Deutscher Bundestag **Drucksache 18/13031**

18. Wahlperiode 23.06.2017

Unterrichtung

durch die Bundesregierung

Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes

Inhaltsübersicht

Zugeleitet mit Schreiben des Bundesministeriums des Innern vom 22. Juni 2017 gemäß Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt

GUTACHTEN
von unabhängigen Sachverständigen

Vorgelegt im Frühjahr 2017
von
Prof. Dr. Dr. h.c. mult. Hans-Jörg Albrecht
Prof. Dr. Ralf Poscher

Unter Mitarbeit von
Dr. Michael Kilchling
Dr. Philipp Lassahn, LL.M.

Inhaltsverzeichnis

Seite

Seite

Seite

A. Einführung

I. Hintergrund

Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt[1] sieht vor, dass die §§ 4a, 20j und 20k BKAG fünf Jahre nach ihrem Inkrafttreten unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren sind. Die Normen traten am 1. Januar 2009 in Kraft.[2] Am 2. Juli 2015 hat der Deutsche Bundestag sein Einvernehmen zur Bestellung der Sachverständigen erteilt. Seither haben einerseits das Max-Planck-Institut für ausländisches und internationales Strafrecht, Abteilung Kriminologie, Freiburg i.Br., unter Leitung von Professor Dr. Dr. h. c. Hans-Jörg Albrecht und andererseits Herr Professor Dr. Ralf Poscher, Freiburg i. Br., in fortlaufender Abstimmung mit dem Bundesministerium des Innern (folgend BMI) an einer normativ-empirischen Untersuchung der §§ 4a, 20j und 20k BKAG gearbeitet.

Im Oktober 2016 wurde dem BMI eine Vorabfassung des dogmatischen Teils dieses Gutachtens zur Verfügung gestellt.

II. Gegenstand und Ziel der Untersuchung

Die Evaluation zielt auf eine staatsrechtswissenschaftliche Einschätzung der §§ 4a, 20j und 20k BKAG auf empirischer Grundlage. Es geht darum, die Normanwendung in der Praxis, insbesondere durch das Bundeskriminalamt (folgend BKA), zu bewerten. Dies erfordert zum einen die Erhebung empirischer Daten zur bisherigen praktischen Handhabung der untersuchten Vorschriften. Zum zweiten ist eine darauf aufsetzende Analyse der verfassungs- und verwaltungsrechtlichen Fragestellungen verlangt. Diese soll auch aus einer Effektivitätsperspektive praktische Bedürfnisse aufzeigen, die sich aus dem Umgang mit den Normen ergeben. Im Hinblick auf identifizierte Risiken und Bedürfnisse werden ggf. Vorschläge für Anpassungen der normativen Grundlagen gemacht.

Dabei wird auch legistisch erwogen, ob und inwieweit sich einzelne Regelungselemente zusammenfassen und verallgemeinern lassen. Die Empfehlungen zielen zunächst auf die polizeirechtlichen Regelungen des BKAG und verstehen sich zugleich als erster Baustein für das Fernziel der Entwicklung eines allgemeinen Teils der Sicherheitsgesetze des Bundes.

Wie in Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vorgesehen, ist der Untersuchungsgegenstand auf die Erfahrungen mit den §§ 4a, 20j und 20k BKAG beschränkt. Als Untersuchungszeitraum wurden die Jahre einschließlich 2009 bis einschließlich 2014 gewählt. Da sich in diesem Zeitraum keine Rasterfahndung ereignet hatte, wurde zusätzlich die Rasterfahndung im Rahmen der EG[3] Advent als Untersuchungsgegenstand hinzugefügt.

Die Normen haben folgenden Wortlaut:

§ 4a

Abwehr von Gefahren des internationalen Terrorismus

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

1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
3. die oberste Landesbehörde um eine Übernahme ersucht.

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

---

1 BGBl. I 2008, 3083, 3094.

2 Siehe Art. 7 Abs. 1 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, BGBl. I 2008, 3083, 3094.

3 EG = Ermittlungsgruppe.

Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können.

(2) [1]Die Befugnisse der Länder und anderer Polizeibehörden des Bundes bleiben unberührt. [2]Die zuständigen obersten Landesbehörden und, soweit zuständig, anderen Polizeibehörden des Bundes sind unverzüglich zu benachrichtigen, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt. [3]Die Aufgabenwahrnehmung erfolgt in gegenseitigem Benehmen. [4]Stellt das Bundeskriminalamt bei der Aufgabenwahrnehmung nach Absatz 1 Satz 1 Nr. 2 die Zuständigkeit einer Landespolizeibehörde fest, so gibt es diese Aufgabe an diese Polizeibehörde ab, wenn nicht ein Fall des Absatzes 1 Satz 1 Nr. 1 oder 3 vorliegt.

§ 20j

Rasterfahndung

(1) [1]Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist; eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll. [2]Von den Verfassungsschutzämtern des Bundes und der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach Satz 1 nicht verlangt werden.

(2) [1]Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf andere im Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. [2]Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen vom Bundeskriminalamt nicht verwendet werden.

(3) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. [2]Die getroffene Maßnahme ist zu dokumentieren. [3]Diese Dokumentation ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Löschung der Daten oder der Vernichtung der Akten nach Satz 1 folgt, zu vernichten.

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

§ 20k

Verdeckter Eingriff in informationstechnische Systeme

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

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

[2]Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. [3]Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) [1]Es ist technisch sicherzustellen, dass

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

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

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) [1]Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

[2]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. [3]Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(4) [1]Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. [2]Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

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

(6) [1]Die Anordnung ergeht schriftlich. [2]In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

[3]Die Anordnung ist auf höchstens drei Monate zu befristen. [4]Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. [5]Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) [1]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. [2]Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [3]Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. [4]Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes). [5]Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. [6]Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. [7]Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [8]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

III. Vorgehen

In methodischer Hinsicht war die Untersuchung vor allem durch ihre Interdisziplinärität geprägt. Einerseits ging es darum, die Anwendungspraxis der untersuchten Normen empirisch zu erfassen. Andererseits war auf dieser Grundlage eine staatsrechtliche und dogmatisch-systematische Bewertung der Normen zu erstellen. Die empirischen und normativen Komponenten lassen sich dabei nicht in unterschiedliche zeitliche Phasen der Untersuchung unterteilen, sondern sind vielmehr permanent und vielfach verschränkt. So war es etwa für die Erarbeitung der empirischen Fragestellungen unerlässlich, bereits im Vorhinein die aus normativ-dogmatischer Sicht entscheidenden Fragen zu stellen und Probleme zu antizipieren. Ebenso war es bei der späteren staatsrechtlichen Bewertung erforderlich, immer wieder die Rückkopplung an empirische Befunde zu suchen. Empirischer und normativer Sachverstand haben so fortlaufend zusammengewirkt.

In instrumenteller Hinsicht war für die Untersuchung neben der allgemeinen, vor allem für die dogmatische Analyse bedeutsamen Recherche und Einordnung von Rechtsprechung und juristischer Literatur vor allem die Auswertung zahlreicher Unterlagen aus der Anwendungspraxis erforderlich. Hierbei handelte es sich um Unterlagen, die regelmäßig vom BKA selbst, im Übrigen durch andere in den Umgang mit den §§ 4a, 20j und 20k BKAG involvierten Einrichtungen, etwa das AG Wiesbaden, erstellt wurden. Diese Unterlagen wurden, soweit sie noch vorhanden waren und nicht unter Verschluss gehalten wurden,[4] auf Anfrage der Gutachter meist elektronisch übermittelt, in einigen Fällen auch zur Einsichtnahme vor Ort zur Verfügung gestellt.[5] Im Übrigen wurden Fragen der Gutachter im Schriftverkehr, in drei größeren Gesprächsrunden[6] sowie in individuellen Telefonaten und in zwei größeren Telefonkonferenzen[7], jeweils mit unterschiedlicher Zusammensetzung, geklärt.

IV. Herausforderungen

Eine erste Herausforderung für die Evaluation ergab sich aus der Bestimmung der Reichweite des Gutachtenauftrags. Denn Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt beschränkt den Auftrag zwar explizit auf §§ 4a, 20j und 20k BKAG. Allerdings legt der Verweis auf § 4a BKAG als allgemeine Kompetenzvorschrift eine extensive Interpretation nahe. Hinzu kam das Problem, inwieweit nicht in § 20k und § 20j BKAG, sondern in anderen Vorschriften geregelte Annexfragen zu berücksichtigen sind, soweit sie zur Bewertung der beiden Eingriffsnormen relevant werden – etwa mit Blick auf die Speicherung, Löschung und Weitergabe erhobener Daten. Auf Grund der expliziten Beschränkung des Gutachtenauftrags auf die §§ 4a, 20j und 20k BKAG wurde als Leitlinie gewählt, sich möglichst auf den Kern dieser Regelungen zu beschränken. Es sind im Folgenden also lediglich solche Aspekte berücksichtigt, die in einem spezifischen und untrennbaren Zusammenhang mit §§ 4a, 20j oder 20k BKAG stehen. Eine vertiefte oder gar gesonderte Untersuchung der allgemeinen Vorschriften zur Datenspeicherung, -löschung, -weitergabe usw. (vor allem §§ 20v ff. BKAG) erfolgte daher nicht.

Eine Herausforderung ergab sich auch aus der Verkündung der Entscheidung des Bundesverfassungsgerichts (folgend BVerfG) zur teilweisen Verfassungswidrigkeit des BKAG am 20. April 2016.[8] Dieses Urteil betraf auch Teile des Evaluierungsgegenstandes, insbesondere § 20k BKAG. Zwar deckte sich das Urteil weitgehend mit der bis zu diesem Zeitpunkt erarbeiteten verfassungsrechtlichen Analyse und Prognose. Gleichwohl war eine umfassende und vertiefte Auseinandersetzung mit den sehr umfangreichen Entscheidungsgründen erforderlich – nicht zuletzt, um die Verfassungskonformität vorgeschlagener Neuregelungen umfassend abschätzen zu können.

Eine größere Schwierigkeit bestand hingegen darin, dass bei Beginn der Untersuchung in Folge der Umsetzung datenschutzrechtlicher Löschungspflichten evaluationsrelevante Dokumentationen teilweise bereits vernichtet waren.[9] Vor diesem Hintergrund beruhen viele der Einschätzungen in diesem Gutachten auf Aussagen der Beamten des BKA. Um den Erfolg künftiger Evaluationsvorhaben besser zu sichern, dürfte es sich grundsätzlich anbieten, gemeinsam mit Evaluationsklauseln wie Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus die Speicherung anonymisierter Daten für Evaluationszwecke zuzulassen und zu regeln.

---

4 Zum Problem der Datenzugänglichkeit in dieser Untersuchung noch unten A.IV und B.I.1.

5 Im September 2016 wurde an zwei verschiedenen Terminen Akteneinsicht in den Räumlichkeiten des BKA in Berlin genommen.

6 Diese größeren Besprechungen fanden statt beim BKA in Wiesbaden (11/2015), im BMI in Berlin (5/2016) sowie beim BKA in Berlin (6/2016).

7 Die Telefonkonferenzen fanden unter Beteiligung von Mitarbeitern sowohl des BKA als auch des BMI im Juli und im September 2016 statt.

8 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09.

9 Hierzu auch noch unten B.I.1.

Andernfalls droht der Erfolg gerade bei aufwändigen Evaluationsaufgaben, die u.a. ein längeres Ausschreibungsverfahren und ein Einvernehmen des Bundestages erfordern, gefährdet zu werden.

Zusammenfassend lässt sich sagen, dass der Lauf der Untersuchung in diesem Fall durchaus von verschiedenen, teils nicht unerheblichen Herausforderungen geprägt war, die sich aber im Großen und Ganzen gut bewältigen ließen.

B. Darstellung der Ergebnisse

I. Empirische Ausgangssituation

1. Vorbemerkung

Für die Evaluation standen ausschließlich aggregierte Häufigkeitsdaten aus internen Erhebungen des BKA zur Verfügung. Anders als in dem Untersuchungskonzept ursprünglich vorgesehen standen fallbezogene Akten oder Aufzeichnungen lediglich zu einem einzigen Fallkomplex[10] zur Verfügung. Für alle anderen förmlichen Gefahrenabwehrvorgänge waren die Akten und dazugehörige Datenbestände und andere fallbezogene Informationen aufgrund des Eintritts der Löschungsfristen[11] entweder bereits gelöscht oder vernichtet bzw. der Zugang zu noch vorhandenen (Rest-) Beständen gesperrt. Die gesperrten Akten betreffen drei Fallkomplexe, bei denen eine oder mehrere Benachrichtigungen zum Zeitpunkt der Untersuchung noch zurückgestellt waren[12] und die daher aus Gründen der Rechtsschutzsicherung vorgehalten wurden. Eine Ausnahme zum Zwecke der vom Gesetzgeber eigentlich explizit vorgesehenen wissenschaftlichen Evaluation ist gesetzlich nicht vorgesehen. Nach Rechtsauffassung des BKA waren diese Akten daher für die Evaluation nicht einsehbar. Die nachfolgende Darstellung muss sich mithin auf eine deskriptive Auflistung der im Laufe der Verfahren durchgeführten Maßnahmen beschränken. Vertiefte einzelfallbezogene Analysen zur Anwendungspraxis, insbesondere solche zur Bewertung des Erkenntnisgewinns durch die Einzelmaßnahmen, waren daher ebenso wenig möglich wie fallübergreifende Analysen zur Einsatzbreite und Einsatztiefe der Maßnahmen gemäß §§ 20j und 20k BKAG.

Ebenfalls nicht zielführend erschien eine ersatzweise Kontrollabfrage bei dem für die Anordnung der unter Richtervorbehalt stehenden Maßnahmen zuständigen Amtsgericht Wiesbaden nach Duplikaten der relevanten Anträge. Es ist offenbar Praxis, dass die Antragsunterlagen mit Anordnungs- bzw. Ablehnungsvermerk im Original an das BKA zurückgereicht werden. Nach Entscheidung werden bei Gericht keine Kopien gezogen und keine fallbezogenen Unterlagen archiviert. Dies macht eine Ex-post-Kontrolle der Anträge und der Begründungsdichte ebenso unmöglich wie der richterlichen Entscheidungspraxis.

2. Entwicklung der relevanten Sachverhalte im Untersuchungszeitraum

a. Ausgangssachverhalte

Um die praktische Bedeutung der Zuständigkeitsregelung des § 4a BKAG für die Abwehr terroristischer Gefahren bewerten zu können, bedarf es zunächst der quantitativen Erfassung der Grundgesamtheit. Das sind alle Verdachtsfälle, bei denen eine mögliche Zuständigkeit des BKA geprüft wurde.

Die Anzahl der potenziellen Verdachtsfälle – sog. Ausgangssachverhalte – und ihre zeitliche Verteilung ergeben sich aus *Schaubild 1*. Dabei können zwei Phasen unterschieden werden: in den Jahren 2009 bis 2013 war ein stabiles Niveau mit einem jährlichen Fallaufkommen von jeweils ca. 200 Sachverhalten[13] (plus/minus 10) zu verzeichnen. Ab 2013 setzt dann eine signifikante Zunahme ein, und zwar auf zunächst 335 Sachverhalte in 2014 und ca. 500[14] Sachverhalte in 2015. Das ist ein jahresbezogener Anstieg von 57 % (2014) bzw. 49 % (2015).

Insgesamt wurden in dem angegebenen Siebenjahreszeitraum ca. 1.850 Sachverhalte überprüft.

---

[10] Fallkomplex „Komet“; siehe unten B.I.3.b.ii).

[11] § 20v Abs. 6 BKAG.

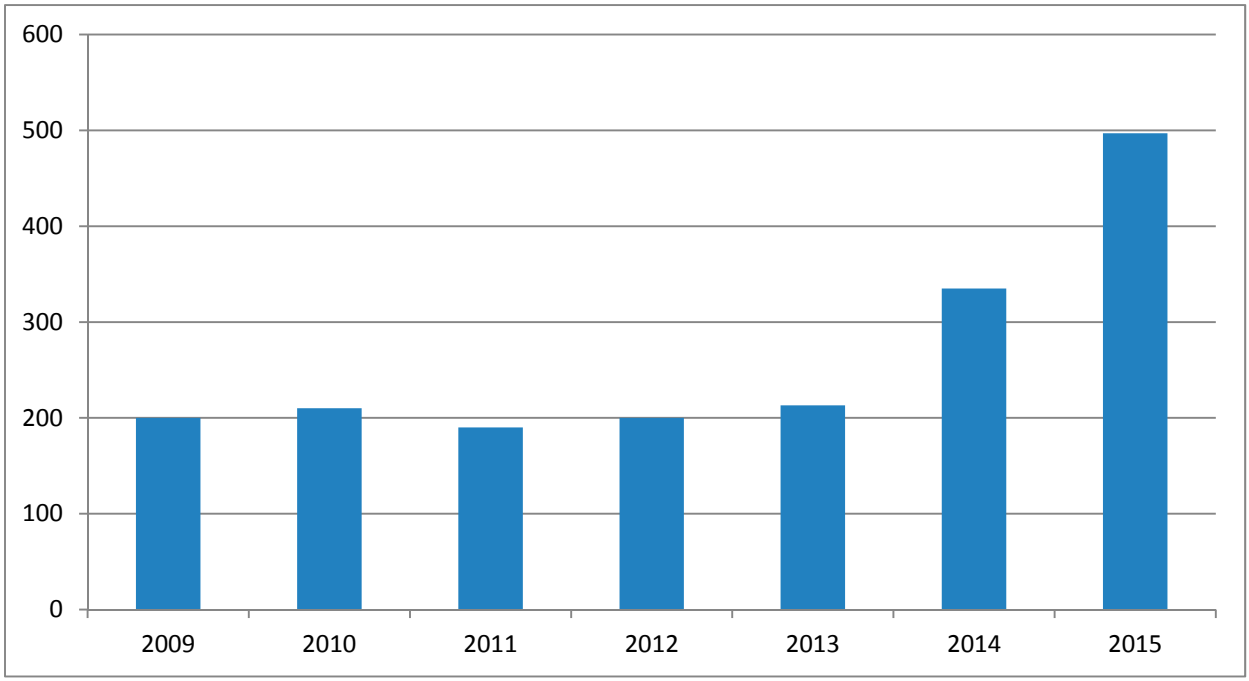
[12] Vgl. unten B.I.2.b.

[13] Summe für die Jahre 2009-2012 jeweils auf 10er-Werte gerundet; 2013: 213 Sachverhalte.

[14] 497 Sachverhalte bis zum Stichtag der Erhebung am 4.12.2015.

Schaubild 1

Anzahl der Ausgangssachverhalte*



* Quelle: BKA (Stand 04.12.2015); Summe für die Jahre 2009-2012 auf 10er gerundet.

b. Förmliche Gefahrenabwehrvorgänge

Aus dieser Grundgesamtheit von potenziellen Verdachtsfällen wurden nach Prüfung durch das BKA 17 förmliche Gefahrenabwehrvorgänge (GAV) generiert, die dann durch das Amt (weiter-) geführt wurden.[15] Dies sind die einschlägigen Fälle gemäß § 4a BKAG, sog. § 4a-Lagen. Von diesen Vorgängen waren bis Ende 2015 16 abgeschlossen. Das ist ein Anteil von 0,9 % der Ausgangssachverhalte. Diese 16 Fallkomplexe werden im Weiteren näher analysiert.

[15] Quelle: Bericht ST 41 vom 26.11.15.

Tabelle 1

Gefahrenabwehrvorgänge gemäß § 4a BKAG:
Sachverhalt, Ursprung (Hinweisgeber) und rechtliche Einordnung*

	Internes Acronym	Fallbeschreibung	Rechtliche Einordnung (§ 4a BKAG)
1.	EG FIMO	Kompensationsgeschäft mit Sprengstoff und Rauschgift	Abs. 1 Satz 1 Nr. 1
2.	EG Reise Pakistan	Aufenthalt in Ausbildungslagern	Abs. 1 Satz 1 Nr. 2 (Satz 2)
3.	EG Levante	Planungen terroristischer Gruppierungen aus dem Libanon	Abs. 1 Satz 1 Nr. 1
4.	EI Bosnien	Mutmaßlicher Anschlag bosnischer Extremisten	Abs. 1 Satz 1 Nr. 3
5.	EG Lampe	Mutmaßliche Anschlagsplanungen/ -vorbereitungen auf jüdische/israelische Einrichtungen	Abs. 1 Satz 1 Nr. 1
6.	EG 400	Mutmaßliche Anschlagsplanungen durch Mitglieder der Fatah al-Islam	Abs. 1 Satz 1 Nr. 1
7.	GAV Nova	Hinweis auf bevorstehende Einreise von fünf mutmaßlichen Attentätern	Abs. 1 Satz 1 Nr. 1 u. 2
8.	EG Komet	Mutmaßliche Anschlagsplanungen	Abs. 1 Satz 1 Nr. 1
9.	EG Poseidon	Mutmaßliche Anschlagsplanungen durch österreichische Gruppierung	Abs. 1 Satz 1 Nr. 1 u. 2
10.	EG Geist	Mutmaßliche Anschlagsplanungen	Abs. 1 Satz 1 Nr. 2
11.	GAV PKK	Mutmaßlicher Selbstmordanschlag durch die PKK	Abs. 1 Satz 1 Nr. 1 u. 2
12.	EG KWAS	Mutmaßliche Vorbereitung und Durchführung eines Terroraktes	Abs. 1 Satz 1 Nr. 1 (Satz 2)
13.	EG Robinson	Potenzielle Gefährdung durch Nutzer einer verdächtigen E-Mail-Adresse	Abs. 1 Satz 1 Nr. 2 (Satz 2)
14.	EG Advent	Möglicherweise geplanter Anschlag durch Anhänger des IS	Abs. 1 Satz 1 Nr. 2
15.	GAV Lacrima	Mögliche Einbindung einer individuellen Person in Anschlagspläne des IS	Abs. 1 Satz 1
16.	GAV Stereo	Mögliche Anschlagspläne einer individuellen Person	Abs. 1 Satz 1

* Im Evaluationszeitraum abgeschlossene Fälle (n = 16); Quelle: interne Erhebung BKA.

In Tabelle 1 sind die Vorgänge zunächst nach ihrem Sachverhalt (nebst internem Fallacronym), dem Ursprung des Verdachts sowie der rechtlichen Einordnung durch das BKA ausgewiesen. Bis auf einen Fall, in dessen Fokus der Aufenthalt in pakistanischen Ausbildungslagern stand, haben alle Verfahrenskomplexe Anschlagsplanungen oder zumindest den Umgang mit Sprengstoff zum Gegenstand. Zwei Komplexe gehen auf eigene Vorermittlungen durch das BKA zurück, vier weitere auf Hinweise deutscher Dienste; die Mehrzahl der Fälle (9 Vorgänge) haben ihren Ursprung in Hinweisen ausländischer Behörden.

Was die rechtliche Grundlage für die Zuständigkeit des BKA betrifft, so gab es in dem genannten Zeitraum lediglich einen einzigen Ersuchensfall gem. § 4a Abs. 1 Nr. 3 BKAG, bei dem eine Landespolizei um die Übernahme des Falles ersucht hat. In sechs Fällen hat das BKA die eigene Zuständigkeit mit dem Vorliegen einer länderübergreifenden Gefahr begründet (§ 4a Abs. 1 Nr. 1) sowie ebenfalls in sechs Fällen auch oder ausschließlich mit der Nichterkennbarkeit einer expliziten Landeszuständigkeit (§ 4a Abs. 1 Nr. 2). In drei Fällen wurde ergänzend die Situation des § 4a Abs. 1 Satz 2 (Verhütung einer schweren terroristischen Straftat) mit bejaht. Dabei handelt es sich jeweils um die rechtliche Bewertung des BKA. In den beiden letzten Fällen wurde die Zuständigkeit lediglich mit einem undifferenzierten Verweis auf § 4a Abs. 1 Satz 1 begründet.

Tabelle 2

Anzahl betroffener Personen

	Internes Acronym	**Potenzielle Gefahrenverursacher***	**Mitbetroffene Personen****	**Insgesamt**
1.	EG FIMO	unbekannt	unbekannt	unbekannt
2.	EG Reise Pakistan	13	54	67
3.	EG Levante	28	268	296
4.	EI Bosnien	3	612	615
5.	EG Lampe	6	184	190
6.	EG 400	3	110	113
7.	GAV Nova	2	0	2
8.	EG Komet	9	136	145
9.	EG Poseidon	4	0	4
10.	EG Geist	2	5	7
11.	GAV PKK	5	223	228
12.	EG KWAS	1	20	21
13.	EG Robinson	1	0	1
14.	EG Advent	4	9	13
15.	GAV Lacrima	4	noch offen***	noch offen***
16.	GAV Stereo	1	noch offen***	noch offen***
	Insgesamt	(mind.) **86**	(mind.) **1.621**	(mind.) **1.702**

* Siehe hierzu auch Fußnote 17.

** Soweit sie in den Kreis der gem. § 20w Abs. 1 BKAG zu benachrichtigenden Personen fallen;

*** zum Zeitpunkt der Erhebung; Quelle: interne Erhebung BKA.

Tabelle 2 weist die Zahl der durch die eingeleiteten Maßnahmen insgesamt betroffenen Personen aus und gibt damit einen gewissen Anhaltpunkt zu der Eingriffsbreite der Maßnahmen. Als mitbetroffen definiert bzw. erfasst wurden alle Personen, die in den Kreis der gem. § 20w Abs. 1 BKAG zu benachrichtigenden Personen[16] fallen.

[16] Die konkrete Zusammensetzung des relevanten Personenkreises unterscheidet sich je nach Einzelmaßnahme, vgl. § 20w Abs. 1 Nr. 1 bis 10 BKAG.

Im Einzelnen ergibt sich, dass ca. 86 Personen als potenzielle Gefahrenverursacher[17] unmittelbare Zielpersonen der zur Gefahrenabklärung eingesetzten verdeckten Ermittlungsmaßnahmen waren; das sind im Durchschnitt 5,4 direkt Betroffene pro Vorgang. Weitaus größer war daneben der Kreis der indirekt mitbetroffenen Personen. Ihre Anzahl summiert sich auf mindestens 1.621; das ergibt eine durchschnittliche Streubreite auf ca. 101 mutmaßlich unbeteiligte Dritte pro Fallkomplex. Nur in drei Fällen waren keine unbeteiligten Personen von den Maßnahmen betroffen; in allen anderen Verfahrenskomplexen war dies hingegen der Fall; dabei lag deren konkrete Anzahl stets höher als diejenige der unmittelbaren Zielpersonen. Die höchste Anzahl mitbetroffener Dritter beträgt 612, in fünf weiteren Fällen lag sie ebenfalls im – niedrigeren – dreistelligen Bereich, und lediglich in zwei Fällen waren es weniger als 10. Alle Angaben beziehen sich auf bekannte Betroffene bzw. Mitbetroffene; in drei Fällen war die konkrete Anzahl einer oder beider Gruppen (noch) offen. Beide Gruppen zusammen summieren sich auf (mindestens) 1.702.

Tatsächlich benachrichtigt wurden während des Untersuchungszeitraumes insgesamt 100 Personen. Lediglich in einem Fall („EG Geist“) wurden alle Betroffenen benachrichtigt. Die Gründe für die Nichtbenachrichtigung wurden dokumentiert. Im Fall 14 wurden alle 13 Benachrichtigung gem. § 20w Abs. 3 Satz 1 BKAG um ein Jahr zurückgestellt, in den Fällen Nr. 2 und 5 wurden insgesamt 14 Benachrichtigungen mit Genehmigung des AG Wiesbaden um 4 bzw. 5 Jahre zurückgestellt. Alle weiteren Benachrichtigungen sind auf der Grundlage von § 20w Abs. 1 Satz 2, 3 oder 4 BKAG unterblieben.

In *Tabelle 3* sind die jeweiligen zeitlichen Parameter sowie die Gesamtdauer der einschlägigen Verfahren nach Kalendertagen ausgewiesen. Die Informationen über die Verfahrensdauer können dabei zunächst ein Indiz für die Komplexität der Ermittlungsarbeit sein. Darüber hinaus lassen sie, zumindest indirekt auf einer aggregierten Ebene, auch Rückschlüsse auf die mit den begleitenden verdeckten Ermittlungsmaßnahmen verbundene Überwachungsdauer zu. Diese kann man individuell oder kumulativ[18] bewerten.

Zunächst wird erkennbar, dass sich in der Verteilung der Ermittlungskomplexe über die Kalenderjahre der eingangs dargestellte Anstieg der Ausgangssachverhalte seit 2014[19] hier nicht wiederspiegelt. Die höhere Anzahl von Prüfvorgängen hat mithin nicht in einer Zunahme der § 4a-Lagen geführt. Tendenziell ist sogar eher das Gegenteil festzustellen: während in den Jahren 2009 und 2010 jeweils vier förmliche GAV eingeleitet wurden, waren es in den Folgejahren lediglich einer (2012 und 2014) bzw. zwei (2013). Die Auflistung für 2015 ist nicht abschließend, da wie erwähnt nur die beiden zum Untersuchungszeitpunkt abgeschlossenen Vorgänge einbezogen wurden; mindestens ein weiterer Vorgang[20] ist dokumentiert.

---

[17] Das sind nicht notwendigerweise Gefährder im Sinne der polizeilichen Gefährderdefinition: „Ein Gefährder ist eine Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche im Sinne des § 100a der Strafprozessordnung (StPO), begehen wird“, Arbeitsgemeinschaft der Leiter der Landeskriminalämter und des Bundeskriminalamtes (AG Kripo) (2004), zitiert nach Wissenschaftliche Dienste des Deutschen Bundestages Nr. 36/08 vom 23.7.2008.

[18] Roßnagel, NJW 2010, 1238, spricht bildlich von „Überwachungs-Gesamtrechnung“.

[19] Siehe oben Schaubild 1.

[20] Der eingangs erwähnte 17. Fall.

Tabelle 3

Dauer der Verfahren gemäß § 4a BKAG

	Internes Acronym	**Verfahrensbeginn**	**Verfahrensende**	**Dauer***
1.	EG FIMO	13.02.09	11.05.09	119
2.	EG Reise Pakistan	14.05.09	16.10.09	156
3.	EG Levante	27.07.09	15.10.09	81
4.	EI Bosnien	03.09.09	25.09.09	23
5.	EG Lampe	11.02.10	22.03.10	40
6.	EG 400	11.03.10	30.03.10	21
7.	GAV Nova	08.11.10	31.03.11	150
8.	EG Komet	19.11.10	07.09.11	300
9.	EG Poseidon	10.06.11	13.02.12	254
10.	EG Geist	07.07.11	16.04.12	289
11.	GAV PKK	02.10.12	28.02.13	147
12.	EG KWAS	24.05.13	02.08.13	70
13.	EG Robinson	26.07.13	31.10.13	98
14.	EG Advent	12.12.14	05.05.15	144
15.	GAV Lacrima	12.02.15	29.01.16	352
16.	GAV Stereo	11.10.15	29.01.16	115

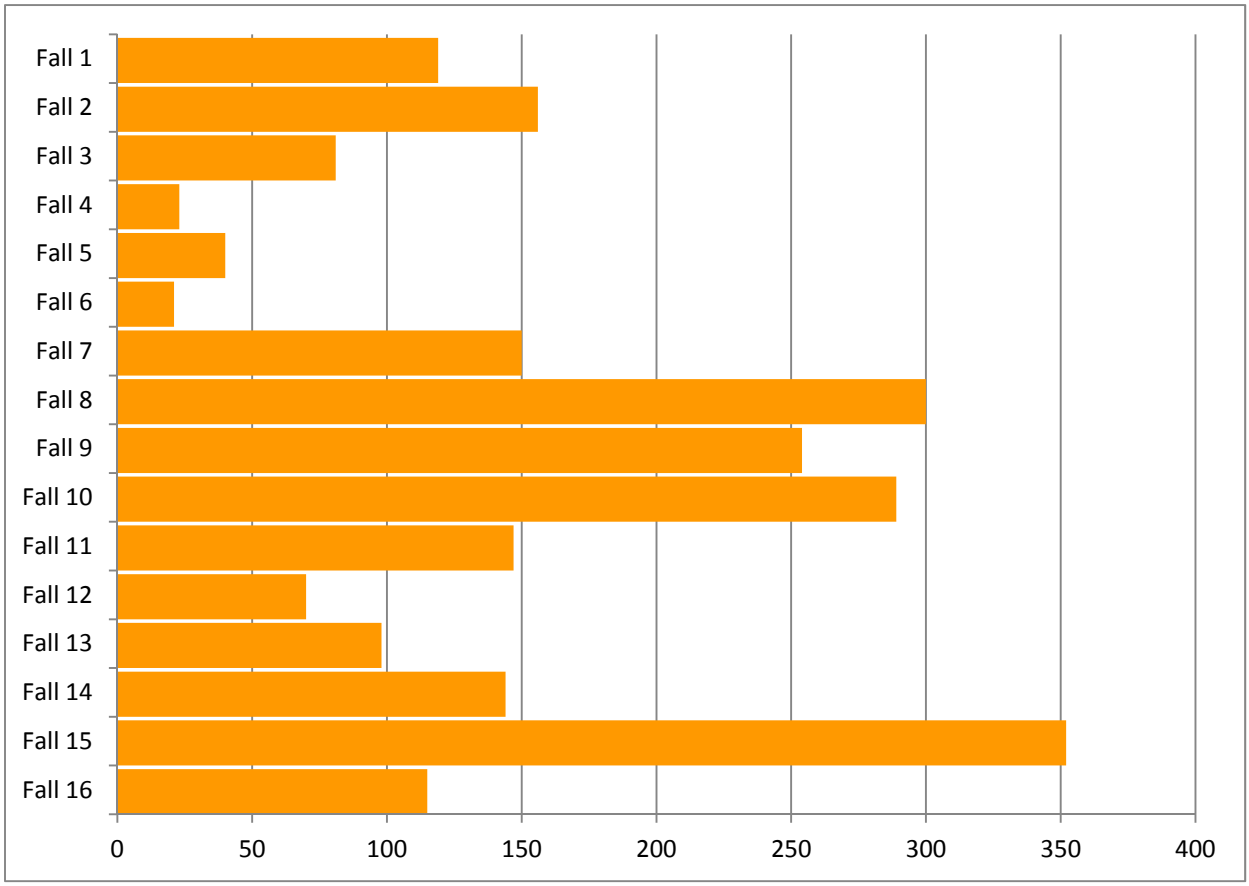
* Dauer in Kalendertagen, siehe auch Schaubild 2; Quelle: interne Erhebung BKA.

Auf die einzelnen Verfahren bezogen zeigt sich dann ein sehr uneinheitliches Bild. In jeweils drei Fällen dauerte das Verfahren weniger als 50 Tage bzw. weniger als 100 Tage. In fünf Verfahren dauerten die Ermittlungen bis zu 150 Tage, und in weiteren 4 Fallkomplexen noch einmal deutlich länger, davon in zweien annähernd doppelt so lange (289 bzw. 300 Tage). Das längste Verfahren zog sich über fast ein ganzes Jahr hin (Fall Nr. 15: 352 Tage). Die Verfahrensdauern werden in Schaubild 2 auch ergänzend visualisiert.

Die zeitliche Dauer eines Verfahrens und die Ermittlungsintensität, soweit sie sich in der Anzahl der durchgeführten Einzelmaßnahmen manifestiert, stehen im Übrigen nicht unbedingt in Relation. So kamen in den drei Fällen mit der kürzesten Verfahrensdauer (Nr. 4, 5 und 6) jeweils mehrere Dutzend Maßnahmen zur Anwendung; hingegen wurde in dem Fallkomplex „Poseidon“ (Nr. 9), der sich über einen Zeitraum von gut 10 Monate erstreckte, keine einzige verdeckte Ermittlungsmaßnahme registriert (siehe Tabelle 5). Die einzelnen Maßnahmen werden im nachfolgenden Unterabschnitt näher dargestellt.

Schaubild 2

Verfahrensdauer in Tagen



* Kalendertage; zu den genauen Zeitangaben vgl. Tabelle 3; Quelle: interne Erhebung BKA.

3. Konkrete Maßnahmen

a. Überblick über das Maßnahmenspektrum insgesamt

Alle in den relevanten Gefahrenabwehrvorgängen zum Einsatz gebrachten verdeckten Ermittlungsmaßnahmen gem. §§ 20a ff. BKAG sind in *Tabelle 4* umfassend aufgelistet. Sie sind den jeweiligen Verfahrenskomplexen zugeordnet. Aussagen zu deren zeitlicher Abfolge können nicht getroffen werden, da die hierfür erforderlichen Fallakten wie erwähnt nicht (mehr) zugänglich waren. Dasselbe gilt für die ursprünglich geplanten Analysen zu möglichen kriminalistischen Zusammenhängen und Interdependenzen zwischen den einzelnen Maßnahmen und deren finalem Ertrag (aus Ermittler-) und möglichen Konsequenzen (aus Betroffenensicht).

Tabelle 4

Übersicht über alle eingesetzten verdeckten Ermittlungsmaßnahmen gemäß BKAG

	Verdeckte Ermittlungsmaßnahmen:												
Fall Nr.	**§ 20g Abs. 2 Nr. 1**	**§ 20g Abs. 2 Nr. 2**	**§ 20g Abs. 2 Nr. 3**	**§ 20g Abs. 2 Nr. 4**	**§ 20h**	**§ 20i**	**§ 20j**	**§ 20k**	**§ 20l Abs. 1**	**§ 20l Abs. 2**	**§ 20m**	**§ 20n**	**Insg.**
1.	0	0	0	0	0	0	**0**	**0**	5	0	3	0	**8**
2.	1	1	0	0	0	13	**0**	**0**	7	0	7	1	**30**
3.	1	1	0	0	0	28	**0**	**0**	9	0	9	0	**48**
4.	0	0	0	0	0	6	**0**	**0**	20	0	20	1	**47**
5.	6	2	6	0	0	4	**0**	**0**	40	1	7	1	**67**
6.	1	0	1	0	0	4	**0**	**0**	16	0	12	1	**35**
7.	0	0	0	0	0	0	**0**	**0**	4	0	4	0	**8**
8.	15	4	4	2	1	1	**0**	**5**	187	6	188	5	**426**
9.	0	0	0	0	0	0	**0**	**0**	0	0	0	0	**0**
10.	1	1	0	0	2	0	**0**	**0**	0	0	1	0	**5**
11.	5	5	5	0	0	5	**0**	**0**	3	0	3	4	**30**
12.	1	1	0	0	0	0	**0**	**0**	18	0	0	1	**21**
13.	0	0	0	0	0	0	**0**	**0**	1	0	5	0	**6**
14.	2	2	2	0	0	2	**1**	**0**	21	0	21	1	**52**
15.	4	2	4	2	1	0	**0**	**0**	66	0	34	3	**116**
16.	0	0	0	0	0	0	**0**	**0**	0	0	0	0	**0**
Insg.	**37**	**19**	**22**	**4**	**4**	**63**	**1**	**5**	**397**	**7**	**322**	**18**	**899**

***** Quelle: interne Erhebung BKA;

§ 20g Abs. 2 Nr. 1 BKAG = Längerfristige Observation; § 20g Abs. 2 Nr. 2 = Bildaufnahmen/akustische Überwachung außerhalb Wohnung; § 20g Abs. 2 Nr. 3 = Observation mir sonstigen techn. Mitteln; § 20g Abs. 2 Nr. 4 = VP-Einsatz; § 20g Abs. 2 Nr. 5 = VP-Einsatz m. Richtervorbehalt (keine Anwendung); § 20h = Wohnraumüberwachung; § 20i = Ausschreibung zur polizeiliche Beobachtung; **§ 20j = Rasterfahndung**; **§ 20k = Online-Durchsuchung**; § 20l Abs. 1 = TKÜ; § 20l Abs. 2 = Quellen-TKÜ; § 20m = Verkehrsdatenerhebung; § 20n = IMSI-Catcher.

Insgesamt kamen in den 16 § 4a-Verfahren n=899 verdeckte Ermittlungsmaßnahmen zum Einsatz. Das ergibt einen Durchschnittswert von 56 Einzelmaßnahmen pro Fall. Mit Ausnahme von 2 Fallkomplexen ohne einschlägige Maßnahmen (Nr. 9 und 16) kamen in allen Verfahren auch mehrere Instrumente gebündelt zum Einsatz. Am überwachungsintensivsten war dabei der Fallkomplex Nr. 8 („Komet“) mit einer Gesamtzahl von 426 verdeckten Einzelmaßnahmen. Hervor sticht auch Fall Nr. 15, in dem ebenfalls mehr als 100 individuelle Maßnahmen zum Einsatz kamen (n=116). Insgesamt wurden in der Hälfte aller Verfahren 30 und mehr Anwendungen gezählt (Maximum 67).

Über das gesamte Einsatzspektrum kamen mit Ausnahme des § 20g Abs. 2 Nr. 5 BKAG auch sämtliche gesetzlich vorgesehenen Maßnahmen zur Anwendung, und zwar in deutlich unterschiedlicher Häufigkeit. Am seltensten wurde die Rasterfahndung durchgeführt, mit gerade einem Einsatz, am häufigsten die TKÜ mit 397 sowie die Verkehrsdatenüberwachung mit 323 Anwendungen. Anders als im repressiven Bereich steht dabei die TKÜ in der Variante der Inhaltsüberwachung an der Spitze. Dies ist auch plausibel erklärbar, da die individuelle und inhaltsbezogene Informationsgewinnung hier herausragende Bedeutung hat, etwa bei der Gefahrenabschätzung.

Die funktionale Informationsgewinnung, etwa zur Feststellung von interpersonalen Beziehungen, die typischerweise bereits aus kommunikationsbezogenen Metadaten generiert werden können und für die eine Inhaltüberwachung daher nicht stets erforderlich wäre, hat quantitativ zwar ebenfalls eine beachtliche Bedeutung, erscheint aber nicht so dominant wie im strafprozessualen Einsatzbereich.[21] Auffallend ist darüber hinaus, dass in den hier analysierten Fällen keine einzige Funkzellenabfrage erfolgte. Annähernd die Hälfte aller TKÜ-Maßnahmen sowie fast 60 Prozent aller Verkehrsdatenabfragen gehen auf das Konto eines einzigen Falles (Nr. 8). In fünf weiteren Fällen dominieren ebenfalls TKÜ-Maßnahmen, wenn auch auf deutlich niedrigerem Niveau. Daneben gab es überhaupt nur drei Vorgänge, in denen keine Telefone abgehört wurden.

Recht bedeutsam erscheint in der Anwendungspraxis mit insgesamt 63 Einsätzen auch die Maßnahme gemäß § 20i BKAG (Ausschreibung zur polizeilichen Beobachtung), gefolgt von der längerfristigen Observation (§ 20g Abs. 2 Nr. 1), die insgesamt 37 mal zum Einsatz kam. Fast die Hälfte dieser Einsätze erfolgte ebenfalls in Fall Nr. 8 („Komet"), der im Untersuchungszeitraum insgesamt das ermittlungsintensivste GAV gewesen ist. Es ist denn auch der einzige Ermittlungskomplex, in dem die Online-Durchsuchung zur Anwendung kam. Es ist auch derjenige Gefahrenabwehrvorgang mit der zweitlängsten Dauer und dem größten Aufwand, was den Einsatz sehr vieler ganz verschiedener verdeckter Ermittlungsmaßnahmen und der damit verbundenen Ressourcen betrifft. Die auffallend hohe Anzahl an Zugriffen auf Verkehrsdaten ist dabei sicherlich auch im Zusammenhang mit der technischen Vorbereitung der Online-Durchsuchungen zu sehen. Auf diesem Fall basieren auch die wesentlichen Ausführungen und Schlussfolgerungen zur Praxis der Online-Durchsuchung in dem rechtlichen Teil des Gutachtens. Der Fall mündete zwischenzeitlich auch in ein Strafverfahren.

Die Übersicht zeigt schließlich auch, dass die beiden hier zur Beurteilung stehenden Maßnahmen, Rasterfahndung und Online-Durchsuchung, eindeutig nicht zu den 'Standard'-Maßnahmen zählen. Ihr Einsatz wird abschließend dargestellt.

b. Maßnahmen gemäß § 20j und § 20k BKAG

i) Rasterfahndung

Die Rasterfahndung gem. § 20j BKAG dient der Ermittlung und Identifikation von potenziellen (weiteren) Gefährdern.[22] Sie kam lediglich in einem Fallkomplex zur Anwendung (Fall Nr. 14: „Advent"). Da die Akten zu diesem Fall gesperrt sind, war eine Auswertung der diesbezüglichen Aufzeichnungen nicht möglich. Die Ausführungen im dogmatischen Teil stützen sich insofern auf Auskünfte des BKA zu diesem Fall.[23]

ii) Online-Durchsuchung

Der verdeckte Zugriff auf informationstechnische Systeme gem. § 20k BKAG („Online-Durchsuchung") soll den Sicherheitsbehörden die Möglichkeit geben, auf die gespeicherten Inhalte auf Computern potenzieller Gefährder zugreifen zu können.[24] Hierfür muss eine individuell produzierte und programmierte Software („Trojaner") in dem Zielsystem platziert werden. Die Maßnahme ist erfolgreich, wenn es – der programmierten Funktionalität der installierten Spähsoftware entsprechend – tatsächlich zu der Ausleitung und Übermittlung von Daten aus dem Zielsystem kommt. Ziel der Maßnahme ist vorrangig die Gefahrerforschung mit dem Ziel, Fallkonstellationen aufzuklären, bei denen bereits Tatsachen die Annahme rechtfertigen, dass (terroristische) Straftaten i. S. d. § 4a Abs. 1 Satz 2 BKAG begangen werden könnten.[25]

---

[21] Hierzu ausführlicher Albrecht/Grafe/Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO (2008) = Bundestagsdrucksache 16/8434, sowie Albrecht et al., Schutzlücken durch den Wegfall der Vorratsdatenspeicherung? (2011), www.mpg.de/5000721/vorratsdatenspeicherung.pdf.

[22] Siehe auch B.II.2.a.

[23] Siehe unter B.II.2.c.

[24] Siehe auch B.II.3.a.

[25] Siehe auch B.II.3.b.ii).

Tabelle 5

Einsatz der Online-Durchsuchung gemäß § 20k BKAG[26]

Jahr	Angeordnet	Software aufgespielt	Anzahl der Zielsysteme	Daten ausgeleitet	Dauer*
2009	0	0	0	0	–
2010	4	3	3	2	15
2011	1***	1	1	0	71**
2012	0	0	0	0	–
2013	0	0	0	0	–
2014	0	0	0	0	–
Insgesamt	**5*****	**4**	**4**	**2**	**86**

* Dauer der aktiven Funktion (Datenausleitung) in Kalendertagen;

** davon 28 Einsatztage ab Jahresbeginn 2011 auf der Grundlage des Ursprungsbeschlusses sowie 43 weitere unmittelbar anschließend nach Verlängerungsbeschluss des AG Wiesbaden;

*** zuzüglich 2 Verlängerungsbeschlüsse in 2011; Quelle: interne Erhebung BKA.

Alle durchgeführten Einsätze (einschließlich der Einsatzversuche) der Online-Durchsuchung[27] beziehen sich auf den Fall Nr. 8 („Komet“), in dessen Fokus 9 Personen als potenzielle Verdächtige[28] standen. Insgesamt wurden Einsätze gegen fünf konkrete Zielpersonen vorbereitet, beantragt und gerichtlich angeordnet, davon vier im Jahr 2010 und einer in 2011. In drei dieser vier Einsatzfälle aus 2010 sind die Maßnahmen dann weiter bis in das Stadium des Aufspielens der Spähsoftware in die Zielsysteme gelangt, darunter in einem Fall bezogen auf 2 Zielsysteme ein und derselben Person. Auch in dem weiteren Einsatz im Jahr 2011 ist das Aufspielen gelungen, sodass im Evaluationszeitraum insgesamt vier Geräte (Zielsysteme) zeitweise mit der Spähsoftware bestückt waren.

Am Ende kam es dann lediglich in einem Fall tatsächlich auch zum erfolgreichen Abschluss der Maßnahme, d.h. zur konkreten Datenausleitung aus beiden präparierten Zielsystemen (ein PC und ein Notebook). Auf der Grundlage einer rechtzeitig erwirkten Verlängerungsanordnung war die Ausleitungsfunktion bis zur Deaktivierung im März 2011 über einen Zeitraum von insgesamt 86 Tagen aktiv, davon 15 Tage in 2010. Im Hinblick auf die effektive Verfahrensdauer – der Fall wurde erst seit dem 19. November 2010 als GAV geführt[29] – haben die Vorbereitung und der Einsatz der Online-Durchsuchung zu einem recht frühen Zeitpunkt begonnen.

4. Verhältnis zwischen empirischer und dogmatisch-legistischer Analyse

Auf dieser empirischen Grundlage setzt die folgende rechtsdogmatische und legistische Analyse auf. Wie sich auch im Laufe der Untersuchung gezeigt hat, lassen sich die empirischen und normativen Komponenten nicht trennen, sondern sind vielfach verschränkt.[30] Dementsprechend wurde auch für die folgende Darstellung der Ergebnisse der Weg gewählt, die Erkenntnisse aus der empirischen Analyse jeweils dort und punktuell anzuführen, wo sie für die Formulierung dogmatischer und legistischer Einschätzungen und Empfehlungen relevant werden.

---

26 Gemäß Forschungsauftrag wurden nur Maßnahmen für den Zeitraum 2009 bis 2014 dokumentiert.

27 Siehe oben Tabelle 4.

28 Siehe oben Tabelle 2.

29 Siebe oben Tabelle 3.

30 Siehe oben A.III.

II. Rechtsdogmatische und legistische Analyse

Die folgende rechtliche Einschätzung der §§ 4a, 20j und 20k BKAG ist nach den einzelnen Normen aufgeschlüsselt. Dies entspricht auch der Struktur der Kommunikation des Evaluationsteams mit BMI und BKA während der laufenden Untersuchung.

Wie bereits angesprochen galt es zunächst zu klären, wie der genaue Gegenstand und Umfang der Untersuchung zu bestimmen waren. Da Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus den Evaluationsauftrag ausdrücklich auf die §§ 4a, 20j und 20k BKAG begrenzt, wurde insofern ein restriktiver Ansatz verfolgt. Es werden also lediglich solche Aspekte berücksichtigt, die in einem spezifischen und untrennbaren Zusammenhang mit den §§ 4a, 20j oder 20k BKAG stehen. Eine vertiefte oder gar gesonderte Untersuchung der allgemeinen Vorschriften zur Datenspeicherung, -löschung, -weitergabe usw. (vor allem §§ 20v ff. BKAG) hat nicht stattgefunden.[31] Dafür wurden die legistischen Implikationen der Analysen der Regelungen für die Systematik des BKAG mit in den Blick genommen.

1. § 4a BKAG

a. Hintergrund und Ziele der Norm

Die Bündelung von Kompetenzen zur Abwehr von Gefahren des internationalen Terrorismus beim BKA ist als Reaktion auf die in den letzten Jahren beständig zunehmende Bedrohungslage durch global operierende terroristische Gruppierungen und Gefährder einzuordnen. Der internationale Terrorismus entwickelt sich zu einem zunehmend amorphen und diffusen Phänomen. Das bedeutet auch, dass sich Anschlagspläne, -abläufe, -orte oft erst in fortgeschrittenen Szenarien oder sehr spontan konkretisieren. Daher werden Probleme bei der Ermittlung polizeilicher Zuständigkeiten wahrscheinlicher. Insbesondere drohte vor der Verabschiedung von Art. 73 Abs. 1 Nr. 9a GG bzw. dem darauf beruhenden § 4a BKAG eine Zuständigkeitslücke, wenn einerseits der Verdacht noch nicht strafprozessual relevant erhärtet war (in welchem Falle regelmäßig der Generalbundesanwalt zuständig wäre) und sich andererseits noch keine Zuständigkeit einer Landespolizeistelle bestimmen ließ.[32] Auf diese Situation hat der Gesetzgeber mit § 4a BKAG reagiert und die Zuständigkeit zur Abwehr von Gefahren des internationalen Terrorismus auf Bundesebene verankert. Das BKA erhielt damit erstmals in weitem Umfang Gefahrenabwehrbefugnisse.[33]

b. Verfassungskonformität

§ 4a BKAG beruht auf dem exklusiven Bundeskompetenztitel des Art. 73 Abs. 1 Nr. 9a GG. Das BVerfG hat am 20. April 2016 die Verfassungskonformität von § 4a BKAG zu Recht bestätigt,[34] da die Norm im Wesentlichen lediglich die Kompetenzvorschrift des Art. 73 Abs. 1 Nr. 9a GG im einfachen Recht abbildet. Das BVerfG hat dabei auch klargestellt, dass Art. 73 Abs. 1 Nr. 9a GG auch die Kompetenz zur vorbeugenden Verhütung von Straftaten miterfasst.[35] Dies ist zutreffend, da jedenfalls im kompetenzrechtlichen Sinn auch die Straftatenverhütung Teil der Gefahrenabwehr ist.

c. Normanwendung

i) Institutioneller Anwendungsrahmen

Zur praktischen Handhabung von § 4a BKAG wurden in den Gefährdungsreferaten ST 33 und ST 44 des BKA Bewertungsstellen für die Einordnung und Begleitung von Vorgängen nach § 4a BKAG eingerichtet. Bei Vorliegen eines Gefährdungshinweises wird dort zum einen eine Gefährdungsbewertung erstellt, zum anderen wird der Sachverhalt gemäß den tatbestandlichen Voraussetzungen des § 4a Abs. 1 BKAG auf eine Zuständigkeit

---

31 Siehe bereits oben A.IV und B.I.2.b.

32 Zum Verhältnis von BKA und Generalbundesanwalt vgl. auch Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Berlin 2009, S. 60 ff.

33 Davor war das BKA vor allem als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und als Strafverfolgungsbehörde zuständig; hierzu und zur Entstehungsgeschichte von § 4a BKAG s. auch Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Berlin 2009, S. 17 ff.

34 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 88 f.

35 Siehe BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 88. Dies wurde in den gegen § 4a BKAG gerichteten Verfassungsbeschwerden teilweise bezweifelt.

des BKA geprüft. Wie gesehen resultierten im Untersuchungszeitraum aus ca 1.850 überprüften Sachverhalten 17 förmliche Gefahrenabwehrvorgänge nach § 4a BKAG (§ 4a-Lagen).[36]

ii) Auslegungsfragen

Ungeachtet der grundsätzlichen Verfassungskonformität von § 4a BKAG stellen sich in der Anwendungspraxis der Norm einige nicht unwesentliche Auslegungsfragen. Zumindest die Begriffe des „internationalen Terrorismus“ und der „länderübergreifenden Gefahr“ bedürfen einer Präzisierung, die ihre Handhabung auch in schwierigen Fällen anleiten kann. Der Rekurs auf den Gefahrenbegriff als solchen verweist darüber hinaus auf die Frage, wie weit die neue Aufgabe des BKA reicht und inwieweit Vorfeldmaßnahmen grundsätzlich vorgesehen sind (auch wenn die einzelnen Eingriffsbefugnisse dann an höhere Schwellen geknüpft sind).

(1) „Internationaler Terrorismus”

§ 4a Abs. 1 BKAG erweitert die Zuständigkeit des BKA auf Fälle des „internationalen Terrorismus“. Eine ausdrückliche und direkte Terrorismusdefinition enthält das BKAG dabei nicht. Über § 20a Abs. 2 i. V. m. § 4a Abs. 1 S. 2 BKAG wird Terrorismus lediglich indirekt beschrieben. Gegenstand der Definition ist weder der Terrorismus als Gesamtphänomen noch „Gefahren des internationalen Terrorismus“ in ihrer Gesamtheit. Vielmehr wird allein im Rahmen der ergänzenden Kompetenz zur Straftatenverhütung näher beschrieben, welche Art von Straftaten verhütet werden dürfen – namentlich solche, „die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können.“ Die Terminologie ist insofern an gängige, etwa in EU-Richtlinien oder UN-Resolutionen verwendete Formulierungen angelehnt.[37] Vom BVerfG wurde die gewählte Definition aus verfassungsrechtlicher Sicht wie erwähnt nicht beanstandet.[38]

Legistisch und mit Blick auf die Handhabbarkeit der Norm in der Anwendungspraxis ist zunächst zu kritisieren, dass die Terrorismusdefinition indirekt, gleichsam „versteckt“ geraten ist. Dadurch wird schon ihr Anspruch unklar. Denn erst vor dem Hintergrund der Inbezugnahme in § 20a Abs. 2 BKAG wird deutlich, dass hier allgemein beschrieben werden soll, was für die Zwecke des BKAG unter internationalem Terrorismus zu verstehen ist.[39] Dann ist aber nicht verständlich, weshalb die Definition nicht eindeutiger auf die neue Aufgabenzuweisung (Abwehr von Gefahren des internationalen Terrorismus) in ihrer Gesamtheit ausgerichtet ist, sondern erst im Rahmen der dieser grundsätzlichen Aufgabenbeschreibung (§ 4a Abs. 1 Satz 1 BKAG) nachgelagerten Frage der Straftaten-verhütung (§ 4a Abs. 1 Satz 2 BKAG) geregelt wurde. Schließlich war auch in der untersuchten Anwendungspraxis lediglich in drei von 17 förmlichen Gefahrenabwehrvorgängen die Straftatenverhütung einschlägig.[40] Regelungsklarer erschiene es demgegenüber, den Begriff des Terrorismus oder der Gefahren des Terrorismus zunächst als solchen zu definieren und dann in einem zweiten Schritt klarzustellen, dass die Kompetenz zur Abwehr solcher Gefahren auch die Straftatenverhütung umfassen soll.

In der Sache bedürfte es keiner grundsätzlichen Änderungen der gewählten Definition, zumal diese wie gesehen an etablierte internationale Formulierungen anknüpft und auch vom BVerfG nicht beanstandet wurde. Auch im BKA geht man davon aus, den Begriff weitgehend problemlos handhaben zu können. Dort war man bislang allerdings auch regelmäßig mit paradigmatischen Fällen konfrontiert.[41] Zur Konkretisierung und Subsumtion orientiert man sich in der Praxis des BKA an EU- und UN-“Terrorlisten“ – wenn die dort genannten Personen oder Gruppen an einem Vorgang beteiligt sind, kann dies als Indiz für eine Zuordnung der befürchteten Straftat zum Internationalen Terrorismus gewertet werden. Zusätzlich greift das BKA auf eigene Erkenntnisse und

---

36 Siehe oben B.I.2.b.

37 Vgl. Art. 1 Abs. 1 des Rahmenbeschlusses 2002/475/JI des Rates vom 13. Juni 2002, auf den etwa Art. 1 Abs. 4 der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates Bezug nimmt. Vgl. auch die Resolution Nr. 1566 des UN-Sicherheitsrats (2004).

38 Siehe oben B.II.1.b.

39 Diese Lesart liegt auch eingedenk der großen Ähnlichkeit zu den entsprechenden Formulierungen in EU- und UN-Texten nahe, die ja ebenfalls einen umfassenderen Anspruch haben; hierzu oben Fn. 37. Die Regierungsbegründung des Gesetzes ist insofern unergiebig, vgl. Bundestgasdrucksache 16/10121, S. 20 f.

40 Siehe oben B.I.2.b.

41 Überwiegend ging es um islamistischen Terrorismus (unterschiedlicher geografischer Provenienz), siehe oben Tabelle 1 unter B.I.2.b.

Beobachtungen bestimmter Gruppen im Rahmen seiner Zentralstellenfunktion sowie auf Gutachten des BND zurück. Ergänzend werden in einigen Fällen Verfolgungsermächtigungen nach den §§ 89a, 129b StGB herangezogen.[42] All diesen Hilfen kommt aber lediglich indizielle Bedeutung zu. Entscheidend ist in der Praxis letztlich die Subsumtion des im jeweiligen Einzelfall ermittelnden Amtswalters des BKA.

Es ergeben sich allerdings auch dann noch potentiell gewichtige Auslegungsschwierigkeiten jedenfalls unter zwei Aspekten. So ist erstens fraglich, welcher Grad an Internationalität erforderlich ist, um einen Einzelfall dem „internationalen Terrorismus" zuzuordnen (unten (a)). Zweitens kann es im Einzelfall Schwierigkeiten bereiten, Personen oder Gruppen als terroristisch einzuordnen, soweit sie nämlich zwar gegen den Bestand von Staaten gerichtet sind, die politische Führung der Bundesrepublik sich aber gleichwohl dazu entschließt, (wenn auch nur teilweise, diffuse oder vorübergehende) Bündnisse mit solchen Personen oder Gruppen einzugehen (unten (b)).

(a) Internationalität

Die Verlagerung der Gefahrenabwehrzuständigkeit auf die Ebene des BKA reagiert wie gesehen auf die zunehmende Internationalität, Diffusität und Amorphität terroristischer Phänomene. Dies wird in § 4a BKAG mit dem Begriff des „internationalen Terrorismus" einzufangen versucht. Fraglich wird dadurch zunächst, welches Maß an Internationalität, d. h. an globaler Vernetztheit, die terroristische Gefahr bzw. der Gefährder im Einzelfall aufweisen muss. Insbesondere in Fällen des „homegrown terrorism", also der Radikalisierung über Fernkommunikationsmedien wie vor allem das Internet,[43] können sich Zweifel ergeben. Schließlich kam es gerade in der jüngeren Vergangenheit vermehrt zu Fällen, in denen Einzeltäter ohne feste Verbindungen zu organisierten terroristischen Gruppen Anschläge durchführten und es in diesen Zusammenhängen lediglich zu einseitigen Sympathie- und Loyalitätsbekundungen der Täter oder zu bloß nachträglichen Billigungen durch die in Bezug genommenen terroristischen Gruppen kam, ohne dass vorher ein nennenswerter Austausch stattgefunden hätte oder sich ein solcher zumindest nicht nachweisen ließ.[44]

Auch derartige Fälle, auch lose, einseitige, rein ideologische Bezüge müssen aber als Teil des internationalen Terrorismus angesehen werden, solange ihr Bezugs- bzw. Anknüpfungspunkt eine mit internationalem Anspruch operierende und mit hinreichend festen Strukturen ausgestattete Organisation ist.[45] Denn schließlich drückt sich in dieser typischen Diffusität und Amorphität die besondere Unberechenbarkeit und die spezifische Gefährlichkeit des neuartigen internationalen Terrorismus aus, auf welche die neue Aufgabenzuweisung in § 4a BKAG gerade reagieren soll. Eine übermäßige Ausdehnung der Zuständigkeit des BKA ist dabei nicht zu befürchten, vor allem weil die Kompetenzverteilung zwischen BKA und den jeweiligen LKÄ noch von den weiteren einschränkenden Voraussetzungen des § 4a Abs. 1 Satz 1 BKAG abhängt.[46] Diese Einschätzung wird durch die Anwendungspraxis mit lediglich 17 § 4a-Lagen im Untersuchungszeitraum erhärtet.[47] Einem solchen relativ weiten Verständnis von Internationalität entspricht auch die beim BKA vorherrschende Ansicht. Auch nach dortiger Einschätzung sollen bereits sehr geringe und lose, auch rein ideologische Bezüge genügen, solange das Phänomen, an das angeknüpft wird, hinreichend international strukturiert und organisiert ist. Freilich wird aus der Praxis berichtet, dass in derartigen Fällen die Gefahrenabwehr ohnehin sehr anspruchsvoll und schwierig ist, weil es bis zur Realisierung der Gefahr nur selten genügende Hinweise geben wird.

(b) Politische Allianzen

Neben der Frage der internationalen Vernetzung der Gefährder kann sich vor allem das Problem stellen, dass die Einordnung von Gruppen oder Personen als „terroristisch" eine hoch politische Entscheidung sein kann. Denn wenn terroristische Gruppen auch darüber definiert werden, dass sie die „Grundstrukturen eines Staates"

---

[42] In diesem Rahmen kommt es zu sog. Strukturermittlungsverfahren, also zu Verfahren, die auf die Ermittlung von Strukturen (potentiell terroristische Gruppierungen und Organisationen) gerichtet sind und nicht wie sonst üblich auf einzelne Personen. Sind die entsprechenden Gruppierungen an einem Vorgang beteiligt, kann dies wiederum als Indiz für die Zuordnung zum Internationalen Terrorismus gesehen werden.

[43] Hierzu auch Rux, JZ 2007, 285 (285 f.).

[44] Beispiele hierfür finden sich wohl in vielen der jüngeren Terroranschläge, etwa in Sydney im Dezember 2014, in Orlando im Juni 2016 oder in Nizza im Juli 2016. Auch bei den jüngsten Anschlägen in Berlin im Dezember 2016, London im März 2017 und Manchester im Mai 2017 sind die Bezüge und Vernetzungen noch nicht abschließend geklärt.

[45] Vgl. hierzu die Regierungsbegrüdung, BT-Drs. 16/10121, S. 21.

[46] Es muss also entweder eine länderübergreifende Gefahr vorliegen, die Zuständigkeit einer Landesbehörde nicht erkennbar sein oder eine oberste Landesbehörde muss um die Übernahme durch das BKA ersuchen.

[47] Siehe oben B.I.2.b.

beseitigen wollen, kann es vorkommen, dass eine Gruppe dieses Merkmal deshalb erfüllt, weil sie die politische Führung eines Staates bekämpft, dessen Bekämpfung die Bundesrepublik Deutschland als legitim erachtet. So kann sich insbesondere in politisch unübersichtlichen Lagen, wie sie derzeit im Nahen und Mittleren Osten herrschen, die Situation ergeben, dass die politische Führung der Bundesrepublik sich dazu entscheidet, zumindest implizite politische Bündnisse mit bestimmten nicht-staatliche Gruppen einzugehen, die gegen den Bestand eines oder mehrerer Staaten oder deren Führung gerichtet sind oder solche Gruppen gar mit Waffen zu beliefern. Ein derartiges wenn auch implizites außenpolitisches Bündnis macht es aber auch für die Rechtsordnung im Innern schwierig, die verbündete Gruppe als „terroristisch“ zu qualifizieren.

i. Bisherige Praxis: Subsumtion durch den Rechtsanwender

Das wirft die Frage auf, ob das politische Element in der Entscheidung darüber, welche Personen oder Gruppen als terroristisch qualifiziert werden, nicht auch prozedural deutlicher abgebildet werden sollte. Nach derzeitiger Rechtslage handelt es sich bei dem Begriff des internationalen Terrorismus und bei seiner Konkretisierung in § 4a Abs. 1 Satz 2 BKAG um Rechtsbegriffe auf Tatbestandsseite, deren Ausfüllung und Subsumtion dem Rechtsanwender, also Beamten des BKA und potentiell den Gerichten, obliegt.

ii. Bedarf für größere Transparenz und klarere Zuordnung des politischen Entscheidungselements?

Will man das politische Element in der Einordnung von Gruppen oder Personen als terroristisch deutlicher, transparenter und kritisierbarer machen, bestünde eine Möglichkeit darin, die Entscheidung in der Hierarchie auf Ebene der politischen Führung hochzuzonen und etwa einem Ministerium (bspw. dem Außen- oder Innenministerium) zuzuweisen. Allerdings bietet es sich kaum an, ein Ministerium in jedem Einzelfall von Ermittlungen im Zusammenhang mit § 4a BKAG einzuschalten. Oft ist schließlich gerade zu Beginn solcher Ermittlungen schlicht unklar, welche Personen oder Gruppen überhaupt beteiligt und wie sie ideologisch und politisch einzuschätzen sind. Auch grundsätzlich würde eine zu umfängliche, zu sehr auf den Einzelfall zielende Beteiligung der politischen Führungen die Ermittlungen unnötig hemmen und verkomplizieren.

Die Subsumtionsentscheidung im Einzelfall sollte daher grundsätzlich beim konkret ermittelnden Amtswalter des BKA belassen werden. Diese Zuständigkeit könnte aber durch Mechanismen ergänzt werden, die eine Beteiligung der Bundesregierung oder eines Ministeriums in durch abstrakte Vorgaben anleitender Funktion ermöglichen würden – etwa in Form von eigenen Terrorlisten der Bundesregierung, die zumindest als Orientierung, Indiz oder Regelvermutung fungieren könnten. Auf diese Weise würde einerseits die Transparenz der Einstufungen erhöht sowie politische Kritik und Diskussion ermöglicht. Andererseits bliebe die Subsumtion zunächst dem im Einzelfall ermittelnden Amtswalter des BKA belassen.

Rechtstechnisch gibt es zwei Möglichkeiten, diesen Ansatz weiter zu verfolgen. Einerseits ließen sich Terrorlisten in Form von Rechtsverordnungen auf Grundlage entsprechender Verordnungsermächtigungen im BKAG erstellen. Andererseits könnten solche Listen als Verwaltungsvorschriften erlassen werden. Rechtsverordnungen brächten den Vorteil höherer Rechtsförmlichkeit und Publizität mit sich. Verwaltungsvorschriften hingegen lassen sich leichter ändern und anpassen. Die damit einhergehende Flexibilität könnte bei der Einordnung von Personen oder Gruppen als terroristisch von Bedeutung sein. Ein Indiz dafür kann darin gesehen werden, dass „Terrorlisten“ der EU und der UN (s.o.) in der Praxis des BKA bisher kaum relevant waren, weil sie regelmäßig nicht ausreichend aktuell sind, um mit der hoch dynamischen und fragmentierten Landschaft des internationalen Terrorismus Schritt zu halten.

Sollte die Form der Verwaltungsvorschrift gewählt werden, so müssten sie dann aber – so wie die Listen der EU und UN auch – veröffentlicht werden, um dem Ausgangsziel höherer Transparenz gerecht zu werden.

(2) „Länderübergreifende Gefahr“

Neben der Definition des internationalen Terrorismus stellt sich in der Auslegung von § 4a Abs. 1 Satz 1 Nr. 1 BKAG die Frage, was unter einer „länderübergreifenden Gefahr“ zu verstehen ist, die in sechs von 17 der untersuchten § 4a-Lagen angenommen wurde.[48] Fraglich ist insbesondere, ob es erforderlich ist, dass zwei oder mehr Bundesländer einen direkten Bezug zur jeweiligen terroristischen Gefahr im Einzelfall aufweisen müssen.[49] Dann würde es etwa nicht ausreichen, dass die Gefahr andere Bundesländer lediglich mittelbar, etwa durch Einschüchterung auch der dortigen Bevölkerung betrifft. Vielmehr wäre erforderlich, dass sich die Gefahr

[48] Siehe oben. B.I.2.b.

[49] Siehe Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 38 f.

entweder in zwei oder mehr Bundesländern realisiert oder zumindest die terroristische Vereinigung in zwei oder mehr Bundesländern aktiv ist.[50] Dies würde bedeuten, dass im Falle von ohne feste Verbindungen zu derartigen länderübergreifenden Vereinigungen operierende Einzeltäter oder Gruppen, die ihre Anschlagspläne auf ein Bundesland begrenzen, die Kompetenz zur Gefahrenabwehr nicht beim BKA läge. Demgegenüber lässt sich § 4a Abs. 1 Satz 1 Nr. 1 BKAG auch so verstehen, dass es genügen soll, wenn sich der Schaden zwar in nur einem Bundesland ereignet, aber die Auswirkungen (Verunsicherung der Bevölkerung etc.) über das Land hinausgingen.[51] Das allerdings ist bei jedem terroristischen Anschlag größeren Ausmaßes der Fall, weshalb sich allein aus diesem Effekt kaum eine länderübergreifende Gefahr im Sinn des Gesetzes ergeben kann; denn das Merkmal der länderübergreifenden Gefahr würde sonst leerlaufen.

Daher ist ein direkter Bezug mindestens zweier Bundesländer – entweder zur Vorbereitung oder zur Realisierung des Anschlags – erforderlich, um von einer länderübergreifenden Gefahr zu sprechen. Dem entspricht auch die Auslegungs- und Subsumtionspraxis des BKA, das von einer länderübergreifenden Gefahr nur dann ausgeht, wenn Gefährder sich im Zusammenhang mit dem Anschlag bzw. der Anschlagsplanung in mehreren Bundesländern aufhalten oder bewegen oder die Gefahr sich in mehreren Ländern zu realisieren droht.

Bei Unklarheiten, wenn also etwa konkrete Anhaltspunkte für die Betroffenheit mehrerer Länder vorliegen und sich im Nachhinein herausstellt, dass eine länderübergreifende Gefahr nicht gegeben war, kann u. U. § 4a Abs. 1 Satz 1 Nr. 2 BKAG helfen (Unerkennbarkeit der Zuständigkeit einer Landesbehörde). In der Tat sind in der Anwendungspraxis regelmäßig Überschneidungen dieser beiden Kompetenzvorschriften zu beobachten.[52] Im Übrigen ist vorsorglich darauf hinzuweisen, dass die Zuständigkeitsfrage grundsätzlich objektiv zu beurteilen ist.

(3) „Gefahren“ (dogmatisch-systematische Einordnung)

Der Begriff der Gefahr als solcher in § 4a Abs. 1 Satz 1 BKAG umfasst zunächst (konkrete) Gefahren im klassischen Sinn. In § 4a Abs. 1 Satz 2 BKAG wird dem BKA darüber hinaus die vorgelagerte Kompetenz zur Verhütung von Straftaten des internationalen Terrorismus zugewiesen. Dabei handelt es sich freilich jeweils um (bloße) Aufgabenzuweisungsnormen. Die Gefahrbegriffe in ihrer Funktion als Eingriffsschwellen für konkrete Eingriffsbefugnisse werden im Rahmen der Befugnisnormen präzisiert und kategorisiert. § 20a Abs. 2 BKAG fungiert dabei als eine Art Scharniernorm, die die Gefahrenbegriffe der Befugnisse in §§ 20b ff. BKAG an die inzidente Terrorismusdefinition in § 4a Abs. 1 Satz 2 BKAG[53] koppelt.

Ob eine Eingriffsnorm dem Bereich der Gefahrenabwehr zuzuordnen ist oder den Bereich der Straftatenverhütung betrifft, ergibt sich aus dem Tatbestand der Eingriffsnorm selbst. Ein Beispiel für eine Befugnisnorm, die zur Straftatenverhütung ermächtigt, ist etwa § 20b Abs. 2 BKAG.[54]

Daneben vermittelt die Aufgabe der Straftatenverhütung dem BKA die Kompetenz auch zu eingriffsfreien Verhütungsmaßnahmen wie etwa der Lage- und Milieubeobachtung und -analyse.

iii) Zusammenarbeit von Bund und Ländern

Wegen der Neuschaffung einer Bundeskompetenz für die Bekämpfung der Gefahren des internationalen Terrorismus in § 4a BKAG auf der Grundlage von Art. 73 Abs. 1 Nr. 9a GG stand die Befürchtung im Raum, dass sich das BKA zu einer Art „deutschem FBI“ entwickeln und sich faktisch in einem großen Umfang den Landespolizeibehörden überordnen könnte.

Diese Befürchtungen haben sich in der Anwendungsrealität des § 4a BKAG indes nicht bestätigt. Das wird bereits daran deutlich, dass es im Untersuchungszeitraum von sechs Jahren insgesamt lediglich 17 Einsatzlagen nach § 4a BKAG gab. Eine massive Ausweitung des eigenen Zuständigkeitsbereichs durch das BKA ist schon vor diesem quantitativen Hintergrund derzeit nicht zu befürchten. Dafür spricht insbesondere auch, dass trotz Anstieg der Ausgangssachverhalte seit 2014 die Zahl der § 4a-Lagen nicht zunahm.[55] Zugleich bedeutet die

---

50 Graulich, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 4a Rn. 8.

51 So wohl die Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 20 f.

52 Siehe oben B.I.2.b.

53 Hierzu oben B.II.1.c.ii)(1).

54 Siehe die Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 23.

55 Siehe oben B.I.2.

geringe Fallzahl auch, dass sich bislang nur wenige seriöse Aussagen zum praktischen Ablauf der Zusammenarbeit von Bund und Ländern im Rahmen von § 4a BKAG machen lassen. Schon deshalb könnte es angezeigt sein, den Gebrauch von § 4a BKAG weiterhin zu beobachten.

(1) Benehmensregel

In qualitativer Hinsicht ist vor allem die praktische Anwendung der Benehmensregel in § 4a Abs. 2 Satz 3 BKAG bedeutsam für die Handhabung von § 4a BKAG und ihre Auswirkungen auf das Verhältnis von Bund und Ländern. § 4a Abs. 2 S. 3 BKAG sieht vor, dass die Wahrnehmung der Aufgaben nach § 4a BKAG im gegenseitigen Benehmen zwischen dem BKA und der oder den jeweiligen Landesbehörden[56] erfolgt.

(a) Hintergrund und Bedeutung

Zweck dieser Regelung ist vor allem die Vermeidung von Mehrfacheingriffen durch unterschiedliche Behörden bei unklarer Zuständigkeitslage.[57] Benehmen bedeutet dabei im Gegensatz zum Einvernehmen, dass die Behörden letztlich nicht zu einer Übereinkunft gelangen müssen. Vielmehr genügt es, wenn sich die Behörden gegenseitig Gelegenheit zur Stellungnahme geben und das BKA die Stellungnahme der Landesbehörden in die eigenen Erwägungen einstellt.[58]

(b) Handhabung in der Praxis

In der Praxis wird das Benehmen hergestellt, indem das BKA zunächst die Landesbehörde mittels eines E-Post-Schreibens in Kenntnis setzt, dass es einen Gefahrenabwehrvorgang nach § 4a BKAG eingeleitet hat. Das Benehmen wird also generell für eine konkrete Einsatzlage nach § 4a BKAG und nicht in Bezug auf jede einzelne im Rahmen dieser Einsatzlage ggf. durchgeführte Eingriffsmaßnahme hergestellt. Dies verträgt sich mit § 4a BKAG, der nicht davon spricht, dass jede einzelne Maßnahme im Benehmen mit der jeweils anderen Behörde durchzuführen ist, sondern dass „die Aufgabenwahrnehmung“ insgesamt im gegenseitigen Benehmen zu erfolgen hat. Zusätzlich zum Inkenntnissetzen via E-Post wird das Vorgehen in gemeinsamen Besprechungen im GTAZ[59] in Berlin abgestimmt. Unter diesen Umständen wird die Praxis dem Erfordernis der Aufgabenwahrnehmung in gegenseitigem Benehmen gerecht. Eine Inkenntnissetzung allein oder auch eine bloße Anhörung würde demgegenüber nicht ausreichen.

(2) Kein Weisungsrecht

Ein Weisungsrecht gegenüber Landespolizeibehörden steht dem BKA im Rahmen von § 4a BKAG nicht zu. Auch im – bislang allein theoretischen – Fall offener Kompetenzkonflikte im Bereich der Abwehr von Gefahren des internationalen Terrorismus steht dem BKA also keine Handhabe zur Verfügung, um im Extremfall die eigene Ermittlungs- und Gefahrenabwehrtaktik gegenüber abweichenden Ansichten der Landesbehörden durchsetzen zu können.[60] Ein solches Weisungsrecht einer Bundes- über eine Landesbehörde stellte jenseits der Bundesauftragsverwaltung nach Art. 85 Abs. 3 GG einen deutlichen Fremdkörper im Verwaltungssystem des Grundgesetzes dar. Zudem hat sich hierfür in der Evaluation kein praktisches Bedürfnis abgezeichnet. Auch von Seiten des BKA wird es sowohl auf Grund der bisherigen Erfahrungen als auch aus grundsätzlichen Erwägungen heraus für weder erforderlich noch sinnvoll gehalten. Insofern sind einer zu massiven Ausweitung der Kompetenzen des BKA und einer Überordnung über Landesbehörden also ebenfalls Grenzen gesetzt, deren Aufweichung zur Zeit nicht zu befürchten ist.

---

[56] § 4a Abs. 2 Satz 3 BKAG sieht auch eine Benehmensregel für das Verhältnis des BKA zu anderen möglicherweise betroffenen Bundespolizeibehörden vor. Dies bleibt hier aber insofern außer Betracht, als es im Ausgangspunkt um Auswirkungen von § 4a BKAG auf das föderale Kompetenzgefüge geht.

[57] Dies wird etwa in der Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 21, nicht klar.

[58] Siehe die Regierungsbegründung, BT-Drs. 16/10121, S. 21. Aus anderen Kontexten vgl. etwa Ginzky, in: BeckOK Umweltrecht, 38. Ed. 2015, § 45k WHG Rn. 16. S. auch Gellermann, in: Landmann/Rohmer, Umweltrecht, 78. EL 2015, § 22 BNatSchG Rn. 30 (Versuch der Abstimmung genügt).

[59] GTAZ = Gemeinsames Terrorismusabwehrzentrum in Berlin. Beteiligt sind verschiedene Behörden – neben dem BKA etwa das Bundesamt für Verfassungsschutz, aber auch das Bundesamt für Migration und Flüchtlinge, der Generalbundesanwalt u.a.

[60] Skeptisch hierzu Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Berlin 2009, S. 59 f.

(3) Zuständigkeit für Ersuchen nach § 4a Abs. 1 Satz 1 Nr. 3 BKAG

§ 4a Abs. 1 Satz 1 Nr. 3 BKAG begründet eine Zuständigkeit des BKA für den Fall, dass eine oberste Landesbehörde um eine Übernahme der Gefahrenabwehr ersucht. Dieser Fall ist in der Praxis im Untersuchungszeitraum lediglich ein Mal vorgekommen.[61] Eine interne Subsumtionshilfe des BKA geht davon aus, dass jedenfalls bei Gefahr im Verzug ein Ersuchen durch ein LKA genügt.[62] Bei einem LKA handelt es sich allerdings nicht um eine oberste Landesbehörde; wird das BKA also durch ein LKA um Übernahme der Gefahrenabwehr ersucht, wird eine Zuständigkeit nach § 4a Abs. 1 Satz 1 Nr. 3 BKAG nicht begründet.

Da in der Praxis die LKÄ, nicht oberste Landesbehörden wie etwa die Landesministerien, mit den Ermittlungen befasst sind, haben sie die direkteren und umfassenderen Kenntnisse über Gefährdungssachverhalte und können sachnäher einschätzen, ob eine Übernahme des Vorgangs durch das BKA angezeigt ist. Die notwendige Einschaltung der obersten Landesbehörden im Fall von § 4a Abs. 1 Satz 1 Nr. 3 BKAG fungiert demgegenüber als Instrument, das der Wahrung der föderalen Kompetenzordnung dient: Das Übernahmeersuchen soll nicht allein einer polizeilichen Logik folgen, sondern es soll zusätzlich einer landespolitischen Kontrolle unterliegen. Vor dem Hintergrund dieser grundsätzlichen Gemengelage bietet es sich als vermittelnde Lösung durchaus an, für Eilfälle die Möglichkeit zu schaffen, dass auch ein Übernahmeersuchen durch ein LKA die vorläufige Zuständigkeit des BKA begründen kann. Diese würde dann lediglich bis zu der unverzüglich herbeizuführenden Entscheidung der obersten Landesbehörde bestehen. Denn bei Gefahr im Verzug ist es angezeigt, dass sich zunächst die polizeiliche Logik durchsetzt. Dafür bedürfte es allerdings einer entsprechenden Änderung von § 4a Abs. 1 Satz 1 Nr. 3 BKAG. Nach derzeitiger Gesetzeslage kann allein das Ersuchen durch eine oberste Landesbehörde eine Zuständigkeit des BKA begründen.

iv) Internationale Kooperation

Nach den Erfahrungen des BKA hat die Einführung der Kompetenz zur Gefahrenabwehr in § 4a BKAG zur Verbesserung der Kooperation mit ausländischen Stellen geführt. Deren Kooperationsbereitschaft habe merklich zugenommen, seit man in der Lage ist, Vorgänge und Informationsanfragen explizit einem eigenen Gefahrenabwehrkontext zuzuordnen. Tatsächlich kamen auch in der Anwendungspraxis die ermittlungsursächlichen Hinweise in etwa der Hälfte der § 4a-Lagen von ausländischen Behörden.[63]

d. Zwischenfazit zu § 4a BKAG

i) Grundsätzlicher Bedarf für die Regelung

Vor dem Hintergrund der zunehmenden und immer komplexer werdenden Gefahren erscheint die Hochzonung der Kompetenz zur Abwehr von Gefahren des internationalen Terrorismus auf Bundesebene in § 4a BKAG als gerechtfertigt, zumal die Norm in Umsetzung von Art. 73 Abs. 1 Nr. 9a GG erlassen wurde und weitgehend mit diesem übereinstimmt. Daneben ist erneut zu betonen, dass § 4a BKAG im Übrigen vor allem den Zweck verfolgt, Mehrfacheingriffe durch verschiedene Kompetenzträger zu verhindern. Gerade unter diesem Gesichtspunkt gibt es einen grundsätzlichen Bedarf für eine Regelung wie § 4a BKAG.

ii) Verfassungskonformität

§ 4a BKAG beruht auf dem Kompetenztitel des Art. 73 Abs. 1 Nr. 9a GG und reagiert auf die aktuellen Erscheinungsformen des internationalen Terrorismus. Die Norm ist in ihrer jetzigen Form verfassungsgemäß.

iii) Auslegungsfragen

In der Auslegung der Norm ergeben sich einige Herausforderungen. Insbesondere die Begriffe des „internationalen Terrorismus“ und der „länderübergreifenden Gefahr“ werfen Fragen auf. Diese lassen sich allerdings im Wege der Auslegung weitgehend klären.

---

61 Siehe oben B.I.2 sowie Tabelle 1.

62 Auch in dem bisher einzigen Praxisfall erfolgte das Ersuchen durch eine Landespolizeibehörde, siehe oben B.I.2.

63 Siehe oben Tabelle 1 unter B.I.2.

iv) Normanwendung

Die Auslegung und Handhabung der Regel in der Praxis entspricht ihren normativen Vorgaben weitgehend. Eine Ausnahme bildet die – allerdings lediglich an einer einzelnen Stelle in einer internen Subsumtionshilfe zu findenden – Vorstellung des BKA, dass bei Gefahr im Verzug eine Zuständigkeit nach § 4a Abs. 1 Satz 1 Nr. 3 BKAG auch dann begründet wird, wenn ein LKA an Stelle einer obersten Landesbehörde um die Übernahme der Gefahrenabwehr ersucht.

e. Änderungsvorschläge

i) „Internationaler Terrorismus“: Schaffung einer klareren Regelungsstruktur

Eine detailliertere Definition des Begriffs „internationaler Terrorismus“ sollte im Gesetz schon wegen der Diffusität, Vielgestaltigkeit und Dynamik des internationalen Terrorismus nicht versucht werden. „Terrorismus“ muss vielmehr ein generischer Begriff bleiben, auch, um auf die gerade aktuell zu beobachtenden schnellen Veränderungen in diesem Bereich reagieren zu können. Allerdings erscheint es schon aus Gründen der Regelungsklarheit empfehlenswert, die „versteckte“ Terrorismusdefinition aus § 4a Abs. 1 Satz 2 BKAG offener zu gestalten und ihre regelungssystematische Bedeutung klarzustellen. Will man sich aus den genannten Gründen beispielsweise nicht auf eine abschließende Terrorismusdefinition einlassen und gleichwohl eine regelungsklarere Struktur von § 4a Abs. 1 BKAG erreichen, so könnte die Norm etwa wie folgt umformuliert werden:

§ 4a

Abwehr von Gefahren des internationalen Terrorismus

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

1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
3. die oberste Landesbehörde um eine Übernahme ersucht.

[2]Gefahren des internationalen Terrorismus sind Gefahren der Verwirklichung von Straftaten, die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können. [3]Das Bundeskriminalamt kann in den in Satz 1 bezeichneten Fällen auch zur Verhütung von Straftaten nach Satz 2 tätig werden.

(2) [1]Die Befugnisse der Länder und anderer Polizeibehörden des Bundes bleiben unberührt. [2]Die zuständigen obersten Landesbehörden und, soweit zuständig, anderen Polizeibehörden des Bundes sind unverzüglich zu benachrichtigen, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt. [3]Die Aufgabenwahrnehmung erfolgt in gegenseitigem Benehmen. [4]Stellt das Bundeskriminalamt bei der Aufgabenwahrnehmung nach Absatz 1 Satz 1 Nr. 2 die Zuständigkeit einer Landespolizeibehörde fest, so gibt es diese Aufgabe an diese Polizeibehörde ab, wenn nicht ein Fall des Absatzes 1 Satz 1 Nr. 1 oder 3 vorliegt.

ii) Einbindung der politischen Führung?

Einer stärkeren Einbeziehung der politischen Führung in die Einordnung von Personen oder Gruppen als terroristisch sind jedenfalls Grenzen gesetzt. So würden sich Zeit- und Geheimhaltungsprobleme ergeben, wenn bei jeder Ermittlung im Einzelfall und bereits frühzeitig eine Beteiligung der politischen Führung erforderlich wäre. Eine Alternative liegt daher wie gesehen in der Erstellung von eigenen Terrorlisten der Bundesregierung.

iii) Ersuchen durch LKA bei Gefahr im Verzug

Da bei Gefahr im Verzug die Bedeutung der polizeilichen Handlungslogik in den Vordergrund tritt, bietet es sich an, dass auch ein Übernahmeersuchen durch ein LKA eine Zuständigkeit des BKA zur Abwehr von Gefahren des internationalen Terrorismus begründen kann. § 4a Abs. 1 Satz 1 BKAG könnte insofern wie folgt umformuliert werden:

§ 4a

Abwehr von Gefahren des internationalen Terrorismus

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

1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
3. die oberste Landesbehörde um eine Übernahme ersucht**; bei Gefahr im Verzug genügt es bis zur unverzüglich herbeizuführenden Entscheidung der obersten Landesbehörde, wenn ein Landeskriminalamt um die Übernahme ersucht.**

[...]

2. § 20j BKAG

a. Hintergrund und Ziele der Norm

§ 20j BKAG ermächtigt das BKA zu sog. Rasterfahndungen. Dabei handelt es sich um die Ermittlung und Zusammenführung verschiedener Datenbestände, um anhand von sog. Kreuztreffern diejenigen Personen zu ermitteln, die die gerasterten Merkmale erfüllen. Die Rasterfahndung ist also ein Instrument zur Ermittlung von zuvor unbekannten Gefährdern anhand bekannter Parameter. § 20j BKAG ermöglicht es dem BKA dabei, Datenbestände sowohl von anderen öffentlichen als auch von privaten Stellen zu beschaffen. Zur Gefahrenabwehr wurde die Rasterfahndung insbesondere nach dem 11. September 2001 eingeführt.[64]

Die Beschaffung und der Abgleich von Datenbeständen im Rahmen der Rasterfahndung bedeutet Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 GG) der Betroffenen. Vor diesem Hintergrund äußerte sich das BVerfG im Jahr 2006 grundlegend zur Verfassungskonformität der präventiven Rasterfahndung. Frühe Normierungen bzw. ihre Auslegung und Handhabung in der Praxis wurden dabei als zu weitgehend eingestuft.[65] Das BVerfG verlangte für die Rasterfahndung die Beschränkung auf eine konkrete Gefahr; als reine Vorfeldmaßnahme sei sie nicht zulässig.[66] Damit wurde der Anwendungsbereich für die Rasterfahndung als typischer Gefahrerforschungsmaßnahme zwar beschnitten. Dies führt allerdings nicht zur Nutzlosigkeit der Rasterfahndung. Lediglich die rein präventive Rasterung ohne Stützung auf ein konkretes Wahrscheinlichkeitsurteil scheidet aus.

b. Verfassungskonformität

§ 20j BKAG und damit die Rasterfahndung als solche wurde vom BVerfG weitgehend als verfassungsgemäß bestätigt.[67] Dabei hat das Gericht noch einmal betont, dass dies auch daran liegt, dass § 20j BKAG i. V. m. § 20a Abs. 2 BKAG eine konkrete Gefahr voraussetzt. Auch die Löschungsregelungen in § 20j Abs. 3 Satz 1 und Satz 2 BKAG hat das Gericht als verfassungsgemäß erachtet. Als verfassungswidrig verworfen wurde hingegen zu Recht die zu kurze Aufbewahrungsfrist der Löschungsprotokolle in § 20j Abs. 3 Satz 3 BKAG. Denn die in dieser Vorschrift vorgesehene Löschung der Dokumentation am Ende des Kalenderjahres, das der Löschung der Daten oder der Vernichtung der Akten folgt, bringt es mit sich, dass die verfassungsrechtlich erforderliche Nachvollziehbarkeit und Kontrolle strukturell gefährdet wird.[68]

c. Normanwendung

Die Rasterfahndung nach § 20j BKAG wurde jedenfalls bis November 2015 lediglich einmal angewendet (EG Advent) und stellt damit eine auch im Vergleich zu anderen Maßnahmen sehr selten eingesetzte Befugnis dar.[69] Nach Auskunft des BKA konnte in diesem Fall keine Person ermittelt werden. Auf dieser Grundlage

---

64 So schuf etwa das Land NRW in § 31 PolGNW eine im Jahr 2003 in Kraft getretene Ermächtigungsgrundlage für die Rasterfahndung. Inzwischen finden sich Ermächtigungsgrundlagen in allen Landespolizeigesetzen. Zudem ist die Maßnahme auch zur Strafverfolgung vorgesehen, s. § 98a StPO.

65 BVerfGE 115, 320 (367 ff.). Anknüpfungspunkt des Verfahrens war der damalige § 31 Abs. 1 PolGNW.

66 BVerfGE 115, 320 (357).

67 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 206 f.

68 Siehe BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 271-273.

69 Siehe oben Tabelle 4 und B.I.3.b.i).

gelangte das BKA zu der Einschätzung, dass sich in diesem Fall eine konkrete Gefahr nicht mehr valide begründen ließ. Die entsprechenden Gefahrermittlungen wurden daher eingestellt.

Auf Grund der sehr geringen Fallzahl und weil die Akten zum einzigen Anwendungsfall gesperrt sind, lassen sich zur Anwendungspraxis von § 20j BKAG nur kaum Aussagen treffen.

i) Institutioneller Anwendungsrahmen

Der vom BVerfG im Jahr 2006 beanstandeten zu weitgehenden Handhabung der Rasterfahndung[70] wird im BKA vor allem durch die Beteiligung des Rechtsreferats (IZ 14, vormals KI 15) bei der konkreten Entscheidungsfindung entgegengewirkt. Dass man im BKA tatsächlich nicht leichtfertig mit der Kompetenz zur Rasterfahndung umgeht, zeigt sich auch darin, dass das Instrument (jedenfalls bis November 2015) erst ein Mal zum Einsatz kam.

Als weitere institutionelle Sicherung kommt hinzu, dass die Rasterfahndung nach § 20j Abs. 4 BKAG nur durch die Amtsleitung beantragt und nur durch ein Gericht angeordnet werden kann.[71] Dieses Erfordernis wird auch aus ermittlungspraktischer Sicht im BKA als unproblematisch angesehen.

ii) Gefahrenschwelle

§ 20j BKAG erlaubt die Rasterfahndung, soweit eine Gefahr vorliegt „für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist“. Eine solche Gefahr soll in der Regel auch dann vorliegen, „wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll.“ Laut dem auch für § 20j BKAG geltenden § 20a Abs. 2 BKAG muss es sich zudem um eine „im Einzelfall bestehende Gefahr für die öffentliche Sicherheit im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2“ handeln.

Das Problem dieser Formulierung und Konstruktion liegt auf der Hand. Mit Blick auf die Gefahrenschwelle handelt es sich bei § 20j BKAG um eine sehr komplex und unübersichtlich geratene Norm. Nicht zuletzt entstehen ggf. auch extrem lange, unübersichtliche Verweisungsketten (von § 20j zunächst auf § 4a BKAG, von dort auf § 129a StGB, von dort wiederum auf andere Normen des Strafgesetzbuches, u. U. auch auf das Waffengesetz oder das Kriegswaffenkontrollgesetz). Die Beschreibung der für die Rasterfahndung notwendigen Gefahrenschwelle ist daher sehr unübersichtlich. Dieser Missstand ist auf einen grundsätzlichen Mangel an Systematik der im BKAG verwendeten Gefahrenbegriffe zurückzuführen. Die Fragmentierung von Gefahrenbegriff und -dogmatik wurde in der Literatur bereits eingehend kritisiert.[72]

Klar ist wiederum auch nach der aktuellen Formulierung der Norm, dass eine Rasterfahndung nicht bei einer bloß abstrakten Gefahr zulässig ist, wie es auch im Urteil des BVerfGs betont wird.[73] Die bisher einzige Anwendung der Rasterfahndung ist diesem letztgenannten Erfordernis – basierend auf den Schilderungen des BKA – gerecht geworden. Es wurde keineswegs versucht, lediglich auf Grund einer unspezifischen allgemeinen Bedrohungslage potentielle künftige Gefährder zu ermitteln. Vielmehr bestanden in diesem Einzelfall Hinweise auf einen konkreten Anschlag in Deutschland durch vier Personen. Zu einem der Gefahrenverursacher bestanden allerdings lediglich fragmentarische Erkenntnisse. Zwecks Ermittlung der Echt-Identität dieses Gefahrenverursachers wurden – ausgehend von den vorhandenen fragmentarischen Erkenntnissen – Massendaten sowohl von staatlichen als auch von privaten Stellen erhoben und sowohl automatisiert als auch manuell abgeglichen. Der Abgleich ergab dann allerdings keine Person, die zu den fragmentarischen Erkenntnissen zum Gefahrenverursacher passte. Die Gefahrermittlungen wurden später insgesamt eingestellt. Der Fall verdeutlicht, dass die Rasterfahndung gerade dann als Instrument in Betracht kommt, wenn Unklarheit über die Person eines Gefahrenverursachers – und damit regelmäßig zusammenhängend: Unklarheit über das Vorliegen einer Gefahr – besteht. Es handelt sich also bei der Rasterfahndung typischerweise um ein Instrument der Gefahrerforschung, das auf einen Gefahrverdacht reagiert. Das wird auch in § 20j BKAG deutlich, der es genügen lässt, dass „konkrete

---

70 BVerfGE 115, 320 (367 ff.).

71 Zuständig für die Anordnung ist das AG Wiesbaden, s. § 20v Abs. 2 S. 1 BKAG.

72 Siehe nur Waechter, JZ 2015, 8 (8 ff.).

73 Siehe oben B.II.2.a sowie BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 207.

Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 4a Abs. 1 Satz 2 begangen werden soll."[74]

Aus Sicht des BKA ist die Norm zwar letztlich handhabbar, was vor allem an der institutionalisierten Einbindung des Rechtsreferats liegt. Im Laufe der Untersuchung wurde aber der Eindruck gewonnen, dass es sich bei § 20j BKAG jedenfalls für die operativen Einheiten zumindest um eine nicht besonders klare oder leicht handhabbare Norm handelt. Es liegt daher nahe, das auch in § 20j BKAG deutlich sichtbare Problem großer Unsicherheiten im System des Gefahrenbegriffs durch eine insgesamt konsistentere Formulierung jedenfalls der zentralen dogmatischen Begriffe im BKAG anzugehen.[75]

iii) Auswirkungen auf die Zusammenarbeit von Bund und Ländern

Nennenswerte oder spezifische Auswirkungen auf das föderale Kompetenzgefüge sind durch § 20j BKAG nicht zu befürchten. Zwar bewirkt die Norm, dass das BKA nun u. U. bei Landesbehörden Informationen sammeln kann. Insoweit unterscheiden sich Landesbehörden im Rahmen von § 20j BKAG aber nicht von beliebigen anderen privaten oder öffentlichen Stellen. Dass es nur einen untersuchten Anwendungsfall gab, deutet darauf hin, dass schon wegen des geringen Umfangs und der – mit Blick auf die Berührung föderaler Belange – eher geringen Intensität der Maßnahmen auch faktische Auswirkungen auf das Verhältnis zwischen und die Zusammenarbeit von Bund und Ländern nicht in relevantem Ausmaß zu befürchten sind.

iv) Eilfälle

Eine Eilregelung für § 20j BKAG war noch im Regierungsentwurf enthalten.[76] Auch das BVerfG hält Eilregelungen auch im Kontext derartiger Befugnisse, denen es aus grundrechtlicher Perspektive eine hohe Eingriffsintensität zuschreibt, für grundsätzlich zulässig.

Allerdings erscheint eine Eilregelung, also die Möglichkeit, bei Gefahr im Verzug unter vereinfachten prozeduralen Bedingungen eine Rasterfahndung vornehmen zu können, aus Sicht des BKA nicht erforderlich. Denn die Maßnahme ist in der Praxis regelmäßig derart vorbereitungsintensiv, dass sie in einem Eilfall ohnehin nicht sinnvoll eingesetzt werden könnte. Die einzig denkbare Konstellation, in der eine Eilregelung einen Gewinn für die Praxis brächte, wäre der Fall, dass eine Rasterfahndung bereits genehmigt und vorbereitet, dann aber zunächst doch nicht durchgeführt wurde, und sich zum Ende des Genehmigungszeitraums neue Verdachtsmomente ergeben, die eine kurzfristige Durchführung der Rasterfahndung dann doch angezeigt erscheinen lassen. Dieses Szenario ist aber so unwahrscheinlich, dass der praktische Bedarf für eine Eilregelung insgesamt als sehr gering zu bewerten ist.

v) Anwendungshindernisse

Nennenswerte Anwendungshindernisse sieht das BKA im Rahmen von § 20j BKAG nicht. Dass die Befugnis bisher so selten genutzt wurde, liegt einerseits daran, dass sie in vielen Fällen nicht erforderlich ist – etwa, weil bereits alle Gefahrenverursacher identifiziert sind oder aber, weil sich der Gefahrverdacht bereits anderweitig ausräumen lässt. Andererseits gibt es Fälle, in denen eine Rasterfahndung schlicht unpraktikabel ist – etwa, weil zu wenig über die zu identifizierenden Personen bekannt oder die Tätergruppe gerade normalisiert ist und sich daher keine hinreichend vielversprechenden Ansatzpunkte für die Erhebung bestimmter Daten ergeben.

Bei der Umsetzung einer Rasterfahndung dürften sich veritable Probleme in relevantem Ausmaß wohl lediglich im bislang hypothetischen Szenario ergeben, dass die datenführende Stelle die Kooperation verweigert. Falls die benötigten Daten nicht direkt preisgegeben würden, würde die Beschlagnahme des übergeordneten Datenbestandes erforderlich, in dem die Zieldaten enthalten sind. Dabei würde es sich in der Regel um einen ungleich größeren Datenbestand handeln, der zunächst auf die benötigten Daten durchsucht werden müsste. Es ergäben sich also erstens technische Probleme bei der Durchführung der Rasterfahndung; die Maßnahme könnte im Ernstfall schlicht zu aufwändig oder zu zeitintensiv sein. Zweitens könnten sich rechtliche Probleme ergeben. Denn bei der Durchsuchung der beschlagnahmten Gesamtdatensätze würden u. U. Daten Unbeteiligter intensiver von den Behörden zur Kenntnis genommen, als dies bei der Rasterfahndung normalerweise der Fall wäre.

---

[74] Die Wendung „Tatsachen, die die Annahme rechtfertigen…" ist die typische Formulierung des Gefahrverdachts, siehe Pieroth/Schlink/Kniesel, Polizeirecht, 8. Aufl. 2014, § 4 Rn. 50 ff. Zur Einordnung in das System der Gefahrenabwehrdogmatik eingehend noch unten B.II.4.

[75] Siehe unter B.II.4.

[76] Siehe Bundestagsdrucksache 16/10121, S. 9, 28.

Es stellte sich dann die Frage, ob die entstehenden datenschutzrechtlichen Probleme, also die Eingriffe in das Recht auf informationelle Selbstbestimmung, sich bereits ihrerseits über § 20j BKAG, ggf. i. V. m. Vorschriften des VwVG, rechtfertigen ließen. Derartige Szenarien sind aber insgesamt, auch aus Sicht des BKA, höchst unwahrscheinlich. Vielmehr werde die überwiegende Mehrzahl datenführender privater Stellen in Deutschland bei Vorlage einer vom Gericht erlassenen Anordnung nach § 20j BKAG kooperieren. Daher bedarf es keiner Ergänzung des BKAG um spezifische Vollstreckungsregelungen für § 20j BKAG.

d. Zwischenfazit zu § 20j BKAG

i) Grundsätzlicher Bedarf für die Befugnis

Trotz der sehr geringen Fallzahl handelt es sich bei der Rasterfahndung nach Einschätzung des BKA um ein unentbehrliches Instrument. Der Wert der Kompetenz aus § 20j BKAG ergebe sich insbesondere aus der Effizienz und – zumindest relativen – Schnelligkeit des Mittels zur Identifizierung von Zielpersonen bzw. zur Feststellung, dass eine gesuchte Zielperson nicht existiert. So diene die Kompetenz nicht zuletzt dazu – wie auch im einzigen hier untersuchten Anwendungsfall – Gefahrverdachtssituationen möglichst schnell ausräumen zu können.

Tatsächlich bedeutet ein spärlicher Rückgriff auf eine Eingriffsbefugnis nicht automatisch, dass sie entbehrlich ist. Dieser Umstand kann vielmehr erstens auf eine besonders behutsame, um die Verhältnismäßigkeit ihres Vorgehens bemühte Verwaltungspraxis hindeuten. Zweitens ist der internationale Terrorismus kein Massenphänomen. Ernsthafte Anschlagsplanungen sind auf relativ kleine Kreise und relativ seltene Fälle beschränkt. Das hat sich auch darin gezeigt, dass es zwar nur wenige § 4a-Lagen gab, die dann aber oft mit relativ umfangreichen Ermittlungen einhergingen.[77] Werden sie realisiert, bringen sie aber erhebliche Auswirkungen mit sich. Dies rechtfertigt es, auch bei solchen gefahrenabwehrrechtlichen Kompetenzen von einem realen Bedarf zu sprechen, die nur selten eingesetzt werden. Dass es immerhin einen Anwendungsfall gab, in dem die Rasterfahndung erfolgreich (zur Entkräftung des Gefahrverdachts) eingesetzt wurde, zeigt jedenfalls, dass die Norm nicht gänzlich entbehrlich ist, zumal auf diese Maßnahme erst zurückgegriffen wird, wenn die Rasterung polizeiinterner Datenbestände keine Abhilfe verspricht. Es besteht daher kein Grund, an der Zweckmäßigkeit der Befugnis des BKA zur Vornahme von Rasterfahndungen nach § 20j BKAG zu zweifeln.

ii) Auslegungsfragen

§ 20j BKAG eröffnet keine komplizierten Auslegungsfragen. Allerdings ist die Formulierung der Gefahrenschwellen überkomplex und unübersichtlich geraten und erschwert die Handhabung der Norm.

iii) Verfassungskonformität

§ 20j BKAG ist mit Ausnahme der zu kurzen Aufbewahrungsfrist für die Löschungsprotokolle in § 20j Abs. 3 Satz 3 BKAG verfassungskonform.

iv) Normanwendung

Im einzigen untersuchten Anwendungsfall bestand eine Gefahrverdachtslage in einem konkreten Einzelfall. Die Norm wurde in diesem Fall – die Schilderungen des BKA zur Tatsachengrundlage nehmend – rechtmäßig und nicht in einer Art und Weise angewendet, wie es bisweilen befürchtet wurde (rein präventive Rasterung ohne Beschränkung auf konkrete Sachverhalte).[78]

e. Änderungsvorschläge

i) Aufbewahrungsfrist für Löschungsprotokolle

Der Gesetzgeber muss auf die Verfassungswidrigkeit der Aufbewahrungsfrist der Löschungsprotokolle in § 20j Abs. 3 Satz 3 BKAG reagieren. Das BVerfG hat die Frist zu Recht als zu kurz verworfen. Die Frist müsse nämlich „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

---

77 Siehe oben B.I.2.b und B.I.3 (vor allem Tabelle 2, 3 und 4 sowie Schaubild 2).

78 Zur Einordnung in die Dogmatik des Gefahrenbegriffs noch unten B.II.4.

noch vorliegen.“[79] Routinemäßige periodische Kontrollen durch den Datenschutzbeauftragten hat es nach Auskunft des BKA bislang nicht gegeben; wegen des zu erwartenden nicht unerheblichen Aufwands ist damit zu rechnen, dass solche Kontrollen jedenfalls nicht häufiger als alle zwei Jahre durchgeführt werden. Die Benachrichtigung Betroffener erfolgt nach dem in § 20w Abs. 1 Satz 1 Nr. 5, Abs. 2 und Abs. 3 BKAG geregelten Ausgangsfall auch dann, wenn sie zunächst zurückgestellt wird, binnen zwölf Monaten nach Beendigung der Maßnahme.[80] Danach ist eine weitere Verlängerung der Zurückstellung nur auf Grund gerichtlicher Anordnung möglich. Erst nach einem Zeitraum von fünf Jahren darf ggf. endgültig von der Benachrichtigung abgesehen werden. Innerhalb von fünf Jahren nach Beendigung der Maßnahme kann also immer noch eine Benachrichtigung nach § 20w Abs. 1 Satz 1 Nr. 5 BKAG erfolgen. Dann ist aber auch kein Grund ersichtlich, weshalb die Löschungsprotokolle vor Ablauf dieser Frist gelöscht werden sollten. Andernfalls droht strukturell die nach der zutreffenden Ansicht des BVerfG maßgebliche Gefahr, dass die Löschungsprotokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen nicht mehr vorliegen. Eine Löschungsfrist von fünf Jahren sollte daher erforderlich, aber – da es lediglich um eine typisierende Betrachtung geht – auch ausreichend sein.

Vor diesem Hintergrund könnte § 20j Abs. 3 BKAG etwa wie folgt geändert werden:

§ 20j

Rasterfahndung

[...]

(3) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. [2]Die getroffene Maßnahme ist zu dokumentieren. [3]Diese Dokumentation ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und **fünf Jahre nach der Beendigung der Maßnahme** zu vernichten. **[3]Ist über die Maßnahme nach Absatz 1eine Benachrichtigung des Betroffenen erfolgt, kann die Dokumentation nach Satz 2 bereits am Ende des Kalenderjahres, das dem Jahr der Benachrichtigung folgt, gelöscht werden.**

[...]

ii) Gefahrenschwelle

Daneben bietet sich eine regelungsklarere Gestaltung der Gefahrenschwelle in § 20j BKAG an. Vorschläge hierzu werden nach einer Analyse des parallel gelagerten Problems im Rahmen von § 20k BKAG formuliert.[81]

3. § 20k BKAG

a. Hintergrund und Ziele der Norm

§ 20k BKAG reagiert auf die Entwicklung, dass im Bereich terroristischer Bedrohungen, gerade im Phänomenbereich des internationalen Terrorismus, zunehmend moderne Technologien und vor allem Verschlüsselungen eingesetzt werden.[82] Dies gilt bereits für weit im Vorfeld liegende Phasen, in denen spätere Gefährder in Kontakt mit terroristischen Ideologien kommen, aber ebenso für spätere Phasen der Anschlagsplanung bis hin zur Koordination bei der Anschlagsrealisierung. Wegen des nicht selten jungen Alters der Gefährder – gerade auch im Bereich des islamistisch motivierten Terrorismus – wird sich die Tendenz zum Gebrauch der jeweils aktuellsten Technologien auf absehbare Zeit nicht ändern.

Die zunehmende Komplexität und Diversifizierung von Kommunikationskanälen und vor allem der immer weiter verbreiteten Verschlüsselungstechnologien führt dazu, dass Überwachungsmechanismen entweder immer umfassender oder immer näher an der Schnittstelle zwischen Mensch und Maschine ansetzen müssen, um noch effektiv zu sein. Dieser Logik folgend hat der Gesetzgeber in der Novelle des BKAG 2009 Befugnisse wie die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) nach § 20l BKAG und den verdeckten Zugriff auf

---

79 Siehe BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 272 (zunächst zu § 20v BKAG, aber mit anschließender Beziehung der Ausführungen auch auf § 20j Abs. 3 S. 3 BKAG).

80 Zur Benachrichtigungspraxis in den bisherigen § 4a-Lagen, siehe oben B.I.2.b.

81 Siehe unten. B.II.4.

82 Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 28.

informationstechnische Systeme nach § 20k BKAG („Online-Durchsuchung“) geschaffen. Beide Normen sollen eine Überwachungslücke schließen, die andernfalls auf Grund der zunehmenden Substitutierung klassischer Kommunikations- und Speichermedien durch solche Mittel droht, die sich nicht mehr mit konventionellen Mitteln überwachen lassen. Im Gegensatz zu Vorschriften der Telekommunikationsüberwachung soll § 20k BKAG gerade keine Eingriffe in das Fernmeldegeheimnis nach Art. 10 GG ermöglichen. Er ermächtigt vielmehr zu Eingriffen in das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 i. V. m. Art. 1 GG.

b. Verfassungskonformität

In seinem Urteil zum BKAG vom 20.4.2016 hat das BVerfG die Kompetenz zum Zugriff auf informationstechnische Systeme im Grundsatz als verfassungsgemäß bestätigt. Das gilt allerdings nur für die Befugnis als solche. Die konkrete Ausgestaltung wurde teils für verfassungswidrig erklärt, teils nur unter der Bedingung einer verfassungskonform einschränkenden Auslegung aufrechterhalten.

i) Verfahren (gerichtliche Anordnung)

Das Verfahren zur Anordnung einer Online-Durchsuchung durch ein Gericht[83] in § 20k Abs. 5 und Abs. 6 BKAG wurde für verfassungsgemäß erachtet. Dabei hat das BVerfG noch einmal betont, dass die Anordnungsdauer von drei Monaten keinen Regelzeitraum, sondern eine Obergrenze darstellt und die Anordnungsdauer im Einzelfall jeweils einer konkreten Verhältnismäßigkeitsprüfung bedarf.[84]

ii) Gefahrenschwelle

Zunächst hat das Gericht klargestellt, dass die in § 20k BKAG formulierte Gefahrenschwelle dahingehend auszulegen ist, „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.“ Dabei soll es genügen, wenn ein „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.“[85]

Diese Ausführungen lassen sich als Reaktion auf den Umstand verstehen, dass die Online-Durchsuchung zwar als sehr eingriffsintensive Maßnahme eingeschätzt wird, zugleich aber funktional ein Instrument auch der Gefahrerforschung ist. Daher soll nicht eine konkrete Gefahr im klassischen Sinn erforderlich sein, bei der das Schadensereignis bereits weitgehend konkretisiert ist. Vielmehr werden die Anforderungen insofern gelockert. Grundsätzlich wurde die Formulierung der Gefahrenschwelle vom Gericht als verfassungsgemäß eingestuft. Wie schon im Rahmen von § 20j BKAG[86] zeigt sich aber auch hier, dass es große Unsicherheiten im System des Gefahrenbegriffs gibt, die eine insgesamt konsistentere Formulierung jedenfalls der zentralen dogmatisch definierten Begriffe im BKAG nahelegen.[87]

iii) Schutz des Kernbereiches privater Lebensgestaltung

Die Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung in § 20k BKAG sind keiner verfassungskonformen Auslegung zugänglich und wurden für verfassungswidrig erklärt.

Das Gericht hat dabei zunächst festgehalten, dass die Anforderungen des Kernbereichsschutzes im Fall der Online-Durchsuchung – im Gegensatz etwa zur Wohnraumüberwachung – sich tendenziell stärker auf den Zeitraum der Daten*auswertung* als auf die Daten*erhebung* beziehen. Das hat seinen Grund darin, dass die Miterfassung kernbereichsrelevanter Daten auf Grund der Kernbereichsblindheit der Erhebungssoftware schlechterdings nicht ausgeschlossen werden kann.[88] Daher soll auf der Erhebungsebene ein Kernbereichsschutz nur so weit wie möglich erfolgen – sollten sich etwa einmal Softwarelösungen entwickeln lassen, mit deren Hilfe sich

---

[83] Zuständig ist nach § 20v Abs. 2 S. 1 BKAG das AG Wiesbaden.

[84] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 216.

[85] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 213.

[86] Siehe oben B.II.2.c.ii).

[87] Dazu ausführlich unten B.II.4.

[88] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 218 f.

bereits die Erhebung kernbereichsrelevanter Daten ausschließen ließe, so müssten sie auch eingesetzt werden.[89] Eine entsprechende Regelung sieht § 20k Abs. 7 Satz 2 BKAG vor, der vom Gericht als verfassungskonform bestätig wurde. Da ein entsprechend automatisierter Schutz auf Erhebungsebene bislang aber nicht möglich ist – und nach Einschätzung des BKA auch in absehbarer Zukunft nicht möglich sein wird[90] – verlagert sich der Schwerpunkt des Kernbereichsschutzes derzeit auf die Auswertungsebene.

In der Auswertungsphase sei insbesondere eine hinreichend unabhängige Kontrolle erforderlich, die „im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird."[91] Die Hinzuziehung von Bediensteten des BKA sei „zur Gewährleistung von ermittlungsspezifischem Fachverstand" möglich. Die Bediensteten dürften allerdings nicht federführend mit der Aufgabe betraut sein; die „tatsächliche Durchführung und Entscheidungsverantwortung" dürfe nicht in ihren Händen liegen.[92] Daher sind § 20 Abs. 7 Satz 3 und Satz 4 BKAG, die die Sichtung der Daten durch den Datenschutzbeauftragten und weitere Bedienstete des BKA regeln, verfassungswidrig. Die bisher vorgesehene bloße „Sachleitung" eines Gerichts genügt nicht. Im Übrigen sind die inhaltlichen Vorgaben zum Kernbereichsschutz in § 20k Abs. 7 BKAG (Verwertungsverbot und Löschungspflicht für Kernbereichsdaten, Dokumentation, Löschung der Dokumentation) verfassungskonform. In gewisser Parallele zu § 20j Abs. 3 Satz 3 BKAG hat das BVerfG allerdings die zu kurze Aufbewahrungsfrist der Löschungsprotokolle in § 20k Abs. 7 Satz 8 BKAG als verfassungswidrig verworfen.[93]

c. Normanwendung

Im Untersuchungszeitraum wurde die Online-Durchsuchung lediglich in einem Gefahrenabwehrvorgang angewendet (EG Komet). Es wurden gegen fünf Gefährder insgesamt sieben Anordnungen nach § 20k BKAG beantragt. Bei zwei Anträgen handelte es sich um Folgeanträge (zu jeweils verschiedenen Betroffenen), so dass effektiv von fünf verschiedenen Anordnungen auszugehen ist.[94] Das Amtsgericht Wiesbaden hat auf alle der gestellten Anträge hin entsprechende Anordnungen erlassen. In Folge von vier der Anordnungen wurde Software auf Zielsysteme aufgespielt. Nur eine der Anordnungen führte letztlich auch dazu, dass Daten von insgesamt zwei Zielsystemen (stationärer PC sowie Laptop) ausgeleitet wurden. Insgesamt wurden ca. 70.000 Inhalte erhoben.[95] Verfahrensrelevante Daten wurden dabei nicht erlangt.

Die sehr geringe Fallzahl macht es erneut schwierig, Aussagen zur Anwendungspraxis zu treffen. Allerdings kam es immerhin bereits zu Datenausleitungen und damit auch zu Maßnahmen des Kernbereichsschutzes, die auf ihre Gesetzes- und Verfassungskonformität überprüft werden und als Ansatzpunkt für die Skizzierung einer verfassungskonformen Praxis unter Beachtung der nunmehr vom BVerfG formulierten Anforderungen dienen können. An dieser Stelle ist freilich erneut auf die teilweise eingeschränkte Datenlage hinzuweisen.[96]

i) Ablauf von Online-Durchsuchungen

Das Vorgehen bei der Online-Durchsuchung wurde den Gutachtern von der zuständigen informationstechnischen Abteilung des BKA detailliert dargestellt. Bei der Online-Durchsuchung handelt es sich um eine relativ zeitaufwändige, vorbereitungsintensive und sensible Maßnahme. Für jeden Einzelfall wird eine spezielle Durchsuchungssoftware entwickelt, die erstens den ermittlungstaktischen Bedürfnissen und zweitens dem Umfang der gerichtlichen Anordnung angepasst wird. Die jeweilige Software ist auf die in der Anordnung gestatteten Möglichkeiten begrenzt. Ein Nachladen von Modulen ist nach Aussage BKA nicht möglich. Probleme stellen sich bisher vor allem beim Aufspielen der Software auf das Zielsystem. Nach derzeitiger Lage erfordert dies regelmäßig einen relativ aufwändigen und – technisch bedingt – nicht immer absolut zielgenauen Fernzugriff auf das Zielsystem.

---

89 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 219.

90 Nach Einschätzung des BKA ist es unmöglich, eine solche Software zu entwickeln, weil Wertungen und rechtliche Subsumtionen erforderlich sind, um eine Zuordnung zum Kernbereich vorzunehmen.

91 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

92 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

93 Zur Frage der Aufbewahrungsfristen für Löschungsprotokolle bei § 20j BKAG siehe oben. B.II.2.b.

94 Zur empirischen Ausgangslage insgesamt siehe oben B.I.3.b.ii).

95 Bei diesen Inhalten handelt es sich weitgehend um die von den Überwachungstools (Keylogger, Screencaptures) jeweils erhobenen Einzelergebnisse, also Vorgänge wie das Aufrufen bestimmter Programme oder Internetseiten sowie die dazugehörigen Maus- und Tastaturaktivitäten.

96 Siehe oben B.I.1.

(1) Umfang und Ziele

Zu einer vollständigen Spiegelung von Festplatten oder einem „Aufschalten“ auf das Zielsystem ist es bisher nicht gekommen. Auch eine Live-Betreuung im Sinn eines zeitechten Beobachtens der Vorgänge am Zielsystem durch Bedienstete des BKA hat nicht stattgefunden. Derart intensive und umfangreiche Zugriffe wurden laut BKA einerseits aus Verhältnismäßigkeitserwägungen unterlassen, andererseits aus ermittlungstaktischen Gründen – wird das Zielsystem auf Grund zu komplexer Aktivitäten der Überwachungssoftware ungewöhnlich ausgelastet, droht dies dem Nutzer aufzufallen und kann so zur Entdeckung der Überwachung führen. In den Anwendungen der Maßnahme im Untersuchungszeitraum wurde daher lediglich mit Keyloggern[97] und Screencaptures[98] gearbeitet. Ein Hauptziel der Online-Durchsuchungen war es, die auf dem Zielsystem eingegebenen Passwörter abzufangen, um mit diesen dann unbemerkt die Emailpostfächer der Betroffenen durchsuchen zu können. Für diese anschließende Durchsuchung erfolgt jeweils ein eigenständiger Beschluss; als Ermächtigungsgrundlage wird § 20l Abs. 1 BKAG herangezogen.

(2) Adressaten

In der Praxis hat sich gezeigt, dass die Online-Durchsuchung in etwa der Hälfte der Fälle auf Zielsysteme solcher Personen bezogen war, die nicht selbst im Verdacht standen, Gefährder zu sein. Der Sachverhalt lag in diesen Fällen aber so, dass es Anhaltspunkte dafür gab, dass potentielle Gefährder die informationstechnischen Systeme der im Übrigen unbeteiligten Personen nutzen und womöglich mittels dieser Systeme verfahrensrelevante Informationen austauschen oder verarbeiten würden. Ein solches Vorgehen lässt das Gesetz zu, weil es bewusst davon spricht, dass es um Eingriffe in „vom Betroffenen genutzte“ und nicht nur in ihm auch gehörende informationstechnische Systeme geht. Andernfalls wäre ein Instrument zur Online-Durchsuchung auch weitgehend wertlos. Insofern bestehen auch aus grundrechtlicher Sicht keine Bedenken, solange nur darauf geachtet wird, dass die von Unbeteiligten erhobenen, nicht verfahrensrelevanten Daten nicht genutzt und unverzüglich wieder gelöscht werden – unabhängig von etwaiger Kernbereichsrelevanz.

ii) Verhältnis zur Quellen-TKÜ

Die Online-Durchsuchung weist funktionale Ähnlichkeiten zur Quellen-TKÜ nach § 20l Abs. 2 BKAG auf. In beiden Fällen kommt es zum heimlichen Zugriff auf informationstechnische Systeme und zur Ausleitung von Daten.[99]

(1) Notwendigkeit der Abgrenzung

Auch wenn der Gutachtenauftrag auf § 20k BKAG beschränkt ist, ist eine Abgrenzung von Online-Durchsuchung und Quellen-TKÜ erforderlich. Denn nur wenn sich beide Instrumente hinreichend voneinander trennen lassen, ist gewährleistet, dass es nach Anordnung einer Quellen-TKÜ nicht zur faktischen Online-Durchsuchung kommt und umgekehrt. Schließlich soll die Regelung in unterschiedlichen Eingriffsnormen vor allem darauf reagieren, dass die Maßnahmen jeweils unterschiedliche Grundrechtseingriffe bedingen. Die Quellen-TKÜ zielt auf die Überwachung laufender Kommunikation (§ 20l Abs. 2 Satz 1 Nr. 1 BKAG) und ist daher allein an Art. 10 GG zu messen.[100] Die Online-Durchsuchung ist kein Mehr zur Quellen-TKÜ, sondern ermächtigt zum Zugriff auf alle auf einem informationstechnischen System gespeicherten oder verfügbaren Daten, die nicht Teil einer *laufenden* Kommunikation sind.[101] Sie ist daher allein am Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 i. V. m. Art. 1 GG, zu messen.

---

97 Hierbei handelt es sich um die Übertragung von Tastaturanschlägen, ggf. beschränkt auf solche Anschläge, die bestimmte zuvor definierte Bedingungen erfüllen. Diese Technik dient hauptsächlich der Ausleitung von Passwörtern. Grenzen für die Ausleitung von Kommunikationsinhalten oder sonstigen vom Nutzer verfassten Texten ergeben sich vor allem aus der nichtlinearen Arbeitsweise der meisten Nutzer.

98 Hierbei handelt es sich um Screenshots, die automatisch aufgenommen werden, wenn bestimmte zuvor definierte Bedingungen eintreten.

99 Die Quellen-TKÜ wurde im Untersuchungszeitraum siebenmal beantragt. Zu einer Ausleitung verfahrensrelevanter Daten kam es nicht. Vgl. auch oben Tabelle 4 unter B.I.3.a.

100 Vgl. BVerfGE 120, 274 (309).

101 Siehe hierzu auch die Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 28.

(2) Abgrenzbarkeit und Probleme

Um der grundrechtlichen Abgrenzung gerecht zu werden, müssen derzeit in der Praxis zwei vollständig separierte Überwachungstools entwickelt und verwendet werden. Die Schwierigkeit besteht vor allem darin, die Fähigkeiten der Tools jeweils entsprechend zu beschränken.

(a) Online-Durchsuchung

Auch bei der Online-Durchsuchung kann es (etwa über die Ausleitung von auf dem Zielsystem gespeicherten Chatprotokollen) zur Ausleitung von individuellen Kommunikationsinhalten kommen. Das ist auch unproblematisch, solange es nicht zur Erfassung der *laufenden* Kommunikation kommt. In einem Vermerk des BKA zur Online-Durchsuchung ist allerdings die Rede davon, dass das Ziel der Online-Durchsuchung nach § 20k BKAG darin liege, „Kommunikation zwischen den Störern" festzustellen. Insofern muss noch einmal betont werden, dass nach der aktuellen Gesetzeslage jedenfalls keine laufende Kommunikation erfasst werden darf. Insofern ist lediglich ein Zugriff auf die auf dem Rechner gespeicherten Inhalte vergangener Kommunikation zulässig.

Wegen der Verwendung von Screencaptures und Keyloggern ist es darüber hinaus möglich, dass faktisch auch Zugriffe auf vom Betroffenen aktuell bearbeitete Kommunikationsinhalte erfolgen (etwa Erfassen von Chateingaben über Keylogger oder Ausleitung von Screenshots bei geöffnetem Chat- oder Emailprogramm).[102] Dieser Effekt lässt sich zwar durch technische Vorkehrungen minimieren (Begrenzung der Screenshots auf bestimmte Bereiche des Bildschirms, Begrenzung des Keyloggings auf bestimmte Anwendungen oder Zeitfenster). Er lässt sich aber nicht vollständig ausschließen. Im Unterschied zur Software der Quellen-TKÜ ermöglichen allerdings die für die Online-Durchsuchung entwickelten Tools keine systematische Erfassung von Gesprächsinhalten bzw. von laufender Kommunikation. Insbesondere wird auch bei der Verwendung von Screencaptures und Keyloggern stets am Zielsystem selbst angesetzt und nicht auf dem Übertragungsweg der kommunikativen Inhalte nach der Absendung durch den Betroffenen. Für die Online-Durchsuchung ist also im Wesentlichen sichergestellt, dass lediglich die insofern verfassungsrechtlich zulässigen technischen Mittel und Wege der Datenerhebung genutzt werden.

(b) Quellen-TKÜ

Demgegenüber stellt sich das Problem der Abgrenzung ungleich schärfer im Rahmen der Quellen-TKÜ. Vor dem Hintergrund aktueller technischer Entwicklungen wird es immer schwieriger, dem verfassungsrechtlichen Gebot Rechnung zu tragen, dass mit der Software zur Quellen-TKÜ ausschließlich die laufende Kommunikation überwacht werden darf. Hier sehen gerade die operativen Einheiten im BKA ein zunehmendes Problem.

Denn diese Vorgabe hat in der Praxis erstens zur Konsequenz, dass das Überwachungstool jeweils speziell auf einzelne Kommunikationssoftwares zugeschnitten entwickelt werden muss, um die Erhebung nicht kommunikationsrelevanter Dateneingaben zu verhindern. Mit steigender technischer Komplexität, Diversität und Verschlüsselungsleistung moderner Kommunikationswege wird eine solche dienstespezifische Entwicklung von Tools aber immer aufwändiger. Die Entwicklung der Überwachungsmittel ist dann regelmäßig so arbeits- und zeitintensiv, dass sie bei Fertigstellung bereits veraltet sein können, weil die Nutzer inzwischen andere Dienste bevorzugen, die nach gänzlich anderer Software-Logik operieren (so dass sich auch eine Modifizierung oder Ergänzung der zunächst entwickelten Software nicht als Lösung anbietet). Auch der Zugriff auf die Service-Provider ist oft nicht vielversprechend. Denn da diese nicht selten im Ausland ansässig oder unseriös sind, ist die Kooperation zeitintensiv und schwierig.

Zweitens ist es oftmals technisch aufwändig oder unmöglich beim Zugriff auf die laufende Kommunikation keine gespeicherten Daten (etwa über vergangene Kommunikation, aber u. U. auch elektronische Adressbücher o. ä.) mitauszuleiten und mitzuerheben. Ob und in welchem Umfang solche technischen Bedingungen vorliegen, ist aus technischen Gründen – ggf. auch für die Dienste-Provider selbst – vor der Erhebung kaum abzusehen. Es droht also strukturell zu Fällen zu kommen, in denen bei Maßnahmen der Quellen-TKÜ faktische Online-Durchsuchungen in Bezug auf abgeschlossene Kommunikationen stattfinden müssten, um auf solche Kommunikationsdaten zugreifen zu können. Zwar sind nach dem BKAG beide Maßnahmen zur Gefahrenabwehr

[102] Im Rahmen der EG Komet kam es zu Screenshots bei der Benutzung von Emailprogrammen und auch zum Abgreifen von Informationen über die Internetnutzung des Betroffenen – etwa die bei der Registrierung für eine muslimische Partnerbörse eingegebenen Daten.

Das Aufrufen von Internetseiten als solches, das mittels der bei der Online-Durchsuchung eingesetzten Screencaptures und Keyloggern ebenfalls überwacht werden kann, ist dagegen nicht Teil der von Art. 10 GG geschützten Individualkommunikation, s. Durner, in: Maunz/Dürig, GG-Kommentar, Stand: 77. EL Juli 2016, Art. 10 Rn. 51, 92; vgl. auch BVerfGE 115, 166 (182); 120, 274 (340 ff.).

zulässig. Doch ergeben sich jeweils unterschiedliche Anforderungen, insbesondere in Hinblick darauf, welche Maßnahmen zum Kernbereichsschutz erforderlich werden. Auch bestehen Unsicherheiten in Beweisverwertungsfragen für anschließende Strafverfahren, weil eine Maßnahme zur Online-Durchsuchung in der StPO nicht vorgesehen ist.

Ob die Software zur Quellen-TKÜ vor diesem Hintergrund den verfassungsrechtlichen Vorgaben gerecht wird, ist nicht Gegenstand dieses Gutachtens.[103] Beruhend auf den Schilderungen der informationstechnischen Abteilung des BKA kann man zumindest davon ausgehen, dass die Software der Online-Durchsuchung sich so zuschneiden lässt, dass eine systematische Überwachung laufender Kommunikation ausgeschlossen wird. Es ist folglich eine Frage des Einzelfalls, ob diese Voraussetzungen erfüllt werden. Das Problem liegt eher darin, dass der Aufwand zur Einhaltung derart hoch ist, dass er für den Einsatz von Maßnahmen nach § 20l Abs. 2 BKAG eine prohibitive Wirkung zu entfalten droht.[104]

(3) Ausblick

Das Problem der Abgrenzung des Fernmeldegeheimnisses nach Art. 10 GG vom Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. Art. 1 GG wird sich immer drängender stellen. In der Sache wird es dabei vor allem um die Frage gehen, ob für die Unterscheidung von laufender Kommunikation und gespeicherten Daten technisch-formale Kriterien wie etwa der Speicherort der Kommunikationsdaten (u. a.: Arbeitsspeicher/Festplattenspeicher) oder aber ein eher funktional-phänomenologischer Ansatz (wann geht es in der Sache/ dem Erscheinungsbild nach um laufende Kommunikation?) entscheidend sein sollten.

Eine genaue Definition dessen, was mit „laufender Kommunikation“ gemeint und wie sie zu bestimmen ist, wurde bislang in Rechtsprechung und Literatur nicht erarbeitet.[105] In dieser Frage wird in der Zukunft eine juristische Diskussion erforderlich sein, an deren Ende eine Neuausrichtung der Dogmatik zu Art. 10 GG stehen könnte. Erst dann lässt sich verlässlich abschätzen, wie insbesondere neuartige Mischphänomene wie der Austausch über die gemeinsame Bearbeitung eines von einem Cloud-Provider zur Verfügung gestellten elektronischen Textdokuments oder die automatisierte, nicht zu verhindernde Mitausleitung von Inhalten vergangener Kommunikation bei bestimmten Chat-Diensten zu bewerten sind.

Insofern ist es nach wie vor nicht undenkbar, die Dogmatik möglichst in Parallele zum Umgang mit analogen Vorgängen (wie etwa dem klassischen Briefverkehr) weiter zu entwickeln. Ein Zugriff auf die laufende Kommunikation und damit ein Problem von Art. 10 GG wären bei einer solchen Betrachtung nur Vorgänge, die sich abspielen, nachdem der Kommunikationsinhalt aus dem Machtbereich des Urhebers entlassen wurde (also etwa eine Email/ Chatnachricht auch abgeschickt wurde). Andererseits ließe sich ein eher phänomenologischer Ansatz verfolgen, der darauf abstellt, welche Daten auf einen laufenden Kommunikationsvorgang bezogen und vom Nutzer solchen Vorgängen gewidmet sind.

Als alternativer Ausweg könnte es sich womöglich anbieten, in den Vorschriften zur Quellen-TKÜ vorzusehen, dass die automatische Mitausleitung bestimmter, nicht per se der laufenden Kommunikation zuzuordnender, Daten ebenfalls von der Ermächtigung umfasst wird („Quellen-TKÜ plus“).

Mehr als solche ersten Ansatzpunkte können aber in diesem Gutachten nicht angeboten werden. Eine Lösung kann hier nur angedeutet werden. Es handelt sich um ein Problem, das primär § 20l BKAG betrifft und einer eigenständigen Untersuchung bedürfte. Hier geht es allein um eine Bewertung von § 20k BKAG.

iii) Verfahren, gerichtliche Zuständigkeiten und formelle Anforderungen

Das Erfordernis der Beantragung von Online-Durchsuchungen durch die Behördenleitung (§ 20k Abs. 5 BKAG) ist in der Praxis unproblematisch, zumal es funktional verstanden und gehandhabt wird, d. h. wie in § 20k BKAG vorgesehen kann der Behördenleiter sich bei der Anordnung, etwa durch die Vizepräsidenten des BKA oder bei deren Abwesenheit durch den dienstältesten Abteilungsleiter, vertreten lassen.[106]

---

[103] Ein vom BSI anerkanntes, externes Prüflabor hat eine Software- und Quellcodeprüfung der Quellen-TKÜ-Software durchgeführt und ist zum Ergebnis gekommen, dass die Software rechts- und SLB-konform ist.

[104] Zu den geringen Einsatzzahlen der Instrumente nach § 20k und § 20l Abs. 2 BKAG vgl. wiederum Tabelle 4 unter B.I.3.a.

[105] Vgl. BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 234, wo die Bedeutung der Beschränkung auf Eingriffe in die „laufende Kommunikation“ betont, aber nicht näher beschrieben wird, wann es sich (noch) um solche handelt.

[106] Vgl. hierzu Schenke, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 20k Rn. 36.

Nach § 20v Abs. 2 Satz 1 BKAG ist das AG Wiesbaden für die Anordnung von Online-Durchsuchungen zuständig. Nach Auskunft des BKA wurde vor dem Erlass von § 20k BKAG erwogen, die Anordnungszuständigkeit eingedenk der besonderen Eingriffstiefe auf den Ermittlungsrichter beim BGH zu verlagern. Daneben wurde auch eine Vermittlung der Anordnung durch den Generalbundesanwalt angedacht. Letzterer Gedanke ist allerdings in Übereinstimmung mit dem BKA abzulehnen, weil eine Beteiligung des Generalbundesanwalts bei der Anordnung der gefahrenabwehrrechtlichen Maßnahme nach § 20k BKAG eine systemwidrige Vermengung von Gefahrenabwehr und Strafverfolgung bedeutete. Die Verlagerung der Anordnungszuständigkeit auf den Ermittlungsrichter beim BGH hingegen erscheint durchaus sinnvoll. Auf diese Weise ließe sich ein angemessenes institutionelles Gegengewicht zu dem die Anordnung beantragenden Präsidenten des BKA (oder seines Vertreters) sicherstellen. Entscheidet man sich für diesen Schritt, müsste allerdings auch erwogen werden, die Anordnungsbefugnis für ähnlich gewichtige Maßnahmen, etwa § 20j BKAG, entsprechend zu verlagern.

Die vom Amtsgericht Wiesbaden im Untersuchungszeitraum ergangenen insgesamt sieben Anordnungen entsprachen weitgehend den formalen Vorgaben des § 20k Abs. 6 BKAG. Die Anordnungen waren dabei regelmäßig personenbezogen ausgestaltet, d.h. sie umfassten mehrere Zielsysteme der selben Person. Zu einer der Anordnungen allerdings ließ sich lediglich eine Kurzfassung finden, d. h. keine Version, die die tragenden Gründe enthielt. Nach Auskunft des BKA wurde in diesem Fall ein Beschluss mit Gründen nicht ausgestellt. Soweit diese Auskunft zutrifft, hat das AG Wiesbaden in diesem einen Fall gegen das Erfordernis aus § 20k Abs. 6 Satz 2 Nr. 4 BKAG verstoßen, in der Anordnung die wesentlichen Gründe anzugeben.

iv) Anordnungsdauer

Die maximale Dauer von drei Monaten je Anordnung ist aus Sicht des BKA ausreichend. Sie wurde in allen im Untersuchungszeitraum ergangenen Anordnungen ausgeschöpft; schon auf Grund der sehr niedrigen Fallzahl kann hieraus aber nicht der Schluss gezogen werden, das Amtsgericht Wiesbaden habe keine hinreichende Einzelfallprüfung vorgenommen und den Rahmen der Anordnungsdauer stets pauschal ausgeschöpft.

v) Eilfälle

Wie auch im Fall der Rasterfahndung nach § 20j BKAG sieht das BKA keinen Bedarf für die Regelung eines Eilverfahrens bei Gefahr im Verzug.[107] Schon weil die Überwachungssoftware für jeden Einsatz bedarfsgerecht neu programmiert werden muss und das Aufspielen der Software sehr aufwändig ist, ist die Online-Durchsuchung ein sehr zeit- und vorbereitungsintensives Instrument. Jedenfalls solange sich daran nichts ändert, ist eine Eilregelung nicht erforderlich. Eine solche wäre lediglich für das Szenario hilfreich, in dem zum Ende eines bereits laufenden Anordnungszeitraums, in dem ein einzelfallgerechtes Tool zwar bereits entwickelt, aber noch nicht benutzt wurde, sich erst kurzfristig Umstände ergeben, die eine Online-Durchsuchung sinnvoll erscheinen lassen. Dieses Szenario ist aber nach Einschätzung des BKA derart unwahrscheinlich, dass es am grundsätzlich fehlenden Bedarf für eine Eilregelung nichts ändert.

vi) Gefahrenschwelle

Ähnlich wie auch bei § 20j BKAG ist die Formulierung der Gefahrenschwellen in § 20k Abs. 1 BKAG übermäßig komplex und unübersichtlich geraten. Da die verschiedenen Eingriffsnormen im BKAG jeweils an verschiedene verfassungsgerichtliche Entscheidungen zu den jeweiligen Sachbereichen anknüpfen, sind die konkreten Formulierungen zudem von Norm zu Norm unterschiedlich, was die Systembildung und Orientierung im Gesetz erheblich erschwert und zu der Fehlvorstellung führen kann, mit jeder unterschiedlichen Formulierung müsse sich auch ein unterschiedlicher normativer Gehalt verbinden. So wurde etwa § 20k Abs. 1 Satz 2 BKAG in internen Dokumenten des BKA unzutreffend dahin ausgelegt, er würde die Erforderlichkeitsanforderungen senken. Allenfalls kann § 20k Abs. 1 Satz 2 BKAG aber den Effekt haben, die Anforderung an die Gefahrenschwelle zu senken.

[107] Eine entsprechende Eilregelung war im Gesetzgebungsverfahren ursprünglich noch vorgesehen, s. die Regierungsbegründung, Bundestagsdrucksache 16/10121, S. 10. Vgl. auch Bundestagsdrucksache 16/11391, S. 2.

Aus Sicht des BKA ist die Norm zwar letztlich handhabbar, was vor allem an der institutionalisierten Einbindung des Rechtsreferats liegt. Im Laufe der Untersuchung wurde aber der Eindruck gewonnen, dass es sich bei § 20k BKAG wie bei § 20j BKAG jedenfalls für die operativen Einheiten um eine zumindest nicht besonders klare oder leicht handhabbare Norm handelt. Auch die Beurteilung der Anwendungspraxis legt daher nahe, eine insgesamt konsistentere Formulierung jedenfalls der zentralen dogmatisch definierten Begriffe im BKAG in Angriff zu nehmen.[108]

vii) Anwendungshindernisse und mögliche Lösungen

Die Online-Durchsuchung dient wie die Quellen-TKÜ dazu, die Eingriffsbefugnisse der Sicherheitsbehörden den modernen technischen Entwicklungen anzupassen. Allerdings lässt sich die Maßnahme bislang kaum effektiv oder zielgenau anwenden, wie schon die geringe Fallzahl zeigt. Nach Aussage des BKA hat sich mehrfach der Fall ereignet, dass eine Maßnahme nach § 20k BKAG erwogen, dann aber auf Grund technischer Schwierigkeiten letztlich nicht ergriffen wurde. Das Hauptproblem in der Praxis liegt darin, die Überwachungssoftware treffsicher auf teils hochkonspirativ genutzte Zielsysteme aufzuspielen.[109] Bislang ist dafür ein aufwändiges Hacking ohne Hardwarekontakt erforderlich.

Da alle Hinweise dafür sprechen, dass das BKA von der Befugnis nur sehr zurückhaltend und mit grundrechtlichem Verantwortungsbewusstsein Gebrauch macht und die Befugnis grundsätzlich verfassungsgemäß sowie politisch gewollt ist, sollte nach Wegen gesucht werden, so weit wie möglich auf die derzeit bestehenden Anwendungshindernisse zu reagieren.

(1) Wohnungsdurchsuchung

Zur Wohnungsbetretung oder gar -durchsuchung zum Zwecke des Aufbringens von Überwachungssoftware ermächtigt § 20k BKAG entgegen einiger im Vorfeld zur Entscheidung des BVerfGs vom 20. April 2016 vorgetragener Befürchtungen[110] eindeutig nicht. Ein Recht zur Wohnungsbetretung lässt sich auch nicht als Annexkompetenz in § 20k BKAG hineinlesen.[111] Davon geht auch das BKA aus.

Zudem würde ein reines Betretungsrecht nicht ausreichen, da die Zielsysteme häufig mobiler Natur und in der Wohnung verborgen sein können. Das gilt umso mehr, als es regelmäßig mehrere und im Zuge der technischen Entwicklung auch immer kleinere Endgeräte geben wird, die meist nicht offen in der Wohnung liegen, sondern eher in Schubladen o. ä. verstaut sein werden. Erforderlich wäre daher eine Durchsuchungsbefugnis im Sinn von Art. 13 Abs. 2 GG.

Aus Sicht des BKA ist ein solches Durchsuchungsrecht sehr wünschenswert. Es würde dem BKA zumindest eine zusätzliche Handlungsoption eröffnen, um die Überwachungssoftware auf Zielsysteme von Betroffenen aufzuspielen.

Darüber hinaus könnte ein Wohnungsdurchsuchungsrecht zum Zweck der Aufspielung von Überwachungssoftware nicht nur aus einer Effektivitätsperspektive einen Gewinn darstellen. Vielmehr würde das Aufspielen der Software in solchen Fällen auch sehr viel zielgenauer erfolgen können. Das einem Hacking ohne Hardwarekontakt anhaftende Streuungsrisiko würde auf diese Weise ausgeschlossen.[112] Auch wenn eine solche zweckgebundene Durchsuchungskompetenz einen neuartigen Eingriff in das Grundrecht des Betroffenen aus Art. 13 GG mit sich brächte, könnten sich im Hinblick auf den Schutz der Grundrechte Unbeteiligter Vorteile ergeben.

Vor diesem Hintergrund ist es grundsätzlich zu empfehlen, das BKA dazu zu ermächtigen, Wohnungen der Betroffenen zu dem Zweck zu betreten und zu durchsuchen, die für eine Überwachung nach § 20k BKAG erforderliche Software aufzubringen.[113]

---

[108] Dazu unten B.II.4.

[109] Dieses Problem stellt sich ebenso im Rahmen der Quellen-TKÜ nach § 20l Abs. 2 BKAG und es würde sich ebenso im Rahmen einer u. U. neu zu schaffenden einheitlichen Überwachungsbefugnis („Quellen-TKÜ plus“) stellen.

[110] Siehe die Verfassungsbeschwerde des Gerhart Baum u. a. vom Verfassungsbeschwerde Baum u. a. aus dem Jahr 2009, S. 26 f. (http://www.schweigepflicht-online.de/BKAG%20Beschwerdeschrift%20Presseversion.pdf).

[111] Hierzu etwa Soiné, NVwZ 2012, 1585 (1588 f.). Zu notwendigen Begleitmaßnahmen im Rahmen von § 100c BKAG vgl. auch BGHSt 46, 266.

[112] Aktuell ist Aufbringen am Zielsystem nur über die Infizierung via Datenaustausch über das Internet möglich.

[113] Zu den bei einer entsprechenden Änderung zu bedenkenden Aspekten näher noch unten B.II.3.e.ii).

(2) Umleitung von Datenströmen

Als weiteres Mittel, das insbesondere ein zielgenaues Aufspielen von Überwachungssoftware ermöglichen könnte, kommt eine Verpflichtung der Access-Provider zur Umleitung von Proxy-Server-Datenströmen in Betracht. Für eine solche Maßnahme würde das BKA im Rechenzentrum des Providers (z. B. Telekom) temporär eine spezielle Rechner-/Servereinheit bereitstellen, die mit dem Netzwerk des Providers verbunden wird. Der Provider konfigurierte sein Netzwerk so, dass der Datenstrom des überwachten Telekommunikationsanschlusses über die bereitgestellte Rechner-/Servereinheit als Zwischeninstanz weitergeleitet wird. Dadurch, dass die Einheit an dieser Position im Netzwerk den eingehenden Datenstrom entgegennähme und weiterleitete, könnte der Inhalt des Datenstroms verändert werden – etwa dergestalt, dass ein über den überwachten Telekommunikationsanschluss angeforderter Download einer ausführbaren Datei durch die Einheit kurzzeitig angehalten, die ausführbare Datei (z. B. Adobe Flash Player) durch eine zuvor durch das BKA präparierte ausführbare Datei (im Beispiel Adobe Flash Player erweitert um Überwachungssoftware) ausgetauscht und schließlich der Download mit der nun veränderten ausführbaren Datei fortgesetzt wird (Vorgang erfolgt automatisiert und bedarf keines Benutzereingriffs). Von der Umleitung wäre ausschließlich der Netzwerkverkehr des überwachten Anschlusses betroffen. Zum Aufspielen der Software wäre eine Kenntnisnahme von persönlichen Inhalten der Benutzer durch Beamte des BKA nicht erforderlich.

Allerdings gibt es auch mit Blick auf die Umleitung von Datenströmen einige Unsicherheiten. So ist aus Sicht des BKA eine nicht unerhebliche Manipulation von Datenströmen erforderlich, um das Aufbringen von Überwachungssoftware auf einzelne Zielsysteme zu ermöglichen. Überdies ist bislang unklar, unter welchen Bedingungen eine solche Umleitung bei welchen Access-Providern technisch möglich ist. Zudem müssten die Provider zum Stillschweigen verpflichtet werden. Daher stellt die Installation von Überwachungssoftware per Hardwarekontakt jedenfalls die vielversprechendere Variante dar.

Gleichwohl sollte der Gesetzgeber aus Effektivitäts- und Konsistenzgründen der Frage weiter nachgehen, ob nicht zusätzlich zum Wohnungsbetretungsrecht auch eine Befugnis zur Umleitung von Datenströmen geschaffen werden sollte.

viii) Verhältnismäßigkeit

Die Befugnis zur Online-Durchsuchung als solche wurde vom BVerfG zutreffend als verfassungskonform, also auch als verhältnismäßig, beurteilt. Die bisherige Handhabung der Vorschrift durch das BKA liefert keine Hinweise auf eine unverhältnismäßige Handhabung im Einzelfall. Insbesondere hat die empirische Untersuchung gezeigt, dass es nicht zu einer wahllosen Streuung von Maßnahmen gekommen ist, sondern vielmehr zu nur einigen wenigen § 4a-Lagen, die dann jeweils durch relativ intensive Ermittlungen und Eingriffe gekennzeichnet waren.[114] Mit Blick auf § 20k BKAG zeigen bereits die geringe Fallzahl und die zeitliche Dauer der Maßnahmen, dass man insbesondere das Erforderlichkeitskriterium sehr ernst nimmt.[115] Auch in den internen Unterlagen des BKA zeigt sich, dass man dort das Instrument der Online-Durchsuchung als *ultima ratio* ansieht.

ix) Kernbereichsschutz

Wie gesehen wurden die Regeln zum Kernbereichsschutz in § 20k Abs. 7 BKAG zu Recht weitgehend als unzureichend verworfen.[116] Schon aus diesem Grund war auch die bisherige Normanwendungspraxis auf Ebene der Einzelmaßnahmen verfassungswidrig.

(1) Praktische Erfahrungen mit dem Kernbereichsschutz

Grund für die Verfassungswidrigkeit war insbesondere die nicht hinreichende Unabhängigkeit der für den Kernbereichsschutz zuständigen Stelle. Mit Blick auf die technischen Abläufe, den Arbeitsaufwand etc. kann die bisherige Handhabung aber durchaus richtungweisend für eine künftige verfassungsgemäße Praxis des Kernbereichsschutzes sein.

---

114 Siehe oben B.I.2 und B.I.3.

115 Siehe oben Tabelle 5 unter B.I.3.b.ii).

116 Siehe oben B.II.3.b.iii).

Nach den Erfahrungen im Rahmen der im Untersuchungszeitraum einzigen erfolgreichen Online-Durchsuchung (Datenausleitung von zwei Zielsystemen) handelt es sich bei den Maßnahmen zum Kernbereichsschutz in der Auswertungsphase um ein sehr aufwändiges Verfahren. Zur Verdeutlichung sei angeführt, dass nach den bisherigen Erfahrungen etwa ein Kernbereichsinhalt auf ca. 70.000 überprüfte Inhalte kam.[117] Die Dokumentation der Prüfung umfasst 11 Aktenordner. Das bedeutet auch, dass es mit den bisherigen Ressourcen kaum möglich sein dürfte, mehrere Maßnahmen der Online-Durchsuchung gleichzeitig zu verfolgen.

Wo immer es geht, lässt sich freilich auf technische Hilfsmittel zurückgreifen, auch wenn sich die Kernaufgabe der juristischen Bewertung der Inhalte nicht automatisieren lässt. So hat das BKA eigens eine spezielle Software entwickelt, um die Administration und Protokollierung der bisher erforderlichen, händisch durchgeführten Kernbereichsanalyse im Rahmen der im Untersuchungszeitraum einzigen Online-Durchsuchung zu ermöglichen. Diese Software hat sich aus Sicht der beteiligten Personen als sehr hilfreich erwiesen.

(2) Umsetzung der „Sachleitung" durch das Amtsgericht Wiesbaden

Der künftig nicht mehr interessierende Begriff der Sachleitung[118] ist dahingehend auszulegen, dass er mindestens eine effektive Einwirkungsmöglichkeit des Gerichts während des Auswertungsverfahrens voraussetzt. Denn andernfalls lässt sich nicht von einer „Leitung" sprechen. Die vergangene praktische Handhabung von § 20k Abs. 7 Satz 3 BKAG wird dem so verstandenen Sachleitungserfordernis noch gerecht. In der Praxis hat das Amtsgericht Wiesbaden zunächst abstrakte Leitlinien für die Kernbereichsanalyse formuliert. Hinzu kamen stichprobenartige Kontrollen, die Abklärung von Zweifelsfällen sowie eine abschließende Überprüfung der BKA-internen Dokumentation durch das Gericht. Zwar fand die Kernbereichsanalyse in den Räumen des BKA in Berlin statt, was die faktischen Einwirkungsmöglichkeiten des Gerichts auf den Ablauf der Analyse notwendig begrenzen musste. Richter des Amtsgerichts Wiesbaden waren allerdings in den Räumlichkeiten – zwar lediglich punktuell, aber immerhin mehrfach – zugegen. Vor diesem Hintergrund und eingedenk der Vorgabe von Leitlinien und der Absicherung der letztlichen Kontroll- und Entscheidungshoheit lag immerhin die inhaltliche Steuerung in der Sache beim Amtsgericht Wiesbaden. Daher war der Ablauf der Kernbereichsanalyse derart gestaltet, dass sich noch von einer „Sachleitung" des Gerichts (§ 20k Abs. 7 Satz 3 BKAG) sprechen lässt.

(3) Gesetzeswidrigkeit der bisherigen Praxis

In anderen Teilen allerdings ist die bisherige Praxis nicht nur als verfassungswidrig, sondern auch als gesetzeswidrig, d. h. nicht mit § 20k Abs. 7 BKAG konform, zu beurteilen.

So wurde nach einem Vermerk in den Akten des BKA im Rahmen der Kernbereichsanalyse der Begriff des Kernbereichs privater Lebensgestaltung sowohl von den an der Auswertung beteiligten Ermittlungsbeamten des BKA als auch vom Amtsgericht Wiesbaden dahingehend ausgelegt, dass er solche Vorgänge nicht umfasse, die allgemein üblich sind und sich für gewöhnlich bei jedermann ereignen können. Denn solche Vorgänge könnten gerade wegen ihrer Alltäglichkeit und damit Banalität nicht hinreichend für die Persönlichkeitsbildung oder -entfaltung bedeutsam sein. Dieser Definition entsprechend wurden auf dem Zielsystem aufgerufene pornographische Inhalte nicht als kernbereichsrelevant eingestuft. Der ebenfalls beteiligte Datenschutzbeauftragte des BKA teilte diese Einschätzung des BKA und des AG Wiesbaden zu Recht nicht. Abgesehen von der zu Grunde gelegten tatsächlichen Annahme ist auch die Auslegung des Kernbereichsbegriffes unzutreffend, da die allgemeine Üblichkeit einer Verhaltensweise nichts über ihre Bedeutung für die höchstpersönlichen, fundamentalen Fragen der eigenen Lebensgestaltung besagt. Auch vertrauliche Gespräche im engsten Familienkreis sind einerseits verbreitet und alltäglich, fallen aber andererseits in den Kernbereich privater Lebensgestaltung.

Auch die in einer internen Richtlinie des BKA zu findende Überlegung, der Kernbereich sei nicht betroffen, soweit das fragliche Datum „verfahrensrelevant" ist, bedarf zumindest der Klarstellung. Jedenfalls kann damit nicht gemeint sein, dass ein Datum sich nur irgendwie für das Verfahren, etwa auch zu Gefahrenabwehrmaßnahmen, verwerten lassen muss, um verfahrensrelevant zu sein. Andernfalls nämlich könnte ein Datum bspw. gerade deshalb aus dem Kernbereich herausfallen, weil es sich dazu eignete, den Betroffenen unter Verwendung von Daten aus seiner Intimsphäre in seinem Umfeld zu diskreditieren und dadurch eine von ihm ausgehende

[117] Dabei handelte es sich um 6 Screenshots von Emails, in denen vermutlich die Schwester des potentiellen Gefährders Ausführungen über ihr privates Beziehungsleben machte.

[118] Zur verfassungsrechtlichen Unzulänglichkeit einer bloßen Sachleitungsregelung siehe oben B.II.3.b.iii).

Gefahr zu bekämpfen. Genau eine solche Instrumentalisierung höchstpersönlicher Informationen durch staatliche Behörden will Art. 1 Abs. 1 GG aber vermeiden.

d. Zwischenfazit zu § 20k BKAG

i) Grundsätzlicher Bedarf für die Regelung

Trotz der geringen Fallzahl ist eingedenk des immer schneller voranschreitenden technischen Fortschritts davon auszugehen, dass eine Regelung wie § 20k BKAG notwendig ist, um die Sicherheitsbehörden in die Lage zu versetzen, mit der Entwicklung der technischen Ausstattung potentieller Gefährder Schritt zu halten.

ii) Verfassungskonformität

Die grundsätzliche Befugnis zur Online-Durchsuchung ist verfassungsgemäß. Die bisherige Ausgestaltung des Kernbereichsschutzes in § 20 k Abs. 7 BKAG ist allerdings verfassungswidrig; dazu gehört insbesondere auch die zu kurze Dauer der Aufbewahrung von Löschungsprotokollen.

iii) Auslegungsfragen

§ 20k BKAG eröffnet keine komplizierten Auslegungsfragen. Allerdings ist insbesondere die Formulierung der Gefahrenschwellen überkomplex und unübersichtlich geraten und erschwert die Handhabung der Norm.

iv) Normanwendung

Die bisherige Anwendung von § 20k BKAG teilt naturgemäß die Verfassungswidrigkeit im Hinblick auf den dort nur unzureichend gewährten Kernbereichsschutz. Als verfassungswidrig erwies sich allerdings auch das Verständnis des Kernbereichs der privaten Lebensgestaltung, auch wenn das BKA in diesem Verständnis – entgegen dem eigenen Datenschutzbeauftragten – durch das AG Wiesbaden fälschlicher Weise bestätigt wurde.

Als größtes Effektivitätsproblem in der Anwendungspraxis erweisen sich Design und Aufspielen der Überwachungssoftware auf die zu überwachenden Zielsysteme.

e. Änderungsvorschläge

i) Gefahrenschwellen

Es bietet sich vor allem eine regelungsklarere Gestaltung der Gefahrenschwelle in § 20k BKAG an. Da sich das gleiche Problem im Rahmen von § 20j BKAG stellte, werden Vorschläge hierzu in einer nachgelagerten übergreifenden Analyse formuliert.[119]

ii) Wohnungsdurchsuchung[120]

Eine Kompetenz zur Infiltration informationstechnischer Systeme in der Wohnung des Betroffenen müsste wie gesehen erstens zur Durchsuchung (und nicht nur zur bloßen Betretung) ermächtigen, da die Zielsysteme sich meist nicht nach bloßer Umschau in der Wohnung auffinden lassen werden.

Zweitens muss die Durchsuchung heimlich erfolgen dürfen. Daher ist auch nach derzeitiger Rechtslage der Rückgriff auf § 20t BKAG keine Lösung, weil § 20t i. V. m. § 46 Abs. 2 BPolG nur die offene Durchsuchung (mit Benachrichtigung des Adressaten) vorsieht. Drittens darf die Durchsuchung ausschließlich dem Zweck dienen, die Überwachungssoftware auf das Zielgerät aufzuspielen. Andernfalls drohte die Systematik des Durchsuchungsrechts unterlaufen zu werden, das Wohnungsdurchsuchungen grundsätzlich nur als offene Maßnahmen erlaubt.[121]

Überdies würde sich die Frage der Gerichtszuständigkeit stellen. Bei heimlichen Maßnahmen, auch bei der zweckgebundenen heimlichen Wohnraumdurchsuchung, ist die Anordnungszuständigkeit dem Gericht zuzuweisen, in dessen Bezirk die beantragende Behörde ihren Sitz hat. So gilt auch bei der heimlichen Wohnraumüberwachung nach § 20h BKAG die reguläre Regelung der örtlichen Zuständigkeit nach § 20v Abs. 1

---

[119] Siehe unter B.II.4.

[120] Vgl. bereits oben B.II.3.c.vii)(1). Zu landesrechtlichen Durchsuchungsrechten zum Zwecke der Installation technischer Mittel in Wohnungen vgl. § 15 Abs. 5 HessSOG sowie den inzwischen aufgehobenen Art. 34e BayPAG.

[121] Vgl. § 20t BKAG i.V.m. § 46 Abs. 2 BPolG; § 106 StPO.

Satz 2 BKAG.[122] Die Zuständigkeit für ein potentielles Wohnungsdurchsuchungsrecht zum Zwecke der Installation von Überwachungssoftware sollte daher ebenfalls beim AG Wiesbaden liegen.

Es ist nicht zu übersehen, dass es sich bei einem solchen Recht zur heimlichen Wohnungsdurchsuchung um einen erheblichen Eingriff in das Recht auf Unverletzlichkeit der Wohnung nach Art. 13 GG handeln würde. Die Einhaltung der gesetzlichen und verfassungsrechtlichen Vorgaben im Einzelfall wäre von höchster Bedeutung. Daher verstehen sich die hier befürworteten Vorschläge zur Erweiterung der technischen Möglichkeiten zur Einleitung einer Online-Durchsuchung unter der Bedingung einer Fortentwicklung der Evaluationspflicht, die besonders auch die oben gemachten Vorschläge zur verbesserten Dokumentation aufgreift.[123] Wollte man also ein Durchsuchungsrecht schaffen, sollte in einem gewissen zeitlichen Abstand eine Nachevaluation erfolgen, um den Umgang mit der neuen Befugnis zu beurteilen und um insbesondere zu überprüfen, ob sich die erhofften Vorteile auch tatsächlich einstellen würden.

Schließlich ist zu bedenken zu geben, dass die zunehmende Verlagerung von Kommunikation und Datenverarbeitung auf mobile Endgeräte das Aufspielen von Überwachungssoftware in einer Weise erschwert, die auch mittels Wohnungsdurchsuchungen nicht ohne Weiteres behoben werden kann. Schließlich befinden sich mobile Endgeräte meist weitgehend ununterbrochen in unmittelbarer Nähe des Nutzers.

iii) Umleitung von Datenströmen

Entschiede sich der Gesetzgeber dazu, eine Kompetenz zur Umleitung von Datenströmen zu schaffen, wären zumindest eine Anpassung von § 110 TKG und die Schaffung einer auf diesen verweisende Scharniernorm im BKAG erforderlich.

iv) Datenerhebung und Kernbereichsschutz

Zentraler Kritikpunkt und Grund für die weitgehende Verfassungswidrigkeit von § 20k BKAG war die unzureichende Regelung zum Schutz des Kernbereichs privater Lebensgestaltung.[124] Dabei verwundert es nicht, dass die Frage dieses Schutzes im Rahmen von § 20k BKAG eine besondere Rolle spielt. Denn informationstechnische Systeme werden meist zu einer sehr umfänglichen Datenspeicherung und -verarbeitung genutzt und enthalten daher regelmäßig auch eine Vielzahl von Informationen, die dem Kernbereich der privaten Lebensgestaltung des Nutzers, aber auch von Dritten, zuzuordnen sind. Ein staatlicher Zugriff auf diese Systeme bringt typischerweise die Gefahr mit sich, dass solche Kernbereichsdaten in den Machtbereich von Sicherheitsbehörden überführt werden.

(1) Hintergrund

Anknüpfungspunkt für den Schutz von Kernbereichsdaten ist in der Rechtsprechung des BVerfGs die Menschenwürdegarantie des Art. 1 Abs. 1 GG.[125] Es soll Konstellationen geben, in denen es staatlichen Behörden schlicht verwehrt sein muss, auf höchstpersönliche Daten des Bürgers zuzugreifen. Hierbei geht es allerdings nicht um die Abdichtung eines Kernbereichs von Daten im Sinn eines physischen oder idealen Raumes. Anliegen des Menschenwürdeschutzes ist es vielmehr sicherzustellen, dass ein jedem Einzelnen zukommender basaler Achtungsanspruch stets eingehalten wird. Menschenwürde ist ein notwendig relationales Konzept.[126] Zu fragen ist also danach, welche Art des staatlichen Zugriffs auf oder Umgangs mit kernbereichsrelevanten Informationen geeignet ist, eine grundsätzliche Missachtung der Subjektqualität des Betroffenen auszudrücken. Mit Blick auf Art. 1 Abs. 1 GG problematisch ist der heimliche Zugriff auf informationstechnische Systeme wie ihn § 20k BKAG vorsieht vor allem deshalb, weil staatlicherseits in einen Raum bzw. ein System vorgedrungen wird, das gerade dazu bestimmt ist, dem Zugriff nicht autorisierter Dritter verborgen zu blieben. Das Potential für eine verfassungswidrige staatliche Missachtung des Einzelnen liegt also in der Verletzung einer besonderen

---

[122] Vgl. auch § 105 i.V.m. §§ 162, 169 StPO. Anders bei der offenen Wohnungsdurchsuchung nach § 46 Abs. 1 Satz 2 BPolG StPO, bei der die Anordnungszuständigkeit bei dem Gericht liegt, in dessen Bezirk sich die Wohnung befindet.

[123] Siehe oben A.IV.

[124] Siehe oben B.II.3.b.iii).

[125] Vgl. BVerfGE 6, 32 (41); 80, 367 (373); 120, 274 (335).

[126] Zu alldem Poscher, JZ 2009, 269 (269 ff.).

Privatheitserwartung.[127] Es haftet der Online-Durchsuchung ebenso an wie Maßnahmen der Telekommunikations- und Wohnraumüberwachung. Die Privatheitserwartungen werden jedenfalls dann verletzt, wenn Kernbereichsdaten gezielt zu ermittlungstaktischen Maßnahmen verwendet werden – etwa wenn ein in einem extremistisch sittenstrengen Umfeld agierender Betroffener durch Streuung von Informationen über höchstpersönliche Unzulänglichkeiten, nicht hinreichend sittenstrenge sexuelle Vorlieben o. ä. diskreditiert werden soll.[128] In solchen Fällen liegt eine Missachtung des Einzelnen vor, die geeignet ist, eine Menschenwürdeverletzung zu begründen.

Dagegen lässt sich nicht in jedem Falle der bloß automatischen Erhebung oder auch der Kenntnisnahme durch Ermittlungsbeamte von einer fundamentalen Missachtung, die eine Verletzung der Menschenwürde bedeutet, sprechen. Regelmäßig wird das Ziel der Datenerhebung gerade nicht darin liegen, kernbereichsrelevante Daten zum Nachteil des Betroffenen zu nutzen. Vielmehr geht es darum, nicht dem Kernbereich zuzuordnende, sondern auf ein abzuwehrendes Schadensereignis bezogene Informationen zu erhalten, um den Schutz überragend wichtiger Rechtsgüter zu gewährleisten. Wenn mit dieser Zielrichtung und trotz erheblichen behördlichen Vermeidungsaufwands dennoch einmal kernbereichsrelevante Daten in untergeordnetem Umfang miterhoben und dann wieder gelöscht werden, liegt darin keine grundsätzliche Missachtung der betroffenen Person. Vielmehr drückt sich in einem entsprechend zielgerichteten und aufwändigen Verfahren die Achtung eines informationellen Kernbereichs gerade aus. Insbesondere die bloße Erfassung, d.h. die Übertragung privater Daten in staatliche Datenbestände als solche, begründet noch keine Würdeverletzung. In diese Richtung lässt sich auch das BVerfG verstehen, wenn es formuliert, kernbereichsrelevante Daten sollten den Sicherheitsbehörden lediglich „nach Möglichkeit“ nicht offenbar werden.[129]

(2) Bedeutung der Heimlichkeit

Eine Besonderheit des Zugriffs nach § 20k BKAG liegt zudem in der Heimlichkeit der Maßnahme. Maßnahmen wie die Online-Durchsuchung, aber auch Telekommunikations- und Wohnraumüberwachung, bedeuten regelmäßig einen Zugriff auf besonders informationssensible Räume oder Systeme ohne Kenntnis des Betroffenen, obwohl zugleich eine besondere Privatheitserwartung für diese Räume oder Systeme besteht.[130] Zwar begründet die Heimlichkeit nicht erst das Potential für Würdeverstöße im Kontext höchstpersönlicher Daten; so stellte bspw. auch die persönliche Diskreditierung mittels durch offene Maßnahmen erlangter Informationen eine staatliche Missachtung des Einzelnen dar. Die Heimlichkeit des Zugriffs verstärkt allerdings das Potential für Würdeverletzungen insofern, als sie erstens Mitwirkungsmöglichkeiten des Betroffenen im Verfahren ausschließt und ihr zweitens die Gefahr innewohnt, dass das Zielsystem auch nach dem Beginn der Überwachungsmaßnahme weiter zur Speicherung und Verarbeitung kernbereichsrelevanter Informationen genutzt wird. Nur wenn diese beiden Nachteile durch adäquate Sicherungen kompensiert werden, lässt sich die Einschätzung aufrecht erhalten, dass gerade der zur Sicherung der Vertraulichkeit kernbereichsrelevanter Daten getriebene Aufwand dazu führt, dass in der gelegentlichen bloßen Kenntnisnahme kernbereichsrelevanter Informationen durch staatliche Stellen keine Würdeverletzung liegt.

(3) Allgemeine Regelung des Kernbereichsschutzes

Vor diesem Hintergrund lassen sich einige verfassungsrechtliche Grundregeln für den Kernbereichsschutz bei der Datenerhebung mit besonderen technischen Mitteln formulieren. Sie finden ihren Niederschlag auch in bisherigen Entscheidungen des BVerfGs zu entsprechend kernbereichssensiblen sicherheitsrechtlichen Maßnahmen. Da diese Grundregeln für alle dieser Maßnahmen gelten, ist zu erwägen, ob die Regelungen zum Kernbereichsschutz nicht in einem allgemeinen Teil etwa des BKAG getroffen werden sollten. Normen, die Maßnahmen der heimlichen Überwachung solcher Orte und Sachen regeln, die ihrer Eigenart nach eine zentrale Rolle für den Kernbereich der privaten Lebensgestaltung spielen, könnten dann – jeweils soweit es sinnvoll er-

---

[127] Angesichts der zunehmenden Vernetzung von informationstechnischen Geräten könnte eine Zeit kommen, zu der diese Einschätzung auf Grund der technischen Entwicklung wieder in Frage zu stellen sein könnte. Das Verständnis eines Computers als „elektronisches Tagebuch“ etwa dürfte bereits heutzutage kaum aktuell sein.

[128] In diesem Sinn lässt sich etwa die Veröffentlichung der Sammlung pornographischer Materialien von Osama Bin Laden durch US-amerikanische Behörden einordnen, vgl. etwa http://www.reuters.com/article/us-binladen-porn-idUSTRE74C4RK20110513.

[129] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

[130] Zur Zeitgemäßheit der Privatheitserwartungen s.o. Fn. 127.

scheint – auf diesen allgemeinen Teil des Kernbereichsschutzes verweisen. Neben der in § 20k BKAG geregelten Online-Durchsuchung[131] kommen insbesondere Maßnahmen der Telekommunikations-überwachung[132] und der Wohnraumüberwachung[133] in Betracht. Dabei könnte die Verweisungsvorschrift für die Telekommunikationsüberwachung dem Umstand, dass in Bezug auf diesen Eingriff besondere Maßnahmen des Kernbereichsschutzes nur erforderlich sind, soweit besondere Anhaltspunkte für seine mögliche Betroffenheit bestehen[134] – wie etwa bei Telefonaten zwischen Eheleuten –, dadurch Rechnung tragen, dass der Rechts-folgenverweis durch entsprechende Anhaltspunkte bedingt wird.

(a) Vor- und Nachteile einer allgemeinen Regelung

Die Schaffung einer allgemeinen Regelung zum Kernbereichsschutz bringt vor allem den Vorteil mit sich, das Gesetz übersichtlicher und leichter handhabbar zu gestalten. Zudem würden die Grundprinzipien des Kernbereichsschutzes einheitlich unter einer entsprechenden Überschrift aufgeführt, anstatt in einzelnen Befugnisnormen versprengt zu sein. Eine solche Regelungstechnik hat zudem den Vorteil, dem Gesetzesanwender ebenso wie dem Bürger die Bedeutung des Kernbereichsschutzes als allgemeinem und verfassungsrechtlich besonders fundierten Anliegen noch einmal gesondert vor Augen zu führen.

Demgegenüber besteht eine Schwierigkeit vor allem darin, dass sich die kernbereichssensiblen Erhebungsmethoden in technischer Hinsicht unterscheiden. Einige Maßnahmen ermöglichen daher bspw. einen größeren Kernbereichsschutz bereits auf Erhebungsebene als andere. Die Lösung durch flexible generalklauselartige Formulierungen bringt insofern allerdings keinen wirklichen Verlust an Regelungsklarheit mit sich, da auch bei einer Normierung im Rahmen der jeweiligen Eingriffsbefugnis auf den Stand der Technik verwiesen werden muss (so etwa im aktuellen § 20k Abs. 7 Satz 2 BKAG).

Zweitens könnte aus sicherheitsbehördlicher Perspektive die Sorge bestehen, dass eine allgemeine Regelung es mit sich bringt, dass nicht in jeder Spezialbefugnis stets der Rahmen des verfassungsrechtlich gerade noch Zulässigen ausgeschöpft werden könnte. Allerdings dürften die operativ spürbaren Auswirkungen insofern allenfalls marginal sein und würden auch durch den Vorzug der einheitlichen Regelung und der Steigerung von Klarheit und Flexibilität kompensiert.

Im Ergebnis ist daher anzuraten, nach Möglichkeit die Normierung einer einheitlichen allgemeinen Kernbereichsschutzregelung anzugehen. Die dabei zu berücksichtigenden Inhalte werden im Folgenden skizziert.

(b) Möglicher Inhalt: Allgemeine Grundregeln des Kernbereichsschutzes

Zunächst ist eine Differenzierung zwischen der Erhebung der Daten, ihrer anschließenden Auswertung sowie ihrer späteren Verwendung möglich. In jeder dieser Phasen gibt es unterschiedliche allgemeine Anforderungen, deren konkrete Ausprägungen sich dann wiederum für jede der Maßnahmen unterscheiden werden.

i. Datenerhebung

- *Umfang der Erhebung*

Im Bereich der Datenerhebung gilt der Grundsatz, dass die Erhebung kernbereichsrelevanter Daten soweit wie technisch und ermittlungstechnisch möglich zu unterbleiben hat.[135] Die Ausprägung dieses Grundsatzes unterscheidet sich in den einzelnen Erhebungsvarianten deutlich. So ist es bei Maßnahmen mit Live-Betreuung, etwa bei der akustischen Wohnraumberwachung, möglich, die Datenerhebung zu unterbrechen, sobald der Kernbereich privater Lebensgestaltung betroffen wird. Bei Maßnahmen, in denen nicht laufend entstehende Informationen in Echtzeit abgegriffen werden können, sondern auf bereits gespeicherte Datensätze zugegriffen wird oder Daten automatisiert erfasst werden, besteht diese Möglichkeit nicht. Der Schutz verlagert sich dementsprechend weitgehend auf die Auswertungsebene.[136] Das gilt insbesondere für die Online-Durchsuchung. Das Programmieren einer Software, die die Aussortierung kernbereichsrelevanter Daten vornehmen könnte, ist nach derzeitigem Stand der Technik nicht möglich und wird nach Einschätzung des BKA auch in absehbarer Zeit

[131] Hierzu BVerfGE 120, 274.
[132] Hierzu BVerfGE 113, 348.
[133] Hierzu BVerfGE 109, 279.
[134] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 238 ff.
[135] Vgl. BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 219.
[136] So auch BVerfGE 120, 274 (337).

ausgeschlossen bleiben, weil die von der Software zu bewältigenden Aufgaben überkomplex wären und insbesondere rechtliche Wertungsentscheidungen erfordern würden.[137]

- *Integrität des Zielsystems*

Soweit zur Erhebung von Daten Veränderungen an Räumen, Sachen oder informationstechnischen Systemen des Betroffenen vorgenommen werden müssen, gilt zudem, dass die Veränderungen erstens nur soweit erfolgen dürfen, als sie für die Datenerhebung unerlässlich sind und zweitens soweit und sobald wie möglich automatisiert rückgängig zu machen sind.[138]

ii. Datenauswertung

Soweit sich nicht (wie etwa im Fall einer Live-Betreuung mit Unterbrechungsmöglichkeit) mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen lässt, dass die erhobenen Daten auch Informationen aus dem Kernbereich der privaten Lebensgestaltung enthalten, sind die erhobenen Datenbestände vor der weiteren Kenntnisnahme durch eine unabhängige Stelle zu sichten und auf kernbereichsrelevante Daten durchzugehen.

- *Ablauf der Sichtung*

Nach der Rechtsprechung des BVerfGs genügt eine bloß stichprobenartige Kontrolle nicht; vielmehr sind alle kernbereichsrelevanten Daten sind „herauszufiltern“[139]. Das bedeutet, dass tatsächlich alle erhobenen Daten vor der Weiterleitung an mit Sicherheitsaufgaben betraute Stellen gleichsam händisch durchgesehen werden müssen.

Nach den bisherigen Erfahrungen handelt es sich bei Maßnahmen zum Kernbereichsschutz im Rahmen der Online-Durchsuchung wie gesehen um ein sehr aufwändiges Verfahren.[140] Es sollte daher über Möglichkeiten nachgedacht werden, die vom BKA entwickelte Software zur Administrierung die Kernbereichsanalyse den zukünftig mit dieser Aufgabe betrauten Stellen zur Verfügung zu stellen. Dies hat das BVerfG in seinem Urteil zu § 20k BKAG auch ermöglicht.[141]

- *Unabhängige Stelle*

Zentraler Kritikpunkt an der bisherigen Regelung zum Kernbereichsschutz in § 20k Abs. 7 BKAG war vor allem die mangelnde Unabhängigkeit der dort betrauten Stelle. Die Auswertung erfolgte nach der Konzeption des Gesetzes bisher lediglich durch den Datenschutzbeauftragten sowie zwei weitere Bedienstete des BKA, von denen mindestens einer die Befähigung zum Richteramt haben musste. Dem anordnenden Gericht kam dabei lediglich die „Sachleitung“ zu, wobei gerade diese offene Formulierung in der Praxis wie gesehen dazu geführt hat, dass sich das Gericht weitgehend auf die Erstellung abstrakter Richtlinien, die Beurteilung von Zweifelsfällen und einige Stichproben beschränkt hat.[142] Nach der Rechtsprechung des BVerfGs muss die Auswertung der Daten insgesamt künftig von einer solchen Stelle ausgeführt werden, die nicht mit Sicherheitsaufgaben betraut ist.[143]

Als solche kommt zum Einen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Betracht, zum anderen ein Gericht. Gegen eine Betrauung des BfDI spricht, dass er seinem generellen Aufgabenzuschnitt nach für den Datenschutz einzutreten hat und daher im Spannungsfeld von Gefahrenabwehr und Kernbereichsschutz von vorneherein nicht als ebenso unabhängige Stelle erscheint wie ein Gericht. Zudem erscheint eine Annäherung des BfDI an den operativen Bereich der Sicherheitsbehörden systemwidrig. Bei der Betrauung eines Gerichts droht diese Gefahr schon deshalb nicht, weil die Scheidung der Staatsgewalten formal und organisatorisch sehr viel exakter und deutlicher ist als die zwischen BfDI und den übrigen Teilen der Verwaltung. Aus diesen Gründen erscheint es vorzugswürdig, ein Gericht mit der Auswertung der erhobenen Daten zu betrauen.

---

137 Hierzu bereits oben B.II.3.c.ix).

138 So auch bereits jetzt § 20k Abs. 2 BKAG.

139 Siehe BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 220 sowie BVerfGE 120, 274 (338 f.).

140 Siehe oben B.II.3.c.ix)(1).

141 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

142 Insofern ließ sich zwar noch von einer „Sachleitung“ sprechen, doch die Kontrolle kam nicht den nunmehr ausgesprochenen Vorstellungen des BVerfGs nahe. Dazu oben B.II.3.c.ix)(2).

143 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

Dabei ist denkbar, entweder das anordnende Gericht oder ein davon verschiedenes auszuwählen. Gegen die Betrauung des anordnenden Gerichts spricht, dass die Kernbereichsanalyse einen erheblichen Arbeitsaufwand mit sich bringt. Wenn möglich empfiehlt es sich vor diesem Hintergrund, das anordnende Gericht nicht mit der zusätzlichen Herausforderung zu belasten, bei der Entscheidung über die Anordnung einer Überwachungsmaßnahme die sachfremde Erwägung der Minimierung eigener Arbeitsbelastung ausschließen zu müssen. Andererseits könnten sich bei Zusammenfallen von Anordnungskompetenz und Auswertungsaufgabe hilfreiche Synergieeffekte ergeben. So könnten Erfahrungswerte im Umgang mit erhobenen Daten bei der Einschätzung des Anordnungsantrags helfen. Umgekehrt könnte die Befassung mit der Materie im Rahmen der Anordnungsantragsprüfung einen leichteren Einstieg in die Datenauswertung ermöglichen. Grundsätzlich spricht der hohe Arbeitsaufwand außerdem tendenziell dafür, eine Kammer und nicht einen Einzelrichter mit der Kernbereichsanalyse zu beauftragen. Gegen eine Betrauung des BGH spricht dabei jedenfalls, dass es in diesem Fall keine Möglichkeit der Beschwerde gäbe – insbesondere hätte also das BKA keine Handhabe, die Einordnung eines bestimmten Inhalts als kernbereichsrelevant überprüfen zu lassen.[144]

Aus rechtlicher oder gar verfassungsrechtlicher Perspektive lässt sich aber keine eindeutige Präferenz formulieren, welches Gericht für die Kernbereichsprüfung zuständig sein sollte. Letztlich ist an dieser Stelle eine politisch-pragmatische Entscheidung gefragt. Diese wird sich nach einer politischen Logik richten und auch Aspekte wie die politische Durchsetzbarkeit der Zusatzbelastung etwa einer einzelnen Landesjustiz und damit eines einzelnen Landeshaushaltes zu berücksichtigen haben.[145]

- *Einbeziehung sicherheitsbehördlichen Sachverstands*

Auch und gerade in der Auswertungsphase ist neben der grundgesetzlich gebotenen Unabhängigkeit der zuständigen Stelle gleichzeitig die Einbeziehung von Fachkenntnis angezeigt. Bei der Überprüfung von Inhalten auf ihre Kernbereichsrelevanz können sich Zweifelsfälle ergeben, die ohne Expertise aus dem betroffenen Phänomenbereich oder ohne vertiefte Kenntnisse des Ermittlungsvorgangs nicht sachgerecht aufgelöst werden können. Die Gründe dafür können in einem hochkonspirativen Vorgehen der Gefährder liegen (Entwicklung eigener Sprachcodes), aber auch auf bestimmte sprachliche Gepflogenheiten zurückgehen (etwa besonders „blumige“ Ausdrucksweise im Arabischen o. ä.). Insofern dürfte sich gerade die Einbindung von Beamten des BKA anbieten.

Das Erfordernis, bei der Analyse sicherheitsbehördlichen Sachverstand einzubeziehen, wurde auch vom BVerfG anerkannt.[146] Die Hinzuziehung einzelner Sicherheitsbeamter durch das überprüfende Gericht ist also im Grundsatz verfassungsrechtlich zulässig. Voraussetzung ist dabei allerdings, dass die tatsächliche Durchführung der Analyse und die Entscheidungsverantwortung bei der unabhängigen Stelle verbleiben. Als Gegenbeispiel kann insofern die bisherige Praxis dienen.[147]

- *Einbeziehung von Sprachmittlern*

In vielen Fragen der Kernbereichsanalyse wird zudem die Hinzuziehung eines Sprachmittlers erforderlich werden. Sprachmittler spielen dabei eine ambivalente Rolle für den Kernbereichsschutz. Einerseits sind sie nicht notwendig selbst Teil der Sicherheitsbehörden. Wenn ein privater Sprachmittler einen Inhalt als kernbereichsrelevant identifizieren und sein Urteil etwa durch abstrakte Einordnungen und Umschreibungen plausibel machen kann, lässt sich der Inhalt löschen, ohne dass eine Sicherheitsbehörde überhaupt Kenntnis genommen hat. Andererseits erscheint jedenfalls die Einbeziehung privater – wenn auch sicherheitsüberprüfter und zuverlässiger – Dritter in die sensible Auswertungsphase nicht per se kernbereichsschonend, gerade wenn sie – wie im Falle der Sprachmittler –mitunter sogar umfassendere Kenntnis von kernbereichsrelevanten Inhalten erhalten können als die beteiligten staatlichen Stellen. Eingedenk dieser Ambivalenz bietet es sich an, zumindest eine gesetzliche Grundlage für die Beteiligung von Sprachmittlern bei der Kernbereichsanalyse zu schaffen. In einer Vorschrift zur allgemeinen Regelung des Kernbereichsschutzes sollten Sprachmittler also durchaus aufgeführt

---

144 Vgl. §§ 304 StPO.

145 Bei der Kalkulierung der erforderlichen Ressourcen und zu erwartenden Kosten ist insbesondere zu beachten, dass es wegen der Gefahrenabwehrrelevanz der Maßnahme zumindest im Rahmen der Kernbereichsanalyse mitunter zu Eilfällen kommen könnte (zur mangelnden Erforderlichkeit einer Eilfallregelung bei der Anordnung der Maßnahme siehe oben B.II.3.c.v)), so dass die Einrichtung einer richterlichen Rufbereitschaft erforderlich werden kann; darüber hinaus muss das beteiligte Personal gesondert sicherheitsüberprüft werden, es würden sich besondere Anforderungen an die physische Absicherung des Gebäudes stellen, ggf. Aufenthaltsräume für Mitarbeiter zur Verfügung stehen müssen etc.

146 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 224.

147 Dazu oben B.II.3.c.ix).

und ebenso behandelt werden wie sonstige sachverständige Personen, die zur Unterstützung der unabhängigen Stelle hinzugezogen werden können.

- *Geheimhaltungspflichten und Sanktionen*

Für die Beteiligung sowohl von Ermittlungsbeamten wie auch Sprachmittlern gilt nach den Ausführungen des BVerfGs, dass sie wirksam zur Geheimhaltung über das im Rahmen ihrer Einbeziehung erlangte kernbereichsrelevante Wissen verpflichtet und dass entsprechende Sanktionsmechanismen vorhanden sein müssen, um diese Geheimhaltungspflicht durchzusetzen.[148] Insofern genügt es in der Vorschrift, die den Kernbereichsschutz regelt, dieses Erfordernis abstrakt zu normieren. Die entsprechenden Pflichten und Sanktionsmechanismen im Einzelfall können dann jeweils über das beamtenrechtliche Instrumentarium oder individuelle Vereinbarungen eingeführt und abgesichert werden.

- *Eilregelungen?*

Mit Blick auf die Anordnung einiger Erhebungsmethoden, mit denen typischerweise Kernbereichsdaten erhoben zu werden drohen, ist wie am Beispiel von § 20k BKAG gesehen wegen des großen Vorbereitungsaufwands eine Eilregelung nicht erforderlich.[149] Anders könnte sich die Situation allerdings auch bei solchen Maßnahmen im Bereich der Auswertungsphase darstellen. Liegen die Informationen einmal auf staatlicher Seite vor und scheiterte der Zugriff von Sicherheitsbehörden allein an einer noch erforderlichen Kernbereichsanalyse, kann es in Eilfällen geboten sein, diese zu suspendieren. Ist Gefahr im Verzug, könnte zunächst der Bestand der erhobenen Daten direkt und umfänglich der Sicherheitsbehörde zugänglich gemacht werden, deren Bedienstete ihn dann auf die zur eiligen Gefahrenabwehr erforderlichen Informationen sichten könnten. Dabei müsste eine Überprüfung der Eilbedürftigkeit sowie des anschließenden sicherheitsbehördlichen Gebrauchs der Daten gewährleistet sein, um den Wegfall der unabhängigen Vorabkontrolle zu kompensieren und damit einen Kernbereichsschutzaufwand zu gewährleisten, der es gleichwohl ausschließt, von einer fundamentalen Missachtung des Einzelnen zu sprechen. Zudem bliebe der Grundsatz unangetastet, dass kernbereichsrelevante Informationen von keiner staatlichen Stelle verwendet werden dürfen. Auch ließe sich ein Eilfall nicht durch eine strukturelle Überlastung des Gerichts mit einem der Gefahrenabwehraufgabe angemessen zügigen Auswertungsschutz begründen. Anderes kann allenfalls insoweit gelten, als es in Sonderkonstellationen zu nicht vorhersehbaren, außergewöhnlichen Überlastungen käme.

Freilich würde es in der Praxis im Rahmen des Einsatzes besonderer Mittel der Datenerhebung ohnehin allenfalls höchst selten zum Gebrauch einer Eilkompetenz in der Auswertungsphase kommen, weil es nur wenige Szenarien geben dürfte, in denen Gefahr im Verzug ist und zugleich offene Maßnahmen noch nicht das Mittel der Wahl bilden. Daher bleibt es einer politisch-pragmatischen Entscheidung des Gesetzgebers überlassen, ob er entsprechende Eilfallregelungen schaffen möchte oder nicht; eine eindeutige Empfehlung lässt sich nicht abgeben. Deshalb wurde in den folgenden Normierungsvorschlägen auf Formulierungen hierzu verzichtet.

- *Besonderheiten der heimlichen Erhebung*

Wie gesehen werden kernbereichssensible Erhebungsmaßnahmen meist ohne das Wissen des Betroffenen durchgeführt. Aus dem Blickwinkel der Menschenwürdegarantie, Art. 1 Abs. 1 GG, ist insofern wie gesehen problematisch, dass der Betroffene vor Durchführung der Maßnahme keine effektiven verfahrensrechtlichen Positionen innehaben kann und dass er überwachte Räume, Sachen oder Systeme auch nach dem Beginn der Maßnahme weiterhin zur Kommunikation, Speicherung oder Verarbeitung kernbereichsrelevanter Inhalte verwenden wird.[150]

Um diese Defizite derart zu kompensieren, dass dem aus Art. 1 Abs. 1 GG folgenden fundamentalen Achtungsanspruch des Einzelnen genügt wird, muss zunächst der Grundsatz gelten, dass die offene Erhebung den Vorrang hat, wo immer sie möglich ist.[151] Insofern ist eine strenge Erforderlichkeitsprüfung angezeigt. Im Übrigen wird die Kompensation (insbesondere des Fehlens vorgelagerter Verfahrenspositionen) im Wesentlichen über Protokollierungs- und Benachrichtigungspflichten erreicht.[152] Soweit solche ihre Regelung aktuell bereits in

---

148 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 139, 224.

149 Dazu oben B.II.3.c.v).

150 Hierzu bereits oben B.II.3.e.iv)(2).

151 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 215.

152 Zu ersteren sogleich unten.

den §§ 20v und 20w BKAG finden, sind sie aber nicht Gegenstand dieses Gutachtens und daher auch nicht der folgenden Formulierungsvorschläge.

- *Fragen der Protokollierung und Löschung*

Da sich die Frage der Löschung kernbereichsrelevanter Daten und deren Protokollierung ebenfalls für alle kernbereichssensiblen Erhebungsbefugnisse gleichermaßen stellt, lässt sich auch insofern eine einheitliche Regelung andenken. Die bisherige Aufbewahrungsfrist von höchstens einem Jahr wurde durch das BVerfG als zu kurz verworfen.[153] Insofern liegt das Problem der Sache nach parallel zur Fristenregelung in § 20j Abs. 3 Satz 3 BKAG. Es geht darum, eine effektive datenschutzrechtliche Kontrolle durch den Betroffenen und den Datenschutzbeauftragten zu ermöglichen. Da auch hier nicht ersichtlich ist, dass die Sicherheitsbehörden durch eine auch recht hohe Aufbewahrungsfrist unangemessen belastet würden, kann eine Formulierung in Parallele zum oben für § 20j Abs. 3 S. 3 BKAG angeregten Änderungsvorschlag gewählt werden.[154]

iii. Weitere Nutzung der Daten

Nach Einschätzung des BVerfGs sollen nicht kernbereichsrelevante Daten, die durch besonders sensible Maßnahmen wie § 20k BKAG gewonnen wurden, einer besonderen Zweckbindung unterliegen und nur unter besonderen, strengen Voraussetzungen weitergegeben und verwendet werden dürfen.[155] Dies soll hier nur der Vollständigkeit halber Erwähnung finden, ist aber nicht mehr Teil der hiesigen, auf die §§ 4a, 20j und 20k BKAG beschränkten Untersuchung.

Selbstverständlich bleibt es insofern bei dem Grundsatz, dass Kernbereichsdaten als solche keinesfalls in einer die Subjektqualität des Einzelnen missachtenden Art und Weise genutzt werden dürfen – auch nicht zur Gefahrenabwehr.

iv. Ansatz für eine Neuregelung

Unter Konsolidierung der vorstehenden Überlegungen und der bisherigen Regelungen kernbereichsrelevanter Datenerhebungsmaßnahmen im BKAG lässt sich als ein erster Ansatzpunkt der folgende Regelungsvorschlag anbieten. Darüber hinaus ließe sich insbesondere erwägen, ob auch solche Fragen in einer allgemeinen Normierung der Grundregeln zu Datenerhebung und Kernbereichsschutz aufgegriffen werden sollten, die nicht Gegenstand der hiesigen Untersuchung sind (etwa die aktuell in § 20w BKAG geregelten Benachrichtigungspflichten).

§ [...] BKAG

Schutz des Kernbereichs der privaten Lebensgestaltung bei der Datenerhebung mit besonderen Mitteln

(1) Für den Einsatz besonderer Mittel der Datenerhebung gelten die folgenden Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung, soweit dies in den nachstehenden Vorschriften angeordnet wird.

(2) Die Erhebung von Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind, hat soweit wie technisch möglich zu unterbleiben.

(3) Die Erhebung von Daten darf nur soweit ohne Kenntnis des Betroffenen erfolgen, als eine offene Erhebung den Erfolg der Maßnahme vereiteln würde.

(4) Auf andere als die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlichen Personen bezogene Daten dürfen nur erhoben werden, soweit dies unvermeidbar ist, um den Zweck der Erhebungsmaßnahme zu erreichen.

---

153 Siehe oben B.II.3.b.iii) sowie B.II.2.b.

154 Siehe oben B.II.2.e.i). Vgl. auch BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 129, 226, 271-273.

155 BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 283. Diese Einschätzung lässt sich durchaus kritisch sehen, weil nicht ersichtlich ist, weshalb die Weitergabe solcher bereits von einer unabhängigen Stelle als nicht kernbereichsrelevant eingeordneter Daten noch eine Grundrechtsgefährdung begründen sollte, die über diejenige hinausgeht, die sich Falle der Weitergabe von aus anderen Maßnahmen gewonnenen Daten ergibt.

(5) [1]Veränderungen, die zur Erhebung von Daten an Räumen, Sachen oder informationstechnischen Systemen vorgenommen werden müssen, dürfen nur erfolgen, soweit sie für die Datenerhebung unerlässlich sind. [2]Sie sind soweit und sobald wie möglich automatisiert rückgängig zu machen. [3]Eingesetzte technische Mittel sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [4]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) [1]Soweit es Anhaltspunkte dafür gibt, dass die erhobenen Daten auch Informationen aus dem Kernbereich der privaten Lebensgestaltung enthalten, sind die erhobenen Daten unverzüglich und vor einer Verwendung auf kernbereichsrelevante Daten zu sichten; Inhalte, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind, sind unverzüglich zu löschen. [2]Die Aufgabe nach Satz 2 wird [vom anordnenden Gericht] in eigener Entscheidungsverantwortung durchgeführt. [3]Es kann sachverständige Personen, insbesondere auch Sprachmittler, hinzuziehen, soweit dies zur Bewertung der Kernbereichsrelevanz einzelner Inhalte erforderlich ist. [4]Die sachverständigen Personen sind durch geeignete Maßnahmen zur Verschwiegenheit zu verpflichten.

(7) In keinem Fall dürfen kernbereichsrelevante Daten durch das BKA oder sonstige öffentliche Stellen verwendet werden.

(8) [1]Die Tatsachen der Erfassung der kernbereichsrelevanten Daten und ihrer Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [2]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch fünf Jahre nach Beendigung der Maßnahme, mittels derer die Daten erhoben wurden. [3]Ist über diese Maßnahme eine Benachrichtigung des Betroffenen erfolgt, kann die Dokumentation bereits am Ende des Kalenderjahres, das dem Jahr der Benachrichtigung folgt, gelöscht werden.

Noch einmal sei betont, dass es zusätzlich allgemeiner Regelungen zur weiteren Kennzeichnung und Verwendung der Daten sowie zu Benachrichtigungspflichten bei verdeckten Maßnahmen bedürfte, wie sie aktuell in den §§ 20v f. BKAG geregelt sind. Diese Fragen bleiben hier lediglich deshalb ausgeklammert, weil sie nicht Gegenstand der hiesigen Untersuchung sind.

Im Fall der Normierung einer allgemeinen Regel zum Kernbereichsschutz ließe sich § 20k BKAG etwa wie folgt umstrukturieren:

§ 20k

Verdeckter Eingriff in informationstechnische Systeme

[...]

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

(4) [1]Die Anordnung ergeht schriftlich. [2]In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

[3]Die Anordnung ist auf höchstens drei Monate zu befristen. [4]Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. [5]Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(5) Für die Datenerhebung und den Kernbereichsschutz gilt m Übrigen § [...].

4. Ansätze für eine Konsolidierung der Gefahrenschwellen im BKAG

a. Hintergrund

Die Analyse von § 20j und § 20k BKAG hat gezeigt, dass es ein besonderes Bedürfnis nach Systematisierung der Gefahren- und Eingriffsschwellen im BKAG gibt. Die Normen verwenden jeweils eigene, detaillierte Beschreibungen der erforderlichen Gefahr, ohne dabei auf eine systematische Dogmatik zurückzugreifen oder an abstrakte Kategorisierungen anzuknüpfen. In jedem Einzelfall wird ein jeweils eigentümlicher Subsumtionsvorgang erforderlich; der Rückgriff auf bekannte Kategorien und Beispielsszenarien wird verkompliziert. Das macht das Gesetz unübersichtlich; seine Handhabung wird schwierig und aufwändig.

b. Ursachen aktueller Unsicherheiten

Die in der Analyse von § 20j und § 20k BKAG ans Licht gekommenen Unsicherheiten liegen nicht darin begründet, dass es tiefgreifende gefahrendogmatische Besonderheiten bei der Abwehr von Gefahren des internationalen Terrorismus durch das BKA gäbe. Die Schwierigkeiten verweisen vielmehr auf grundsätzliche Probleme und Unklarheiten in der Dogmatik des allgemeinen polizeirechtlichen Gefahrenbegriffs. Diese Probleme werden lediglich durch das Auftreten neuartiger, diffuserer Gefahren- und Bedrohungsszenarien im Rahmen des internationalen Terrorismus immer deutlicher erkennbar, weil diese bislang selten gebliebenes Anschauungsmaterial für aus gefahrendogmatischer Sicht komplizierte Konstellationen bieten.

Die aktuellen Entwicklungen im Bereich des internationalen Terrorismus bieten nun einen Ansatzpunkt, um die auch insgesamt oft unklare innere Systematik des Gefahrenbegriffs grundsätzlich zu überdenken und zu ordnen. Wie sehr heutige Bedrohungsszenarien die polizeirechtliche Gefahrendogmatik vor neue Herausforderungen stellen, wird gerade auch im jüngsten Urteil des BVerfGs zum BKAG deutlich, in dem immer wieder durchscheint, dass die mit den neu ins BKAG eingefügten Befugnissen ins Auge gefassten Phänomene sich nicht mit einer einzigen, klassischen Gefahrenkategorie einfangen lassen. Die Unterscheidung von Gefahr und Gefahrverdacht bzw. das Instrument der Gefahrerforschungseingriffe spielt hierbei eine zentrale Rolle. Denn insbesondere im Phänomenbereich des ideologischen Terrorismus ergibt sich strukturell häufig die Situation, dass eine dürftige Informationslage besteht, gleichzeitig aber der Vorbereitungsaufwand für die Schadensrealisierung immer geringer wird und sich Schadensereignisse oft kurzfristig realisieren. Zugleich sind regelmäßig bedeutende Rechtsgüter betroffen, auch wenn das Schadensereignis an sich oft, mitunter bis kurz vor Ausführung der Tat, in ggf. mehrfachen Hinsichten (Art der Begehung, Ort, betroffene Personen) unkonkretisiert bleibt.

c. Kategorisierungen des Gefahrenbegriffs

Vor dem Hintergrund dieser dogmatischen Irritationen hat das BVerfG in seinem Urteil zum BKAG auch Anknüpfungspunkte für eine neue Kategorisierung und systematische Abschichtung der Gefahrenschwellen formuliert.[156] Gerade vor diesem Hintergrund bietet sich eine gute Gelegenheit, die Eingriffstatbestände im BKAG in verfassungskonformer Weise neu zu ordnen und dadurch die Übersichtlichkeit und Handhabbarkeit des Gesetzes zu verbessern. Die verschiedenartigen Herausforderungen für den polizeirechtlichen Gefahrenbegriff lassen sich dabei am besten bewältigen, indem man nach den gefahrenabwehrrelevanten Parametern eines Gefahrenszenarios differenziert.

i) Prognosebasis des Wahrscheinlichkeitsurteils: konkret oder abstrakt

Eine erste, traditionelle Weichenstellung für die Gestalt des Gefahrbegriffs bezieht sich auf die Art der Tatsachen, auf denen das Wahrscheinlichkeitsurteil beruht, das der Gefahrenprognose zu Grunde liegt.[157] Zum einen kann das Wahrscheinlichkeitsurteil darüber, ob in der Zukunft ein Schaden an einem polizeilich geschützten Rechtsgut eintreten wird, auf der Grundlage aller in einem konkreten Sachverhalt verfügbaren gefahrenrelevanten Umstände getroffen werden. Die konkrete Gefahr beruht auf einem solchen konkreten Wahrscheinlichkeitsurteil. Zum anderen kann das Wahrscheinlichkeitsurteil aber auch lediglich auf typischen schadensrelevanten Umständen eines Sachverhalts beruhen. Die abstrakte Gefahr beruht auf einem solchen abstrakten Wahrscheinlichkeitsurteil. Es abstrahiert für die Beurteilung eines Sachverhalts von untypischen Umständen des Einzelfalls. Daher muss etwa auch derjenige Hund einer bestimmten Rasse, die unter eine Hundeverordnung fällt, einen Maulkorb tragen, bei dem infolge einer guten Hundeschule das Risiko von Schäden nicht größer ist als bei anderen weniger gefährlichen Rassen. Das Wahrscheinlichkeitsurteil wird in solchen Fällen nicht über der

[156] Vgl. BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 104, 109 ff.

[157] Zum Folgenden Pieroth/Schlink/Kniesel, Polizeirecht, 8. Aufl. 2014, § 4 Rn. 9 ff.

Klasse der Ereignisse mit diesem konkreten Hund, sondern über der Klasse der Hunde der als gefährlich eingeschätzten Rasse gebildet.

ii) Art des Wahrscheinlichkeitsurteils: objektiv oder subjektiv

Zum anderen lassen sich Wahrscheinlichkeitsurteile danach unterscheiden, welche Perspektive, von der aus die Prognosebasis beurteilt wird, maßgeblich sein soll.[158] Traditionell liegt dem polizeilichen Gefahrbegriff – wie dem der Alltagssprache – eine objektive Perspektive zu Grunde, die auf das Urteil eines objektiven Beobachters des Sachverhalts, der die Prognosebasis bildet, abstellt. Darin unterscheidet sich die Gefahr von einem bloßen Verdacht, der auf der subjektiven Perspektive des jeweils Handelnden beruht. Bezieht sich der Verdacht auf die Wahrscheinlichkeit eines künftigen Schadensereignisses, ist vom Gefahrverdacht die Rede. Traditionell wird er in den Polizeigesetzen damit umschrieben, dass darauf abgestellt wird, dass „Tatsachen die Annahme [einer Gefahr] rechtfertigen".

Objektiver Gefahr und subjektivem Gefahrverdacht korrespondieren traditionell zwei unterschiedlichen Maßnahmetypen. Wenn das Vorliegen einer objektiven Gefahr als solches noch unsicher ist, also im Fall des Gefahrverdachts, zielt die polizeiliche Maßnahme zunächst auf die weitere Sachverhaltsaufklärung. Es werden zunächst Gefahrermittlungsmaßnahmen ergriffen, die nicht direkt hemmend auf Geschehensabläufe einwirken, sondern darauf abzielen, Informationen zu beschaffen, um den Sachverhalt weiter aufzuklären. Solche Gefahrermittlungseingriffe können entweder dazu dienen, aufzuklären, ob überhaupt eine Gefahr vorliegt oder dazu, das drohende Schadensereignis weiter zu konkretisieren.[159] Klassischerweise verlangten daher die Tatbestände typischer Gefahrermittlungsmaßnahmen – wie etwa der Durchsuchung – keine objektive Gefahr, sondern „Tatschen, die die Annahme rechtfertigen", dass eine bestimmte Gefahr vorläge.[160] Maßnahmen zur Abwehr einer Gefahr setzten traditionell hingegen keinen bloßen Verdacht, der noch der Aufklärung bedarf, sondern das Vorliegen einer objektiven Gefahr voraus.[161] Grundsätzlich sind erst bei Vorliegen einer objektiven Gefahr Maßnahmen angezeigt, die in einen andernfalls zur Gefahrrealisierung führenden Geschehensverlauf eingreifen – wie etwa die Zwangseinwirkung auf Personen oder Sachen oder die Räumung eines Ortes.

Verunklart wird diese traditionell klare Zuordnung von objektiver Gefahr und Gefahrenabwehr auf der einen und Gefahrverdacht und Gefahrermittlung auf der anderen Seite dadurch, dass Uneinigkeit darüber besteht, wie das Polizeirecht auf Szenarien reagieren soll, in denen die Polizei aus Gründen zeitlichen Handlungsdrucks bei Vorliegen eines Gefahrverdachts keine traditionellen Gefahrermittlungsmaßnahmen ergreifen kann, sondern Maßnahmen auf Grund traditioneller Abwehrbefugnisse ergreifen muss. Anders als noch das Preußische Oberverwaltungsgericht hat die Nachkriegsrechtsprechung Gefahrverdacht und Anscheinsgefahren der objektiven Gefahr für diese Situationen gleichgestellt. Die ganz h.L. ist dem gefolgt, während einige Stimmen in der Literatur andere Lösungen für diese Sonderkonstellationen für angemessener erachten – wie etwa eine Beweismaßreduktion gerade auch im Sinn der Effektivität der Gefahrenabwehr.[162] Von der Uneinigkeit für diese Sonderfälle, die sich im Ergebnis kaum je forensisch auswirkt, sollte sich jedoch die gesetzliche Systematik nicht beirren lassen. Sie sollte vielmehr an der traditionellen Zuordnung des Begriffs der Gefahr zu Gefahrenabwehrmaßnahmen einerseits und des Tatbestandmerkmals der „Tatsachen, die die Annahme rechtfertigen" zu Gefahrermittlungsmaßnahmen andererseits festhalten. Diese Unterteilung wird daher auch für die folgenden Vorschläge zu Grunde gelegt.

---

[158] Zum Folgenden vgl. einerseits Poscher, Gefahrenabwehr, Berlin 1999, S. 9 ff.; Jaeckel, Gefahrenabwehrrecht und Risikodogmatik, 2010, S. 114 ff., 145 ff.; auch etwa Götz, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl. 2008, § 6 Rn. 14 ff. Vgl. andererseits etwa Thiel, Polizei- und Ordnungsrecht, 2013, § 8 Rn. 195; s. auch Gusy, Polizei- und Ordnungsrecht, 7. Aufl. 2009, § 3 Rn. 108, 114 f., 121; Kugelmann, Polizei- und Ordnungsrecht, 2. Aufl., 5. Kap. Rn. 98 f.

[159] Gefahrerforschungseingriffe können freilich doppelfunktionalen Charakter haben – Aufklärung des Gefahrenszenarios einerseits und Vorbereitung der Gefahrenabwehr andererseits (Bsp.: Durchsuchung einer Wohnung, um Anschlagspläne zu finden, hier kann zugleich in Frage stehen, ob es solche Pläne überhaupt gibt und zugleich kann das Auffinden der Pläne das Schadensereignis konkretisieren und so eine effektive Gefahrenabwehr vorbereiten).

[160] Zur Ermächtigung der Polizei zu Gefahrerforschungsmaßnahmen im Preußischen Polizeirecht s. Naas, Die Entstehung des Preußischen Polizeiverwaltungsgesetzes von 1931, Tübingen 2003, S. 281. Zur Wendung der „Tatsachen, die die Annahme rechtfertigen" als typischer Formulierung von Gefahrerforschungsmaßnahmen vgl. auch Ennuschat/Ibler/Remmert, Öffentliches Recht in Baden-Württemberg, München 2014, § 2 Rn. 111.

[161] Vgl. Pieroth/Schlink/Kniesel, Polizeirecht, 8. Aufl. 2014, § 4 Rn. 52.

[162] Zu alldem Poscher, Gefahrenabwehr, Berlin 1999, S. 30 ff.

iii) Konkretisierung des Schadensereignisses

Des Weiteren kann man Gefahren danach unterscheiden, in welchen Hinsichten das Schadensereignis bereits konkretisierbar ist. Ein Schadensereignis lässt sich dabei analytisch unterteilen in eine zeitliche Dimension (wann ereignet sich der Schaden?), eine räumliche (wo findet das Ereignis statt?), in eine sachliche bzw. modale (welche Art von Schaden/ mit welchen Mitteln wird er herbeigeführt? etc.) sowie in eine personale. Letztere lässt sich zusätzlich in eine aktive (wer ist der/ sind die Störer?) und eine passive Komponente (wer sind die Geschädigten?) unterteilen.

Das in einer Gefahrensituation befürchtete Schadensereignis kann in jeder der Dimensionen mehr oder weniger konkret sein. Auf der Skala vom gänzlich unkonkretisierten Schadensereignis („es wird zu Schäden an polizeilich geschützten Rechtsgütern kommen“) bis zum in allen Dimensionen konkretisierten Ereignis, wie es den Gegenstand der Gefahr im klassischen Sinn bildet („Herr X wird in fünf Minuten im Park vom Hund des Herrn Y gebissen werden“), sind verschiedene Konkretisierungsstufen denkbar.

Das jüngste Urteil des BVerfGs zum BKAG lässt sich so verstehen, dass jedenfalls bei der Bekämpfung von Gefahren des internationalen Terrorismus die Eingriffsvoraussetzungen in der Weise gelockert sind, dass das prognostizierte Schadensereignis nicht in jeder der Dimensionen bereits konkretisierbar sein muss. Vielmehr könne es genügen, dass ein „noch nicht seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist“, wenn „das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie [...] in überschaubarer Zukunft“ Straftaten begehen wird.[163] Polizeirechtssystematisch lässt sich im Falle eines solchen teilkonkretisierten Schadensereignisses von einer Gefahrenlage sprechen.[164]

d. Konsolidierung und Konsequenzen für §§ 20j und 20k BKAG

Die unterschiedlichen Parameter des Gefahrbegriffs lassen sich nun theoretisch in beliebiger Weise kombinieren. Von den theoretisch möglichen Alternativen sind allerdings nur einige für das Polizeirecht im Allgemeinen und das BKAG im Besonderen relevant.[165] Relevant ist zunächst die konkrete Gefahr im klassischen Sinn, d.h. der Fall eines konkreten, objektiven Gefahrenurteils, das sich auf ein weitgehend konkretisiertes Schadensereignis bezieht. Die konkrete Gefahrenbegriff ist gemeint, wenn im Gesetz ohne weitere Qualifizierung von einer „Gefahr“ die Rede ist – wie etwa in § 20a Abs. 2 BKAG.[166] Entsprechend ermächtigen diese Vorschriften auch zu Gefahrenabwehrmaßnahmen. Abstrakte Gefahren spielen dagegen für das BKAG eine nur geringe Rolle. Die zentrale klassische Maßnahme zur Abwehr abstrakter Gefahren, die Polizeiverordnung, findet in den §§ 20a ff. BKAG keine Ermächtigungsgrundlage. Der Sache nach liegt aber etwa den Maßnahmen gemäß § 20d Abs. 1 Nr. 2 BKAG eine abstrakte Gefahr zu Grunde, da sie nicht auf einem konkreten Wahrscheinlichkeitsurteil in Bezug auf eine konkrete Person, sondern auf einem typisierenden Urteil auf Grund bestimmter Merkmale eines Ortes beruhen. Die Besonderheit der Regelung besteht darin, dass konkrete Maßnahmen zur Abwehr einer abstrakten Gefahr dienen – die konkreten Kontrollen nach § 20d Abs. 1 Nr. 2 BKAG verringern etwa die abstrakte Gefahr von Anschlägen, weil sie potentielle Täter abschrecken.

Besondere Mittel der Datenerhebung, wie sie §§ 20j, 20k BKAG regeln, dienen in der Regel nicht der Gefahrenabwehr, sondern der Gefahrermittlung. Regelmäßig werden durch die bloße Erhebung von Daten Gefahren nicht bereits abgewehrt. Beide Befugnisse zielen vielmehr auf die Beschaffung weiterer Informationen, um entweder aufzuklären, ob überhaupt eine Gefahr vorliegt und wie sie beschaffen sein könnte, oder um tatsächlich Gefahrenabwehrmaßnahmen auf die neu gewonnenen Informationen stützen zu können. Dem entspricht auch die bisherige Anwendung in der Praxis – so hatte insbesondere die hier untersuchte Rasterfahndung nach § 20j BKAG (EG Advent) zum Ergebnis, einen zuvor bestehenden Gefahrverdacht auszuräumen. Sobald die Sicherheitsbehörden mit einer konkreten Gefahr konfrontiert sind, wird es in aller Regel auch ohnehin zu spät sein, um die zeit- und vorbereitungsintensiven Maßnahmen nach §§ 20j und 20k BKAG noch nutzen zu können. Zutreffenderweise verlangen diese Tatbestände daher auch nicht das objektive Vorliegen einer Gefahr, sondern

---

[163] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 112. Freilich ist nicht ersichtlich, weshalb diese Überlegung auf den Bereich terroristischer Gefahren beschränkt sein soll. Gerade im Bereich der organisierten Kriminalität können sich ähnliche Szenarien ergeben (Bsp.: Eine als Auftragsmörder bekannte Person reist ein, über potentielle Opfer ist aber noch wenig oder nichts bekannt; auch hier könnten Überwachungsmaßnahmen u. U. gerechtfertigt erscheinen).

[164] Dieser Begriff wird inzwischen auch vom BVerfG verwendet, s. BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 207.

[165] Daneben sind sogar noch weitere Unterteilungen denkbar. So können etwa bei einzelnen der Paramater die Anforderungen variieren – etwa ein bestimmter Grad an Wahrscheinlichkeit oder zeitlicher Nähe des Schadensereignisses verlangt werden oder es können bestimmte Anforderungen an die ggf. betroffenen Rechtsgüter gestellt werden (bspw. nur Leib, Leben oder andere hochrangige Rechtsgüter).

[166] Vgl. BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn.112 zum klassischen Gefahrenbegriff.

lediglich „Tatsachen, die die Annahme … rechtfertigen“ und formulieren damit einen Verdachtstatbestand, dem ein subjektives Wahrscheinlichkeitsurteil aus der Perspektive des sorgfältigen handelnden Beamten zu Grunde liegt.

Gleichzeitig handelt es sich um gerade im Fall von § 20k BKAG um besonders schwerwiegende Grundrechtseingriffe. Sie dürfen daher keinesfalls bereits auf der Grundlage eines bloß typisierenden abstrakten Wahrscheinlichkeitsurteils getroffen werden. Das BVerfG hat immer wieder betont, dass pauschale Annahmen, die auf bloß statistischem Wissen oder nicht quantifizierter polizeilicher Erfahrung beruhen, für entsprechende Maßnahmen nicht ausreichen, sondern dass eine Prognose erforderlich ist, die alle relevanten Umstände des Betroffenen berücksichtigt.[167] Das Wahrscheinlichkeitsurteil muss ein konkretes sein, was das Gericht zuweilen dadurch zum Ausdruck gebracht hat, dass es konkrete Tatschen verlangt. Ein abstraktes Wahrscheinlichkeitsurteil reicht zur Legitimation von Maßnahmen dieser Eingriffsintensität nicht aus.[168]

Schließlich zielen die §§ 20j und 20k BKAG mit dem internationalen Terrorismus auf einen Phänomenbereich, in dessen Kontext es typischerweise zu kurzfristigen und zugleich sehr schwerwiegenden Schadensrealisierungen kommen kann, die in ihren Einzelheiten vorab aber oft kaum konkretisierbar sind. Das Urteil des BVerfG hat darauf reagiert, indem es es trotz der Intensität der Eingriffe für verhältnismäßig erachtet hat, dass der Gesetzgeber die Konkretisierbarkeit des befürchteten Schadensereignisses lockert. Es reicht aus, dass bestimmte „Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen [...].“[169] Es genügen also Szenarien einer bloßen Gefahrenlage.

Die Tatbestände der §§ 20j und 20k BKAG verlangen also ein konkretes subjektives Wahrscheinlichkeitsurteil hinsichtlich eines gegenüber der klassischen Gefahr lediglich teilkonkretisierten Schadensereignisses. Systematisch haben sie einen konkreten Gefahrenlagenverdacht zur Voraussetzung. Dies sollte bei den §§ 20j und 20k BKAG – und auch bei allen anderen vergleichbaren Gefahrermittlungsmaßnahmen – durch eine einheitliche gesetzliche Formulierung des jeweiligen Gefahrerfordernisses zum Ausdruck gebracht werden.

e. Vereinheitlichung der Schutzgüter?

Im Rahmen der tatbestandlichen Konsolidierung der Gefahrenschwellen von § 20j und § 20k BKAG stellt sich zudem die Frage, ob auch die sich in der aktuellen Fassung marginal unterscheidenden Formulierungen der Schutzgüter vereinheitlicht werden sollten. Zwar werden in beiden Vorschriften „Leib, Leben oder Freiheit einer Person“ als qualifizierte Schutzgüter benannt. Daneben kennt § 20j BKAG allerdings noch „den Bestand oder die Sicherheit des Staates“ sowie „Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist“ als weitere Schutzgüter, während § 20k BKAG formuliert, dass es um „solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt,“ gehen muss. Die unterschiedlichen Formulierungen sind weitgehend auf Zufälligkeiten wie etwa unterschiedliche Formulierungen in den der Normierung jeweils vorausgehenden Entscheidungen des BVerfGs zurückzuführen.[170] In der Sache und vor allem bei der Normanwendung auf operativer Ebene verbinden sich mit den Abweichungen in der Formulierung keine relevanten Unterschiede.[171] Dies spricht tendenziell dafür, auch hier eine Vereinheitlichung vorzunehmen.

Es besteht aber keine besondere Dringlichkeit, da die unterschiedlichen Formulierungen hier – anders als im Falle der Gefahrenschwellen – nicht auf tieferliegende systematische Unsicherheiten hindeuten, die nach einer möglichst baldigen und umfassenden Auflösung verlangten. Die Frage ist daher den politisch-pragmatischen Erwägungen des Gesetzgebers anheimzustellen und wird hier nicht in Form konkreter Formulierungsvorschläge weiter verfolgt.

f. Änderungsvorschläge

Es bietet sich an, § 20j und § 20k BKAG derart neu zu fassen, dass sie die vorstehenden Überlegungen zur dogmatischen Systematisierung der für das BKAG relevanten Gefahrenschwellen aufgreifen und verdeutlichen. Dies bringt nicht zuletzt den großen Vorteil einer erleichterten praktischen Handhabung der Normen mit sich.

---

[167] Vgl. etwa BVerfG, Beschl. v. 15.3.2001 = NJW 2001, 2320 (2321); Beschl. v. 24.7.2015 = NVwZ 2016, 53.

[168] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 207.

[169] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 213.

[170] Vgl. etwa BVerfGE 120, 274 (274 ff., 328) sowie BVerfGE 115, 320 (320 ff.).

[171] Hinzu kommt, dass in der Praxis kaum Fälle denkbar sind, in denen nicht zumindest zugleich auch die übrigen Schutzgüter (Leib, Leben etc.) betroffen sind.

In sprachlicher Anlehnung auch an die neue Rechtsprechung des BVerfGs[172] könnten sie insofern wie folgt lauten:

§ 20j

Rasterfahndung

(1) [1]Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, **wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, vorliegt. [2]Dabei genügt es, wenn eine Schädigung dieser Rechtsgüter wenigstens seiner Art nach konkretisierbar und zeitlich absehbar ist oder zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eines dieser Rechtsgüter schädigen wird.**

(2) Von den Verfassungsschutzämtern des Bundes und der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach **Absatz 1** nicht verlangt werden.

[...]

§ 20k

Verdeckter Eingriff in informationstechnische Systeme

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

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

[2]Dabei genügt es, wenn eine Schädigung dieser Rechtsgüter wenigstens seiner Art nach konkretisierbar und zeitlich absehbar ist oder zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eines dieser Rechtsgüter schädigen wird. [3]Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

[...]

Diese Regelungstechnik, die darauf verzichtet, den Begriff der konkreten Gefahrenverdachtslage als solchen zu definieren, sondern ihn als dogmatische Kategorie voraussetzt, steht im Einklang mit der umschreibenden Tradition des Polizeirechts, das auch die Begriffe der konkreten und abstrakten Gefahr lediglich als dogmatische, nicht aber im Text der Gesetze selbst nutzt.

Dass abstrakte Gefahren nicht für Maßnahmen des BKA genügen und Eingriffe „ins Blaue hinein“ unzulässig sind, wird zusätzlich über § 20a Abs. 2 BKAG klargestellt.

[172] BVerfG, Urt.v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 112, 213.

C. Zusammenfassung und Fazit

Die Untersuchung hat vor allem gezeigt, dass die Anwendung der zu evaluierenden Normen in der Praxis bislang eine relative Seltenheit ist (17 Gefahrenabwehrvorgänge nach § 4a BKAG, eine Maßnahme nach § 20j BKAG, fünf Anordnungen und Datenausleitungen nur von zwei Zielsystemen im Rahmen von § 20k BKAG). Es kommt insbesondere nicht zu vielfältigen, wahllosen Überwachungen, sondern zu relativ wenigen, dafür dann aber intensiven Ermittlungs- und Eingriffsszenarien.[173] Die Befürchtungen, dass mit der BKA-Novelle von 2009 eine massive Ausweitung der Gefahrenabwehr- und Überwachungstätigkeit des BKA einsetzen würde, haben sich nicht bestätigt.

Zudem haben sich jedenfalls die untersuchten Normen weitgehend als verfassungskonform erwiesen. Auch die Anwendungspraxis kann im Großen und Ganzen als überwiegend beuhtsam und grundrechtsschonend bezeichnet werden. Die allerdings bedeutende Ausnahme hierzu bildet die bisherige Umsetzung des Kernbereichsschutzes im Rahmen von § 20k Abs. 7 BKAG. Insofern war die Praxis einerseits bereits deshalb selbst verfassungswidrig, weil sie auf der Anwendung eines verfassungswidrigen Gesetzes beruhte. Darüber hinaus war die praktische Anwendung auch mit Blick auf die Auslegung des Kernbereichsbegriffs zum Teil gesetzes- und verfassungswidrig.

Aus einer Effektivitätsperspektive ist festzustellen, dass die Zusammenarbeit zwischen Bundes- und Landesbehörden nach § 4a BKAG weitgehend reibungslos funktioniert hat. Die neuen Eingriffsbefugnisse aus § 20j und § 20k BKAG hingegen haben bislang wenig zur Abwehr von Gefahren des internationalen Terrorismus beigetragen. Das liegt insbesondere im Fall von § 20k BKAG vor allem an Schwierigkeiten bei der Aufbringung der Überwachungssoftware. Diese wird in der Praxis auch durch ein hochkonspiratives und technisch fortschrittliches Vorgehen der Gefährder erschwert. Insofern sind normative Anpassungen kein Allheilmittel. Aber die Schaffung zusätzlicher Befugnisse wie eines auf § 20k BKAG zugeschnittenen Wohnungsdurchsuchungsrechts und einer Norm zur Umleitung von Datenströmen bei Access-Providern könnte dazu beitragen, die Effektivität der Befugnisse zu steigern, ohne unabsehbare Bürden für den Grundrechtsschutz mit sich zu bringen. Es muss dabei allerdings sichergestellt sein, dass die wissenschaftliche Evaluation der Befugnisse fortgeschrieben wird.

Am jetzigen Bestand der untersuchten Normen zu bemängeln ist aus legistischer Perspektive insbesondere die sprachliche Abfassung. Die Vorschriften sind allesamt recht umständlich und unübersichtlich geraten. Insbesondere finden sich Formulierungsunterschiede in den Normen, ohne dass klar ist, ob und welche inhaltlichen Unterschiede damit beabsichtigt sind. Dem Gesetzgeber ist in jedem Fall zu raten, bei der anstehenden Neufassung vieler Normen des BKAG den Versuch einer systematischeren und sprachlich konsistenteren Ordnung zu unternehmen.

[173] S. hierzu insbesondere die Ergebnisse der empirischen Analyse, oben B.I.

D. Übersicht über die Änderungsvorschläge

Im Folgenden werden die an den untersuchten Normen selbst vorgeschlagenen Änderungen zusammengefasst. Ggf. notwendig werdende Änderungen an anderen Normen, etwa auf Grund von Verweisungszusammenhängen, werden nicht dargestellt.

I. § 4a BKAG

§ 4a

Abwehr von Gefahren des internationalen Terrorismus

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

1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
3. die oberste Landesbehörde um eine Übernahme ersucht**; bei Gefahr im Verzug genügt es bis zur unverzüglich herbeizuführenden Entscheidung der obersten Landesbehörde, wenn ein Landeskriminalamt um die Übernahme ersucht.**

[2]Gefahren des internationalen Terrorismus sind Gefahren der Verwirklichung von Straftaten, die in § 129a Abs. 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können. [3]Das Bundeskriminalamt kann in den in Satz 1 bezeichneten Fällen auch zur Verhütung von Straftaten nach Satz 2 tätig werden.

(2) [1]Die Befugnisse der Länder und anderer Polizeibehörden des Bundes bleiben unberührt. [2]Die zuständigen obersten Landesbehörden und, soweit zuständig, anderen Polizeibehörden des Bundes sind unverzüglich zu benachrichtigen, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt. [3]Die Aufgabenwahrnehmung erfolgt in gegenseitigem Benehmen. [4]Stellt das Bundeskriminalamt bei der Aufgabenwahrnehmung nach Absatz 1 Satz 1 Nr. 2 die Zuständigkeit einer Landespolizeibehörde fest, so gibt es diese Aufgabe an diese Polizeibehörde ab, wenn nicht ein Fall des Absatzes 1 Satz 1 Nr. 1 oder 3 vorliegt.

II. § 20j BKAG

§ 20j

Rasterfahndung

(1) [1]Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen aus Dateien zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, **wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, vorliegt. [2]Dabei genügt es, wenn eine Schädigung dieser Rechtsgüter wenigstens seiner Art nach konkretisierbar und zeitlich absehbar ist oder zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eines dieser Rechtsgüter schädigen wird.**

(2) Von den Verfassungsschutzämtern des Bundes und der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach **Absatz 1** nicht verlangt werden.

(3) [1]Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf andere im Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. [2]Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen vom Bundeskriminalamt nicht verwendet werden.

(4) [1]Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. [2]Die getroffene Maßnahme ist zu dokumentieren. [3]Diese Dokumentation ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und **fünf Jahre nach der Beendigung der Maßnahme** zu vernichten. **[3]Ist über die Maßnahme nach Absatz 1eine Benachrichtigung des Betroffenen erfolgt, kann die Dokumentation nach Satz 2 bereits am Ende des Kalenderjahres, das dem Jahr der Benachrichtigung folgt, gelöscht werden.**

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

III. § 20k BKAG

§ 20k

Verdeckter Eingriff in informationstechnische Systeme

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

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

[2]Dabei genügt es, wenn eine Schädigung dieser Rechtsgüter wenigstens seiner Art nach konkretisierbar und zeitlich absehbar ist oder zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft eines dieser Rechtsgüter schädigen wird. [3]Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

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

(3) [1]Die Anordnung ergeht schriftlich. [2]In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

[3]Die Anordnung ist auf höchstens drei Monate zu befristen. [4]Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. [5]Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(4) Für die Datenerhebung und den Kernbereichsschutz gilt m Übrigen § [...].

IV. Allgemeine Regelung zu Datenerhebung und Kernbereichsschutz

§ [...] BKAG

Schutz des Kernbereichs der privaten Lebensgestaltung bei der Datenerhebung mit besonderen Mitteln

(1) Für den Einsatz besonderer Mittel der Datenerhebung gelten die folgenden Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung, soweit dies in den nachstehenden Vorschriften angeordnet wird.

(2) Die Erhebung von Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind, hat soweit wie technisch möglich zu unterbleiben.

(3) Die Erhebung von Daten darf nur soweit ohne Kenntnis des Betroffenen erfolgen, als eine offene Erhebung den Erfolg der Maßnahme vereiteln würde.

(4) Auf andere als die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlichen Personen bezogene Daten dürfen nur erhoben werden, soweit dies unvermeidbar ist, um den Zweck der Erhebungsmaßnahme zu erreichen.

(5) [1]Veränderungen, die zur Erhebung von Daten an Räumen, Sachen oder informationstechnischen Systemen vorgenommen werden müssen, dürfen nur erfolgen, soweit sie für die Datenerhebung unerlässlich sind. [2]Sie sind soweit und sobald wie möglich automatisiert rückgängig zu machen. [3]Eingesetzte technische Mittel sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [4]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) [1]Soweit es Anhaltspunkte dafür gibt, dass die erhobenen Daten auch Informationen aus dem Kernbereich der privaten Lebensgestaltung enthalten, sind die erhobenen Daten unverzüglich und vor einer Verwendung auf kernbereichsrelevante Daten zu sichten; Inhalte, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind, sind unverzüglich zu löschen. [2]Die Aufgabe nach Satz 2 wird [vom anordnenden Gericht] in eigener Entscheidungsverantwortung durchgeführt. [3]Es kann sachverständige Personen, insbesondere auch Sprachmittler, hinzuziehen, soweit dies zur Bewertung der Kernbereichsrelevanz einzelner Inhalte erforderlich ist. [4]Die sachverständigen Personen sind durch geeignete Maßnahmen zur Verschwiegenheit zu verpflichten.

(7) In keinem Fall dürfen kernbereichsrelevante Daten durch das BKA oder sonstige öffentliche Stellen verwendet werden.

(8) [1]Die Tatsachen der Erfassung der kernbereichsrelevanten Daten und ihrer Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [2]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch fünf Jahre nach Beendigung der Maßnahme, mittels derer die Daten erhoben wurden. [3]Ist über diese Maßnahme eine Benachrichtigung des Betroffenen erfolgt, kann die Dokumentation bereits am Ende des Kalenderjahres, das dem Jahr der Benachrichtigung folgt, gelöscht werden.

V. Weitere Empfehlungen und Anregungen

Zu den folgenden Punkten lassen sich bislang lediglich grundsätzliche Empfehlungen oder Anregungen festhalten. Hier sind zunächst politische Vorentscheidungen des Gesetzgebers geboten, bevor konkrete Formulierungsvorschläge gemacht werden könnten.

1. § 4a BKAG

Im Rahmen von § 4a BKAG ist zu überlegen, ob ermessenslenkende Listen geschaffen werden, in denen Gruppierungen und Personen durch eine politisch verantwortliche Stelle wie das BMI als terroristisch oder auch als nicht-terroristisch qualifiziert werden.[174] Solche könnten in Form von Rechtsverordnungen oder – zu veröffentlichenden – allgemeinen Verwaltungsvorschriften erlassen werden.

2. § 20k BKAG

Um zu gewährleisten, dass die Online-Durchsuchung künftig effektiv angewendet werden kann, lässt sich die grundsätzliche Empfehlung formulieren, dass das BKA ermächtigt werden sollte, Wohnungen von Betroffenen mit dem Ziel zu durchsuchen, Überwachungssoftware auf die von den Betroffenen genutzten Zielsysteme aufzuspielen.[175]

Überdies ist zu erwägen, ob eine Vorschrift zur Umleitung von Datenströmen durch Service-Provider geschaffen werden soll.[176]

3. Gerichtliche Zuständigkeit bei § 20j und § 20k BKAG

Mit Blick sowohl auf § 20j und § 20k BKAG ist zu erwägen, ob die gerichtliche Anordnungszuständigkeit auf den BGH verlagert werden sollte.[177]

---

[174] Siehe oben. B.II.1.e.ii).

[175] S.o. B.II.3.c.vii)(1) und B.II.3.e.ii).

[176] S.o. B.II.3.c.vii)(2) und B.II.3.e.iii).

[177] S.o. B.II.3.c.iii).

4. Gerichtliche Zuständigkeiten im Rahmen des Kernbereichsschutzes

Ebenfalls einer Vorentscheidung durch den Gesetzgeber bedürfen die Fragen, welches Gericht mit der Kernbereichsanalyse erhobener Datenbestände befasst werden soll und ob das anordnende und das auswertende Gericht identisch sein sollen.

5. Online-Durchsuchung und Quellen-TKÜ

Nicht zum Untersuchungsgegenstand zählte die Quellen-TKÜ nach § 20l BKAG. Bei der Untersuchung der Online-Durchsuchung hat sich aber gezeigt, dass die sich wandelnden technischen und generellen Bedingungen der Telekommunikation grundlegende Fragen für die einfachrechtliche Ausgestaltung des Instruments und die verfassungsrechtliche Dogmatik um Art. 10 GG aufwerfen.[178]

6. Fortschreibung der Evaluation

Aufgrund der bisher geringen Fallzahlen sollte die Evaluation fortgeschrieben werden. Dies gilt umso mehr, wenn die obigen Vorschläge zur Ausweitung der Befugnisse im Rahmen der Online-Durchsuchung aufgegriffen werden sollten.[179] Die Evaluation ist schließlich auch ein Instrument der demokratischen Kontrolle der Sicherheitsbehörden. Ihre Ergebnisse sollten daher in einer Form, die aus einer operativen Perspektive unbedenklich ist, der Öffentlichkeit zur Verfügung gestellt werden. Dies sollte bei einer zukünftigen Regelung der Evaluation bereits auf der Ebene des Gesetzes klargestellt werden.

Ferner ist dringend anzuraten, dass Löschungsfristen auf den Evaluierungszeitraum abgestimmt werden und dass in künftigen Evaluationsvorschriften die Zugriffsmöglichkeiten der Gutachter auf die relevanten behördlichen Datenbestände ausdrücklich geregelt werden.

E. Ausblick

Die Gefahren durch den internationalen Terrorismus werden in absehbarer Zeit kaum geringer werden, sondern eher noch zunehmen. Zudem ist damit zu rechnen, dass der Phänomenbereich immer diffuser und das Vorgehen der Gefährder immer konspirativer und technisch versierter werden wird. In der Folge wird höchstwahrscheinlich das gesellschaftliche und politische Verlangen nach auf diese Umstände reagierenden Kompetenzbündelungen und zusätzlichen oder erweiterten Eingriffsbefugnissen anwachsen. Die Gefahrenabwehrtätigkeit des BKA wird daher in Zukunft eher noch zunehmen. In der hiesigen Untersuchung ließen sich auf Grund der noch sehr geringen Fallzahlen an vielen Stellen lediglich vorläufige Einschätzungen abgeben.

Freiburg, den 20. Juni 2017

---

[178] Siehe oben B.II.3.c.ii).

[179] Siehe oben. B.II.3.e.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333