L e i t s ä t z e

zum Urteil des Ersten Senats vom 20. April 2016

- 1 BvR 966/09 -
- 1 BvR 1140/09 -

1. a) Die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen (Wohnraumüberwachungen, Online-Durchsuchungen, Telekommunikationsüberwachungen, Telekommunikationsverkehrsdatenerhebungen und Überwachungen außerhalb von Wohnungen mit besonderen Mitteln der Datenerhebung) ist zur Abwehr von Gefahren des internationalen Terrorismus im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar.

   b) Die Ausgestaltung solcher Befugnisse muss dem Verhältnismäßigkeitsgrundsatz genügen. Befugnisse, die tief in das Privatleben hineinreichen, müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein, setzen voraus, dass eine Gefährdung dieser Rechtsgüter hinreichend konkret absehbar ist, dürfen sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken, verlangen überwiegend besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie einen Schutz von Berufsgeheimnisträgern, unterliegen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle und müssen mit Löschungspflichten bezüglich der erhobenen Daten flankiert sein.

2. Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung.

   a) Die Reichweite der Zweckbindung richtet sich nach der jeweiligen Ermächtigung für die Datenerhebung; die Datenerhebung bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren.

   b) Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung). Dies setzt voraus,

dass es sich um eine Verwendung der Daten durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter handelt. Für Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme müssen zusätzlich für jede weitere Nutzung auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein.

c) Der Gesetzgeber kann darüber hinaus eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung).

Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientieren sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes.

Für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen darf die Verwendung zu einem geänderten Zweck allerdings nur erlaubt werden, wenn auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sind.

3. Die Übermittlung von Daten an staatliche Stellen im Ausland unterliegt den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung. Bei der Beurteilung der neuen Verwendung ist die Eigenständigkeit der anderen Rechtsordnung zu achten. Eine Übermittlung von Daten ins Ausland verlangt eine Vergewisserung darüber, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 966/09 -
- 1 BvR 1140/09 -

Verkündet
am 20. April 2016
Sommer
Amtsinspektorin
als Urkundsbeamtin
der Geschäftsstelle

IM NAMEN DES VOLKES

In den Verfahren
über
die Verfassungsbeschwerden

I. 1. des Herrn B…,

2. des Herrn F…,

3. des Herrn Sch…,

4. des Herrn Prof. Dr. H…,

5. des Herrn Dr. N…,

6. des Herrn H…

- Bevollmächtigte: 1. Rechtsanwalt Dr. Dr. h.c. Burkhard Hirsch,
Rheinallee 120, 40545 Düsseldorf,

2. Rechtsanwalt Gerhart R. Baum
in Sozietät Rechtsanwälte Baum, Reiter & Collegen,
Benrather Schloßallee 101, 40597 Düsseldorf -

gegen § 14, § 20c Abs. 3, § 20g, § 20h, § 20k, § 20l, § 20u Abs. 1 und 2, § 20v und § 20w des Bundeskriminalamtgesetzes (BKAG) in der Fassung vom 31. Dezember 2008 (BGBl 2008, S. 3083 ff.)

- 1 BvR 966/09 -,

II. 1. des Herrn W…,

2. des Herrn St…,

3. des Herrn Dr. T…,

4. der Frau R…,

5. des Herrn N…,

6. des Herrn T…,

7. der Frau M…,

8. der Frau K…,

9. des Herrn B…

- Bevollmächtigter: Rechtsanwalt Sönke Hilbrans
in Sozietät dka Rechtsanwälte Fachanwälte,
Immanuelkirchstraße 3-4, 10405 Berlin -

gegen a) § 20g Abs. 1 und 2, § 20h Abs. 1, 2 und 5,
§ 20j Abs. 1, § 20k Abs. 1 und 7,
§ 20l Abs. 1 und 6, § 20m Abs. 1,
§ 20v Abs. 4 Satz 2 und Abs. 6 Satz 5,
§ 20w Abs. 2 Satz 1 und 2 BKAG,

b) § 20h Abs. 5 Satz 10, § 20k Abs. 7 Satz 8,
§ 20l Abs. 6 Satz 10 BKAG,

c) § 20u Abs. 1 und 2 BKAG in Verbindung mit
§ 53 Abs. 1 Satz 1 Nr. 2 und 3 StPO

- 1 BvR 1140/09 -

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 7. Juli 2015 durch

U r t e i l

für Recht erkannt:

1. § 20h Absatz 1 Nummer 1 c des Bundeskriminalamtgesetzes in der Fassung des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (Bundesgesetzblatt I Seite 3083) und in der Fassung späterer Gesetze verstößt gegen Artikel 13 Absatz 1 des Grundgesetzes und ist nichtig.

2. § 20v Absatz 6 Satz 5 Bundeskriminalamtgesetz verstößt gegen Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 10 Absatz 1, Artikel 13 Absatz 1, jeweils in Verbindung mit Artikel 19 Absatz 4 des Grundgesetzes, und ist nichtig.

3. § 14 Absatz 1 (ohne Satz 1 Nummer 2), § 20g Absatz 1 bis 3, §§ 20h, 20j, 20k, 20l, § 20m Absatz 1, 3, § 20u Absatz 1, 2 und § 20v Absatz 4 Satz 2, Absatz 5

Satz 1 bis 4 (ohne Satz 3 Nummer 2), Absatz 6 Satz 3 des Bundeskriminalamtgesetzes sind nach Maßgabe der Urteilsgründe mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 10 Absatz 1, Artikel 13 Absatz 1 und 3 - auch in Verbindung mit Artikel 1 Absatz 1 und Artikel 19 Absatz 4 Grundgesetz - nicht vereinbar.

4. Bis zu einer Neuregelung, längstens jedoch bis zum 30. Juni 2018 gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass Maßnahmen gemäß § 20g Absatz 2 Nummern 1, 2 b, 4 und 5 Bundeskriminalamtgesetz nur durch ein Gericht angeordnet werden dürfen; bei Gefahr im Verzug gilt § 20g Absatz 3 Satz 2 bis 4 Bundeskriminalamtgesetz entsprechend.

   Maßnahmen gemäß § 20g Absatz 1 Satz 1 Nummer 2, § 20l Absatz 1 Satz 1 Nummer 2 und § 20m Absatz 1 Nummer 2 Bundeskriminalamtgesetz dürfen nur angeordnet werden, wenn die Voraussetzungen des § 20k Absatz 1 Satz 2 Bundeskriminalamtgesetz in der in den Urteilsgründen dargelegten verfassungskonformen Auslegung vorliegen.

   Eine weitere Verwendung von Daten gemäß § 20v Absatz 4 Satz 2 Bundeskriminalamtgesetz oder eine Übermittlung von Daten gemäß § 20v Absatz 5 und § 14 Absatz 1 Bundeskriminalamtgesetz betreffend Daten aus Wohnraumüberwachungen (§ 20h Bundeskriminalamtgesetz) ist nur bei Vorliegen einer dringenden Gefahr und betreffend Daten aus Online-Durchsuchungen (§ 20k Bundeskriminalamtgesetz) nur bei Vorliegen einer im Einzelfall drohenden Gefahr für die jeweils maßgeblichen Rechtsgüter zulässig.

5. Die Verfassungsbeschwerde des Beschwerdeführers zu 4. in dem Verfahren 1 BvR 966/09 hat sich durch seinen Tod erledigt.

6. Im Übrigen werden die Verfassungsbeschwerden zurückgewiesen.

7. Die Bundesrepublik Deutschland hat den Beschwerdeführern ihre notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

G r ü n d e:

A.

I.

Die Verfassungsbeschwerden richten sich gegen Regelungen des Bundeskriminalamtgesetzes (im Folgenden: BKAG), die als Unterabschnitt 3a durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl I S. 3083) mit Wirkung zum 1. Januar 2009 eingefügt wurden. Der Bundesgesetzgeber hat so auf der Grundlage des hierfür im Jahre 2006 neu geschaffenen Art. 73 Abs. 1 Nr. 9a GG (BGBl I S. 2034) dem Bundeskriminalamt über die bisherigen Aufgaben der Strafverfolgung hinaus die bis dahin allein den Ländern vorbehaltene Aufgabe der Abwehr von Gefahren des internationalen Terrorismus übertragen. Gegenstand der Verfassungsbeschwerden ist daneben eine bereits zuvor bestehende Regelung des Bundeskriminalamtgesetzes zur Übermittlung von Daten ins Ausland, die durch die Aufgabenerweiterung ein weiteres Anwendungsfeld erhält. 1

II.

Die Verfassungsbeschwerden wenden sich zum einen gegen die Einräumung verschiedener Ermittlungsbefugnisse. Angegriffen ist die Ermächtigung zur Befragung von Personen gemäß § 20c BKAG sowie zum Einsatz von besonderen Mitteln der Datenerhebung außerhalb von Wohnungen gemäß § 20g Abs. 1 bis 3 BKAG, wozu insbesondere das geheime Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes, die Erstellung von Bildaufnahmen, die Anbringung von Peilsendern und der Einsatz von Vertrauenspersonen und Verdeckten Ermittlern gehören. Weiter richten sich die Verfassungsbeschwerden gegen die Befugnis zur Durchführung optischer und akustischer Wohnraumüberwachungen gemäß 2

§ 20h BKAG, zur Rasterfahndung gemäß § 20j BKAG, zu Zugriffen auf informationstechnische Systeme gemäß § 20k BKAG, zur Überwachung der laufenden Telekommunikation gemäß § 20l BKAG sowie zur Erhebung von Telekommunikationsverkehrsdaten gemäß § 20m Abs. 1, 3 BKAG. Angegriffen sind insoweit auch § 20u BKAG, der den Schutz zeugnisverweigerungsberechtigter Personen regelt, sowie § 20w BKAG, der die Pflicht zur Benachrichtigung der betroffenen Personen nach Abschluss der Überwachungsmaßnahme anordnet.

Zum anderen wenden sich die Verfassungsbeschwerden gegen Regelungen zur Datennutzung. Dies betrifft zunächst die Regelung zur Nutzung der nach dem Unterabschnitt 3a des Gesetzes erhobenen Daten gemäß § 20v Abs. 4 Satz 2 BKAG durch die Behörde selbst. Zur Prüfung gestellt sind des Weiteren die Befugnisse gemäß § 20v Abs. 5 BKAG - mit Ausnahme des Satzes 3 Nr. 2 - zur Übermittlung dieser Daten an andere öffentliche Stellen im Inland. Schließlich richten sich die Angriffe auch gegen § 14 Abs. 1 Satz 1 Nr. 1 und 3 und Satz 2, Abs. 7 BKAG, der allgemein die Übermittlung von Daten an ausländische Stellen erlaubt. Nicht Gegenstand des Verfahrens ist demgegenüber § 14a BKAG, der daneben eine spezielle Befugnis zur Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union begründet. 3

Die für das Verfahren maßgeblichen Normen lauten: 4

§ 4a Abwehr von Gefahren des internationalen Terrorismus

(1) Das Bundeskriminalamt kann die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus in Fällen wahrnehmen, in denen

1. eine länderübergreifende Gefahr vorliegt,

2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder

3. die oberste Landesbehörde um eine Übernahme ersucht.

Es kann in diesen Fällen auch Straftaten verhüten, die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Bege-

hung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können.

(2) Die Befugnisse der Länder und anderer Polizeibehörden des Bundes bleiben unberührt. Die zuständigen obersten Landesbehörden und, soweit zuständig, anderen Polizeibehörden des Bundes sind unverzüglich zu benachrichtigen, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt. Die Aufgabenwahrnehmung erfolgt in gegenseitigem Benehmen. Stellt das Bundeskriminalamt bei der Aufgabenwahrnehmung nach Absatz 1 Satz 1 Nr. 2 die Zuständigkeit einer Landespolizeibehörde fest, so gibt es diese Aufgabe an diese Polizeibehörde ab, wenn nicht ein Fall des Absatzes 1 Satz 1 Nr. 1 oder 3 vorliegt.

Unterabschnitt 2

§ 14 Befugnisse bei der Zusammenarbeit im internationalen Bereich

(1) Das Bundeskriminalamt kann an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen anderer Staaten sowie zwischen- und überstaatliche Stellen, die mit Aufgaben der Verhütung oder Verfolgung von Straftaten befaßt sind, personenbezogene Daten übermitteln, soweit dies erforderlich ist

1. zur Erfüllung einer ihm obliegenden Aufgabe,

2. zur Verfolgung von Straftaten und zur Strafvollstreckung nach Maßgabe der Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten oder der Vorschriften über die Zusammenarbeit mit dem Internationalen Strafgerichtshof oder

3. zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit.

Gleiches gilt, wenn Anhaltspunkte dafür vorliegen, daß Straftaten von erheblicher Bedeutung begangen werden sollen.

(2) bis (6) …

(7) Die Verantwortung für die Zulässigkeit der Übermittlung trägt das Bundeskriminalamt. § 10 Abs. 4 Satz 2 gilt entsprechend. Das Bundeskriminalamt hat die Übermittlung und ihren Anlaß aufzuzeichnen. Der Empfänger personenbezogener Daten ist darauf hinzuweisen, daß sie nur zu dem Zweck genutzt werden dürfen, zu dem sie über-

mittelt worden sind. Ferner ist ihm der beim Bundeskriminalamt vorgesehene Löschungszeitpunkt mitzuteilen. Die Übermittlung personenbezogener Daten unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde. Die Übermittlung unterbleibt außerdem, soweit, auch unter Berücksichtigung des besonderen öffentlichen Interesses an der Datenübermittlung, im Einzelfall schutzwürdige Interessen der betroffenen Person an dem Ausschluss der Übermittlung überwiegen. Zu den schutzwürdigen Interessen der betroffenen Person gehört auch das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat. Die schutzwürdigen Interessen der betroffenen Person können auch dadurch gewahrt werden, dass der Empfängerstaat oder die empfangende zwischen- oder überstaatliche Stelle im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

Unterabschnitt 3a Abwehr von Gefahren des internationalen Terrorismus

§ 20a Allgemeine Befugnisse

(1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgabe nach § 4a Abs. 1 Satz 1 die notwendigen Maßnahmen treffen, um eine Gefahr abzuwehren, soweit nicht dieses Gesetz die Befugnisse des Bundeskriminalamtes besonders regelt. Die §§ 15 bis 20 des Bundespolizeigesetzes gelten entsprechend.

(2) Gefahr im Sinne dieses Unterabschnitts ist eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2.

§ 20b Erhebung personenbezogener Daten

(1) Das Bundeskriminalamt kann, sofern in diesem Unterabschnitt nichts anderes bestimmt ist, personenbezogene Daten erheben, soweit dies zur Erfüllung der ihm nach § 4a Abs. 1 obliegenden Aufgabe erforderlich ist.

(2) Zur Verhütung von Straftaten gemäß § 4a Abs. 1 Satz 2 ist eine Erhebung personenbezogener Daten nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass

1. die Person eine Straftat gemäß § 4a Abs. 1 Satz 2 begehen will und die erhobenen Daten zur Verhütung dieser Straftat erforderlich sind oder

2. die Person mit einer Person nach Nummer 1 nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und

   a) von der Vorbereitung einer Straftat gemäß § 4a Abs. 1 Satz 2 Kenntnis hat,

   b) aus der Verwertung der Tat Vorteile ziehen oder

   c) die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte (Kontakt- und Begleitperson) und die Verhütung dieser Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) bis (8) …

§ 20c Befragung und Auskunftspflicht

(1) Das Bundeskriminalamt kann eine Person befragen, wenn Tatsachen die Annahme rechtfertigen, dass die Person sachdienliche Angaben für die Erfüllung der dem Bundeskriminalamt nach § 4a Abs. 1 Satz 1 obliegenden Aufgabe machen kann. Zum Zwecke der Befragung kann die Person angehalten werden. Auf Verlangen hat die Person mitgeführte Ausweispapiere zur Prüfung auszuhändigen.

(2) Die befragte Person ist verpflichtet, Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben, soweit dies zur Erfüllung der dem Bundeskriminalamt nach § 4a Abs. 1 Satz 1 obliegenden Aufgabe erforderlich ist. Eine weitergehende Auskunftspflicht besteht nur für die entsprechend den §§ 17 und 18 des Bundespolizeigesetzes Verantwortlichen und entsprechend den Voraussetzungen des § 20 Abs. 1 des Bundespolizeigesetzes für die dort bezeichneten Personen sowie für die Personen, für die gesetzliche Handlungspflichten bestehen, soweit die Auskunft zur Abwehr einer Gefahr erforderlich ist.

(3) Unter den in den §§ 52 bis 55 der Strafprozessordnung bezeichneten Voraussetzungen ist der Betroffene zur Verweigerung der Auskunft berechtigt. Dies gilt nicht, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person erforderlich ist. Eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozessordnung genannte Person ist auch in den Fällen des Satzes 2 zur Verweigerung der Aus-

kunft berechtigt. Die betroffene Person ist über ihr Recht zur Verweigerung der Auskunft zu belehren. Auskünfte, die gemäß Satz 2 erlangt wurden, dürfen nur für den dort bezeichneten Zweck verwendet werden.

(4) § 136a der Strafprozessordnung gilt entsprechend. § 12 des Verwaltungsvollstreckungsgesetzes findet keine Anwendung.

§ 20g Besondere Mittel der Datenerhebung

(1) Das Bundeskriminalamt kann personenbezogene Daten mit den besonderen Mitteln nach Absatz 2 erheben über

1. den entsprechend § 17 oder § 18 des Bundespolizeigesetzes Verantwortlichen oder entsprechend den Voraussetzungen des § 20 Abs. 1 des Bundespolizeigesetzes über die dort bezeichnete Person zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. die Person, bei der Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 begehen wird, oder

3. eine Kontakt- oder Begleitperson,

wenn die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besondere Mittel der Datenerhebung sind

1. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden soll (längerfristige Observation),

2. der Einsatz technischer Mittel außerhalb von Wohnungen in einer für den Betroffenen nicht erkennbaren Weise

   a) zur Anfertigung von Bildaufnahmen oder -aufzeichnungen von Personen oder Sachen, die sich außerhalb von Wohnungen befinden, oder

b) zum Abhören oder Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes,

3. sonstige besondere für Observationszwecke bestimmte technische Mittel zur Erforschung des Sachverhalts oder zur Bestimmung des Aufenthaltsortes einer in Absatz 1 genannten Person,

4. der Einsatz von Privatpersonen, deren Zusammenarbeit mit dem Bundeskriminalamt Dritten nicht bekannt ist (Vertrauensperson), und

5. der Einsatz eines Polizeivollzugsbeamten unter einer ihm verliehenen und auf Dauer angelegten Legende (Verdeckter Ermittler).

(3) Maßnahmen nach Absatz 2 Nr. 5, die sich gegen eine bestimmte Person richten oder bei denen der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist, dürfen nur auf Antrag der zuständigen Abteilungsleitung oder deren Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzuge kann die Anordnung einer Maßnahme nach Satz 1 durch die Abteilungsleitung nach Satz 1 oder deren Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die übrigen Maßnahmen nach Absatz 2 Nr. 1 bis 5 dürfen, außer bei Gefahr im Verzuge, nur durch die Abteilungsleitung nach Satz 1 oder deren Vertretung angeordnet werden. Die Anordnung ist unter Angabe der maßgeblichen Gründe aktenkundig zu machen und auf höchstens einen Monat zu befristen; im Fall des Absatzes 2 Nr. 4 und 5 ist die Maßnahme auf höchstens zwei Monate zu befristen. Die Verlängerung der Maßnahme bedarf einer neuen Anordnung. Die Entscheidung über die Verlängerung der Maßnahme darf in den Fällen des Absatzes 2 Nr. 1, 2 Buchstabe b, Nr. 4 und 5 nur durch das Gericht getroffen werden. Die Sätze 4 und 5 gelten entsprechend.

(4) …

§ 20h Besondere Bestimmungen über den Einsatz technischer Mittel in oder aus Wohnungen

(1) Das Bundeskriminalamt kann zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen

1. das nichtöffentlich gesprochene Wort einer Person abhören und aufzeichnen,

   a) die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist,

   b) bei der konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 begehen wird, oder

   c) die eine Kontakt- und Begleitperson einer Person nach Buchstabe a oder b ist, und

2. Lichtbilder und Bildaufzeichnungen über diese Person herstellen,

wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) Die Maßnahme darf sich nur gegen die in Absatz 1 genannte Person richten und nur in deren Wohnung durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. sich eine in Absatz 1 Nr. 1 Buchstabe a oder b genannte Person dort aufhält und

2. die Maßnahme in der Wohnung dieser Person allein nicht zur Abwehr der Gefahr nach Absatz 1 führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(3) Maßnahmen nach Absatz 1 dürfen nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden. Bei Gefahr im Verzuge kann die Anordnung auch durch den Präsidenten des Bundeskriminalamtes oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung des Präsidenten des Bundeskriminalamtes oder seines Vertreters nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(4) Die Anordnung ergeht schriftlich. In ihr sind anzugeben

1. der Name und die Anschrift der Person, gegen die sich die Maßnahme richtet, soweit möglich,

2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,

3. Art, Umfang und Dauer der Maßnahme und

4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die in den Absätzen 1 und 5 bezeichneten Voraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(5) Die Maßnahme nach Absatz 1 darf nur angeordnet und durchgeführt werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Beobachten nach Satz 1 ist unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Sind das Abhören und Beobachten nach Satz 2 unterbrochen worden, so darf es unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 20j Rasterfahndung

(1) Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, so-

weit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist; eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll. Von den Verfassungsschutzämtern des Bundes und der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach Satz 1 nicht verlangt werden.

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf andere im Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen vom Bundeskriminalamt nicht verwendet werden.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Die getroffene Maßnahme ist zu dokumentieren. Diese Dokumentation ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten oder der Vernichtung der Akten nach Satz 1 folgt, zu vernichten.

(4) Die Maßnahme darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.

§ 20k Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder

2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung

folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) Die Maßnahme nach Absatz 1 darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,

2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie

4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes). Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der

Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 20l Überwachung der Telekommunikation

(1) Das Bundeskriminalamt kann ohne Wissen des Betroffenen die Telekommunikation einer Person überwachen und aufzeichnen,

1. die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist, und dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, geboten ist,

2. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 vorbereitet,

3. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder

4. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird,

und die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

§ 20k Abs. 2 und 3 gilt entsprechend. § 20k bleibt im Übrigen unberührt.

(3) Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden. Bei Gefahr im Verzuge kann die Anordnung durch den Präsidenten des Bundeskriminalamtes oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit diese Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(4) Die Anordnung ergeht schriftlich. In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes und

4. im Fall des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(5) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), dem Bundeskriminalamt die Maßnahmen nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den Absätzen 1 und 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden,

ist die Maßnahme unzulässig. Soweit im Rahmen von Maßnahmen nach den Absätzen 1 und 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den Absätzen 1 und 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 20m Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten

(1) Das Bundeskriminalamt kann ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1 und § 113a des Telekommunikationsgesetzes) erheben zu

1. den entsprechend § 17 oder § 18 des Bundespolizeigesetzes Verantwortlichen zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 vorbereitet,

3. der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder

4. der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird,

wenn die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) …

(3) § 20l Abs. 3 bis 5 gilt entsprechend mit der Maßgabe, dass an die Stelle des Präsidenten des Bundeskriminalamtes oder seines Vertreters die zuständige Abteilungsleitung oder deren Vertretung tritt. Abweichend von § 20l Abs. 4 Nr. 2 genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

§ 20u Schutz zeugnisverweigerungsberechtigter Personen

(1) Maßnahmen nach diesem Unterabschnitt, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozessordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. § 20c Abs. 3 bleibt unberührt. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozessordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.

(2) Soweit durch eine Maßnahme eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5 der Strafprozessordnung genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken.

(3) Die Absätze 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozessordnung Genannten das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 gelten nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.

§ 20v Gerichtliche Zuständigkeit, Kennzeichnung, Verwendung und Löschung

(1) bis (2) …

(3) Die durch Maßnahmen nach den §§ 20g bis 20n erhobenen personenbezogenen Daten sind zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(4) Eine Maßnahme nach diesem Unterabschnitt ist unzulässig, soweit besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen. Das Bundeskriminalamt darf die nach diesem Unterabschnitt erhobenen personenbezogenen Daten verwenden,

1. um seine Aufgabe nach § 4a Abs. 1 Satz 1 wahrzunehmen oder

2. soweit dies zur Wahrnehmung seiner Aufgaben nach den §§ 5 und 6 erforderlich ist.

(5) Das Bundeskriminalamt kann die nach diesem Unterabschnitt erhobenen personenbezogenen Daten an andere Polizeien des Bundes und der Länder sowie an sonstige öffentliche Stellen übermitteln, soweit dies erforderlich ist

1. zur Herbeiführung des gegenseitigen Benehmens nach § 4a Abs. 2 Satz 3,

2. zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit oder zur Verhütung von Straftaten, die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet sind, im Fall einer Maßnahme nach den §§ 20h, 20k oder § 20l nur zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, oder

3. zur Verfolgung von Straftaten, wenn ein Auskunftsverlangen nach der Strafprozessordung zulässig wäre. Daten, die nach den §§ 20h, 20k oder § 20l erhoben worden sind, dürfen nur zur Verfolgung von Straftaten übermittelt werden, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind.

In Fällen des Satzes 1 Nr. 2 ist § 20a Abs. 2 insoweit nicht anzuwenden, als die Gefahr im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2 stehen muss. Die vom Bundeskriminalamt nach diesem Unterabschnitt erlangten personenbezogenen Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder

2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

Die vom Bundeskriminalamt nach diesem Unterabschnitt erlangten personenbezogenen Daten dürfen an den Bundesnachrichtendienst übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass diese Daten für die Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Abs. 2 des BND-Gesetzes zur Sammlung von Informationen über die in § 5 Abs. 1 Satz 3 Nr. 1 bis 3 des Artikel 10-Gesetzes genannten Gefahrbereiche erforderlich sind. Nach § 20h erhobene Daten dürfen nur übermittelt werden, um bei dem Bundesamt für Verfassungsschutz, den Verfassungsschutzbehörden der Länder, dem Bundesnachrichtendienst oder dem Militärischen Abschirmdienst Auskünfte einzuholen, die für die Erfüllung der Aufgabe des Bundeskriminalamtes nach § 4a Abs. 1 Satz 1 erforderlich sind. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(6) Sind die durch eine Maßnahme nach diesem Unterabschnitt erlangten personenbezogenen Daten zur Erfüllung des der Maßnahme zugrunde liegenden Zwecks und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, sind sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Die Akten sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten folgt, zu löschen. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist, dürfen die Daten ohne Einwilligung der Betroffenen nur zu diesem Zweck verwendet werden; sie sind entsprechend zu sperren. Eine Löschung unterbleibt, soweit die Daten zur Verfolgung von Straftaten oder nach Maßgabe des § 8 zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich sind.

§ 20w Benachrichtigung

(1) Über eine Maßnahme nach den §§ 20g bis 20n sind zu benachrichtigen im Fall

1. des § 20g Abs. 2 Nr. 1 bis 3 (längerfristige Observation, Bildaufnahmen, technische Observationsmittel) die Zielperson sowie die erheblich mitbetroffenen Personen,

2. des § 20g Abs. 2 Nr. 4 und 5 (Einsatz Vertrauensperson und Verdeckter Ermittler)

   a) die Zielperson,

   b) die erheblich mitbetroffenen Personen,

   c) die Personen, deren nicht allgemein zugängliche Wohnung die Vertrauensperson oder der Verdeckte Ermittler betreten hat,

3. des § 20h (Wohnraumüberwachung)

   a) die Person, gegen die sich die Maßnahme richtete,

   b) sonstige überwachte Personen,

   c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,

4. des § 20i (Ausschreibung) die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind,

5. des § 20j (Rasterfahndung) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,

6. des § 20k (Verdeckter Eingriff in informationstechnische Systeme) die Zielperson sowie die mitbetroffenen Personen,

7. des § 20l (Telekommunikationsüberwachung) die Beteiligten der überwachten Telekommunikation,

8. des § 20m Abs. 1 (Erhebung von Verkehrsdaten) die Beteiligten der betroffenen Telekommunikation,

9. des § 20m Abs. 2 (Erhebung von Nutzungsdaten) der Nutzer,

10. des § 20n (IMSI-Catcher) die Zielperson.

Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nr. 6, 7 und 8 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Fall des § 20g Abs. 2 Nr. 4 und 5 auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers oder der Vertrauensperson möglich ist. Wird wegen des zugrunde liegenden Sachverhaltes ein strafrechtliches Ermittlungsverfahren geführt, erfolgt die Benachrichtigung durch die Strafverfolgungsbehörde entsprechend den Vorschriften des Strafverfahrensrechts. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren.

(3) Erfolgt die nach Absatz 2 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der gerichtlichen Zustimmung. Im Fall der §§ 20h und 20k beträgt die Frist sechs Monate. Das Gericht bestimmt die Dauer der weiteren Zurückstellung, im Fall der §§ 20h und 20k jedoch nicht länger als sechs Monate. Verlängerungen der Zurückstellungsdauer sind zulässig. Fünf Jahre nach Beendigung der Maßnahme kann mit gerichtlicher Zustimmung endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme.

III.

Die Beschwerdeführer im Verfahren 1 BvR 966/09 sind Rechtsanwälte, Journalisten, ein Arzt und ein Diplom-Psychologe, von denen die meisten in der Menschenrechtspolitik aktiv sind. Die Beschwerdeführer und Beschwerdeführerinnen im Verfahren 1 BvR 1140/09 sind - als Privatpersonen auftretende - ehemalige 5

und gegenwärtige Abgeordnete des Deutschen Bundestags, die sich weithin gleichfalls in der Menschenrechtspolitik engagieren und teilweise auch als Rechtsanwalt oder Arzt tätig sind. Sie rügen der Sache nach die Verletzung von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 5 Abs. 1 Satz 2, Art. 10, Art. 12, Art. 13, zum Teil auch in Verbindung mit Art. 1 Abs. 1, Art. 19 Abs. 4 und Art. 20 Abs. 3 GG.

1. Die Verfassungsbeschwerden seien zulässig. 6

Die Beschwerdeführer und Beschwerdeführerinnen seien von den angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen. Sie gerieten, wie sie im Einzelnen darlegen, beruflich, als Abgeordnete oder privat wiederholt in Kontakt zu Personen, die extremistischen und terroristischen Organisationen zugerechnet würden oder Ziel staatlicher Überwachung im Rahmen der Terrorismusbekämpfung seien. Hinzu kämen Kontakte zu regierungsnahen und parlamentarischen Gesprächspartnern, zu Menschenrechtsaktivisten sowie zu - auch militanten - Separatisten und Oppositionellen aus dem Ausland, insbesondere auch aus Krisen- und Bürgerkriegsregionen. Es sei daher nicht fernliegend, im Rahmen dieser Kontakte Ziel oder Drittbetroffener einer der angegriffenen Maßnahmen zu werden. § 20u Abs. 1 BKAG in Verbindung mit § 53 Abs. 1 Satz 1 Nr. 4 StPO schütze nur in einem Teilbereich der vorgenannten Aktivitäten vor Überwachungsmaßnahmen des Bundeskriminalamts. Angesichts der Streubreite der Vorschriften, der Geheimhaltung des Vollzugs des Gesetzes und einer nur unzureichenden Pflicht zur Benachrichtigung des von einer Überwachungsmaßnahme Betroffenen reiche dies aus, um ihre Beschwerdebefugnis zu begründen. 7

Die Beschwerdefrist des § 93 Abs. 3 BVerfGG sei beachtet. Dies gelte auch für den schon früher und nicht erst im letzten Jahr in das Gesetz eingefügten § 14 BKAG. Die hier geregelte Übermittlung von Daten an das Ausland erhalte durch die neuen Befugnisse des Bundeskriminalamts zur Datenerhebung einen neuen Anwendungs- und Regelungsgehalt. Dies führe dazu, dass die Beschwerdefrist des § 93 Abs. 3 BVerfGG neu in Gang gesetzt werde. 8

2. Die Verfassungsbeschwerden seien begründet. 9

a) Die parallele Aufgabenwahrnehmung von Landespolizeibehörden und Bundeskriminalamt nach § 4a Abs. 2 BKAG sowie die Einräumung eines Ermessensspielraumes des Bundeskriminalamts bei der Wahrnehmung seiner Aufgaben nach § 4a Abs. 1 BKAG seien nicht mit der verfassungsrechtlichen Kompetenzord- 10

nung nach Art. 73 Abs. 1 Nr. 9a GG vereinbar. Art. 73 Abs. 1 Nr. 9a GG gebe dem Bund auch nicht die Kompetenz für Regelungen zur Verhütung von Straftaten, die im Vorfeld der Abwehr konkreter Gefahren ansetze. § 20g Abs. 1 Satz 1 Nr. 2 und 3, § 20l Abs. 1 Satz 1 Nr. 2 BKAG seien daher schon formell verfassungswidrig.

b) Der für die Aufgabenbestimmung des Bundeskriminalamts verwendete Begriff des „internationalen Terrorismus“ sei mehrdeutig und verstoße gegen den Grundsatz der Normenklarheit. Gleiches gelte für den in § 20a Abs. 2 BKAG normierten Gefahrenbegriff mit seiner Bezugnahme auf § 4a Abs. 1 Satz 2 BKAG. Auch das in § 20g Abs. 1, § 20h Abs. 1, § 20j Abs. 1, § 20l Abs. 1, § 20m Abs. 1 und § 20w Abs. 2 BKAG festgelegte Schutzgut der „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“, sei mangels Bestimmtheit verfassungswidrig. 11

c) § 20c Abs. 3 BKAG verletze - ebenso wie § 20u Abs. 2 BKAG - Art. 1 Abs. 1, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 5 Abs. 1 Satz 2 und Art. 12 Abs. 1 GG. 12

d) Die in § 20g Abs. 1 Satz 1 Nr. 2 BKAG bezüglich der besonderen Mittel der Datenerhebung normierte Befugnis zur Straftatenverhütung sei ferner mit dem Gebot der Normenklarheit nicht vereinbar. Die geringen tatbestandlichen Voraussetzungen wahrten nicht das Gebot der Verhältnismäßigkeit. Die Regelung überlasse der Verwaltung, wo die Grenze zu ziehen sei zwischen unverdächtigem und solchem Verhalten, das erwarten lässt, dass jemand eine Straftat begehen wird. Auch der Begriff der „Kontakt- und Begleitperson“ in § 20g Abs. 1 Satz 1 Nr. 3 BKAG sei zu unbestimmt. 13

§ 20g Abs. 1, 2 BKAG verstoße gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, soweit die Beschwerdeführer in ihren Berufen betroffen seien gegen Art. 12 GG und, soweit sie in ihren Wohn- und Kanzleiräumen betroffen seien, gegen Art. 13 Abs. 1 GG. Die Norm ermögliche die Erstellung eines weitreichenden Profils der überwachten Person und den Zugriff auf nicht für die Öffentlichkeit bestimmte Kommunikation, auch durch systematische Täuschung durch Vertrauenspersonen und den Einsatz Verdeckter Ermittler. Durch die Möglichkeit der Inanspruchnahme von Nichtstörern und eine Datenerhebung zur Verhütung von Straftaten werde der Grundrechtseingriff trotz niedriger Eingriffsschwelle noch vertieft. 14

In § 20g Abs. 3 BKAG sei für besondere Mittel der Datenerhebung in verfassungswidriger Weise teilweise kein Richtervorbehalt vorgesehen. Zudem habe der 15

Gesetzgeber die besondere Gefahr additiver Grundrechtseingriffe nicht berücksichtigt, weil neben dem Bundeskriminalamt auch Landespolizeibehörden tätig bleiben könnten.

e) Der Einsatz technischer Mittel in Wohnungen gemäß § 20h BKAG sei insbesondere mit Art. 13 Abs. 1, 4 GG unvereinbar. Der Begriff der „Sachen von bedeutendem Wert“ in § 20h Abs. 1 BKAG erfülle nicht die Anforderungen der „gemeinen Gefahr“ des Art. 13 Abs. 4 GG. Inkonsistent sei, dass in die Unverletzlichkeit der Wohnung anders als bei dem Zugriff auf informationstechnische Systeme schon zum bloßen Schutz von Sachwerten eingegriffen werden dürfe. Die in § 20h BKAG verwandte Formel einer „dringenden“ Gefahr für die Gesundheit Dritter sei unbestimmt. Verfassungswidrig sei die Erlaubnis von Maßnahmen gegen Zustandsstörer, Begleit- und Kontaktpersonen sowie von Vorfeldermittlungen gemäß § 20h Abs. 1 Nr. 1 b BKAG. Der Kreis möglicher Adressaten werde angesichts der nur schwer nachvollziehbaren Verweisungskette nicht hinreichend bestimmt und in der Sache übermäßig ausgeweitet. § 20h Abs. 1 Nr. 2 BKAG sei unverhältnismäßig. Die optische Wohnraumüberwachung dürfe allenfalls unter erheblich höheren Eingriffsvoraussetzungen als die akustische Wohnraumüberwachung oder subsidiär zu dieser eingesetzt werden. 16

§ 20h Abs. 2 BKAG verstoße gegen den Verhältnismäßigkeitsgrundsatz, denn die Regelung erlaube bereits eine Überwachung der Wohnung von Unbeteiligten, wenn sich dort eine Person, die eine Gefahr verursache oder eine Straftat im Sinne des § 4a Abs. 1 Satz 2 BKAG vorbereite, aufhalte. 17

§ 20h Abs. 4 BKAG verletze Art. 13 Abs. 1 in Verbindung mit Art. 19 Abs. 4 GG, da für die Anordnung der Wohnraumüberwachung nur die Angabe der wesentlichen Gründe verlangt werde und eine richterliche Verlaufskontrolle fehle. 18

f) Die Regelung zur Rasterfahndung nach § 20j BKAG verstoße gegen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Sie sei unverhältnismäßig, soweit eine „Gefahr“ bereits dann vorliegen solle, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 BKAG begangen werden solle. Eine Rasterfahndung käme nur in Betracht, wenn eine hinreichend konkrete Gefahr für hochrangige Rechtsgüter vorliege und diese tatsachengestützt sei. 19

g) Die Regelung zum Zugriff auf informationstechnische Systeme in § 20k BKAG verstoße gegen Art. 13 Abs. 1 GG, weil nicht ausgeschlossen sei, dass die 20

Infiltration eines informationstechnischen Systems durch Betreten der Wohnung erfolgen könne.

§ 20k Abs. 1 Satz 1 BKAG lasse eine Ausforschung der Persönlichkeit des Betroffenen zu. Die Tiefe des Eingriffs im konkreten Fall sei abhängig vom Stand der Technik und damit entwicklungsoffen. § 20k Abs. 1 Satz 1 BKAG beschränke sich nicht auf den Schutz überragend wichtiger Rechtsgüter. 21

Nicht hinnehmbar sei, dass § 20k Abs. 4 Satz 1 BKAG den Zugriff auf informationstechnische Systeme von Zustandsstörern erlaube. Dies werde dem personalisierten Gefahrbegriff für heimliche Überwachungsmaßnahmen nicht gerecht. Unverhältnismäßig lang sei die mögliche Dauer der Anordnung von bis zu drei Monaten nach § 20k Abs. 6 Satz 3 BKAG. 22

h) Die Telekommunikationsüberwachung nach § 20l Abs. 1 Satz 1 Nr. 2 BKAG sei mit dem Bestimmtheitsgebot nicht vereinbar, weil der Gesetzgeber nicht konkretisiere, wann jemand eine Straftat im Sinne des § 4a Abs. 1 Satz 2 BKAG vorbereite. § 20l Abs. 1 Satz 2 BKAG genüge dem verfassungsrechtlich gebotenen Schutz beruflich genutzter Anschlüsse von Arztpraxen und Rechtsanwaltskanzleien nicht. 23

Unverhältnismäßig sei die Quellen-Telekommunikationsüberwachung nach § 20l Abs. 2 BKAG. Es sei nicht möglich, auf einen Rechner zuzugreifen und hierbei lediglich laufende Telekommunikationsvorgänge abzuhören. Eine Überwachungssoftware, die auch andere Informationen erfasse, sei aber als Online-Durchsuchung zu werten. Ob gleichwohl Maßnahmen der Quellen-Telekommunikationsüberwachung stattfänden, sei aufgrund der Heimlichkeit der Maßnahme nicht überprüfbar. 24

i) Die Erhebung von Telekommunikationsverkehrsdaten nach § 20m BKAG greife unverhältnismäßig in Art. 10 Abs. 1 GG und bezüglich der als Rechtsanwalt und Arzt tätigen Beschwerdeführer in Art. 12 Abs. 1 GG ein. Sie ermögliche die Erstellung von Kontaktprofilen, Bewegungsbildern und die Standortüberwachung in Echtzeit. Die Streubreite und die Anknüpfung an ein nur vage bestimmtes Vorbereitungsstadium (§ 20m Abs. 1 Nr. 2 BKAG) erhöhten das Eingriffsgewicht. Bedenklich sei gerade in Bezug auf Berufsgeheimnisträger, dass § 20m Abs. 1 Nr. 2 bis 4 BKAG auch Nichtstörer als Zielpersonen erfasse und schon ein nur mittelbarer Bezug zu einer Gefahr ausreiche. 25

j) Die angegriffenen Vorschriften würden den verfassungsrechtlichen Anforderungen an Transparenz und effektiven Rechtsschutz nicht gerecht. Die Benachrichtigungspflichten seien unzureichend geregelt. § 20w Abs. 1 Satz 3 BKAG lege es mit offenen Kriterien weitgehend in die Hand der Ermittlungsbehörde, auf eine Benachrichtigung der Betroffenen zu verzichten; eine gerichtliche Überprüfung finde nicht statt. Die Zurückstellung der Benachrichtigung zum Schutz von Sachen gemäß § 20w Abs. 2 Satz 1 BKAG und zur Sicherung der weiteren Verwendung von Verdeckten Ermittlern oder Vertrauenspersonen verletze die Beschwerdeführer in ihrem verfassungsrechtlichen Recht auf Benachrichtigung zur Erlangung von Rechtsschutz. Der Verweis auf die Benachrichtigungsregelungen der Strafprozessordnung in § 20w Abs. 2 Satz 2 BKAG sei unzureichend, da das Strafverfahrensrecht selbst Lücken bei der Benachrichtigung des Betroffenen aufweise. Zudem werde damit der für eine Zurückhaltung der Benachrichtigung tragende Bezugspunkt in verfassungsrechtlich bedenklicher Weise ausgewechselt. Statt der Gefährdung des Zwecks der Überwachungsmaßnahme werde auf die Gefährdung eines strafverfahrensrechtlichen Untersuchungszwecks abgestellt. § 20w Abs. 3 Satz 5 BKAG sei mit den Anforderungen an einen effektiven Rechtsschutz nicht vereinbar, da bereits nach fünf Jahren von der Benachrichtigung des Betroffenen endgültig abgesehen werden könne. 26

k) Es fehle an ausreichenden gesetzlichen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung. 27

Vollständig fehlten solche Regelungen für die Überwachung außerhalb von Wohnungen nach § 20g BKAG. Sie seien aber jedenfalls für die längerfristige Observation und für die Überwachung mittels akustischer und optischer Mittel geboten. Auch außerhalb von Wohnungen könne der Kernbereich privater Lebensgestaltung berührt sein, etwa wenn sich die Zielperson außerhalb der Wohnung mit Familienangehörigen oder anderen Vertrauten bespreche. 28

§ 20h Abs. 5 Satz 1 BKAG beschränke den Schutz des Kernbereichs privater Lebensgestaltung auf „Äußerungen“, obgleich auch durch die optische Wohnraumüberwachung kernbereichsrelevante Verhaltensweisen erfasst werden könnten. § 20h Abs. 5 Satz 3 BKAG sei unzureichend, da bei Zweifeln über die Kernbereichsrelevanz der Beobachtungen eine automatische Aufzeichnung erlaubt sei. Ferner beschränke § 20h Abs. 5 Satz 4 BKAG in unzulässiger Weise die gerichtliche Durchsicht der erhobenen Daten auf diese Fallkonstellation. Für den Fall des „Live“-Mithörens helfe das Gebot der Löschung kernbereichsrelevanter Daten nach § 20h Abs. 5 Satz 6 und 7 BKAG nicht. § 20h Abs. 5 Satz 9 und 10 BKAG 29

(ebenso wie § 20k Abs. 7 Satz 8 und in § 20l Abs. 6 Satz 10 BKAG) verletzten die Garantie eines effektiven Rechtsschutzes, da die zu dokumentierende Erfassung und Löschung spätestens zum Ende des nächsten Jahres und damit möglicherweise noch vor einer Benachrichtigung des Betroffenen zu löschen seien.

Der verdeckte Zugriff auf informationstechnische Systeme sei nach § 20k Abs. 7 Satz 1 BKAG nur dann unzulässig, wenn durch ihn „allein“ Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst würden. Danach wäre der Zugriff auf ein informationstechnisches System schon zulässig, wenn sich darauf nur irgendwelche Daten befinden würden, die nicht dem Kernbereich privater Lebensgestaltung zuzurechnen wären. Da die Verarbeitung ausschließlich kernbereichsrelevanter Informationen auf einem informationstechnischen System auszuschließen sei, laufe die Vorschrift leer. Entsprechendes gelte für die Überwachung der Telekommunikation nach § 20l Abs. 6 Satz 1 BKAG. Demgegenüber sei es geboten, mittels einer fundierten Prognoseentscheidung zu vermeiden, dass überhaupt kernbereichsrelevante Daten erfasst würden. § 20k Abs. 7 Satz 3, 4 BKAG werde der gebotenen Durchsicht der erhobenen Daten durch eine unabhängige Stelle nicht gerecht; als eine solche komme grundsätzlich nur ein Gericht in Frage. An der Sichtung nach § 20k Abs. 7 Satz 3, 4 BKAG würden aber im Wesentlichen Personen des Bundeskriminalamts beteiligt. Was unter der vorgesehenen „Sachleitung“ des anordnenden Gerichts zu verstehen sei, bleibe unklar; sie sichere die Unabhängigkeit der Sichtung nicht. 30

l) Der Schutz von Berufsgeheimnisträgern sei im Bundeskriminalamtgesetz nur unzureichend ausgestaltet. 31

§ 20u Abs. 1 BKAG verstoße gegen Art. 1 Abs. 1 und Art. 3 Abs. 1 GG. Er schütze die in § 53 Abs. 1 Satz 1 Nr. 1, 2 und 4 StPO genannten Berufsgeheimnisträger - Geistliche, Abgeordnete und Verteidiger - nur insoweit, als sich die Maßnahme gegen sie selbst richte. Da sich eine Maßnahme aber in der Regel gegen einen Verdächtigen richten werde, laufe der Schutz des § 20u Abs. 1 BKAG weitgehend leer. Das Verwertungsverbot des § 20u Abs. 1 Satz 6 BKAG begründe einen nur unzureichenden Schutz. 32

§ 20u Abs. 2 BKAG verstoße gegen Art. 1 Abs. 1, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 5 Abs. 1 und Art. 12 Abs. 1 GG sowie gegen das Rechtsstaatsprinzip, bei einer Überwachung von Kanzleiräumen auch gegen Art. 13 Abs. 1 GG. 33

Ärzte, Psychotherapeuten, Journalisten oder nicht als Verteidiger tätige Anwälte seien weniger weitreichend vor Überwachungsmaßnahmen geschützt als Geistliche, Verteidiger oder Abgeordnete, ohne dass dies zu rechtfertigen sei. Die Unterscheidung zwischen Rechtsanwälten und Verteidigern sei willkürlich und ein geringerer Schutzbedarf von nicht-strafrechtlichen Mandatsbeziehungen nicht ersichtlich. Das Berufsgeheimnis der Anwälte werde durch die Möglichkeit entsprechender Überwachungsmaßnahmen grundsätzlich in Frage gestellt, womit auch Art. 12 Abs. 1 GG verletzt werde. Gleiches gelte für das ärztliche Berufsgeheimnis, das in seinem Wesenskern getroffen werde. Auch die durch Art. 5 Abs. 1 Satz 2 GG gewährleisteten Funktionsvoraussetzungen der freien Presse schütze § 20u Abs. 2 BKAG nicht ausreichend. Im Übrigen sei der bloße Verweis auf eine Abwägung zu unbestimmt. 34

m) Verfassungswidrig sei das Gesetz auch, weil es auf gebotene verfahrensrechtliche Sicherungen und materiell-eingriffsrechtliche Abstufungen verzichte, um eine von Verfassungs wegen verbotene Rundumüberwachung durch die kumulative Anwendung eingriffsintensiver Maßnahmen zu verhindern. 35

n) Die Vorschriften zur weiteren Nutzung einmal erhobener Daten durch das Bundeskriminalamt selbst und zu ihrer Weiterleitung an sonstige innerstaatliche Behörden seien verfassungswidrig. 36

§ 20v Abs. 4 Satz 2 BKAG erlaube eine Nutzung der Daten unter gegenüber den Erhebungsvoraussetzungen abgesenkten Anforderungen und unabhängig von einer konkreten Bedrohung von Schutzgütern und emanzipiere sich als Aufgabennorm von konkreten Gefahren im polizeirechtlichen Sinne. Das unterlaufe den Grundsatz der Zweckbindung, wonach Daten nur zu dem Zweck verarbeitet werden dürften, zu dem sie erhoben worden seien. Auch die nach § 20v Abs. 4 Satz 2 Nr. 2 BKAG mögliche Nutzung der vom Bundeskriminalamt erhobenen Daten zur Wahrung der Aufgaben nach §§ 5 und 6 BKAG reiche weit in das Vorfeld von Rechtsgutverletzungen und entspreche nicht dem Gewicht der Rechtsgüter, die die Datenerhebung erfordere. 37

Auch § 20v Abs. 5 Satz 1 Nr. 1 bis 3, Satz 4, 5 BKAG erlaube die Datennutzung unter abgesenkten Anforderungen. § 20v Abs. 5 Satz 1 BKAG sei nicht bestimmt genug, weil die Behörden nicht benannt würden, an die Informationen übermittelt werden dürften. § 20v Abs. 5 Satz 1 Nr. 3 BKAG verstoße gegen Art. 13 GG sowie gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Nur im Fall des Art. 13 Abs. 4 GG 38

sei eine Verwendung von Erkenntnissen erlaubt, die mittels eines Spähangriffs erlangt worden seien, nicht aber zum Zwecke der Strafverfolgung.

Auch § 20v Abs. 6 Satz 5 BKAG mit seinem Verweis auf die Nutzung von Daten zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung nach Maßgabe des § 8 BKAG werde dem Grundsatz nicht gerecht, dass die sekundäre Verwendung von Daten sich nach den Voraussetzungen ihrer Erhebung richten müsse. 39

o) § 14 Abs. 1 BKAG sei nicht mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie mit Art. 10 Abs. 1 und Art. 13 Abs. 1 GG vereinbar. Es dürften Daten - insbesondere aus der Wohnraumüberwachung und aus einem Zugriff auf informationstechnische Systeme - an ausländische Behörden unter Voraussetzungen übermittelt werden, die für ihre Erhebung unzureichend wären. 40

IV.

Zu den Verfassungsbeschwerden haben die Bundesregierung, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, mittels einer gemeinsamen Stellungnahme die Datenschutzbeauftragten der Länder, das Bundesverwaltungsgericht und der Bundesgerichtshof Stellung genommen. 41

1. Die Bundesregierung hält die Verfassungsbeschwerden teils für unzulässig, jedenfalls aber für unbegründet. 42

a) Die Rüge des § 20c Abs. 3 BKAG sei mangels Beschwer unzulässig. Die Norm regle eine offene Ermittlungsmaßnahme von begrenzter Streubreite, gegen die die Beschwerdeführer nicht die erforderliche eigene, unmittelbare und gegenwärtige Beschwer geltend gemacht hätten. Unzulässig sei auch die Rüge des § 14 Abs. 1 BKAG, der bereits vor Inkrafttreten des beschwerdegegenständlichen Gesetzes Teil des Bundeskriminalamtgesetzes gewesen sei, so dass die Beschwerdefrist des § 93 Abs. 3 BVerfGG nicht eingehalten sei. 43

b) Im Übrigen seien die Verfassungsbeschwerden zulässig, aber unbegründet. 44

aa) Der Bundesgesetzgeber verfüge gemäß Art. 73 Abs. 1 Nr. 9a GG über die Kompetenz, dem Bundeskriminalamt die Abwehr von Gefahren und auch die im angegriffenen Gesetz vorgesehenen Maßnahmen der Gefahrenverhütung zuzu- 45

weisen. Da es bei der Straftatenverhütung um Sachverhalte gehe, in denen eine Straftat noch nicht begangen worden sei, handele es sich bei ihr um eine besondere Form der Gefahrenabwehr, die bereits vor der Schwelle einer konkreten Gefahr greife.

bb) Die im Gesetz vorgesehenen Eingriffsbefugnisse dienten dem Schutz verfassungsrechtlich geschützter Rechtsgüter von besonderem Gewicht und entsprächen damit dem Verhältnismäßigkeitsprinzip im engeren Sinne. Die angegriffenen Normen seien hinreichend bestimmt. Die qualifizierten Eingriffsbefugnisse gingen dabei von einem ähnlichen materiellen Standard aus. 46

Zum einen sehe das Gesetz Befugnisse zur Gefahrenabwehr vor. § 20a Abs. 2 BKAG stelle klar, dass der in den Befugnisnormen verwendete Gefahrenbegriff eine konkrete Gefahr bezeichne. § 20h Abs. 1 und § 20l Abs. 1 Satz 1 Nr. 1 BKAG verlangten das qualifizierte Erfordernis einer dringenden Gefahr. Überdies müssten sich alle angegriffenen Ermittlungsbefugnisse nach § 4a Abs. 1 Satz 2 BKAG auf bestimmte, als Tatbestand einzeln aufgeführte Straftaten beziehen, die in § 129a Abs. 1 und 2 StGB bezeichnet seien. Das Erfordernis eines Bezugs zum „internationalen Terrorismus“ bei der Abwehr konkreter Gefahren in § 4a Abs. 1 Satz 1 BKAG bestimme und qualifiziere die Befugnisse darüber hinaus. Der Begriff des „internationalen Terrorismus“ als solcher diene aber nicht als Grundlage einer Eingriffsbefugnis. 47

Neben die Befugnisse zur Abwehr konkreter Gefahren träten Befugnisse zur Straftatenverhütung gemäß § 4a Abs. 1 Satz 2 BKAG. Auch diese blieben hinreichend begrenzt. Die insoweit in Bezug genommenen Straftatbestände nach § 129a StGB beträfen allesamt qualifizierte Rechtsgüter; die Straftaten müssten terroristischen Zielen dienen und eine qualifizierte Schadensneigung aufweisen. Alle in Frage stehenden Befugnisnormen, die sich auf die Aufgabenbestimmung des § 4a Abs. 1 Satz 2 BKAG bezögen, verlangten darüber hinaus das Vorliegen von „Tatsachen“ oder „konkreten Vorbereitungshandlungen“, durch die die Vorbereitung einer Straftat objektiv erkennbar werde. Das Eingreifen im Rahmen der Straftatenverhütung werde hiermit in den Bereich einer individualisierten Gefahrenprognose gebracht. „Tatsachen“ im Sinne des Gesetzes seien Sachverhalte, die sich auf das individualisierte Verhalten bestimmter Personen bezögen. 48

Die Befugnis zur Abwehr konkreter Gefahren für „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“, entspreche den verfassungsrechtlichen Anforderungen. Die doppelte Qualifikation in Bezug auf den 49

Wert der Sache und ihre Bedeutung für das öffentliche Interesse stelle klar, dass hieran anknüpfende Überwachungsmaßnahmen nur in besonders gelagerten Fällen zulässig seien, in denen am Erhalt der zu schützenden Sachwerte ihrerseits rechtlich geschützte Einrichtungen hingen, die über den Wert der Sache selbst in beträchtlichem Umfang hinausgingen.

cc) Die Datenerhebung gemäß § 20g BKAG stünde unter einem strengen Erforderlichkeitsvorbehalt und setze eine konkrete Gefahr für qualifizierte Rechtsgüter voraus. Die durch § 20g Abs. 2 BKAG aufgrund einer behördlichen Anordnung ermöglichten Maßnahmen berührten allesamt weder einen geschriebenen grundsätzlichen Richtervorbehalt noch griffen sie so intensiv in die Sphäre der Betroffenen ein, dass sie einen ungeschriebenen Richtervorbehalt auslösen könnten. Zur Ermittlung eingesetzte Personen dürften nach § 20g Abs. 3 Satz 1 BKAG die Wohnung des Betroffenen nur auf richterliche Anordnung betreten. 50

dd) Die Wohnraumüberwachung gemäß § 20h BKAG stehe ebenfalls unter einem Erforderlichkeitsvorbehalt und werde dem in Art. 13 Abs. 4 GG normierten Erfordernis gerecht, Grundrechtseingriffe nur bei einer „dringenden“ Gefahr zuzulassen. Der Grundrechtseingriff werde durch eine auch mögliche optische Wohnraumüberwachung nicht vertieft, der Grundrechtsschutz des Art. 13 GG sei medienübergreifend. Eine permanente richterliche Verlaufskontrolle der Wohnraumüberwachung sei verfassungsrechtlich nicht geboten. 51

ee) Die Rasterfahndung nach § 20j BKAG sei ein zur Gefahrenabwehr geeignetes Instrument, weil sie den Zweck erfülle, in einer Gefahrensituation weitere Ermittlungsansätze zu gewinnen. Aus der Rechtsprechung des Bundesverfassungsgerichts lasse sich herleiten, dass der Gesetzgeber unter den Bedingungen bestimmter Tatbestandsvoraussetzungen nicht in jedem Fall am Erfordernis des konkreten Gefahrenmaßstabs festhalten müsse. Vor diesem Hintergrund erscheine die Regelung des § 20j Abs. 1 Satz 1, 2. Halbsatz BKAG verfassungsrechtlich unbedenklich. 52

ff) Die in § 20k Abs. 6 Satz 2 Nr. 4 BKAG normierte Nennung der „wesentlichen Gründe“ für die Anordnung einer Überwachungsmaßnahme entspreche den verfassungsrechtlichen Vorgaben. Wenn das Bundesverfassungsgericht in seiner Rechtsprechung die Fachgerichte auf bestimmte Inhalte einer angemessenen Entscheidungsbegründung verpflichte, folge daraus nicht, dass der Gesetzgeber diese auch in gleicher Präzision zum Gegenstand der gesetzlichen Regelung machen müsse. 53

gg) Die Telekommunikationsüberwachung gemäß § 20l BKAG halte die Grenzen der materiellen Angemessenheit ein. Soweit es um die Befugnis nach § 20l Abs. 1 Satz 1 Nr. 2 BKAG zur Straftatenverhütung gehe, verweise die Norm auf mehrfach qualifizierte, tatbestandlich aufgezählte Straftaten, nicht einfach nur auf eine bestimmte Gruppe von Straftaten. Die zu schützenden Rechtsgüter würden benannt. 54

Die ermittelnde Behörde sei in der Lage, den Zugriff nach § 20l Abs. 2 BKAG auf Daten der laufenden Kommunikation zu beschränken. Die Überwachung der Telekommunikation dürfe daher nicht mit einem Eingriff in informationstechnische Systeme gleichgesetzt werden. 55

hh) Die Abfragebefugnis zur Abwehr konkreter Gefahren in § 20m Abs. 1 Nr. 1 BKAG entspreche den verfassungsrechtlichen Vorgaben. Gleiches gelte für die Abfragebefugnis im Rahmen der Straftatenverhütung, die das Vorliegen „bestimmter Tatsachen“ zur Vorbereitung einer Straftat verlange. 56

ii) Hinsichtlich der Adressaten der Ermittlungsmaßnahmen sei zu beachten, dass eine Zurechnung im Bereich des Gefahrenabwehrrechts allein nach der Frage der Verursachung einer Gefahr, nicht aber nach dem Schuldprinzip erfolge. Ein Nichtstörer dürfe nur unter erhöhten Anforderungen und in speziellen Ausnahmekonstellationen in Anspruch genommen werden. Dies lasse sich beispielsweise für die Inanspruchnahme von in § 20b Abs. 2 BKAG näher definierten Kontakt- und Begleitpersonen nach § 20h Abs. 1 Nr. 1 c BKAG zeigen. Es kämen danach nur diejenigen als Adressaten einer Überwachungsmaßnahme in Betracht, die einen spezifisch tatbezogenen Kontakt mit einem Störer oder Nichtstörer im Sinne des Gesetzes gehabt hätten, nicht aber jedermann, der mit diesen Personen kommuniziere. Dies sei auch bei einer Wohnraumüberwachung zulässig. 57

jj) § 20w BKAG richte ein differenziertes Benachrichtigungsregime für die Ermittlungsbefugnisse ein, das dem Umstand Rechnung zu tragen habe, dass neben dem aus Art. 19 Abs. 4 GG folgenden Rechtsschutzinteresse der Ermittlungsadressaten auch die Ermittlungsinteressen der Allgemeinheit und mögliche Rechtspositionen Dritter verfassungsrechtlichen Schutz genössen und von der Benachrichtigung berührt sein könnten. 58

kk) Der Kernbereichsschutz sei als Folge des Grundrechtsschutzes stets zu beachten und müsse nicht in jeder polizeigesetzlichen Regelung abgebildet werden. Verfassungsrechtlich geboten erscheine ein gesetzlich normierter Kernbe- 59

reichsschutz nur, wenn die Art der Eingriffsbefugnisse eine Berührung des Kernbereichs typischerweise möglich erscheinen lasse. Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes könnten je nach Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein.

Unter diesen Voraussetzungen sei der Verzicht auf einen gesetzlich normierten Kernbereichsschutz in § 20g BKAG, der keine herausgehobenen Elemente kernbereichssensibler Ermittlungstätigkeit enthalte, verfassungsrechtlich nicht zu beanstanden. 60

Durch die Unterscheidung in § 20h Abs. 5 BKAG zwischen automatischen Aufzeichnungen, über deren Verwertung das anordnende Gericht zu entscheiden habe, und anderen Ermittlungsformen, bei denen die Behörde über Abbruch oder Fortsetzung der Ermittlungen entscheide, werde sichergestellt, dass die vor Ort ermittelnden Beamten überhaupt nur solche Informationen zur Kenntnis nehmen könnten, an deren fehlender Kernbereichsrelevanz kein Zweifel bestehe. Automatisierte Aufzeichnungen als solche verstießen nicht gegen den Schutz des Kernbereichs privater Lebensgestaltung. Verfassungsrechtlich nicht erforderlich sei, dass sämtliche Informationen, die im Rahmen einer potentiell kernbereichsrelevanten Befugnisnorm erhoben würden, durch eine unabhängige Stelle zu kontrollieren seien. 61

Wenn in § 20k Abs. 7, § 20l Abs. 6 BKAG angeordnet werde, dass eine Überwachungsmaßnahme unzulässig sei, wenn „allein“ Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, komme hierin zum Ausdruck, dass die ermittelnden Behörden eine Einschätzung ex ante darüber abgeben müssten, ob die Maßnahmen geeignet seien, die Ermittlungsziele weiterzubringen, ohne den Kernbereich zu verletzen. Äußerungen, die beispielsweise die Planung einer schweren Straftat thematisierten, würden der Rechtsprechung des Bundesverfassungsgerichts zu Folge gar nicht vom Kernbereichsschutz umfasst, also auch dann nicht, wenn sie in einer besonders privaten Situation getätigt würden. 62

§ 20k Abs. 7 Satz 3 BKAG ordne an, dass die erhobenen Daten unter der Sachleitung des anordnenden Gerichts durch den Datenschutzbeauftragten des Bundeskriminalamts und zwei Beamte, von denen einer die Befähigung zum Richteramt haben müsse, auf Kernbereichsrelevanz durchzusehen seien, weil sich die ermittelten Informationen bei der Durchsicht elektronischer Dateien ohne zusätzli- 63

che technische Fertigkeiten der beteiligten Beamten überhaupt nicht entschlüsseln ließen.

Die Regeln zur Löschung einer dokumentierten Kernbereichsverletzung und zur Benachrichtigung des Betroffenen seien ein Kompromiss zwischen den Rechtsschutzanliegen eines Betroffenen und der Vermeidung einer zu langen Speicherung sensibler personenbezogener Daten. Sie genügten den Anforderungen des Art. 19 Abs. 4 GG. 64

ll) Hinsichtlich des Schutzes von Berufsgeheimnisträgern sei die herausgehobene Schutzbedürftigkeit des Strafverteidigers gegenüber anderen Berufen in der Rechtsprechung anerkannt. Die Regelungen des § 20u Abs. 2 BKAG genügten daher sowohl materiell als auch ihrer Bestimmtheit nach den Anforderungen des Grundgesetzes. Ob die Regelung des § 20u BKAG den Schutzbereich des Art. 12 GG berühre, erscheine zweifelhaft; denn die einschlägigen Regelungen hätten keine berufsregelnde Tendenz. Selbst im Falle der Eröffnung des Schutzbereichs handele es sich aber um eine bloße Berufsausübungsregelung, die durch ein Gesetz und einen Gemeinwohlbelang gerechtfertigt sei. 65

mm) Die gesetzlichen Vorschriften zur Verwendung der vom Bundeskriminalamt zur Abwehr von Gefahren des internationalen Terrorismus erhobenen Daten entsprächen den verfassungsrechtlichen Vorgaben. 66

§ 20v Abs. 4 Satz 2 BKAG stelle klar, dass das Bundeskriminalamt die ermittelten Daten nur zur Erfüllung der gesetzlichen Aufgaben nach §§ 4a, 5, 6 BKAG verwenden dürfe. Bei dieser Regelung handele es sich um beschränkte Verwendungsregeln, die durch die Kohärenz der zu schützenden Rechtsgüter in gleicher Weise gerechtfertigt seien wie die Ermittlungsbefugnisse selbst. 67

Die Datenübermittlungsregeln des § 20v Abs. 5 Satz 1 BKAG verhielten sich akzessorisch zu den Kompetenzen des Bundeskriminalamts, bildeten im Bereich der Gefahrenabwehr den gesetzlichen Gefahrenmaßstab ab und beschränkten sich im Bereich der Strafverfolgung bei den besonders eingriffsintensiven Befugnissen der §§ 20h, 20k, 20l BKAG auf die Verfolgung schwerer Straftaten. Die Regelungen genügten auch dem Erfordernis der Normenklarheit. Die Datenübermittlung an „sonstige öffentliche Stellen“ werde durch die Zweckgebundenheit der Übermittlung beschränkt. § 20v Abs. 5 Satz 5 BKAG sehe für die Übermittlung von Informationen, die mit Hilfe des besonders eingriffsintensiven § 20h BKAG ermittelt worden seien, keine Zweckänderung vor. 68

2. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hält die angegriffenen Vorschriften in wesentlichen Punkten aus denselben Gründen für verfassungswidrig wie die Beschwerdeführer. Bedenklich sei, dass die Aufgaben und Befugnisse des Bundeskriminalamts nicht hinreichend klar von denen der Polizeibehörden der Länder sowie der Verfassungsschutzbehörden des Bundes und der Länder abgegrenzt seien. Zweifelhaft sei, ob die Befugnisse zur Straftatenverhütung nach § 4a Abs. 1 Satz 2 BKAG hinreichend normenklar ausgestaltet und die möglichen Eingriffe im Gefahrenvorfeld verhältnismäßig seien. Soweit Maßnahmen zum Schutz von „Sachen von bedeutendem Wert“ erlaubt würden, seien sie unverhältnismäßig; wann die Erhaltung einer Sache im öffentlichen Interesse „geboten“ sei, lasse sich den Vorschriften nicht entnehmen. Der Richtervorbehalt des § 20g Abs. 3 BKAG sei unzureichend und weise hinsichtlich der verschiedenen Observationsmittel wie auch im Verhältnis zu strafrechtlichen Vorschriften Wertungswidersprüche auf. Aufgrund unklarer Begrenzungen unverhältnismäßig weit seien die Regelungen zur Inanspruchnahme des Zustands- und Nichtstörers sowie von Kontakt- und Begleitpersonen. Überwiegend verfassungswidrig sei auch die Regelung der Benachrichtigungspflichten in § 20w BKAG. Eine dem § 20w Abs. 2 Satz 1 BKAG entsprechende Regelung habe das Bundesverfassungsgericht in Fällen der akustischen Wohnraumüberwachung bereits für unzulässig erklärt, und die Beschränkungen der Benachrichtigung in § 20w Abs. 1 Satz 1 Nr. 1, Nr. 2 b, Satz 3 BKAG seien zu unbestimmt; verfassungswidrig sei auch die Möglichkeit eines endgültigen Absehens von einer Benachrichtigung gemäß § 20w Abs. 3 Satz 5 BKAG. In Übereinstimmung mit den Argumenten der Beschwerdeführer hält der Bundesdatenschutzbeauftragte die in den angegriffenen Vorschriften getroffenen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung für unzureichend. Ebenso teilt er die verfassungsrechtlichen Bedenken der Beschwerdeführer hinsichtlich des Schutzes zeugnisverweigerungsberechtigter Personen gemäß § 20u BKAG. § 20v Abs. 5 Satz 1 Nr. 3 BKAG sei unverhältnismäßig, weil die Verwendung von Daten aus einer Wohnraumüberwachung oder dem Zugriff auf informationstechnische Systeme schon für die Verfolgung von Straftaten erlaubt werde, die im Höchstmaß mit „mindestens“ fünf Jahren bedroht seien. Im Falle des § 14 BKAG würden die verfassungsrechtlich gebotenen Restriktionen des § 20v Abs. 4, 5 BKAG für die Verwendung der Daten ins Leere laufen. 69

3. Die Datenschutzbeauftragten der Länder teilen im Wesentlichen gleichfalls die verfassungsrechtlichen Bedenken der Beschwerdeführer und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. 70

Insbesondere sei der im Gesetz verwandte Gefahrbegriff nicht hinreichend normenklar und trennscharf formuliert. Die Befugnisse im Vorfeld der Gefahrenabwehr und zur Strafverfolgung genügten nicht den besonders hohen Anforderungen an die Bestimmtheit des Eingriffsanlasses. Für die Definition der Kontakt- und Begleitperson machen sie ergänzend geltend, dass § 20b Abs. 2 Nr. 2 BKAG seiner Bedeutung nach systematisch unklar und der Sache nach zu unbestimmt sei. Hinsichtlich der möglichen Dauer einer Anordnung zur Online-Durchsuchung weisen sie auf Wertungswidersprüche zwischen § 20k Abs. 6 BKAG und anderen Ermächtigungsnormen hin; die besondere Eingriffsintensität einer Online-Durchsuchung bedinge eine kürzere als die dreimonatige Anordnungsfrist. 71

4. Das Bundesverwaltungsgericht weist durch die Mitglieder des für das Polizeirecht zuständigen 6. Senats darauf hin, dass - nach der Rechtsprechung des Gerichts zu polizeilichen Meldeauflagen - für die Erfüllung polizeilicher Aufgaben im Vorfeld der Gefahrenabwehr die Bestimmtheitsanforderungen spezifisch an der Vorfeldsituation ausgerichtet sein müssen. Sehe der Gesetzgeber in solchen Lagen Grundrechtseingriffe vor, habe er hierfür eine spezielle Rechtsgrundlage mit handlungsbegrenzenden Tatbestandselementen zu schaffen. 72

Hinsichtlich der Benachrichtigung des von einer Überwachungsmaßnahme Betroffenen habe das Gericht im Zusammenhang mit Maßnahmen der Telekommunikationsüberwachung unter dem G10-Gesetz entschieden, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 GG eine Benachrichtigung gebieten könne, wenn diese Form der Kenntnisgewähr Voraussetzung der Inanspruchnahme gerichtlichen Rechtsschutzes sei. Begrenzungen dieses Anspruchs, der einer gesetzlichen Ausgestaltung bedürfe, seien allerdings nicht ausgeschlossen. Im Lichte des Art. 19 Abs. 4 GG sei auch die grundsätzlich bestehende Pflicht zur Vernichtung nicht mehr erforderlicher Daten zu sehen. Die Vernichtungspflicht müsse für die Fälle, in denen der Betroffene die gerichtliche Kontrolle staatlicher Informations- und Datenerhebungsmaßnahmen anstrebe, mit der Rechtsschutzgarantie so abgestimmt werden, dass der Rechtsschutz nicht unterlaufen oder vereitelt werde. Die die Telekommunikationsüberwachung veranlassende Behörde sei grundrechtlich verpflichtet, den von der heimlichen Überwachungsmaßnahme Betroffenen so bald wie möglich zu unterrichten. Die Verzögerung der Mitteilung begründe einen neben der Datenerhebung liegenden, eigenständigen Grundrechtseingriff, der als solcher Gegenstand einer gerichtlichen Feststellung sein könne. 73

V.

In der mündlichen Verhandlung haben sich geäußert: die Beschwerdeführer, die Bundestagsfraktion Bündnis 90/Die Grünen, die Bundesregierung durch den Bundesminister des Inneren, das Bundeskriminalamt, der Generalbundesanwalt, das Bundesamt für Sicherheit in der Informationstechnik, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und der Bayerische Landesbeauftragte für den Datenschutz. Als sachkundige Dritte wurden Prof. Dr. Matthias Bäcker, Prof. Dr. Felix Freiling, der Richter am Amtsgericht Wiesbaden Frank Hoffrichter, die Bundesrechtsanwaltskammer, der Deutsche Anwaltverein e.V., der Chaos Computer Club e.V., Netzpolitik.org und Amnesty International angehört. Die Bundesrechtsanwaltskammer hat ihre Stellungnahme mittels eines Schriftsatzes betreffend den Schutz von Rechtsanwälten nach § 20u Abs. 1, 2 BKAG ergänzt. Der Chaos Computer Club e.V. hat seine in der mündlichen Verhandlung getätigten Ausführungen mittels einer schriftlichen Stellungnahme zu den technischen Risiken bei der Infiltration eines informationstechnischen Systems, zum Schutz des Kernbereichs privater Lebensgestaltung, zur Quellen-Telekommunikationsüberwachung und zur Überprüfbarkeit von Trojaner-Funktionen weiter unterlegt. 74

B.

Die Verfassungsbeschwerden sind im Wesentlichen zulässig. 75

I.

Die Beschwerdeführerinnen und Beschwerdeführer wenden sich mit ihren Verfassungsbeschwerden gegen Überwachungs- und Ermittlungsbefugnisse des Bundeskriminalamts, dabei eigens auch gegen einen unzureichenden Schutz des Kernbereichs privater Lebensgestaltung und gegen Überwachungen zeugnisverweigerungsberechtigter Personen, sowie gegen Regelungen zur Datennutzung. Unmittelbar richten sich ihre Angriffe gegen die die Behörde jeweils ermächtigenden Befugnisnormen, mittelbar aber auch gegen die weiteren Regelungen, mit denen der Gesetzgeber diese Befugnisse zur Gewährleistung ihrer Verhältnismäßigkeit flankiert und ohne die ihre Verfassungsmäßigkeit nicht beurteilt werden kann. Bei verständiger Auslegung der Verfassungsbeschwerden erstrecken sich ihre Angriffe damit auf § 14 Abs. 1 Satz 1 Nr. 1 und 3, Satz 2, Abs. 7, § 20c, § 20g Abs. 1 bis 3, § 20h, § 20j, § 20k, § 20l, § 20m Abs. 1, 3, § 20u Abs. 1, 2 und 4, 76

§ 20v Abs. 4 Satz 2, Abs. 5 (ohne den nicht substantiiert beanstandeten Satz 3 Nr. 2) und Abs. 6 sowie auf § 20w BKAG.

II.

Die Verfassungsbeschwerde des Beschwerdeführers zu 4) im Verfahren 1 BvR 966/09 hat sich durch seinen Tod erledigt. Die Voraussetzungen für eine Fortführung des Verfahrens nach dem Tod (vgl. BVerfGE 109, 279 <304>; 124, 300 <318 f.>) liegen nicht vor. 77

Unzulässig ist die Verfassungsbeschwerde in diesem Verfahren, soweit sie sich gegen § 20c BKAG richtet. Die Vorschrift ermächtigt allein zu Maßnahmen, die als offene Vollzugsakte gegenüber den Betroffenen ergehen; eine Verfassungsbeschwerde ist nur insoweit zulässig, als entsprechende Maßnahmen gegen sie selbst ergangen sind und sie sich dagegen vor den Fachgerichten erfolglos zur Wehr gesetzt haben (vgl. BVerfGE 122, 63 <78 ff.> m.w.N.). Dies ist hier nicht geschehen. 78

III.

Im Übrigen sind die Verfassungsbeschwerden zulässig. 79

1. Die Beschwerdeführerinnen und Beschwerdeführer sind beschwerdebefugt. Sie rügen eine mögliche Verletzung ihrer Grundrechte unmittelbar durch die angegriffenen Bestimmungen. Sie machen geltend, dass die angegriffenen Datenerhebungsbefugnisse in ihr Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG, ihr Grundrecht auf Wahrung des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG sowie ihre Grundrechte aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowohl in der Ausformung als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als auch als Recht auf informationelle Selbstbestimmung eingreifen, und tragen eingehend vor, dass diese unverhältnismäßig ausgestaltet seien. Eine mögliche Grundrechtsverletzung ist insoweit hinreichend dargelegt. Dies gilt auch, soweit die Beschwerdeführer bezüglich der Befugnisse zur Datenerhebung eine Verletzung dieser Grundrechte in Verbindung mit Art. 1 Abs. 1 GG durch einen unzureichend normierten Schutz des Kernbereichs privater Lebensgestaltung rügen und Grundrechtsverletzungen durch die ihrer Ansicht nach unzureichenden und gleichheitswidrigen Regelungen zum Schutz zeugnisverweigerungsberechtigter Personen geltend machen. Möglich erscheint eine Grundrechtsverletzung schließlich auch durch die von ihnen 80

angegriffenen Vorschriften zur Datenverwendung. In der weiteren Verwendung von Daten kann eine eigene Grundrechtsverletzung liegen; maßgeblich sind insoweit die Grundrechte, die jeweils für deren Erhebung einschlägig waren (vgl. BVerfGE 100, 313 <359 f., 391>; 109, 279 <374 f.>; 110, 33 <68 f.>; 113, 348 <365>; 125, 260 <312 f., 333>; 133, 277 <372 ff.>; stRspr).

2. Die Beschwerdeführer und Beschwerdeführerinnen sind durch die angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen. Ihre Verfassungsbeschwerden erfüllen damit die spezifischen Anforderungen für Verfassungsbeschwerden unmittelbar gegen ein Gesetz. 81

a) Den Beschwerdeführern fehlt es nicht an einer unmittelbaren Betroffenheit. Zwar bedürfen die angegriffenen Befugnisse der Umsetzung durch weitere Vollzugsakte. Von einer unmittelbaren Betroffenheit durch Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu (vgl. BVerfGE 133, 277 <311 Rn. 83>; stRspr). Die durch die angegriffenen Vorschriften ermöglichten Ermittlungs- und Überwachungsmaßnahmen werden grundsätzlich heimlich durchgeführt. Die im Gesetz vorgesehenen Benachrichtigungspflichten fangen dies nur teilweise auf, weil sie möglicherweise erst spät greifen und weitreichende Ausnahmen kennen. Keine Kenntnis erhalten die Betroffenen in der Regel auch von der weiteren Nutzung oder Übermittlung der Daten, die durch die angegriffenen Vorschriften erlaubt werden. Die Beschwerdeführer sind deswegen nicht darauf zu verweisen, entsprechende Vollzugsakte abzuwarten und gegen diese vorzugehen. 82

b) Die Beschwerdeführer sind auch selbst und gegenwärtig betroffen. 83

Die Beschwerdeführer legen dar, dass sie wegen ihrer spezifischen politischen, beruflichen und privaten Verbindungen zu potenziellen Zielpersonen von den angegriffenen Maßnahmen mit hinreichender Wahrscheinlichkeit betroffen sind. Sie verweisen darauf, dass sie aufgrund ihrer politischen Tätigkeit, ihrer beruflichen Tätigkeit als Rechtsanwälte oder Psychotherapeuten oder aufgrund ihres Engagements in Menschenrechtsfragen leicht auch mit Personen in Kontakt geraten können, die möglicherweise dem internationalen Terrorismus zugerechnet werden. Angesichts der Streubreite der angegriffenen Vorschriften, die nicht von vornherein auf einen begrenzten spezifischen Personenkreis zugeschnitten sind, sondern nach § 4a BKAG der Abwehr des internationalen Terrorismus allgemein 84

dienen und hierbei in weitem Umfang auch gutgläubige Dritte mit erfassen können, ist eine hinreichende Wahrscheinlichkeit ihrer gegenwärtigen Betroffenheit in eigenen Rechten dargetan (vgl. BVerfGE 109, 279 <307 f.>; 113, 348 <363 f.>; 133, 277 <312 f. Rn. 86 f.>).

3. Die Verfassungsbeschwerden sind nach § 93 Abs. 3 BVerfGG fristgerecht eingelegt. Dies gilt auch hinsichtlich § 14 Abs. 1, 7 BKAG. Die Vorschrift wurde zwar nicht durch das hier in Rede stehende Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl I S. 3083) eingeführt oder modifiziert, sondern geht zurück auf das Bundeskriminalamtgesetz in der Fassung vom 7. Juli 1997 (BGBl I S. 1650) und wurde vor dem Inkrafttreten des Unterabschnitts 3a des Bundeskriminalamtgesetzes zuletzt durch Artikel 9 des Gesetzes zur Ausführung des Römischen Statuts des Internationalen Strafgerichtshofs vom 17. Juli 1998 vom 21. Juni 2002 (BGBl I S. 2144) geändert. Durch die Reform des Bundeskriminalamtgesetzes zum 1. Januar 2009 hat § 14 Abs. 1, 7 BKAG jedoch einen neuen Gehalt bekommen. Dem Bundeskriminalamt wurden hierdurch erstmals die Aufgabe der präventiven Bekämpfung des internationalen Terrorismus und entsprechend neue Befugnisse übertragen. Damit bezieht sich die Übermittlung von Daten gemäß § 14 Abs. 1, 7 BKAG nunmehr auch auf Informationen, die mit neuen Mitteln aufgrund der neuen Aufgabe erlangt werden. Hierin liegt eine geänderte Beschwer, die die Beschwerdefrist gegen die Vorschrift erneut in Gang setzt (vgl. BVerfGE 78, 350 <356>; 79, 1 <13 f.>; 80, 137 <149>; 100, 313 <356>). 85

C.

Soweit sich die Verfassungsbeschwerden gegen die Ermittlungs- und Überwachungsbefugnisse richten, sind sie in verschiedener Hinsicht begründet. 86

I.

In kompetenzrechtlicher Hinsicht sind die angegriffenen Vorschriften indes verfassungsgemäß. 87

1. Die Gesetzgebungskompetenz des Bundes ergibt sich aus Art. 73 Abs. 1 Nr. 9a GG. Die angegriffenen neuen Befugnisse des Bundeskriminalamts beziehen sich ausschließlich auf die Wahrnehmung der Aufgaben nach § 4a Abs. 1 BKAG und sind hierdurch begrenzt. Satz 1 der Vorschrift lehnt sich dabei seinem Wortlaut nach eng an Art. 73 Abs. 1 Nr. 9a GG an, und Satz 2 BKAG führt dies, 88

ausdrücklich auf Satz 1 bezugnehmend, weiter aus. Dass dabei auch die Straftatenverhütung erfasst wird, ist durch Art. 73 Abs. 1 Nr. 9a GG nicht ausgeschlossen. Grenzen einer Vorverlagerung von Maßnahmen in das Vorfeld konkreter Gefahren ergeben sich aus rechtsstaatlichen, insbesondere grundrechtlichen Anforderungen, nicht aber aus dem Kompetenztitel des Art. 73 Abs. 1 Nr. 9a GG. Der Begriff der Gefahrenabwehr schließt kompetenzrechtlich die Straftatenverhütung ein. Unbedenklich ist auch, dass die angegriffenen Vorschriften Handlungsbefugnisse begründen, die sich teilweise mit denen der Landespolizeibehörden überschneiden. Der verfassungsändernde Gesetzgeber hat dies bewusst in Kauf genommen.

2. Die angegriffenen Vorschriften sind auch nicht unter dem Gesichtspunkt der Verwaltungskompetenz zu beanstanden. Ungeachtet der Frage, wie das Verhältnis des Art. 87 Abs. 1 Satz 2 GG zu Art. 73 Abs. 1 Nr. 9a und 10 GG genauer zu bestimmen ist, zielte die Einführung des Art. 73 Abs. 1 Nr. 9a GG im Jahre 2006 von vornherein darauf, die neu zu schaffenden Regelungen in die Hände des Bundeskriminalamts zu legen. Nach dem Wortlaut des neuen Kompetenztitels soll ausdrücklich die Abwehr von Gefahren des internationalen Terrorismus „durch das Bundeskriminalpolizeiamt“ geregelt werden. Deshalb lässt sich die Verwaltungskompetenz des Bundeskriminalamts als Bundesbehörde jedenfalls auf eine Zusammenschau von Art. 73 Abs. 1 Nr. 9a GG und Art. 87 Abs. 1 Satz 2 GG stützen. 89

II.

Die angegriffenen Überwachungs- und Ermittlungsbefugnisse ermächtigen zu Grundrechtseingriffen, die in Abhängigkeit von dem jeweils betroffenen Grundrecht und dem verschiedenen Eingriffsgewicht je einzeln am Grundsatz der Verhältnismäßigkeit und am Grundsatz der Normenklarheit und Bestimmtheit zu messen sind. Ihnen gemeinsam ist allerdings, dass die danach möglichen Eingriffe überwiegend schwer wiegen, mit dem Zweck der Abwehr von Gefahren des internationalen Terrorismus aber ein legitimes Ziel verfolgen und hierfür auch geeignet und erforderlich sind. 90

1. Die angegriffenen Befugnisse ermächtigen das Bundeskriminalamt im Rahmen der Gefahrenabwehr und Straftatenverhütung zur heimlichen Erhebung personenbezogener Daten und begründen - unterschieden je nach der in Frage stehenden Befugnis - Eingriffe in die Grundrechte aus Art. 13 Abs. 1, Art. 10 Abs. 1 und Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, letzteres sowohl in seiner Ausprägung als Recht auf Gewährleistung der Vertraulichkeit und Integrität 91

informationstechnischer Systeme als auch als Recht auf informationelle Selbstbestimmung.

Es handelt sich bei all diesen Befugnissen um Rechtsgrundlagen für Überwachungs- und Ermittlungsmaßnahmen, die meistens ohne Kenntnis der Betroffenen heimlich durchgeführt werden und dabei tief in die Privatsphäre eingreifen können. Auch wenn hierbei berechtigte Vertraulichkeitserwartungen in verschiedenem Umfang berührt werden und das Eingriffsgewicht der Befugnisse sich deutlich unterscheidet, haben sie in aller Regel ein Eingriffsgewicht, das jedenfalls schwer wiegt. Anders liegt es nur bei einzelnen Maßnahmen gemäß § 20g Abs. 1, 2 BKAG. 92

2. Die Verfassungsmäßigkeit der Befugnisse hängt von den sich aus diesen Grundrechten jeweils ergebenden Grenzen und den hierbei für die Befugnisse je einzeln zu ermittelnden Verhältnismäßigkeitsanforderungen ab. Dabei muss die Einräumung dieser Befugnisse aber in allen Fällen nach dem Grundsatz der Verhältnismäßigkeit einem legitimen Ziel dienen und zu dessen Erreichung geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 67, 157 <173>; 70, 278 <286>; 104, 337 <347 ff.>; 120, 274 <318 f.>; 125, 260 <316>; stRspr). 93

Alle angegriffenen Befugnisse sind zudem am Grundsatz der Normenklarheit und Bestimmtheit zu messen, der der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Verwaltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient (vgl. BVerfGE 113, 348 <375 ff.>; 120, 378 <407 f.>; 133, 277 <336 Rn. 140>; stRspr). Für die hier in Frage stehenden Befugnisse zur heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre hineinwirken können, stellt er besonders strenge Anforderungen. Da ihre Handhabung von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden kann, kann ihr Gehalt - anders als etwa durch Verwaltungsakt zu vollziehende auslegungsbedürftige Begriffe des Verwaltungsrechts sonst - nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden. Im Einzelnen unterscheiden sich hierbei die Anforderungen allerdings maßgeblich nach dem Gewicht des Eingriffs und sind insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden (vgl. BVerfGE 110, 33 <55>; 113, 348 <376>). 94

3. Die angegriffenen Vorschriften dienen einem legitimen Ziel und sind hierfür geeignet und erforderlich. 95

a) Die Befugnisse dienen einem legitimen Ziel. Sie geben dem Bundeskriminalamt Aufklärungsmittel an die Hand, mit denen dieses seine neue Aufgabe der Abwehr von Gefahren des internationalen Terrorismus wahrnehmen soll. Der Begriff des internationalen Terrorismus ist dabei durch die Aufgabenbeschreibung des § 4a Abs. 1 BKAG und dessen Verweis auf § 129a Abs. 1, 2 StGB in enger Anlehnung an den EU-Rahmenbeschluss vom 13. Juni 2002 und die internationale Begrifflichkeit (ABl. EU Nr. L 164 S. 3; 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) definiert und - in Übereinstimmung mit den Vorstellungen des verfassungsändernden Gesetzgebers bei Schaffung des Art. 73 Abs. 1 Nr. 9a GG (vgl. BTDrucks 16/813, S. 12) - auf spezifisch charakterisierte Straftaten von besonderem Gewicht begrenzt. Straftaten mit dem Gepräge des Terrorismus in diesem Sinne 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. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (vgl. BVerfGE 115, 320 <357 f.>; 120, 274 <319>; 133, 277 <333 f. Rn. 133>). 96

b) Die Einräumung der fraglichen Überwachungs- und Ermittlungsbefugnisse ist zur Erreichung dieses Ziels geeignet. Sie geben dem Bundeskriminalamt Mittel zur Aufklärung an die Hand, die dazu beitragen können, den Gefahren des internationalen Terrorismus entgegenzutreten. Die verschiedenen Befugnisse sind hierfür jedenfalls im Grundsatz auch erforderlich. Jede Befugnis ermöglicht spezifische Maßnahmen, die jedenfalls nicht immer durch andere ersetzt werden können. Mildere Mittel, die gleichermaßen effektiv ebenso weitgehende Aufklärungsmöglichkeiten zur Abwehr des internationalen Terrorismus ermöglichten, sind nicht ersichtlich. Dies lässt freilich unberührt, dass auch die Anwendung der Befugnisse im Einzelfall dem Grundsatz der Geeignetheit und Erforderlichkeit zu folgen hat. 97

III.

Begrenzungen ergeben sich maßgeblich aus den Anforderungen der Verhältnismäßigkeit im engeren Sinne. Danach müssen die Überwachungs- und Ermitt- 98

lungsbefugnisse mit Blick auf das Eingriffsgewicht angemessen ausgestaltet sein. Es ist Aufgabe des Gesetzgebers, einen Ausgleich zwischen der Schwere der mit den hier zur Prüfung stehenden Eingriffen in die Grundrechte potentiell Betroffener auf der einen Seite und der Pflicht des Staates zum Schutz der Grundrechte auf der anderen Seite zu schaffen.

1. Der Gesetzgeber hat dabei auf der einen Seite das Eingriffsgewicht der durch die angegriffenen Vorschriften erlaubten Maßnahmen in Rechnung zu stellen. Sie ermöglichen - je nach Befugnis in verschiedenem Umfang - tiefgreifende Eingriffe in die Privatsphäre und können im Einzelfall auch in private Rückzugsräume eindringen, deren Schutz für die Wahrung der Menschenwürde von besonderer Bedeutung ist. Dabei hat der Gesetzgeber in seine Abwägung auch die Entwicklung der Informationstechnik einzustellen, die die Reichweite von Überwachungsmaßnahmen zunehmend ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen. Überwachungsmaßnahmen erhalten dadurch ein gesteigertes Eingriffsgewicht, dem in der Abwägung Rechnung zu tragen ist. 99

2. Auf der anderen Seite hat der Gesetzgeber einen wirksamen Schutz der Grundrechte und Rechtsgüter der Bürgerinnen und Bürger zu sichern. Für die verfassungsrechtliche Prüfung der Angemessenheit ist zu berücksichtigen, dass die verfassungsmäßige Ordnung, der Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person Schutzgüter von hohem verfassungsrechtlichem Gewicht sind. Dementsprechend hat das Bundesverfassungsgericht hervorgehoben, dass die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm - unter Achtung von Würde und Eigenwert des Einzelnen - zu gewährleistende Sicherheit der Bevölkerung Verfassungswerte sind, die mit anderen hochwertigen Verfassungsgütern im gleichen Rang stehen. Es hat den Staat deshalb für verpflichtet erachtet, das Leben, die körperliche Unversehrtheit und die Freiheit des Einzelnen zu schützen, das heißt vor allem, auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren (vgl. BVerfGE 115, 320 <346 f.>; siehe auch BVerfGE 49, 24 <56 f.>; 90, 145 <195>; 115, 118 <152 f.>). 100

Bei der Prüfung der Angemessenheit der angegriffenen Vorschriften ist zudem zu beachten, dass es sich nicht um Normen handelt, die in ihrer Eingriffswirkung mit großer Streubreite gleichsam die gesamte Bevölkerung betreffen. Es geht vielmehr ganz überwiegend um Bestimmungen, die die Sicherheitsbehörden einzelfallbezogen in den Stand setzen sollen, schwerwiegende Gefahren für Rechts- 101

güter von Verfassungsrang abzuwehren und Straftaten von großem Gewicht zu verhüten.

Dabei ist die Entscheidung über die Erhebung der Daten im Blick auf die Gefahren, die vom internationalen Terrorismus ausgehen, auch für den Informationsaustausch zwischen den innerstaatlichen Stellen und die möglichst effektive Zusammenarbeit mit den Sicherheitsbehörden anderer Staaten von besonderer Bedeutung. Ein funktionierender Informationsaustausch setzt im Interesse des verfassungsrechtlich gebotenen Schutzes der Menschen eine Übermittlung von im Inland erhobenen Erkenntnissen voraus und ist im Gegenzug auf Unterrichtungen durch ausländische Stellen angewiesen. 102

IV.

Für tief in die Privatsphäre eingreifende Ermittlungs- und Überwachungsbefugnisse, wie sie ganz überwiegend hier in Frage stehen, hat das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne übergreifende Anforderungen abgeleitet. Diese betreffen spezifisch breitenwirksame Grundrechtsgefährdungspotenziale, insbesondere solche der elektronischen Datenverarbeitung (vgl. BVerfGE 100, 313 <358 ff.>; 115, 320 <341 ff.>; 125, 260 <316 ff.>; 133, 277 <335 ff. Rn. 138 ff.>), ebenso wie einzelfallbezogene Maßnahmen gegen Betroffene, die in den Fokus der handelnden Behörden geraten sind (BVerfGE 107, 299 <312 ff.> - Telekommunikationsverkehrsdatenerhebung -, BVerfGE 110, 33 <52 ff.>; 113, 348 <364 ff.>; 129, 208 <236 ff.> - Telekommunikationsüberwachung nach Bundes-, Landes- und Strafprozessrecht -, BVerfGE 109, 279 <335 ff.> - Wohnraumüberwachung -, BVerfGE 112, 304 <315 ff.> - GPS-Observierung -, BVerfGE 120, 274 <302 ff.> - Online-Durchsuchung -). 103

1. Heimliche Überwachungsmaßnahmen, sofern sie, wie die meisten der hier in Rede stehenden Maßnahmen, tief in die Privatsphäre eingreifen, sind mit der Verfassung nur vereinbar, wenn sie dem Schutz oder der Bewehrung von hinreichend gewichtigen Rechtsgütern dienen, für deren Gefährdung oder Verletzung im Einzelfall belastbare tatsächliche Anhaltspunkte bestehen. Sie setzen grundsätzlich voraus, dass der Adressat der Maßnahme in die mögliche Rechtsgutverletzung aus Sicht eines verständigen Dritten den objektiven Umständen nach verfangen ist. Eine vorwiegend auf den Intuitionen der Sicherheitsbehörden beruhende bloße Möglichkeit weiterführender Erkenntnisse genügt zur Durchführung solcher Maßnahmen nicht (vgl. BVerfGE 107, 299 <321 ff.>; 110, 33 <56>; 113, 348 <377 f., 380 f.>; 120, 274 <328>; 125, 260 <330>). Die Verfassung setzt so der 104

Absenkung der Eingriffsschwellen für Maßnahmen der Straftatenverhütung, die heimlich durchgeführt werden und tief in die Privatsphäre hineinreichen können, deutliche Grenzen; für weniger tief in die Privatsphäre eingreifende Maßnahmen reichen die verfassungsrechtlich zulässigen Gestaltungsmöglichkeiten zur Straftatenverhütung demgegenüber weiter.

Bei der näheren Ausgestaltung der Einzelbefugnisse kommt es für deren Angemessenheit wie für die zu fordernde Bestimmtheit maßgeblich auf das Gewicht des jeweils normierten Eingriffs an. Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und berechtigte Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen. Besonders tief in die Privatsphäre dringen die Wohnraumüberwachung sowie der Zugriff auf informationstechnische Systeme. 105

a) Heimliche Überwachungsmaßnahmen müssen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein. 106

Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an, die der Gesetzgeber insoweit in - jeweils näher bestimmte - erhebliche, schwere und besonders schwere Straftaten eingeteilt hat. So bedarf die Durchführung einer Wohnraumüberwachung des Verdachts einer besonders schweren Straftat (vgl. BVerfGE 109, 279 <343 ff.>), die Durchführung einer Telekommunikationsüberwachung oder die Nutzung von vorsorglich erhobenen Telekommunikationsverkehrsdaten des Verdachts einer schweren Straftat (vgl. BVerfGE 125, 260 <328 f.>; 129, 208 <243>) und die Durchführung einer anlassbezogenen Telekommunikationsverkehrsdatenerhebung oder einer Observation etwa durch einen GPS-Sender einer - im ersten Fall durch Regelbeispiele konkretisierten - Straftat von erheblicher Bedeutung (vgl. BVerfGE 107, 299 <321 f.>; 112, 304 <315 f.>; zu letzterer Entscheidung vgl. auch EGMR, Uzun v. Deutschland, Entscheidung vom 2. September 2010, Nr. 35623/05, § 70, NJW 2011, S. 1333 <1337>, zu Art. 8 EMRK). 107

Für Maßnahmen, die der Gefahrenabwehr dienen und damit präventiven Charakter haben, kommt es unmittelbar auf das Gewicht der zu schützenden Rechtsgüter an (vgl. BVerfGE 125, 260 <329>). Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig. Hierzu gehören Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes (vgl. 108

BVerfGE 120, 274 <328>; 125, 260 <330>). Einen uneingeschränkten Sachwertschutz hat das Bundesverfassungsgericht demgegenüber nicht als ausreichend gewichtig für solche Maßnahmen angesehen. Es hat den Zugriff auf vorsorglich gespeicherte Daten (vgl. BVerfGE 125, 260 <330>) oder die Durchführung von Wohnraumüberwachungen jedoch auch bei einer gemeinen Gefahr (vgl. BVerfGE 109, 279 <379>) und Online-Durchsuchungen bei einer Gefahr für Güter der Allgemeinheit, die die Existenz der Menschen berühren (vgl. BVerfGE 120, 274 <328>), für im Grundsatz mit der Verfassung vereinbar gehalten. Der Gesetzgeber ist nicht gehindert, die maßgebliche Schwelle für den Rechtsgüterschutz dieser Überwachungsmaßnahmen hiervon ausgehend auch einheitlich zu bestimmen.

b) Die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität ist im Bereich der Gefahrenabwehr zum Schutz der genannten Rechtsgüter grundsätzlich nur verhältnismäßig, wenn eine Gefährdung dieser Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist (vgl. BVerfGE 120, 274 <328 f.>; 125, 260 <330 f.>). 109

Auch diese Anforderungen hängen im Einzelnen zunächst von Art und Gewicht des Eingriffs ab. Für die besonders tief in die Privatsphäre eindringenden Eingriffe der Wohnraumüberwachung verlangt Art. 13 Abs. 4 GG eine dringende Gefahr. Der Begriff der dringenden Gefahr nimmt dabei nicht nur im Sinne des qualifizierten Rechtsgüterschutzes auf das Ausmaß, sondern auch auf die Wahrscheinlichkeit eines Schadens Bezug (vgl. BVerfGE 130, 1 <32>). 110

Im Übrigen müssen die Anforderungen an eine hinreichend konkret absehbare Gefahrenlage hinsichtlich der genannten Rechtsgüter im Verhältnis zur Belastung des Betroffenen bestimmt werden. Verfassungsrechtlich ausreichend sind hierfür zunächst die Anforderungen zur Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren gegenüber polizeipflichtigen Personen nach den Maßgaben des allgemeinen Sicherheitsrechts für die hier relevanten Schutzgüter. Der traditionelle polizeirechtliche Begriff der „konkreten Gefahr“ setzt eine Sachlage voraus, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung eines polizeilichen Schutzguts führt (vgl. BVerfGE 115, 320 <364>; BVerwGE 116, 347 <351>). Ein noch engerer zeitlicher Zusammenhang wird gefordert, wenn es nach der jeweiligen Ermächtigungsgrundlage auf eine „unmittelbar bevorstehende“ oder „gegenwärtige Gefahr“ ankommt (vgl. BVerwGE 45, 51 <57 f.>). 111

Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein für je- 112
de Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen für bestimmte Bereiche mit dem Ziel schon der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. Allerdings müssen die Eingriffsgrundlagen auch dann eine hinreichend konkretisierte Gefahr in dem Sinne verlangen, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen (vgl. BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>). Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfGE 120, 274 <328 f.>; 125, 260 <330 f.>). In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist.

Dagegen wird dem Gewicht eines Eingriffs durch heimliche polizeirechtliche 113
Überwachungsmaßnahmen nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weiter in das Vorfeld einer in ihren Konturen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird. Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur relativ

diffuse Anhaltspunkte für mögliche Gefahren bestehen. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. BVerfGE 120, 274 <329>; vgl. auch BVerfGE 110, 33 <59>; 113, 348 <377>). Solche Offenheit genügt für die Durchführung von eingriffsintensiven heimlichen Überwachungsmaßnahmen nicht. Nicht ausreichend für solche Maßnahmen ist insoweit etwa allein die Erkenntnis, dass sich eine Person zu einem fundamentalistischen Religionsverständnis hingezogen fühlt.

c) Gestufte Anforderungen ergeben sich hinsichtlich der Frage, wieweit Überwachungsmaßnahmen als Maßnahmen der Umfeldüberwachung auch gegenüber Personen durchgeführt werden dürfen, die nicht als Handlungs- oder Zustandsverantwortliche beziehungsweise Tatverdächtige in besonderer Verantwortung stehen. 114

Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürfen sich unmittelbar nur gegen diejenigen als Zielperson richten, die für die drohende oder dringende Gefahr verantwortlich sind (vgl. BVerfGE 109, 279 <351, 352>; 120, 274 <329, 334>). Diese Maßnahmen dringen so tief in die Privatsphäre ein, dass sie auf weitere Personen nicht ausgedehnt werden dürfen. Verfassungsrechtlich nicht zu beanstanden ist allerdings, wenn die gegen die Verantwortlichen angeordneten Maßnahmen, soweit unvermeidbar, auch Dritte miterfassen (vgl. BVerfGE 109, 279 <352 ff.>). Deshalb kann die Überwachung der Wohnung eines Dritten erlaubt werden, wenn aufgrund bestimmter Tatsachen vermutet werden kann, dass die Zielperson sich dort zur Zeit der Maßnahme aufhält, sie dort für die Ermittlungen relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (vgl. BVerfGE 109, 279 <353, 355 f.>). Ebenso kann eine Online-Durchsuchung auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht. 115

Eine Anordnung von anderen heimlichen Überwachungsmaßnahmen ist auch unmittelbar gegenüber Dritten nicht schlechthin ausgeschlossen. In Betracht kommt insoweit eine Befugnis zur Überwachung von Personen aus dem Umfeld einer Zielperson, etwa von - näher einzugrenzenden - Kontaktpersonen oder Nachrichtenmittlern. Solche Befugnisse rechtfertigen sich aus der objektiven Natur 116

der Gefahrenabwehr und der Wahrheitsermittlung im strafrechtlichen Ermittlungsverfahren. Ihre Erstreckung auf Dritte steht unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat voraus. Hierfür reicht es nicht schon, dass sie mit einer Zielperson überhaupt in irgendeinem Austausch stehen. Vielmehr bedarf es zusätzlicher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird (vgl. BVerfGE 107, 299 <322 f.>; 113, 348 <380 f.>). Eine Überwachung von Personen, die - allein gestützt auf die Tatsache eines Kontaktes zu einer Zielperson - erst versucht herauszufinden, ob sich hierüber weitere Ermittlungsansätze erschließen, ist verfassungsrechtlich unzulässig. Dies hindert hinsichtlich solcher Kontaktpersonen allerdings von Verfassungs wegen nicht Ermittlungsmaßnahmen geringerer Eingriffstiefe mit dem Ziel, gegebenenfalls die Eingriffsschwelle für intensivere Überwachungsmaßnahmen zu erreichen.

2. Übergreifende Anforderungen ergeben sich aus dem Verhältnismäßigkeits- 117
grundsatz auch in verfahrensrechtlicher Hinsicht. Die hier ganz überwiegend in Rede stehenden eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, und gegenüber den Betroffenen heimlich durchgeführt werden, bedürfen grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung (vgl. dazu auch EGMR, Klass u.a. v. Deutschland, Urteil vom 6. September 1978, Nr. 5029/71, § 56; EGMR [GK], Zakharov v. Russland, Urteil vom 4. Dezember 2015, Nr. 47143/06, §§ 258, 275; EGMR, Szabó und Vissy v. Ungarn, Urteil vom 12. Januar 2016, Nr. 37138/14, § 77). Dies gilt für Maßnahmen der Wohnraumüberwachung bereits gemäß Art. 13 Abs. 3 und 4 GG (vgl. hierzu BVerfGE 109, 279 <357 ff.>) und folgt im Übrigen unmittelbar aus dem Verhältnismäßigkeitsgrundsatz (vgl. BVerfGE 120, 274 <331 ff.>; 125, 260 <337 ff.>).

Der Gesetzgeber hat das Gebot vorbeugender unabhängiger Kontrolle in spe- 118
zifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung zu verbinden. Hieraus folgt zugleich das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung des Antrags auf Anordnung, die es dem Gericht oder der unabhängigen Stelle erst erlaubt, eine effektive Kontrolle auszuüben. Insbesondere bedarf es der vollständigen Information seitens der antragstellenden Behörde über den zu beurteilenden Sachstand (vgl. BVerfGE 103, 142 <152 f.>). In Anknüpfung hieran ist es Aufgabe

und Pflicht des Gerichts oder der sonst entscheidenden Personen, sich eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte heimliche Überwachungsmaßnahme den gesetzlichen Voraussetzungen entspricht. Hierfür die notwendigen sachlichen und personellen Voraussetzungen zu schaffen, obliegt der Landesjustizverwaltung und dem Präsidium des zuständigen Gerichts (vgl. BVerfGE 125, 260 <338>).

3. Neben den verfassungsrechtlichen Anforderungen an die allgemeinen Eingriffsvoraussetzungen ergeben sich aus den jeweiligen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG für die Durchführung von besonders eingriffsintensiven Überwachungsmaßnahmen besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung. 119

a) Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit gegenüber Überwachung. Er wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen (vgl. BVerfGE 109, 279 <313>; stRspr). 120

Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen (vgl. BVerfGE 109, 279 <313>; 120, 274 <335>; stRspr). Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen (vgl. BVerfGE 109, 279 <321 ff.>). Dieser Kreis deckt sich nur teilweise mit dem der Zeugnisverweigerungsberechtigten. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen (vgl. BVerfGE 109, 279 <330>; 113, 348 <391 f.>). 121

Demgegenüber ist die Kommunikation unmittelbar über Straftaten nicht ge- 122
schützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat. Die Besprechung und Planung von Straftaten gehört ihrem Inhalt nach nicht zum Kernbereich privater Lebensgestaltung, sondern hat Sozialbezug (vgl. BVerfGE 80, 367 <375>; 109, 279 <319 f., 328>; 113, 348 <391>). Dies bedeutet freilich nicht, dass der Kernbereich unter einem allgemeinen Abwägungsvorbehalt in Bezug auf öffentliche Sicherheitsinteressen steht. Ein höchstpersönliches Gespräch fällt nicht schon dadurch aus dem Kernbereich privater Lebensgestaltung heraus, dass es für die Aufklärung von Straftaten oder Gefahren hilfreiche Aufschlüsse geben kann. Aufzeichnungen oder Äußerungen im Zwiegespräch, die zum Beispiel ausschließlich innere Eindrücke und Gefühle wiedergeben und keine Hinweise auf konkrete Straftaten enthalten, gewinnen nicht schon dadurch einen Gemeinschaftsbezug, dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen (vgl. BVerfGE 109, 279 <319>). Auch können trotz Straftatenbezugs Situationen, in denen Einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie Beichtgespräche oder vertrauliche Gespräche mit einem Psychotherapeuten oder einem Strafverteidiger, der höchstpersönlichen Privatsphäre unterfallen, die dem Staat absolut entzogen ist (vgl. BVerfGE 109, 279 <322>). Ein hinreichender Sozialbezug besteht demgegenüber dann, wenn Gespräche - auch mit Vertrauenspersonen - sonst unmittelbar Straftaten zu ihrem Gegenstand haben (vgl. BVerfGE 109, 279 <319>).

b) Der Kernbereich privater Lebensgestaltung beansprucht gegenüber allen 123
Überwachungsmaßnahmen Beachtung. Können sie typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten (vgl. BVerfGE 109, 279 <318 f.>; 113, 348 <390 f.>; 120, 274 <335 ff.>). Außerhalb solch verletzungsgeneigter Befugnisse bedarf es eigener Regelungen nicht. Grenzen, die sich im Einzelfall auch hier gegenüber einem Zugriff auf höchstpersönliche Informationen ergeben können, sind bei deren Anwendung unmittelbar von Verfassungs wegen zu beachten.

c) Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf 124
nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden (vgl. BVerfGE 109, 279 <314>; 120, 273 <339>; stRspr). Dies bedeutet jedoch nicht, dass jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß oder eine Menschenwürdeverletzung begründet. Angesichts der Handlungs- und Prognose-

unsicherheiten, unter denen Sicherheitsbehörden ihre Aufgaben wahrnehmen, kann ein unbeabsichtigtes Eindringen in den Kernbereich privater Lebensgestaltung im Rahmen von Überwachungsmaßnahmen nicht für jeden Fall von vornherein ausgeschlossen werden (vgl. BVerfGE 120, 274 <337 f.>). Die Verfassung verlangt jedoch für die Ausgestaltung der Überwachungsbefugnisse die Achtung des Kernbereichs als eine strikte, nicht frei durch Einzelfallerwägungen überwindbare Grenze.

aa) Absolut ausgeschlossen ist damit zunächst, den Kernbereich zum Ziel staatlicher Ermittlungen zu machen und diesbezügliche Informationen in irgendeiner Weise zu verwerten oder sonst zur Grundlage der weiteren Ermittlungen zu nehmen. Auch wenn hierdurch weiterführende Erkenntnisse erlangt werden können, scheidet ein gezielter Zugriff auf die höchstprivate Sphäre - zu der freilich nicht die Besprechung von Straftaten gehört (siehe oben C IV 3 a) - von vornherein aus. Insbesondere darf der Kernbereichsschutz nicht unter den Vorbehalt einer Abwägung im Einzelfall gestellt werden. 125

bb) Des Weiteren folgt hieraus, dass bei der Durchführung von Überwachungsmaßnahmen dem Kernbereichsschutz auf zwei Ebenen Rechnung getragen werden muss. Zum einen sind auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zum anderen sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren (vgl. BVerfGE 120, 274 <337 ff.>; 129, 208 <245 f.>). 126

d) In diesem Rahmen kann der Gesetzgeber den Schutz des Kernbereichs privater Lebensgestaltung in Abhängigkeit von der Art der Befugnis und deren Nähe zum absolut geschützten Bereich privater Lebensgestaltung für die verschiedenen Überwachungsmaßnahmen verschieden ausgestalten (vgl. BVerfGE 120, 274 <337>; 129, 208 <245>). Er hat hierbei jedoch auf beiden Ebenen Vorkehrungen zu treffen. 127

Auf der Ebene der Datenerhebung ist bei verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt (vgl. BVerfGE 109, 279 <318, 320, 324>; 113, 348 <391 f.>; 120, 274 <338>). Für Gespräche mit Personen höchstpersönlichen Vertrauens kann unter 128

Umständen, die typischerweise auf eine vertrauliche Situation hinweisen, die Vermutung geboten sein, dass sie dem Kernbereichsschutz unterfallen und nicht überwacht werden dürfen (vgl. BVerfGE 109, 279 <321 ff.>; 129, 208 <247>). Eine solche Vermutung darf der Gesetzgeber als widerleglich ausgestalten und dabei insbesondere darauf abstellen, ob im Einzelfall Anhaltspunkte bestehen, dass in dem Gespräch Straftaten besprochen werden. Demgegenüber reicht es zur Widerlegung der Höchstvertraulichkeit eines Gespräches nicht, dass neben höchstpersönlichen Fragen auch Alltägliches zur Sprache kommen wird (vgl. BVerfGE 109, 279 <330>). In jedem Fall ist der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt (vgl. BVerfGE 109, 279 <318, 324, 331>; 113, 348 <392>; 120, 274 <338>).

Auf der Ebene der Auswertung und Verwertung hat der Gesetzgeber für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor deren Verwendung durch die Sicherheitsbehörden herausfiltert (vgl. BVerfGE 109, 279 <331 f., 333 f.>; 120, 274 <338 f.>). Die von Verfassungs wegen geforderten verfahrensrechtlichen Sicherungen gebieten jedoch nicht in allen Fallkonstellationen, dass neben staatlichen Ermittlungsbehörden weitere unabhängige Stellen eingerichtet werden (vgl. BVerfGE 129, 208 <250>). Die Erforderlichkeit einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab. Dabei kann auf die Sichtung durch eine unabhängige Stelle umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt. Unberührt bleibt auch die Möglichkeit des Gesetzgebers, die notwendigen Regelungen zu treffen, um den Ermittlungsbehörden für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen. In jedem Fall hat der Gesetzgeber die sofortige Löschung von gegebenenfalls erfassten höchstpersönlichen Daten vorzusehen und jegliche Verwendung auszuschließen. Die Löschung ist in einer Weise zu protokollieren, die eine spätere Kontrolle ermöglicht (vgl. BVerfGE 109, 279 <318 f., 332 f.>; 113, 348 <392>; 120, 274 <337, 339>). 129

4. Eigene verfassungsrechtliche Grenzen ergeben sich hinsichtlich des Zusammenwirkens der verschiedenen Überwachungsmaßnahmen. Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewe- 130

gungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können (vgl. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; stRspr). Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem „additiven“ Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt (vgl. BVerfGE 112, 304 <319 f.>). Die aus dem Gebot der Zweckbindung folgenden Grenzen für einen Austausch von Daten zwischen den Behörden bleiben hierdurch unberührt (siehe unten D I).

5. Eigene verfassungsrechtliche Grenzen heimlicher Überwachungsmaßnahmen können sich unter Verhältnismäßigkeitsgesichtspunkten gegenüber bestimmten Berufs- und anderen Personengruppen ergeben, deren Tätigkeit von Verfassungs wegen eine besondere Vertraulichkeit voraussetzt. Der Gesetzgeber muss gewährleisten, dass die Behörden bei der Anordnung und Durchführung von Überwachungsmaßnahmen solche Grenzen beachten. 131

Angesichts der schon grundsätzlich hohen Anforderungen an die Anordnung solcher Maßnahmen und der großen Bedeutung einer effektiven Terrorismusabwehr für die demokratische und freiheitliche Ordnung (vgl. BVerfGE 115, 320 <357 f.>; 120, 274 <319>; 133, 277 <333 f. Rn. 133>), die Sicherheit der Menschen sowie mit Blick auf die Vielgestaltigkeit der in Ausgleich zu bringenden Gesichtspunkte und zugleich die Notwendigkeit, Missbrauchsmöglichkeiten zu begrenzen, ist der Gesetzgeber in der Regel nicht verpflichtet, bestimmte Personengruppen von Überwachungsmaßnahmen von vornherein gänzlich auszunehmen (vgl. BVerfGE 129, 208 <262 ff.>). Vielmehr kann er den Schutz der Vertraulichkeit jedenfalls in der Regel von einer Abwägung im Einzelfall abhängig machen. 132

Bei der Abgrenzung und Ausgestaltung der zu schützenden Vertraulichkeitsbeziehungen verbleibt dem Gesetzgeber ein Gestaltungsspielraum. Er hat das öffentliche Interesse an einer effektiven Gefahrenabwehr in Ausgleich zu bringen mit dem Gewicht, das die Maßnahmen gegenüber auf besondere Vertraulichkeit verwiesenen Berufsgeheimnisträgern entfalten. Dabei hat er neben dem spezifischen Eingriffsgewicht, das diese Maßnahmen gegenüber solchen Personen hinsichtlich der insoweit allgemein maßgeblichen Grundrechte entfalten, auch zu berücksichtigen, wie sie sich auf weitere Grundrechte, insbesondere auf Art. 4 Abs. 1, Art. 5 Abs. 1 und Art. 12 Abs. 1 GG oder das freie Mandat nach Art. 38 Abs. 1 GG auswirken. Sofern er hierbei einzelne Berufsgruppen einem strikteren 133

Schutz unterstellt, müssen diese in Bezug auf die Überwachungsziele geeignet abgegrenzt sein.

6. Der Verhältnismäßigkeitsgrundsatz stellt auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (BVerfGE 133, 277 <365 Rn. 204>; vgl. auch BVerfGE 65, 1 <44 ff.>; 100, 313 <361, 364>; 109, 279 <363 f.>; 125, 260 <334 ff.>; stRspr; vgl. ähnlich auch Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25. Januar 2012, KOM[2012] 10 endgültig - Stand nach Abschluss des Trilogs, 16. Dezember 2015: 15174/15; Stand 28. Januar 2016: 5463/16, Anlage). Die insoweit geltenden Anforderungen ergeben sich aus dem jeweiligen Grundrecht in Verbindung mit Art. 19 Abs. 4 GG (vgl. BVerfGE 125, 260 <335>; 133, 277 <366 Rn. 206>). 134

Transparenz der Datenerhebung und -verarbeitung soll dazu beitragen, dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt (BVerfGE 133, 277 <366 Rn. 206>). Durch sie soll, soweit möglich, den Betroffenen subjektiver Rechtsschutz ermöglicht und zugleich einer diffusen Bedrohlichkeit geheimer staatlicher Beobachtung entgegengewirkt werden (vgl. BVerfGE 125, 260 <335>; ähnlich EuGH, Urteil vom 8. April 2014 - C-293/12, C-594/12 -, Digital Rights Ireland Ldt/Minister for Communications, Marine and Natural Resources u.a., NJW 2014, S. 2169 <2170>, Rn. 37). Je weniger die Gewährleistung subjektiven Rechtsschutzes möglich ist, desto größere Bedeutung erhalten dabei Anforderungen an eine wirksame aufsichtliche Kontrolle und an die Transparenz des Behördenhandelns gegenüber der Öffentlichkeit (vgl. BVerfGE 133, 277 <366 f. Rn. 207>). 135

a) Zu den Anforderungen an die verhältnismäßige Ausgestaltung der fraglichen Überwachungsmaßnahmen gehört die gesetzliche Anordnung von Benachrichtigungspflichten. Da solche Maßnahmen, um ihren Zweck zu erreichen, heimlich durchgeführt werden müssen, hat der Gesetzgeber zur Gewährleistung subjektiven Rechtsschutzes im Sinne des Art. 19 Abs. 4 GG vorzusehen, dass die Betroffenen zumindest nachträglich von den Überwachungsmaßnahmen grundsätzlich in Kenntnis zu setzen sind. Ausnahmen kann er in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Sie sind jedoch auf das unbedingt Erforderliche zu beschränken (BVerfGE 125, 260 <336>). Denkbar sind 136

Ausnahmen von den Benachrichtigungspflichten etwa, wenn die Kenntnis von der Maßnahme dazu führen würde, dass diese ihren Zweck verfehlt, wenn die Benachrichtigung nicht ohne Gefährdung von Leib und Leben einer Person geschehen kann, oder wenn ihr überwiegende Belange einer betroffenen Person entgegenstehen, etwa weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde. Liegen zwingende Gründe vor, die eine nachträgliche Benachrichtigung ausschließen, ist dies richterlich zu bestätigen und in regelmäßigen Abständen zu prüfen (BVerfGE 125, 260 <336 f.>).

b) Zur Flankierung von informationsbezogenen Eingriffen, deren Vornahme oder Umfang die Betroffenen nicht sicher abschätzen können, hat der Gesetzgeber überdies Auskunftsrechte vorzusehen. Einschränkungen sind nur zulässig, wenn sie gegenläufigen Interessen von größerem Gewicht dienen. Gesetzliche Ausschlusstatbestände müssen sicherstellen, dass die betroffenen Interessen einander umfassend und auch mit Blick auf den Einzelfall zugeordnet werden (BVerfGE 120, 351 <365>). Wenn dann aber dennoch die praktische Wirksamkeit solcher Auskunftsrechte angesichts der Art der Aufgabenwahrnehmung - wie bei der heimlichen Datenverarbeitung zur Abwehr von Gefahren durch den internationalen Terrorismus - sehr begrenzt bleibt, ist das verfassungsrechtlich hinnehmbar (vgl. BVerfGE 133, 277 <367 f. Rn. 209 ff.>). 137

c) Eine verhältnismäßige Ausgestaltung der Überwachungsmaßnahmen verlangt im Lichte des Art. 19 Abs. 4 GG außerdem, dass die Betroffenen nach Benachrichtigung in zumutbarer Weise eine gerichtliche Rechtmäßigkeitskontrolle erwirken können (vgl. hierzu auch Art. 51, Art. 52 des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, a.a.O.). 138

Überdies setzt eine verhältnismäßige Ausgestaltung wirksame Sanktionen bei Rechtsverletzungen voraus. Würden auch schwere Verletzungen der Eingriffsvoraussetzungen im Ergebnis sanktionslos bleiben mit der Folge, dass der Schutz des Persönlichkeitsrechts angesichts der immateriellen Natur dieses Rechts verkümmern würde, widerspräche dies der Verpflichtung der staatlichen Gewalt, die Entfaltung der Persönlichkeit wirksam zu schützen. Dies kann insbesondere der Fall sein, wenn eine unberechtigte Erhebung oder Verwendung der Daten mangels materiellen Schadens regelmäßig ohne einen der Genugtuung der Betroffe- 139

nen dienenden Ausgleich bliebe. Der Gesetzgeber hat diesbezüglich allerdings einen weiten Gestaltungsspielraum (vgl. BVerfGE 125, 260 <339 f.> m.w.N.).

d) Weil eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen (vgl. BVerfGE 133, 277 <369 Rn. 214>). 140

Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt zunächst eine mit wirksamen Befugnissen ausgestattete Stelle - wie nach geltendem Recht die Bundesdatenschutzbeauftragte - voraus (vgl. grundlegend BVerfGE 65, 1 <46>). Dazu ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten der Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält (BVerfGE 133, 277 <370 Rn. 215>). Angesichts 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 der Ausstattung der Aufsichtsinstanz zu berücksichtigen (vgl. BVerfGE 133, 277 <370 f. Rn. 217>). Die Gewährleistung der verfassungsrechtlichen Anforderungen einer wirksamen aufsichtlichen Kontrolle obliegt dem Gesetzgeber und den Behörden gemeinsam (vgl. BVerfGE 133, 277 <371 Rn. 220>). 141

e) Zur Gewährleistung von Transparenz und Kontrolle bedarf es schließlich einer gesetzlichen Regelung von Berichtspflichten. 142

Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie 143

sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen (vgl. BVerfGE 133, 277 <372 Rn. 221 f.>).

7. Zu den übergreifenden Verhältnismäßigkeitsanforderungen gehört auch die Regelung von Löschungspflichten (vgl. BVerfGE 65, 1 <46>; 133, 277 <366 Rn. 206>; stRspr). Mit ihnen ist sicherzustellen, dass eine Verwendung personenbezogener Daten auf die die Datenverarbeitung rechtfertigenden Zwecke begrenzt bleibt und nach deren Erledigung nicht mehr möglich ist. Die Löschung der Daten ist zur Gewährleistung von Transparenz und Kontrolle zu protokollieren. 144

V.

Die angegriffenen polizeirechtlichen Überwachungsbefugnisse genügen den vorstehend dargelegten verfassungsrechtlichen Anforderungen hinsichtlich ihrer jeweiligen Eingriffsvoraussetzungen in verschiedener Hinsicht nicht. 145

1. Nur teilweise mit der Verfassung vereinbar ist § 20g Abs. 1 bis 3 BKAG. 146

a) § 20g Abs. 1 BKAG erlaubt die Überwachung außerhalb von Wohnungen unter dem Einsatz besonderer, in § 20g Abs. 2 BKAG näher bestimmten Mittel der Datenerhebung. Er ermächtigt das Bundeskriminalamt damit zu Eingriffen in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). 147

Die Vorschrift ermächtigt demgegenüber nicht auch zu Eingriffen in Art. 10 Abs. 1 GG. Anders als die §§ 20l, 20m BKAG erlauben die in § 20g Abs. 2 BKAG genannten Mittel keine Maßnahmen, die in das Telekommunikationsgeheimnis eingreifen. Sie gestatten auch keine Maßnahmen, die in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen, wie eine Manipulation von solchen Systemen zur Observation. Auch ist die Vorschrift nicht an Art. 13 Abs. 1 GG zu messen. Sie berechtigt allein zur Überwachung außerhalb von Wohnungen (vgl. BTDrucks 16/9588, S. 23) und setzt damit voraus, dass auf sie gestützte Überwachungsmaßnahmen, wie gegebenenfalls auch technisch sichergestellt werden muss, an der Wohnungstür enden. Die darüber hinausgehenden Befugnisse des § 20g Abs. 4 BKAG sind nicht Gegenstand des vorliegenden Verfahrens. 148

b) Hinsichtlich seines Eingriffsgewichts deckt § 20g Abs. 1, 2 BKAG ein weites Spektrum ab. Es umfasst hierbei auch gravierende Eingriffe. 149

Die Vorschrift erlaubt Überwachungen außerhalb von Wohnungen mit den in Absatz 2 genannten Mitteln. Hierzu gehören insbesondere die längerfristige Observation, die Erstellung von heimlichen Bildaufzeichnungen, das Abhören des nichtöffentlich gesprochenen Wortes, das Nachverfolgen mittels Peilsendern oder der Einsatz von Vertrauenspersonen und Verdeckten Ermittlern. 150

Das Eingriffsgewicht dieser Maßnahmen kann sehr unterschiedlich sein. Es reicht von eher geringeren bis mittleren Eingriffen, wie dem Erstellen einzelner Fotos oder der zeitlich begrenzten schlichten Beobachtung, bis zu schweren Eingriffen wie dem langfristig-dauerhaften heimlichen Aufzeichnen von Wort und Bild einer Person. Insbesondere wenn diese Maßnahmen gebündelt durchgeführt werden und dabei unter Nutzung moderner Technik darauf zielen, möglichst alle Äußerungen und Bewegungen zu erfassen und bildlich wie akustisch festzuhalten, können sie tief in die Privatsphäre eindringen und ein besonders schweres Eingriffsgewicht erlangen. 151

Ebenso wie die Abwendung von anderen gewichtigen Rechtsgutverletzungen oder die Verfolgung von erheblichen Straftaten kann das öffentliche Interesse an einer effektiven Terrorismusabwehr solche Eingriffe jedoch rechtfertigen (siehe oben C II 3 a). Vorausgesetzt ist dabei, dass sie verhältnismäßig ausgestaltet sind. Das ist hier allerdings nur teilweise der Fall. 152

c) Nicht zu beanstanden ist die an das allgemeine Sicherheitsrecht angelehnte Regelung der Eingriffsvoraussetzungen in § 20g Abs. 1 Nr. 1, Abs. 2 BKAG. 153

aa) Die Vorschrift begrenzt Überwachungsmaßnahmen auf den Schutz hinreichend gewichtiger Rechtsgüter. 154

Dies gilt zunächst insoweit, als sie Maßnahmen zum Schutz des Bestandes oder der Sicherheit des Staates oder von Leib, Leben oder Freiheit einer Person erlaubt. Nichts anderes gilt aber auch, soweit sie Überwachungsmaßnahmen zum Schutz von Sachen von bedeutendem Wert gestattet, deren Erhaltung im öffentlichen Interesse geboten ist. Bei verständiger Auslegung kann hierunter nicht schon allein der Schutz von bedeutsamen Sachwerten verstanden werden. Gemeint sind hier im gesetzlichen Zusammenhang mit der Terrorismusabwehr vielmehr etwa 155

wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (vgl. BVerfGE 133, 277 <365 Rn. 203>).

Die Eingriffsbefugnisse sind dabei gemäß § 20g Abs. 1 Nr. 1 BKAG darüber hinaus weiter dadurch eingeschränkt, dass Maßnahmen zum Schutz der genannten Rechtsgüter nur erlaubt sind, wenn diese durch eine der in § 4a Abs. 1 Satz 2 BKAG genannten Straftaten bedroht sind. Dies ergibt sich schon aus der Aufgabennorm des § 4a BKAG selbst, in die die Befugnisse der §§ 20a ff. BKAG eingebunden sind. Die Eingriffsbefugnisse werden so auf die Abwehr von Gefahren des internationalen Terrorismus begrenzt. Dabei verweist der Gesetzgeber weder lediglich auf einen unbestimmten Begriff des Terrorismus noch pauschal auf § 129a StGB als solchen, sondern bestimmt, dass die Gefahr für die Rechtsgüter von bestimmten, in § 129a StGB einzeln festgelegten und besonders qualifizierten Straftaten ausgehen muss. Die Norm ist so auf den Schutz von besonders gewichtigen Rechtsgütern vor besonders bedrohlichen Angriffen begrenzt. Ungeachtet der Frage, wo diesbezüglich die verfassungsrechtlichen Grenzen für solche Maßnahmen im Allgemeinen - etwa auch für entsprechende Befugnisse nach den Landespolizeigesetzen - liegen, wird damit jedenfalls vorliegend den Verhältnismäßigkeitsanforderungen genügt. 156

Demgegenüber kann die in § 20g Abs. 1 Nr. 1 BKAG erfolgte Bezugnahme auf die in § 20a Abs. 2 BKAG enthaltene Legaldefinition der Gefahr nicht dahingehend verstanden werden, dass § 20a Abs. 2 BKAG die Begrenzung der Rechtsgüter in § 20g Abs. 1 Nr. 1 BKAG überspielt und schon für sich jede Gefahr für die öffentliche Sicherheit im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2 BKAG ausreichen lässt. Zwar konkretisiert § 20a Abs. 2 BKAG den Gefahrenbegriff für alle nachfolgenden Befugnisse hinsichtlich des Erfordernisses der Einzelfallbezogenheit. Er hat bei verständiger und verfassungsrechtlich gebotener Auslegung jedoch nicht die Funktion, die in den Einzelbefugnissen spezifisch begrenzten Anforderungen an den Rechtsgüterschutz aufzuheben. 157

bb) § 20g Abs. 1 Nr. 1 BKAG setzt auch einen hinreichend konkretisierten Anlass für die Anordnung der Maßnahmen voraus. Die Vorschrift stellt auf das Vorliegen einer Gefahr ab. Gemäß § 20a Abs. 2 BKAG ist hierunter eine „im Einzelfall bestehende Gefahr“ und damit eine konkrete Gefahr im Sinne des allgemeinen Sicherheitsrechts zu verstehen. Angesichts der Konturen, die dieser Begriff durch die fachgerichtliche Rechtsprechung erhalten hat, sind hiergegen unter Bestimmtheits- und Verhältnismäßigkeitsgesichtspunkten keine Bedenken zu erheben. 158

cc) Keine verfassungsrechtlichen Bedenken bestehen weiter gegen die in § 20g Abs. 1 Nr. 1 BKAG vorgenommene Bestimmung der Adressaten der Maßnahmen unter Rückgriff auf §§ 17, 18 und 20 BPolG und damit die Grundsätze der polizeirechtlichen Verantwortlichkeit. Der Gesetzgeber darf auch insoweit auf die Figuren des allgemeinen Sicherheitsrechts zurückgreifen. Ob hierbei im konkreten Kontext der Terrorismusabwehr durch das Bundeskriminalamt die Zustandsverantwortlichkeit gemäß § 18 BPolG praktisch wirksam werden kann, oder ob die Vorschrift insoweit im Ergebnis leerläuft (vgl. Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 75 ff.), ist verfassungsrechtlich unerheblich. Bezogen auf die hier in Frage stehenden Befugnisse des § 20g Abs. 1, 2 BKAG, die weder in Art. 10 Abs. 1 GG noch in die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme noch in Art. 13 Abs. 1 GG eingreifen, ist auch nicht zu beanstanden, dass eine Überwachung gemäß § 20 BPolG unter den Voraussetzungen der Notstandspflicht auch gegen den Nichtstörer angeordnet werden darf. Die diesbezüglichen Vorschriften sind eng gefasst und streng auszulegen. Erforderlich ist das Vorliegen einer gegenwärtigen Gefahr für die in § 20g Abs. 1 Satz 1 BKAG genannten Rechtsgüter, für deren Abwehr die Maßnahme unmittelbar zielführend sein muss. Unter diesen Maßgaben ist eine Inanspruchnahme des Nichtstörers nicht unverhältnismäßig. Insbesondere öffnet sie damit auch keinen Weg, die Voraussetzungen für die Inanspruchnahme von Kontaktpersonen zu umgehen. 159

dd) Zu unbestimmt oder unverhältnismäßig ist die Vorschrift auch nicht hinsichtlich der in § 20g Abs. 2 BKAG definierten Mittel der Überwachung. Allerdings umfassen diese - ungeachtet ihres unterschiedlichen Eingriffsgewichts im Einzelnen - auch sehr schwerwiegende Grundrechtseingriffe, wie etwa die Möglichkeit von langfristig angelegten Wort- und Bildaufzeichnungen privater Gespräche und Situationen oder das Ausnutzen von Vertrauen durch Verdeckte Ermittler oder Vertrauenspersonen. Zur Abwehr der in § 20g Abs. 1 Nr. 1 BKAG genannten besonders gewichtigen Gefahren können jedoch auch diese schwerwiegenden Eingriffe - nach Maßgabe einer im Einzelfall vorzunehmenden Prüfung der Verhältnismäßigkeit - verfassungsrechtlich gerechtfertigt sein. 160

Keinen Bedenken unterliegt auch die technikoffene Bestimmung der Überwachungsmittel in § 20g Abs. 2 Nr. 2 und 3 BKAG. Der Gesetzgeber ist nicht dazu verpflichtet, die erlaubten Mittel für Überwachungen auf den jeweiligen technischen Stand und Zeitpunkt des Gesetzgebungsverfahrens zu begrenzen. Soweit die Art der erlaubten Überwachung aus der Norm hinreichend erkennbar ist, kann er in die Ermächtigung auch künftige technische Entwicklungen einbeziehen. Al- 161

lerdings bleibt die Ermächtigung, wie bei ihrer Auslegung zu beachten ist, auf solche technische Mittel beschränkt, die in ihrer Qualität und in Blick auf das Eingriffsgewicht den bereits bekannten Mitteln entsprechen. Im Übrigen obliegt es dem Gesetzgeber, die technische Entwicklung insoweit aufmerksam zu beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe korrigierend einzugreifen (vgl. BVerfGE 112, 304 <316 f.>).

d) Mit den verfassungsrechtlichen Anforderungen nicht zu vereinbaren ist hingegen § 20g Abs. 1 Nr. 2 BKAG. Die Eingriffsvoraussetzungen genügen weder dem Grundsatz der Bestimmtheit noch dem Grundsatz der Verhältnismäßigkeit im engeren Sinne. 162

aa) § 20g Abs. 1 Nr. 2 BKAG ergänzt die auf die Gefahrenabwehr begrenzte Eingriffsgrundlage des § 20g Abs. 1 Nr. 1 BKAG und soll nach der Vorstellung des Gesetzgebers schon früher ansetzen und der Straftatenverhütung dienen. 163

Nach den oben dargelegten Maßstäben ist der Gesetzgeber hieran nicht grundsätzlich gehindert und zwingt ihn die Verfassung nicht, Sicherheitsmaßnahmen auf die Abwehr von - nach tradiertem Verständnis - konkreten Gefahren zu beschränken. Allerdings bedarf es aber auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (vgl. BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>; 120, 274 <328 f.>; 125, 260 <330>). In Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht (siehe oben C IV 1 b). Die diesbezüglichen Anforderungen sind normenklar zu regeln. 164

bb) Dem genügt § 20g Abs. 1 Nr. 2 BKAG nicht. Zwar knüpft die Vorschrift an eine mögliche Begehung terroristischer Straftaten an. Die diesbezüglichen Prognoseanforderungen sind hierbei jedoch nicht hinreichend gehaltvoll ausgestaltet. Die Vorschrift schließt nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft 165

terroristische Straftaten begeht. Damit gibt sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand und eröffnet Maßnahmen, die unverhältnismäßig weit sein können.

e) Verfassungsrechtlich nicht zu beanstanden ist bei verfassungskonformer Auslegung demgegenüber § 20g Abs. 1 Nr. 3 in Verbindung mit § 20b Abs. 2 Nr. 2 BKAG. 166

§ 20g Abs. 1 Nr. 3 BKAG erlaubt Maßnahmen auch gegenüber Kontakt- oder Begleitpersonen. Der Begriff der Kontakt- und Begleitpersonen wird dabei in § 20b Abs. 2 Nr. 2 BKAG eingegrenzt und ist bei sachgerechter Auslegung als zusammenfassende Bezeichnung allein der dort genannten Personengruppen zu verstehen. 167

In dieser Eingrenzung ist § 20g Abs. 1 Nr. 3 BKAG verfassungsrechtlich tragfähig. Der Gesetzgeber eröffnet hier nicht ins Blaue hinein die Möglichkeit der Überwachung des gesamten Umfelds einer Zielperson, um so - gestützt lediglich auf die Tatsache eines Kontaktes mit dieser - erst herauszufinden, ob sich hierüber weitere Ermittlungsansätze erschließen. Für die Anordnung von Maßnahmen gegenüber Dritten verlangt die Vorschrift vielmehr, dass diese eine besondere, in § 20b Abs. 2 Nr. 2 BKAG näher definierte Tatnähe aufweisen. Tatsachen, die die Annahme rechtfertigen, dass eines der in § 20b Abs. 2 Nr. 2 BKAG genannten Nähekriterien vorliegt, sind danach eine eigene, in den Gründen der Anordnung darzulegende Voraussetzung für entsprechende Maßnahmen. In dieser Ausgestaltung ist eine Regelung, die Überwachungsmaßnahmen auch gegenüber selbst nicht verantwortlichen Personen erlaubt, verfassungsrechtlich nicht zu beanstanden (vgl. BVerfGE 107, 299 <322 f.>; 113, 348 <380 f.>). Dem entspricht freilich, dass bei der Anwendung der Vorschrift die Voraussetzungen des § 20b Abs. 2 Nr. 2 BKAG nicht ihrerseits aus dem bloßen Kontakt oder der bloßen persönlichen Nähe des Betreffenden zur Zielperson hergeleitet werden können. 168

Keine Bedenken sind dabei auch gegen die Merkmale des § 20b Abs. 2 Nr. 2 a bis c BKAG im Einzelnen zu erheben. Freilich dürfen die Merkmale von Verfassungs wegen nicht entgrenzend weit verstanden werden, so dass sie jede Person einschlössen, die mit der Zielperson im weiten Vorfeld von etwaigen Straftaten in wirtschaftlichem Kontakt steht. Vielmehr begrenzt § 20b Abs. 2 Nr. 2 b BKAG die Vorteilsziehung auf die Verwertung der Tat und damit auf Früchte, die sich gerade aus deren Unrechtsgehalt ergeben, und verlangt auch § 20b Abs. 2 Nr. 2 c BKAG, dass die Instrumentalisierung des Betroffenen in einem engen 169

Konnex zur Tat selbst steht. Liegen diese Voraussetzungen vor, sind entsprechende Anordnungen verfassungsrechtlich gerechtfertigt. Dem steht nicht entgegen, dass damit Maßnahmen auch gegen gutgläubige Dritte gerichtet werden können, denen eine Gefahr nicht zugerechnet werden kann. Zwar liegt hierin ein besonders schwerer Eingriff, der jedoch als Inanspruchnahme für überragend wichtige Gemeinwohlinteressen - ähnlich wie Zeugen- oder Notstandspflichten - verfassungsrechtlich gerechtfertigt ist.

f) Nach dem Grundsatz der Verhältnismäßigkeit nicht in jeder Hinsicht tragfähig sind die verfahrensmäßigen Anforderungen in § 20g Abs. 3 BKAG. 170

aa) Keinen Bedenken unterliegt allerdings, dass die Überwachungsmaßnahmen nach dieser Vorschrift zwar jeweils nur für eine vertretbar begrenzte Zeit angeordnet werden dürfen, aber deren Verlängerung nicht durch eine Obergrenze beschränkt wird. Der Gesetzgeber konnte davon ausgehen, dass eine konkretisierte Gefahrenlage, wie sie für die Anordnung oder Verlängerung der Maßnahmen vorausgesetzt ist, in der Regel nicht für einen übermäßig langen Zeitraum vorliegt, so dass eine unverhältnismäßige Dauerüberwachung hierdurch im Allgemeinen nicht droht. Im Übrigen kann eine Begrenzung, auch wenn eine absolute Höchstdauer nicht ausdrücklich bestimmt ist, aus dem Grundsatz der Verhältnismäßigkeit im Einzelfall folgen, da mit zunehmender Dauer der Observationsmaßnahmen der Eingriff in das allgemeine Persönlichkeitsrecht immer intensiver wird und auch dazu führen kann, dass eine weitere Verlängerung verfassungsrechtlich nicht mehr zu rechtfertigen ist (vgl. BVerfGE 109, 279 <362>). 171

bb) Unter Verhältnismäßigkeitsgesichtspunkten unzureichend ist demgegenüber die Regelung des Richtervorbehalts in § 20g Abs. 3 BKAG. 172

§ 20g Abs. 3 BKAG sieht einen Richtervorbehalt unmittelbar für die erstmalige Anordnung der Maßnahme nur beim Einsatz Verdeckter Ermittler vor (vgl. § 20g Abs. 3 Satz 1 BKAG). In anderen Fällen erlaubt er die erstmalige Anordnung unmittelbar durch das Bundeskriminalamt selbst und fordert eine richterliche Entscheidung erst für deren etwaige Verlängerung (§ 20g Abs. 3 Satz 8 BKAG). Dies gilt einerseits für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes und den Einsatz von Vertrauenspersonen oder Verdeckten Ermittlern (§ 20g Abs. 2 Nr. 2 b, 4 und 5 BKAG) sowie anderseits für längerfristige Observationen (§ 20g Abs. 2 Nr. 1 BKAG), wobei auch die Fälle eingeschlossen sind, in denen diese mittels Bildaufzeichnungen oder dem Einsatz von technischen Mitteln wie Peilsendern (vgl. § 20g Abs. 2 Nr. 2 a, 3 BKAG) durchgeführt werden. 173

Diese Regelung genügt den verfassungsrechtlichen Anforderungen nur teilweise. Nicht zu beanstanden ist allerdings, dass für die Anfertigung von Bildaufnahmen sowie für nur kurzfristige Observationen - auch mittels Bildaufzeichnungen oder technischer Mittel wie Peilsender - ein Richtervorbehalt nicht vorgesehen ist. Bleiben die Überwachungsmaßnahmen in dieser Weise begrenzt, haben sie kein so großes Eingriffsgewicht, dass deren Anordnung durch einen Richter verfassungsrechtlich geboten ist (vgl. strenger für die Observation mittels GPS-Sender Supreme Court of the United States, United States v. Jones, 132 S. Ct. 945 [2012]; zur Überwachung eines Verdächtigen mittels GPS zurückhaltender wiederum EGMR, Uzun v. Deutschland, Entscheidung vom 2. September 2010, Nr. 35623/05, NJW 2011, S. 1333 <1336 f.>, zu Art. 8 EMRK). Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen im Sinne des § 20g Abs. 2 Nr. 1 BKAG längerfristig - zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender - durchgeführt werden, wenn nichtöffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss. Insoweit reicht es nicht, die Anordnung der Maßnahmen zunächst der Sicherheitsbehörde selbst zu überlassen und die disziplinierende Wirkung wegen des Erfordernisses einer richterlichen Entscheidung erst für deren Verlängerung - möglicherweise auf der Grundlage der so gewonnenen Erkenntnisse - vorzusehen. Soweit für diese Maßnahmen eine erstmalige Anordnung ohne richterliche Entscheidung vorgesehen ist, genügt § 20g BKAG einer verhältnismäßigen verfahrensrechtlichen Ausgestaltung nicht. 174

g) § 20g BKAG genügt schließlich auch insoweit nicht den verfassungsrechtlichen Anforderungen, als er keine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung enthält. 175

§ 20g BKAG ermächtigt zu Überwachungsmaßnahmen von verschiedener Qualität und Nähe zur Privatsphäre. Indem die Vorschrift dabei aber auch die Erlaubnis zu längerfristigen Bildaufzeichnungen und einem auf eine lange Zeit angelegten Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes umfasst, ermöglicht sie Überwachungsmaßnahmen, die typischerweise tief in die Privatsphäre eindringen können. Zwar handelt es sich bei diesen Maßnahmen immer um eine Überwachung außerhalb von Wohnungen. Das stellt aber nicht in Frage, dass auch insoweit - sei es im Auto, sei es abseits in einem Restaurant, sei es zurückgezogen bei einem Spaziergang - mit einiger Wahrscheinlichkeit höchstver- 176

trauliche Situationen erfasst werden können, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (vgl. Poscher, JZ 2009, S. 269 <271 f.>).

Die Vorschrift weist demnach hinsichtlich mancher Befugnisse eine Kernbereichsnähe auf, die eine ausdrückliche gesetzliche Regelung zum Schutz des Kernbereichs privater Lebensgestaltung erforderlich macht. Der Gesetzgeber hat hierzu in normenklarer Weise Schutzvorschriften sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der Datenauswertung und Datenverwertung vorzusehen (siehe oben C IV 3 c bb, d). An solchen Vorschriften fehlt es, so dass § 20g Abs. 1, 2 BKAG auch insoweit mit der Verfassung nicht zu vereinbaren sind. 177

2. § 20h BKAG genügt den verfassungsrechtlichen Anforderungen gleichfalls nur teilweise. 178

a) § 20h BKAG erlaubt die akustische und optische Überwachung in Wohnungen. Er greift damit in Art. 13 Abs. 1 GG ein. 179

Mit der Befugnis zur Wohnraumüberwachung ermächtigt die Vorschrift zu Grundrechtseingriffen, die besonders schwer wiegen. Sie erlaubt dem Staat auch in Räume einzudringen, die privater Rückzugsort des Einzelnen sind und einen engen Bezug zur Menschenwürde haben (vgl. BVerfGE 109, 279 <313 f.>). Dies schließt, wie sich aus Art. 13 Abs. 3, 4 GG ergibt, Überwachungsmaßnahmen nicht aus. Die Abwehr von Gefahren des internationalen Terrorismus kann solche Maßnahmen rechtfertigen (siehe oben C II 3 a). Sie stehen aber unter besonders strengen Anforderungen, die § 20h BKAG nicht in jeder Hinsicht erfüllt. 180

b) Keinen verfassungsrechtlichen Bedenken unterliegt § 20h Abs. 1, 2 BKAG allerdings insoweit, als er - in Bezug auf alle möglichen Adressaten übergreifend - die allgemeinen Voraussetzungen der Wohnraumüberwachung regelt. 181

aa) Die Vorschrift genügt zunächst insoweit den verfassungsrechtlichen Anforderungen, als sie Maßnahmen auf den Schutz besonders gewichtiger Rechtsgüter beschränkt, dabei das Vorliegen einer dringenden Gefahr erfordert und als Adressaten die Handlungs- und Zustandsverantwortlichen bestimmt. 182

§ 20h Abs. 1 BKAG erlaubt Wohnraumüberwachungen nur zum Schutz besonders gewichtiger Rechtsgüter. Die hier bestimmten Rechtsgüter sind von solchem Gewicht, dass sie auch geeignet sind, eine Wohnraumüberwachung zu rechtfertigen (siehe oben C IV 1 a). Das gilt bei einem hier geboten engen, auf den 183

Zusammenhang der Terrorismusabwehr bezogenen Verständnis auch für „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“ (vgl. BVerfGE 133, 277 <365 Rn. 203>).

bb) In Übereinstimmung mit Art. 13 Abs. 4 GG verlangt die Vorschrift weiter das Vorliegen einer dringenden Gefahr. Zu berücksichtigen sind hierfür sowohl das Ausmaß als auch die Wahrscheinlichkeit des zu erwartenden Schadens (vgl. BVerfGE 130, 1 <32>). An das Vorliegen einer dringenden Gefahr, deren Anforderungen über die einer konkreten Gefahr noch hinausgehen, sind strenge Anforderungen zu stellen (vgl. BVerwGE 47, 31 <40>; BGHSt 54, 69 <83 f.>). Damit ist ein unter Verhältnismäßigkeitsgesichtspunkten hinreichend konkreter Anlass für die Durchführung solcher Maßnahmen gewährleistet (siehe oben C IV 1 b). 184

cc) Unverhältnismäßig ist die Regelung auch nicht deshalb, weil sie sowohl die akustische als auch die optische Wohnraumüberwachung erlaubt. Dass die Verfassung eine optische Wohnraumüberwachung für Eingriffe zur Gefahrenabwehr nach Art. 13 Abs. 4 GG nicht schon grundsätzlich ausschließt, ergibt sich aus einem Umkehrschluss zu Art. 13 Abs. 3 GG. Allerdings hat die Verbindung von akustischer und optischer Überwachung ein wesentlich größeres Eingriffsgewicht als etwa nur eine akustische Überwachung und bedarf besonderer Rechtfertigung. Dementsprechend sind die Anforderungen an die Geeignetheit, Erforderlichkeit und Angemessenheit bei der Anordnung der Maßnahmen für jede der Überwachungsformen eigens und gegebenenfalls auch mit Blick auf deren Verbindung zu prüfen. Dabei reicht es für die zusätzliche Anordnung einer optischen Überwachung regelmäßig nicht, auf bloße Erleichterungen für die Zuordnung von Stimmen zu verweisen, sondern bedarf es gewichtiger, für den Erfolg der Überwachung maßgeblicher eigener Gründe. Diesen Anforderungen kann und muss im Rahmen der Gesetzesanwendung Rechnung getragen werden. § 20h Abs. 1 Nr. 1 und 2 BKAG, der die akustische und die optische Wohnraumüberwachung als eigene und damit auch eigens zu prüfende Überwachungsmaßnahmen ausgestaltet, bietet hierfür eine hinreichende Grundlage. 185

c) Teilweise unverhältnismäßig und mit der Verfassung nicht vereinbar ist demgegenüber die Bestimmung der möglichen Adressaten von Wohnraumüberwachungen. 186

aa) Keine Bedenken bestehen insoweit freilich gegen § 20h Abs. 1 Nr. 1 a BKAG, der zur Anordnung von Wohnraumüberwachungen gegen die polizeilich Verantwortlichen nach §§ 17, 18 BPolG als Zielpersonen ermächtigt (siehe oben C IV 1 c). 187

Nicht zu beanstanden ist gleichfalls, dass § 20h Abs. 2 BKAG dabei die Überwachung solcher Personen nicht nur in deren eigener Wohnung, sondern auch in der Wohnung Dritter erlaubt, wenn sich die Zielperson dort aufhält und Maßnahmen in der Wohnung der Zielperson allein nicht zur Abwehr der Gefahr führen werden. Allerdings hat das Bundesverfassungsgericht für solche Überwachungsmaßnahmen in Wohnungen Dritter eingrenzende Maßgaben zur Auslegung vorgeschrieben. Es bedarf insoweit eines konkretisierten Verdachts, dass sich die Zielperson zur Zeit der Maßnahme in der Wohnung des Dritten aufhält. Dies ist gegebenenfalls durch andere Maßnahmen, wie eine Observation, sicherzustellen. Nicht auf konkrete Anhaltspunkte gestützte Vermutungen für die Anwesenheit der Zielperson in der Wohnung des Dritten reichen für den Beginn der Maßnahme nicht aus (vgl. BVerfGE 109, 279 <356>). Darüber hinaus muss eine hinreichende Wahrscheinlichkeit bestehen, hierbei verfahrensrelevante Informationen zu gewinnen. Erforderlich sind auch insoweit tatsächliche Anhaltspunkte dafür, dass die Zielperson in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird. Bloße Vermutungen und eine Überwachung ins Blaue hinein, allein getragen von der Hoffnung auf Erkenntnisse, genügen nicht (vgl. BVerfGE 109, 279 <356 f.>). 188

bb) Verfassungsrechtlich tragfähig ist auch § 20h Abs. 1 Nr. 1 b BKAG, der eine Wohnraumüberwachung gegenüber Personen erlaubt, bei denen konkrete Vorbereitungshandlungen die Annahme der Begehung terroristischer Straftaten rechtfertigen. 189

Anders als in § 20g Abs. 1 Nr. 2 BKAG wird hier kein besonders weit ins Gefahrvorfeld vorverlagerter eigener Eingriffstatbestand geschaffen, sondern setzt die Vorschrift - im Einklang mit Art. 13 Abs. 4 GG - eine dringende Gefahr für qualifizierte Rechtsgüter voraus, für deren Abwehr die Überwachung erforderlich sein muss. Darüber hinaus ist auch der Kreis der Adressaten der Maßnahme in dieser Bestimmung hinreichend eingegrenzt: Indem die Vorschrift die Kenntnis von konkreten Vorbereitungshandlungen für - näher qualifizierte - terroristische Straftaten verlangt, setzt sie ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen voraus. Sie stellt damit auf einen den verfassungsrechtlichen Anforde- 190

rungen genügenden Anlass für die Durchführung solcher Maßnahmen ab (siehe oben C IV 1 b).

cc) Nicht mit Art. 13 Abs. 1, 4 GG vereinbar ist demgegenüber die Erlaubnis von Wohnraumüberwachungen auch gegenüber Kontakt- und Begleitpersonen (§ 20h Abs. 1 Nr. 1 c BKAG). Sie ist unverhältnismäßig. 191

Die Wohnraumüberwachung ist ein besonders schwerwiegender Eingriff, der tief in die Privatsphäre eindringt. Sie hat ihrer Grundtypik nach eine stärker belastende Wirkung als Überwachungsmaßnahmen außerhalb von Wohnungen oder auch als Maßnahmen der Telekommunikationsüberwachung und findet von ihrem Eingriffsgewicht nur bei Eingriffen in informationstechnische Systeme eine Entsprechung. Deshalb bleibt die Angemessenheit einer solchen Überwachungsmaßnahme nur gewahrt, wenn sie von vornherein ausschließlich auf Gespräche der gefahrenverantwortlichen Zielperson selbst gerichtet ist (vgl. BVerfGE 109, 279 <355>). Eine Erstreckung unmittelbar auf Dritte ist unverhältnismäßig und scheidet für einen solch gravierenden Eingriff aus (siehe oben C IV 1 c). 192

Unberührt bleibt hiervon, dass, soweit unvermeidbar, durch eine Wohnraumüberwachung in der Wohnung der Zielperson verfassungsrechtlich unbedenklich auch unbeteiligte Dritte erfasst werden dürfen (vgl. § 20h Abs. 2 Satz 3 BKAG) und zur Überwachung der Zielperson, wie dargelegt, sogar Wohnraumüberwachungen in Wohnungen Dritter durchgeführt werden dürfen. 193

d) Keinen verfassungsrechtlichen Bedenken unterliegt die Wohnraumüberwachung auch hinsichtlich ihrer verfahrensrechtlichen Ausgestaltung. Insbesondere ist sie durch einen Richter anzuordnen. Wenn das Gesetz dabei die Angabe der „wesentlichen Gründe“ verlangt (§ 20h Abs. 4 Nr. 4 BKAG), liegt hierin - wie in den entsprechenden anderen Vorschriften des Gesetzes auch (vgl. § 20k Abs. 6 Nr. 4 BKAG) - keine Zurücknahme der verfassungsrechtlichen Prüfungs- und Begründungspflichten (vgl. BVerfGE 109, 279 <359 f.>), sondern die Betonung, dass alle rechtlich maßgeblichen Gesichtspunkte tragfähig dargelegt werden müssen. 194

Verfassungsrechtlich unbedenklich ist auch das Fehlen einer zeitlichen Obergrenze gegenüber einer wiederholten Anordnung der Wohnraumüberwachung, da eine zeitliche Begrenzung gegebenenfalls einzelfallbezogen aus Verhältnismäßigkeitsgesichtspunkten herzuleiten ist (vgl. BVerfGE 109, 279 <362>). 195

e) Verfassungsrechtlich unzureichend ist demgegenüber die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung in § 20h Abs. 5 BKAG. Sie genügt den Anforderungen des Art. 13 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG nicht. 196

aa) Da Wohnraumüberwachungen besonders tief in die Privatsphäre und den persönlichen, zur Wahrung der Menschenwürde besonders wichtigen Rückzugsraum des Einzelnen eindringen können, sind ihnen gegenüber die Anforderungen an den Kernbereichsschutz besonders streng (vgl. BVerfGE 109, 279 <313 ff., 318 ff., 328 ff.>). 197

(1) Besondere Anforderungen gelten zum einen auf der Erhebungsebene. Bei der Prüfung, ob die Wahrscheinlichkeit einer Erfassung höchstprivater Situationen besteht, sind im Interesse der Effektivität des Kernbereichsschutzes Vermutungsregeln zugrunde zu legen (vgl. BVerfGE 109, 279 <320>). Danach gilt die Vermutung, dass Gespräche, die in Privaträumen mit Personen des besonderen persönlichen Vertrauens (siehe oben C IV 3 a) geführt werden, dem Kernbereich privater Lebensgestaltung unterfallen und nicht überwacht werden dürfen (vgl. BVerfGE 109, 279 <321 ff.>). Für Räume, in denen solche Gespräche zu erwarten sind, scheidet entsprechend auch eine automatische Dauerüberwachung aus (vgl. BVerfGE 109, 279 <324>). Diese Vermutung kann widerlegt werden, sofern für bestimmte Gespräche konkrete Anhaltspunkte vorliegen, dass sie im Sinne der oben dargelegten Maßstäbe einen unmittelbaren Straftatenbezug - der auch vorliegt, wenn sie mit höchstpersönlichen Inhalten durchsetzt sind - aufweisen oder ihnen insgesamt ein höchstvertraulicher Charakter fehlen wird. Hierfür reicht hingegen nicht schon die Prognose, dass sich in einem Gespräch höchstvertrauliche und alltägliche Fragen mischen werden (vgl. BVerfGE 109, 279 <330>; siehe oben C IV 3 a, d). 198

Besteht danach die Wahrscheinlichkeit, dass eine Überwachungsmaßnahme in den Kernbereich privater Lebensgestaltung eindringt, ist die Maßnahme zu unterlassen. Fehlen - auch unter Berücksichtigung der Vermutungsregeln - Anhaltspunkte für ein Eindringen in den höchstpersönlichen Privatbereich, dürfen die Maßnahmen demgegenüber durchgeführt werden. Wenn es dabei dennoch zur Erfassung höchstvertraulicher Situationen kommt, sind die Maßnahmen unverzüglich abzubrechen (vgl. BVerfGE 109, 279 <320, 323 f.>). Bestehen in dieser Lage über den höchstvertraulichen Charakter - etwa aus sprachlichen Gründen - Zweifel oder gibt es konkrete Anhaltspunkte, dass im Zusammenhang mit dem Aus- 199

tausch höchstprivater Gedanken auch Straftaten besprochen werden, kann die Überwachung in Form einer automatischen Aufzeichnung fortgeführt werden.

(2) Spezifische verfassungsrechtliche Anforderungen ergeben sich zum anderen aber auch auf der Auswertungs- und Verwertungsebene. Hier ist eine Sichtung der Ergebnisse der Überwachung durch eine unabhängige Stelle vorzusehen. Diese Sichtung dient sowohl der Rechtmäßigkeitskontrolle als auch dem Herausfiltern höchstvertraulicher Daten, so dass diese nach Möglichkeit der Sicherheitsbehörde gegenüber nicht offenbar werden. Dabei sind der unabhängigen Stelle Aufzeichnungen aus der Wohnraumüberwachung vollständig vorzulegen (vgl. BVerfGE 109, 279 <333 f.>; anders BVerfGK 11, 164 <178>). 200

Für den Fall, dass ungeachtet aller Schutzvorkehrungen dennoch kernbereichsrelevante Informationen erfasst werden, sind ein Verwertungsverbot und eine Löschungspflicht, einschließlich der Protokollierung der Löschung, vorzusehen (siehe oben C IV 3 c bb, d, 7). 201

bb) Hiervon ausgehend genügt § 20h Abs. 5 BKAG zwar den verfassungsrechtlichen Anforderungen auf der Erhebungsebene, nicht aber auf der Verwertungsebene. 202

(1) § 20h Abs. 5 Satz 1, 2, 3 und 5 BKAG ordnet der Sache nach an, dass bei Wohnraumüberwachungen eine Prüfung vorzunehmen ist, ob kernbereichsrelevante Informationen erfasst werden. Indem er die Überwachung nur bei der prognosegestützten Annahme erlaubt, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden, und den Abbruch der Maßnahmen vorsieht, wenn es entgegen der Prognose im Zuge der Wohnraumüberwachung Anhaltspunkte dafür gibt, dass es doch zur Erfassung höchstprivater Informationen kommt, genügt die Vorschrift den verfassungsrechtlichen Anforderungen. Das gilt auch für die Erlaubnis zur automatischen Aufzeichnung nach Satz 3, die die Rechtmäßigkeitsvoraussetzungen von Satz 1 nicht aufhebt, sondern an die nach Satz 2 gebotene Unterbrechung des persönlichen Abhörens und Beobachtens anknüpft. Wenn in § 20h Abs. 5 Satz 1 BKAG kernbereichsrelevante „Äußerungen“ unter Schutz gestellt werden, ist dieses sachgerecht so zu verstehen, dass hierunter auch bildlich erfasste entsprechende Situationen fallen können. 203

(2) Nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen genügen indes die Regelungen zum Kernbereichsschutz auf der Verwertungsebene. Zwar 204

sieht das Gesetz eine Sichtung von Aufzeichnungen durch ein Gericht vor, jedoch begrenzt es diese Sichtung auf die automatischen Aufzeichnungen in Zweifelsfällen (§ 20h Abs. 5 Satz 4 BKAG). Der Gesetzgeber lässt sich insoweit ersichtlich von der Erwägung leiten, dass eine weitere unabhängige Sichtung nicht erforderlich ist, weil die Erfassung von höchstpersönlichen Informationen bei richtiger Gesetzesanwendung auf der Erhebungsstufe durch § 20h Abs. 5 Satz 1 und 2 BKAG ausgeschlossen wird. Damit lässt sich eine solche Beschränkung der unabhängigen Sichtung für Aufzeichnungen aus Wohnraumüberwachungen aber nicht rechtfertigen. Denn das Ziel solcher Sichtung liegt nicht allein in dem Herausfiltern von Zweifelsfällen, sondern auch in der Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen insgesamt. Dies aber gewährleistet die nur eingeschränkte Kontrollbefugnis des Gerichts gemäß § 20h Abs. 5 Satz 4 BKAG nicht. Freilich lässt das Grundgesetz dem Gesetzgeber Raum, bei der Ausgestaltung der im Grundsatz umfassenden Kontrollbefugnis für Ausnahmefälle bei Gefahr im Verzug besondere Regelungen vorzusehen.

In Übereinstimmung mit den verfassungsrechtlichen Anforderungen hat der Gesetzgeber demgegenüber ein Verwertungsverbot sowie die sofortige Löschung, einschließlich deren Protokollierung, für dennoch erfasste höchstpersönliche Daten geregelt. Verfassungswidrig ist jedoch die kurze Frist des § 20h Abs. 5 Satz 10 BKAG, innerhalb derer die Löschungsprotokolle zu löschen sind. Diese ist so kurz bemessen, dass während der Aufbewahrungszeit der Löschungsprotokolle typischerweise weder mit einer Kontrolle durch den Datenschutzbeauftragten noch durch die Betroffenen gerechnet werden kann und die Protokollierung der Löschung damit ihren Sinn verliert (vgl. Bäcker, a.a.O., S. 88; vgl. hierzu auch BVerfGE 100, 313 <400>; 109, 279 <332 f.>). Weil die Löschungsprotokolle selbst keine die Betroffenen belastenden Daten enthalten, kann diese kurze Frist insbesondere nicht mit deren Schutz gerechtfertigt werden. 205

3. Verfassungsrechtlich unbedenklich ist die Regelung der Eingriffsvoraussetzungen der Rasterfahndung gemäß § 20j BKAG. 206

Die Regelung begründet einen Eingriff in das Recht auf informationelle Selbstbestimmung. Sie ist hinsichtlich ihrer Eingriffsvoraussetzungen aber hinreichend bestimmt und verhältnismäßig ausgestaltet, so dass der Eingriff gerechtfertigt ist. Insbesondere wird die Rasterfahndung für den Schutz von hinreichend gewichtigen Rechtsgütern erlaubt (siehe oben C IV 1 a, V 1 c aa) und setzt gemäß § 20j Abs. 1 Satz 1 in Verbindung mit § 20a Abs. 2 BKAG eine konkrete Gefahr voraus. Verfassungsrechtlich nicht zu beanstanden ist insoweit auch das Regel- 207

beispiel in § 20j Abs. 1 Satz 1, 2. Halbsatz BKAG, mit dem der Gesetzgeber die geforderte Gefahrenlage exemplarisch konkretisiert. Die diesbezüglichen Anforderungen (vgl. BVerfGE 115, 320 <363 ff.>) bleiben hierdurch unberührt. Auch in verfahrensrechtlicher Hinsicht ist die Regelung verhältnismäßig ausgestaltet, insbesondere verlangt sie die Anordnung durch einen Richter.

4. § 20k BKAG ist bei verfassungskonformer Auslegung hinsichtlich seiner allgemeinen Eingriffsvoraussetzungen mit der Verfassung vereinbar. Nicht den verfassungsrechtlichen Anforderungen genügen demgegenüber die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung. 208

a) § 20k Abs. 1 BKAG ermächtigt zu einem Zugriff auf informationstechnische Systeme und erlaubt die geheime Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen oder vernetzten fremden Computern (wie etwa der sogenannten Cloud) abgelegte oder hinterlassene Daten erhoben und deren Verhalten im Netz nachvollzogen werden kann. Die Vorschrift begründet damit einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). 209

Mit dieser eigenständigen Ausprägung des allgemeinen Persönlichkeitsrechts trägt die Verfassung der heute weit in die Privatsphäre hineinreichenden Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung Rechnung (vgl. BVerfGE 120, 274 <302 ff.>). Tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente werden heute zunehmend in Dateiform angelegt, gespeichert und teilweise ausgetauscht. Weite Bereiche auch der höchstpersönlichen Kommunikation finden elektronisch mit Hilfe von Kommunikationsdiensten im Internet oder im Rahmen internetbasierter sozialer Netzwerke statt. Dabei befinden sich die Daten, auf deren Vertraulichkeit die Betroffenen angewiesen sind und auch vertrauen, in weitem Umfang nicht mehr nur auf eigenen informationstechnischen Systemen, sondern auf denen Dritter. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich 210

insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.

b) Die Anforderungen des § 20k Abs. 1, 2 BKAG für einen Zugriff auf informationstechnische Systeme genügen bei verfassungskonformer Auslegung den verfassungsrechtlichen Anforderungen. 211

aa) Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme stehen allerdings unter strengen Bedingungen (vgl. BVerfGE 120, 274 <322 ff., 326 ff.>). Insbesondere müssen die Maßnahmen davon abhängig sein, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen (vgl. BVerfGE 120, 274 <326, 328>). Dem genügt § 20k Abs. 1 BKAG. Die Vorschrift beschränkt die Maßnahmen auf den Schutz von hinreichend qualifizierten Rechtsgütern. Auch genügt sie den verfassungsrechtlichen Anforderungen insoweit, als sie in Satz 1 - in Verbindung mit § 20a Abs. 2 BKAG - auf das Vorliegen bestimmter Tatsachen abstellt, die die Annahme rechtfertigen, dass eine im Einzelfall bestehende Gefahr vorliegt. 212

Einer verfassungskonform einschränkenden Auslegung bedarf allerdings § 20k Abs. 1 Satz 2 BKAG. Die in dieser Vorschrift eröffnete Möglichkeit, auch schon im Vorfeld einer konkreten Gefahr Maßnahmen durchzuführen, wenn bestimmte Tatsachen auf eine im Einzelfall erst drohende Gefahr einer Begehung terroristischer Straftaten hinweisen, ist dahingehend auszulegen, dass Maßnahmen nur erlaubt sind, wenn die Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, und wenn erkennbar ist, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (vgl. BVerfGE 120, 274 <329>). Ausreichend ist insoweit auch, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten eines Betroffenen eine konkrete Wahrscheinlichkeit begründet, dass er solche Straftaten in überschaubarer Zukunft begehen wird (siehe oben C IV 1 b). 213

Da § 20k Abs. 1 Satz 2 BKAG in enger Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts formuliert ist (vgl. BVerfGE 120, 274 <329>), ist davon auszugehen, dass der Gesetzgeber hierauf Bezug nehmen wollte. Die Vorschrift ist damit noch einer verfassungskonformen Auslegung zugänglich. 214

bb) Im Übrigen genügt die Vorschrift hinsichtlich ihrer materiellen Eingriffsvoraussetzungen dem Verhältnismäßigkeitsgrundsatz. Insbesondere regelt § 20k Abs. 2 BKAG, dass die durch den Zugriff bedingten Veränderungen an dem informationstechnischen System zu minimieren, deren Nutzbarkeit durch Dritte zu vermeiden und sie nach Beendigung soweit möglich rückgängig zu machen sind (vgl. hierzu BVerfGE 120, 274 <325 f.>). Dass damit Folgeschäden nicht völlig ausgeschlossen werden können, macht die Maßnahme nicht von vornherein unverhältnismäßig. Zur Beachtung des Verhältnismäßigkeitsgrundsatzes im Einzelfall gehört auch, dass ein offener Zugriff auf die Datenbestände einer Zielperson vor einer heimlichen Infiltration grundsätzlich Vorrang hat. 215

c) Keine Bedenken bestehen weiter gegen die verfahrensrechtliche Ausgestaltung der Vorschrift (vgl. § 20k Abs. 5, 6 BKAG). Die Anordnung einer Maßnahme ist nur durch den Richter möglich und dabei sachhaltig zu begründen (vgl. BVerfGE 120, 274 <331 ff.>; siehe oben C IV 2). Die mögliche lange Dauer von drei Monaten, für die die Maßnahme angeordnet werden kann, ist verfassungsrechtlich allerdings nur mit der Maßgabe tragfähig, dass es sich hierbei für die jeweilige Anordnung um eine Obergrenze handelt und sich die tatsächliche Dauer der Anordnung nach einer Verhältnismäßigkeitsprüfung im Einzelfall richtet. 216

d) Nicht in jeder Hinsicht genügen demgegenüber die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung den verfassungsrechtlichen Anforderungen. 217

aa) Da der heimliche Zugriff auf informationstechnische Systeme typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich trägt und damit eine besondere Kernbereichsnähe aufweist, bedarf es ausdrücklicher gesetzlicher Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (vgl. BVerfGE 120, 274 <335 ff.>). Die diesbezüglichen Anforderungen sind dabei mit denen der Wohnraumüberwachung nicht in jeder Hinsicht identisch und verschieben den Schutz ein Stück weit von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene (vgl. BVerfGE 120, 274 <337>). Dies hat seinen Grund in dem spezifischen Charakter des Zugriffs auf informationstechnische Systeme. Schutzmaßnahmen vor Kernbereichsverletzungen zielen hier nicht pri- 218

mär auf die Verhinderung des Erfassens und Festhaltens eines nur flüchtigen, höchstvertraulichen Moments an einem Ort privater Zurückgezogenheit, sondern auf die Verhinderung des Auslesens höchstvertraulicher Informationen aus einem Gesamtdatenbestand von ohnehin digital vorliegenden Informationen, die in ihrer Gesamtheit typischerweise nicht schon als solche den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufweisen. Die Überwachung vollzieht sich hier nicht als ein zeitlich gegliedertes Geschehen an verschiedenen Orten, sondern als Zugriff mittels eines Ausforschungsprogramms, sodass - bezogen auf den Zugriff selbst - weitgehend die Alternativen von ganz oder gar nicht bestehen.

Dementsprechend sind die Anforderungen an den Kernbereichsschutz auf der Erhebungsebene ein Stück weit zurückgenommen. Allerdings ist auch hier vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen; können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt (vgl. BVerfGE 120, 274 <338>). 219

Können demgegenüber kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist ein Zugriff auf das informationstechnische System jedoch auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden. Der Gesetzgeber hat insofern dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür kommt dabei einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch das Bundeskriminalamt herausfiltert (vgl. BVerfGE 120, 274 <338 f.>). 220

bb) Diesen Anforderungen genügt § 20k Abs. 7 BKAG nur teilweise. 221

(1) Bei verfassungskonformer Auslegung nicht zu beanstanden sind allerdings die Regelungen auf der Ebene der Datenerhebung. Satz 2 der Vorschrift sieht in Einklang mit den genannten Anforderungen vor, dass alle technischen Möglichkeiten zur Vermeidung der Erhebung von kernbereichsrelevanten Informationen zu nutzen sind. Im Übrigen verbietet die Vorschrift den Zugriff auf informationstechnische Systeme dann nur, wenn durch sie „allein“ Informationen aus dem Kernbereich privater Lebensgestaltung erfasst werden. Das ist nach den dargelegten 222

Maßstäben verfassungsrechtlich tragfähig. Hierbei ist die Vorschrift von Verfassungs wegen allerdings so auszulegen, dass eine Kommunikation über Höchstvertrauliches nicht schon deshalb aus dem strikt zu schützenden Kernbereich herausfällt, weil sich in ihr höchstvertrauliche mit alltäglichen Informationen vermischen (vgl. BVerfGE 109, 279 <330>). Die Vorschrift ist insoweit in Einklang mit den verfassungsrechtlichen Schutzanforderungen des Kernbereichs privater Lebensgestaltung und dem hierbei zugrunde gelegten Begriffsverständnis zu verstehen und anzuwenden (siehe oben C IV 3 a, d).

(2) Demgegenüber fehlt es für die in Rede stehenden Maßnahmen an verfas- 223
sungsrechtlich hinreichenden Vorkehrungen auf der Ebene des nachgelagerten Kernbereichsschutzes. § 20k Abs. 7 Satz 3, 4 BKAG sieht keine hinreichend unabhängige Kontrolle vor.

Die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle 224
dient neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden. Dies setzt voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird. Hierdurch wird eine - durch gesonderte Verschwiegenheitspflichten abgesicherte - Hinzuziehung auch eines Bediensteten des Bundeskriminalamts zur Gewährleistung von ermittlungsspezifischem Fachverstand nicht ausgeschlossen. Ebenso kann darüber hinaus für die Sichtung auf technische Unterstützung - etwa auch zur Sprachmittlung - durch das Bundeskriminalamt zurückgegriffen werden. Die tatsächliche Durchführung und Entscheidungsverantwortung muss jedoch maßgeblich in den Händen von dem Bundeskriminalamt gegenüber unabhängigen Personen liegen.

Das sichert die derzeitige Regelung nicht. Sie überlässt die Sichtung im We- 225
sentlichen Bediensteten des Bundeskriminalamts selbst. Dass einer der Bediensteten als behördeninterner Datenschutzbeauftragter weisungsfrei ist, ändert daran ebenso wenig wie die Unterstellung der Sichtung unter eine allgemein bleibende „Sachleitung“ des anordnenden Gerichts.

Demgegenüber stellt § 20k Abs. 7 Satz 5 bis 7 BKAG die weiteren auf Verwer- 226
tungsebene gebotenen Vorkehrungen an einen wirksamen Kernbereichsschutz verfassungsrechtlich tragfähig sicher. Verfassungswidrig ist allerdings auch hier die übermäßig kurze Dauer für die Aufbewahrung der Löschungsprotokolle gemäß § 20k Abs. 7 Satz 8 BKAG (siehe oben C IV 3 d).

5. Nur teilweise mit der Verfassung zu vereinbaren ist § 20l BKAG. 227

a) § 20l BKAG regelt die Telekommunikationsüberwachung und begründet damit Eingriffe in Art. 10 Abs. 1 GG. An Art. 10 Abs. 1 GG ist dabei nicht nur § 20l Abs. 1 BKAG zu messen, der die herkömmliche Telekommunikationsüberwachung regelt, sondern auch § 20l Abs. 2 BKAG, der die Quellen-Telekommunikationsüberwachung erlaubt, sofern durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird. Zwar setzt diese technisch einen Zugriff auf das entsprechende informationstechnische System voraus. Jedoch erlaubt § 20l Abs. 2 BKAG ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Die Vorschrift hat damit lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und - ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems - eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Von daher ist sie nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern an Art. 10 Abs. 1 GG zu messen (vgl. BVerfGE 120, 274 <309>). 228

Eine Überwachung der Telekommunikation begründet Eingriffe, die schwer wiegen (vgl. BVerfGE 113, 348 <382>; 129, 208 <240>). Sie sind jedoch zur Abwehr des internationalen Terrorismus gerechtfertigt (siehe oben C II 3 a), sofern die Eingriffsgrundlagen im Einzelnen verhältnismäßig begrenzt sind. Dies ist durch § 20l BKAG nur teilweise sichergestellt. 229

b) § 20l Abs. 1 Nr. 1 bis 4 BKAG regelt verschiedene Eingriffstatbestände gegenüber verschiedenen Adressaten. Nicht alle genügen den verfassungsrechtlichen Anforderungen. 230

Keinen verfassungsrechtlichen Bedenken unterliegt freilich auch hier die auf den Schutz qualifizierter Rechtsgüter gerichtete und allein auf die Abwehr dringender Gefahren beschränkte Befugnis zur Überwachung gegenüber den polizeirechtlich Verantwortlichen gemäß § 20l Abs. 1 Nr. 1 BKAG. 231

Mit der Verfassung nicht zu vereinbaren ist demgegenüber die nicht näher eingeschränkte Erstreckung der Telekommunikationsüberwachung nach § 20l Abs. 1 Nr. 2 BKAG auf Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie terroristische Straftaten vorbereiten. Die Vorschrift, die über die Abwehr einer konkreten Gefahr hinaus die Eingriffsmöglichkeiten mit dem Ziel 232

der Straftatenverhütung vorverlagert, verstößt in ihrer konturenarmen offenen Fassung gegen den Bestimmtheitsgrundsatz und ist unverhältnismäßig weit. Es gelten insoweit die gleichen Erwägungen wie zu § 20g Abs. 1 Nr. 2 BKAG (siehe oben C V 1 d). Die geringfügigen Formulierungsunterschiede gegenüber jener Vorschrift begründen keinen substantiellen Unterschied. Dies erhellt auch die Gesetzesbegründung, die den Gehalt des § 20l Abs. 1 Nr. 2 BKAG zum Teil mit den Worten, die der Gesetzgeber in § 20g Abs. 1 Nr. 2 BKAG benutzt, paraphrasiert (vgl. BTDrucks 16/10121, S. 31). Soweit sich § 20l Abs. 2 BKAG auf diese Vorschrift bezieht, kann nichts anderes gelten.

Demgegenüber ist die mögliche Erstreckung der Telekommunikationsüberwachung auf Nachrichtenmittler gemäß § 20l Abs. 1 Nr. 3 und 4 BKAG bei verfassungskonformer Auslegung mit Art. 10 Abs. 1 GG vereinbar. Die Vorschrift, die in ihrer Formulierung eng an § 100a Abs. 3 StPO angelehnt ist, ist hinreichend auslegungsfähig und genügt den Anforderungen des Bestimmtheitsgrundsatzes. Wie die Regelung zu den Kontakt- und Begleitpersonen in § 20b Abs. 2 Nr. 2 BKAG erlaubt die Vorschrift nicht, Überwachungsmaßnahmen ins Blaue hinein auf alle Personen zu erstrecken, die mit der Zielperson Nachrichten ausgetauscht haben, sondern setzt eigene, in der Anordnung darzulegende Anhaltspunkte voraus, dass der Nachrichtenmittler von der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist. 233

c) Keinen durchgreifenden verfassungsrechtlichen Bedenken unterliegen die zusätzlichen weiteren Voraussetzungen, unter denen § 20l Abs. 2 BKAG subsidiär eine Quellen-Telekommunikationsüberwachung erlaubt. Insbesondere ist die Vorschrift nicht deshalb verfassungswidrig, weil sie, wie die Beschwerdeführer meinen, in ihrer Nummer 1 unerfüllbare Anforderungen stellt. Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit. Insoweit ist es nicht Aufgabe des vorliegenden Verfahrens, hierüber eine Klärung herbeizuführen. Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist. Andernfalls kommt allein ein Vorgehen auf der Grundlage des § 20k Abs. 1 BKAG in Betracht. Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein, liefe die Vorschrift folglich bis auf weiteres leer. Auch dies machte sie jedoch nicht widersprüchlich und verfassungswidrig, weil damit nicht ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können. Dabei schließt der für 234

die Quellen-Telekommunikationsüberwachung erforderliche Zugriff auf das informationstechnische System eine Erfüllung dieser Voraussetzungen auch nicht etwa schon begrifflich aus mit der Folge, dass die Vorschrift selbstwidersprüchlich wäre. Denn maßgeblich ist nicht, ob durch eine technisch aufwendige Änderung des Überwachungsprogramms selbst - sei es durch die Behörde, sei es durch Dritte - dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden kann, sondern ob das Programm so ausgestaltet ist, dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.

d) Verfahrensrechtlich normiert § 20l Abs. 3 BKAG in Einklang mit den verfassungsrechtlichen Anforderungen einen Richtervorbehalt (vgl. BVerfGE 125, 260 <337 f.>). Es fehlt indes eine gesetzliche Regelung, die - wie verfassungsrechtlich geboten (siehe oben C IV 2) - für die Anordnung der Telekommunikationsüberwachung eine Mitteilung der Gründe verlangt. Dies lässt sich auch nicht im Wege der verfassungskonformen Auslegung überwinden. Denn jedenfalls vor dem Hintergrund, dass das Gesetz in anderen Vorschriften eine Pflicht zur Begründung ausdrücklich anordnet (vgl. § 20g Abs. 3 Satz 6, § 20h Abs. 4, § 20k Abs. 6 BKAG), ist seine Deutung, nach der das Absehen von einer Regelung über die Mitteilung der Gründe hier als bewusste Entscheidung zu verstehen ist, nicht hinreichend sicher ausgeschlossen. 235

e) Die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung gemäß § 20l Abs. 6 BKAG sind mit der Verfassung im Wesentlichen vereinbar. 236

aa) Die Telekommunikationsüberwachung ist ein schwerer Eingriff, der eine besondere Kernbereichsnähe aufweist. Als inhaltliche Überwachung jeder Art von telekommunikationsbasiertem Austausch begründet sie typischerweise die Gefahr, auch höchstprivate Kommunikation, die dem Schutz des Kernbereichs privater Lebensgestaltung unterliegt, zu erfassen. Insofern bedarf es besonderer gesetzlicher Schutzvorkehrungen (vgl. BVerfGE 113, 348 <390 f.>; 129, 208 <245>). 237

Allerdings ist die Telekommunikationsüberwachung ihrem Gesamtcharakter nach nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung (vgl. BVerfGE 113, 348 <391>). Sie erfasst Kommunikation aller Art in allen Situationen, die immer technisch vermittelt ist. Höchstvertrauliche Kommunikation ist ein kleiner Teil 238

von ihr, der bei der Überwachung miterfasst zu werden droht, nicht aber - wie die Überwachung des Rückzugsbereichs der privaten Wohnung - typusprägend ist. Sie unterscheidet sich insoweit auch von Online-Durchsuchungen. Denn während diese oft gesamthaft über lange Zeit angesammelte Informationen einschließlich höchstprivater Aufzeichnungen erfassen und dabei unter Umständen durch deren Verknüpfung sowie das Nach- oder Mitverfolgen der Bewegungen im Internet auch geheim gehaltene Schwächen und Neigungen erschließen können, bezieht sich die Telekommunikationsüberwachung auf einzelne Akte unmittelbarer Kommunikation. Ihre Kernbereichsnähe beschränkt sich vor allem darauf, dass sie hierbei auch den höchstpersönlichen Austausch zwischen Vertrauenspersonen umfasst (vgl. BVerfGE 129, 208 <247>).

Dem kann der Gesetzgeber durch weniger strenge Anforderungen an den Kernbereichsschutz Rechnung tragen. Allerdings ist auch hier auf der Erhebungsstufe eine Prüfung geboten, ob die Wahrscheinlichkeit der Erfassung höchstprivater Gespräche besteht, deren Überwachung gegebenenfalls zu verbieten ist. Können solche nicht mit hinreichender Wahrscheinlichkeit identifiziert werden, darf die Überwachung durchgeführt werden - nach Maßgabe einer Verhältnismäßigkeitsprüfung im Einzelfall auch in Form einer automatischen Dauerüberwachung (vgl. BVerfGE 113, 348 <391 f.>; 129, 208 <245>). 239

Für den nachgelagerten Kernbereichsschutz sind zwar Verwertungsverbote und Löschungspflichten einschließlich einer diesbezüglichen Protokollierungspflicht vorzusehen, nicht aber in jedem Fall auch die Sichtung durch eine unabhängige Stelle (vgl. BVerfGE 129, 208 <249>). Der Gesetzgeber kann eine solche Sichtung für die Telekommunikationsüberwachung vielmehr davon abhängig machen, in welchem Ausmaß mit einer etwaigen Erfassung höchstprivater Informationen zu rechnen ist. Dies kann auch in Wechselwirkung mit den Schutzvorkehrungen auf der Ebene der Datenerhebung stehen. 240

Der Gesetzgeber hat hierbei nicht unerheblichen Gestaltungsspielraum. So hat das Bundesverfassungsgericht im Zusammenhang mit einer Regelung, die auf der Stufe der Datenerhebung wie vorliegend § 20l Abs. 6 Satz 1 BKAG ausgestaltet war, sogar den vollständigen Verzicht auf eine unabhängige Sichtung als verfassungsmäßig beurteilt; es hat dabei freilich das auf der Erhebungsstufe geregelte Verbot von Telekommunikationsüberwachungen bei einem ausschließlichen Kernbereichsbezug sehr streng verstanden und danach eine Telekommunikationsüberwachung immer schon dann als verboten angesehen, wenn den Behörden erkennbar ist, dass es sich um die Kommunikation zwischen Personen des 241

höchstpersönlichen Vertrauens handelt (vgl. BVerfGE 129, 208 <247>). Wenn in dieser Weise die Erfassung kernbereichsrelevanter Gespräche schon bei der Datenerhebung vermieden wird und so Zweifelsfälle weitgehend ausgeschlossen werden, ist eine Sichtung durch eine unabhängige Stelle für die Telekommunikationsüberwachung nicht erforderlich. Ein derart strenger Schutz auf der Erhebungsebene ist verfassungsrechtlich jedoch nicht geboten. Der Gesetzgeber muss nicht für jedes Gespräch zwischen Vertrauenspersonen ein Erhebungsverbot vorsehen, sondern kann dieses von weiteren Voraussetzungen abhängig machen und Widerlegungsmöglichkeiten für die Schutzbedürftigkeit solcher Kommunikation zulassen (siehe oben C IV 3 d). Erlaubt der Gesetzgeber in dieser Weise auch die Erhebung von Informationen, für die Zweifel bestehen können, ob sie dem Kernbereich privater Lebensgestaltung unterfallen, bedarf es für solche Aufzeichnungen dann aber auch der Sichtung durch eine unabhängige Stelle.

bb) § 20l Abs. 6 BKAG genügt diesen Anforderungen im Wesentlichen. 242

(1) § 20l Abs. 6 Satz 1 BKAG ordnet der Sache nach an, dass vor einer Telekommunikationsüberwachung im Hinblick auf den Kernbereichsschutz eine Prüfung stattfindet und Maßnahmen zu unterlassen sind, wenn tatsächliche Anhaltspunkte bestehen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Da auch dieser Vorschrift ein verfassungsrechtliches Begriffsverständnis zugrunde zu legen ist, nach dem Gespräche mit Personen engsten Vertrauens nicht schon dann aus dem strikten Schutz herausfallen, wenn sich in ihnen Höchstpersönliches und Alltägliches vermischt (vgl. BVerfGE 109, 279 <330>), ist hiergegen nichts zu erinnern. In Einklang mit der Verfassung sieht das Gesetz auch vor, dass die Maßnahme abzubrechen ist, wenn höchstvertrauliche Gespräche den überwachenden Personen unmittelbar zur Kenntnis kommen, und begrenzt das Gesetz die Überwachung bei aufkommenden Zweifel auf eine automatische Aufzeichnung, § 20l Abs. 6 Satz 2, 3 BKAG. 243

Allerdings erlaubt das Gesetz darüber hinaus automatische Aufzeichnungen auch allgemein, also auch, wenn hierbei neben anderen kernbereichsrelevante Gespräche erfasst werden können (vgl. § 20l Abs. 6 Satz 2, 1. Halbsatz BKAG). In Bezug auf Telekommunikationsüberwachungen ist dies verfassungsrechtlich jedoch noch hinnehmbar. Die diesbezüglichen strengeren Vorgaben der Wohnraumüberwachung (vgl. BVerfGE 109, 279 <324>), die ihrem Grundtypus nach eine noch größere Kernbereichsnähe aufweisen, gelten hier nicht. Freilich bedarf die Anordnung einer solchen automatischen Überwachung hinsichtlich ihres zeitlichen und sachlichen Umfangs einer strengen Verhältnismäßigkeitsprüfung im Ein- 244

zelfall. Ebenso setzt die mit dieser Regelung in Kauf genommene Erfassung von höchstpersönlichen Informationen wirksame Schutzvorkehrungen auf der Stufe der Aus- und Verwertung voraus.

(2) Auch diesbezüglich erfüllt die Vorschrift die verfassungsrechtlichen Anforderungen weitgehend. Sie sieht nicht nur die erforderlichen Verwertungsverbote und Löschungspflichten, sondern für automatische Aufzeichnungen auch eine der Datenverwendung vorgelagerte Sichtung durch ein Gericht vor. Dass diese auf automatische Aufzeichnungen und damit die Erfassung von Zweifelsfällen beschränkt ist, ist verfassungsrechtlich nicht zu beanstanden. Anders als für die Wohnraumüberwachung kann die unabhängige Sichtung für die Telekommunikationsüberwachung auf Zweifelsfälle beschränkt werden. 245

Verfassungswidrig ist demgegenüber auch hier die zu knappe Aufbewahrungsfrist der Löschungsprotokolle gemäß § 20l Abs. 6 Satz 10 BKAG (siehe oben C IV 3 d). 246

6. § 20m Abs. 1, 3 BKAG teilt, soweit er sich mit § 20l BKAG deckt, dessen verfassungsrechtliche Mängel und ist insoweit auch seinerseits verfassungswidrig. Darüber hinaus ist die Vorschrift mit der Verfassung vereinbar. 247

a) § 20m Abs. 1, 3 BKAG, der die Erhebung von Telekommunikationsverkehrsdaten erlaubt, begründet einen Eingriff in das Telekommunikationsgeheimnis gemäß Art. 10 Abs. 1 GG. Dieses schützt nicht nur die Inhalte der Kommunikation, sondern auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172>; 130, 151 <179>; stRspr). 248

Ein Eingriff in Art. 10 Abs. 1 GG durch Erhebung von Telekommunikationsverkehrsdaten wiegt, auch wenn hierdurch nicht unmittelbar der Inhalt der Kommunikation erfasst wird, schwer (vgl. BVerfGE 107, 299 <318 ff.>; für die vorsorgliche Speicherung solcher Daten vgl. auch BVerfGE 125, 260 <318 ff.>). Er kann bei verhältnismäßiger Ausgestaltung zur Terrorismusabwehr jedoch gerechtfertigt sein. Wie bei § 20l BKAG ist dies auch hier nicht in jeder Hinsicht der Fall. 249

b) Für die verfassungsrechtliche Beurteilung der Vorschrift, deren Eingriffsvoraussetzungen sich mit denen des § 20l Abs. 1, 3 bis 5 BKAG im Wesentlichen 250

decken, gelten die diesbezüglichen Ausführungen entsprechend. Da insoweit Anforderungen verfehlt werden, die sich für eingriffsintensive Ermittlungs- und Überwachungsmaßnahmen schon übergreifend aus dem Verhältnismäßigkeitsgrundsatz ergeben (siehe oben C IV 1 b, 2), gilt für die Telekommunikationsverkehrsdatenerhebung nichts anderes als für die inhaltliche Überwachung der Telekommunikation.

Danach ist § 20m Abs. 1 Nr. 2 BKAG mit der Verfassung nicht vereinbar und bedarf § 20m Abs. 1 Nr. 3 und 4 BKAG einer verfassungskonformen Auslegung; auch fehlt es an einer gesetzlichen Pflicht, die Anordnung der Maßnahme sachhaltig zu begründen (siehe oben C V 5 b, d). 251

Im Übrigen ist § 20m Abs. 1, 3 BKAG mit der Verfassung vereinbar. Soweit er auf § 113a TKG (a.F.) verweist, läuft er leer, da das Bundesverfassungsgericht § 113a TKG (a.F.) für nichtig erklärt hat (vgl. BVerfGE 125, 260 <347 ff.>). Die Vorschrift entfaltet insoweit keine Beschwer. Die Neufassung des Telekommunikationsgesetzes durch Gesetz vom 10. Dezember 2015 (BGBl I S. 2218), dessen § 113a schon vom Regelungsgegenstand nicht identisch ist mit dem des § 113a TKG (a.F.), wird durch den Verweis nicht erfasst und ist nicht Gegenstand des vorliegenden Verfahrens. Keinen verfassungsrechtlichen Bedenken unterliegt auch § 20m Abs. 3 Satz 2 BKAG, der für die Anordnung der Maßnahme Erleichterungen bezüglich der Bezeichnung der zu erhebenden Daten vorsieht; hierdurch bleibt unberührt, dass gemäß § 20m Abs. 1 BKAG nur auf einzelne Personen bezogene Datenerhebungen zulässig sind. 252

VI.

Die angegriffenen Ermittlungs- und Überwachungsbefugnisse sind in verschiedener Hinsicht auch hinsichtlich der weiteren, gleichartig an sie zu stellenden Anforderungen (siehe oben C IV 4 bis 7) nicht mit der Verfassung vereinbar. Es fehlt an flankierenden Regelungen, ohne die die Verhältnismäßigkeit dieser Eingriffe nicht gewahrt ist. 253

1. Keinen Bedenken unterliegt allerdings, dass das Gesetz keine ausdrückliche Regelung enthält, die mit Blick auf das Zusammenwirken der verschiedenen Befugnisse das Verbot der Rundumüberwachung näher ausformt (siehe oben C IV 4). Das Verbot der Rundumüberwachung gilt als Ausprägung des Verhältnismäßigkeitsgrundsatzes zur Wahrung eines in der Menschenwürde wurzelnden unverfügbaren Kerns der Person unmittelbar von Verfassungs wegen und ist von den 254

Sicherheitsbehörden im Rahmen ihrer Befugnisse von sich aus zu beachten (vgl. BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>; stRspr). Weiterer gesetzlicher Konkretisierung bedarf es insoweit nicht. Soweit es um die hierfür erforderliche Koordination der Befugnisse innerhalb des Bundeskriminalamts selbst geht, durfte der Gesetzgeber davon ausgehen, dass diese angesichts der vergleichsweise übersichtlichen Größe und Strukturen des Bundeskriminalamts im Rahmen der Leitungsverantwortung hinreichend gewährleistet ist. Soweit es demgegenüber um die Abstimmung mit Überwachungsmaßnahmen anderer Behörden geht, ist zu berücksichtigen, dass Beschränkungen des Informationsflusses zwischen den Sicherheitsbehörden auch eine grundrechtsschützende Dimension haben (vgl. BVerfGE 133, 277 <323 Rn. 113>). Es ist deshalb verfassungsrechtlich nicht zu beanstanden, dass das Gesetz zur Verhinderung einer Rundumüberwachung auf eine Abstimmung im Rahmen der allgemeinen Vorschriften sowie insbesondere gemäß § 4a Abs. 2 BKAG vertraut.

2. Nicht in jeder Hinsicht mit den Anforderungen der Verfassung vereinbar ist dagegen die Ausgestaltung des Schutzes von Berufs- und anderen Personengruppen, deren Tätigkeit von Verfassungs wegen eine besondere Vertraulichkeit ihrer Kommunikation voraussetzt. 255

a) Allerdings hat der Gesetzgeber in § 20u BKAG eine Regelung geschaffen, die den verfassungsrechtlichen Anforderungen diesbezüglich weithin entspricht. Insbesondere ist nicht zu beanstanden, dass § 20u Abs. 2 BKAG - in enger Anlehnung an § 160a StPO - die Überwachung von Berufsgeheimnisträgern grundsätzlich nicht strikt, sondern nur nach Maßgabe einer Abwägung im Einzelfall ausschließt, und ein strikteres Überwachungsverbot in § 20u Abs. 1 BKAG nur für einen kleinen Personenkreis vorgesehen ist, für den der Gesetzgeber besonderen Schutzbedarf sieht (vgl. BVerfGE 129, 208 <258 ff.>). Bei der nach § 20u Abs. 2 BKAG vorzunehmenden Abwägung sind die Grundrechte der Betroffenen angemessen zu gewichten. Dabei ist die Abwägung durch den Verhältnismäßigkeitsgrundsatz strukturiert. In Entsprechung zu § 160a Abs. 2 Satz 1, 2. Halbsatz StPO gebietet die Verfassung insoweit die Vermutung, dass von einem Überwiegen des Interesses des Bundeskriminalamts an der Erhebung der Daten in der Regel nicht auszugehen ist, wenn die Maßnahme nicht der Abwehr einer erheblichen Gefahr dient. 256

b) Verfassungsrechtlich nicht tragfähig ist insoweit allerdings die Ausgestaltung des Schutzes der Vertrauensverhältnisse von Rechtsanwälten zu ihren Mandanten. Die vom Gesetzgeber herangezogene Unterscheidung zwischen Strafver- 257

teidigern und den in anderen Mandatsverhältnissen tätigen Rechtsanwälten ist als Abgrenzungskriterium für einen unterschiedlichen Schutz schon deshalb ungeeignet, weil die in Frage stehenden Überwachungsmaßnahmen nicht der Strafverfolgung, sondern der Gefahrenabwehr dienen, die Strafverteidigung also hier gerade nicht entscheidend ist.

c) Darüber hinaus sind Grundrechtsverletzungen durch § 20u BKAG nicht zu erkennen. Ein Anspruch auf strikteren Schutz ergibt sich insbesondere nicht aus Art. 5 Abs. 1 Satz 2 GG für Medienvertreter (vgl. BVerfGE 107, 299 <332 f.>). Weitere Grenzen ergeben sich auch nicht aus Art. 3 Abs. 1 GG. Der Gesetzgeber darf die Zuerkennung eines strengeren Schutzes vor Überwachungsmaßnahmen als Ausnahme für spezifische Schutzlagen verstehen, hinsichtlich derer er einen erheblichen Einschätzungsspielraum hat. Die Anerkennung einer solchen besonderen Schutzbedürftigkeit von Geistlichen und Abgeordneten gegenüber anderen Berufsgruppen wurde durch die Entscheidung des Zweiten Senats vom 12. Oktober 2011 als zumindest tragfähig angesehen. Eine Pflicht zur Ausweitung dieses besonders strikten Schutzes auf weitere Gruppen kann hieraus nicht abgeleitet werden (vgl. BVerfGE 129, 208 <258 ff., 263 ff.>). Unberührt bleibt, dass in die für die anderen Berufsgeheimnisträger gebotene Abwägung auch unter Berücksichtigung des Art. 12 Abs. 1 GG die Vertrauensbedürftigkeit der jeweiligen Kommunikationsbeziehungen im jeweiligen Einzelfall maßgeblich einzufließen hat und darüber hinaus eine Überwachung - etwa für psychotherapeutische Gespräche - auch unter dem Gesichtspunkt des Kernbereichs privater Lebensgestaltung ausgeschlossen sein kann (siehe oben C IV 3 a). 258

3. Die Regelungen zur Gewährleistung von Transparenz, Rechtsschutz und aufsichtlicher Kontrolle genügen gleichfalls den verfassungsrechtlichen Anforderungen nicht in jeder Hinsicht. 259

a) Bei sachgerechter Auslegung nicht zu beanstanden ist allerdings die Regelung der Benachrichtigungspflichten in § 20w BKAG. Die in enger Anlehnung an § 101 Abs. 4 bis 6 StPO formulierte Vorschrift genügt den verfassungsrechtlichen Anforderungen (vgl. BVerfGE 129, 208 <250 ff.>). 260

Dies gilt auch für § 20w Abs. 2 Satz 1, 2. Halbsatz BKAG, der das Absehen von einer Benachrichtigung zur Sicherung des weiteren Einsatzes eines Verdeckten Ermittlers erlaubt. Denn anders als für die Zurückstellung der Benachrichtigung über den Einsatz von Verdeckten Ermittlern im Rahmen einer Wohnraumüberwachung, für die dieser Gesichtspunkt nicht ausreicht (vgl. BVerfGE 109, 279 261

<366 f.>), geht es bei dieser Ausnahme von der Benachrichtigungspflicht um den Einsatz von Verdeckten Ermittlern als solchen. Allerdings ist die Vorschrift so auszulegen, dass nicht schon jede bloß abstrakte Möglichkeit einer Beeinträchtigung der weiteren Verwendung der betreffenden Ermittlungsperson ausreicht, um von der Benachrichtigung abzusehen, sondern die Notwendigkeit eines solchen Schutzes für eine absehbare weitere Verwendung der betreffenden Person konkretisierbar sein muss.

Verfassungsmäßig ist auch das endgültige Absehen von einer Benachrichtigung nach Ablauf von mindestens fünf Jahren gemäß § 20w Abs. 3 Satz 5 BKAG. In Übereinstimmung mit der derzeitigen Praxis, wie sie in der mündlichen Verhandlung von Vertretern des Bundeskriminalamts geschildert wurde, setzt die Entscheidung über ein endgültiges Absehen von der Benachrichtigung bei verfassungskonformer Auslegung voraus, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden. 262

b) Auskunftsrechte sowie die Möglichkeit einer nachträglichen gerichtlichen Kontrolle und gegebenenfalls Wiedergutmachung werden in Bezug auf die angegriffenen Ermittlungs- und Überwachungsbefugnisse gleichfalls in verfassungsrechtlich nicht zu beanstandender Weise gewährleistet. 263

Vom Grundsatz her ist ein Auskunftsrecht in § 19 BDSG anerkannt, dessen Anwendbarkeit für das Bundeskriminalamtgesetz nach § 37 BKAG nicht ausgeschlossen ist. Dass dabei im Zusammenhang mit Ermittlungen des Bundeskriminalamts zur Terrorismusabwehr häufig die Ausnahmetatbestände des § 19 Abs. 4 BDSG greifen dürften, nimmt diesen Rechten in tatsächlicher Hinsicht zwar erheblich an Wirksamkeit, ist aber für eine effektive Aufgabenwahrnehmung unvermeidlich und verfassungsrechtlich hinzunehmen (vgl. BVerfGE 133, 277 <367 f. Rn. 210>). 264

Die von der Verfassung geforderte Eröffnung nachträglichen Rechtsschutzes im Falle der unrechtmäßigen Überwachung ergibt sich aus Verwaltungsprozessrecht, hier der Feststellungs- oder Fortsetzungsfeststellungsklage, für die in solchen Fällen in der Regel ein Feststellungsinteresse anzuerkennen ist (vgl. Happ, in: Eyermann, VwGO, 14. Aufl. 2014, § 43 Rn. 34; Schmidt, in: Eyermann, a.a.O., § 113 Rn. 87 ff., 93; vgl. hierzu auch BVerfGE 96, 27 <39 f.>); Ansprüche auf Wiedergutmachung lassen sich auf die zivilrechtlichen Grundsätze zur Entschädigungspflicht bei schweren Eingriffen in das allgemeine Persönlichkeitsrecht stützen (siehe oben C IV 6 c). 265

c) Nicht verfassungsrechtlich hinreichend ausgestaltet ist demgegenüber die aufsichtliche Kontrolle (siehe oben C IV 6 d). Zwar ist nach den Vorschriften des Bundesdatenschutzgesetzes eine Kontrolle durch die Bundesdatenschutzbeauftragte eröffnet und verfügt diese insoweit auch über ausreichende Befugnisse (vgl. BVerfGE 133, 277 <370 Rn. 215>). Es fehlt jedoch an einer hinreichenden gesetzlichen Vorgabe zu turnusmäßigen Pflichtkontrollen, deren Abstand ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf (vgl. BVerfGE 133, 277 <370 f. Rn. 217>). 266

Auch fehlt es an einer umfassenden Protokollierungspflicht, die es ermöglicht, die jeweiligen Überwachungsmaßnahmen sachhaltig zu prüfen (vgl. BVerfGE 133, 277 <370 Rn. 215>). Das Gesetz sieht zwar vereinzelt Protokollierungspflichten vor wie § 20k Abs. 3 BKAG für den Eingriff in informationstechnische Systeme oder § 20w Abs. 2 Satz 3 BKAG für die Zurückstellung einer Benachrichtigung. Selbst dort, wo eine Protokollierung der Benachrichtigung vorgesehen ist, bleibt unklar, ob sie sich auch auf die Gründe für das Absehen bezieht. Die Regelungen bleiben jedenfalls punktuell und stellen eine nachträgliche Kontrolle der Überwachungsmaßnahmen nicht hinreichend sicher. Zwar werden zumindest wichtige Ergebnisse der Datenerhebung auf der Grundlage der allgemeinen Regeln zur Aktenführung dokumentiert. Jedoch ist dies weder umfassend klar noch in Bezug auf die datenschutzrechtlichen Erfordernisse einer wirksamen Kontrolle gesetzlich geregelt. Dies fällt umso mehr für den Bereich der Gefahrenabwehr ins Gewicht, wo die Aufklärung und Abwehr von Gefahren nicht wie im Strafprozess als Ermittlungsverfahren gegen bestimmte einzelne Personen durchgeführt werden müssen. Es ist insoweit nicht ersichtlich, dass die Nachvollziehbarkeit der Datenerhebung - auch für Betroffene in etwaigen späteren Strafverfahren - sichergestellt ist. Daran ändert die richterliche Anordnung der Maßnahme nichts. Denn aus dieser ergibt sich nur die Erlaubnis zu deren Durchführung, nicht aber, ob und wie hiervon Gebrauch gemacht wurde. Im Übrigen ist anders als für das Strafverfahren in § 100b Abs. 4 Satz 2 StPO noch nicht einmal eine Unterrichtung des anordnenden Gerichts über die Ergebnisse der Ermittlungen vorgesehen. 267

d) Schließlich fehlt es für eine verhältnismäßige Ausgestaltung der angegriffenen Überwachungsbefugnisse auch an Berichtspflichten gegenüber Parlament und Öffentlichkeit (vgl. BVerfGE 133, 277 <372 Rn. 221 f.>). Weder sieht das Gesetz Berichte darüber vor, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde, noch darüber, wieweit die Betroffenen hierüber benachrichtigt wurden. Da sich die Wahrnehmung der in Frage stehenden Befugnisse sowohl dem Betroffenen als auch der Öffentlichkeit 268

weitgehend entzieht, sind solche Berichte zur Ermöglichung einer öffentlichen Diskussion und demokratischen Kontrolle in regelmäßigen Abständen verfassungsrechtlich geboten (siehe oben C IV 6 e).

4. Verfassungsrechtlich nicht in jeder Hinsicht tragfähig ist auch die Regelung zur Löschung der Daten gemäß § 20v Abs. 6 BKAG. 269

a) Die Grundstruktur der Regelung ist freilich verfassungsrechtlich nicht zu beanstanden. Die Daten sind nach Erfüllung des der Datenerhebung zugrundeliegenden Zwecks zu löschen (Satz 1). Dies verweist auf die verfassungsrechtlichen Grundsätze zur Zweckbindung (siehe unten D I). Mit Blick auf eine weitere Verwendung der Daten gemäß § 20v Abs. 4 Satz 2 BKAG kommt danach bei verfassungskonformer Auslegung ein Absehen von einer Löschung über den unmittelbaren Anlassfall hinaus nur insoweit in Betracht, als sich aus ihnen konkrete Ermittlungsansätze für die Abwehr von Gefahren des internationalen Terrorismus ergeben. Die Löschung ist aktenkundig zu machen (Satz 2). Die Löschung kann für eine etwaige gerichtliche Überprüfung zurückgestellt werden; die Daten sind dann zu sperren (Satz 4). Verfahrensrechtlich steht die Vorschrift in Kontext mit § 32 BKAG. Nach dessen Absatz 3 sind neben der Einzelfallbearbeitung auch periodisierte Prüfungen der Löschungspflichten vorgesehen. 270

Für Maßnahmen der Rasterfahndung sind in § 20j Abs. 3 BKAG entsprechende eigene Löschungspflichten vorgesehen, die diese Regelung in verfassungsrechtlich nicht zu beanstandender Weise konkretisieren. 271

b) Verfassungsrechtlich nicht tragfähig ist demgegenüber die Anordnung der sehr kurzen Frist zur Löschung der „Akten“ in § 20v Abs. 6 Satz 3 BKAG, mit der das Gesetz die Löschung der Löschungsprotokolle regelt. Löschungsprotokolle dienen der Ermöglichung der späteren Nachvollziehbarkeit und Kontrolle. Die Frist ihrer Aufbewahrung muss demnach so bemessen sein, dass die Protokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen und im Rahmen der nächsten periodisch anstehenden Kontrolle durch die Datenschutzbeauftragte noch vorliegen (vgl. hierzu auch BVerfGE 100, 313 <400>). 272

Entsprechendes gilt für die Frist des § 20j Abs. 3 Satz 3 BKAG. 273

c) Verfassungswidrig ist darüber hinaus § 20v Abs. 6 Satz 5 BKAG. Die Vorschrift sieht ein Absehen von der Löschung auch nach Zweckerfüllung vor, soweit die Daten zur Verfolgung von Straftaten oder - nach Maßgabe des § 8 BKAG - zur 274

Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich sind. Sie erlaubt damit die Speicherung der Daten in Blick auf eine Nutzung zu neuen, nur allgemein umschriebenen Zwecken, für die das Gesetz keine Ermächtigungsgrundlage enthält und in dieser Offenheit auch nicht schaffen kann.

D.

Soweit sich die Verfassungsbeschwerden gegen die Befugnisse zur weiteren Nutzung der Daten und zu ihrer Übermittlung an inländische und ausländische Behörden richten, greifen die Rügen gleichfalls in verschiedener Hinsicht durch. 275

I.

Die Anforderungen an die weitere Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung (vgl. BVerfGE 65, 1 <51, 62>; 100, 313 <360 f., 389 f.>; 109, 279 <375 ff.>; 110, 33 <73>; 120, 351 <368 f.>; 125, 260 <333>; 130, 1 <33 f.>; 133, 277 <372 ff. Rn. 225 f.>; stRspr). 276

Erlaubt der Gesetzgeber die Nutzung von Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus, muss er hierfür eine eigene Rechtsgrundlage schaffen (vgl. nur BVerfGE 109, 279 <375 f.>; 120, 351 <369>; 130, 1 <33>; stRspr). Er kann insoweit zum einen eine weitere Nutzung der Daten im Rahmen der für die Datenerhebung maßgeblichen Zwecke vorsehen; stellt er sicher, dass die weitere Nutzung der Daten den näheren verfassungsrechtlichen Anforderungen der Zweckbindung genügt, ist eine solche Regelung verfassungsrechtlich grundsätzlich zulässig (1.). Er kann zum anderen aber auch eine Zweckänderung erlauben; als Ermächtigung zu einer Datennutzung für neue Zwecke unterliegt sie spezifischen verfassungsrechtlichen Anforderungen (2.). 277

1. Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. 278

a) Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt. 279

b) Nicht zu den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde je neu beachtet werden müssen, gehören grundsätzlich die für die Datenerhebung maßgeblichen Anforderungen an Einschreitschwellen, wie sie traditionell die hinreichend konkretisierte Gefahrenlage im Bereich der Gefahrenabwehr und der hinreichende Tatverdacht im Bereich der Strafverfolgung darstellen. Das Erfordernis einer hinreichend konkretisierten Gefahrenlage oder eines qualifizierten Tatverdachts bestimmt den Anlass, aus dem entsprechende Daten erhoben werden dürfen, nicht aber die erlaubten Zwecke, für die die Daten der Behörde dann zur Nutzung offen stehen. 280

Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung - allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen - als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. Dies trägt dem Umstand Rechnung, dass sich die Generierung von Wissen - nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen geht - nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lässt. In den dargelegten Grenzen erkennt das die Rechtsordnung an. Diese Grenzen gewährleisten zugleich, dass damit keine Datennutzung ins Blaue hinein eröffnet ist. Durch die Bindung an die für die Datenerhebung maßgeblichen Auf- 281

gaben und die Anforderungen des Rechtsgüterschutzes hat auch eine Verwendung der Daten als Spurenansatz einen hinreichend konkreten Ermittlungsbezug, den der Gesetzgeber nicht durch weitere einschränkende Maßgaben absichern muss.

Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Diese Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung zu legitimieren. 282

Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht. 283

2. Der Gesetzgeber kann eine weitere Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung). Er hat dann allerdings sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird (vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <377>; 120, 351 <369>; 130, 1 <33 f.>; 133, 277 <372 f. Rn. 225>). 284

a) Die Ermächtigung zu einer Nutzung von Daten zu neuen Zwecken begründet einen neuen Eingriff in das Grundrecht, in das durch die Datenerhebung eingegriffen wurde (vgl. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 f.>; 125, 260 <312 f., 333>; 133, 277 <372 Rn. 225>; vgl. auch EGMR, Weber und Saravia v. Deutschland, Entscheidung vom 29. Juni 2006, Nr. 54934/00, § 79, NJW 2007, S. 1433 <1434>, zu Art. 8 EMRK). Zweckänderungen sind folglich jeweils an den Grundrechten zu messen, die für die Datenerhebung maßgeblich waren. Das gilt für jede Art der Verwendung von Daten zu einem anderen Zweck 285

als dem Erhebungszweck, unabhängig davon, ob es sich um die Verwendung als Beweismittel oder als Ermittlungsansatz handelt (vgl. BVerfGE 109, 279 <377>).

b) Die Ermächtigung zu einer Zweckänderung ist dabei am Verhältnismäßig- 286
keitsgrundsatz zu messen. Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken benutzt werden (vgl. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277 <372 f. Rn. 225> m.w.N.).

aa) Während nach der früheren Rechtsprechung des Bundesverfassungsge- 287
richts insoweit als Maßstab der Verhältnismäßigkeitsprüfung darauf abgestellt wurde, ob die geänderte Nutzung mit der ursprünglichen Zwecksetzung „unvereinbar“ sei (vgl. BVerfGE 65, 1 <62>; 100, 313 <360, 389>; 109, 279 <376 f.>; 110, 33 <69>; 120, 351 <369>; 130, 1 <33>), ist dies inzwischen durch das Kriterium der hypothetischen Datenneuerhebung konkretisiert und ersetzt worden. Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen wie denen des vorliegenden Verfahrens kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (vgl. BVerfGE 125, 260 <333>; 133, 277 <373 f. Rn. 225 f.>; der Sache nach ist diese Konkretisierung nicht neu, vgl. bereits BVerfGE 100, 313 <389 f.>, und findet sich unter der Bezeichnung „hypothetischer Ersatzeingriff“ auch in BVerfGE 130, 1 <34>). Das Kriterium der Datenneuerhebung gilt allerdings nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus (vgl. BVerfGE 133, 277 <374 Rn. 226>). So steht die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell entgegen (vgl. BVerfGE 100, 313 <390>). Auch können Gesichtspunkte der Vereinfachung und der Praktikabilität bei der Schaffung von Übermittlungsvorschriften es rechtfertigen, dass nicht alle Einzelanforderungen, die für die Datenerhebung erforderlich sind, in gleicher Detailliertheit für die Übermittlung der Daten gelten. Das Erfordernis einer Gleichgewichtigkeit der neuen Nutzung bleibt hierdurch jedoch unberührt.

bb) Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass 288
die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuer-

hebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <377>; 110, 33 <73>; 120, 351 <369>; 130, 1 <34>).

Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde - ein konkreter Ermittlungsansatz ergibt. 289

Der Gesetzgeber kann danach - bezogen auf die Datennutzung von Sicherheitsbehörden - eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist. 290

Anderes gilt allerdings auch hier für Informationen aus Wohnraumüberwachungen oder dem Zugriff auf informationstechnische Systeme. Angesichts des besonderen Eingriffsgewichts dieser Maßnahmen muss für sie jede neue Nutzung der Daten wie bei der Datenerhebung selbst auch durch eine dringende Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder eine im Einzelfall hinreichend konkretisierte Gefahr (siehe oben C IV 1 b) gerechtfertigt sein. 291

cc) In diesen Anforderungen an die Zulässigkeit einer Zweckänderung liegt eine konkretisierende Konsolidierung einer langen Rechtsprechung beider Senate des Bundesverfassungsgerichts (vgl. BVerfGE 65, 1 <45 f., 61 f.>; 100, 313 <389 f.>; 109, 279 <377>; 110, 33 <68 f., 73>; 120, 351 <369>; 125, 260 <333>; 130, 1 <33 f.>; 133, 277 <372 f. Rn. 225>). Hierin liegt keine Verschärfung der Maßstäbe, sondern eine behutsame Einschränkung, indem das Kriterium der hypothetischen Datenneuerhebung nicht strikt angewandt (vgl. bereits BVerfGE 133, 277 <374 Rn. 226>), sondern in Blick auf die - die zu fordernde Aktualität der Ge- 292

fahrenlage bestimmenden - Eingriffsschwellen gegenüber früheren Anforderungen (vgl. insbesondere BVerfGE 100, 313 <394>; 109, 279 <377>) teilweise zurückgenommen wird. Wollte man, wie es in einem Sondervotum befürwortet wird, darüber hinaus auch auf das Erfordernis eines vergleichbar gewichtigen Rechtsgüterschutzes verzichten, würden die Grenzen der Zweckbindung als Kernelement des verfassungsrechtlichen Datenschutzes (vgl. BVerfGE 65, 1 <45 f., 61 f.>) - erst recht wenn zugleich die Voraussetzung eines konkreten Ermittlungsansatzes als zu streng angesehen wird - für das Sicherheitsrecht praktisch hinfällig (oder beschränkten sich allenfalls noch rudimentär auf Daten aus Wohnraumüberwachungen und Online-Durchsuchungen).

II.

Ausgehend von den vorstehenden Maßstäben genügt § 20v Abs. 4 Satz 2 BKAG, der die Verwendung der vom Bundeskriminalamt erhobenen Daten durch dieses selbst regelt, den verfassungsrechtlichen Anforderungen nicht. Die Vorschrift ist verfassungswidrig. 293

1. Die in § 20v Abs. 4 Satz 2 Nr. 1 BKAG allein zur Wahrnehmung der Aufgabe der Abwehr von Gefahren des internationalen Terrorismus geregelte Datennutzung ist zwar im Grundsatz mit verfassungsrechtlichen Anforderungen vereinbar; es fehlt jedoch an einer hinreichenden Begrenzung für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen. 294

a) Im Grundsatz bestehen gegen die Regelung keine durchgreifenden verfassungsrechtlichen Bedenken. 295

aa) Die Vorschrift erlaubt dem Bundeskriminalamt eine Verwendung der von ihm zur Terrorismusabwehr erhobenen Daten zur Wahrnehmung seiner Aufgabe nach § 4a Abs. 1 Satz 1 BKAG. Damit eröffnet sie zunächst - als innere Konsequenz der Ermächtigung zur Datenerhebung - eine Nutzung der Daten zu dem ihrer Erhebung konkret zugrundeliegenden Zweck. Darüber hinaus eröffnet sie aber auch eine über das jeweilige Ermittlungsverfahren hinausreichende Nutzung der Daten. Mit dem Verweis auf § 4a Abs. 1 Satz 1 BKAG ist diese weitere Nutzung der Daten auf die Abwehr von Gefahren des internationalen Terrorismus begrenzt. Bei sachgerechtem Verständnis dieser Verweisung ergibt sich hieraus zugleich, dass die Daten allein zur Verhinderung der in § 4a Abs. 1 Satz 2 BKAG qualifizierten Straftaten und damit zum Schutz nur von solchen hochrangigen Rechtsgütern genutzt werden dürfen, zu deren Schutz auch die Datenerhebungs- 296

befugnisse des Unterabschnitts 3a - einschließlich der besonders eingriffsintensiven Überwachungsbefugnisse der §§ 20g ff. BKAG - eingesetzt werden dürfen.

(1) Die Verweisung auf § 4a Abs. 1 Satz 1 BKAG wirft hinsichtlich ihrer Bedeutung allerdings Zweifel auf. Sie können im Wege der Auslegung jedoch überwunden werden, so dass die Vorschrift nicht an Bestimmtheitsanforderungen scheitert. Zwar ist unklar, wie sich § 4a Abs. 1 Satz 1 und 2 BKAG voneinander abgrenzen: Während sich Satz 1 für die Zuweisung der Aufgabe der Gefahrenabwehr an den Wortlaut des Art. 73 Abs. 1 Nr. 9a GG anlehnt, der auch die Straftatenverhütung mitumfasst (siehe oben C I 1), wird die Straftatenverhütung in Satz 2 von der Gefahrenabwehr bewusst unterschieden. Da § 4a Abs. 1 Satz 1 BKAG angesichts seines Charakters als Aufgabennorm für die Gefahrenabwehr jedoch Ermittlungen im Vorfeld konkreter Gefahren einschließt, ist der Verweis in § 20v Abs. 4 Satz 2 Nr. 1 BKAG letztlich doch hinreichend auslegungsfähig: Die Vorschrift will eine Nutzung der Daten allgemein, gegebenenfalls auch als Spurenansatz, zur Abwehr von Gefahren des internationalen Terrorismus eröffnen. 297

Die Regelung ist auch nicht insoweit zu unbestimmt, als § 4a Abs. 1 BKAG nur allgemein auf „Gefahren des internationalen Terrorismus“ abstellt. Auch wenn § 20v Abs. 4 Satz 2 Nr. 1 BKAG allein auf Satz 1 der Vorschrift verweist, ist für die Konkretisierung der dort genannten Gefahren auf die nähere Definition in Satz 2 zurückzugreifen, der bestimmte Straftaten abschließend aufführt und näher qualifiziert. Dass die dort unter dem Gesichtspunkt der Straftatenverhütung aufgeführten Straftaten auch für die Gefahrenabwehr nach Satz 1 maßgeblich sind, entspricht der Systematik des Gesetzes auch sonst (vgl. nur § 20a Abs. 2 BKAG). 298

(2) Indem § 20v Abs. 4 Satz 2 Nr. 1 BKAG eine Datennutzung nur zur Abwehr von Gefahren durch terroristische Straftaten im Sinne des § 4a Abs. 1 Satz 2 BKAG erlaubt, ist zugleich gewährleistet, dass diese Nutzung allein zum Schutz von Rechtsgütern eröffnet wird, zu deren Schutz auch von den Datenerhebungsbefugnissen Gebrauch gemacht werden darf. Dies gilt auch für Daten aus besonders eingriffsintensiven Überwachungsmaßnahmen, die nur zum Schutz besonders hochrangiger Rechtsgüter gerechtfertigt sind. 299

Fast alle in § 4a Abs. 1 Satz 2 BKAG in Verbindung mit § 129a Abs. 1, 2 StGB genannten Straftaten betreffen Delikte, die unmittelbar gegen Leib und Leben gerichtet sind oder - etwa als gemeingefährliche Delikte - ihren Unrechtsgehalt maßgeblich aus solchen Gefahren beziehen beziehungsweise Sachen von bedeutendem Wert betreffen, deren Erhaltung als wesentliche Infrastrukturen im öffentli- 300

chen Interesse geboten ist. Soweit dies hinsichtlich einzelner in § 129a StGB genannter Delikte nicht zwangsläufig der Fall ist, ist zu berücksichtigen, dass die Verhinderung solcher Straftaten gemäß § 4a Abs. 1 Satz 1, 2 BKAG nur dann in den Aufgabenbereich des Bundeskriminalamts fällt, wenn diese eine gesetzlich näher bestimmte terroristische Dimension haben. Damit ist bei sachgerechtem Verständnis der Norm hinreichend gesichert, dass die durch die einzelnen Ermittlungsbefugnisse gewonnenen Informationen auch bei der weiteren Verwendung gemäß § 20v Abs. 4 Satz 2 Nr. 1 BKAG stets dem Schutz solcher Rechtsgüter dienen, zu deren Schutz auch bei eingriffsintensiven Maßnahmen schon die Erhebung der Daten gerechtfertigt wurde.

bb) Nicht zu beanstanden ist grundsätzlich auch, dass § 20v Abs. 4 Satz 2 Nr. 1 BKAG die weitere Nutzung der Daten allgemein und damit unabhängig von konkreten Gefahren oder konkreten Ermittlungsansätzen auch als Spurenansatz erlaubt. Soweit nicht Daten aus Wohnraumüberwachungen oder Online-Durchsuchungen betroffen sind (siehe unten D II 1 b), hält sich dies im Rahmen der Zweckbindung. Es handelt sich um Daten, die das Bundeskriminalamt im Rahmen seiner Befugnisse zur Terrorismusabwehr erhoben hat, die es für diese Aufgabe weiter nutzen können soll und die dem Schutz derselben Rechtsgüter dienen, für deren Schutz sie erhoben werden durften. In dieser Situation muss ihre weitere Nutzung nach den oben entwickelten Maßstäben grundsätzlich nicht jeweils erneut von einer konkretisierten Gefahrenlage abhängig gemacht werden, sondern konnte der Gesetzgeber dem Bundeskriminalamt die weitere Nutzung dieser Daten für die Terrorismusabwehr ohne weitere Einschränkungen erlauben (siehe oben D I 1 b). Hiervon unberührt bleiben freilich die Löschungspflichten nach Erreichung des mit der Datenerhebung verfolgten Zwecks (siehe oben C IV 7, VI 4 a). 301

b) Unverhältnismäßig weit ist § 20v Abs. 4 Satz 2 Nr. 1 BKAG hingegen insoweit, als er sich undifferenziert auf alle Daten erstreckt und damit auch die weitere Verwendung von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen einschließt. Die Vorschrift eröffnet damit die weitere Verwendung solcher Informationen auch unabhängig von dem Vorliegen einer dringenden (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall hinreichend konkretisierten Gefahrenlage (siehe oben C IV 1 b; D I 2 b bb). Dies ist mit den Anforderungen des Übermaßverbots nicht vereinbar. Für Informationen aus diesen besonders intensiven Überwachungsmaßnahmen bedarf jede über das ursprüngliche Ermittlungsverfahren hinausgehende Nutzung jeweils erneut des Vorliegens aller Eingriffsvo- 302

raussetzungen, wie es für eine Datenneuerhebung mit diesen Mitteln verfassungsrechtlich geboten wäre (siehe oben D I 1 b).

2. Unvereinbar mit den verfassungsrechtlichen Anforderungen ist auch § 20v Abs. 4 Satz 2 Nr. 2 BKAG zur Verwendung der Daten zum Zeugen- und Personenschutz. Der einschränkungslos allgemeine Verweis auf die Aufgaben des Bundeskriminalamts nach §§ 5 und 6 BKAG genügt den oben entwickelten Maßstäben schon mangels Bestimmtheit nicht. 303

III.

§ 20v Abs. 5 BKAG, der die Übermittlung von Daten an andere Behörden regelt, genügt den verfassungsrechtlichen Anforderungen bezüglich verschiedener Regelungen nicht. 304

1. § 20v Abs. 5 BKAG stellt verschiedene Rechtsgrundlagen zur Übermittlung von zur Terrorismusabwehr erhobenen Daten an andere Behörden bereit. Es handelt sich hierbei um Ermächtigungen, mit denen der Gesetzgeber im Einzelfall anlassbezogen eine Zweckänderung der Datennutzung erlaubt. Er öffnet damit die Datennutzung durch andere Behörden, die - nach dem Bild einer Doppeltür - dabei auch ihrerseits zur Abfrage und Verwendung dieser Daten berechtigt sein müssen (vgl. BVerfGE 130, 151 <184>). Die Vorschrift eröffnet somit Grundrechtseingriffe, die jeweils an den Grundrechten zu messen sind, in die bei Erhebung der übermittelten Daten eingegriffen wurde (vgl. BVerfGE 100, 313 <360, 391>; 109, 279 <375>; 110, 33 <68 f.>; 125, 260 <312 f., 333>; 133, 277 <372 Rn. 225>; vgl. auch EGMR, Weber und Saravia v. Deutschland, Entscheidung vom 29. Juni 2006, Nr. 54934/00, § 79, NJW 2007, S. 1433 <1434>, zu Art. 8 EMRK). 305

2. § 20v Abs. 5 BKAG verstößt nicht gegen die Anforderungen des Bestimmtheitsgebots. Das gilt auch insoweit, als die Vorschrift übergreifend eine Übermittlung an „sonstige öffentliche Stellen“ erlaubt. Welche Stellen hierunter zu verstehen sind, richtet sich nach den jeweiligen Übermittlungszwecken, die die verschiedenen Übermittlungsbefugnisse näher regeln. Die möglichen Adressaten einer Übermittlung sind damit auf der Grundlage der Zuständigkeitsvorschriften hinreichend verlässlich bestimmbar. 306

3. Die Übermittlungsbefugnisse sind indes insoweit verfassungswidrig, als ihre Voraussetzungen den oben entwickelten Anforderungen in Bezug auf das Kriteri- 307

um der hypothetischen Datenneuerhebung (siehe oben D I 2 b) nicht genügen.

a) Keinen verfassungsrechtlichen Bedenken unterliegt allerdings § 20v Abs. 5 Satz 1 Nr. 1 BKAG. Die Datenübermittlung zur Herbeiführung des gegenseitigen Benehmens ist schon keine Zweckänderung. Sie dient der Koordinierung der Gefahrenabwehr in einer Weise, wie sie für die Aufgabenwahrnehmung durch das Bundeskriminalamt gemäß § 4a Abs. 2 BKAG stets geboten ist und ist damit in der Datenerhebungsvorschrift notwendig enthalten. Dies rechtfertigt auch die Weite der Regelung, die Einschränkungen der Datenübermittlung nicht enthält. Da eine Abstimmung nur hinsichtlich solcher Maßnahmen in Betracht kommt, die auf einer rechtmäßigen Datennutzung beruhen, ist auch ein Unterlaufen der Zweckbindung von Informationen aus Wohnraumüberwachungen oder Online-Durchsuchungen, deren Nutzung stets auch das Vorliegen einer hinreichend konkretisierten Gefahrenlage voraussetzt, nicht zu befürchten. 308

Die Vorschrift ist allerdings funktional eng auszulegen. Sie erlaubt allein die Übermittlung von Informationen für die Koordination der Aufgabenwahrnehmung zwischen den Bundes- und Landesbehörden. Auf diese interne Abstimmung ist die Nutzung der Daten nach dieser Vorschrift beschränkt. Sollen demgegenüber die Daten von der Zielbehörde auch operativ genutzt werden können, richtet sich die Übermittlung nach § 20v Abs. 5 Satz 1 Nr. 2 ff. BKAG. 309

b) § 20v Abs. 5 Satz 1 Nr. 2 BKAG, der die Übermittlung von Daten zur Gefahrenabwehr regelt, genügt im Wesentlichen den verfassungsrechtlichen Anforderungen. Unverhältnismäßig ist die Vorschrift allerdings insoweit, als sie eine Datenübermittlung allgemein schon zur Verhütung bestimmter Straftaten erlaubt. 310

aa) § 20v Abs. 5 Satz 1 Nr. 2 BKAG erlaubt zum einen die Übermittlung von Daten aus Maßnahmen gemäß §§ 20h, 20k oder 20l BKAG zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit. Mit dieser Schwelle, die unmittelbar Art. 13 Abs. 4 GG entnommen ist, orientiert sich der Gesetzgeber für die Zweckänderung an den Voraussetzungen einer hypothetischen Datenneuerhebung und ist eine Übermittlung auch von Informationen aus besonders eingriffsintensiven Maßnahmen einschließlich Wohnraumüberwachungen und Online-Durchsuchungen gerechtfertigt. Zwar ist es grundsätzlich Aufgabe des Gesetzgebers, die zu schützenden Rechtsgüter im Rahmen der Eingriffsvoraussetzungen näher zu konkretisieren und so auch dem offenen Begriff der öffentlichen Sicherheit des Art. 13 Abs. 4 GG, der nur einen Rahmen vorgibt, näheres Profil zu geben (vgl. entsprechend für Art. 14 Abs. 3 GG BVerfGE 134, 242 <294 Rn. 177>). Vor- 311

liegend lässt sich eine solche Konkretisierung jedoch aus dem Regelungszusammenhang ableiten. Bei verständiger Auslegung muss es sich bei der dringenden Gefahr für die öffentliche Sicherheit um eine Gefahr für die in §§ 20h, 20k und 20l BKAG genannten besonders hochrangigen Rechtsgüter handeln (vgl. hierzu auch BVerfGE 109, 279 <379>).

bb) Nicht zu beanstanden ist auch, dass für die Übermittlung von Daten, die durch andere Maßnahmen erhoben wurden, nur eine erhebliche Gefahr für die öffentliche Sicherheit verlangt wird. Unbedenklich ist dies zunächst in Bezug auf Daten, die durch niederschwelligere Eingriffe (vgl. etwa §§ 20b ff. oder §§ 20q ff. BKAG) erlangt werden. Diese dürfen schon grundsätzlich unter weniger strengen Anforderungen übermittelt werden. Verfassungsmäßig ist die Vorschrift aber auch in Bezug auf Daten aus eingriffsintensiven Maßnahmen wie gemäß §§ 20g, 20j oder 20m BKAG. Denn der Begriff der öffentlichen Sicherheit bezieht sich auch hier nicht im umfassenden Sinne der polizeilichen Generalklausel auf die Unverletzlichkeit der Rechtsordnung (vgl. Schoch, in: Schoch, Besonderes Verwaltungsrecht, 15. Aufl. 2013, 2. Kap., Rn. 109 f. m.w.N.), sondern erhält seine Konturen in der Verbindung mit dem Begriff der „erheblichen“ Gefahr. Nach dem Verständnis des allgemeinen Sicherheitsrechts setzt dieser voraus, dass eine Gefahr für ein bedeutsames Rechtsgut gegeben sein muss, zu denen insbesondere Leib, Leben, Freiheit oder der Bestand des Staates gerechnet werden (vgl. Schoch, in: Schoch, a.a.O., 2. Kap., Rn. 150 m.w.N.). Auch hier ergibt sich bei einer verfassungsgeleiteten Auslegung der Vorschrift, dass für die Übermittlung von Daten aus besonders eingriffsintensiven Maßnahmen ein hinreichend gewichtiger Rechtsgüterschutz vorausgesetzt wird. 312

cc) Unverhältnismäßig weit und damit verfassungswidrig ist § 20v Abs. 5 Satz 1 Nr. 2 BKAG demgegenüber insoweit, als er eine Übermittlung auch allgemein zur Verhütung der in § 129a Abs. 1, 2 StGB genannten Straftaten erlaubt. Zwar sind dies nur besonders schwerwiegende Straftaten. Indem das Gesetz eine Übermittlung aber allgemein zur Verhütung solcher Straftaten erlaubt, fehlt es an jeder eingrenzenden Konkretisierung des Übermittlungsanlasses und können Informationen, auch wenn sie aus eingriffsintensiven Maßnahmen stammen, schon mit Blick auf einen nur potentiellen Informationsgehalt als Spurenansatz übermittelt werden. Dies genügt nach den oben entwickelten Maßstäben verfassungsrechtlichen Anforderungen nicht (siehe oben D I 2 b bb). Eine Übermittlung von Daten aus eingriffsintensiven Überwachungsmaßnahmen an andere Sicherheitsbehörden ist eine Zweckänderung und kommt nur dann in Betracht, wenn sich aus 313

ihnen zumindest ein konkreter Ermittlungsansatz für die Aufdeckung entsprechender Straftaten ergibt. Dies stellt die Vorschrift nicht sicher.

c) Nicht mit der Verfassung vereinbar ist auch § 20v Abs. 5 Satz 1 Nr. 3 BKAG, der die Übermittlung von Daten zur Strafverfolgung regelt. 314

aa) Unverhältnismäßig ist die Regelung zum einen insoweit, als sie in ihrer ersten Fallgruppe eine Übermittlung von Daten allgemein an die Maßstäbe eines Auskunftsverlangens nach der Strafprozessordnung knüpft und sich damit auch auf Daten aus nicht in Nr. 3 Satz 2 eigens geregelten, aber eingriffsintensiven Überwachungsmaßnahmen wie nach §§ 20g, 20j oder 20m BKAG bezieht. Mit der Anknüpfung an die Strafprozessordnung nimmt die Vorschrift insbesondere auf § 161 Abs. 1, 2 StPO Bezug. Dieser sichert die verfassungsrechtlich geforderte Begrenzung der Datenübermittlung jedoch nicht. Insbesondere folgt aus dieser Vorschrift nicht, dass die Daten nur zur Verfolgung solcher Straftaten genutzt werden dürfen, für die sie mit entsprechenden Mitteln erhoben werden dürften (siehe oben D I 2 b). § 161 Abs. 1 StPO regelt vielmehr eine Auskunfts- und damit Datenübermittlungspflicht für die Verfolgung von Straftaten aller Art. Die Beschränkungen des § 161 Abs. 2 StPO beziehen sich allein auf eine Verwertung der Daten zu Beweiszwecken im Strafverfahren. Demgegenüber schließen sie nicht aus, dass die Daten als Ermittlungsansatz auch zur Aufklärung aller, auch geringfügiger Straftaten genutzt werden dürfen (vgl. Schmitt, in: Meyer-Goßner/Schmitt, StPO, 58. Aufl. 2015, § 161 Rn. 18d f.). Dies stellt die verfassungsrechtlich gebotene Begrenzung der geänderten Datennutzung auf einen gleichgewichtigen Rechtsgüterschutz nicht sicher. Überdies gewährleistet die Vorschrift nicht, dass nur solche Daten übermittelt werden dürfen, die konkrete Ermittlungsansätze zur Aufdeckung der fraglichen Straftaten erkennen lassen. 315

bb) Unverhältnismäßig ist die Regelung zum anderen aber auch insoweit, als sie in Satz 2 für die Nutzung von Daten aus Maßnahmen gemäß §§ 20h, 20k und 20l BKAG eigene Anforderungen stellt. Der Gesetzgeber erlaubt deren Übermittlung zur Verfolgung von Straftaten, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind (§ 20v Abs. 5 Satz 1 Nr. 3, 2. Satz BKAG). Für Daten aus Maßnahmen gemäß §§ 20k und 20l BKAG wirkt dies gegenüber dem allgemeinen Verweis auf die Vorschriften der Strafprozessordnung und damit auf § 161 Abs. 1, Abs. 2 Satz 1 StPO als Einschränkung, für Daten aus Wohnraumüberwachungen hingegen, deren Verwendungsänderung in § 161 Abs. 2 Satz 2, § 100d Abs. 5 Nr. 3 StPO enger geregelt ist, als Erweiterung. Unabhängig hiervon genügt diese Schwelle dem Kriterium der hypothetischen Datenneuerhebung 316

nicht. Für die Wohnraumüberwachung hat das Bundesverfassungsgericht ausdrücklich festgestellt, dass eine Höchststrafe von mindestens fünf Jahren keine hinreichende Schwelle für die Anordnung einer solchen Maßnahme bildet und dies auch für jede weitere Verwendung der Daten, einschließlich einer solchen als Spurenansatz gilt (vgl. BVerfGE 109, 279 <347 f., 377>). Nichts anderes kann für den Zugriff auf informationstechnische Systeme gelten, der als vergleichbar schwerer Eingriff unter denselben Anforderungen steht. Weniger streng sind zwar die Anforderungen an die Telekommunikationsüberwachung. Doch setzen die Datenerhebung und entsprechend eine zweckändernde Übermittlungsbefugnis auch hier zumindest die Ausrichtung an schweren Straftaten voraus (vgl. BVerfGE 125, 260 <328 f.>; 129, 208 <243>). Es ist deshalb unverhältnismäßig, wenn § 20v Abs. 5 Satz 1 Nr. 3, 2. Satz BKAG schon Straftaten mit einer Höchststrafe von mindestens fünf Jahren genügen lässt, womit auch Delikte eingeschlossen sind, die nur zur mittleren Kriminalität zu rechnen sind und unter Umständen auch Delikte der Massenkriminalität wie den einfachen Diebstahl, die öffentliche Verleumdung oder die einfache Körperverletzung umfassen.

Verfassungsrechtlich zu beanstanden ist weiterhin, dass Daten aus optischen Wohnraumüberwachungen von einer Übermittlung an die Strafverfolgungsbehörden nicht ausgeschlossen sind. Art. 13 Abs. 3 GG erlaubt für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies darf durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden. 317

cc) Während an die Übermittlung von Daten aus besonders eingriffsintensiven Überwachungsmaßnahmen qualifizierte Anforderungen zu stellen sind, ist eine Übermittlung von Daten, die durch niederschwelligere Eingriffe erhoben wurden (vgl. etwa §§ 20b ff., §§ 20q ff. BKAG), in weitergehendem Umfang verfassungsrechtlich erlaubt. Die Voraussetzungen des § 20v Abs. 5 Satz 1 Nr. 3 BKAG können hierfür eine tragfähige Grundlage bilden. Der Gesetzgeber muss hier jedoch zwischen den verschiedenen Daten unterscheiden. In der derzeitigen Fassung ist die Vorschrift undifferenziert weit und damit unverhältnismäßig. 318

d) Nicht mit den verfassungsrechtlichen Anforderungen vereinbar ist auch § 20v Abs. 5 Satz 3 Nr. 1 BKAG, der die Übermittlung von Daten an die Verfassungsschutzbehörden und den Militärischen Abschirmdienst erlaubt. 319

Die Vorschrift, die für alle Daten außer solche aus Wohnraumüberwachungsmaßnahmen gilt (vgl. § 20v Abs. 5 Satz 5 BKAG), erlaubt eine Übermittlung an die 320

vorgenannten Behörden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Daten zur Sammlung und Auswertung von Informationen erforderlich sind über Bestrebungen, die in den Aufgabenbereich der Verfassungsschutzbehörden oder des Militärischen Abschirmdienstes fallen. Damit genügt sie dem für eine zweckändernde Datenübermittlung maßgeblichen Kriterium der hypothetischen Neuerhebung nicht (siehe oben D I 2 b). Zwar dient die Datenübermittlung angesichts der insoweit in Bezug genommenen Aufgaben der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes grundsätzlich dem Schutz besonders gewichtiger Rechtsgüter. Auch kann eine Übermittlung von bestimmten Daten wie solchen aus Maßnahmen gemäß § 20g BKAG mit Blick auf den für eine hypothetische Neuerhebung maßgeblichen § 8 BVerfSchG - über dessen Verfassungsmäßigkeit hier nicht zu entscheiden ist - in relativ weitem Umfang gerechtfertigt sein. Eine Regelung jedoch, die für praktisch alle Daten ohne konkretisierende Eingriffsschwelle die Übermittlung zur allgemeinen Unterstützung bei der Aufgabenwahrnehmung erlaubt, ist unverhältnismäßig weit. Das Kriterium der hypothetischen Datenneuerhebung verlangt zwar grundsätzlich nicht, dass eine für die Datenerhebung geforderte konkretisierte Gefahrenlage - wie sie ungeachtet ihres im Wesentlichen auf das Vorfeld von Gefahren beschränkten Handlungsauftrags grundsätzlich auch für Datenerhebungen der Verfassungsschutzbehörden verlangt wird (vgl. BVerfGE 100, 313 <383 f.>; 120, 274 <329 f.>; 130, 151 <205 f.>) - jeweils neu auch immer zur Voraussetzung einer Übermittlung gemacht werden muss (siehe oben D I 2 b bb). Verfassungsrechtlich geboten ist jedoch, dass nur Daten übermittelt werden dürfen, die aus Sicht des Bundeskriminalamts als konkrete Ermittlungsansätze für die Aufdeckung von Straftaten oder Gefahren für hochrangige Rechtsgüter zugleich konkrete Erkenntnisse zu einer Gefährdung hochrangiger Rechtsgüter erkennen lassen (vgl. für die Datenübermittlung von Nachrichtendiensten an das Bundeskriminalamt BVerfGE 133, 277 <329 Rn. 123>), die für die Lagebeurteilung nach Maßgabe der Aufgaben des Verfassungsschutzes bedeutsam sind. Für die Übermittlung von Daten aus Online-Durchsuchungen bedarf es darüber hinaus - ebenso wie für die vom Gesetzgeber insoweit bereits gesondert geregelten Daten aus Wohnraumüberwachungen - des Vorliegens der für die Datenerhebung maßgeblichen Eingriffsschwelle selbst, das heißt einer im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>).

e) Entsprechend genügt auch § 20v Abs. 5 Satz 4 BKAG den verfassungsrechtlichen Anforderungen nicht. Die Vorschrift erlaubt eine Übermittlung von Daten an den Bundesnachrichtendienst unter entsprechenden Maßgaben wie § 20v Abs. 5 Satz 3 Nr. 1 BKAG. Die Unterschiede in den Formulierungen haben - auch unter Berücksichtigung der Gesetzesbegründung (vgl. BTDrucks 16/9588, 321

S. 34) - keinen erkennbar sachlichen Gehalt und vermögen jedenfalls die verfassungsrechtliche Beurteilung nicht zu ändern. Die verfassungsrechtlichen Mängel des § 20v Abs. 5 Satz 3 Nr. 1 BKAG gelten auch für diese Vorschrift.

4. Hinsichtlich aller Übermittlungsbefugnisse fehlt es übergreifend schließlich an gesetzlichen Regelungen, die eine hinreichende aufsichtliche Kontrolle sicherstellen. Die für die Datenerhebung geltenden Anforderungen an eine sachhaltige Protokollierung und eine effektive Kontrolle durch die Bundesdatenschutzbeauftrage gelten auch hier (vgl. oben C IV 6 d). 322

IV.

§ 14 Abs. 1 Satz 1 Nr. 1 und 3, Satz 2 BKAG, der - sofern nicht für Mitgliedstaaten der Europäischen Union die hier nicht streitgegenständliche Regelung des § 14a BKAG einschlägig ist - die Übermittlung von Daten an öffentliche Stellen anderer Staaten regelt, genügt den verfassungsrechtlichen Anforderungen teilweise gleichfalls nicht. 323

1. Die Übermittlung von personenbezogenen Daten an öffentliche Stellen anderer Staaten ist, wie die Übermittlung an innerstaatliche Stellen auch, eine Zweckänderung. Sie ist insoweit nach den allgemeinen Grundsätzen jeweils an den Grundrechten zu messen, in die bei der Datenerhebung eingegriffen wurde (siehe oben D I 2 a). Für die Übermittlung ins Ausland gelten aber auch mit Blick auf die Achtung fremder Rechtsordnungen und -anschauungen eigene verfassungsrechtliche Bedingungen. 324

a) Eine Übermittlung von Daten ins Ausland führt dazu, dass die Gewährleistungen des Grundgesetzes nach der Übermittlung nicht mehr als solche zur Anwendung gebracht werden können und stattdessen die im Ausland geltenden Standards Anwendung finden. Dies steht einer Übermittlung ins Ausland jedoch nicht grundsätzlich entgegen. Das Grundgesetz bindet die Bundesrepublik Deutschland mit der Präambel, Art. 1 Abs. 2, Art. 9 Abs. 2, Art. 16 Abs. 2, Art. 23 bis Art. 26 und Art. 59 Abs. 2 GG in die internationale Gemeinschaft ein und hat die deutsche öffentliche Gewalt programmatisch auf internationale Zusammenarbeit ausgerichtet (vgl. BVerfGE 63, 343 <370>; 111, 307 <318 f.>; 112, 1 <25, 27>). Hierzu gehört ein Umgang mit anderen Staaten auch dann, wenn deren Rechtsordnungen und -anschauungen nicht vollständig mit den deutschen innerstaatlichen Auffassungen übereinstimmen (vgl. BVerfGE 31, 58 <75 ff.>; 63, 343 <366>; 91, 335 <340, 343 ff.>; 108, 238 <247 f.>). Ein solcher Datenaustausch 325

zielt auch darauf, die zwischenstaatlichen Beziehungen im gegenseitigen Interesse wie auch die außenpolitische Handlungsfreiheit der Bundesregierung zu erhalten (vgl. BVerfGE 108, 129 <137>).

Auch bei der Entscheidung über eine Übermittlung von personenbezogenen Daten ins Ausland bleibt die deutsche Staatsgewalt im Ausgangspunkt allerdings an die Grundrechte gebunden (Art. 1 Abs. 3 GG); die ausländische Staatsgewalt ist nur ihren eigenen rechtlichen Bindungen verpflichtet. 326

Von daher ergeben sich zum einen Grenzen einer Übermittlung in Blick auf die Wahrung datenschutzrechtlicher Garantien. Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürfen durch einen Austausch zwischen den Sicherheitsbehörden nicht in ihrer Substanz unterlaufen werden. Der Gesetzgeber hat daher dafür Sorge zu tragen, dass dieser Grundrechtsschutz durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen ebenso wenig ausgehöhlt wird wie durch eine Entgegennahme und Verwertung von durch ausländische Behörden menschenrechtswidrig erlangten Daten. 327

Zum anderen ergeben sich Grenzen in Blick auf die Nutzung der Daten durch den Empfängerstaat, wenn dort Menschenrechtsverletzungen zu besorgen sind. Zwingend auszuschließen ist danach jedenfalls die Datenübermittlung an Staaten, wenn zu befürchten ist, dass elementare rechtsstaatliche Grundsätze verletzt werden (vgl. BVerfGE 108, 129 <136 f.>). Keinesfalls darf der Staat seine Hand zu Verletzungen der Menschenwürde reichen (vgl. BVerfG, Beschluss des Zweiten Senats vom 15. Dezember 2015 - 2 BvR 2735/14 -, Rn. 62 m.w.N.). 328

b) Die Übermittlung von Daten an das Ausland setzt danach eine Begrenzung auf hinreichend gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen (aa), sowie die Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland voraus (bb). Im Übrigen bedarf es auch hier der Sicherstellung einer wirksamen inländischen Kontrolle (cc). Die Anforderungen sind durch normenklare Grundlagen im deutschen Recht sicherzustellen (dd). 329

aa) Für die Anforderungen an den Übermittlungs- und Nutzungszweck gelten grundsätzlich die nach deutscher Rechtsordnung maßgeblichen verfassungsrechtlichen Kriterien der Zweckänderung (siehe oben D I 2): Eine Übermittlung ist zulässig, soweit die übermittelten Daten auch für den Übermittlungszweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (Kriterium der hypo- 330

thetischen Datenneuerhebung). Die Übermittlung muss damit der Aufdeckung vergleichbar gewichtiger Straftaten oder dem Schutz vergleichbar gewichtiger Rechtsgüter dienen, wie sie für die ursprüngliche Datenerhebung maßgeblich waren. Sie ist allerdings grundsätzlich nicht an das Vorliegen der für die Datenerhebung erforderlichen Konkretisierung der Gefahrenlage oder des Tatverdachts gebunden; es reicht, dass sich aus den übermittelten Informationen oder der Anfrage des Empfängerstaats im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung solcher Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für solche Rechtsgüter ergeben. Strenger sind insoweit die Voraussetzungen für die Übermittlung von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen, für die die für die Datenerhebung maßgeblichen Eingriffsschwellen vollständig vorliegen müssen (siehe oben D I 2 b bb; vgl. ferner BVerfGE 109, 279 <377, 379>; 120, 274 <329 ff.>).

Hinsichtlich der damit verbundenen Beurteilung der für das Empfängerland zu eröffnenden Nutzung der Daten, wie sie insbesondere bei einem ausländischen Übermittlungsersuchen erforderlich ist, ist die Eigenständigkeit der jeweils anderen Rechtsordnung zu berücksichtigen. Für die Frage der Gleichgewichtigkeit der Nutzungszwecke ist insoweit einzustellen, dass die deutsche Rechtsordnung hier auf eine andere Rechtsordnung trifft, deren Abgrenzungslinien, Kategorien und Wertungen mit denen der deutschen Rechtsordnung und auch des Grundgesetzes nicht identisch sind und auch nicht sein müssen. Dass Zweckbegrenzungen in der ausländischen Rechtsordnung insoweit im Einzelnen nicht identisch zur deutschen Rechtsordnung abgebildet werden, steht einer Übermittlung nicht von vornherein entgegen. Verwendungsbeschränkungen sind den Empfangsbehörden bei der Übermittlung klar und ausdrücklich mitzuteilen. 331

bb) Die Übermittlung personenbezogener Daten ins Ausland setzt weiter einen datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen vereinbaren Umgang mit den übermittelten Daten im Empfängerstaat (1) und eine entsprechende Vergewisserung hierüber seitens des deutschen Staates (2) voraus. 332

(1) Eine Übermittlung von Daten ins Ausland verlangt, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist. 333

(a) Für die Anforderungen an den datenschutzrechtlichen Umgang mit den übermittelten Daten ist allerdings nicht erforderlich, dass im Empfängerstaat vergleichbare Regelungen zur Verarbeitung personenbezogener Daten wie nach der 334

deutschen Rechtsordnung gelten oder ein gleichartiger Schutz gewährleistet ist wie nach dem Grundgesetz. Das Grundgesetz anerkennt vielmehr die Eigenständigkeit und Verschiedenartigkeit der Rechtsordnungen und respektiert sie grundsätzlich auch im Rahmen des Austauschs von Daten. Abgrenzungen und Wertungen müssen nicht mit denen der deutschen Rechtsordnung und auch des deutschen Grundgesetzes übereinstimmen.

Erlaubt ist eine Übermittlung der Daten ins Ausland jedoch nur, wenn auch durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Dies bedeutet nicht, dass in der ausländischen Rechtsordnung institutionelle und verfahrensrechtliche Vorkehrungen nach deutschem Vorbild gewährleistet sein müssen; insbesondere müssen nicht die formellen und institutionellen Sicherungen vorhanden sein, die datenschutzrechtlich für deutsche Stellen gefordert werden (siehe oben C IV 6). Geboten ist in diesem Sinne die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat (vgl. ähnlich EuGH, Urteil vom 6. Oktober 2015 - C-362/14 -, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 <3155>, Rn. 73; vgl. auch Art. 8 EMRK; dazu EGMR [GK], Zakharov v. Russland, Urteil vom 4. Dezember 2015, Nr. 47143/06, §§ 227 ff.; Art. 17 Abs. 1 Satz 1 Internationaler Pakt über bürgerliche und politische Rechte vom 19. Dezember 1966, BGBl 1973 II S. 1534, UNTS 999, S. 171; Art. 12 Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948, Res. 217 A III der UN-Generalversammlung, GAOR III, Doc. A/810, S. 71; vgl. dazu The right to privacy in the digital age, UN General Assembly Resolution 68/167 vom 18. Dezember 2013, UN Doc. A/Res/68/167 [2014], Z. 4). In Betracht zu nehmen ist insoweit insbesondere, ob für die Verwendung der Daten die - bei der Übermittlung mitgeteilten - Grenzen durch Zweckbindung und Löschungspflichten sowie grundlegende Anforderungen an Kontrolle und Datensicherheit wenigstens grundsätzlich Beachtung finden. Maßgeblich für diese Beurteilung sind die innerstaatlichen Rechtsvorschriften und die internationalen Verpflichtungen des Empfängerstaats sowie ihre Umsetzung in der täglichen Anwendungspraxis (vgl. ähnlich EuGH, Urteil vom 6. Oktober 2015 - C-362/14 -, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 <3155>, Rn. 75). 335

(b) Hinsichtlich der Besorgnis etwaiger Menschenrechtsverletzungen durch die Nutzung der Daten im Empfängerstaat muss insbesondere gewährleistet erscheinen, dass sie dort weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden (vgl. Art. 16a Abs. 3 336

GG). Der Gesetzgeber hat insgesamt Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Art. 1 Abs. 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird.

(2) Die Gewährleistung des geforderten Schutzniveaus im Empfängerstaat muss nicht für jeden Fall einzeln geprüft und durch völkerrechtlich verbindliche Einzelzusagen abgesichert werden. Der Gesetzgeber kann diesbezüglich auch eine generalisierende tatsächliche Einschätzung der Sach- und Rechtslage der Empfängerstaaten durch das Bundeskriminalamt ausreichen lassen. Diese kann so lange Geltung beanspruchen, wie sie nicht durch entgegenstehende Tatsachen in besonders gelagerten Fällen erschüttert wird (vgl. BVerfG, Beschluss des Zweiten Senats vom 15. Dezember 2015 - 2 BvR 2735/14 -, Rn. 69 m.w.N.). 337

Lassen sich Entscheidungen mit Blick auf einen Empfängerstaat nicht auf solche Beurteilungen stützen, bedarf es aber einer mit Tatsachen unterlegten Einzelfallprüfung, aus der sich ergibt, dass die Beachtung jedenfalls der grundlegenden Anforderungen an den Umgang mit Daten hinreichend gewährleistet ist (siehe oben D IV 1 b bb (1)). Erforderlichenfalls können und müssen verbindliche Einzelgarantien abgegeben werden. Grundsätzlich ist eine verbindliche Zusicherung geeignet, etwaige Bedenken hinsichtlich der Zulässigkeit der Datenübermittlung auszuräumen, sofern nicht im Einzelfall zu erwarten ist, dass die Zusicherung nicht eingehalten wird (vgl. BVerfGE 63, 215 <224>; 109, 38 <62>; BVerfG, Beschluss des Zweiten Senats vom 15. Dezember 2015 - 2 BvR 2735/14 -, Rn. 70). Welche Anforderungen im Einzelnen gelten, kann der Gesetzgeber auch von einer Einzelfallabwägung abhängig machen. 338

Die Vergewisserung über das geforderte Schutzniveau - sei es generalisiert, sei es im Einzelfall - ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können (vgl. auch EuGH, Urteil vom 6. Oktober 2015 - C-362/14 -, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 <3155 ff.>, Rn. 78, 81, 89). 339

cc) Auch ansonsten gelten in Deutschland die Anforderungen an eine wirksame aufsichtliche Kontrolle einschließlich einer hierfür geeigneten Protokollierung 340

der jeweiligen Übermittlungsvorgänge sowie das Erfordernis von Berichtspflichten (siehe oben C IV 6 d, e).

dd) Die vorstehend entwickelten Maßgaben müssen in einer den Grundsätzen der Bestimmtheit und Normenklarheit entsprechenden Weise gesetzlich ausgeformt sein. Dazu gehört auch, dass Ermächtigungsgrundlagen, die, soweit zulässig, eine Übermittlung von Daten zur Informationsgewinnung durch einen Abgleich mit Daten ausländischer Behörden und einen Rückfluss ergänzender Erkenntnisse herbeiführen sollen, als solche normenklar ausgestaltet sind. 341

2. Die Übermittlungstatbestände des § 14 Abs. 1 Satz 1 Nr. 1, 3 und Satz 2 BKAG sind mit diesen Anforderungen nicht vereinbar. 342

a) § 14 Abs. 1 Satz 1 Nr. 1 BKAG genügt, soweit er als eigene Ermächtigungsgrundlage zu verstehen ist (vgl. Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 14 BKAG, Rn. 6), den verfassungsrechtlichen Anforderungen an eine Zweckänderung nicht. Indem er dem Bundeskriminalamt eine Datenübermittlung allgemein zur Erfüllung der ihm obliegenden Aufgaben erlaubt, fehlt es an Maßgaben, die sicherstellen, dass Daten aus eingriffsintensiven Überwachungsmaßnahmen nur für Zwecke übermittelt werden dürfen, die dem Kriterium der hypothetischen Datenneuerhebung entsprechen (vgl. oben D I 2 b). Die Befugnis ist damit nicht hinreichend eingegrenzt und unverhältnismäßig. 343

b) Gleichfalls zu weit und deshalb mit den verfassungsrechtlichen Anforderungen nicht vereinbar ist § 14 Abs. 1 Satz 1 Nr. 3 BKAG in Bezug auf Daten aus Wohnraumüberwachungen. Nach den oben entwickelten Maßgaben ist für diese sicherzustellen, dass sie nur bei Vorliegen einer dringenden Gefahr übermittelt werden dürfen (siehe oben D I 2 b bb; vgl. ferner BVerfGE 109, 279 <377, 379>). Eine solche Begrenzung enthält die Vorschrift nicht. 344

Hinsichtlich anderer Daten ist die Vorschrift bei sachgerechter Auslegung demgegenüber verfassungsrechtlich nicht zu beanstanden. Indem die Vorschrift in Anknüpfung an die Terminologie des allgemeinen Sicherheitsrechts eine „erhebliche Gefahr“ für die öffentliche Sicherheit verlangt, erlaubt sie eine Übermittlung nur zum Schutz besonders qualifizierter Rechtsgüter und kann - entsprechend der Regelung des § 20v Abs. 5 Satz 1 Nr. 2 BKAG (siehe oben D III 3 b bb) - im Lichte der entsprechenden Datenerhebungsvorschriften ausgelegt werden. Da die Vorschrift überdies klarstellt, dass es sich hierbei um eine auch im Einzelfall beste- 345

hende Gefahr handeln muss, erfüllt sie auch die Anforderungen an die Übermittlung von Daten aus Online-Durchsuchungen (siehe oben D I 2 b bb).

c) Mit den Anforderungen an eine Zweckänderung nicht vereinbar ist schließlich der Übermittlungstatbestand des § 14 Abs. 1 Satz 2 BKAG. 346

Die Vorschrift stellt nicht hinreichend sicher, dass die Übermittlung von Daten in Anknüpfung an das Kriterium der hypothetischen Datenneuerhebung auf den Schutz hinreichend gewichtiger Rechtsgüter begrenzt bleibt (vgl. oben D I 2 b). Sie erlaubt eine Übermittlung allgemein zur Verhütung von Straftaten von erheblicher Bedeutung, ohne zu unterscheiden, mit welchen Mitteln die jeweiligen Daten erhoben wurden. Diese Schwelle rechtfertigt jedoch die Übermittlung von Daten aus besonders eingriffsintensiven Maßnahmen nicht. Knüpft der Gesetzgeber bei Übermittlungen zur Gefahrenabwehr wie hier zur Straftatenverhütung für die Bestimmung der neuen Zwecke nicht unmittelbar an Rechtsgütern, sondern an der Art der zur verhütenden Straftaten an, so ist insoweit an die entsprechenden Gewichtungen, die für die strafprozessuale Datenerhebung gelten, anzuknüpfen. Danach ist etwa die Übermittlung von Daten aus Maßnahmen der Telekommunikationsüberwachung auf die Verhütung von schweren Straftaten und von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen auf die Verhütung von besonders schweren Straftaten beschränkt (vgl. BVerfGE 109, 279 <343 ff.>; 125, 260 <328 f.>; 129, 208 <243>; siehe auch oben C IV 1 a). Entsprechende Anforderungen sieht die Vorschrift für die Übermittlung indessen nicht vor. 347

Darüber hinaus genügt die Vorschrift auch hinsichtlich des geforderten Konkretisierungsgrads der Gefahrenlage nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen. Indem sie zur Übermittlung von Daten unterschiedslos dann ermächtigt, wenn „Anhaltspunkte“ für eine künftige Straftatenbegehung bestehen, erlaubt sie auch eine Übermittlung von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen, ohne eine dringende Gefahr (vgl. BVerfGE 109, 279 <377, 379> zur Wohnraumüberwachung) oder eine im Einzelfall hinreichend konkretisiert drohende Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.> zur Online-Durchsuchung) zur Voraussetzung zu machen. Dies ist mit den oben dargelegten Anforderungen nicht vereinbar (vgl. oben D I 2 b bb). Soweit hingegen andere Daten betroffen sind, ist gegen diese Eingriffsschwelle nichts zu erinnern. Indem die Vorschrift Anhaltspunkte über eine Straftatenbegehung verlangt, macht sie die Übermittlung davon abhängig, dass sich aus den übermittelten Daten zumindest konkrete Ermittlungsansätze ergeben. Dies steht mit den verfassungsrechtlichen Anforderungen in Einklang. 348

d) Keinen durchgreifenden verfassungsrechtlichen Bedenken unterliegt demgegenüber die übergreifende Regelung des § 14 Abs. 7 BKAG. 349

aa) Indem § 14 Abs. 7 Satz 7 BKAG anordnet, dass die Übermittlung unterbleibt, soweit im Einzelfall schutzwürdige Interessen der Betroffenen am Ausschluss der Übermittlung überwiegen, lässt die Regelung Raum für die von Verfassungs wegen geforderte Vergewisserung, dass die gebotenen menschenrechtlichen Standards eingehalten werden. 350

bb) Den datenschutzrechtlichen Anforderungen des Grundgesetzes trägt § 14 Abs. 7 BKAG Rechnung, indem er die Übermittlung verfahrensrechtlich ausgestaltet und Anforderungen an die Vergewisserung über ein angemessenes Datenschutzniveau im Empfängerstaat festlegt. 351

(1) Die Vorschrift begründet eine Verantwortung des Bundeskriminalamts für die Zulässigkeit der Datenübermittlung und verlangt damit insbesondere auch die Prüfung, ob sich aus den übermittelten Informationen selbst oder im Zusammenhang mit einem Übermittlungsersuchen hinreichend plausibel Anhaltspunkte ergeben, nach denen die Übermittlung der Daten für die jeweiligen Zwecke erlaubt ist. Bei sachgerechtem Verständnis stellt die Norm zugleich sicher, dass der Übermittlungszweck förmlich mitgeteilt sowie darauf hingewiesen wird, dass die Daten nur zu diesem Zweck genutzt werden dürfen. Nicht zu beanstanden ist insoweit, dass die Zweckbindung nur in Form eines Hinweises, nicht aber durch eine förmliche Verpflichtung abgesichert wird und auch über den Löschungszeitraum nur ein informatorischer Hinweis auf die deutsche Rechtslage vorgeschrieben ist. Grundsätzlich reicht es, wenn sich die Behörden mit Blick auf die Sach- und Rechtslage im Empfängerstaat in tatsächlicher Hinsicht über das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat vergewissern. 352

(2) Eine solche Vergewisserung sieht § 14 Abs. 7 Satz 7 bis 9 BKAG vor. Bei verfassungskonformer Auslegung ist diese Regelung mit den verfassungsrechtlichen Anforderungen vereinbar. Sie verbietet eine Übermittlung, wenn nach Maßgabe einer Abwägung im Einzelfall schutzwürdige Interessen der betroffenen Person überwiegen und zählt hierzu das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat. Bei einer Auslegung im Licht der Verfassung ist die Beachtung der grundrechtlichen Anforderungen an einen angemessenen datenschutzrechtlichen Umgang im Empfängerstaat allerdings nicht lediglich ein Abwägungsgesichtspunkt, der im Einzelfall zur Disposition der Behörden steht. Vielmehr sind insoweit grundrechtliche Mindestanforderungen stets zur Geltung zu 353

bringen. Ist eine Vergewisserung über einen zumindest elementaren Anforderungen genügenden rechtsstaatlichen Umgang des Empfängerstaats mit den übermittelten Daten nicht anders zu erreichen, bedarf es insoweit des Rückgriffs auf eine Einzelfallgarantie nach § 14 Abs. 7 Satz 9 BKAG. Bei diesem Verständnis sind gegen die Verfassungsmäßigkeit der Regelung keine Bedenken zu erheben. Die allgemeine Vorschrift des § 27 Abs. 1 Nr. 1 BKAG stützt die Regelung dabei ergänzend ab.

e) Im Übrigen genügen die Übermittlungsregelungen des § 14 Abs. 1 BKAG insoweit nicht den verfassungsrechtlichen Anforderungen, als es an einer hinreichenden Regelung der aufsichtlichen Kontrolle sowie der Anordnung von Berichtspflichten zur Übermittlungspraxis fehlt (siehe oben C IV 6 d, e). Demgegenüber ist eine Protokollierungspflicht, wie verfassungsrechtlich geboten, in § 14 Abs. 7 Satz 3 BKAG vorgesehen (vgl. BVerfGE 133, 277 <370 Rn. 215>). Angesichts der Anwendbarkeit des § 19 BDSG fehlt es auch nicht an Auskunftsrechten der Betroffenen (vgl. BVerfGE 120, 351 <364 f.>; siehe oben C IV 6 b; C VI 3 b). 354

E.

I.

1. Die Feststellung einer Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Satz 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären (BVerfGE 109, 190 <235>). Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden 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 (vgl. BVerfGE 33, 1 <13>; 33, 303 <347 f.>; 40, 276 <283>; 41, 251 <266 ff.>; 51, 268 <290 ff.>; 109, 190 <235 f.>). Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (vgl. BVerfGE 40, 276 <283>; 41, 251 <267>). 355

2. Danach sind § 20h Abs. 1 Nr. 1 c und § 20v Abs. 6 Satz 5 BKAG für verfassungswidrig und nichtig zu erklären. Die Vorschriften genügen den verfassungsrechtlichen Anforderungen nicht und eine Regelung mit vergleichbarem Regelungsgehalt kann der Gesetzgeber auch durch Nachbesserung nicht herbeiführen. 356

Demgegenüber sind § 20g Abs. 1 bis 3, §§ 20h, 20j, 20k, 20l, § 20m Abs. 1, 3 - diesbezüglich auch § 20v Abs. 6 Satz 3, 2. Halbsatz - und § 20u Abs. 1, 2 sowie § 20v Abs. 4 Satz 2, Abs. 5 Satz 1 bis 4 (ohne Satz 3 Nr. 2), § 14 Abs. 1 Satz 1 Nr. 1 und 3, Satz 2 BKAG lediglich für mit der Verfassung unvereinbar zu erklären; die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung bis zum Ablauf des 30. Juni 2018 zu verbinden. Die Gründe für die Verfassungswidrigkeit dieser Vorschriften betreffen nicht den Kern der mit ihnen eingeräumten Befugnisse, sondern nur einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung; die Reichweite ihrer Beurteilung als insgesamt verfassungswidrig ergibt sich dabei maßgeblich daraus, dass es an einzelnen übergreifend die Verhältnismäßigkeit sichernden Regelungen, etwa zur Gewährleistung einer effektiven Aufsicht, fehlt. Der Gesetzgeber kann in diesen Fällen die verfassungsrechtlichen Beanstandungen nachbessern und damit den Kern der mit den Vorschriften verfolgten Ziele auf verfassungsmäßige Weise verwirklichen. Angesichts der großen Bedeutung einer wirksamen Bekämpfung des internationalen Terrorismus für den freiheitlichen und demokratischen Rechtsstaat ist unter diesen Umständen ihre vorübergehende Fortgeltung eher hinzunehmen als deren Nichtigkeitserklärung, die dem Bundeskriminalamt bis zu einer Neuregelung zentrale Ermittlungsbefugnisse bei der Abwehr des internationalen Terrorismus nehmen würde. 357

Die Anordnung der Fortgeltung bedarf mit Blick auf die betroffenen Grundrechte jedoch einschränkender Maßgaben. Anzuordnen ist zum einen, dass Maßnahmen gemäß § 20g Abs. 2 Nr. 1, 2 b, 4 und 5 BKAG nur durch das Gericht angeordnet werden dürfen; bei Gefahr im Verzug gilt § 20g Abs. 3 Satz 2 bis 4 BKAG entsprechend. Zum anderen dürfen Maßnahmen gemäß § 20g Abs. 1 Nr. 2, § 20l Abs. 1 Nr. 2 und § 20m Abs. 1 Nr. 2 BKAG nur angeordnet werden, wenn die Voraussetzungen des § 20k Abs. 1 Satz 2 BKAG in der in den Urteilsgründen dargelegten verfassungskonformen Auslegung vorliegen. Schließlich ist eine weitere Verwendung von Daten gemäß § 20v Abs. 4 Satz 2 BKAG oder eine Übermittlung von Daten gemäß § 20v Abs. 5 und § 14 Abs. 1 BKAG betreffend Daten aus Wohnraumüberwachungen (§ 20h BKAG) nur bei Vorliegen einer dringenden Gefahr und betreffend Daten aus Online-Durchsuchungen (§ 20k BKAG) nur bei Vorliegen einer im Einzelfall drohenden Gefahr für die jeweils maßgeblichen Rechtsgüter zulässig. 358

II.

Die Entscheidung ist teilweise mit Gegenstimmen ergangen. Dies gilt insbesondere für die Verwerfung von § 20g Abs. 1 Nr. 2, § 20l Abs. 1 Nr. 2 und § 20m Abs. 1 Nr. 2 BKAG als verfassungswidrig (anstatt sie einer verfassungskonformen Auslegung zuzuführen), für die Annahme der Ermittlungsbefugnisse des § 20g BKAG als kernbereichstypisch, für die Beanstandung unzureichender Aufsichtsbefugnisse, Berichts- und Sanktionspflichten und teilweise auch fehlender Richtervorbehalte, die mit 5:3 Stimmen ergangen sind. 359

Die Auslagenentscheidung beruht auf § 34a Abs. 2 BVerfGG. 360

Kirchhof Gaier Eichberger

Schluckebier Masing Paulus

Baer Britz

Abweichende Meinung des Richters Eichberger

zum Urteil des Ersten Senats vom 20. April 2016

- 1 BvR 966/09 -
- 1 BvR 1140/09 -

Ich kann das Urteil in einer Reihe der in Bezug auf die angegriffenen Normen gezogenen Schlussfolgerungen und in Teilen der Begründung nicht mittragen. 1

I.

Das Urteil fasst die in der Rechtsprechung des Gerichts entwickelten Grundsätze zur Datenerhebung und Datenweitergabe bei eingriffsintensiven Ermittlungsmaßnahmen für den hier maßgeblichen Bereich der Terrorismusabwehr zusammen, konsolidiert sie und entwickelt sie in Teilen fort. Den übergreifend formulierten Grundsätzen zu den spezifischen verfassungsrechtlichen Anforderungen an den Einsatz dieser Ermittlungs- und Überwachungsmaßnahmen und an die weitere Verwendung der daraus gewonnenen Erkenntnisse kann ich in weiten Teilen zustimmen. In einer ganzen Reihe von Punkten stellt der Senat jedoch überzogene Anforderungen an die Datenerhebung und -weiterverwendung und insbesondere an die daraus von ihm abgeleiteten Ausgestaltungspflichten für den Gesetzgeber. Zwar bewegt sich das Urteil in den grundsätzlichen verfassungsrechtlichen Wertungen zur Zulässigkeit von Eingriffen in die Freiheitsrechte aus Gründen der vom Staat zu gewährleistenden Sicherheit wie auch in den daraus im Einzelnen abgeleiteten Anforderungen auf der Linie der hierzu vor allem in den letzten 12 Jahren entwickelten Rechtsprechung des Gerichts. Vorgaben dieser Strenge und Detailgenauigkeit an den Gesetzgeber ließen und lassen sich nach meiner Überzeugung der Verfassung aber nicht entnehmen (vgl. meine bereits in diese Richtung zielende Abweichende Meinung in BVerfGE 125, 380 zum Urteil des Senats zur Vorratsdatenspeicherung - BVerfGE 125, 260). 2

Die vom Senat aufgestellten Grundsätze sind fast ausschließlich auf der Stufe der Verhältnismäßigkeitsprüfung im engeren Sinne vorgenommene Ableitungen aus der Abwägung zwischen den Belastungen eingriffsintensiver Maßnahmen für die Grundrechte der Betroffenen einerseits und den Schutzpflichten des Staates bei der Abwehr terroristischer Gefahren andererseits. Dabei berücksichtigt der 3

Senat nicht ausreichend, dass dem Gesetzgeber auch auf dieser Stufe der Verhältnismäßigkeitsprüfung eine Einschätzungsprärogative in Bezug auf die tatsächliche Beurteilung einer Gefahrenlage und ihre prognostische Entwicklung zukommt. Auch hat der Gesetzgeber einen ersten Zugriff bei der Gewichtung des mit dem Gesetz verfolgten Regelungsziels. Zwar unterliegt die vom Gesetzgeber vorgenommene Abwägung auf der Ebene der Verhältnismäßigkeitsprüfung im engeren Sinne einer grundsätzlich strengen Kontrolle durch das Bundesverfassungsgericht, ohne jedoch die Kontrollperspektive im Hinblick auf tatsächliche Einschätzungsprärogative und den Wertungsspielraum bei der Gewichtung des legitimen Ziels zu verlassen.

Auf dieser Grundlage gelange ich schon im Ausgangspunkt zu einer anderen 4
Gewichtung bei der beschriebenen Abwägung, als sie der Entscheidung des Senats zugrunde liegt. Dies führt zu teilweise anderen Ergebnissen bei den Grundsätzen, insbesondere aber bei den konkreten Schlussfolgerungen für die angegriffenen Maßnahmen. Zwar sind die Grundrechtsberechtigten bereits durch die latente Drohung heimlicher Überwachungs- und Ermittlungsmaßnahmen Belastungen mit höchster Eingriffsintensität ausgesetzt und im Falle ihres Einsatzes auch direkt davon betroffen. Bei der Gewichtung der latenten Bedrohungslage ist jedoch zu berücksichtigen, dass die allermeisten der angegriffenen Normen zu Einzelmaßnahmen und nicht zu generalisierten Datenerhebungen mit großer Streubreite ermächtigen. Sofern durch den konkreten Einsatz von Ermittlungsmaßnahmen Menschen betroffen werden, die keine oder nur in geringem Umfang ihnen zurechenbare Verantwortung für den Ermittlungsanlass gegeben haben, wird ihnen damit in staatsbürgerlicher Inpflichtnahme ein Sonderopfer abverlangt für die öffentliche Gewährleistung von Sicherheit. Es ist bedauerlich, dass diese nach meiner Überzeugung völlig zutreffende Beschreibung und Bewertung der Ermittlungsmaßnahmen gegenüber im polizeirechtlichen Sinne nicht Verantwortlichen keinen Eingang in die Urteilsgründe gefunden hat.

Ausgehend davon, dass es sich bei im Grunde all den im Urteil wiedergege- 5
benen übergreifenden Anforderungen an Verfahren und flankierende Schutzbestimmungen bei der Datenerhebung und -weitergabe und bei den daraus für die angegriffenen Normen gezogenen Konsequenzen um Ableitungen aus dem Verhältnismäßigkeitsgrundsatz handelt, hätte der Senat dem Gesetzgeber weniger detaillierte Vorgaben machen dürfen. Nicht alle der dem Gesetzgeber vorgeschriebenen Anforderungen an Verfahren, Transparenz und Kontrolle sind, selbst wenn viele von ihnen sinnvoll und richtig sein mögen, auch verfassungsrechtlich

genau so gefordert. Hier wäre nach meiner Überzeugung deutlich mehr an richterlicher Zurückhaltung geboten gewesen. Stattdessen führt das Urteil durch die Generalisierung früherer Erkenntnisse in einer Art allgemeinen Teil trotz zu begrüßender Konsolidierungsschritte im Ergebnis jedenfalls zu einer problematischen Verfestigung der überzogenen verfassungsrechtlichen Anforderungen in diesem Bereich. Die vom Gesetzgeber zu berücksichtigenden genauen verfassungsrechtlichen Vorgaben für je nach Überwachungs- und Ermittlungsmaßnahme differenzierten Eingriffsschwellen, abgeschichteten Schutzgutanforderungen, an die den Einzelmaßnahmen angepassten flankierenden Schutzvorkehrungen und Weiterverwendungsdirektiven haben damit ein von ihm nur mit enormen Regulierungsaufwand zu bewältigendes Maß an Komplexität erreicht. Die daraus resultierenden umfänglichen Regelwerke in den Bundes- und Landespolizeigesetzen werden auch auf der Ebene des Vollzugs die Polizeibeamten oft vor nur schwer lösbare Probleme stellen. Zwar sind klare gesetzliche Vorgaben gerade im Bereich eingriffsintensiver Überwachungsmaßnahmen unverzichtbar, sollten aber - solange keine gegenteiligen Erkenntnisse vorliegen - auf der Grundlage eines grundsätzlichen Vertrauens auf gesetzmäßiges und insbesondere auch verhältnismäßiges Handeln der Sicherheitsbehörden in ihren Einzelentscheidungen deutlich zurückhaltender ausfallen. Sobald strukturelle Unzuträglichkeiten bekannt würden, bliebe es dem Gesetzgeber unbenommen, hinsichtlich der Eingriffsvoraussetzungen und der flankierenden Schutzmaßnahmen nachzubessern.

II.

Trotz des im beschriebenen Umfang abweichenden Ansatzes kann ich einem Großteil der im Urteil formulierten übergreifenden Grundsätze zur Datenerhebung, Datenweitergabe und auch zur Übermittlung ins Ausland zustimmen. Dies gilt über weite Strecken auch im Hinblick auf die daraus für die angegriffenen Regelungen abgeleiteten Schlussfolgerungen. Sie überzeugen und sind gut begründet. Die damit verbundenen Anforderungen an eine anspruchsvolle Gesetzgebung und Erschwernisse des Polizeivollzugs müssen zum Schutz der betroffenen Freiheitsrechte hingenommen werden. In verschiedenen Aussagen der allgemeinen Grundsätze und bei einer Reihe der daraus abgeleiteten gezogenen Schlüsse auf die Verfassungswidrigkeit von Einzelnormen, halte ich den Standpunkt des Urteils - auch wenn es sich dabei um Fortführungen früherer Entscheidungen handelt - jedoch für überzogen und so verfassungsrechtlich nicht gefordert. Hierbei geht es vor allem um folgende Punkte: 6

1. Ungeachtet der bereits prinzipiell angezeigten größeren Zurückhaltung des Gerichts in Bezug auf detaillierte Vorgaben an den Gesetzgeber für die flankierenden Verfahrens- und sonstige Schutzvorschriften halte ich es nach wie vor für überzogen, aus dem Verhältnismäßigkeitsgrundsatz abzuleiten, dass dem von einer eingriffsintensiven Überwachungsmaßnahme Betroffenen neben dem Zugang zu einer gerichtlichen Rechtmäßigkeitskontrolle auch wirksame Sanktionsmechanismen einschließlich eines etwaigen Ausgleichsanspruchs bei einer Rechtsverletzung zur Verfügung gestellt werden müssten (Urteil C IV 6 c), dass eine Kontrolle der Datenerhebung und -verarbeitung regelmäßig in Abständen durchgeführt werden müsste, deren Dauer ein gewisses Höchstmaß von etwa zwei Jahren nicht überschreiten dürfe (Urteil C IV 6 d) und dass der Gesetzgeber zur Gewährleistung von Transparenz und Kontrolle wegen der Heimlichkeit der Datenerhebung regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit sicherzustellen habe (Urteil C IV 6 e). Für all diese Sicherungsmaßnahmen gibt es gute, im Urteil nachgewiesene Gründe. Dies allein rechtfertigt es allerdings nicht, sie dem Gesetzgeber als verfassungsrechtlich geboten vorzuschreiben und ihm dadurch andere Lösungswege zu versperren, die er im Rahmen seines Gestaltungsspielraums zur Erreichung eines verfassungsrechtlich gebotenen Sicherheitsniveaus hätte beschreiten können. Es hätte genügt - und Weitergehendes ist auch nicht gerechtfertigt - dem Gesetzgeber lediglich das Sicherheitsniveau vorzugeben. 7

2. In geringerem Umfang verfassungswidrig, als vom Senat angenommen, sind die angegriffenen einzelnen Ermittlungs- und Überwachungsbestimmungen. 8

a) Der Senat hält die Ermächtigungen zu einigen Aufklärungs- und Datenerhebungsmaßnahmen zum Zwecke der Straftatenverhütung für zu unbestimmt und unverhältnismäßig (Urteil C V 1 d bb, 5 b, 6 b), soweit darin lediglich gefordert wird, dass „Tatsachen“ oder auch „bestimmte Tatsachen“ die Annahme rechtfertigen, dass eine Person Straftaten im Sinne des § 129a StGB „begehen wird“ oder „vorbereitet“ (vgl. § 20g Abs. 1 Nr. 2; § 20l Abs. 1 Satz 1 Nr. 2 und § 20m Abs. 1 Nr. 2 BKAG). Damit unterlässt er es ohne Not, den in diesen Fällen möglichen Weg der verfassungskonformen Auslegung zu wählen. Der Senat hat in den allgemeinen Grundsätzen des Urteils die Voraussetzungen einer verfassungsgemäßen Gefahrenschwelle für so weit ins Vorfeld einer konkreten Gefahr verlagerte, eingriffsintensive Aufklärungsmaßnahmen erarbeitet. Demzufolge muss wenigstens ein seiner Art nach konkretisiertes und absehbares Geschehen in Richtung einer der genannten Straftaten erkennbar sein oder alternativ das individuelle Ver- 9

halten einer Person die konkrete Wahrscheinlichkeit begründen, dass sie terroristische Straftaten in überschaubarer Zukunft begeht. Die in diesen Formulierungen gelungene Präzisierung des Gefahrbegriffs im Vorfeldbereich der Straftatenverhütung verbunden mit der Ausweitung auf die alternative Möglichkeit einer Anknüpfung an das individuelle Verhalten einer Person sehe ich allerdings als deutlichen Gewinn gegenüber den Vorgaben aus der bisherigen Rechtsprechung, an die hier angeknüpft wird. Die Neuformulierung benennt die Eingriffsvoraussetzungen im Hinblick auf die Eingriffsschwelle in diesem Bereich klarer und trägt den berechtigten Sicherheitsbedürfnissen des Gemeinwesens an dieser Stelle besser als bisher Rechnung. Es widerspricht jedoch weder dem Wortlaut noch dem erkennbaren Willen des Gesetzgebers, die hier in Rede stehenden und für sich genommen insoweit zu offen formulierten Ermittlungsermächtigungen unter Beachtung dieser verfassungsrechtlichen Anforderungen an die Gefahrenschwelle einschränkend auszulegen. Dann wäre es aus Respekt vor dem Gesetzgeber geboten gewesen, die Normen zu erhalten, zumal mit dem Urteil nunmehr eine präzise Bestimmung der Gefahrenschwelle für die Fälle der Straftatenverhütung vorliegt und im Rahmen des Wortlauts der Normen ohne Weiteres zur Anwendung gebracht werden kann.

b) Anders als der Senat halte ich auch das vom Gesetzgeber in § 20g Abs. 3 Satz 5 bis 9 BKAG gewählte Konzept, erst für die Verlängerung eines Großteils der in § 20g Abs. 2 BKAG genannten Überwachungsmaßnahmen einen Richtervorbehalt vorzusehen, für verfassungsrechtlich vertretbar. Die dort vorgesehenen Überwachungsmaßnahmen wiegen zwar teilweise schwer, sind aber durchgängig an die Genehmigung durch den Abteilungsleiter geknüpft und mit einer Protokollierungspflicht verbunden. Damit hat der Gesetzgeber eine noch vertretbare Balance zwischen Aufklärungseffizienz und berechtigten Schutzinteressen der durch die Überwachungsmaßnahmen Betroffenen gefunden, zumal nicht ohne Weiteres davon ausgegangen werden kann, dass das Bundeskriminalamt den im ersten Monat fehlenden Richtervorbehalt regelmäßig zu unverhältnismäßigen Überwachungsmaßnahmen nutzen wird. Sollte sich das Vertrauen des Gesetzgebers in dieses zunächst auf der Ebene des Bundeskriminalamts angesiedelte Kontrollsystem als unberechtigt erweisen, hätte er dies allerdings zu korrigieren. 10

c) Nicht teilen kann ich die Annahme des Senats, § 20g BKAG sei auch deshalb verfassungswidrig, weil er keine Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung enthält (Urteil C V 1 g). 11

Im Ausgangspunkt stimme ich allerdings dem Standpunkt des Urteils zu, dass der Gesetzgeber bei Normen, die zu typischerweise in den Kernbereich privater Lebensgestaltung eingreifenden Überwachungs- und Ermittlungsmaßnahmen ermächtigen, ein Sicherungs- und Kontrollregime vorsehen muss, das die im Urteil im einzelnen umschriebenen Bedingungen zur Vermeidung bereits der Erhebung solcher Daten vorsieht und - sofern dies nicht auszuschließen ist - dann auf der Auswertungs- und Verwertungsebene entsprechende behördenexterne Filter- und Sichtungsmechanismen enthält (Urteil C IV 3 d). Eine Pflicht des Gesetzgebers, schon im Vorhinein ein solches, auf die jeweilige Überwachungsnorm zugeschnittenes System des Kernbereichsschutzes vorzuschreiben, das solche Maßnahmen dann in aller Regel nur unter womöglich aufwändigen Vorkehrungen in verfahrensmäßiger und personeller Hinsicht erlaubt, ist nach meiner Überzeugung von Verfassungs wegen allerdings nur für solche Überwachungs- und Ermittlungsmaßnahmen geboten, von denen zu erwarten ist, dass sie mit einer gewissen Regelmäßigkeit und damit typischerweise kernbereichsrelevante Situationen erfassen. 12

Eine solche Ermächtigungsnorm für Überwachungsmaßnahmen, die typischerweise zur Erhebung kernbereichsrelevanter Daten führen können, ist § 20g BKAG jedoch nicht. Der Senat begründet seine gegenteilige Auffassung mit der Erwägung, die Vorschrift ermächtige unter anderem zu längerfristigen Bildaufzeichnungen und einem auf eine lange Zeit angelegten Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes; sie ermögliche damit Überwachungsmaßnahmen, die typischerweise tief in die Privatsphäre eindringen könnten. Es dürfte zwar in der Tat nicht auszuschließen sein, dass gerade Überwachungsmaßnahmen der beschriebenen Art Situationen erfassen können, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Dass solche Maßnahmen im Einzelfall tief in die Privatsphäre eindringen können, bedeutet jedoch nicht, dass sie dies typischerweise tun, und erst recht nicht, dass sie dann auch typischerweise kernbereichsrelevante Vorgänge erfassen. Der Annahme einer solchen Typik steht vor allem entgegen, dass die Maßnahmen des § 20g Abs. 2 BKAG grundsätzlich im öffentlichen Raum stattfinden. Kommt es dann im konkreten Einzelfall dennoch zur Erfassung von Situationen, in denen der dem Kernbereichsschutz unterfallende Personenkreis in der berechtigten Annahme strenger Vertraulichkeit Höchstpersönliches austauscht, hat das Bundeskriminalamt die dann jeweils gebotenen Maßnahmen zum Schutz des Kernbereichs zu treffen (Urteil C IV 3 b). 13

3. Geht mit der weiteren Verwendung aus Überwachungsmaßnahmen gewonnener Daten eine Zweckänderung einher, liegt darin ein erneuter Eingriff in das Grundrecht, in das bereits bei Erhebung der Daten eingegriffen wurde. Das entspricht gefestigter, auch von mir geteilter Rechtsprechung des Gerichts. Die vom Senat geforderten Bedingungen, unter denen eine solche Zweckänderung erfolgen darf, errichten allerdings teilweise zu hohe Hürden. Sie werden insoweit nicht dem Umstand gerecht, dass es sich um die Weiternutzung bereits verfassungsgemäß erhobener Daten handelt. 14

a) Uneingeschränkt zu begrüßen ist allerdings das grundsätzliche Unterfangen des Urteils, die Figur der „hypothetischen Neuerhebung“ als gedanklichen Ansatz zur Bestimmung der Zweckänderungsbedingungen zu präzisieren und zu konsolidieren (Urteil D I). Mit der Unterscheidung zwischen der weiteren Nutzung von Daten (innerhalb der ursprünglichen Zwecksetzung, seitens derselben Behörde und im Rahmen desselben Aufgabenkreises), für die es als Weiternutzungsschwelle lediglich eines bloßen Spurenansatzes bedarf (Urteil D I 1 b), und der darüber hinausgehenden Zweckänderung vorhandener Daten durch die Weitergabe an andere Behörden, die als legitimierenden Anlass lediglich verlangt, dass sich aus den Daten ein konkreter Ermittlungsansatz ergibt (Urteil D I 2 b bb), schafft das Urteil Rechtsklarheit und nimmt überzogene, aus der undifferenzierten Anwendung des Gedankens der hypothetischen Neuerhebung abgeleitete Anforderungen an den Anlass für die Weitergabe der Daten zurück. Damit trägt es dem Umstand Rechnung, dass die weitere Nutzung und insbesondere die Zweckänderung von Daten zwar den ursprünglichen, bei der Gewinnung der Daten erfolgten Grundrechtseingriff fortführen, das Grundrecht aber typischerweise eben nicht erneut in gleicher Intensität beeinträchtigen. 15

b) Nicht mitzutragen vermag ich jedoch die vom Senat im Anschluss an seine frühere Rechtsprechung (BVerfGE 109, 279 <377, 379>) geforderte Ausnahme von diesem Zweckänderungskonzept bei Daten, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden. Hier verlangt das Urteil unter Berufung auf das besondere Eingriffsgewicht dieser Maßnahmen für jede weitere Nutzung und Zweckänderung die Rechtfertigung durch eine dringende oder eine im Einzelfall hinreichend konkretisierte Gefahr wie bei der Datenerhebung selbst (Urteil D I 1 b, 2 b bb). Der Schluss von der Eingriffsintensität bei der Datenerhebung gerade in diesen beiden Fallgruppen auf die Notwendigkeit einer gleich hohen Anlassschwelle für die Weiternutzung und Zweckänderung überzeugt nicht. In allen anderen Fallgruppen hat der Senat mit dem hier entwickelten neuen Konzept die 16

Notwendigkeit einer Kongruenz zwischen dem gebotenen Erhebungsanlass und dem der Weiterverwendung in dem Urteil soeben zu Recht aufgegeben und stattdessen überzeugend nach dem Grad der Abweichung vom ursprünglichen Erhebungszweck differenziert. Für Daten aus Wohnraumüberwachung und Online-Durchsuchung gilt nichts anderes. Art. 13 Abs. 4 Satz 1 GG fordert eine dringende Gefahr für den Einsatz der Wohnraumüberwachung; zu den Bedingungen der Weiterverwendung der daraus gewonnenen Daten sagt er nichts. Vergleichbar den anderen eingriffsintensiven Überwachungsmaßnahmen erfolgt auch bei der Wohnraumüberwachung die eigentliche, massive Beeinträchtigung der Privatsphäre durch den Ermittlungszugriff auf den geschützten Bereich. Die weitere, auch zweckändernde Nutzung perpetuiert diesen Eingriff zwar, erreicht aber auch bei der Wohnraumüberwachung (und ebenso bei der Online-Durchsuchung) nicht mehr die ursprüngliche Eingriffsintensität. Die Weiternutzung und Zweckänderung aus diesen gewonnener Erkenntnisse hat daher den allgemeinen Regeln zu folgen. Der Senat hätte seine bisherige Rechtsprechung dementsprechend korrigieren sollen.

Eichberger

Abweichende Meinung des Richters Schluckebier

zum Urteil des Ersten Senats vom 20. April 2016

- 1 BvR 966/09 -
- 1 BvR 1140/09 -

Soweit das Urteil die zu prüfenden gesetzlichen Bestimmungen von Verfassungs wegen beanstandet, vermag ich ihm in weiten Teilen dieses Ergebnisses und der zugehörigen Begründung nicht zuzustimmen. 1

Das Urteil geht zwar im Ansatz zutreffend davon aus, dass es die Aufgabe des Gesetzgebers ist, zwischen den von den Grundrechtseingriffen, die mit den zu prüfenden Eingriffsgrundlagen im Einzelfall verbunden sein können, und dem Schutzauftrag des Staates für die Grundrechte der Menschen und die Rechtsgüter der Allgemeinheit im Rahmen der Verhinderung terroristischer Straftaten einen angemessenen Ausgleich zu finden. In der Umsetzung dessen führt das jedoch zu einer meines Erachtens in verschiedener Hinsicht verfassungsrechtlich verfehlten Verhältnismäßigkeitsprüfung sowie zu überzogenen Anforderungen an die Bestimmtheit einzelner Regelungen. Die vom Senat vertretenen Positionen haben zugleich erhebliche Auswirkungen auf die Landespolizeigesetze der Länder, ohne dass diese Konsequenzen im Verfahren hinreichend vertieft worden wären. Damit beschneidet das Urteil zugleich die politische Gestaltungsmacht des Bundesgesetzgebers über das gebotene Maß hinaus, mittelbar aber auch diejenige der Landesgesetzgeber. Der Senat setzt mit zahlreichen gesetzgebungstechnischen Detailanforderungen letztlich seine konkretisierenden eigenen Vorstellungen von dem Regelwerk in meines Erachtens zu weit gehender Weise an die Stelle derjenigen des demokratisch legitimierten Gesetzgebers, der sich für seine Konzeption politisch zu verantworten hat und diese gegebenenfalls auch leicht korrigieren kann. 2

Anders als der Senat meint, wären einige der beanstandeten Bestimmungen auch verfassungskonform auslegbar gewesen (Voraussetzungen nach § 20g Abs. 1 Nr. 2, § 20l Abs. 1 Nr. 2, § 20m Abs. 1 Nr. 2, § 20v Abs. 4 Nr. 1 BKAG). Die von der Senatsmehrheit vermisste ausdrückliche Aufnahme einer kernbereichsschützenden Regelung für die Datenerhebungsmaßnahmen mit besonderen Mitteln namentlich außerhalb von Wohnungen (§ 20g BKAG) in das Gesetz ist ver- 3

fassungsrechtlich keineswegs geboten, weil insoweit nicht typische Rückzugsräume der Privatheit in Rede stehen. Auch die Ausweitung des Richtervorbehalts für diese Maßnahmen nach § 20g BKAG ist aus Gründen der Verhältnismäßigkeit nicht zwingend. Soweit der Senat für die Auswertung von Überwachungsmaßnahmen zum Kernbereichsschutz die Einrichtung einer „unabhängigen Stelle“ mit maximal einem sachkundigen Bediensteten des Bundeskriminalamts postuliert, beeinträchtigt dies die Wirksamkeit der gerade im Bereich der Gefahrenabwehr oft in besonderem Maße eil- und beschleunigungsbedürftigen Auswertung und Umsetzung von Erkenntnissen. Damit verfehlt er auch insoweit einen angemessenen Ausgleich. Mit den im Einzelnen geforderten zusätzlichen flankierenden verfahrensrechtlichen Maßnahmen, namentlich einer gesteigerten Datenschutzkontrolle und Pflichtkontrollen innerhalb eines bestimmten Zeitraumes sowie Berichtspflichten gegenüber Parlament und Öffentlichkeit und der Einforderung wirksamer Sanktionen bei Rechtsverletzungen werden gesetzesgestaltende Details verlangt, die den Gesetzgeber als Repräsentanten des Souveräns in zu kleinteiliger Weise einschränken. Hinsichtlich der beanstandeten Zweckänderungs- und Übermittlungsvorschriften, die an das Kriterium der hypothetischen Datenneuerhebung anknüpfen, folgen aus der Auffassung des Senats erhebliche Defizite für den Schutz der Grundrechte Dritter und der Rechtsgüter der Allgemeinheit. Dem Rechtsstaat wird partiell ein „Wegsehen“ vor Gefahren für Rechtsgüter und Grundrechte Einzelner angesonnen; den von Gefahren für ihre Rechtsgüter Betroffenen wird damit in bestimmten Konstellationen der erforderliche Schutz vorenthalten.

Im Folgenden skizziere ich nur die wesentlichen Punkte näher, in denen meines Erachtens eine andere Beurteilung geboten gewesen wäre. Soweit einzelne Beanstandungen des Senats nicht angesprochen werden, vermag ich das Urteil in wichtigen Teilen auch mitzutragen. Das gilt insbesondere für die vom Senat akzeptierten reduzierten Anforderungen an den Gefahrbegriff, die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs sowie die Maßnahmen der Umfeldüberwachung bei der ins Vorfeld der klassischen Gefahrenabwehr verschobenen Straftatenverhütung. Zu den einzelnen von mir nicht geteilten verfassungsrechtlichen Bewertungen ist anzumerken: 4

I.

Grundsätzlich ist vorweg festzuhalten, dass der Gesetzgeber bei der Verfolgung des Ziels, eine effektive Abwehr terroristischer Gefahren und Straftaten zu gewährleisten mit der von ihm gewählten Ausgestaltung des Spannungsverhält- 5

nisses zwischen den Grundrechten der von solchen polizeilichen Maßnahmen Betroffenen und den Eingriffsgrundlagen auf der einen Seite sowie seiner Schutzverpflichtung im Blick auf die Grundrechte der Einzelnen und die verfassungsmäßig verankerten Rechtsgüter der Allgemeinheit auf der anderen Seite einen im Wesentlichen angemessenen und zumutbaren Ausgleich gefunden hat. Der Gesetzgeber trägt damit dem Grundsatz Rechnung, dass der Einzelne sich im Rechtsstaat auf effektiven Schutz *durch* den Staat ebenso verlassen können muss wie auf den Schutz seiner Freiheitsgewährleistungen *vor* dem Staat (vgl. meine abw. Meinung in BVerfGE 125, 364 <369>; siehe zur Schutzpflicht bei terroristischen und anderen Bestrebungen auch der Senat in BVerfGE 120, 274 <319>). Soweit damit im Einzelfall auch Grundrechtsträger von solchen Maßnahmen betroffen werden können, die nicht selbst unter Terrorismusverdacht stehen oder die, wie sich später erweist, zu Unrecht in diesen geraten sind, sind die mit den eingreifenden Maßnahmen verbundenen Belastungen grundsätzlich als ihnen von der Gemeinschaft abverlangtes Sonderopfer hinzunehmen.

Die Urteilsgründe leiden indessen daran, dass nach den allgemeinen Ausführungen zu Bedeutung und Gewicht der vom Gesetzgeber verfolgten Ziele hinsichtlich der einzelnen Vorschriften keine substantielle Prüfung der Verhältnismäßigkeit im engeren Sinne und der Bestimmtheit mehr vorgenommen wird, sondern die verfassungsrechtlichen Beanstandungen einzelner Vorschriften lediglich mit der schlichten Rechtsbehauptung begründet werden, die jeweilige Bestimmung sei unverhältnismäßig oder zu unbestimmt. Eine wirkliche Angemessenheits- und Bestimmtheitsprüfung findet jeweils normbezogen nicht mehr statt. Die vom Senat zudem in ihrer Detailliertheit gemachten Vorgaben unter Berufung auf die Wahrung der Verhältnismäßigkeit verdeutlichen zudem die - wohlgemerkt: nur im Ergebnis - außergewöhnlich hohe Prüfungsdichte, die für die gesetzgebungstechnische Ausgestaltung kaum noch Spielräume belässt, wenn denn der Gesetzgeber die Gefahrenabwehr mit den von ihm gewollten Maßnahmen auszustatten gedenkt. Freilich ist die Vorgabe solcher gesetzgebungstechnischer Einzelheiten in der bisherigen jüngeren Spruchpraxis des Senats angelegt. Sie ist dort vornehmlich aber im Blick auf die spezifischen Grundrechtsgefährdungspotenziale der elektronischen Datenverarbeitung sowie die Breitenwirkung bestimmter Maßnahmen entwickelt worden, etwa in den Entscheidungen zur Antiterrordatei als Verbunddatei, sowie zur Vorratsdatenspeicherung, die die anlasslose Speicherung aller Telekommunikationsverkehrsdaten bei den Netzbetreibern vorsah (vgl. BVerfGE 125, 260 <316 ff.>; 133, 277 <320 ff.>). Im vorliegenden Fall geht es jedoch um einzelfallbezogene Maßnahmen gegen Betroffene, die in den Fokus der

6

Verhütung terroristischer Gewalttaten geraten sind. Diese präventiv-polizeilichen Sachverhalte sind zudem dadurch geprägt, dass die in Rede stehenden Maßnahmen - anders als oft im Bereich der Strafverfolgung - in der Regel eine größere Nähe zu drohenden konkreten Rechtsgutsbeeinträchtigungen aufweisen. Die vom Senat hierzu gestellten Anforderungen werden zugleich erhebliche Folgewirkungen für nahezu alle Landespolizeigesetze haben, die weitgehend ähnliche oder gleiche Maßnahmen für die Abwehr von schwerwiegenden Straftaten der organisierten Kriminalität und der allgemeinen Kriminalität vorsehen, ohne dass diese Konsequenzen hinreichend durchdrungen und vertieft worden wären.

Im Ergebnis halte ich die vom Senat vorgenommene enge Verhältnismäßigkeitsprüfung hinsichtlich mehrerer beanstandeter Bestimmungen für nicht überzeugend und zum Teil gar für unangemessen. Dies erhellt sich gerade vor dem Hintergrund, dass das Gesetz mit seinen Eingriffsgrundlagen seit mehr als sieben Jahren in Kraft ist, es - wie die mündliche Verhandlung ergeben hat - seither nur wenige Anwendungsfälle gegeben hat und Misshelligkeiten bei der Gesetzesanwendung bislang nicht zu Tage getreten sind. Im Gegenteil: Die Befragung der zuständigen Beamten des Bundeskriminalamts, die für die operative Anwendung der Vorschriften unmittelbar verantwortlich sind, in der mündlichen Verhandlung hat den Eindruck eines äußerst verantwortungsbewussten Umgangs mit den Eingriffsgrundlagen unter der politischen Ressortverantwortung des zuständigen Ministers und letztlich auch der effektiven parlamentarischen Kontrolle vermittelt. 7

II.

Konkret bleibt zu einzelnen der vom Senat erhobenen Beanstandungen anzumerken: 8

1. Der Senat bemängelt, dass die Eingriffsvoraussetzungen bestimmter Rechtsgrundlagen nicht hinreichend gehaltvoll ausgestaltet und deshalb unverhältnismäßig und unbestimmt seien (§ 20g Abs. 1 Nr. 2, § 20l Abs. 1 Nr. 2, § 20m Abs. 1 Nr. 2 BKAG). Diese Bestimmungen erfordern, dass hinsichtlich der Person, gegen die sich die jeweilige Maßnahme richtet, Tatsachen vorliegen, die die Annahme rechtfertigen, dass sie terroristische Straftaten, wie sie in § 4a Abs. 1 Satz 2 BKAG umschrieben sind, begehen wird (in § 20l und § 20m BKAG ist die Rede von „bestimmten Tatsachen“). Für die vom Gesetzgeber formulierten Eingriffsvoraussetzungen wäre jedoch auf der Grundlage der Ausführungen des Urteils eine verfassungskonforme Interpretation möglich gewesen. Der Normbean- 9

standung hätte es nicht bedurft. Die benutzten Begrifflichkeiten sind im Bereich der Gefahrenabwehr, aber auch des Strafprozessrechts nicht unüblich. Sie sind der Auslegung zugänglich. Eine weitergehende „gehaltvolle Ausgestaltung“ im Gesetz, wie sie der Senat einfordert, ist angesichts der Vielgestaltigkeit der Lebenssachverhalte schwierig und führt nur zu einer textlichen Ausuferung der Normen mit wiederum notwendigerweise allgemein zu haltenden auslegungsbedürftigen weiteren Begriffen.

2. Der Senat vermisst für die in § 20g Abs. 2 BKAG vorgesehenen besonderen Mittel der Datenerhebung eine ausdrückliche gesetzliche Regelung zum Schutz des Kernbereichs privater Lebensgestaltung auch insoweit, wie die dort aufgeführten Überwachungsmaßnahmen außerhalb von Wohnungen stattfinden und von verschiedener Qualität sein und Nähe zur Privatsphäre haben können. Dazu zählen etwa die längerfristige Observation, die Anfertigung von Bildaufnahmen von Personen außerhalb von Wohnungen oder das Abhören und Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes. 10

Diese Bewertung teile ich nicht. Ein typischer Rückzugsbereich ins Private (vgl. BVerfGE 109, 279 <320 f.>) ist in den Fällen technischer Maßnahmen außerhalb von Wohnungen regelmäßig nicht betroffen. Man mag sich zwar zur Besprechung vertraulicher Dinge - diese Beispiele nennt der Senat - auf einen Spaziergang begeben oder auf eine Autofahrt. Das ändert jedoch nichts daran, dass sich die Betroffenen im Grundsatz „in der Öffentlichkeit“ bewegen, nicht jedoch in besonders geschützten Zonen der Privatheit (vgl. BVerfGE 120, 274 <331>). Ein schutzwürdiges Vertrauen wird sich unter solchen Umständen nicht in dem gleich hohen, schlechterdings nicht überbietbaren Maß herausbilden können wie bei Gesprächen in der eigenen Wohnung oder bezogen auf das eigene informationstechnische System. Deshalb hätte es insoweit keiner ausdrücklichen gesetzlichen kernbereichsschützenden Regelung bedurft. Vielmehr kann der Kernbereichsschutz auf der Rechtsanwendungsebene sichergestellt werden. 11

3. Die Ausweitung des Richtervorbehalts auch auf die erstmalige Anordnung von Maßnahmen nach § 20g Abs. 2 Nr. 1 bis 4 BKAG, namentlich solcher außerhalb von Wohnungen, halte ich aus Gründen der Verhältnismäßigkeit für nicht zwingend geboten. Angesichts der Besonderheiten und der typischen Eigendynamik der Fallgestaltungen bei der Verhütung und Abwehr schwerwiegender oder gar terroristischer Straftaten genügt es meines Erachtens, den Richtervorbehalt für die Verlängerung solcher Maßnahmen vorzusehen (§ 20g Abs. 3 Satz 8 BKAG). 12

Im Übrigen beinhalten auch die meisten Landespolizeigesetze - insbesondere zur Verhinderung organisierter Kriminalität - gleiche oder ähnliche Befugnisse mit der Erstanordnungskompetenz der Behördenleitung, wie sie etwa in § 20g Abs. 2 BKAG normiert sind (vgl. z.B. § 15 Abs. 3, § 16 Abs. 5 Satz 1 HSOG, § 16a Abs. 2 Satz 1 PolG NW). Praktisch ist dies unter anderem bei dem Einsatz von Vertrauenspersonen etwa im Bereich der organisierten Kriminalität, insbesondere der Drogenkriminalität von großer Bedeutung.

Allerdings werden sich - nach meinem Verständnis der Urteilsgründe - kaum Auswirkungen auf das Strafprozessrecht ergeben, wo etwa der Einsatz von Vertrauenspersonen der sogenannten Ermittlungsgeneralklausel zugeordnet wird und im Übrigen lediglich in einer Verwaltungsvorschrift geregelt ist (§ 161 StPO; Richtlinien für das Strafverfahren und das Bußgeldverfahren - RiStBV -, Anlage D; kritisch dazu allerdings z.B. Eschelbach, in: SSW-StPO, 2. Aufl. § 110a Rn. 11). Die hier in Rede stehenden präventivpolizeilichen Maßnahmen der Straftatenverhütung im Vorfeld und der Gefahrenabwehr unterscheiden sich von strafprozessrechtlichen Ermittlungsmaßnahmen. Letztere erfolgen unter der Sachleitung eines Justizorgans (Staatsanwaltschaft), bewegen sich im weiteren Verlauf in den schützenden Formen eines differenziert ausgestalteten Verfahrens (Strafprozessordnung) und münden ohnehin regelmäßig in eine richterliche Befassung. Das gilt auch dann, wenn das Verfahren nicht zur Anklage führt, aber andere richterliche Anordnungen im Zuge der Ermittlungen erforderlich werden oder die Maßnahmen nach Verfahrenseinstellung zu einem späteren Zeitpunkt offen gelegt werden. 13

4. Nicht mittragen kann ich weiter die vom Senat geforderte Errichtung einer „unabhängigen Stelle“, die auf der Auswertungs- und Verwertungsebene bei Maßnahmen der Wohnraumüberwachung und der Online-Durchsuchung einen nachgelagerten Kernbereichsschutz sicherstellen soll. Der Senat postuliert, dass diese Kontrolle „im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen“ wahrgenommen wird, in deren Händen die „tatsächliche Durchführung und Entscheidungsverantwortung“ liegen soll (zu § 20h Abs. 5, § 20k Abs. 7 BKAG). Die Zuziehung *eines* Bediensteten des Bundeskriminalamts zur Gewährleistung ermittlungsspezifischen Fachverstandes hält der Senat für nicht ausgeschlossen. Damit geht der Senat über die bisher an den nachgelagerten Kernbereichsschutz gestellten verfassungsrechtlichen Anforderungen weit hinaus (vgl. nur BVerfGE 120, 274 <338 f.> zum Verfassungsschutzgesetz Nordrhein-Westfalen). 14

Entgegen dieser Auffassung halte ich die derzeitige Regelung, die die Sachlei- 15
tung und mithin auch die Entscheidungsverantwortung des anordnenden Richters vorsieht oder jedenfalls einschließt (§ 20h Abs. 3 Satz 1, Abs. 5 Satz 4, § 20k Abs. 7 Satz 3 BKAG) sowie die Pflicht zur unverzüglichen Löschung von kernbereichsrelevanten Inhalten und die Protokollierung der Löschung zum Zwecke der Kontrolle vorschreibt (§ 20h Abs. 5 Satz 7, § 20k Abs. 7 Satz 5 BKAG) für genügend (so für die unverzügliche Löschung kernbereichsrelevanter Inhalte auch noch der Senat in BVerfGE 120, 274 <339> zu Daten aus informationstechnischen Systemen). Die jetzt vom Senat geforderte „unabhängige Stelle“ für die Auswertung und Verwertbarkeitskontrolle stellt gerade im Rahmen der Gefahrenabwehr und Straftatenverhütung die Wirksamkeit der Maßnahmen infrage, weil es hier typischerweise um Fallgestaltungen geht, bei denen die Auswertung von Erkenntnissen oft in hohem Maße beschleunigungs- und eilbedürftig ist. Dem kommt für die Angemessenheitsbeurteilung - im Blick auf die Wirksamkeit der Maßnahme - große Bedeutung zu. Die postulierte „unabhängige Stelle“ müsste während der Dauer der Überwachungsmaßnahmen zumeist permanent aktionsfähig vorgehalten werden. Ihr die erste Sichtung unter weitgehendem Ausschluss der Sicherheitsbehörde um des nachgelagerten Kernbereichsschutzes willen vorzubehalten, vernachlässigt die besonderen Erfordernisse der Abwehr von Gefahren des internationalen Terrorismus und der Verhütung terroristischer Taten (i.S.d. § 4a Abs. 1 BKAG). Anders als oft im strafprozessualen Ermittlungsverfahren liegen bei der Gefahrenabwehr Erhebung und Verwertung der Daten zumeist sehr nahe beieinander. Die gewonnenen Erkenntnisse werden regelmäßig eine schnelle, nicht selten eine sofortige Reaktion erfordern.

Wie sich die vom Senat verlangte Lösung bei einer sogenannten Liveüberwa- 16
chung darstellen soll, bleibt weitgehend im Unklaren. Auch die oft gegebene prozedurale Situation, die bei der Hinzuziehung von Dolmetschern entsteht, wird nicht näher betrachtet. Gerade in fremdsprachigen Konstellationen kommt Sprachmittlern eine zentrale Rolle auch für die Ersteinschätzung von Gesprächen als höchstpersönlich zu. Mitunter werden hier auch sprachliche Besonderheiten (in Mitteleuropa selten vorkommende Sprachen, Dialekte) eine Rolle spielen. Kurzum: Die vom Senat verlangte Lösung trifft mit ihrer Komplizierung die Effektivität der Maßnahmen gerade im Bereich der Wohnraumüberwachung und wird deshalb im Ergebnis den Angemessenheitsanforderungen auf der anderen Seite, nämlich im Blick auf die Verfolgung des gesetzgeberischen Ziels einer wirksamen Abwendung terroristischer Straftaten, nicht hinreichend gerecht. Daran ändert auch nichts die dem Gesetzgeber vom Senat eröffnete Möglichkeit, „die notwendigen Regelungen

zu treffen“, um dem Bundeskriminalamt „für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen“. Dabei bleibt nicht nur im Dunkeln, wie diese - in der Praxis ohnehin eher häufiger vorkommenden - Ausnahmefälle sinnvoll von den Sachverhalten abgegrenzt werden sollen, in denen den Urteilsgründen zufolge allein die „unabhängige Stelle“ durchführungs- und kontrollbefugt sein soll, sondern auch, welche „notwendigen Regelungen“ für diese „Ausnahmekonstellationen“ tatsächlich beanstandungsfrei getroffen werden können. Im Übrigen steht dieses Zugeständnis an den Gesetzgeber, in Ausnahmefällen bei Gefahr im Verzug eine erste Sichtung ohne die „unabhängige Stelle“ vorzunehmen, in deutlichem Kontrast zu der Annahme des Urteils, die besondere Schutzbedürftigkeit der Daten gebiete für den Regelfall die nahezu vollständige Herausnahme des Bundeskriminalamts aus der Erstsichtungsverantwortung.

5. Soweit der Senat auch fehlende flankierende verfahrensrechtliche Rege- 17
lungen zu den Ermittlungs- und Überwachungsbefugnissen reklamiert, um Transparenz, Rechtsschutz und aufsichtliche Kontrolle in jeder Hinsicht zu gewährleisten, halte ich die auf Verhältnismäßigkeitserwägungen gestützten Anforderungen an die hier in Rede stehenden einzelfallbezogenen Maßnahmen zur Terrorismusabwehr teilweise für übermäßig. Neben Benachrichtigungspflichten und Auskunftsansprüchen auch noch Details einer turnusmäßigen datenschutzrechtlichen Pflichtkontrolle in bestimmten Mindestabständen vorzugeben, wirksame Sanktionsnormen bei Rechtsgutsverletzungen (durch solche Maßnahmen) - wohl über die bestehenden Haftungs- und Entschädigungsnormen hinausgehend - und gesetzlich ausgestaltete Berichtspflichten gegenüber Parlament und Öffentlichkeit einzufordern, erscheint mir in Ansehung der hier zu prüfenden Normen, die nicht die spezifischen Risiken vernetzter Datenverarbeitung oder von Datenerhebungen in großer Streubreite bergen, unangemessen und zum Schutz der Grundrechte derjenigen, die einzelfallbezogen in den Fokus der Verhinderung terroristischer Straftaten und der Gefahrenabwehr geraten, nicht geboten.

Diese in letzte Einzelheiten gehenden Anforderungen und Vorgaben halte ich 18
auch im Blick auf das Verhältnis der Verfassungsgerichtsbarkeit zum Gesetzgeber hier für kaum vertretbar. Der Gesetzgeber selbst ist zunächst für die von ihm für zutreffend erachtete Kontroll- und Transparenzdichte politisch verantwortlich. Es ist - abgesehen von besonderen Fallgestaltungen - regelmäßig seine Sache, ob und wie er gegebenenfalls Kontroll- und Transparenzmechanismen in ein Gesetz aufnimmt. Das gilt gerade im Lichte der ohnehin gegebenen parlamentarischen Kontrollmechanismen, wie etwa des Frage- und Informationsrechts der Abgeord-

neten (vgl. dazu BVerfGE 130, 318 <342> m.w.N.) und des Zitierungsrechts des Bundestages sowie seiner Ausschüsse (Art. 43 Abs. 1 GG). Parlamentarische Anfragen vermögen regelmäßig umfangreiche Antworten der Exekutive auszulösen. Im besonderen Fall kommt die Möglichkeit der Einsetzung eines Untersuchungsausschusses in Betracht. Dabei ist die parlamentarische Verantwortlichkeit des zuständigen Ressortministers ebenso im Auge zu behalten wie die kritische Betrachtung und Bewertung durch die Medien. Den Gesetzgeber nun auch noch in dieser Weise mit zahlreichen Ausgestaltungsanforderungen zu Kontrolle, Transparenz und Rechtsschutz gleichsam „an die Hand nehmen“ zu wollen, ist auch durch die bisherigen, in der mündlichen Verhandlung zu Tage getretenen praktischen Erfahrungen nicht veranlasst und engt die originäre Gestaltungsbefugnis des Gesetzgebers in meines Erachtens verfassungsrechtlich nicht angezeigter Weise ein.

III.

Soweit der Senat die Befugnisse zur weiteren Nutzung der im Rahmen der Terrorismusabwehr erhobenen Daten und zu deren Übermittlung an inländische und ausländische Stellen in verschiedener Hinsicht als verfassungswidrig erachtet, vermag ich dem ebenfalls nicht uneingeschränkt zu folgen. Das gilt insbesondere, soweit der Senat die Verwendung der rechtmäßig erhobenen Daten in anderen Zusammenhängen allein zum Schutz derselben oder gleichgewichtiger Rechtsgüter zulassen will. Dies hat allenfalls seine Berechtigung hinsichtlich der Erkenntnisse aus hochinvasiven Eingriffen wie der Wohnraumüberwachung und der Online-Durchsuchung informationstechnischer Systeme, führt jedoch bei anderen Maßnahmen in bestimmten Fallgestaltungen beim Anfall sogenannter Zufallserkenntnisse zu meines Erachtens nicht verantwortbaren Ergebnissen und kann in dieser dogmatischen Rigorosität gewichtige Rechtsgüter Einzelner und der Allgemeinheit schutzlos stellen. 19

1. Das Urteil macht die Übermittlung und Verwendung von Daten zu anderen Zwecken unter anderem davon abhängig, dass diese auch nach der Zweckänderung dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre neue Erhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (Kriterium der hypothetischen Datenneuerhebung). Diese Sichtweise mag ihre Berechtigung bei Erkenntnissen haben, die mittels hochinvasiver, besonders schwerwiegender Eingriffe gewonnen worden sind, wie das etwa bei der Wohnraumüberwachung und der Online-Durchsuchung informationstechnischer Systeme der Fall ist. Bei anderen 20

Eingriffen, bei denen sogenannte Zufallserkenntnisse anfallen, kann dies jedoch - konsequent in der vom Senat verlangten Weise umgesetzt - zu meines Erachtens kaum erträglichen Ergebnissen führen, weil dies von der rechtsstaatlichen Ordnung nicht mehr und nicht weniger verlangt, als vor drohenden Gefahren für ebenfalls wenigstens gewichtige Rechtsgüter die Augen zu verschließen und die Realisierung von Straftaten und die Beschädigung von Rechtsgütern hinzunehmen. Damit verfehlt der Rechtsstaat insoweit seine Schutzaufgabe.

Dies lässt sich an Beispielen verdeutlichen: Für die behördeninterne Zweck- 21
änderung lässt sich vorstellen, dass etwa bei einer Maßnahme der Telefonüberwachung eine Zufallserkenntnis anfällt, die für den Bereich der Aufgaben des Personenschutzes durch das Bundeskriminalamt (§ 5 BKAG) Relevanz hat. Geht es etwa um Hinweise auf einen geplanten „Farbbeutel-Anschlag“, so dürfte diese Zufallserkenntnis nicht an die innerhalb des Bundeskriminalamts zuständige Abteilung weitergegeben werden. Würde sie bei einer Leitungsbesprechung erwähnt, dürfte der zuständige Abteilungsleiter daraus nichts herleiten.

Für die behördenübergreifende Übermittlung und Verwendung solcher Zu- 22
fallserkenntnisse lässt sich für den Bereich des Individualrechtsgüterschutzes das Beispiel bilden, dass es um beiläufige Erkenntnisse über eine Verabredung zur Behelligung von Passanten an einem bestimmten Ort geht, um diese unter der Ablenkung zu bestehlen (vgl. § 242 StGB). Weiter ist vorstellbar, dass konkrete Hinweise zur Einleitung von umweltschädlichen Stoffen in Gewässer oder den Boden anfallen (vgl. §§ 324, 325 StGB). Damit stünden jeweils Rechtsgüter in Rede, bei denen etwa eine Telekommunikationsüberwachung nicht statthaft wäre. Das Bundeskriminalamt dürfte in einem solchen Fall die Zufallserkenntnis nach der Dogmatik des Senats mangels Gleichwertigkeit der Rechtsgüter nicht an die örtlich zuständige Polizei weitergeben, um so gewichtige Rechtsgutsverletzungen zu verhindern. Den gefährdeten Rechtsgütern bliebe der gebotene Schutz versagt.

Unter der Voraussetzung, dass eine solche Zufallserkenntnis aufgrund eines 23
recht- und damit auch verfassungsmäßigen Eingriffs angefallen ist, halte ich es für eine nicht hinnehmbare Konsequenz, dass der Rechtsstaat hier gezielt „wegsehen muss“ und damit den potentiell betroffenen Einzelnen oder Rechtsgütern der Allgemeinheit der gebotene Schutz vorenthalten wird, um auf der anderen Seite dem Schutz der Daten derjenigen, mit denen sich die Maßnahmen befassen, den Vorrang einzuräumen, zumal es hier eben nicht um die Fallgestaltung der Zweckänderung von anlasslos in großer Breite erhobenen Massendaten geht. Im Blick auf

den wirksamen Schutz von Rechtsgütern, dem der Rechtsstaat verpflichtet ist, kann es nicht untersagt sein, einen entsprechenden Hinweis an die zuständige Stelle weiterzugeben, um gefährdete Rechtsgüter vor Schaden zu bewahren. Freilich ist stets Voraussetzung, dass die Erkenntnis bei einem rechtmäßigen Eingriff angefallen ist, dieser sich auch nicht als Umgehungstatbestand erweist und die Verwendung nicht unvereinbar mit der ursprünglichen Zwecksetzung ist (vgl. dazu die Erwähnung dieser Gesichtspunkte in dem Beschluss des Zweiten Senats vom 7. Dezember 2011, BVerfGE 130, 1 <33 f.>; vgl. zum Strafprozess und zur Verwertbarkeit von Zufallserkenntnissen aus einer Telefonüberwachung zwar nicht zu *Beweiszwecken*, wohl aber als *Spurenansatz*: BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 29. Juni 2005 - 2 BvR 866/05 -, NJW 2005, S. 2766 m. Anm. Allgayer, NStZ 2006, S. 603 ff.).

Die gegenteilige Auffassung des Senats ist zwar in seiner jüngeren Spruch- 24
praxis angelegt, dort aber vornehmlich zu Sachverhalten entwickelt worden, die spezifische Grundrechtsgefährdungen zum Gegenstand hatten, welche sich bei der Vernetzung großer Dateien (Antiterrordatei als Verbunddatei) oder der Verwendung anlasslos in großer Breite von Netzbetreibern erhobener und vorzuhaltender Daten ergeben (vgl. BVerfGE 125, 260; 133, 277). Noch in seinem Urteil zur strafprozessualen Wohnraumüberwachung (vom 3. März 2004, BVerfGE 109, 279 <376>) hat es der Senat für die Zweckänderung ausreichen lassen, dass diese durch Allgemeinbelange gerechtfertigt ist, die die grundrechtlich geschützten Interessen überwiegen, und dass die Verwendungszwecke nicht miteinander unvereinbar sind. Diese Anforderungen sind sukzessive ausgebaut worden und haben jetzt einen Punkt erreicht, an dem die Ergebnisse mir für bestimmte Fallgruppen nicht mehr vertretbar erscheinen. Nach meiner Bewertung darf die Zufallserkenntnis in der beschriebenen Fallgestaltung als Gefahrenverhütungsansatz zur Verhinderung einer gewichtigen Straftat oder zur Abwehr von Gefahren für gewichtige Rechtsgüter sehr wohl weitergegeben werden, weil hier Allgemeinbelange (die Schutzverpflichtung des Rechtsstaats) und die gefährdeten Rechtsgüter Dritter oder der Allgemeinheit das grundrechtlich geschützte Interesse des vom Eingriff Betroffenen überwiegen, nachdem die staatliche Stelle die Zufallserkenntnis auf legale Weise bereits erlangt hat. Das gilt auch dann, wenn das gefährdete Rechtsgut nicht in jeder Hinsicht eine Rechtsgutsäquivalenz zu den Eingriffs- und Datenerhebungsvoraussetzungen aufweist.

2. Der Senat hält die Verwendung der nach den in Rede stehenden Regelun- 25
gen erhobenen personenbezogenen Daten zur Wahrnehmung der Aufgaben des

Bundeskriminalamts im Bereich des Zeugenschutzes und des Schutzes von Mitgliedern der Verfassungsorgane (Personenschutz, Innenschutz; §§ 5, 6 BKAG) für in verfassungswidriger Weise unbestimmt. Das vermag nicht zu überzeugen. Eine die hinreichende Bestimmtheit gewährleistende verfassungskonforme Auslegung drängt sich selbst auf der Grundlage der Anforderungen des Senats zur Gleichgewichtigkeit der zu schützenden Rechtsgüter auf. Der nach dem Wortlaut einschränkungslose allgemeine Verweis in § 20v Abs. 4 Satz 2 Nr. 2 BKAG auf die Aufgaben des Bundeskriminalamts nach § 5 und § 6 BKAG erhellt und konturiert sich ohne weiteres aus den Aufgabennormen, auf die verwiesen wird, und ist damit einer einschränkenden verfassungskonformen Auslegung zugänglich. Da die Aufgaben des Personenschutzes, des inneren Schutzes im Sinne des § 5 Abs. 1 Nr. 2 BKAG und des Zeugenschutzes ihrer Natur nach auf den Schutz von Leib, Leben und Freiheit der zu schützenden Personen angelegt sind, stehen hinreichend gewichtige Rechtsgüter in Rede. Werden die anderweit erhobenen personenbezogenen Daten in diesem Sinne verwendet, ist dagegen von Verfassungs wegen selbst auf der Grundlage der maßgeblichen Anforderungen des Senats nichts zu erinnern.

3. Ebenso wenig vermag ich der Würdigung des Senats zuzustimmen, wo- 26
nach § 20v Abs. 5 Satz 1 Nr. 2 BKAG, der die Übermittlung von Daten zur Verhütung der in § 129a Abs. 1 und 2 StGB genannten Straftaten erlaubt, mangels eingrenzender Konkretisierung des Übermittlungsanlasses unverhältnismäßig weit gefasst sei. Der Senat beanstandet, dass die Bestimmung es zulasse, schon mit Blick auf einen nur potentiellen Informationsgehalt als Spurenansatz die Information zu übermitteln. Er verlangt, dass sich aus der Information zumindest ein konkreter Ermittlungsansatz für die Aufdeckung entsprechender Straftaten ergeben müsse. Dies jedoch stelle die Vorschrift nicht sicher.

Damit geht der Senat daran vorbei, dass die Beurteilung der Relevanz der 27
entsprechenden Information oft erst durch die Einfügung in weitere Erkenntnisse möglich ist, die der Zielbehörde vorliegen, und dass die verlangte Bewertung in tragfähiger Weise nur durch diese vorgenommen werden kann. Abgesehen davon wäre aber auch auf der Grundlage der Auffassung des Senats eine verfassungskonforme einengende Auslegung möglich gewesen.

4. Anders als der Senat meint, begegnet meines Erachtens auch die Vorschrift 28
des § 14 BKAG, die die Übermittlung von Daten an öffentliche Stellen anderer Staaten regelt, in verfassungskonformer Auslegung keinen durchgreifenden ver-

fassungsrechtlichen Bedenken. Die vom Senat formulierten Einschränkungen sind zwar unbezweifelbar zutreffend: Durch die Übermittlung darf Menschenrechtsverletzungen in anderen Staaten nicht im Mindesten Vorschub geleistet werden. Insofern ist auch die Anforderung einer Vergewisserung über einen rechtsstaatlichen Umgang mit etwa übermittelten Daten im Empfängerland eine Selbstverständlichkeit. Weitergehend als im Gesetz geschehen hierfür jedoch zusätzlich die Schaffung „normenklarer“ Rechtsgrundlagen und die Sicherstellung einer wirksamen Kontrolle zu fordern, ist angesichts der Vielfalt der in Betracht kommenden Konstellationen und der begrenzten Einwirkungsmöglichkeiten der deutschen Rechtsordnung auf die Standards in anderen Ländern nicht zielführend. Insoweit kommt gerade im Blick auf die mitunter schwierigen Abgrenzungen zwischen den Anforderungen einer effektiven Abwehr terroristischer Gewalttaten und des dafür grundsätzlich unverzichtbaren Austauschs von Informationen im internationalen Rahmen der Einzelfallabwägung sehr große Bedeutung zu. Die Entscheidungspraxis des Bundeskriminalamts ist an Recht und Gesetz, insbesondere an die Grundrechte und Menschenrechte gebunden und letztlich politisch zu kontrollieren und zu verantworten, gegebenenfalls auch fachgerichtlich zu überprüfen. Die Entscheidungen, die hier zu treffen sind, erscheinen auf der Grundlage des § 14 BKAG bei entsprechender Auslegung der Bestimmung als verfassungsrechtlich hinreichend abgesichert. Diese Vorschrift sieht ausdrücklich das Unterbleiben der Übermittlung personenbezogener Daten vor, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde oder im Einzelfall schutzwürdige Interessen der betroffenen Person überwiegen (§ 14 Abs. 7 Satz 4 und 5 BKAG). Zu diesen schutzwürdigen Interessen gehört auch das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat (§ 14 Abs. 7 Satz 6 BKAG). Weitergehende Übermittlungsverbote und Verweigerungsgründe enthält die gemeinsame Vorschrift des § 27 BKAG (vgl. insbes. § 27 Abs. 1, Abs. 2 Nrn. 2 u. 4, Abs. 3 Nr. 2 Alt. 2 BKAG). § 27 Abs. 2 und 3 BKAG nehmen freilich nur auf die Vorschrift des § 14a BKAG Bezug, die die Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union betrifft. Die dort aufgeführten detaillierteren Grundsätze sind bei einer systematischen Auslegung jedoch ohne weiteres auch auf die Auslegung der Regelung für die Übermittlung an Stellen von Nicht-EU-Staaten übertragbar, geben jedenfalls eine hinreichende Richtschnur für das Verständnis und die Auslegung des § 14 BKAG.

Die vom Senat eingeforderten ergänzenden gesetzlichen Regelungen werden 29
das stets einzelfallbezogene Problem ohnehin nicht wirklich lösen können. Die

vom Gesetzgeber nun zu schaffenden Konkretisierungen im Regelwerk werden auch in diesem Zusammenhang nur zu einer das Gegenteil von Normenklarheit bewirkenden textlichen Aufblähung des ohnehin schon überbordenden, nur schwer lesbaren und verständlichen Regelwerks führen. Dem dürfte überdies in der praktischen Anwendung kein nennenswertes Mehr an Schutznutzen für die betroffenen Personen gegenüberstehen.

Schluckebier