ATDG. Dem steht nicht entgegen, dass es sich bei den Daten um bereits anderweitig erhobene Daten handelt, denn sie werden nach eigenen Kriterien zusammengeführt und aufbereitet, um sie anderen Behörden als denen, die sie erhoben haben, zu deren Zwecken zur Verfügung zu stellen. Weitere Eingriffe liegen in den Regelungen zur Verwendung der Daten gemäß den §§ 5 und 6 ATDG in Form von Recherchen, in der Zugriffsmöglichkeit auf die einfachen Grunddaten im Trefferfall gemäß § 5 Abs. 1 Satz 1 und 2, § 6 Abs. 1 Satz 1 ATDG sowie in der Zugriffsmöglichkeit auch auf die erweiterten Grunddaten im Eilfall gemäß § 5 Abs. 2, § 6 Abs. 2 ATDG.

II.

96

Die angegriffenen Vorschriften sind in formeller Hinsicht mit der Verfassung vereinbar. Insbesondere werden die Grenzen der Bundeskompetenzen eingehalten.

97

1. Soweit das Antiterrordateigesetz den Austausch von Informationen zwischen dem Bundeskriminalamt, den Landeskriminalämtern, dem Bundesverfassungsschutz, den Landesverfassungsschutzbehörden sowie weiteren Polizeivollzugsbehörden regelt, kann sich der Bund auf die Gesetzgebungskompetenzen des Art. 73 Abs. 1 Nr. 10 a bis c GG zur Zusammenarbeit der Behörden stützen. Zusammenarbeit ist eine auf Dauer angelegte Form der Kooperation, die die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse umfasst und funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und gemeinsame Informationssysteme erlaubt (vgl. Uhle, in:

Maunz/Dürig, GG, Art. 73 Rn. 231 [Apr. 2010]). Hierunter fällt auch die durch das Antiterrordateigesetz vorgesehene Zusammenarbeit.

98

Die Kompetenz für die Zusammenarbeit zwischen den verschiedenen Polizeibehörden beschränkt sich nicht auf die Strafverfolgung. Art. 73 Abs. 1 Nr. 10 GG soll die Möglichkeit schaffen, föderale Zuständigkeitsgrenzen bei der Erfüllung repressiver und präventiver Aufgaben zu lockern. Der Begriff „Kriminalpolizei“ in Art. 73 Abs. 1 Nr. 10 a GG schließt nicht aus, dass der Bund eine Zusammenarbeit auch zur Verhinderung von Straftaten regeln kann, sondern dient lediglich der Beschränkung auf Regelungen, die sich auf bedeutsame Straftaten von Gewicht beziehen (Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 239 ff. [Apr. 2010]; Heintzen, in: v. Mangoldt/Klein/Starck, GG, Bd. 2, 6. Aufl. 2010, Art. 73 Rn. 114; Stettner, in: Dreier, GG, Bd. 2, 2. Aufl. 2006, Art. 73 Rn. 43; Werthebach/Droste, in: Bonner Kommentar, Bd. 9, Art. 73 Nr. 10 Rn. 109, 118 ff. [Dez. 1998]).

99

Dem Rückgriff auf Art. 73 Abs. 1 Nr. 10 GG steht nicht entgegen, dass das Antiterrordateigesetz eine Zusammenarbeit der Polizei- und Verfassungsschutzbehörden nicht nur fachlich, sondern zugleich fachübergreifend regelt. Art. 73 Abs. 1 Nr. 10 GG erlaubt auch solche fachübergreifenden Regelungen. Dies entspricht nicht nur einem funktionalen Verständnis der Norm, die allgemein eine Effektivierung der Zusammenarbeit der verschiedenen Sicherheitsbehörden über föderale Kompetenzgrenzen hinweg ermöglichen will, sondern wird auch durch ihre ursprüngliche Fassung nahegelegt, die noch nicht in einzelne Buchstaben aufgegliedert war. Den Materialien lässt sich ebenfalls nichts für ein engeres Verständnis entnehmen. Die Änderung der Vorschrift im Jahr 1972 hatte nicht das Ziel, der Norm in dieser Hinsicht einen anderen Sinn zu geben (vgl. BTDrucks VI/1479).

100

2. Soweit § 1 Abs. 1 ATDG als weitere Behörden den Bundesnachrichtendienst, den Militärischen Abschirmdienst, das Zollkriminalamt und die Bundespolizei mit einbezieht, findet dies in Art. 73 Abs. 1 Nr. 1 und Nr. 5 GG eine Kompetenzgrundlage.

101

Die Kompetenz für die Einbeziehung des Bundesnachrichtendienstes ergibt sich aus der Zuständigkeit des Bundes für die Regelung der auswärtigen Beziehungen gemäß Art. 73 Abs. 1 Nr. 1 GG. Allerdings sind die dem Bund insoweit zugewiesenen Kompetenzen durch die Verteilung der Gesetzgebungskompetenzen im Übrigen geprägt und berechtigen den Gesetzgeber nicht, dem Bundesnachrichtendienst allein deshalb, weil es sich um Fälle mit Auslandsbezug handelt, Befugnisse einzuräumen, die auf die Verhütung, Verhinderung oder Verfolgung von Taten als solche gerichtet sind (vgl. BVerfGE 100, 313 <368 ff.>). Vielmehr müssen Regelungen, damit sie auf die Gesetzgebungskompetenz aus Art. 73 Abs. 1 Nr. 1 GG gestützt werden können, in einen Regelungs- und Verwendungszusammenhang eingebettet sein, der auf die Auslandsaufklärung bezogen ist und der politischen Information der Bundesregierung dient (vgl. BVerfGE 100, 313 <370 f.>). Die Beteiligung des Bundesnachrichtendienstes an der Antiterrordatei ist hiermit jedoch vereinbar. Dies gilt zunächst insoweit, als die §§ 5 und 6 ATDG dem Bundesnachrichtendienst Zugriff auf die in der Antiterrordatei gespeicherten Daten ermöglichen. Denn ein Zugriff ist nach diesen Vorschriften nur für die jeweiligen Aufgaben der abfragenden Behörden eröffnet; dem Bundesnachrichtendienst werden damit also keine weiteren, allgemein auf die Verhinderung von Straftaten des internationalen Terrorismus gerichtete Kompetenzen zugewiesen. Hiermit vereinbar ist aber auch, dass der Bundesnachrichtendienst seine eigenen Daten durch Einstellung in die Datei anderen Behörden zugänglich macht. Denn das Antiterrordateigesetz begründet keine neuen, durch Art. 73 Abs. 1 Nr. 1 GG nicht mehr gedeckten Datenerhebungsbefugnisse, sondern knüpft an die jeweils für die eigene Aufgabenerfüllung erhobenen Daten an und verpflichtet lediglich dazu, diese Daten anderen Behörden für deren Aufgaben zugänglich zu machen. Die Regelung des Umfangs solcher zweckändernder Bereitstellung von Daten für andere Aufgabenträger ist kraft Sachzusammenhangs Teil der jeweiligen Kompetenz für die Datenerhebung und den hiermit korrespondierenden Datenschutz (vgl. BVerfGE 125, 260 <314 f.>). Der Gesetzgeber gestaltet hierdurch den Bundesnachrichtendienst nicht in eine vorgelagerte Polizeibehörde um.

102

Entsprechend kann der Bund die Beteiligung des Militärischen Abschirmdienstes auf Art. 73 Abs. 1 Nr. 1 GG (Verteidigung) und der Bundespolizei sowie des Zollkriminalamts auf Art. 73 Abs. 1 Nr. 5 GG (Zoll- und Grenzschutz) stützen. Auch hier tragen die Vorschriften sowohl die Eröffnung eines Zugriffs dieser Behörden auf die Daten als auch die Pflicht zur Einstellung ihrer Daten in die Antiterrordatei.

103

Demgegenüber ließe sich auf Art. 73 Abs. 1 Nr. 1 und 5 GG keine Regelung stützen, die es den anderen an der Antiterrordatei beteiligten Behörden unmittelbar erlaubte, die von diesen Bundesbehörden eingestellten Daten abzurufen. Eine solche Regelung ist im Antiterrordateigesetz auch nicht enthalten. Vielmehr setzt § 5 Abs. 1 und 2 ATDG bei sachgerechtem Verständnis für die Nutzung der Datei seitens

der jeweils Zugriff nehmenden Behörden eigene Datenerhebungsvorschriften, gegebenenfalls auf Landesebene, voraus (vgl. BVerfGE 125, 260 <315>; 130, 151 <193>).

104

3. Dahinstehen kann, ob es für die Führung der Antiterrordatei als Verbunddatei zusätzlich einer Verwaltungskompetenz des Bundes bedarf. Denn eine solche Kompetenz ergäbe sich für die beim Bundeskriminalamt geführte Antiterrordatei jedenfalls aus der Befugnis zur Einrichtung von Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen gemäß Art. 87 Abs. 1 Satz 2 GG.

III.

105

Die durch die angegriffenen Vorschriften errichtete Antiterrordatei ist in ihren Grundstrukturen mit dem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG vereinbar. Der Grundsatz der Verhältnismäßigkeit steht einer solchen Datei, die im Rahmen der Aufklärung und Bekämpfung des internationalen Terrorismus der Informationsanbahnung und in Eilfällen auch der Gefahrenabwehr dient, nicht schon grundsätzlich entgegen. Ihre nähere normative Ausgestaltung muss jedoch auch in ihren Einzelbestimmungen dem Verhältnismäßigkeitsgrundsatz genügen.

106

1. Die Antiterrordatei ist auf ein legitimes Ziel gerichtet. Sie soll den Sicherheitsbehörden in erster Linie schnell und einfach Kenntnis darüber verschaffen, ob bei anderen Sicherheitsbehörden relevante Informationen zu bestimmten Personen aus dem Umfeld des internationalen Terrorismus vorliegen. Damit will sie Vorinformationen vermitteln, mit denen diese Behörden schneller und zielführender Informationssuchen bei anderen Behörden stellen können und die in dringenden Fällen auch eine erste handlungsleitende Gefahreinschätzung ermöglichen. Der Gesetzgeber erstrebt nicht einen allgemeinen Austausch personenbezogener Daten aller Sicherheitsbehörden oder den Abbau jeglicher Informationsgrenzen zwischen ihnen; dies würde den Grundsatz der Zweckbindung als solchen unterlaufen und wäre dann von vornherein unzulässig. Er beabsichtigt und schafft vielmehr nur eine begrenzte Erleichterung des Informationsaustauschs, der die grundsätzliche Maßgeblichkeit der fachrechtlich begrenzten Einzelübermittlungsvorschriften unberührt lässt und sachlich auf die Bekämpfung des internationalen Terrorismus beschränkt ist. Zwar ist der Begriff des „Terrorismus“ nicht aus sich heraus eindeutig. Das Antiterrordateigesetz orientiert sich jedoch, wie sich aus § 2 Satz 1 Nr. 1 a ATDG, der zentralen Bestimmung zu den in der Datei erfassten Personen, ergibt, an § 129a StGB und versteht hierunter konkret definierte, schwerwiegende Straftaten, die auf die Einschüchterung der Bevölkerung oder gegen die Grundstrukturen eines Staates oder einer internationalen Organisation gerichtet sind. Hiergegen bestehen keine verfassungsrechtlichen Bedenken.

107

2. Die angegriffenen Vorschriften sind zur Erreichung dieses Ziels auch geeignet und erforderlich. Mit den gemäß §§ 1 bis 4 ATDG begründeten Speicherungspflichten wird ein Grunddatenbestand geschaffen, der den beteiligten Behörden in § 5 Abs. 1, § 6 Abs. 1 Satz 1 ATDG zur Vorbereitung weiterer Informationsabfragen zur Verfügung gestellt wird und ihnen gemäß § 5 Abs. 2, § 6 Abs. 2 ATDG in besonders dringenden Fällen Informationen zur Abwehr spezifischer Gefahren vermitteln soll. Ein anderes Instrumentarium, das diese Ziele vergleichbar effektiv und weniger belastend sicherstellt, ist nicht ersichtlich.

108

3. Das Antiterrordateigesetz ist in seinen Grundstrukturen auch mit dem Grundsatz der Verhältnismäßigkeit im engeren Sinne vereinbar.

109

Das Gebot der Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere der gesetzgeberischen Grundrechtsbeschränkung bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der sie rechtfertigenden Gründe steht. Dabei ist ein angemessener Ausgleich zwischen dem Eingriffsgewicht der Regelung und dem verfolgten gesetzgeberischen Ziel, zwischen Individual- und Allgemeininteresse herzustellen (vgl. BVerfGE 100, 313 <375 f.>; 113, 348 <382>; 120, 378 <428>; stRspr.).

110

Die angegriffenen Vorschriften sind von erheblichem Eingriffsgewicht (a). Dem stehen jedoch gewichtige öffentliche Belange gegenüber (b). Bei einer Abwägung sind gegen die Errichtung und den Charakter der Antiterrordatei keine grundsätzlichen verfassungsrechtlichen Bedenken zu erheben; es bedarf für die nähere Ausgestaltung der Datei jedoch normenklarer und hinreichend begrenzender Regelungen einschließlich von Bestimmungen zu einer effektiven Kontrolle ihrer Anwendung (c).

111

a) Der durch die angegriffenen Vorschriften geschaffene Informationsaustausch ist von erheblichem Gewicht. Dies ergibt sich aus dem Zusammenwirken der hierfür maßgeblichen Grundrechtseingriffe, die nicht isoliert betrachtet werden können: Das Gewicht der Speicherung der einzustellenden Daten und die Frage ihres zulässigen Umfangs bemessen sich maßgeblich nach Zweck und Charakter der Datei, ebenso wie umgekehrt das Gewicht der Datenverwendung wesentlich vom Umfang der Speicherungspflicht abhängt. Als ein die Schwere des Eingriffs erhöhender Faktor fällt ins Gewicht, dass durch die Datei ein Informationsaustausch zwischen zahlreichen Sicherheitsbehörden mit sehr unterschiedlichen Aufgaben ins Werk gesetzt wird und dieser insbesondere auch den Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden umfasst (aa). Gemindert wird die Schwere des Eingriffs durch die Beschränkung auf bereits erhobene Daten, die Ausgestaltung als Verbunddatei mit einem Schwerpunkt auf der Informationsanbahnung und ihre Ausrichtung allein auf das Ziel der Aufklärung und Bekämpfung des internationalen Terrorismus (bb).

112

aa) Das Eingriffsgewicht der Antiterrordatei ist dadurch erhöht, dass sie einen Informationsaustausch zwischen einer großen Zahl von Sicherheitsbehörden mit zum Teil deutlich verschiedenen Aufgaben und Befugnissen ermöglicht. Bedeutung hat hierbei insbesondere, dass sie auch den Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden umfasst.

113

(1) Die den verschiedenen Sicherheitsbehörden jeweils eingeräumten Datenerhebungs- und –verarbeitungsbefugnisse sind, soweit es um personenbezogene Daten geht, auf ihre spezifischen Aufgaben zugeschnitten und durch sie begrenzt. Entsprechend unterliegen die Daten von Verfassungen wegen hinsichtlich ihrer Verwendung Zweckbindungen und können nicht ohne weiteres an andere Behörden übermittelt werden. Die Aufgliederung der Sicherheitsbehörden nach fachlichen und föderalen Gesichtspunkten entfaltet damit für den Datenschutz auch eine besondere grundrechtliche Dimension. Dass Informationen zwischen den verschiedenen Sicherheitsbehörden nicht umfassend und frei ausgetauscht werden, ist nicht Ausdruck einer sachwidrigen Organisation dieser Behörden, sondern von der Verfassung durch den datenschutzrechtlichen Grundsatz der Zweckbindung grundsätzlich vorgegeben und gewollt.

114

Allerdings schließt der verfassungsrechtliche Grundsatz der Zweckbindung von Daten Zweckänderungen durch den Gesetzgeber nicht aus, wenn diese durch Gemeinwohlbelange gerechtfertigt sind, die die grundrechtlich geschützten Interessen überwiegen (vgl. BVerfGE 100, 313 <360>; 109, 279 <375 f.>; 110, 33 <69>). Für die Beurteilung der Verhältnismäßigkeit eines Informationsaustauschs zwischen verschiedenen Behörden kommt es 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. Für die Verfassungsmäßigkeit solcher Zweckänderungen ist deshalb insbesondere maßgeblich, wieweit die Bindungen der Datenerhebung seitens der übermittelnden oder hier der einstellenden Behörde denen entsprechen, unter denen die abfragenden Behörden Daten erheben können. Ausgeschlossen ist eine Zweckänderung danach dann, wenn mit ihr grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Ermittlungsmethoden umgangen werden, also die Informationen für den geänderten Zweck selbst auf entsprechender gesetzlicher Grundlage nicht oder nicht in dieser Art und Weise erhoben werden dürfen (vgl. BVerfGE 109, 279 <377>; 120, 351 <369>). Dementsprechend hat das Bundesverfassungsgericht wiederholt entschieden, dass die Weiterverwendung von Daten, die aus Eingriffen in das Fernmeldegeheimnis herrühren, nur für Zwecke verfassungsmäßig ist, die auch als Rechtfertigung für die ursprüngliche Erhebung ausgereicht hätten (vgl. BVerfGE 100, 313 <360, 389>; 109, 279 <375 f.>; 110, 33 <73>), und hat zur Gewährleistung dieser Anforderungen verfahrensrechtliche Sicherungen wie Kennzeichnungs- und Protokollierungspflichten für erforderlich gehalten (vgl. BVerfGE 65, 1 <46>; 113, 29 <58>; 124, 43 <70>). Entsprechendes gilt auch für Zweckänderungen der Datenverarbeitung, wenn Daten durch Eingriff in das Recht auf informationelle Selbstbestimmung erhoben wurden. Verfassungsrechtliche Voraussetzungen für die Erhebung, Speicherung und Verarbeitung von Daten dürfen nicht dadurch unterlaufen werden, dass Behörden, für die aufgrund ihrer Aufgabenstellung weniger strenge Anforderungen gelten, Daten im Wege der Übermittlung an Behörden weiterleiten, die ihrerseits strengeren Anforderungen unterliegen.

115

(2) Danach hat die Zusammenführung von Daten der Nachrichtendienste und der Polizeibehörden erhöhtes Gewicht und unterliegt grundsätzlich verfassungsrechtlich engen Grenzen. Denn Polizeibehörden und Nachrichtendienste haben deutlich voneinander unterschiedene Aufgaben. Dementsprechend unterliegen sie hinsichtlich der Offenheit ihrer Aufgabenwahrnehmung sowie bezüglich der Datenerhebung grundlegend verschiedenen Anforderungen.

116

(aa) Den Nachrichtendiensten kommt die Aufgabe zu, Aufklärung bereits im Vorfeld von Gefährdungslagen zu betreiben. Ihr Datenzugriff dient dabei zugleich verschiedenartigen und weit gefassten Zielen wie dem Schutz vor verfassungsfeindlichen Bestrebungen im Inland und vor innerstaatlichen Tätigkeiten ausländischer Geheimdienste, dem Schutz vor gewaltbereiten Bestrebungen, die den gesamten Bereich der „auswärtigen Belange“ gefährden, oder dem Schutz vor Bestrebungen, die gegen den Gedanken der Völkerverständigung oder das friedliche Zusammenleben der Völker gerichtet sind (vgl. § 3 Abs. 1 BVerfSchG, § 1 Abs. 2 BNDG, § 1 Abs. 1 MADG sowie § 1 Abs. 1 i.V.m. § 3 Abs. 1 und § 5 Abs. 1 G 10). Sie haben mannigfaltige Bestrebungen auf ihr Gefahrenpotenzial hin allgemein zu beobachten und sie gerade auch unabhängig von konkreten Gefahren in den Blick zu nehmen (vgl. BVerfGE 122, 120 <145>).

117

Diesem vorfeldbezogenen Aufgabenspektrum entsprechend haben die Nachrichtendienste weitreichende Befugnisse zur Datensammlung, die weder hinsichtlich der konkreten Tätigkeitsfelder spezifisch ausdefiniert noch hinsichtlich der jeweils einzusetzenden Mittel detailscharf ausgestaltet sind. Für die Behörden des Verfassungsschutzes umfassen sie Methoden und Instrumente zur heimlichen Informationsbeschaffung wie etwa den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen (vgl. § 8 Abs. 2 BVerfSchG; § 6 Abs. 1 LVSG Baden-Württemberg). Nach § 5 G 10 darf der Bundesnachrichtendienst zur Informationsgewinnung in bestimmten Fällen mit dem Instrument der strategischen Überwachung internationale Telekommunikationsbeziehungen nach bestimmten Suchbegriffen durchfiltern (vgl. BVerfGE 100, 313 <368 ff.> zur Vorgängervorschrift des § 3 Abs. 1 G 10 a.F.). Unbeschadet der auch hier differenzierten verfassungsrechtlichen Anforderungen, die nicht Gegenstand des vorliegenden Verfahrens sind, spiegeln diese Befugnisse die Weite der Aufgaben der Nachrichtendienste und zeichnen sich durch relativ geringe Eingriffsschwellen aus. Überdies sammeln die Nachrichtendienste Daten grundsätzlich geheim. Der Grundsatz der Offenheit der Datenerhebung gilt für sie nicht, und sie sind von Transparenz- und Berichtspflichten gegenüber den Betroffenen weithin freigestellt. Entsprechend gering sind die Möglichkeiten individuellen Rechtsschutzes. Zum Teil werden diese sogar ganz durch eine politische Kontrolle ersetzt (vgl. Art. 10 Abs. 2 Satz 2 GG).

118

Im Gegenzug und zum Ausgleich zu der Weite dieser Datenerhebungsbefugnisse ist die Zielrichtung der Aufklärung begrenzt. Unbeschadet näherer Differenzierungen zwischen den verschiedenen Diensten beschränkt sie sich im Wesentlichen darauf, fundamentale Gefährdungen, die das Gemeinwesen als Ganzes destabilisieren können, zu beobachten und hierüber zu berichten, um eine politische Einschätzung der Sicherheitslage zu ermöglichen. Ziel ist nicht die operative Gefahrenabwehr, sondern die politische Information. So ist Aufgabe der Tätigkeit des Bundesnachrichtendienstes nicht die Bekämpfung von Straftaten als solchen, sondern übergreifend die Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. In Form von Lageberichten, Analysen und Berichten über Einzelerkenntnisse soll die Bundesregierung in den Stand gesetzt werden, Gefahrenlagen rechtzeitig zu erkennen und ihnen – politisch – zu begegnen (vgl. BVerfGE 100, 313 <371>). Entsprechend zielt auch die Aufklärung der Verfassungsschutzbehörden nicht unmittelbar auf die Verhütung und Verhinderung von konkreten Straftaten oder die Vorbereitung entsprechender operativer Maßnahmen. Auch hier beschränkt sich die Aufgabe der Dienste auf eine Berichtspflicht gegenüber den politisch verantwortlichen Staatsorganen beziehungsweise der Öffentlichkeit (vgl. BVerfGE 130, 151 <206>).

119

Dieser auf die politische Vorfeldaufklärung beschränkte Auftrag der Nachrichtendienste spiegelt sich auch in einer Beschränkung ihrer Befugnisse: Polizeiliche Befugnisse haben sie nicht, und sie dürfen auch im Wege der Amtshilfe nicht die Polizei um Maßnahmen ersuchen, zu denen sie selbst nicht befugt sind (vgl. § 8 Abs. 3 BVerfSchG, § 2 Abs. 3 BNDG, § 4 Abs. 2 MADG, § 3 Abs. 4 des Hessischen Gesetzes über das Landesamt für Verfassungsschutz [VerfSchutzG HE]). Im Falle eines Übermittlungersuchens dürfen sie grundsätzlich nur solche Daten übermitteln, die bei der ersuchten Behörde bereits bekannt sind oder aus allgemein zugänglichen Quellen entnommen werden können (vgl. etwa § 17 Abs. 1 BVerfSchG – auch i.V.m. § 8 Abs. 3 Satz 2 BNDG und § 10 Abs. 4 MADG –, § 8 Abs. 2 Satz 2 VerfSchutzG HE, § 19 Abs. 1 i.V.m. § 7 Abs. 2 Satz 1 HmbVerfSchG).

120

(bb) Von diesem Aufgaben- und Befugnisprofil unterscheidet sich das der Polizei- und Sicherheitsbehörden grundlegend. Ihnen obliegt die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung. Ihre Aufgaben sind geprägt von einer operativen Verantwortung und insbesondere der Befugnis, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen. Dabei sind ihre Aufgaben gesetzlich differenziert umgrenzt und durch ein materiell wie verfahrensrechtlich vielfältig abgestuftes Arsenal von Handlungsbefugnissen unterlegt. Unbeschadet gewisser Aufgaben auch dieser Behörden schon im Vorfeld von Gefahren, sind ihnen Befugnisse gegenüber Einzelnen grundsätzlich nur aus

konkretem Anlass verliehen; Voraussetzung ist in der Regel, dass Anhaltspunkte für einen Tatverdacht oder eine Gefahr vorliegen. Diesem Aufgabenprofil entsprechen auch die Datenerhebungs- und –verarbeitungsbefugnisse dieser Behörden. Sie sind, da sie letztlich Zwangsmaßnahmen bis hin zu Eingriffen in die persönliche Freiheit vorbereiten und begründen können, gesetzlich wesentlich enger und präziser gefasst als diejenigen der Nachrichtendienste sowie vielfältig voneinander abgegrenzt. Entsprechend setzen grundsätzlich auch diese auf den Umgang mit Daten bezogenen Befugnisse – bei vielfältigen Abstufungen im Einzelnen – einen konkreten Anlass, etwa eine Gefahr oder einen Tatverdacht voraus. Soweit der Gesetzgeber die Erhebung personenbezogener Daten ausnahmsweise anlasslos vorsorglich oder zur bloßen Verhütung von Gefahren oder Straftaten erlaubt, ist dies besonders rechtfertigungsbedürftig und unterliegt gesteigerten verfassungsrechtlichen Anforderungen (vgl. BVerfGE 125, 260 <318 ff., 325 ff.>).

121

Entsprechend handelt die Polizei grundsätzlich offen und folgt auch ihr Umgang mit Daten ganz überwiegend dem Grundsatz der Offenheit. Zwar setzt die Aufgabenwahrnehmung der Polizeibehörden in erheblichem Umfang auch Ermittlungen voraus, die gegenüber den Betroffenen zunächst verdeckt erfolgen. Jedoch werden damit nur bestimmte, durch konkrete Verdachtsmomente unterlegte Aufklärungsmaßnahmen oder –phasen abgeschirmt, die die prinzipielle Offenheit der polizeilichen Arbeit unberührt lässt. Vor allem werden insofern die ermittelten Daten bei sich anschließenden Maßnahmen gegenüber Einzelnen – wie der Erhebung der Anklage oder dem Erlass einer Polizeiverfügung – offengelegt und wird dem Betroffenen Gelegenheit gegeben, sich hierzu zu verhalten. Auch die Ermittlungen selbst werden, soweit möglich, offen geführt. Im Strafverfahren zeigt sich dies beispielhaft an den zahlreichen Anhörungs-, Akteneinsichts- und Verteidigungsrechten des Beschuldigten, an der offenen Durchführung von Wohnungsdurchsuchungen (vgl. § 106 StPO), den Vorgaben für die Nutzung von vorsorglich gespeicherten Daten (vgl. BVerfGE 125, 260 <353>) sowie der grundsätzlich öffentlichen und mündlichen Verhandlung am Ende des Anklagevorwurfs im Strafverfahren. Der Einsatz verdeckter Ermittler (§§ 110a ff. StPO) und heimliche Datenerhebungen mit technischen Mitteln (§§ 100a ff. StPO) sind demgegenüber nur ausnahmsweise und unter bestimmten Bedingungen zulässig. Entsprechend unterliegt die Polizei auch im Bereich der Gefahrenabwehr dem Grundsatz der offenen Datenerhebung (vgl. § 21 Abs. 3 BPolG; § 19 Abs. 1 PolG Baden-Württemberg; Art. 30 Abs. 3 BayPAG).

122

Die Rechtsordnung unterscheidet damit zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung hin ausgerichtet und durch detaillierte Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten, die auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können. Eine Geheimpolizei ist nicht vorgesehen.

123

(cc) Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein informationelles Trennungsprinzip. Danach dürfen Daten zwischen den Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen der Datentrennung sind nur ausnahmsweise zulässig. Soweit sie zur operativen Aufgabenwahrnehmung erfolgen, begründen sie einen besonders schweren Eingriff. Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt. Dies muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein; auch die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei nicht unterlaufen werden.

124

bb) Das Eingriffsgewicht der Antiterrordatei ist allerdings dadurch gemindert, dass sie als Verbunddatei ausgestaltet ist, die in ihrem Kern auf die Informationsanbahnung beschränkt ist und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsieht.

125

(1) Die angegriffenen Vorschriften gestalten die Antiterrordatei als Instrumentarium aus, das – außerhalb des Eilfalls gemäß § 5 Abs. 2 und § 6 Abs. 2 ATDG – Informationen nicht unmittelbar zur Aufgabenwahrnehmung durch die jeweiligen Behörden, insbesondere nicht zu operativen Zwecken bereitstellt, sondern nur als Grundlage für weitere Datenübermittlungen. Die Antiterrordatei setzt zwar schon unmittelbar selbst einen Datenaustausch zwischen den beteiligten Behörden ins Werk, indem sie Recherchen in allen Grunddaten erlaubt und den abfragenden Behörden gemäß § 5 Abs. 1 Satz 1 und 2 ATDG einen Zugriff auf die einfachen Grunddaten des § 3 Abs. 1 Nr. 1 a ATDG gewährt. § 6 Abs. 1 Satz 1 ATDG bestimmt jedoch, dass die abfragende Behörde diese Daten nur zur Prüfung, ob sie der gesuchten

Person zuzuordnen sind, und für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung der jeweiligen Aufgabe der Behörde verwenden darf. Die so erlangten Informationen dürfen also grundsätzlich nur genutzt werden, um zu entscheiden, ob und gegenüber welcher Behörde um weitere Informationen nachgesucht werden soll, und um solche Einzelübermittlungsersuchen besser zu begründen. Für die Übermittlung von Daten aus den bei den Fachbehörden geführten Dateien auf Ersuchen im Einzelfall und damit auch zur operativen Aufgabenwahrnehmung ist demgegenüber das jeweils einschlägige Fachrecht maßgeblich. Die Antiterrordatei ermächtigt somit hinsichtlich der einfachen Grunddaten des § 3 Abs. 1 Nr. 1 a ATDG nicht zu einem Informationsaustausch für die Aufgabenwahrnehmung selbst, sondern bereitet ihn nur vor. Das gilt erst recht für die erweiterten Grunddaten des § 3 Abs. 1 Nr. 1 b ATDG, auf die den Behörden im Regelfall gemäß § 5 Abs. 1 Satz 4 ATDG bereits der Zugriff nur nach Maßgabe der fachrechtlichen Übermittlungsvorschriften eröffnet wird.

126

Das Antiterrordateigesetz stützt sich damit maßgeblich auf die fachrechtlichen Grundlagen für Datenübermittlungen und bezieht daraus rechtsstaatliche Grenzen. Im Ergebnis stellt es sicher, dass – außerhalb von § 5 Abs. 2, § 6 Abs. 2 ATDG – ein Austausch von Daten zur unmittelbaren Nutzung für die Aufklärung und Bekämpfung des internationalen Terrorismus nur unter den rechtlichen Voraussetzungen der einzelnen Übermittlungsvorschriften zulässig ist. Es fängt so die geringen, letztlich auf das Kriterium der Erforderlichkeit beschränkten Anforderungen für die Informationsanbahnung im Vorfeld durch Verweis auf die differenzierteren Grenzziehungen bei der Datenübermittlung auf. Diese müssen dann freilich ihrerseits den verfassungsrechtlichen Anforderungen genügen und können sich jedenfalls für Datenübermittlungen zwischen den Nachrichtendiensten und der Polizei nicht mit vergleichbar niederschweligen Voraussetzungen wie der Erforderlichkeit für die Aufgabenwahrnehmung oder der Wahrung der öffentlichen Sicherheit begnügen.

127

(2) Die grundsätzlich auf Informationsanbahnung beschränkte Funktion der Antiterrordatei mindert ihr Eingriffsgewicht wesentlich; dennoch bleibt das Eingriffsgewicht auch in dieser Funktion erheblich. Denn obgleich eine Datennutzung zur operativen Aufgabenwahrnehmung erst aufgrund weiterer Datenübermittlungsvorschriften zulässig ist, führt die Antiterrordatei im Vorfeld dieser Aufgabenwahrnehmung doch schon selbst zu einem unmittelbaren Austausch von Erkenntnissen der Behörden. Sie erlaubt der anfragenden Behörde im Falle eines Treffers nach § 5 Abs. 1 Satz 1 und 2 ATDG generell den Zugriff auf die Grunddaten des § 3 Abs. 1 Nr. 1 a ATDG als Klarinformationen und eröffnet die Möglichkeit zu Recherchen auch in den erweiterten Grunddaten des § 3 Abs. 1 Nr. 1 b ATDG, wobei insoweit im Trefferfall freilich allein ein Fundstellennachweis zu der informationsführenden Behörde und die korrespondierenden einfachen Grunddaten übermittelt werden. Als Instrument der Informationsanbahnung erleichtert die Antiterrordatei damit den fachrechtlichen Austausch und verleiht so den bestehenden Einzelübermittlungsvorschriften materiell ein verändertes Gewicht. Es stellt diese in ein anderes, nun vorinformiertes Umfeld und bewirkt den Austausch von Erkenntnissen für Fälle, in denen er andernfalls unpraktikabel oder unmöglich wäre. Die Antiterrordatei stellt sich so als vorgelagerter Bestandteil dieses fachgesetzlichen Austauschs dar.

128

Die Aufnahme in eine solche Datei kann für die Betroffenen erheblich belastende Wirkung haben. Wer einmal in der Datei erfasst ist, muss damit rechnen, aufgrund einer Abfrage dem Umkreis des Terrorismus zugeordnet und – mittels weiterer, dadurch erleichterter Übermittlungsersuchen – hieran anknüpfenden belastenden Maßnahmen unterworfen zu werden. Die Konsequenzen einer solchen Zuordnung können beträchtlich sein und Einzelne in schwierige Lagen bringen, ohne dass sie um diese Einordnung wissen und eine praktikable Möglichkeit haben, sich hiergegen zu wehren. Die Erheblichkeit dieses Eingriffs verstärkt sich dadurch, dass die Daten abgelöst von den jeweiligen konkreten Hintergründen in der Datei registriert werden und zum Teil auf bloßen Prognosen und subjektiven Einschätzungen der Behörden beruhen können, die naturgemäß unsicher sind. Letztlich können Bürgerinnen und Bürger hierdurch erheblichen Beeinträchtigungen ausgesetzt werden, ohne dafür selbst zurechenbar Anlass gegeben zu haben. Dass belastende Maßnahmen dabei grundsätzlich nicht unmittelbar auf eine Nutzung der Daten der Antiterrordatei nach den angegriffenen Vorschriften allein gestützt werden können, sondern als deren mittelbare Wirkung in Verbindung mit weiteren Vorschriften drohen, ändert nichts daran, dass die Wahrscheinlichkeit solcher Maßnahmen durch die Antiterrordatei erhöht wird.

129

(3) Ein besonders schweres Eingriffsgewicht kommt der Antiterrordatei insoweit zu, als sie in Eilfällen auch einen Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden erlaubt, bei dem die Informationen unmittelbar zur Abwehr von spezifischen Gefahren und damit auch zu operativen Zwecken genutzt werden dürfen.

130

b) Die Einrichtung der Antiterrordatei ist mit dem Übermaßverbot grundsätzlich vereinbar. Dem Eingriffsgewicht für die Betroffenen steht das öffentliche Interesse gegenüber, für die Aufklärung und

Bekämpfung des internationalen Terrorismus einen gezielten Informationsaustausch zwischen den verschiedenen Sicherheitsbehörden und genauere Einschätzungen für die Gefahrenabwehr in wichtigen Eilfällen zu ermöglichen.

131

Der Errichtung einer zentralen Verbunddatei zum Zweck eines gezielten Informationsaustauschs für die Aufgaben der Aufklärung und Bekämpfung des internationalen Terrorismus darf der Gesetzgeber erhebliches Gewicht beimessen. Denn schon angesichts der Zahl der mit diesen Aufgaben befassten Behörden ist die Gewährleistung eines zielführenden Austauschs der Erkenntnisse zwischen ihnen von besonderer Bedeutung. Zurzeit nehmen nach der Errichtungsanordnung mehr als 60 Behörden und Polizeidienststellen an der Antiterrordatei teil. Ungeachtet der Frage, welches Ausmaß an Organisationsdifferenzierung im Einzelnen sachgerecht ist, können die hierbei entstehenden Informationsprobleme für die Aufklärung und Bekämpfung des Terrorismus in einem föderalen Staat mit Gewaltenteilung jedenfalls nicht vollständig auf organisatorischer Ebene gelöst werden.

132

Zur Effektivität der Aufklärung und Bekämpfung des internationalen Terrorismus darf der Gesetzgeber, wenn er einen Informationsaustausch allein auf der Grundlage der Einzelübermittlungsvorschriften für unzureichend hält, eine sie koordinierende Verbunddatei zur Informationsanbahnung wie die Antiterrordatei schaffen. Die Verhinderung und Verfolgung von terroristischen Straftaten, die international organisiert und zur Verbreitung von Angst und Schrecken verübt werden, stellt die zuständigen staatlichen Behörden vor besondere Herausforderungen. Da solche Straftaten besonders schwer zu erfassen sind und die Zielpersonen sich oft in hohem Maße konspirativ verhalten, hängt der Erfolg einer wirksamen Aufgabenwahrnehmung der Sicherheitsbehörden hier in besonderer Weise davon ab, dass wichtige Informationen, die bei einer Behörde anfallen, auch für andere Behörden erschlossen werden und durch das Zusammenführen und Abgleichen der verschiedenen Daten aus diffusen Einzelerkenntnissen aussagekräftige Informationen und Lagebilder werden. Es liegt auf der Hand, dass eine speziell strukturierte Datei mit Grundprofilen von in den Fokus der Behörden geratenen Personen sowie mit Nachweisen, bei welchen Behörden Informationen zu welchen Personen zugänglich sind, die Aufgabenwahrnehmung wesentlich verbessern kann. Ebenso tragfähig ist die Annahme, dass den Behörden in dringenden Eilfällen unmittelbar bestimmte Informationen anderer Behörden zur Verfügung stehen müssen, um diesen eine erste Gefährdungseinschätzung und damit sachgerechte weitere Maßnahmen zu ermöglichen.

133

Für die Bedeutung einer solchen Datei ist dabei das große Gewicht einer effektiven Bekämpfung des Terrorismus für die demokratische und freiheitliche Ordnung zu berücksichtigen. Straftaten mit dem Gepräge des Terrorismus, wie sie das Antiterrordateigesetz zum Bezugspunkt hat (siehe oben D. III. 1.), zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Es ist Gebot unserer verfassungsrechtlichen Ordnung, solche Angriffe nicht als Krieg oder als Ausnahmezustand aufzufassen, die von der Beachtung rechtsstaatlicher Anforderungen dispensieren, sondern sie als Straftaten mit den Mitteln des Rechtsstaats zu bekämpfen. Dem entspricht umgekehrt, dass der Terrorismusbekämpfung im rechtsstaatlichen Rahmen der Verhältnismäßigkeitsabwägung ein erhebliches Gewicht beizumessen ist (vgl. BVerfGE 115, 320 <357 f.>).

134

c) Angesichts der sich gegenüberstehenden Interessen bestehen bei umfassender Würdigung gegen die Grundstrukturen der Antiterrordatei als Instrument der Informationsanbahnung und auch als handlungsanleitende Informationsquelle für eine Gefahreneinschätzung in dringenden Eilfällen keine verfassungsrechtlichen Bedenken. Allerdings entspricht die Regelung der Datei dem Verhältnismäßigkeitsgrundsatz im engeren Sinne nur, wenn sie hinsichtlich der zu erfassenden Daten sowie deren Nutzungsmöglichkeiten normenklar und in der Sache hinreichend begrenzt ausgestaltet ist sowie hierbei qualifizierte Anforderungen an die Kontrolle gestellt und beachtet werden (BVerfGE 125, 260 <325>).

135

aa) Verfassungsrechtlich nicht zu beanstanden sind zunächst die Grundstrukturen, mit denen der Gesetzgeber die Antiterrordatei als Verbunddatei zur Informationsanbahnung errichtet. Es ist im Ausgangspunkt nicht unverhältnismäßig, in diese Datei hinsichtlich bestimmter, dem internationalen Terrorismus vermutlich nahestehender Personen einen Grundbestand an identifizierenden Daten aufzunehmen, die den beteiligten Behörden zur Informationsanbahnung zur Verfügung stehen sollen. Da sie nur rechtlich begrenzte Einzelübermittlungen vorbereiten, ist eine solche Zusammenführung von Daten der Nachrichtendienste und Polizeibehörden durch die Aufgaben der Terrorismusbekämpfung gerechtfertigt. Ebenfalls bestehen keine durchgreifenden Bedenken dagegen, dass in diese Datei über einen Grundbestand an identifizierenden Daten hinaus weitere, inhaltlich aussagekräftigere, sogenannte

erweiterte Grunddaten aufzunehmen sind. Auch diese Daten – die den beteiligten Behörden wegen ihrer höheren Persönlichkeitsrelevanz grundsätzlich nicht als Klarinformationen, wohl aber zur verdeckten Recherche zur Verfügung gestellt werden – haben die Aufgabe, einen gezielteren Informationsaustausch nach Maßgabe des Fachrechts zu ermöglichen, und sind durch das Ziel einer Effektivierung der Terrorismusbekämpfung grundsätzlich gerechtfertigt.

136

Allerdings bedarf es einer Ausgestaltung der Datei, die den Informationsaustausch im Einzelnen normenklar regelt und hinreichend begrenzt. Dies gilt ebenso für die Bestimmung der beteiligten Behörden, die in der Datei zu erfassenden Personen und die über sie zu erfassenden Daten wie für die nähere Regelung der Nutzung dieser Daten. Auch muss eine effektive Kontrolle gewährleistet sein (siehe unten D. IV.).

137

bb) Wegen der großen Bedeutung der Verhinderung von terroristischen Anschlägen ist es ebenfalls nicht zu beanstanden, dass der Gesetzgeber mit der Antiterrordatei darüber hinaus eine Informationsquelle zur Verfügung stellen will, die in dringenden Eilfällen auch eine erste handlungsanleitende Gefährdungseinschätzung der Behörden ermöglichen soll. Freilich liegt hierin ein Eingriff, der besonders schwer wiegt, weil der Datenaustausch in diesen Fällen nicht nur eine Informationsanbahnung nach Maßgabe des Fachrechts ermöglicht, sondern unmittelbar auch operativen Zwecken dient. Jedoch verstößt auch dies nicht von vornherein gegen das Übermaßverbot. Maßgeblich ist insoweit jedoch, dass die gesetzlichen Eingriffsschwellen in Bezug auf die Dringlichkeit und die bedrohten Rechtsgüter in einer Weise begrenzend ausgestaltet sind, die diesem besonderen Eingriffsgewicht Rechnung trägt (siehe unten D. IV. 4. d).

IV.

138

Von diesen Grundsätzen ausgehend genügen die angegriffenen Vorschriften den Anforderungen an eine hinreichend bestimmte und dem Übermaßverbot entsprechende Ausgestaltung der Antiterrordatei in verschiedener Hinsicht nicht. Sie verletzen insoweit das Recht auf informationelle Selbstbestimmung.

139

1. Die Regelung des § 1 Abs. 2 ATDG zur Beteiligung weiterer Polizeivollzugsbehörden an der Antiterrordatei ist mit dem Bestimmtheitsgebot unvereinbar.

140

a) Das Bestimmtheitsgebot soll sicherstellen, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle durchführen können. Ferner erlauben die Bestimmtheit und Klarheit der Norm, dass die betroffenen Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können (vgl. BVerfGE 110, 33 <52 ff.>; 113, 348 <375 ff.>; 120, 378 <407 f.>). Der Gesetzgeber kann dabei, soweit er Anlass, Zweck und Ausmaß selbst festlegt, die genauere Bestimmung dieser Maßstäbe unter Umständen gemäß Art. 80 Abs. 1 GG an die Verwaltung delegieren, die diese dann durch Rechtsverordnung festzulegen hat. Auch hierbei handelt es sich jedoch um gesetzliche Grundlagen im materiellen Sinne, die nicht nur verwaltungsintern für die Behörden, sondern als Außenrecht auch für den Bürger und gegebenenfalls die Gerichte verbindlich sind. Das Bestimmtheitsgebot steht damit in enger Beziehung zu den grundrechtlichen Gesetzesvorbehalten, nach denen Eingriffe in die Grundrechte nur durch Gesetz und gegebenenfalls aufgrund eines Gesetzes eingeschränkt werden können. Hierdurch wird gewährleistet, dass der Umfang von Grundrechtseingriffen in den wesentlichen Aspekten im parlamentarischen Verfahren öffentlich unter Mitwirkung auch der nicht die Regierung tragenden Abgeordneten diskutiert, deren weitere generell-abstrakte Präzisierung durch die Verwaltung gemäß Art. 80 Abs. 1 GG erkennbar als Konkretisierung dieser parlamentarischen Entscheidung ausgewiesen und die insoweit letztlich maßgeblichen Normen für alle verbindlich und durch Ausfertigung und Verkündung erkennbar bekanntgemacht werden. Die demokratische und rechtsstaatliche Funktion des Gesetzesvorbehalts greifen hierbei ineinander. Welche Anforderungen an die Bestimmtheit gesetzlicher Regelung zu stellen sind, richtet sich dabei nach der Intensität der durch die Regelung oder aufgrund der Regelung erfolgenden Grundrechtseingriffe.

141

Nach diesen Maßstäben müssen die an der Antiterrordatei beteiligten Behörden entweder unmittelbar durch Gesetz oder aufgrund eines Gesetzes durch Rechtsverordnung bestimmt werden. Die Entscheidung, welche Behörde ihre Daten in die Datei einzustellen hat und welche Behörde zu deren Abruf berechtigt ist, entscheidet maßgeblich über Umfang und Inhalt der Datei sowie über das Ausmaß der weiteren Nutzung der Daten. Es handelt sich um ein wesentliches Regelungselement, das einer normenklaaren und bestimmten Festlegung mit Wirkung nach außen bedarf. Vor allem aber intensiviert die Einbeziehung einer jeden weiteren Polizeivollzugsbehörde in den Informationsverbund des Antiterrordateigesetzes die Durchbrechung der informationellen Trennung von Nachrichtendiensten und Polizeibehörden. Der

Informationsaustausch zwischen Nachrichtendiensten und Polizeibehörden verleiht den mit dem Antiterrordateigesetz verbundenen Grundrechtseingriffen erhöhtes Gewicht (D. III. 3. a) aa). Dies setzen gerade die Regelungen über die Beteiligung weiterer Polizeivollzugsbehörden an der Antiterrordatei unter Durchbrechung der informationellen Trennung von Nachrichtendiensten und Polizeibehörden auch organisationsrechtlich ins Werk. Die Regelungen über die teilnehmenden Behörden bilden damit den Kern des spezifischen grundrechtlichen Gefährdungspotenzials der Antiterrordatei.

142

b) § 1 Abs. 2 ATDG genügt weder für sich allein noch in Verbindung mit der Errichtungsanordnung gemäß § 12 ATDG den besonderen Anforderungen, die an die gesetzliche Bestimmung der Beteiligung weiterer Polizeivollzugsbehörden an der Antiterrordatei zu stellen sind.

143

aa) Eine hinreichend normenklare gesetzliche Festlegung, aus der sich die beteiligten Behörden unmittelbar selbst bestimmen lassen, liegt nicht schon in § 1 Abs. 2 ATDG allein. Zwar schließen die Bestimmtheitsanforderungen nicht grundsätzlich aus, dass der Gesetzgeber die abrufberechtigten Behörden einer Datei - je nach deren Art und Gegenstand - nur generell abstrakt festlegt. Wenn der Kreis dieser Behörden sich unmittelbar aus dem Gesetz hinreichend bestimmt erschließen lässt, kann es unschädlich sein, wenn hierbei die konkreten Behörden nicht ausdrücklich genannt sind (vgl. BVerfGE 130, 151 <199, 203>). So liegt es vorliegend jedoch nicht. § 1 Abs. 2 ATDG umschreibt die zu beteiligenden Behörden nur nach weiten und wertungs offenen Kriterien. Er verweist auf anderweitige Aufgabenzuweisungen sowie auf Gesichtspunkte der Erforderlichkeit und Angemessenheit, die die Bestimmung der beteiligten Behörden letztlich für allgemeine sicherheitspolitische Opportunitätserwägungen öffnet. Die Vorschrift wird dabei, wie sich aus ihrem Regelungskontext ergibt, auch vom Gesetzgeber selbst nicht so verstanden, dass sie die zu beteiligenden Behörden selbst abschließend bestimmen soll. Vielmehr ergibt sich aus dem in § 12 Nr. 2 ATDG geregelten Erfordernis einer Festlegung dieser Behörden durch die Errichtungsanordnung sowie aus den in § 1 Abs. 2 und § 12 ATDG vorgesehenen - dabei nicht widerspruchsfreien - Benehmens-, Einvernehmens- und Zustimmungserfordernissen, dass der Gesetzgeber mit dieser Vorschrift den Kreis der beteiligten Behörden noch nicht unmittelbar selbst festlegen wollte, sondern dies nach Fachkriterien der eigenständigen Entscheidung der Exekutive überlassen wollte. Dass nach dem derzeitigen Stand der Errichtungsanordnung nur aus drei Bundesländern weitere Polizeivollzugsbehörden an der Antiterrordatei beteiligt werden, bestätigt dies. Jedenfalls bezogen auf eine Datei vom Eingriffsgewicht der Antiterrordatei genügt eine solche Offenheit der beteiligten Behörden den verfassungsrechtlichen Anforderungen nicht.

144

bb) Eine hinreichend klare Bestimmung der beteiligten Behörden ergibt sich auch nicht aus § 1 Abs. 2 ATDG in Verbindung mit der Errichtungsanordnung gemäß § 12 Nr. 2 ATDG. Zwar bestehen keine grundsätzlichen Bedenken gegen eine Delegation der endgültigen Festlegung dieser Behörden auf die Verwaltung. Für eine solche Festlegung reicht angesichts der spezifischen Grundrechtsrelevanz der Bestimmung der an der Antiterrordatei teilnehmenden Behörden jedoch nicht eine Errichtungsanordnung als bloße Verwaltungsvorschrift, die weder gegenüber den in ihren Daten Betroffenen noch gegenüber den Gerichten rechtlich bindende Wirkung hat, und die auch nicht rechtsförmlich ausgefertigt und verkündet wird. Will der Gesetzgeber die Entscheidung über die beteiligten Behörden in die Hände der Exekutive legen, ist er hier nach Maßgabe des Art. 80 Abs. 1 GG auf die Form der Rechtsverordnung verwiesen.

145

2. Nicht in jeder Hinsicht mit den verfassungsrechtlichen Anforderungen vereinbar sind die Vorschriften, die den von der Datei erfassten Personenkreis festlegen. Einige dieser Bestimmungen verletzen den Bestimmtheitsgrundsatz und das Übermaßverbot. Andere bedürfen einer einengenden verfassungskonformen Auslegung.

146

a) Keinen Einwänden unterliegt allerdings § 2 Satz 1 Nr. 1 a ATDG. Die Vorschrift ordnet die Erfassung der Daten von Personen an, die möglicherweise einer terroristischen Vereinigung angehören oder sie unterstützen, und erfasst damit diejenigen, die im Fokus einer effektiven Terrorismusabwehr stehen. Indem die Vorschrift an Strafnormen anknüpft, die bereits ihrerseits strafbares Handeln schon weit in das Vorfeld von Rechtsgutverletzungen vorverlagern, und dabei schon „tatsächliche Anhaltspunkte“ - gegebenenfalls auch nur für Unterstützungshandlungen - ausreichen lässt, öffnet die Vorschrift zwar beträchtlichen Raum für subjektive Einschätzungen der Behörden und ein weites Feld von Unwägbarkeiten. Im Rahmen der Antiterrordatei, die außerhalb von dringenden Eilfällen nur der Informationsanbahnung dient und in diesem Rahmen ermöglichen soll, auch ungesicherte Einschätzungen von Verdachts- und Gefahrenlagen noch im Vorfeld von Ermittlungen zu verwerfen oder zu erhärten, ist diese Ausgestaltung jedoch hinnehmbar. Bei sachgerechter Auslegung stellen diese Tatbestandsmerkmale immerhin hinreichend sicher, dass eine Speicherung nicht auf bloßen Spekulationen beruhen darf. Insbesondere bedürfen tatsächliche Anhaltspunkte einer Rückbindung an konkrete Erkenntnisse und ist der Begriff des Unterstützens - auch von den subjektiven Voraussetzungen her - wie in § 129a Abs. 5 Satz 1 StGB zu verstehen (vgl. BTDrucks

16/2950, S. 15). Schließlich ermöglicht die die Speicherpflichten allgemein begrenzende Klausel am Ende von § 2 Satz 1 ATDG, nach der die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland erforderlich sein muss, Korrekturen, wenn im Einzelfall Zweifel an der Verhältnismäßigkeit der Speicherung bestehen. Zwar ist diese Klausel angesichts ihrer Offenheit ungeeignet, eine von vornherein an sich unbestimmte oder schon grundsätzlich zu weit gefasste Speicherungspflicht zu heilen. Sofern aber, wie vorliegend, eine grundsätzlich tragfähige Festlegung der zu speichernden Daten gegeben ist, ist die Klausel geeignet, für atypische Einzelfälle eine verfassungsrechtlich tragfähige Lösung zu ermöglichen.

147

b) § 2 Satz 1 Nr. 1 b ATDG, der den Kreis der erfassten Personen unter dem Gesichtspunkt der Unterstützung terroristischer Vereinigungen erweitert, ist teilweise mit dem Übermaßverbot nicht vereinbar und verfassungswidrig.

148

aa) Unbedenklich ist die Vorschrift allerdings insoweit, als sie Personen erfasst, die einer Gruppierung angehören, welche eine terroristische Vereinigung unterstützt. Für die Beurteilung der Verhältnismäßigkeit macht es keinen Unterschied, ob eine Unterstützung einzeln oder kollektiv erfolgt. Dementsprechend ist die Speicherung dieser Personen in gleicher Weise verhältnismäßig wie die Speicherung von Unterstützern einer terroristischen Vereinigung nach § 2 Satz 1 Nr. 1 a (2. Alternative) ATDG.

149

bb) Demgegenüber wird der Kreis nochmals erweitert, indem die Vorschrift auch Personen erfasst, die eine unterstützende Vereinigung lediglich unterstützen. Ein Erfordernis eines subjektiven Bezugs zum Terrorismus ist der Vorschrift nicht zu entnehmen. Sie deckt ihrem Wortlaut und nicht fernliegenden Sinn nach damit auch eine Erstreckung der Speicherungspflicht auf Personen, die weit im Vorfeld und möglicherweise ohne Wissen von einem Terrorismusbezug eine in ihren Augen unverdächtige Vereinigung unterstützen, wie zum Beispiel den Kindergarten eines Moscheevereins, den die Behörden jedoch der Unterstützung terroristischer Vereinigungen verdächtigen. Eine solche Öffnung der Norm für die Einbeziehung schon des weitesten Umfelds terroristischer Vereinigungen verstößt gegen den Grundsatz der Normenklarheit und ist mit dem Übermaßverbot nicht vereinbar. Zwar steht es dem Gesetzgeber frei, auch die bloße Unterstützung von unterstützenden Vereinigungen als Grund für eine Speicherung vorzusehen, wenn tatsächliche Anhaltspunkte bestehen, dass sie sich willentlich als Förderung der den Terrorismus unterstützenden Aktivitäten solcher Gruppierungen darstellt. Der Gesetzgeber hat dies gegebenenfalls aber in einer dem Grundsatz der Normenklarheit genügenden Weise in der Vorschrift zum Ausdruck zu bringen. Dem Wortlaut des § 2 Satz 1 Nr. 1 b ATDG lässt sich hierfür nichts entnehmen. Angesichts der Funktionsweise der Antiterrordatei, deren Anwendung den Betroffenen in der Regel nicht bekannt und auch nicht richterlich überprüft wird, darf hierüber keine Unklarheit verbleiben. Deshalb scheidet hier auch eine verfassungskonforme Auslegung aus.

150

c) Nicht vollständig mit der Verfassung vereinbar ist § 2 Satz 1 Nr. 2 ATDG. Die Vorschrift, die Einzelpersonen erfassen soll, die möglicherweise in einer Nähe zum Terrorismus stehen, verbindet eine Reihe von mehrdeutigen und potenziell weiten Rechtsbegriffen. Hinsichtlich der Begriffe der rechtswidrigen Gewalt und des vorsätzlichen Hervorrufens solcher Gewalt lässt sich eine Verfassungswidrigkeit wegen Stimmengleichheit im Senat nicht feststellen; nach Auffassung der vier Mitglieder des Senats, die die Entscheidung insoweit tragen (§ 15 Abs. 4 Satz 3 BVerfGG), ist die Verwendung dieser Merkmale mit dem Grundgesetz vereinbar, sofern den Merkmalen keine übermäßig weite Bedeutung beigelegt wird (aa). Nach der Auffassung der anderen vier Mitglieder des Senats, die für die Entscheidung im Ergebnis nicht tragend wird (§ 15 Abs. 4 Satz 3 BVerfGG), müsste die Vorschrift weitergehend insoweit für verfassungswidrig erklärt werden (bb). Hingegen reicht das bloße Befürworten von Gewalt im Sinne dieser Vorschrift nach der einhelligen Auffassung des Senats für die Erfassung von Personen in der Antiterrordatei nicht. Die Vorschrift verstößt insoweit gegen das Übermaßverbot und ist verfassungswidrig (cc).

151

aa) (1) Zentral stellt die Vorschrift auf den Begriff der rechtswidrigen Gewalt ab. Zwar wird diesem Begriff an anderer Stelle der Rechtsordnung ein sehr weiter Sinn beigelegt, der als Anknüpfungspunkt für eine Qualifizierung der betroffenen Personen als in der Nähe des Terrorismus stehend zu wenig signifikant wäre, als dass er den betroffenen Personenkreis in einer dem Verhältnismäßigkeitsgrundsatz genügenden Weise eingrenzen und eine Speicherung der Daten der Betroffenen verfassungsrechtlich tragen könnte. Das Bundesverfassungsgericht hat verfassungsrechtlich unbeanstandet gelassen, dass die Strafgerichte im Zusammenhang mit dem Nötigungstatbestand (§ 240 StGB) bei der strafrechtlichen Beurteilung von Blockadeaktionen für die Bejahung einer Gewaltanwendung schon die körperliche Kraftentfaltung durch Anbringung von mit Personen verbundenen Metallketten an den Pfosten eines Einfahrtstors genügen ließen, weil die Ankettung der Demonstration eine über den psychischen Zwang hinausgehende Eignung gab, Dritten den Willen der Demonstranten aufzuzwingen (vgl. BVerfGE 104, 92 <102>). Laut Auskunft der

Sicherheitsbehörden in der mündlichen Verhandlung wird das Merkmal rechtswidriger Gewalt in der Praxis jedoch enger verstanden. Im Rahmen des hier zu überprüfenden Gesetzes wäre eine weite Auslegung des Begriffs der rechtswidrigen Gewalt im Sinne des strafrechtlichen Nötigungstatbestandes auch weder durch den Wortlaut noch durch die Zielsetzung des Gesetzes nahegelegt. Entsprechend der gegen terroristische Straftaten gewendeten Zielrichtung der Antiterrordatei ist der Begriff vielmehr dahin zu verstehen, dass er nur Gewalt umfasst, die unmittelbar gegen Leib und Leben gerichtet oder durch den Einsatz gemeingefährlicher Mittel geprägt ist. In dieser Auslegung bestehen gegen die Verhältnismäßigkeit des durch Verwendung des Gewaltbegriffs in § 2 Satz 1 Nr. 2 ATDG erfassten Personenkreises keine verfassungsrechtlichen Bedenken.

152

(2) Erfasst werden nach § 2 Satz 1 Nr. 2 ATDG zudem sowohl Personen, die Gewalt anwenden, unterstützen und vorbereiten, als auch solche, die sie nur befürworten oder durch ihre Tätigkeit vorsätzlich hervorrufen. Dies eröffnete unverhältnismäßig weite Eingriffsmöglichkeiten, wenn für das vorsätzliche Hervorrufen von Gewalt auch der Eventualvorsatz im Sinne strafrechtlicher Terminologie als ausreichend angesehen würde. Wird dem Merkmal des vorsätzlichen Hervorrufens von Gewalt hier jedoch eine Bedeutung beigelegt, wonach nur das willentliche Hervorrufen von Gewalt erfasst ist, wahrt dies den Grundsatz der Verhältnismäßigkeit.

153

bb) Nach Auffassung der anderen vier Mitglieder des Senats, die für die Entscheidung im Ergebnis nicht tragend wird (§ 15 Abs. 4 Satz 3 BVerfGG), ist § 2 Satz 1 Nr. 2 ATDG wegen fehlender Bestimmtheit und übermäßiger Reichweite insgesamt als verfassungswidrig zu erklären. Dem lässt sich nicht dadurch entgehen, dass den Begriffen der rechtswidrigen Gewalt und des vorsätzlichen Hervorrufens eine von den aus dem Strafrecht allgemein bekannten Begrifflichkeiten abweichende engere Interpretation unterlegt wird. Ein solcher Rückgriff auf eine verfassungskonforme Auslegung ist inkonsequent und weicht die datenschutzrechtlichen Bestimmtheitsanforderungen auf.

154

(1) Wie auch die die Entscheidung tragenden Senatsmitglieder sehen, sind maßgebliche Merkmale dieser Vorschrift mehrdeutig und werden an anderer Stelle der Rechtsordnung - und zwar in einem für die Begriffsvorstellungen des Rechtsalltags grundlegenden Bereich des Strafrechts - in einer Weise weit verstanden, die im Kontext der Antiterrordatei mit den Anforderungen an die Verhältnismäßigkeit und dem Übermaßverbot nicht vereinbar ist. So stellt die Vorschrift allgemein auf den Begriff der rechtswidrigen Gewalt ab. Nach eingeführten strafrechtlichen Definitionen reicht hierfür schon das Errichten von physischen Barrieren auf einer Straße (vgl. BVerfGE 104, 92 <101 f.>; BVerfGK 18, 365 <369>). Danach berechnete - bei einem entsprechenden thematischen Bezug - schon die Durchführung von bloßen Blockadeaktionen mit Anketten zur Aufnahme in die Antiterrordatei. Eine zusätzliche Erweiterung liegt darin, dass für eine Speicherung schon das vorsätzliche Hervorrufen solcher Gewalt genügt. Nach den gängigen Vorsatzlehren des Strafrechts ist dieses Merkmal erfüllt, wenn der Betreffende damit rechnet, dass von ihm veröffentlichte Bilder oder Texte Dritte - auch wider seinen Willen - zu Ausschreitungen veranlassen. Solche Auslegungen sind auch nicht etwa fernliegend: Sie knüpfen an den Wortlaut und an allgemein anerkannte strafrechtliche Auslegungsgrundsätze an, auf die zurückzugreifen im Kontext der Norm, die selbst auf Strafrechtsnormen verweist, naheliegt. Sie können aus Sicht der Sicherheitsbehörden auch sinnvoll und attraktiv erscheinen: Sie erlaubten es, einen nochmals wesentlich weiteren Kreis von Personen auch aus dem bloßen Umfeld des Terrorismus zunächst grundsätzlich vom Anwendungsbereich der Datei umfasst anzusehen. Deren Eingrenzung könnten sie dann unter Rückgriff auf die salvatorische Klausel am Ende des § 2 ATDG, nach der die Daten nur zu speichern sind, wenn ihre Kenntnis zur Aufgabenwahrnehmung erforderlich ist, nach sehr subjektiven Kriterien vornehmen.

155

(2) Eine einengende verfassungskonforme Auslegung kommt hier nicht in Betracht.

156

(a) Eine solche Auslegung scheidet für § 2 Satz 1 Nr. 2 ATDG schon deshalb aus, weil der im Zentrum der Norm stehende Begriff der „rechtswidrigen Gewalt“ vom Gesetzgeber bewusst weit und offen gewählt wurde. Im Gesetzgebungsverfahren waren die Unschärfe und übermäßige Reichweite des Gewaltbegriffs Gegenstand ausdrücklicher Kritik (BTPlenarprotokoll 16/71, S. 7100; BT Innenausschuss, Protokoll Nr. 16/24, S. 55; A-Drucks 16(4)131 D, S. 10; A-Drucks 16(4)131 J, S. 10) und wurde zu dessen Eingrenzung sogar ein eigener Gegenvorschlag eingebracht, wonach in Anlehnung an § 129a Abs. 2 StGB rechtswidrige Gewalt nur als Anknüpfungspunkt für die Speicherung dienen sollte, „wenn dies[e] dazu bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen und vom Handeln der Person die Gefahr einer erheblichen Schädigung eines Staates oder einer internationalen Organisation ausgeht“ (vgl. BTDrucks 16/3642, S. 14 f.). Man hatte damit versucht, den Gewaltbegriff ähnlich einzuengen, wie dies auch in internationalen und europäischen

Bestimmungen zur Terrorismusbekämpfung erstrebt wird (vgl. Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, ABl. L 164/3 vom 22. Juni 2002, Art. 1; Entwurf einer Allgemeinen Konvention zum internationalen Terrorismus, in: Measures to eliminate international terrorism, Report of the Working Group vom 3. November 2010, UN Doc. A/C.6/65/L.10.). Hierüber hat sich der Gesetzgeber jedoch in bewusster Entscheidung hinweggesetzt - ersichtlich um den Sicherheitsbehörden weiteren Freiraum zu belassen. Eine solche Entscheidung kann dann aber nicht im Wege der verfassungskonformen Auslegung korrigiert werden.

157

(b) Eine verfassungskonforme Auslegung scheidet hier aber auch aus grundsätzlichen Erwägungen aus. Wenn die gesetzliche Eingriffsgrundlage in der genannten Weise offen formuliert ist und bei Zugrundelegung anerkannter Begriffsdefinitionen nicht fernliegend auch eine derart ausgreifende Auslegung trägt, genügt sie als Grundlage für eine Datenverarbeitung, wie sie vorliegend in Rede steht, nicht dem Grundsatz der Normenklarheit und ist unverhältnismäßig. Der Grundsatz der Normenklarheit zielt gerade darauf, dem Gesetzgeber hinsichtlich der Anforderungen an Grundrechtseingriffe selbst hinreichend klare Entscheidungen abzuverlangen, die die Wahrung des Übermaßverbots hinreichend verlässlich sicherstellen. Werden diese Anforderungen vom Gesetzgeber verfehlt, kann das Bundesverfassungsgericht dieses Manko nicht durch eine verfassungskonforme Auslegung heilen. Der Rückgriff auf die verfassungskonforme Auslegung - mit der im Grunde jede Blankettermächtigung eingegrenzt werden könnte - nimmt die datenschutzrechtlichen Anforderungen an die Bestimmtheit und damit seine Maßstäbe substantiell zurück. Dies führt notwendig zu Inkonsequenzen: Welche der offenen Rechtsbegriffe einer verfassungskonformen Auslegung noch zugänglich sind, welche aber nicht, lässt sich kaum mehr nachvollziehbar abgrenzen. So auch vorliegend: Warum in § 2 Satz 1 Nr. 2 ATDG die Begriffe der „Gewalt“ und des „vorsätzlichen Hervorrufens“ einer verfassungskonform einengenden Auslegung noch zugänglich sein sollen, der Begriff des „Befürwortens“ in derselben Vorschrift oder des „Unterstützens einer unterstützenden Gruppierung“ in § 2 Satz 1 Nr. 1 b ATDG hingegen nicht, lässt sich überzeugend nicht begründen.

158

Dem lässt sich nicht entgegenhalten, dass die Rechtsordnung auch sonst unbestimmte Rechtsbegriffe kennt und Normen immer auslegungsbedürftig sind; kein Einwand ist auch, dass dementsprechend der Gewaltbegriff in verschiedenen Zusammenhängen verschiedene Bedeutung hat. Denn die Anforderungen an die Bestimmtheit und eine hinreichend klare Begrenzung von Rechtsgrundlagen unterscheiden sich je nach Sachbereich und Regelungszusammenhang. Im Datenschutzrecht sind die Anforderungen an die Bestimmtheit und Normenklarheit nach ständiger Rechtsprechung des Bundesverfassungsgerichts besonders hoch (vgl. BVerfGE 65, 1 <46>; 118, 168 <187>; 120, 378 <408>) - und dies muss insbesondere für die Antiterrordatei gelten, die den Datenaustausch von Sicherheitsbehörden noch im Vorfeld von Ermittlungen regelt. Denn anders als der Gesetzesvollzug etwa durch Verwaltungsakt, bei dem behördliche Maßnahmen an den Einzelnen adressiert und mit einer Begründung versehen werden sowie im Einzelfall gerichtlich überprüfbar sind, vollzieht sich die Datenverarbeitung nach dem Antiterrordateigesetz außerhalb jeder unmittelbaren Wahrnehmbarkeit. Sie bleibt informell und gegenüber dem Betroffenen ohne Begründung und kann in der Regel auch nicht gerichtlich überprüft werden. Während eine gewisse Unbestimmtheit von Eingriffsgrundlagen sonst im kontradiktorischen Wechselspiel und durch schrittweise Entwicklung von Auslegungsregeln konkretisiert werden kann, müssen sich hier die Grenzen der Datenverarbeitung für den Betroffenen verlässlich und für die Sicherheitsbehörden möglichst aus sich heraus erkennbar unmittelbar aus dem Gesetz ergeben.

159

Diese qualifizierten Bestimmtheitsanforderungen des grundrechtlichen Datenschutzes beruhen auch nicht auf übersteigertem Misstrauen gegenüber den Sicherheitsbehörden. Vielmehr sollen diese Anforderungen gerade für die noch nicht oder wenig formalisierten Phasen der sicherheitsbehördlichen Aufgabenwahrnehmung, in denen die Datenverarbeitung oftmals eine besondere Rolle spielt, aus sich heraus eindeutige Bedingungen gewährleisten, die die Behörden bei der Wahrnehmung ihrer anspruchsvollen Aufgaben möglichst klar anleiten und auch von Zweifelsfragen entlasten.

160

(c) Eine verfassungskonforme Auslegung ist auch nicht in Respekt vor dem Gesetzgeber geboten. Zwar ist richtig, dass der Gesetzgeber mit dem Antiterrordateigesetz ein anspruchsvolles und differenziertes Regelungskonzept verwirklicht hat, das in verschiedener Hinsicht durch rechtsstaatliche Mäßigung und das ernsthafte Bestreben der Gewährleistung eines angemessenen Datenschutzes gekennzeichnet ist. Die verfassungsrechtliche Beurteilung der konkreten Vorschriften, die dieses Konzept umsetzen, kann sich jedoch nicht nach einer Gesamtbewertung der politischen Anstrengungen des Gesetzgebers richten. Vielmehr ist es Aufgabe des Gerichts, die verfassungsrechtlichen Maßstäbe hiervon unabhängig auch im Einzelnen zur Geltung zu bringen und damit sicherzustellen, dass die in der Gesamtanlage zugrundegelegte Rechtsstaatlichkeit nicht durch offene Einzelbestimmungen wieder entgleitet. Der Respekt vor dem Gesetzgeber gebietet es vielmehr umgekehrt, von einer eigenen Eingrenzung der datenschutzrechtlichen Anforderungen durch das Gericht abzusehen und stattdessen die Vorschriften für

verfassungswidrig zu erklären: Anstatt ihm eine vom Regelungsziel her vielleicht naheliegende, aber ersichtlich nicht gewollte Regelung - jedenfalls bis auf weiteres - durch Auslegung zuzuschreiben, würde dies die Aufgabe der maßgeblichen Grenzziehungen in Wahrung seiner Zuständigkeit an ihn zurückspielen. Es ist auch nicht ersichtlich, dass dies den Gesetzgeber aus fachlichen oder sonst regelungsbedingten Gründen vor besondere Schwierigkeiten gestellt hätte.

161

cc) Besonders weit reicht das Merkmal des Befürwortens von Gewalt. Hier stellt der Gesetzgeber allein auf eine innere Haltung ab, die sich in keinerlei gewaltfördernden Aktivitäten niedergeschlagen haben muss. Die Verwendung dieses Merkmals ist mit der Verfassung nicht vereinbar und die Vorschrift insoweit verfassungswidrig. Die prinzipiell überschießende Reichweite dieses Kriteriums kann auch nicht im Wege einer verfassungskonformen Auslegung ausgeräumt werden. Zwar nennt die Gesetzesbegründung als Beispiel nur Hassprediger, gegen deren Aufnahme in die Datei im Falle eines öffentlichen Anstachelns zu Hass und Gewalt verfassungsrechtlich keine grundsätzlichen Bedenken bestehen. Jedoch ist eine Beschränkung auf solche Fälle in dem grundsätzlich weitergreifenden Wortlaut nicht angelegt. Vielmehr legt dieser ein Verständnis nahe, nach dem es allein auf eine entsprechende Haltung ankommt. Insofern reicht es danach aus, dass hierauf aus tatsächlichen Anhaltspunkten rückgeschlossen werden kann. Das Anknüpfen an ein solches Kriterium, das unmittelbar auf das forum internum abstellt und damit auf den unverfügbaren Innenbereich des Individuums zugreift, ist besonders geeignet, einschüchternde Wirkung auch für die Wahrnehmung der Freiheitsrechte wie insbesondere der Glaubens- und Meinungsfreiheit zu entfalten. Das Gesetz macht hier die subjektive Überzeugung als solche zum Maßstab und legt damit Kriterien zugrunde, die vom Einzelnen nur begrenzt beherrscht und durch rechtstreues Verhalten nicht beeinflusst werden können. Die Erfassung von Personen in der Antiterrordatei nach Maßgabe eines solchen Kriteriums ist mit dem Übermaßverbot nicht vereinbar. § 2 Satz 1 Nr. 2 ATDG ist insoweit verfassungswidrig.

162

d) Verfassungswidrig ist auch § 2 Satz 1 Nr. 3 ATDG. Die dort vorgesehene Einbeziehung von Kontaktpersonen ist weder mit dem Bestimmtheitsgrundsatz noch mit dem Übermaßverbot vereinbar.

163

§ 2 Satz 1 Nr. 3 ATDG bestimmt, dass auch bloße Kontaktpersonen der in den vorangehenden Nummern erfassten Personen in die Antiterrordatei aufzunehmen sind. Das Gesetz erfasst diese als eigene Gruppe, deren Daten den beteiligten Behörden in gleicher Weise zugänglich gemacht werden wie die der anderen in der Datei erfassten Personen. In die Datei aufzunehmen sind dabei auch solche Kontaktpersonen, die von einem Terrorismusbezug der Hauptperson nichts wissen - insoweit allerdings nur mit den einfachen Grunddaten (§ 3 Abs. 1 Nr. 1 a ATDG). Soweit es um Kontaktpersonen geht, die um den Terrorismusbezug der betreffenden Hauptperson wissen, sind darüber hinaus auch die erweiterten Grunddaten (§ 3 Abs. 1 Nr. 1 b ATDG) in die Datei einzustellen.

164

Die Regelung zur Einbeziehung der Kontaktpersonen als eigene Gruppe in den auch Klarinformationen umfassenden Datenaustausch genügt den Bestimmtheitsanforderungen nicht. Welche Personen tatsächlich in die Datei aufzunehmen sind, ist auf ihrer Grundlage nicht vorhersehbar. Auch wenn der Gesetzgeber Personen mit nur flüchtigem oder zufälligem Kontakt ausnimmt, erfasst die Norm im Übrigen die Personen des gesamten gesellschaftlichen Lebensumfelds der in den Nummern 1 und 2 der Vorschrift Genannten - sowohl die des privaten Umfeldes, als auch solche, die in beruflichen oder geschäftlichen Kontakten zu ihnen stehen. Ersichtlich aber sollen nicht alle danach in Betracht kommenden Personen tatsächlich in die Datei aufgenommen werden. In der mündlichen Verhandlung wurde dargelegt, dass die Zahl der zurzeit tatsächlich erfassten Kontaktpersonen gering sei und hinsichtlich der „undolosen“ Kontaktpersonen nur 141 Personen erfasse. Die zunächst äußerst weit definierte Gruppe soll vielmehr nach Maßgabe der Schlussklausel am Ende des § 2 Satz 1 ATDG, nach der die Kenntnis der entsprechenden Daten für die Terrorismusabwehr erforderlich sein muss, wieder weitgehend eingeschränkt werden. Damit wird den Behörden aber kein hinreichend bestimmter Maßstab an die Hand gegeben. Vielmehr bleibt die Bestimmung der zu speichernden Daten letztlich deren freier Einschätzung überlassen.

165

Angeichts der kaum übersehbaren Reichweite des potenziell durch die Regelung erfassten Personenkreises verstößt sie auch gegen das Übermaßverbot. Allerdings ist verfassungsrechtlich nicht prinzipiell ausgeschlossen, Daten auch von Kontaktpersonen in der Antiterrordatei bereitzustellen. In der Regel sind solche Personen, die nicht unter die Nummern 1 und 2 der Vorschrift fallen und damit selbst nicht als potenzielle Unterstützer von terroristischen Aktivitäten gelten, aber nach dem Zweck der Datei nur insoweit von Interesse, als sie Aufschluss über die als terrorismusnah geltende Hauptperson vermitteln können. Hieran muss sich auch die gesetzliche Ausgestaltung orientieren. Möglich wäre es insoweit etwa, Kontaktpersonen mit wenigen Elementardaten zu erfassen und diese - entsprechend der derzeitigen Regelung des § 3 Abs. 1 Nr. 1 b ATDG - als Information zu der entsprechenden terrorismusnahen

Hauptperson nur verdeckt recherchierbar zu speichern. Es könnte so immerhin sowohl die Suche nach Kontaktpersonen durch eine Abfrage, die sich auf die Hauptperson bezieht, ermöglicht werden als auch eine verdeckte Recherche nach dem Namen einer Kontaktperson selbst, die im Trefferfall freilich nur zu einem Nachweis auf die informationsführende Behörde und das dazugehörige Aktenzeichen führte (vgl. auch unten D. IV. 4. c). Eine solche Regelung wäre angesichts des deutlich geringeren Eingriffsgewichts trotz der verbleibenden Weite der potenziell erfassten Personen auch mit den Bestimmtheitsanforderungen vereinbar, die maßgeblich auch von dem Gewicht des in Frage stehenden Grundrechtseingriffs abhängen (vgl. BVerfGE 59, 104 <114>; 86, 288 <311>; 117, 71 <111>). Dies gilt unabhängig davon, ob es sich um Kontaktpersonen handelt, die um den Terrorismusbezug der betreffenden Hauptperson wissen oder nicht.

166

3. Verfassungsrechtlich nicht zu beanstanden ist der in § 3 Abs. 1 Nr. 1 a und b ATDG geregelte Umfang der erfassten Daten. Allerdings bedarf es hinsichtlich

§ 3 Abs. 1 Nr. 1 b ATDG ergänzender Regelungen zu den in der Norm zum Teil enthaltenen Konkretisierungsanforderungen an die Verwaltung.

167

a) Keinen verfassungsrechtlichen Einwänden unterliegt die Bestimmung der in § 3 Abs. 1 Nr. 1 a ATDG umschriebenen Grunddaten, die den beteiligten Behörden ohne qualifizierte Eingriffsschwellen als Klarinformationen zur Verfügung gestellt werden.

168

Umfang und Aussagekraft dieser Daten sind allerdings durchaus erheblich. Da mit ihnen nicht nur aktuelle Informationen, sondern auch frühere Namen, Adressen, Staatsangehörigkeiten und Lichtbilder erfasst werden, können sie einen Teil des Lebenswegs der betreffenden Person erkennbar machen. Überdies umfasst die Vorschrift sensible Daten. Hierzu gehören insbesondere die Angaben zu besonderen körperlichen Merkmalen. Auch wenn hierunter bei sachgerechtem Verständnis nur äußere, miterkennungsdienstlichen Maßnahmen feststellbare Merkmale zu verstehen sind, werden dadurch höchstpersönliche Eigenheiten erfasst. Ähnliches gilt für die in die Datei aufzunehmenden Informationen, die der Sache nach die Herkunft betreffen. Zwar knüpft die Vorschrift nicht differenzierend und potenziell stigmatisierend an eine bestimmte Herkunft an, sondern sieht entsprechende Angaben für alle erfassten Personen gleichermaßen vor. Auch insoweit aber sind diese Angaben nicht belanglos.

169

Dennoch ist die Bestimmung mit dem Übermaßverbot vereinbar. Die Umschreibung der Daten ist hinreichend bestimmt und ihre Reichweite auch bei Gesamtsicht verhältnismäßig. Mit ihnen wird - beschränkt auf möglicherweise terrorismusnahe Personen (siehe oben D. IV. 2.) - ein zwar aussagekräftiges, aber letztlich doch auf äußerliche Parameter beschränktes Grundprofil zur genaueren Identifizierung der Betroffenen erstellt. Angesichts der Bedeutung der Terrorismusbekämpfung ist dies auch unter Einbeziehung der Daten der Nachrichtendienste verfassungsrechtlich nicht zu beanstanden. Dabei ist wiederum zu berücksichtigen, dass die Daten nicht neu ermittelt werden, die Datei also nicht auf die investigative Erstellung eines hinsichtlich der Grunddaten vollständigen Profils zielt, sondern lediglich die Zusammenführung der bei den einzelnen Behörden bereits vorliegenden Daten bewirkt. Freilich dürfte die Speicherung im Ergebnis zu einem großen Teil auch Personen betreffen, bei denen sich letztlich herausstellen wird, dass sie mit dem Terrorismus nichts zu tun haben. Jedoch ist dies für eine Datei, die den Behörden ermöglichen soll, Informationen zu möglichen terroristischen Aktivitäten erst zusammenzufügen, unvermeidbar. Angesichts des hohen Ranges der gegebenenfalls durch terroristische Gewalttaten bedrohten Rechtsgüter sowie der zum Teil sehr schwer aufklärbaren Strukturen gerade von internationalen terroristischen Aktivitäten (siehe oben D. III. 3. b) ist eine solche Vorverlagerung der Terrorismusbekämpfung durch die Zusammenführung der in § 3 Abs. 1 Nr. 1 a ATDG erfassten Grunddaten rechtsstaatlich nicht ausgeschlossen.

170

b) Keinen verfassungsrechtlichen Einwänden hinsichtlich des Übermaßverbots unterliegt auch der Umfang der nach § 3 Abs. 1 Nr. 1 b ATDG zu speichernden erweiterten Grunddaten, die den beteiligten Behörden grundsätzlich nur zur verdeckten Recherche und als Klardaten in Eilfällen zur Verfügung gestellt werden. Allerdings hat der Gesetzgeber sicherzustellen, dass für diejenigen Merkmale, deren Gehalt erst durch eine weitere abstrakt-generelle Konkretisierung der Verwaltung Profil gewinnt, die für die Anwendung maßgeblichen Konkretisierungen nachvollziehbar dokumentiert und veröffentlicht werden.

171

aa) Verfassungsrechtlich unbedenklich ist die Speicherung der Merkmale des § 3 Abs. 1 Nr. 1 b aa bis ff, jj, ll, mm, oo, pp und qq ATDG.

172

(1) Die nach diesen Vorschriften in die Antiterrordatei einzustellenden Merkmale sind vom Gesetzgeber hinreichend bestimmt gefasst und nicht auf den Zwischenschritt einer abstrakt-generellen Konkretisierung durch die Verwaltung angelegt. Die Reichweite der Speicherungspflicht ist aus ihnen unmittelbar

erkennbar, und ihre Anwendung kann im Rahmen der aufsichtlichen und gegebenenfalls gerichtlichen Kontrolle ohne weiteres geprüft werden. Dass die Merkmale zum Teil in standardisierter Form mittels eines Computerprogramms gespeichert werden, ist unerheblich. Die interne Vorgabe von Standards hat keine andere Bedeutung als Vorgaben durch norminterpretierende Verwaltungsvorschriften sonst. Dies gilt jedenfalls vorliegend, wo den Behörden eine Anwendung der Vorschriften gemäß § 3 Abs. 1 Nr. 1 b rr ATDG auch in Ergänzung zu den vorgegebenen Standards möglich ist.

173

(2) Die nach diesen Vorschriften zu erfassenden Merkmale sind auch in Blick auf Umfang und Aussagegehalt mit dem Übermaßverbot vereinbar.

174

Allerdings reicht die mögliche Aussagekraft dieser Daten weit. Mit den Telekommunikationsanschlüssen, -endgeräten und E-Mailadressen werden praktisch alle modernen Kommunikationsmittel und mit den Bankverbindungen die Koordinaten praktisch aller größeren finanziellen Transaktionen erfasst; zugleich wird durch die Speicherung der genutzten Fahrzeuge eine Grundlage für Beobachtungen zur privaten Mobilität geschaffen. Dies sind die Basisdaten eines großen Teils individueller Kommunikation. Verbunden werden diese Daten überdies mit Angaben zur Ausbildung, zu individuell erworbenen Fähigkeiten und persönlichen Umständen, die Einblick in die persönliche Biographie geben. In der Kombination der verschiedenen Angaben, zumal verbunden mit den einfachen Grunddaten, lassen sich detaillierte Aussagen zu den Betroffenen zusammentragen, die sich leicht zu einem verdichteten Steckbrief zusammenfügen. Gewicht hat dies insbesondere, weil in der Datei aus verschiedenen Erhebungskontexten auch Daten der Nachrichtendienste mit denen der Polizeibehörden zusammengeführt werden (siehe oben D. III. 3. a) aa).

175

Umgekehrt ist auch hier zu berücksichtigen, dass die Vorschriften nicht eine Erhebung neuer Daten, sondern allein die Zusammenführung von bei den einzelnen Behörden bereits vorhandenen Daten vorsehen. Vor allem aber stehen diesem Eingriffsgewicht die überaus gewichtigen öffentlichen Interessen einer effektiven Aufklärung und Bekämpfung des internationalen Terrorismus gegenüber (siehe oben D. III. 3. b). Angesichts der eminenten Gefahren terroristischer Straftaten für höchste individuelle Rechtsgüter und die Rechtsordnung als Ganze ist die zusammenführende Speicherung dieser Daten bei einer Gesamtabwägung für die vom Gesetzgeber verfolgten Ziele mit dem Übermaßverbot vereinbar.

176

Dies gilt zunächst für das Ziel, diese Daten in Eilfällen als Klarinformationen zu einer handlungsanleitenden ersten Gefahren einschätzung bereitstellen zu können. Soweit der Gesetzgeber damit in besonders dringenden Gefahrensituationen das Ergreifen von polizeilichen Maßnahmen ermöglichen will - und die Nutzung auf solche gewichtigen Nottfälle begrenzt (so in § 5 Abs. 2 ATDG, siehe unten D. IV. 4. d) -, ist die zusammenführende Bereitstellung dieser bei den verschiedenen Diensten vorhandenen Daten verfassungsrechtlich gerechtfertigt.

177

Dies gilt aber auch für den weiteren mit der Speicherung dieser Daten verfolgten Zweck, nämlich für deren verdeckte Nutzung zur Informationsanbahnung. Denn gerade weil die mit diesen Daten geschaffenen Aufklärungsmöglichkeiten inhaltlich weit reichen, können sie Ermittlungen zur Terrorismusabwehr wesentlich zielführender machen und besteht an ihrer Bereitstellung auch ein gewichtiges öffentliches Interesse. Weil die Daten dabei auf einen terrorismusnahen Personenkreis und auf bereits erhobene Daten beschränkt bleiben, ist gegen ihre Bereitstellung grundsätzlich nichts einzuwenden. Entscheidend für die erweiterten Grunddaten ist dabei, dass sie den Behörden zur Informationsanbahnung nur verdeckt bereitgestellt, als Klarinformationen aber nur nach Maßgabe des Fachrechts übermittelt werden. Zwar nimmt ihnen dies nicht schon überhaupt das Eingriffsgewicht. Auch die verdeckte Bereitstellung eröffnet eine Nutzungsmöglichkeit außerhalb ihres ursprünglichen Kontexts durch den Abgleich der verschiedenen Daten untereinander sowie mit anderen Informationen und kann neue Erkenntnisse schaffen, mit denen eine fachrechtliche Übermittlung dieser Daten erst zielführend möglich und zulässig wird (siehe oben D. III. 3. a) bb) [2]). Jedoch wird das Eingriffsgewicht der Speicherung durch eine nur verdeckte Bereitstellung deutlich gemindert. Denn bei einer verdeckten Bereitstellung der Daten ist - wenn das Nutzungsregime konsequent ausgestaltet ist (siehe unten D. IV. 4. c) - gewährleistet, dass die Daten den ermittelnden Behörden durch die Abfragen noch nicht unmittelbar selbst bekannt werden, sondern erst auf Grundlage der fachrechtlichen Übermittlungsvorschriften und deren differenzierter Eingriffsschwellen und Voraussetzungen. Personenbezogene Informationen ergeben sich folglich aus diesen Daten allenfalls im Rückschluss aus der Treffermeldung, nicht aber aus einer Übermittlung dieser Daten selbst. Eine zusammenführende Speicherung von Daten zu einer in dieser Art auf die Vorbereitung eines Austauschs beschränkten verdeckten Nutzung darf sich auch auf die hier in Frage stehenden erweiterten Grunddaten erstrecken.

178

bb) Mit der Verfassung vereinbar ist auch die Speicherung der Merkmale gemäß § 3 Abs. 1 Nr. 1 b gg, hh, ii, kk, nn ATDG. Für diese Merkmale hat der Gesetzgeber jedoch sicherzustellen, dass die für ihre Anwendung erforderlichen Konkretisierungen durch die Verwaltung dokumentiert und veröffentlicht werden.

179

(1) Die Vorschriften genügen dem Bestimmtheitsgebot.

180

Allerdings sind diese Bestimmungen besonders konkretisierungsbedürftig und lassen aus sich heraus für die Bürgerinnen und Bürger noch nicht abschließend erkennbar werden, welche Informationen tatsächlich in der Datei erfasst werden. So reicht etwa das Spektrum der besonderen Fähigkeiten zur Vorbereitung und Durchführung terroristischer Straftaten, der Tätigkeiten in öffentlichen Amtsgebäuden oder der Orte und Gebiete, an denen sich terrorismusnahe Personen treffen, außerordentlich weit. Auch lässt sich, was unter Volks- oder Religionszugehörigkeit erfasst werden soll, angesichts der verschiedenen ausdifferenzierten Konkretisierungsmöglichkeiten schwer aus der Norm allein einschätzen. Die genaue Festlegung der in der Datei aufzunehmenden Informationen soll dementsprechend auch nach dem Verständnis des Gesetzgebers noch nicht abschließend in den gesetzlichen Bestimmungen selbst liegen, sondern erst in weiteren abstrakt-generellen Konkretisierungen der Sicherheitsbehörden, die diese auf einer ersten Stufe mittels der Errichtungsanordnung gemäß § 12 Nr. 3 ATDG und schließlich in einem standardisierten Computerprogramm festzulegen haben (vgl. BTDrucks 16/2950, S. 17). Ungeachtet der Ausgestaltung des § 3 Abs. 1 ATDG als strikte Speicherungspflicht wollte der Gesetzgeber mit diesen Bestimmungen ersichtlich nicht abschließend festlegen, dass alle Informationen, die unter die hier genannten Tatbestandsmerkmale subsumiert werden können, tatsächlich in die Datei aufzunehmen sind. Vielmehr sollen hierüber erst die Behörden entscheiden.

181

Trotz dieser Offenheit und Konkretisierungsbedürftigkeit genügen die Vorschriften im Gesamtkontext der Datei den Anforderungen der Normenklarheit und dem Bestimmtheitsgrundsatz. Das Bestimmtheitsgebot verbietet nicht von vornherein die Verwendung unbestimmter Rechtsbegriffe (BVerfGE 118, 168 <188>). Der Gesetzgeber ist jedoch gehalten, seine Vorschriften so bestimmt zu fassen, wie dies nach der Eigenart der zu ordnenden Lebenssachverhalte mit Rücksicht auf den Normzweck möglich ist (BVerfGE 78, 205 <212>; vgl. auch BVerfGE 110, 370 <396>; 117, 71 <111>). Erforderlich ist, dass sich unbestimmte Rechtsbegriffe durch eine Auslegung der betreffenden Normen nach den Regeln der juristischen Methodenlehre hinreichend konkretisieren lassen und verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind (vgl. BVerfGE 21, 73 <79 f.>; 118, 168 <188>; 120, 274 <316>; stRspr).

182

Im Kontext der primär auf die Informationsanbahnung der heterogenen Sicherheitsbehörden ausgerichteten Antiterrordatei mit ihrem Ziel, verstreute und auch nicht gesicherte Erkenntnisse zur Effektivierung der Terrorismusabwehr für andere Behörden leichter erschließbar zu machen, kann eine präzisere gesetzliche Umschreibung der zu speichernden Daten sinnvoll nicht verlangt werden. Die Frage, welche Aspekte im Einzelnen für die Ermittlungen erheblich sein können, steht in enger Wechselwirkung mit dem Kenntnisstand der Behörden, kann sich kurzfristig durch unvorhergesehene Ereignisse ändern und dann eine zügige Aktualisierung erfordern. Die abschließende Eingrenzung der relevanten Kriterien ist insoweit nur auf der Grundlage spezifisch fachlicher Einblicke und aktueller Einschätzungen möglich. Unter diesen Umständen ist aus dem Gesichtspunkt der Bestimmtheit nicht zu beanstanden, wenn der Gesetzgeber die zu speichernden Daten noch konkretisierungsbedürftig offen umschreibt und ein gestuftes Verfahren für deren Konkretisierung bei der Anwendung vorsieht, in dem die tatsächlich in die Datei einzustellenden Angaben nach fachlichen Kriterien präzisiert und eingegrenzt werden. Eine solche Konkretisierung ist, auch wenn sie abstrakt-generelle Festlegungen von erheblicher Bedeutung enthält, keine Aufgabe, die zwingend dem Gesetzgeber selbst obliegt. Vielmehr kann sie im gewaltenteiligen Staat rechtsstaatlich unbedenklich der Exekutive anvertraut werden. Maßgeblich ist hierbei, dass der Gesetzgeber den Behörden vorliegend nicht etwa eine Blankettvollmacht erteilt, sondern die Merkmale konkretisierungsfähig umschrieben hat. Die Gesichtspunkte und Zielrichtung der zu speichernden Daten sind gesetzlich in einer Weise sachhaltig formuliert und mit Beispielen und Beurteilungsgesichtspunkten unterlegt, dass sie als Grundlage einer Konkretisierung durch die Verwaltung aussagekräftig sind und hierfür klare Leitlinien und Grenzen enthalten. Zu berücksichtigen ist hierbei wiederum, dass es allein um die Konkretisierung des Umfangs der in die Datei einzustellenden, bei den einspeichernden Behörden bereits vorhandenen Daten zu solchen Personen geht, die als dem Terrorismus möglicherweise nahestehend angesehen werden können und insoweit vom Gesetzgeber selbst hinreichend begrenzt umschrieben sein müssen (siehe oben D. IV. 2.).

183

(2) Als Ausgleich für die Offenheit und Konkretisierungsbedürftigkeit dieser Vorschriften hat der Gesetzgeber sicherzustellen, dass die für die Anwendung der Bestimmungen im Einzelfall letztlich

maßgebliche Konkretisierung und Standardisierung seitens der Sicherheitsbehörden nachvollziehbar dokumentiert und veröffentlicht wird.

184

Angesichts der aus dem Gesetz selbst nur begrenzt erkennbaren Bedeutung der gesetzlichen Merkmale in der Anwendungspraxis bedürfen sie nachvollziehbarer Konkretisierung und Standardisierung durch die Verwaltung. Die Unbestimmtheit der hier zu beurteilenden Vorschriften bedarf deshalb eines Ausgleichs durch besondere Konkretisierungs- und Transparenzanforderungen an die Verwaltung, weil die Anwendung der vorliegenden Datei in der Regel von den Betroffenen nicht wahrgenommen wird und sich die Konkretisierung der unbestimmten Rechtsbegriffe damit nicht im Wechselspiel von Verwaltungsakt und gerichtlicher Kontrolle vollzieht. Mangels verwaltungsgerichtlicher Kontrolle fällt somit ein zentraler Mechanismus notwendiger Begrenzung unbestimmter Befugnisnormen weitgehend aus. Zur Kompensation dieser Besonderheit hat der Gesetzgeber zu gewährleisten, dass die Verwaltung die für die Anwendung der Antiterrordatei im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt und verlässlich dokumentiert (vgl. SächsVerfGH, Urteil vom 10. Juli 2003 - Vf. 43-II-00 -, juris, Rn. 193 ff.) wie auch in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Eine solche Festlegung, Dokumentation und Offenlegung dient zum einen der Einhegung der der Verwaltung eingeräumten Befugnisse, indem sie einer uferlosen oder missbräuchlichen Anwendung der Vorschrift vorbeugt (vgl. SächsVerfGH, a.a.O., Rn. 198). Zum anderen sichert sie ein hinreichendes Kontrollniveau. Die Dokumentation und Offenlegung der von der Verwaltung festgelegten Kriterien versetzt insbesondere die Datenschutzbeauftragten in die Lage, zu kontrollieren, ob die sich auch nach Vorstellung des Gesetzgebers in Stufen vollziehende Anwendung der Vorschriften durch die Exekutive rationalen Kriterien folgt und durch Sinn und Zweck des Gesetzes geleitet ist.

185

Die derzeitige Rechtslage genügt diesen Anforderungen nicht uneingeschränkt. Allerdings werden die in Frage stehenden unbestimmten Rechtsbegriffe nach gegenwärtiger Praxis durch einen - in das maßgebliche Computerprogramm eingebundenen - Katalog der zu speichernden Merkmale konkretisiert und standardisiert. Die Bundesregierung hat dem Senat diesbezüglich ein „Katalog-Manual“ vorgelegt, in dem die für die Anwendung des § 3 Abs. 1 Nr. 1 b ATDG im Einzelfall maßgeblichen Vorgaben und Kriterien dokumentiert sind. Die gesetzlichen Tatbestandsmerkmale werden in ihm durch vorgegebene Eingabealternativen - deren Beurteilung im Einzelnen nicht Gegenstand des vorliegenden Verfahrens ist - einengend präzisiert sowie die Anwendung und Bedeutung der Bestimmungen in der Praxis nachvollziehbar offengelegt.

186

Verfassungsrechtliche Bedenken bestehen jedoch in formeller Hinsicht. Das Antiterrordateigesetz macht zu einer Dokumentations- und Veröffentlichungspflicht für die Konkretisierung der in § 3 Abs. 1 Nr. 1 b ATDG enthaltenen unbestimmten Rechtsbegriffe keine hinreichend klaren Vorgaben. Schon dass eine Konkretisierung der zu erfassenden Daten in Form eines informationstechnisch aufgearbeiteten standardisierten Katalogs realisiert werden soll, lässt sich dem Gesetz nicht unmittelbar, sondern erst im Rückgriff auf die Materialien entnehmen. Das Gesetz sieht allerdings in § 12 Nr. 3 ATDG die Festlegung von Einzelheiten hinsichtlich der nach § 3 Abs. 1 ATDG zu speichernden Daten durch die Errichtungsanordnung vor. Hierunter sind jedoch - zumindest nach dem Verständnis der Norm in der Praxis - nicht die für ihre Anwendung letztlich maßgebenden Festlegungen zu verstehen, wie sie aus dem Katalog-Manual ersichtlich sind, sondern lediglich Konkretisierungen auf mittlerer Ebene, die derzeit im Hinblick auf viele Merkmale wenig über den Gesetzeswortlaut hinausgehen. Die in dem Manual dokumentierten Vorgaben werden demgegenüber nicht als Teil der Errichtungsanordnung verstanden. Jedenfalls aber ist weder für das Manual unmittelbar noch für die Errichtungsanordnung als solche eine Veröffentlichung vorgeschrieben. Vielmehr werden beide als „Verschlussache - Nur für den Dienstgebrauch“ behandelt.

187

Damit genügt die derzeitige Rechtslage den Anforderungen an eine rechtsstaatliche Ausgestaltung nicht. Will der Gesetzgeber an den unbestimmten Rechtsbegriffen in § 3 Abs. 1 Nr. 1 b gg, hh, ii, kk, nn ATDG festhalten, bedarf es einer ergänzenden Bestimmung, die eine nachvollziehbare Dokumentation und Veröffentlichung der vom Gesetzgeber vorgesehenen Konkretisierung dieser Merkmale durch die Sicherheitsbehörden gewährleistet.

188

(3) Die gemäß § 3 Abs. 1 Nr. 1 b gg, hh, ii, kk, nn ATDG in die Datei aufzunehmenden Merkmale sind ihrem Inhalt nach mit dem Übermaßverbot vereinbar. Zwar handelt es sich um Daten, die - zumal in Verbindung mit den anderen zu speichernden Merkmalen - unter Umständen höchstpersönliche Umstände offenlegen können. Angesichts der begrenzenden Funktion der Datei und der Bedeutung der Terrorismusabwehr (vgl. oben D. III. 3. a) bb), b) bewegt sich der Gesetzgeber hiermit jedoch in dem ihm zukommenden Gestaltungsspielraum.

189

Dies gilt auch für die Merkmale der Volks- und Religionszugehörigkeit gemäß § 3 Abs. 1 Nr. 1 b gg und hh ATDG. Allerdings gelten für die Aufnahme dieser Merkmale besonders hohe Anforderungen, da für sie gemäß Art. 3 Abs. 3 GG ein besonderer verfassungsrechtlicher Diskriminierungsschutz besteht und die Religionszugehörigkeit überdies durch Art. 140 GG, Art. 136 Abs. 3 WRV vor einem Offenbarenmüssen besonders geschützt ist. Entsprechend gelten diese Daten auch sonst als besonders sensibel (vgl. § 3 Abs. 9, § 28 Abs. 6 bis 9 BDSG, Art. 8 Abs. 1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Art. 6 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [BGBl 1985 II S. 539]). Die Berücksichtigung auch dieser Daten ist angesichts der Bedeutung einer wirksamen Terrorismusabwehr aber nicht von vornherein ausgeschlossen. Für sie ist allerdings von Verfassungs wegen eine zurückhaltende Umsetzung geboten. Dem ist dadurch Rechnung zu tragen, dass die Aufnahme entsprechender Angaben nicht über eine lediglich identifizierende Bedeutung hinausgeht.

190

cc) Mit dem Übermaßverbot vereinbar ist auch das Freitextfeld gemäß § 3 Abs. 1 Nr. 1 b rr ATDG. Es handelt sich hierbei nicht um eine Blankovollmacht zur Ergänzung der Datei um beliebige weitere Informationen, sondern um eine Öffnung für Hinweise und Bewertungen, die durch die Standardisierung und Katalogisierung der Eingaben sonst nicht abgebildet werden. Sie haben sich, wie sich aus dem Wortlaut ergibt, dabei stets auf die gesetzlich definierten Grunddaten oder erweiterten Grunddaten zu beziehen und sind inhaltlich durch sie gebunden. Als bloße Ergänzungen erlaubt die Vorschrift auch nicht etwa, ganze Akten in die Datei einzustellen, sondern begrenzt entsprechende Eingaben - nach derzeitiger Praxis durch eine technische Begrenzung auf 2.000 Zeichen - auf punktuelle Erläuterungen. In diesem Verständnis sind gegen die Bestimmung keine verfassungsrechtlichen Bedenken zu erheben.

191

4. Nicht in jeder Hinsicht mit dem Übermaßverbot vereinbar sind die Regelungen zur Verwendung der Daten.

192

a) Verfassungsrechtlich unbedenklich sind allerdings Abfrage und Nutzung in Bezug auf die einfachen Grunddaten gemäß § 3 Abs. 1 Nr. 1 a ATDG geregelt.

193

aa) § 5 Abs. 1 Satz 1 und 2 ATDG geben den beteiligten Behörden auf diese Daten einen unmittelbaren Zugriff als Klarinformationen. Dabei kann eine Behörde sowohl namenbezogene Abfragen vornehmen als auch Abfragen, die sich auf einzelne oder mehrere der in § 3 Abs. 1 Nr. 1 a ATDG genannten Angaben erstrecken und damit der Identifizierung ihr noch nicht bekannter Personen dienen. Im Trefferfall wird dann jeweils auf die Gesamtheit der zu den betreffenden Personen gespeicherten einfachen Grunddaten Zugriff gegeben. Dabei errichtet § 5 Abs. 1 Satz 1 ATDG keine qualifizierten Eingriffsschwellen. Für eine Abfrage reicht es, dass sie für die Erfüllung der jeweiligen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich ist. Höhere Eingriffsschwellen verlangt das Gesetz auch nicht für die - in ihm selbst noch nicht geregelten, sondern vorausgesetzten (siehe oben D. II. 2.) - Abrufbefugnisse der beteiligten Behörden; es geht ersichtlich davon aus, dass auch insoweit die niederschweligen allgemeinen Datenerhebungsbefugnisse reichen.

194

Damit sind den beteiligten Behörden Abfragen und Recherchen in den Grunddaten in weitem Umfang eröffnet. Dies bedeutet jedoch nicht, dass diese Befugnisse unbegrenzt sind. Eine Grenze liegt insbesondere darin, dass § 5 ATDG lediglich Einzelabfragen, nicht aber auch eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern erlaubt. Die Vorschrift setzt damit einen konkreten Ermittlungsanlass voraus. Auch steht jede Abfrage unter der im Einzelfall sachhaltig zu prüfenden Voraussetzung der Erforderlichkeit. Im Übrigen ermächtigt die Vorschrift nach ihrer derzeitigen Ausgestaltung weder zu einer automatischen Bilderkennung noch zur Verwendung von Ähnlichkeitsfunktionen oder zur Abfrage mit unvollständigen Daten (so genannten „wildcards“).

195

bb) Trotz der verbleibenden Weite der Abrufmöglichkeiten, insbesondere durch den Verzicht auf begrenzende Eingriffsschwellen, ist die Regelung mit dem Verhältnismäßigkeitsgrundsatz vereinbar. Maßgeblich hierfür sind die Nutzungsregelungen. Eine Nutzung der übermittelten Daten ist gemäß § 6 Abs. 1 Satz 1 ATDG ausschließlich zur Identifizierung ermittlungsrelevanter Personen und zur Vorbereitung von Einzelübermittlungersuchen an die informationsführende Behörde erlaubt. Darüber hinausgehende ermittlungs- oder handlungsleitende Informationen dürfen die Behörden aus diesen Angaben nicht ziehen. Sie können sie erst in einem weiteren Schritt nach Maßgabe des Fachrechts erlangen. Auch die Weiterverwendung der Daten zu anderen Zwecken ist nur mit Zustimmung der informationsführenden Behörde, das heißt bei sachgerechtem Verständnis wiederum nur nach Maßgabe des Fachrechts zulässig.

Bezogen auf die einfachen Grunddaten des § 3 Abs. 1 a ATDG ist ein solcher auf das Vorfeld begrenzter Austausch angesichts der großen Bedeutung der Terrorismusabwehr unter Verhältnismäßigkeitsgesichtspunkten nicht zu beanstanden. § 5 Abs. 1 Satz 1 und 2, § 6 Abs. 1 Satz 1 ATDG sind insoweit verfassungsgemäß.

196

b) Mit dem Übermaßverbot vereinbar sind auch die durch § 5 Abs. 1 Satz 1 und 3 ATDG eröffneten Recherchen in Bezug auf die erweiterten Grunddaten des § 3 Abs. 1 Nr. 1 b ATDG, soweit diese namenbezogen durchgeführt werden.

197

§ 5 Abs. 1 Satz 1 ATDG erlaubt Abfragen hinsichtlich aller in die Antiterrordatei eingestellten Daten und damit auch Recherchen in den erweiterten Grunddaten. Wenn eine Abfrage nach einer namentlich eingegebenen Person zu einem Treffer in den erweiterten Grunddaten führt, erhält die Behörde gemäß § 5 Abs. 1 Satz 3 ATDG jedoch nicht Zugang auf die erweiterten Grunddaten selbst, sondern nur eine Treffermeldung verbunden mit dem Nachweis, bei welcher Behörde und unter welchem Aktenzeichen entsprechende Informationen geführt werden. Der Zugriff auf die erweiterten Grunddaten selbst wird erst auf Einzellersuchen nach Maßgabe des Fachrechts durch Freischaltung seitens der informationsführenden Behörde ermöglicht (§ 5 Abs. 1 Satz 3 und 4 ATDG). Recherchen in Bezug auf die erweiterten Grunddaten des § 3 Abs. 1 Nr. 1 b ATDG bleiben folglich verdeckt. Ihre Übermittlung als Klarinformationen ist ein eigenständiger, nachgelagerter Rechtsakt und steht unter den jeweiligen fachrechtlichen Voraussetzungen für eine Einzelübermittlung der Daten, die hier ihrerseits die verfassungsrechtlichen Anforderungen erfüllen müssen. Gegen eine solche verdeckte Nutzung der erweiterten Grunddaten ist trotz ihrer Reichweite verfassungsrechtlich nichts zu erinnern.

198

c) Mit dem Übermaßverbot nicht vereinbar ist hingegen die Ermächtigung zu merkmalsbezogenen Recherchen in den erweiterten Grunddaten, die der abfragenden Behörde im Trefferfall nicht nur eine Fundstelle zu weiterführenden Informationen vermittelt, sondern unmittelbar Zugang zu den entsprechenden einfachen Grunddaten des § 3 Abs. 1 Nr. 1 a ATDG verschafft. § 5 Abs. 1 Satz 2 Nr. 1 a ATDG ist insoweit verfassungswidrig.

199

Der Informationsgehalt der erweiterten Grunddaten gemäß § 3 Abs. 1 Nr. 1 b ATDG reicht inhaltlich weit und kann höchstpersönliche sowie die Biographie der Betroffenen nachzeichnende Informationen enthalten (siehe oben D. IV. 3. b) aa) [2]). Der Zugriff auf solche Informationen muss unter Verhältnismäßigkeitsgesichtspunkten deshalb deutlich beschränkter bleiben als in Bezug auf die einfachen Grunddaten gemäß § 3 Abs. 1 Nr. 1 a ATDG. Der Gesetzgeber selbst sieht deshalb grundsätzlich nur eine verdeckte Recherche in diesen Daten vor und stellt ihre Übermittlung als Klarinformationen unter den Vorbehalt der fachrechtlichen Übermittlungsvorschriften. Indem er bei Recherchen in diesen Daten im Trefferfall jedoch zugleich Zugriff auf die einfachen Grunddaten als Klarinformationen gewährt, nimmt er für merkmalsbezogene Recherchen, das heißt für die „Inverssuche“, diese Einschränkung der Sache nach in erheblichem Umfang zurück. Durch die Verbindung einer Treffermeldung bezüglich erweiterter Grunddaten mit den individualisierten Informationen der einfachen Grunddaten werden auch die abgefragten erweiterten Grunddaten individuell zuordenbar und als personenbezogene Information auswertbar. So kann eine Behörde durch Abfrage einzelner oder mehrerer Merkmale - zum Beispiel durch die Suche nach Personen mit einer bestimmten Religionszugehörigkeit und Ausbildung, die einen bestimmten Treffpunkt frequentieren (vgl. § 3 Abs. 1 Nr. 1 b hh, jj, nn ATDG) - eine Recherche vornehmen und erhält im Trefferfall nicht nur die Angabe, welche Behörde insoweit Informationen führt, sondern auch alle Namen, Adressen sowie sonstige in § 3 Abs. 1 Nr. 1 a ATDG genannten Informationen von allen Personen, auf die die abgefragten Merkmale zutreffen.

200

Eine solch weitgehende Nutzung trägt der inhaltlichen Reichweite der erweiterten Grunddaten nicht hinreichend Rechnung. Ungeachtet der Frage, ob es gerechtfertigt sein kann, einzelne der erweiterten Grunddaten wie etwa die Telekommunikationsanschlüsse auch den einfachen Grunddaten zuzuordnen, ist die Möglichkeit der individuellen Erschließung des weitreichenden Informationsgehalts aller erweiterten Grunddaten im Rahmen von merkmalsbezogenen Recherchen mit dem Übermaßverbot nicht vereinbar. Wenn der Gesetzgeber in diesem Umfang Daten in die Datei einzustellen anordnet, dürfen diese im Rahmen der Informationsanbahnung nur zur Ermöglichung eines Fundstellennachweises genutzt werden. Dementsprechend muss eine Nutzungsregelung so ausgestaltet sein, dass dann, wenn sich eine Recherche auch auf erweiterte Grunddaten erstreckt, nur das Aktenzeichen und die informationsführende Behörde angezeigt werden, nicht aber auch die korrespondierenden einfachen Grunddaten.

201

d) Keinen verfassungsrechtlichen Bedenken - auch nicht für den Fall einer Inverssuche (vgl. vorstehend unter c) - unterliegt demgegenüber die Nutzung der erweiterten Grunddaten im Eilfall gemäß § 5 Abs. 2, § 6 Abs. 2 ATDG.

202

Zwar handelt es sich hierbei um die weitestgehende Nutzungsmöglichkeit der in der Antiterrordatei zusammengeführten Daten. Denn der Zugriff erstreckt sich hier zusätzlich zu den einfachen auch auf alle erweiterten Grunddaten als Klarinformationen und eröffnet dabei auch nicht nur eine Datennutzung zur Vorbereitung weiterer Übermittlungersuchen, sondern - im Sinne einer handlungsleitenden Gefahreinschätzung - auch zur Terrorismusabwehr selbst (§ 6 Abs. 2 ATDG). Daraus ergibt sich insbesondere wegen der damit verbunden Überwindung des informationellen Trennungsprinzips zwischen Nachrichtendiensten und Polizei ein besonders schweres Eingriffsgewicht (siehe oben D. III. 3. a) aa), bb) [3]).

203

Die Voraussetzungen, unter denen eine solche Nutzung erlaubt ist, sind jedoch hinreichend eng gefasst, um den Eingriff zu rechtfertigen. Erlaubt sind Zugriff und Nutzung der Daten nur zum Schutz besonders gewichtiger Rechtsgüter, das heißt zunächst zum Schutz von Leib, Leben, Gesundheit oder Freiheit von Personen. Ersichtlich sind im Kontext dieser Norm unter Gesundheitsbeeinträchtigungen nur schwerwiegende Gesundheitsverletzungen mit dauerhaften Folgen gemeint. Soweit die Vorschrift darüber hinaus auch den Schutz von Sachen mit erheblichem Wert vorsieht, stellt der Gesetzgeber klar, dass es nicht um den Schutz des Eigentums oder der Sachwerte als solcher geht, sondern um Sachen, „deren Erhaltung im öffentlichen Interesse geboten ist“ (§ 5 Abs. 2 Satz 1 ATDG). Gemeint sind im Zusammenhang mit der Terrorismusabwehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Auch enthält die Vorschrift hohe Eingriffsschwellen. Es bedarf für die Schutzgüter einer gegenwärtigen Gefahr, die sich nicht nur auf tatsächliche Anhaltspunkte stützt, sondern durch bestimmte Tatsachen unterlegt sein muss. Dabei sind Zugriff und Nutzung der Daten nur erlaubt, wenn dies unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann. Der Zugriff auf die Daten ist überdies verfahrensrechtlich gesichert. Die weitere Verwendung der Daten steht weiterhin unter Zustimmungsvorbehalt der jeweils informationsführenden Behörden, über deren Erteilung - wie der Zusammenhang der Norm nahelegt - nach Maßgabe des jeweiligen Fachrechts zu entscheiden ist. Insgesamt sind damit die Anforderungen streng; entsprechend ist die Vorschrift in der bisherigen Praxis auch erst einmal zur Anwendung gekommen. Gegen eine solche Regelung sind verfassungsrechtlich keine Bedenken zu erheben. Sie genügt dem Übermaßverbot und hat auch vor dem informationellen Trennungsprinzip Bestand.

204

5. Der Verhältnismäßigkeitsgrundsatz stellt auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Bedingt durch Zweck und Funktionsweise der Datei gewährleistet das Antiterrordateigesetz Transparenz hinsichtlich des Informationsaustauschs nur in begrenztem Umfang und öffnet damit den Betroffenen auch nur eingeschränkte Rechtsschutzmöglichkeiten; die Kontrolle über seine Anwendung liegt damit im Wesentlichen bei der Aufsicht durch die Datenschutzbeauftragten. Dies ist mit der Verfassung vereinbar, wenn für die effektive Ausgestaltung der Aufsicht verfassungsrechtliche Maßgaben beachtet werden.

205

a) Bei der Speicherung und Nutzung personenbezogener Daten für die behördliche Aufgabenwahrnehmung hat der Gesetzgeber unter Verhältnismäßigkeitsgesichtspunkten auch Anforderungen an Transparenz, Rechtsschutz und aufsichtliche Kontrolle zu beachten (vgl. BVerfGE 125, 260 <325 ff.>).

206

Transparenz der Datenverarbeitung soll dazu beitragen, dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt. Zugleich ermöglicht sie den Bürgerinnen und Bürgern, sich entsprechend zu verhalten. Gegenüber den Betroffenen bildet sie überdies die Voraussetzung für einen wirksamen Rechtsschutz. Indem sie den Einzelnen Kenntnis hinsichtlich der sie betreffenden Datenverarbeitung verschafft, setzt sie sie in die Lage, die Rechtmäßigkeit der entsprechenden Maßnahmen - erforderlichenfalls auch gerichtlich - prüfen zu lassen und etwaige Rechte auf Löschung, Berichtigung oder Genugtuung geltend zu machen (vgl. BVerfGE 100, 313 <361>; 109, 279 <363>; 118, 168 <207 f.>; 120, 351 <361>; 125, 260 <335>; stRspr).

207

Die aufsichtliche Kontrolle flankiert die subjektivrechtliche Kontrolle durch die Gerichte objektivrechtlich. Sie dient - neben administrativen Zwecken - der Gewährleistung der Gesetzmäßigkeit der Verwaltung insgesamt und schließt dabei den Schutz der subjektiven Rechte der Betroffenen ein. Dass auch Anforderungen an die aufsichtliche Kontrolle zu den Voraussetzungen einer verhältnismäßigen Ausgestaltung der Datenverarbeitung gehören können (vgl. BVerfGE 100, 313 <361> unter Verweis auf

BVerfGE 30, 1 <23 f., 30 f.>; 65, 1 <46>; 67, 157 <185>), trägt dem Umstand Rechnung, dass es sich bei der Speicherung und Verarbeitung von Daten um Eingriffe handelt, die für die Betroffenen oftmals nicht unmittelbar wahrnehmbar sind und deren Freiheitsgefährdende Bedeutung vielfach nur mittelbar oder erst später im Zusammenwirken mit weiteren Maßnahmen zum Tragen kommt. Eingriffe in das Recht auf informationelle Selbstbestimmung können deshalb auch dann unverhältnismäßig sein, wenn sie nicht durch ein hinreichend wirksames aufsichtsrechtliches Kontrollregime flankiert sind. Dies hat umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle sichergestellt werden kann.

208

b) Das Antiterrordateigesetz enthält wenige Regelungen zur Herstellung von Transparenz und zur Gewährleistung individuellen Rechtsschutzes. Im Wesentlichen begnügt es sich mit der Anerkennung von - inhaltlich wie verfahrensrechtlich begrenzt wirksamen - Auskunftsrechten. Angesichts der Funktion und Wirkweise dieser Datei ist das jedoch nicht zu beanstanden.

209

aa) Als maßgebliches Instrument zur Gewährleistung von Transparenz sieht das Antiterrordateigesetz Auskunftsansprüche nach Maßgabe des Bundesdatenschutzgesetzes vor (§ 10 Abs. 2 ATDG). Diese Ansprüche unterliegen freilich Grenzen und sind zum Teil nur mit beträchtlichem Verfahrensaufwand realisierbar. Angesichts der Funktion des Antiterrordateigesetzes genügen sie jedoch verfassungsrechtlichen Anforderungen.

210

(1) § 10 Abs. 2 ATDG gewährt grundsätzlich einen Anspruch auf Auskunft, ob Daten des Auskunftssuchenden in der Datei erfasst sind. Durch Verweis auf § 19 BDSG und die Grenzen der Auskunftserteilung nach den für die datenverantwortlichen Behörden jeweils geltenden Rechtsvorschriften ist dieser Anspruch indessen begrenzt. So bleibt die Auskunft etwa ausgeschlossen, wenn sie die Aufgabenwahrnehmung der informationsführenden Behörde gefährdet (vgl. § 19 Abs. 4 Nr. 1 BDSG; § 15 Abs. 2 Nr. 1 BVerfSchG; Art. 48 Abs. 2 Nr. 1 BayPAG) oder die Ausforschung des Erkenntnisstandes einer Verfassungsschutzbehörde zu befürchten ist (vgl. etwa § 15 Abs. 2 Nr. 2 BVerfSchG; Art. 11 Abs. 3 Nr. 2 BayVSG; § 14 Abs. 2 Nr. 2 VSG NRW). Für die Antiterrordatei ist davon auszugehen, dass diesen Ausnahmen außerhalb von Fehlanzeigen Bedeutung zukommen und sie den Auskunftsanspruch deutlich einschränken können. Die Auskunftsrechte sind deshalb aber nicht unzureichend. Einschränkungen der Auskunftspflicht setzen voraus, dass sie gegenläufigen Interessen von größerem Gewicht dienen und die gesetzlichen Ausschlussstatbestände sicherstellen, dass die betroffenen Interessen einander umfassend und auch mit Blick auf den Einzelfall zugeordnet werden (vgl. BVerfGE 120, 351 <364 f.>). Weitergehende Auskunftsrechte ergeben sich aus der Verfassung auch nicht für die Antiterrordatei.

211

(2) Für verdeckt gespeicherte Daten gemäß § 4 ATDG ist die Geltendmachung von Auskunftsansprüchen mit erheblichem Verfahrensaufwand verbunden. Anders als für die anderen Daten kann hier der Auskunftsanspruch gemäß § 10 Abs. 2 ATDG nicht einheitlich gegenüber dem Bundeskriminalamt geltend gemacht werden, sondern nur gegenüber den einzelnen informationsführenden Behörden. Gegebenenfalls kann damit ein Antrag auf Auskunft bei allen Behörden, die Daten in die Antiterrordatei einspeichern, erforderlich sein. Trotz der Schwerfälligkeit eines solchen Verfahrens ist auch diese Regelung verfassungsrechtlich noch hinnehmbar. Sie ist eine Konsequenz und Kehrseite der auch im Interesse der Betroffenen ergangenen Entscheidung, bestimmte Daten als so geheim einzustufen, dass sie nur vollständig verdeckt in die Datei eingestellt werden und für keine Behörde - auch nicht das Bundeskriminalamt - erkennbar sind. Ob Daten einer solchen Geheimhaltung bedürfen, ist eine Entscheidung des Gesetzgebers, die grundsätzlich in seiner Verantwortung liegt und verfassungsrechtlich vertretbar ist. Erschwert der Gesetzgeber aus Geheimschutzgründen in dieser Weise schon den Informationsaustausch zwischen den Behörden selbst, ist auch die entsprechende Erschwerung der Auskunftsansprüche hinnehmbar. Eine mögliche Bündelung der Auskunftspflicht durch das Bundeskriminalamt, die die Schwerfälligkeit letztlich geteilter Auskunftspflichten nicht substantiell beseitigen könnte, muss der Gesetzgeber nicht vorsehen.

212

(3) Insgesamt sind damit die Auskunftsansprüche verfassungsrechtlich vertretbar ausgestaltet. Sie können freilich nur ein Mindestmaß an Transparenz für die Einzelnen gewährleisten. Angesichts des Zwecks und der Wirkweise der Antiterrordatei ist dieses jedoch verfassungsrechtlich hinzunehmen.

213

bb) Im Übrigen kennt das Antiterrordateigesetz weder einen Grundsatz der Offenheit der Datennutzung noch einen Richtervorbehalt noch eigene nachträgliche Benachrichtigungspflichten, die über die Benachrichtigungspflichten aus anderen Vorschriften hinausgehen. Es verzichtet damit auf wichtige Instrumentarien zur Gewährleistung der Verhältnismäßigkeit der Datennutzungsregelungen. Angesichts des Zwecks der Antiterrordatei ist dies jedoch verfassungsrechtlich gerechtfertigt. Die Antiterrordatei dient im Kern der Informationsanbahnung zur Vorbereitung weiterer Ermittlungen im Rahmen der Abwehr des

internationalen Terrorismus. Dass solche Ermittlungen grundsätzlich nicht dem Grundsatz der Offenheit folgen können, liegt auf der Hand. Auch ein Richtervorbehalt ist im Rahmen der Antiterrordatei kein geeignetes Mittel, das verfassungsrechtlich geboten wäre. Wegen der geringen rechtlichen Durchformung der Befugnisse gemäß § 5 Abs. 1 ATDG und der Eilbedürftigkeit der Entscheidung bei einem Zugriff gemäß § 5 Abs. 2 ATDG würde ein richterlicher Prüfvorbehalt weitgehend leerlaufen. Ebenfalls ist das Absehen von spezifischen Benachrichtigungspflichten verfassungsrechtlich vertretbar. Eine Benachrichtigungspflicht käme ohne substantielle Beeinträchtigung der Funktionsweise der Datei nur für die Fälle in Betracht, in denen Personen endgültig aus der Datei herausgenommen werden. Der Nutzen einer derart beschränkten Benachrichtigungspflicht ist im Vergleich zum damit verbundenen Aufwand jedoch zu gering, als dass sie unter Verhältnismäßigkeitsgesichtspunkten geboten wäre.

214

c) Weil eine Transparenz der Datenverarbeitung und die Ermöglichung individuellen Rechtsschutzes durch das Antiterrordateigesetz nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen.

215

aa) Die Gewährleistung einer wirksamen Aufsicht setzt zunächst sowohl auf Bundes- wie auf Landesebene mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen - wie nach geltendem Recht die Datenschutzbeauftragten - voraus. Weiter ist erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Dabei muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält.

216

In Blick auf den Charakter der Antiterrordatei als eine Bund und Länder übergreifende Verbunddatei ist Sorge dafür zu tragen, dass deren effektive Kontrolle nicht aufgrund föderaler Zuständigkeitsunklarheiten hinter der Effektivierung des Datenaustauschs zurückbleibt. Dies bedeutet nicht, dass dem Datenschutzbeauftragten des Bundes ein umfassender Zugriff auch auf solche Protokolldaten zu gewähren ist, die das Einstellen und Abrufen der Daten seitens der Landesbehörden betreffen. Vielmehr obliegt deren Kontrolle den Landesbeauftragten. Allerdings entspricht es der Antiterrordatei als Verbunddatei, dass es den Datenschutzbeauftragten gestattet sein muss, zusammenzuarbeiten und sich etwa im Wege der Amtshilfe durch Delegation oder Ermächtigung bei der Wahrnehmung ihrer Befugnisse gegenseitig zu unterstützen. Ebenfalls ist zu gewährleisten, dass im Zusammenspiel der verschiedenen Aufsichtsinstanzen auch eine Kontrolle der durch Maßnahmen nach dem Artikel 10-Gesetz gewonnenen Daten - die in einer Datei, welche maßgeblich auch vom Bundesnachrichtendienst befüllt wird, besondere Bedeutung haben - praktisch wirksam sichergestellt ist. Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.

217

Ansichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen - deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf - durchzuführen. Dies ist bei ihrer Ausstattung zu berücksichtigen.

218

bb) Die Gewährleistung der verfassungsrechtlichen Anforderungen einer wirksamen aufsichtlichen Kontrolle obliegt dem Gesetzgeber und den Behörden gemeinsam.

219

Der Gesetzgeber hat in § 8 ATDG die Verantwortung für die Datenverarbeitung geregelt, in § 5 Abs. 4, § 9 ATDG eine differenzierte und umfassende Protokollierung aller Zugriffe auf die Datenbank angeordnet und sieht in § 10 Abs. 1 ATDG eine an die föderale Kompetenzverteilung anknüpfende, sachlich nicht eingeschränkte Aufsicht durch die Datenschutzbeauftragten des Bundes und der Länder vor. Diese Regelungen sind Grundlage für eine wirksame Kontrolle, die im Wesentlichen den verfassungsrechtlichen Anforderungen genügt. Dass dabei gemäß § 10 Abs. 1 ATDG in Verbindung mit § 24 Abs. 4 Satz 4 BDSG in besonderen, strikt zu handhabenden Ausnahmefällen eine Auskunft oder Einsicht unter Umständen verweigert werden kann, stellt die Wirksamkeit dieser Befugnisse nicht in Frage. An einer hinreichenden gesetzlichen Vorgabe fehlt es allerdings hinsichtlich des Erfordernisses turnusmäßig festgelegter Pflichtkontrollen. Den Gesetzgeber trifft insoweit eine Nachbesserungspflicht.

220

Im Übrigen darf der Gesetzgeber zunächst darauf vertrauen, dass die Bestimmungen in einer kooperationsbereiten Behördenpraxis wirksam umgesetzt werden. Er hat insoweit allerdings zu

beobachten, ob hierbei Konflikte auftreten, die gesetzlicher Klarstellungen oder der Einführung etwa von Streitleösungsmechanismen wie dem Ausbau von Klagebefugnissen (vgl. Sächs. OVG, Beschluss vom 25. September 1998 - 3 S 379/98 -, NJW 1999, S. 2832; weitergehend Art. 76 Abs. 2 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [Datenschutz-Grundverordnung] vom 25. Januar 2012, KOM[2012] 11 endgültig) bedürfen.

221

d) Zur Gewährleistung von Transparenz und Kontrolle bedarf es schließlich einer gesetzlichen Regelung von Berichtspflichten.

222

Da sich die Speicherung und Nutzung der Daten nach dem Antiterrordateigesetz der Wahrnehmung der Betroffenen und der Öffentlichkeit weitgehend entzieht, dem auch die Auskunftsrechte nur begrenzt entgegenwirken und weil eine effektive gerichtliche Kontrolle nicht ausreichend möglich ist, sind hinsichtlich Datenbestand und Nutzung der Antiterrordatei regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über den mit der Antiterrordatei ins Werk gesetzten Datenaustausch zu ermöglichen und diesen einer demokratischen Kontrolle und Überprüfung zu unterwerfen.

223

6. Keine verfassungsrechtlichen Bedenken bestehen hinsichtlich der Verfassungsmäßigkeit der in § 11 Abs. 2 und 4 ATDG geregelten Löschungsvorschriften. Dass die Höchstgrenze der Speicherdauer den Lösungsfristen der jeweiligen in die Datei eingestellten Daten gemäß dem für diese geltenden Fachrecht folgt, ist nach der Konzeption der Datei als Verbunddatei naheliegend und jedenfalls verfassungsrechtlich vertretbar.

V.

224

Soweit die angegriffenen Vorschriften die Einbeziehung von Daten in die Antiterrordatei vorsehen, die durch Eingriffe in das Telekommunikationsgeheimnis oder das Grundrecht auf Unverletzlichkeit der Wohnung erhoben werden, verstoßen sie gegen Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.

225

1. Für Datenerhebungen, die in die Grundrechte der Art. 10 Abs. 1 und Art. 13 Abs. 1 GG eingreifen, gelten angesichts deren besonderen Schutzgehalts in der Regel besonders strenge Anforderungen. Diese gesteigerten Anforderungen wirken nach der Rechtsprechung des Bundesverfassungsgerichts auch in den Anforderungen für die Weitergabe und Zweckänderung der hierdurch gewonnenen Daten fort. So darf etwa die Schwelle für die Übermittlung von Daten, die im Rahmen strafprozessualer Maßnahmen durch eine Wohnraumüberwachung erlangt wurden, nicht unter diejenige abgesenkt werden, die bei der Gefahrenabwehr für entsprechende Eingriffe gilt, da durch eine Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden nicht umgangen werden dürfen (vgl. BVerfGE 109, 279 <377 f.>; vgl. auch BVerfGE 100, 313 <389 f., 394>). Ebenso ist eine Weitergabe von Telekommunikationsdaten, die nur unter besonders strengen Bedingungen abgerufen werden dürfen, nur dann an eine andere Stelle zulässig, wenn sie zur Wahrnehmung von Aufgaben erfolgt, deretwegen ein Zugriff auf diese Daten auch unmittelbar zulässig wäre (vgl. BVerfGE 125, 260 <333>; ähnlich bereits BVerfGE 100, 313 <389 f.>; 109, 279 <375 f.>; 110, 33 <73 f.>). Dem entspricht, dass Daten, die aus gewichtigen Eingriffen in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG stammen, zu kennzeichnen sind. Die Erkennbarkeit solcher Daten soll die Beachtung der spezifischen Grenzen für die Datennutzung auch nach deren etwaiger Weiterleitung an andere Stellen sicherstellen.

226

2. Eine vollständige und uneingeschränkte Einbeziehung aller auch durch Eingriff in Art. 10 Abs. 1 und in Art. 13 Abs. 1 GG erhobenen Daten in die Antiterrordatei ist mit diesen Anforderungen nicht vereinbar; nichts anderes kann im Übrigen auch für solche Daten gelten, die durch Eingriff in das - von dem Beschwerdeführer nicht gerügte - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (vgl. BVerfGE 120, 274 <302 f.>) gewonnen wurden. Solche Daten können regelmäßig nur unter strengen Maßgaben erhoben werden und setzen etwa das Vorliegen erhöhter Eingriffsschwellen wie eine qualifizierte Gefahrenlage oder einen qualifizierten Tatverdacht, eine Gefahr für besonders bedeutsame Rechtsgüter beziehungsweise die Verfolgung von besonders gravierenden Straftaten voraus. Zu ihnen gehören insbesondere Informationen, die durch Telekommunikationsüberwachung, Wohnraumüberwachung oder auch Maßnahmen der strategischen Beschränkung (vgl. §§ 5 ff. G 10) gewonnen und gegebenenfalls auf das Artikel 10-Gesetz gestützt wurden. Durch Einstellung in die Antiterrordatei können diese Daten - etwa ein bei einer Abhörmaßnahme in Erfahrung gebrachtes besonderes körperliches Merkmal oder ein seltener Dialekt -

einer großen Anzahl von Behörden ohne weiteres als Vorabinformationen zugänglich gemacht und zur Recherche zur Verfügung gestellt werden, allein damit diese sich über die Identität dieser Person ein Bild machen und entscheiden können, ob sie ein Einzelübermittlungsersuchen stellen wollen (vgl. § 6 Abs. 1 Satz 1 ATDG). Die Informationen werden hierbei unabhängig von bereits geschehenen oder konkret bevorstehenden Terrorakten für Ermittlungsmaßnahmen noch weit im Vorfeld greifbarer Gefahrenlagen zur Verfügung gestellt, für die eine Datenerhebung unter schweren Eingriffen in das Telekommunikationsgeheimnis oder die Unverletzlichkeit der Wohnung nicht gerechtfertigt werden könnte. Auch wenn das Kriterium der verfassungsrechtlichen Zulässigkeit einer hypothetischen Neuerhebung der Daten für die Beurteilung einer Weiterleitung bereits erhobener Daten nicht schematisch abschließend ist und die Berücksichtigung weiterer Gesichtspunkte nicht ausschließt, ist vorliegend eine vollständige und unterschiedslose Einbeziehung auch der durch Eingriff in Art. 10 Abs. 1 und Art. 13 Abs. 1 GG erhobenen Daten mit dem Übermaßverbot bei Gesamtabwägung unvereinbar.

227

3. Hieran ändert die Einlassung der Bundesregierung in der mündlichen Verhandlung nichts, nach der solche Daten künftig nur noch gemäß § 4 ATDG verdeckt gespeichert würden. Aus dem Antiterrordateigesetz ergibt sich eine solche Beschränkung nicht. Indem § 3 Abs. 2 ATDG ausdrücklich auf kennzeichnungspflichtige Daten Bezug nimmt, wird vielmehr erkennbar, dass auch solche Daten grundsätzlich von den Regelungen des Antiterrordateigesetzes umfasst sein sollen. Dementsprechend war auch die bisherige Praxis nach Auskunft der Bundesregierung insoweit jedenfalls nicht einheitlich. Verfassungsrechtlich tragfähig ist diesbezüglich nur eine Regelung, die den Umgang mit diesen Daten in einer dem Grundsatz der Normenklarheit genügenden Form ausdrücklich festlegt.

228

Allerdings wäre eine Regelung, die für solche Daten stets eine verdeckte Speicherung gemäß § 4 ATDG vorsieht, unter Verhältnismäßigkeitsgesichtspunkten mit der Verfassung vereinbar. Sie gewährleistet, dass die entsprechenden Informationen nur nach Maßgabe der fachrechtlichen Übermittlungsvorschriften zugänglich gemacht werden, denen dann ihrerseits die Funktion zukommt, die verfassungsrechtlich gebotenen qualifizierten Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz sicherzustellen. Da dieser Weg in der mündlichen Verhandlung von der Regierung und allen anwesenden Vertretern der Sicherheitsbehörden einhellig als sachgerecht angesehen wurde, besteht kein Anlass zu der Prüfung, ob auch andere Wege - wie die Unterwerfung solcher Daten unter eine Nutzungsregelung wie für die erweiterten Grunddaten (siehe oben D. IV. 4. c) - verfassungsrechtlich zulässig wären.

E.

I.

229

Die teilweise Verfassungswidrigkeit der angegriffenen Vorschriften führt nicht zu deren Nichtigkeitserklärung, sondern nur zur Feststellung ihrer Unvereinbarkeit mit dem Grundgesetz. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2014, dürfen die Vorschriften weiter angewendet werden, jedoch mit der Maßgabe, dass außerhalb des Eilfalls gemäß § 5 Abs. 2 ATDG eine Nutzung der Antiterrordatei nur zulässig ist, sofern der Zugriff auf die Daten von Kontaktpersonen gemäß § 2 Satz 1 Nr. 3 ATDG und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen und gewährleistet ist, dass bei Recherchen in den erweiterten Grunddaten im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Abs. 1 Nr. 3 ATDG, nicht aber zu Informationen gemäß § 3 Abs. 1 Nr. 1 a ATDG gewährt wird. Sobald die Möglichkeit des Zugriffs auf die Daten von Kontaktpersonen und auf Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, ausgeschlossen werden kann, dürfen diese auch für die Nutzung der Datei im Eilfall gemäß § 5 Abs. 2 ATDG nicht mehr genutzt werden.

230

Die bloße Unvereinbarkeitserklärung, verbunden mit einer befristeten Fortgeltung der verfassungswidrigen Regelung, kommt in Betracht, wenn die sofortige Ungültigkeit der beanstandeten Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist (BVerfGE 109, 190 <235 f.>). Dies ist vorliegend der Fall. Die Datei wird vom Gesetzgeber mit plausiblen Gründen als wesentliche Verbesserung für eine wirksame Terrorismusabwehr angesehen. Dabei ist die Grundanlage der Datei und des durch sie ins Werk gesetzten Informationsaustauschs vom Gesetzgeber differenziert ausgestaltet und mit der Verfassung grundsätzlich vereinbar. Da die Verfassungswidrigkeit im Wesentlichen Einzelfragen der Ausgestaltung betrifft, deren belastende Wirkungen durch einschränkende Maßgaben der vorübergehenden Anwendbarkeit der Vorschriften gemildert werden können, ergibt sich angesichts der Bedeutung der Datei für die Abwehr des

internationalen Terrorismus bei einer Gesamtabwägung, dass die angegriffenen Vorschriften vorübergehend weiter angewendet werden können.

231

Als Voraussetzung für eine vorübergehende weitere Anwendbarkeit ist allerdings zuvor die Zugriffsmöglichkeit auf Daten von Kontaktpersonen gemäß § 2 Satz 1 Nr. 3 ATDG auszuschließen sowie sicherzustellen, dass bei Recherchen in den erweiterten Grunddaten und in Daten, die aus Eingriffen in das Telekommunikationsgeheimnis und das Grundrecht auf Unverletzlichkeit der Wohnung herrühren, im Trefferfall allein ein Zugang zu Informationen gemäß § 3 Abs. 1 Nr. 3 ATDG, nicht aber zu Informationen gemäß § 3 Abs. 1 Nr. 1 a ATDG gewährt wird. Die Eilfallregelung des § 5 Abs. 2 ATDG darf ohne zuvor zu erfüllende Maßgaben weiterhin angewendet werden, damit für solche dringenden Gefahren keine Schutzlücke entsteht. Sobald der Zugriff auf diese Daten jedoch für die vorübergehende Nutzung der Daten gemäß § 5 Abs. 1 ATDG ausgeschlossen ist, ist ein solcher Zugriff auch im Rahmen des § 5 Abs. 2 ATDG unzulässig. Denn auch im Eilfall gibt es keinen Grund mehr für einen Zugriff auf verfassungsrechtlich zu Unrecht bereitgestellte Daten, sobald diese ohne weiteres herausgefiltert und gesperrt werden können.

232

Dem Gesetzgeber wird eine großzügige Frist eingeräumt, die es ihm ermöglicht zu prüfen, ob er im Zusammenhang mit der Neuregelung des Antiterrordateigesetzes auch eine Überarbeitung von Bestimmungen anderer Gesetze, die den angegriffenen Vorschriften dieses Verfahrens ähnlich sind, sowie eventuell von Datenübermittlungsvorschriften einzelner Sicherheitsbehörden für angezeigt hält und diese möglicherweise hiermit verbinden will.

II.

233

Die Entscheidung ist zu C. einstimmig, im Übrigen teilweise mit Gegenstimmen ergangen. Die Entscheidung über die Auslagenerstattung beruht auf § 34a Abs. 2 und 3 BVerfGG.

Kirchhof
Schluckebier
Baer

Gaier
Masing

Eichberger
Paulus
Britz