ENTSCHEIDUNGEN / ANMERKUNGEN

BKAG teilweise verfassungswidrig
BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09

Leitsätze

1. a) Die Ermächtigung des BKA 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 GG 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.

Tenor

1. § 20h Abs. 1 Nr. 1 lit. c des BKAG i.d.F. des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA vom 25.12.2008 (BGBl I, S. 3083) und i.d.F. späterer Gesetze verstößt gegen Art. 13 Abs. 1 des GG und ist nichtig.

2. § 20v Abs. 6 S. 5 BKAG verstößt gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1, jeweils i.V.m. Art. 19 Abs. 4 des GG, und ist nichtig.

3. § 14 Abs. 1 (ohne S. 1 Nr. 2), § 20g Abs. 1 bis 3, §§ 20h, 20j, 20k, 20l, § 20m Abs. 1, 3, § 20u Abs. 1, 2 und § 20v Abs. 4 S. 2, Abs. 5 S. 1 bis 4 (ohne S. 3 Nr. 2), Abs. 6 S. 3 des BKAG sind nach Maßgabe der Urteilsgründe mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs.1 und 3 – auch i.V.m. Art. 1 Abs. 1 und Art. 19 Abs. 4 GG – nicht vereinbar.

4. Bis zu einer Neuregelung, längstens jedoch bis zum 30.6.2018 gelten die für mit dem GG unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass Maßnahmen gem. § 20g Abs. 2 Nr. 1, 2 b, 4 und 5 BKAG nur durch ein Gericht angeordnet werden dürfen; bei Gefahr im Verzug gilt § 20g Abs. 3 S. 2 bis 4 BKAG entsprechend.

Maßnahmen gem. § 20g Abs. 1 S. 1 Nr. 2, § 20l Abs. 1 S. 1 Nr. 2 und § 20m Abs.1 Nr. 2 BKAG dürfen nur angeordnet werden, wenn die Voraussetzungen des § 20k Abs. 1 S. 2 BKAG in der in den Urteilsgründen dargelegten verfassungskonformen Auslegung vorliegen.

Eine weitere Verwendung von Daten gem. § 20v Abs. 4 S. 2 BKAG oder eine Übermittlung von Daten gem. § 20v Abs. 5 und § 14 Abs. 1 BKAG betreffend Daten aus Wohnraumüberwachungen (§ 20h BKAG) ist 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.

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.

Gründe

1 A. I. Die Verfassungsbeschwerden richten sich gegen Regelungen des BKAG, die als Unterabschnitt 3a durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA vom 25.12.2008 (BGBl I, S. 3083) mit Wirkung zum 1.1.2009 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 BKA 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 BKAG zur Übermittlung von Daten ins Ausland, die durch die Aufgabenerweiterung ein weiteres Anwendungsfeld erhält.

2 II. Die Verfassungsbeschwerden wenden sich zum einen gegen die Einräumung verschiedener Ermittlungsbefugnisse. Angegriffen ist die Ermächtigung zur Befragung von Personen gem. § 20c BKAG sowie zum Einsatz von besonderen Mitteln der Datenerhebung außerhalb von Wohnungen gem. § 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 gem. § 20h BKAG, zur Rasterfahndung gem. § 20j BKAG, zu Zugriffen auf informationstechnische Systeme gem. § 20k BKAG, zur Überwachung der laufenden Telekommunikation gem. § 20l BKAG sowie zur Erhebung von Telekommunikationsverkehrsdaten gem. § 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.

3 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 gem. § 20v Abs. 4 S. 2 BKAG durch die Behörde selbst. Zur Prüfung gestellt sind des Weiteren die Befugnisse gem. § 20v Abs. 5 BKAG – mit Ausnahme des S. 3 Nr. 2 – zur Übermittlung dieser Daten an andere öffentliche Stellen im Inland. Schließlich richten sich die Angriffe auch gegen § 14 Abs. 1 S. 1 Nr. 1 und 3 und S. 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.

4 Die für das Verfahren maßgeblichen Normen lauten:
(wird ausgeführt)
[...]

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

87 I. In kompetenzrechtlicher Hinsicht sind die angegriffenen Vorschriften indes verfassungsgemäß.
(wird ausgeführt)
[...]

90 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.

91 1. Die angegriffenen Befugnisse ermächtigen das BKA 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 i.V.m. Art. 1 Abs. 1 GG, letzteres sowohl in seiner Ausprägung als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als auch als Recht auf informationelle Selbstbestimmung.

92 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 gem. § 20g Abs. 1, 2 BKAG.

93 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]; st. Rspr).

94 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]; st. Rspr). 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]).

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

96 a) Die Befugnisse dienen einem legitimen Ziel. Sie geben dem BKA 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-Rahmenbeschl. v. 13.6.2002 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 3.11.2010, 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. 9 lit. a GG (vgl. BT-Drs. 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]).

97 b) Die Einräumung der fraglichen Überwachungs- und Ermittlungsbefugnisse ist zur Erreichung dieses Ziels geeignet. Sie geben dem BKA 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.

98 III. Begrenzungen ergeben sich maßgeblich aus den Anforderungen der Verhältnismäßigkeit im engeren Sinne.

(wird ausgeführt)
[...]

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

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

147 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 BKA damit zu Eingriffen in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

148 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. BT-Drs. 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.

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

150 Die Vorschrift erlaubt Überwachungen außerhalb von Wohnungen mit den in Abs. 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.

151 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.

152 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 (s.o. C II 3 a). Vorausgesetzt ist dabei, dass sie verhältnismäßig ausgestaltet sind. Das ist hier allerdings nur teilweise der Fall.

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

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

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

156 Die Eingriffsbefugnisse sind dabei gem. § 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 S. 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.

157 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 gem. § 4a Abs. 1 S. 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.

158 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. Gem. § 20a Abs. 2 BKAG ist hierunter eine „im Einzelfall bestehende Gefahr" und damit eine konkrete Gefahr i.S.d. 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.

159 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 BKA die Zustandsverantwortlichkeit gem. § 18 BPolG praktisch wirksam werden kann, oder ob die Vorschrift insoweit im Ergebnis leerläuft (vgl. *Bäcker*, Terrorismusabwehr durch das BKA, 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 gem. § 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 S. 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.

160 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.

161 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. Allerdings 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.]).

162 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.

163 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.

164 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 (s.o. C IV 1 b). Die diesbezüglichen Anforderungen sind normenklar zu regeln.

165 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 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.

166 e) Verfassungsrechtlich nicht zu beanstanden ist bei verfassungskonformer Auslegung demgegenüber § 20g Abs. 1 Nr. 3 i.V.m. § 20b Abs. 2 Nr. 2 BKAG.

167 § 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.

168 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.

169 Keine Bedenken sind dabei auch gegen die Merkmale des § 20b Abs. 2 Nr. 2 lit. 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 lit. 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 lit. c BKAG, dass die Instrumentalisierung des Betroffenen in einem engen 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.

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

171 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]).

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

173 § 20g Abs. 3 BKAG sieht einen Richtervorbehalt unmittelbar für die erstmalige Anordnung der Maßnahme nur beim Einsatz Verdeckter Ermittler vor (vgl. § 20g Abs. 3 S. 1 BKAG). In anderen Fällen erlaubt er die erstmalige Anordnung unmittelbar durch das BKA selbst und fordert eine richterliche Entscheidung erst für deren etwaige Verlängerung (§ 20g Abs. 3 S. 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 lit. 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 lit. a, 3 BKAG) durchgeführt werden.

174 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, Entsch. v. 2.9.2010, Nr. 35623/05, NJW 2011, S. 1333 [1336 f.], zu Art. 8 EMRK). Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen i.S.d. § 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.

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

176 § 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 höchstvertrauliche Situationen erfasst werden können, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (vgl. *Poscher*, JZ 2009, S. 269 [271 f.]).

177 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 (s.o. 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.

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

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

180 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 (s.o. C II 3 a). Sie stehen aber unter besonders strengen Anforderungen, die § 20h BKAG nicht in jeder Hinsicht erfüllt.

181 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.

182 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.

183 § 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 (s.o. C IV 1 a). Das gilt bei einem hier geboten engen, auf den 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]).

184 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 An-

forderungen 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 (s.o. C IV 1 b).

185 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.

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

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

188 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 *BVerfG* 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.]).

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

190 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 Anforderungen genügenden Anlass für die Durchführung solcher Maßnahmen ab (s.o. C IV 1 b).

191 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 lit. c BKAG). Sie ist unverhältnismäßig.

192 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 (s.o. C IV 1 c).

193 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 S. 3 BKAG) und zur Überwachung der

Zielperson, wie dargelegt, sogar Wohnraumüberwachungen in Wohnungen Dritter durchgeführt werden dürfen.

194 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.

195 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]).

196 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 i.V.m. Art. 1 Abs. 1 GG nicht.

197 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.]).

198 (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 (s.o. 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]; s.o. C IV 3 a, d).

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

200 (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]).

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

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

203 (1) § 20h Abs. 5 S. 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 S. 3, die die Rechtmäßigkeitsvoraussetzungen von S. 1 nicht aufhebt, sondern an die nach S. 2 gebotene Unterbrechung des persönlichen Abhörens und Beobachtens anknüpft. Wenn in § 20h

Abs. 5 S. 1 BKAG kernbereichsrelevante "Äußerungen" unter Schutz gestellt werden, ist dieses sachgerecht so zu verstehen, dass hierunter auch bildlich erfasste entsprechende Situationen fallen können.

204 (2) Nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen genügen indes die Regelungen zum Kernbereichsschutz auf der Verwertungsebene. Zwar 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 S. 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 S. 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 gem. § 20h Abs. 5 S. 4 BKAG nicht. Freilich lässt das GG dem Gesetzgeber Raum, bei der Ausgestaltung der im Grundsatz umfassenden Kontrollbefugnis für Ausnahmefälle bei Gefahr im Verzug besondere Regelungen vorzusehen.

205 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 S. 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.

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

207 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 (s.o. C IV 1 a, V 1 c aa) und setzt gem. § 20j Abs. 1 S. 1 i.V.m. § 20a Abs. 2 BKAG eine konkrete Gefahr voraus. Verfassungsrechtlich nicht zu beanstanden ist insoweit auch das Regelbeispiel in § 20j Abs. 1 S. 1, 2. HS 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.

208 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.

209 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).

210 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 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.

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

212 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 S. 1 – i.V.m. § 20a Abs. 2 BKAG – auf das Vorliegen bestimmter Tatsachen abstellt, die die Annahme rechtfertigen, dass eine im Einzelfall bestehende Gefahr vorliegt.

213 Einer verfassungskonform einschränkenden Auslegung bedarf allerdings § 20k Abs. 1 S. 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 (s.o. C IV 1 b).

214 Da § 20k Abs. 1 S. 2 BKAG in enger Anlehnung an die Rechtsprechung des *BVerfG* 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.

215 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.

216 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.]; s.o. 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.

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

218 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 primär 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.

219 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]).

220 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 BKA herausfiltert (vgl. BVerfGE 120, 274 [338 f.]).

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

222 (1) Bei verfassungskonformer Auslegung nicht zu beanstanden sind allerdings die Regelungen auf der Ebene der Datenerhebung. S. 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 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 (s.o. C IV 3 a, d).

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

224 Die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle 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 BKAs zur Gewährleistung von ermittlungsspezifischem Fachverstand nicht ausgeschlossen. Ebenso kann darüber hinaus für die Sichtung auf technische Unterstützung – etwa auch zur Sprachmittlung – durch das BKA zurückgegriffen werden. Die tatsächliche Durchführung und Entscheidungsverantwortung muss jedoch maßgeblich in den Händen von dem BKA gegenüber unabhängigen Personen liegen.

225 Das sichert die derzeitige Regelung nicht. Sie überlässt die Sichtung im Wesentlichen Bediensteten des BKA 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.

226 Demgegenüber stellt § 20k Abs. 7 S. 5 bis 7 BKAG die weiteren auf Verwertungsebene gebotenen Vorkehrungen an einen wirksamen Kernbereichsschutz verfassungsrechtlich tragfähig sicher. Verfassungswidrig ist allerdings auch hier die übermäßig kurze Dauer für die Aufbewahrung der Löschungsprotokolle gem. § 20k Abs. 7 S. 8 BKAG (s.o. C IV 3 d).

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

228 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]).

229 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 (s.o. C II 3

a), sofern die Eingriffsgrundlagen im Einzelnen verhältnismäßig begrenzt sind. Dies ist durch § 20l BKAG nur teilweise sichergestellt.

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

231 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 gem. § 20l Abs. 1 Nr. 1 BKAG.

232 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 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 (s.o. 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. BT-Drs. 16/10121, S. 31). Soweit sich § 20l Abs. 2 BKAG auf diese Vorschrift bezieht, kann nichts anderes gelten.

233 Demgegenüber ist die mögliche Erstreckung der Telekommunikationsüberwachung auf Nachrichtenmittler gem. § 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.

234 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 Nr. 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 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 BKA inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.

235 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 (s.o. 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 S. 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.

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

237 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]).

238 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 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]).

239 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]).

240 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.

241 Der Gesetzgeber hat hierbei nicht unerheblichen Gestaltungsspielraum. So hat das *BVerfG* im Zusammenhang mit einer Regelung, die auf der Stufe der Datenerhebung wie vorliegend § 20l Abs. 6 S. 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 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 (s.o. 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.

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

243 (1) § 20l Abs. 6 S. 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 S. 2, 3 BKAG.

244 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 S. 2, 1. HS 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 Einzelfall. Ebenso setzt die mit dieser Regelung in Kauf genommene Erfassung von höchstpersönlichen Informationen wirksame Schutzvorkehrungen auf der Stufe der Aus- und Verwertung voraus.

245 (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.

246 Verfassungswidrig ist demgegenüber auch hier die zu knappe Aufbewahrungsfrist der Löschungsprotokolle gem. § 20l Abs. 6 S. 10 BKAG (s.o. C IV 3 d).

247 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.

248 a) § 20m Abs. 1, 3 BKAG, der die Erhebung von Telekommunikationsverkehrsdaten erlaubt, begründet einen Eingriff in das Telekommunikationsgeheimnis gem. 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]; st. Rspr.).

249 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.

250 b) Für die verfassungsrechtliche Beurteilung der Vorschrift, deren Eingriffsvoraussetzungen sich mit denen des § 20l Abs. 1, 3 bis 5 BKAG im Wesentlichen decken, gelten die diesbezüglichen Ausführungen entsprechend. Da insoweit Anforderungen verfehlt werden, die sich für eingriffsintensive Ermittlungs- und Überwachungsmaßnahmen schon übergreifend aus dem Verhältnismäßigkeitsgrundsatz ergeben (s.o. C IV 1 b, 2), gilt für die Telekommunikationsverkehrsdatenerhebung nichts anderes als für die inhaltliche Überwachung der Telekommunikation.

251 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 (s.o. C V 5 b, d).

252 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 *BVerfG* § 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 10.12.2015 (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 S. 2 BKAG, der für die Anordnung der Maßnahme Erleichterungen bezüglich der Bezeichnung der zu erhebenden Daten vorsieht; hierdurch bleibt unberührt, dass gem. § 20m Abs. 1 BKAG nur auf einzelne Personen bezogene Datenerhebungen zulässig sind.

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

254 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 (s.o. 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 Sicherheitsbehörden im Rahmen ihrer Befugnisse von sich aus zu beachten (vgl. BVerfGE 109, 279 [323]; 112, 304 [319]; 130, 1 [24]; st. Rspr.). Weiterer gesetzlicher Konkretisierung bedarf es insoweit nicht. Soweit es um die hierfür erforderliche Koordination der Befugnisse innerhalb des BKA selbst geht, durfte der Gesetzgeber davon ausgehen, dass diese angesichts der vergleichsweise übersichtlichen Größe und Strukturen des BKA im Rahmen der Leitungsverantwortung hinreichend gewährleistet ist. Soweit es demge-

genüber 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 gem. § 4a Abs. 2 BKAG vertraut.

255 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.

256 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 S. 1, 2. Halbs. StPO gebietet die Verfassung insoweit die Vermutung, dass von einem Überwiegen des Interesses des BKA an der Erhebung der Daten in der Regel nicht auszugehen ist, wenn die Maßnahme nicht der Abwehr einer erheblichen Gefahr dient.

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

258 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 S. 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 12.10.2011 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 (s.o. C IV 3 a).

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

260 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.]).

261 Dies gilt auch für § 20w Abs. 2 S. 1, 2. Halbs. 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 [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.

262 Verfassungsmäßig ist auch das endgültige Absehen von einer Benachrichtigung nach Ablauf von mindestens fünf Jahren gem. § 20w Abs. 3 S. 5 BKAG. In Übereinstimmung mit der derzeitigen Praxis, wie sie in der mündlichen Verhandlung von Vertretern des BKA 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.

263 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.

264 Vom Grundsatz her ist ein Auskunftsrecht in § 19 BDSG anerkannt, dessen Anwendbarkeit für das BKAG nach § 37 BKAG nicht ausgeschlossen ist. Dass dabei im Zusammenhang mit Ermittlungen des BKA 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]).

265 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 (s.o. C IV 6 c).

266 c) Nicht verfassungsrechtlich hinreichend ausgestaltet ist demgegenüber die aufsichtliche Kontrolle (s.o. 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]).

267 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 S. 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 S. 2 StPO noch nicht einmal eine Unterrichtung des anordnenden Gerichts über die Ergebnisse der Ermittlungen vorgesehen.

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

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

270 a) Die Grundstruktur der Regelung ist freilich verfassungsrechtlich nicht zu beanstanden. Die Daten sind nach Erfüllung des der Datenerhebung zugrundeliegenden Zwecks zu löschen (S. 1). Dies verweist auf die verfassungsrechtlichen Grundsätze zur Zweckbindung (siehe unten D I). Mit Blick auf eine weitere Verwendung der Daten gem. § 20v Abs. 4 S. 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 (S. 2). Die Löschung kann für eine etwaige gerichtliche Überprüfung zurückgestellt werden; die Daten sind dann zu sperren (S. 4). Verfahrensrechtlich steht die Vorschrift in Kontext mit § 32 BKAG. Nach dessen Abs. 3 sind neben der Einzelfallbearbeitung auch periodisierte Prüfungen der Löschungspflichten vorgesehen.

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

272 b) Verfassungsrechtlich nicht tragfähig ist demgegenüber die Anordnung der sehr kurzen Frist zur Löschung der „Akten" in § 20v Abs. 6 S. 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]).

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

274 c) Verfassungswidrig ist darüber hinaus § 20v Abs. 6 S. 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 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.

275 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.

276 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.]; st. Rspr.).

277 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]; st. Rspr.). 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.).

278 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.

279 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.

280 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.

281 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 i.V.m. 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 Aufgaben 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.

282 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.

283 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.

284 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]).

285 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, Entsch. v. 29.6.2006, 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 als dem Erhebungszweck, unabhängig davon, ob es sich um die Verwendung als Beweismittel oder als Ermittlungsansatz handelt (vgl. BVerfGE 109, 279 [377]).

286 b) Die Ermächtigung zu einer Zweckänderung ist dabei am Verhältnismäßigkeitsgrundsatz 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.).

287 aa) Während nach der früheren Rechtsprechung des *BVerfG* 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.

288 bb) Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (vgl. BVerfGE 100, 313 [389 f.]; 109, 279 [377]; 110, 33 [73]; 120, 351 [369]; 130, 1 [34]).

289 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 i.V.m. weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt.

290 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.

291 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 (s.o. C IV 1 b) gerechtfertigt sein.

292 cc) In diesen Anforderungen an die Zulässigkeit einer Zweckänderung liegt eine konkretisierende Konsolidierung einer langen Rechtsprechung beider Senate des *BVerfG* (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 Gefahrenlage bestimmenden – Eingriffsschwellen gegenüber früheren Anforderungen (vgl. insb. 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).

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

294 1. Die in § 20v Abs. 4 S. 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.

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

296 aa) Die Vorschrift erlaubt dem BKA eine Verwendung der von ihm zur Terrorismusabwehr erhobenen Daten zur Wahrnehmung seiner Aufgabe nach § 4a Abs. 1 S. 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 S. 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 S. 2 BKAG qualifizierten Straftaten und damit zum Schutz nur von solchen hochrangigen Rechtsgütern genutzt werden dürfen, zu deren Schutz auch die Datenerhebungsbefugnisse des Unterabschnitts 3a – einschließlich der besonders eingriffsintensiven Überwachungsbefugnisse der §§ 20g ff. BKAG – eingesetzt werden dürfen.

297 (1) Die Verweisung auf § 4a Abs. 1 S. 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 S. 1 und 2 BKAG voneinander abgrenzen: Während sich S. 1 für die Zuweisung der Aufgabe der Gefahrenabwehr an den Wortlaut des Art. 73 Abs. 1 Nr. 9 lit. a GG anlehnt, der auch die Straftatenverhütung mitumfasst (s.o. C I 1), wird die Straftatenverhütung in S. 2 von der Gefahrenabwehr bewusst unterschieden. Da § 4a Abs. 1 S. 1 BKAG angesichts seines Charakters als Aufgabennorm für die Gefahrenabwehr jedoch Ermittlungen im Vorfeld konkreter Gefahren einschließt, ist der Verweis in § 20v Abs. 4 S. 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.

298 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 S. 2 Nr. 1 BKAG allein auf S. 1 der Vorschrift verweist, ist für die Konkretisierung der dort genannten Gefahren auf die nähere Definition in S. 2 zurückzugreifen, der bestimmte Straftaten abschließend aufführt und näher qualifiziert. Dass die dort un-

ter dem Gesichtspunkt der Straftatenverhütung aufgeführten Straftaten auch für die Gefahrenabwehr nach S. 1 maßgeblich sind, entspricht der Systematik des Gesetzes auch sonst (vgl. nur § 20a Abs. 2 BKAG).

299 (2) Indem § 20v Abs. 4 S. 2 Nr. 1 BKAG eine Datennutzung nur zur Abwehr von Gefahren durch terroristische Straftaten i.S.d. § 4a Abs. 1 S. 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.

300 Fast alle in § 4a Abs. 1 S. 2 BKAG i.V.m.§ 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 öffentlichen 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 gem. § 4a Abs. 1 S. 1, 2 BKAG nur dann in den Aufgabenbereich des BKA 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 gem. § 20v Abs. 4 S. 2 Nr. 1 BKAG stets dem Schutz solcher Rechtsgüter dienen, zu deren Schutz auch bei eingriffsintensiven Maßnahmen schon die Erhebung der Daten gerechtfertigt wurde.

301 bb) Nicht zu beanstanden ist grundsätzlich auch, dass § 20v Abs. 4 S. 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 (s.u. D II 1 b), hält sich dies im Rahmen der Zweckbindung. Es handelt sich um Daten, die das BKA 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 BKA die weitere Nutzung dieser Daten für die Terrorismusabwehr ohne weitere Einschränkungen erlauben (s.o. D I 1 b). Hiervon unberührt bleiben freilich die Löschungspflichten nach Erreichung des mit der Datenerhebung verfolgten Zwecks (s.o. C IV 7, VI 4 a).

302 b) Unverhältnismäßig weit ist § 20v Abs. 4 S. 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 (s.o. 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 Eingriffsvoraussetzungen, wie es für eine Datenneuerhebung mit diesen Mitteln verfassungsrechtlich geboten wäre (s.o. D I 1 b).

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

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

305 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, Entsch. v. 29.6.2006, Nr. 54934/00, § 79, NJW 2007, S. 1433 [1434], zu Art. 8 EMRK).

306 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.

307 3. Die Übermittlungsbefugnisse sind indes insoweit verfassungswidrig, als ihre Voraussetzungen den oben entwickelten Anforderungen in Bezug auf das Kriterium der hypothetischen Datenneuerhebung (s.o. D I 2 b) nicht genügen.

308 a) Keinen verfassungsrechtlichen Bedenken unterliegt allerdings § 20v Abs. 5 S. 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 BKA gem. § 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.

309 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 S. 1 Nr. 2 ff. BKAG.

310 b) § 20v Abs. 5 S. 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.

311 aa) § 20v Abs. 5 S. 1 Nr. 2 BKAG erlaubt zum einen die Übermittlung von Daten aus Maßnahmen gem. §§ 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]). Vorliegend 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]).

312 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 gem. §§ 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.

313 cc) Unverhältnismäßig weit und damit verfassungswidrig ist § 20v Abs. 5 S. 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 (s.o. 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 ihnen zumindest ein konkreter Ermittlungsansatz für die Aufdeckung entsprechender Straftaten ergibt. Dies stellt die Vorschrift nicht sicher.

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

315 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 S. 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 (s.o. 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.

316 bb) Unverhältnismäßig ist die Regelung zum anderen aber auch insoweit, als sie in S. 2 für die Nutzung von Daten aus Maßnahmen gem. §§ 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 S. 1 Nr. 3, S. 2 BKAG). Für Daten aus Maßnahmen gem. §§ 20k und 20l BKAG wirkt dies gegenüber dem allgemeinen Verweis auf die Vorschriften der Strafprozessordnung und damit auf § 161 Abs. 1, Abs. 2 S. 1 StPO als Einschränkung, für Daten aus Wohnraumüberwachungen hingegen, deren Verwendungsänderung in § 161 Abs. 2 S. 2, § 100d Abs. 5 Nr. 3 StPO enger geregelt ist, als Erweiterung. Unabhängig hiervon genügt diese Schwelle dem Kriterium der hypothetischen Datenneuerhebung nicht. Für die Wohnraumüberwachung hat das *BVerfG* 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 S. 1 Nr. 3, S. 2 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.

317 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.

318 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 S. 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.

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

320 Die Vorschrift, die für alle Daten außer solche aus Wohnraumüberwachungsmaßnahmen gilt (vgl. § 20v Abs. 5 S. 5 BKAG), erlaubt eine Übermittlung an die 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 (s.o. 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 gem. § 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 (s.o. D I 2 b bb). Verfassungsrechtlich geboten ist jedoch, dass nur Daten übermittelt werden dürfen, die aus Sicht des BKA 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 BKA 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.]).

321 e) Entsprechend genügt auch § 20v Abs. 5 S. 4 BKAG den verfassungsrechtlichen Anforderungen nicht. Die Vorschrift erlaubt eine Übermittlung von Daten an den Bundesnachrichtendienst unter entsprechenden Maßgaben wie § 20v Abs. 5 S. 3 Nr. 1 BKAG. Die Unterschiede in den Formulierungen haben – auch unter Berücksichtigung der Gesetzesbegründung (vgl. BT-Drs. 16/9588, S. 34) – keinen erkennbar sachlichen Gehalt und vermögen jedenfalls die verfassungsrechtliche Beurteilung nicht zu ändern. Die verfassungsrechtlichen Mängel des § 20v Abs. 5 S. 3 Nr. 1 BKAG gelten auch für diese Vorschrift.

322 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 Bundesdatenschutzbeauftragte gelten auch hier (vgl. oben C IV 6 d).

323 IV. § 14 Abs. 1 S. 1 Nr. 1 und 3, S. 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.

324 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 (s.o. D I 2 a). Für die Übermittlung ins Ausland gelten aber auch mit Blick auf die Achtung fremder Rechtsordnungen und -anschauungen eigene verfassungsrechtliche Bedingungen.

325 a) Eine Übermittlung von Daten ins Ausland führt dazu, dass die Gewährleistungen des GG 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 GG 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 zielt auch darauf, die zwischenstaatlichen Beziehungen im gegenseitigen Interesse wie auch die außenpolitische Handlungsfreiheit der Bundesregierung zu erhalten (vgl. BVerfGE 108, 129 [137]).

326 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.

327 Von daher ergeben sich zum einen Grenzen einer Übermittlung in Blick auf die Wahrung datenschutzrechtlicher Garantien. Die Grenzen der inländischen Datenerhebung und -verarbeitung des GG 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.

328 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*, Beschl. d. *Zweiten Senats* v. 15.12.2015 – 2 BvR 2735/14, Rn. 62 m.w.N.).

329 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).

330 aa) Für die Anforderungen an den Übermittlungs- und Nutzungszweck gelten grundsätzlich die nach deutscher Rechtsordnung maßgeblichen verfassungsrechtlichen Kriterien der Zweckänderung (s.o. D I 2): Eine Übermittlung ist zulässig, soweit die übermittelten Daten auch für den Übermittlungszweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (Kriterium der hypothetischen 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 (s.o. D I 2 b bb; vgl. ferner BVerfGE 109, 279 [377, 379]; 120, 274 [329 ff.]).

331 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 GG 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.

332 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.

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

334 (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 deutschen Rechtsordnung gelten oder ein gleichartiger Schutz gewährleistet ist wie nach dem GG. Das GG 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 GG übereinstimmen.

335 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 (s.o. 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*, Urt. v. 6.10.2015 - 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, Urt. v. 4.12.2015, Nr. 47143/06, §§ 227 ff.; Art. 17 Abs. 1 S. 1 Internationaler Pakt über bürgerliche und politische Rechte vom 19.12.1966, BGBl 1973 II, S. 1534, UNTS 999, S. 171; Art. 12 Allgemeine Erklärung der Menschenrechte v. 10.12.1948, 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 18.12.2013, 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 Empfän-

gerstaats sowie ihre Umsetzung in der täglichen Anwendungspraxis (vgl. ähnlich *EuGH*, Urt. v. 6.10.2015 - C-362/14, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 [3155], Rn. 75).

336 (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 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.

337 (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 BKA ausreichen lassen. Diese kann so lange Geltung beanspruchen, wie sie nicht durch entgegenstehende Tatsachen in besonders gelagerten Fällen erschüttert wird (vgl. *BVerfG*, Beschl. v. 15.12.2015 – 2 BvR 2735/14, Rn. 69 m.w.N.).

338 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 (s.o. 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*, Beschl. v. 15.12.2015 – 2 BvR 2735/14, Rn. 70). Welche Anforderungen im Einzelnen gelten, kann der Gesetzgeber auch von einer Einzelfallabwägung abhängig machen.

339 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*, Urt. v. 6.10.2015 – C-362/14, Schrems/Digital Rights Ireland, NJW 2015, S. 3151 [3155 ff.], Rn. 78, 81, 89).

340 cc) Auch ansonsten gelten in Deutschland die Anforderungen an eine wirksame aufsichtliche Kontrolle einschließlich einer hierfür geeigneten Protokollierung der jeweiligen Übermittlungsvorgänge sowie das Erfordernis von Berichtspflichten (s.o. C IV 6 d, e).

341 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.

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

343 a) § 14 Abs. 1 S. 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 BKA 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. D I 2 b). Die Befugnis ist damit nicht hinreichend eingegrenzt und unverhältnismäßig.

344 b) Gleichfalls zu weit und deshalb mit den verfassungsrechtlichen Anforderungen nicht vereinbar ist § 14 Abs. 1 S. 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 (s.o. D I 2 b bb; vgl. ferner BVerfGE 109, 279 [377, 379]). Eine solche Begrenzung enthält die Vorschrift nicht.

345 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 S. 1 Nr. 2 BKAG (s.o. 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 bestehende Gefahr handeln muss, erfüllt sie auch die Anforderungen an die Übermittlung von Daten aus Online-Durchsuchungen (s.o. D I 2 b bb).

346 c) Mit den Anforderungen an eine Zweckänderung

nicht vereinbar ist schließlich der Übermittlungstatbestand des § 14 Abs. 1 S. 2 BKAG.

347 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. 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]; auch oben C IV 1 a). Entsprechende Anforderungen sieht die Vorschrift für die Übermittlung indessen nicht vor.

348 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. 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.

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

350 aa) Indem § 14 Abs. 7 S. 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.

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

352 (1) Die Vorschrift begründet eine Verantwortung des BKA 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.

353 (2) Eine solche Vergewisserung sieht § 14 Abs. 7 S. 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 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 S. 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.

354 e) Im Übrigen genügen die Übermittlungsregelungen des § 14 Abs. 1 BKAG insoweit nicht den verfas-

sungsrechtlichen Anforderungen, als es an einer hinreichenden Regelung der aufsichtlichen Kontrolle sowie der Anordnung von Berichtspflichten zur Übermittlungspraxis fehlt (s.o. C IV 6 d, e). Demgegenüber ist eine Protokollierungspflicht, wie verfassungsrechtlich geboten, in § 14 Abs. 7 S. 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.]; s.o. C IV 6 b; C VI 3 b).

355 E. I. 1. Die Feststellung einer Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das *BVerfG*, wie sich aus § 31 Abs. 2 S. 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 *BVerfG* 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 *BVerfG* 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]).

356 2. Danach sind § 20h Abs. 1 Nr. 1 lit. c und § 20v Abs. 6 S. 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.

357 Demgegenüber sind § 20g Abs. 1 bis 3, §§ 20h, 20j, 20k, 20l, § 20m Abs. 1, 3 – diesbezüglich auch § 20v Abs. 6 S. 3, 2. HS – und § 20u Abs. 1, 2 sowie § 20v Abs. 4 S. 2, Abs. 5 S. 1 bis 4 (ohne S. 3 Nr. 2), § 14 Abs. 1 S. 1 Nr. 1 und 3, S. 2 BKAG lediglich für mit der Verfassung unvereinbar zu erklären; die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung bis zum Ablauf des 30.6.2018 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 BKA bis zu einer Neuregelung zentrale Ermittlungsbefugnisse bei der Abwehr des internationalen Terrorismus nehmen würde.

358 Die Anordnung der Fortgeltung bedarf mit Blick auf die betroffenen Grundrechte jedoch einschränkender Maßgaben. Anzuordnen ist zum einen, dass Maßnahmen gem. § 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 S. 2 bis 4 BKAG entsprechend. Zum anderen dürfen Maßnahmen gem. § 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 S. 2 BKAG in der in den Urteilsgründen dargelegten verfassungskonformen Auslegung vorliegen. Schließlich ist eine weitere Verwendung von Daten gem. § 20v Abs. 4 S. 2 BKAG oder eine Übermittlung von Daten gem. § 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.

359 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. (*wird ausgeführt*)
[...]