

Prof. Dr. Matthias Bäcker, LL.M.

Mannheim/Mainz, den 11. Mai 2018

Deutscher Bundestag
1. Untersuchungsausschuss
der 19. Wahlperiode
Ausschussdrucksache
19(25)249
14.05.2018

Deutscher Bundestag
1. Untersuchungsausschuss
14. Mai 2018
336

i.V. / 14/05/18

Sicherheitsarchitektur und Terrorismusbekämpfung

Stellungnahme für die Anhörung des 1. Untersuchungsausschusses
der 19. Wahlperiode des Deutschen Bundestages
am 17. Mai 2018

Inhalt

Ergebnisse	3
I. Gegenstand, Erkenntnisziel und Gang der Stellungnahme.....	5
II. Gliederung und Aufgaben der Sicherheitsbehörden.....	5
1. Vertikale Abgrenzungen und Schnittstellen zwischen den Sicherheitsbehörden von Bund und Ländern.....	6
a) Zentralstellenaufgabe des BKA	6
b) Präventive Terrorismusbekämpfung durch das BKA	8
c) Strafverfolgung durch GBA und BKA	10
d) Nachrichtendienstliche Aufklärung durch die Nachrichtendienste des Bundes	11
2. Horizontale Abgrenzungen und Schnittstellen zwischen den Aufgaben der Sicherheitsbehörden	13
a) Polizeiliche Gefahrenabwehr und Strafverfolgung	13
b) Polizei und Nachrichtendienste.....	16
III. Eingriffsbefugnisse der Sicherheitsbehörden.....	18
1. Tatbestandsmuster sicherheitsbehördlicher Überwachungsermächtigungen.....	18
a) Intensität von Überwachungseingriffen	18
b) Tatbestandsmuster im Polizeirecht	19
c) Tatbestandsmuster im Strafprozessrecht	21
d) Tatbestandsmuster im Nachrichtendienstrecht	21
2. Imperative präventivpolizeiliche Maßnahmen im Gefahrvorfeld?	23
IV. Sicherheitsbehördliche Informationsordnung	24
1. Datenüberführung in ein einzelnes Zielverfahren	24
a) Verfassungsrechtlicher Rahmen.....	24
b) Zweckänderungen zwischen Gefahrenabwehr und Strafverfolgung	26
c) Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden	27
2. Verfestigte informationelle Kooperationen von Sicherheitsbehörden	30
a) Gemeinsame Dateien	30
b) Gemeinsame Zentren	32
3. Verfahrenübergreifende Datensammlungen der Sicherheitsbehörden des Bundes.....	33
a) Regulierungsbausteine für und verfassungsrechtliche Anforderungen an sicherheitsbehördliche Datensammlungen.....	33
b) Informationssystem und Informationsverbund des BKA	35
c) Datenverbund der Verfassungsschutzbehörden bei dem BfV	38

Ergebnisse

1. Das Grundgesetz steht einer schlagkräftigen Terrorismusbekämpfung nicht im Weg, setzt ihr jedoch einen kompetenz- und organisationsverfassungsrechtlichen Rahmen. Eingriffsermächtigungen der Sicherheitsbehörden müssen zudem den Grundrechten genügen. Dies ist besonders relevant für Ermächtigungen, die nicht spezifisch auf die Terrorismusbekämpfung zugeschnitten sind und darum auch für weniger dringliche Sicherheitsbelange genutzt werden können.
2. Kompetenzordnung und Organisationsverfassung des Grundgesetzes ermöglichen Umgestaltungen der gegenwärtigen föderalen Ordnung der Terrorismusbekämpfung. Insbesondere eine partielle weitere Zentralisierung dieser Aufgabe wäre zulässig.
 - a) Das BKA könnte im Rahmen seiner Aufgabe als Zentralstelle ermächtigt werden, bestimmte Feststellungen und Bewertungen für die Landespolizeibehörden verbindlich vorzugeben. In beschränktem Maße könnte dem BKA auch eine Weisungsbefugnis hinsichtlich allgemeiner verfahrenstaktischer Fragen erteilt werden.
 - b) Im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus könnte dem BKA darüber hinaus zur Bewältigung von Konflikten mit den Landespolizeibehörden eine Weisungsbefugnis hinsichtlich konkreter operativer Entscheidungen im Einzelfall eingeräumt werden.
 - c) Die Zuständigkeiten des GBA und des BKA bei der Verfolgung terroristischer Straftaten könnten ausgeweitet werden.
3. Die sehr weit reichende Aufgabe des BfV zur eigenständigen Überwachung verfassungsfeindlicher Bestrebungen steht mit der Kompetenzordnung nicht in Einklang. Die zugehörigen Eingriffsermächtigungen verletzen zudem in erheblichem Ausmaß Grundrechte. Das Nachrichtendienstrecht des Bundes bedarf daher insgesamt einer grundlegenden Überarbeitung.
4. Bei der Terrorismusbekämpfung kommt es zu einer strukturellen Gemengelage zwischen polizeilicher Gefahrenabwehr und Strafverfolgung, die das geltende Recht nicht anleitet. Hierdurch drohen Risiken für Beschuldigtenrechte und für das institutionelle Gefüge der Strafverfolgungsbehörden. Eine Möglichkeit, die Gemengelage zumindest teilweise rechtlich aufzulösen, bestünde darin, das Recht des strafrechtlichen Ermittlungsverfahrens um ein strafprozessuales Vorfeldrecht zu ergänzen.
5. Imperative Eingriffsmaßnahmen mit präventivpolizeilicher Zielsetzung können nur begrenzt im Vorfeld der hergebrachten Eingriffsschwelle einer konkreten Gefahr zugelassen werden. Insbesondere die mitunter diskutierte Präventivhaft für „Gefährder“ ließe sich weder mit dem Grundgesetz noch mit der Europäischen Menschenrechtskonvention vereinbaren.
6. Die Strafprozessordnung erlaubt in zu weitem Ausmaß die Weiterverarbeitung strafprozessual erlangter Daten in weiteren präventivpolizeilichen oder strafprozessualen Verfahren.

7. Die Ermächtigungen zu Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden stehen nicht in vollem Umfang mit den Grundrechten in Einklang. Zugleich ermöglichen sie den Nachrichtendiensten in teils dysfunktionalem Ausmaß, Informationen zurückzuhalten.
8. Verfestigte informationelle Kooperationen von Nachrichtendiensten und Polizei- und Strafverfolgungsbehörden sind grundrechtlich besonders sensibel und bedürfen daher einer strengen Regulierung. Das geltende Recht genügt dem nicht vollumfänglich.
 - a) Die Ermächtigung zu erweiterten Nutzungen der Antiterrordatei reicht zu weit und steht mit den Grundrechten nicht in Einklang.
 - b) Die Zusammenarbeit im Gemeinsamen Terrorismusabwehrzentrum bedarf einer gesetzlichen Grundlage, die auch einen wirksamen Kontrollmechanismus installieren muss.
9. Die Ermächtigungen der Sicherheitsbehörden des Bundes zur verfahrenübergreifenden Bevorratung von Daten bedürfen einer Überarbeitung.
 - a) Die Regelungen des neuen BKAG über das Informationssystem des BKA und den polizeilichen Informationsverbund sind in wesentlichen Punkten unklar. Sie verletzen zum Teil Grundrechte, möglicherweise errichten sie teilweise umgekehrt unpraktikabel hohe Hürden für Datenbevorratungen.
 - b) Die Regelungen über den Datenverbund der Verfassungsschutzbehörden im BVerfSchG reichen inhaltlich deutlich zu weit und stehen mit den Grundrechten nicht in Einklang.

I. Gegenstand, Erkenntnisziel und Gang der Stellungnahme

Der Untersuchungsausschuss soll sich nach dem Einsetzungsbeschluss (insbesondere dessen Ziffern B. I. und B. III. 1.) auch rechtsetzungsorientiert mit möglichen Anpassungen von Befugnissen, Organisation und Kooperation der Sicherheitsbehörden befassen. An diesen Teil des Untersuchungsauftrags knüpft meine Stellungnahme an. Zwar sehe ich mich schon mangels umfassender Sachkompetenz nicht dazu berufen, detaillierte Reformvorschläge für die föderale Sicherheitsarchitektur der Terrorismusbekämpfung zu unterbreiten. Jedoch müssen sich solche Reformvorschläge in dem durch das Verfassungsrecht gezogenen Rahmen halten. Ihm gelten die folgenden Ausführungen.¹

Zunächst untersuche ich daher, welche Möglichkeiten für Umgestaltungen des gegenwärtigen föderalen und aufgabenteiligen Geflechts unterschiedlicher Sicherheitsbehörden das Grundgesetz mit Blick auf die Terrorismusbekämpfung offenhält. Dabei beschränke ich mich auf Regelungsmöglichkeiten des Bundesgesetzgebers. Im Vordergrund steht insbesondere die Frage, ob und inwieweit die Terrorismusbekämpfung weitergehend als bisher bei Stellen des Bundes zentralisiert oder zumindest bundesrechtlich geregelt werden könnte, wenn dies als Schlussfolgerung aus der Ausschussarbeit sicherheitspolitisch gewünscht sein sollte. Hierzu bedarf es einer näheren kompetenz- und organisationsverfassungsrechtlichen Analyse der Untergliederung und der Aufgaben der Sicherheitsbehörden. Meine Stellungnahme beschränkt sich dabei auf die Polizei- und Strafverfolgungsbehörden sowie die Nachrichtendienste als die Hauptakteure der Terrorismusbekämpfung (unten II.).

Hohe Bedeutung für den Untersuchungsauftrag haben ausweislich des Einsetzungsbeschlusses (vg. dessen Ziffern B. II. 1.-3.) daneben die sicherheitsrechtlichen Eingriffsbefugnisse zur Terrorismusbekämpfung, insbesondere soweit sie die Informationserhebung durch verdeckte Überwachungsmaßnahmen zum Gegenstand haben. Einen weiteren Schwerpunkt bildet die sicherheitsbehördliche Informationsordnung, welche die Weiterverarbeitung – insbesondere auch den Austausch – einmal erlangter Informationen reguliert. Auch der verfassungsrechtliche Rahmen dieser Regelungskomplexe wird im Folgenden untersucht und das geltende Bundesrecht in ihn eingebettet. Verfassungsrechtliche Grenzen eines weiteren Ausbaus des gegenwärtigen Normbestands ergeben sich primär aus den Grundrechten, teils auch aus der Kompetenzordnung des Grundgesetzes. Gerade mit Blick auf die Ermächtigungen der Sicherheitsbehörden des Bundes zur Erhebung und Weiterverarbeitung von Informationen bedarf zudem auch das geltende Recht einer verfassungsrechtlichen Kritik, da es diese Grenzen nicht vollumfänglich wahrt (unten III. und IV.).

Die Ausführungen beziehen sich grundsätzlich auf den am Tag der Anhörung geltenden Rechtszustand. Hinweise auf später in Kraft tretende Regelungen, insbesondere des ab dem 25. Mai 2018 geltenden neuen BKAG, werden besonders gekennzeichnet.

II. Gliederung und Aufgaben der Sicherheitsbehörden

Die kompetenz- und organisationsverfassungsrechtliche Analyse von Gliederung und Aufgaben der Sicherheitsbehörden hat zwei Anknüpfungspunkte: zum einen die vertikale Verteilung der hoheitlichen Sicherheitsgewähr zwischen den Sicherheitsbehörden von Bund und Ländern

¹ Für eine stärker deskriptiv und fachrechtlich ansetzende Darstellung der gegenwärtigen Sicherheitsarchitektur verweise ich auf die Stellungnahme von Benjamin Rusteberg, für eine konsequent an den Leitfragen des Untersuchungsausschusses ausgerichtete Untersuchung auf die Stellungnahme von Heinrich Amadeus Wolff.

(unten 1.), zum anderen die horizontale Abgrenzung unterschiedlicher Typen und Aufgaben von Sicherheitsbehörden (unten 2.).

1. Vertikale Abgrenzungen und Schnittstellen zwischen den Sicherheitsbehörden von Bund und Ländern

Die Kompetenzordnung des Grundgesetzes weist sowohl die polizeiliche Gefahrenabwehr als auch den Vollzug des Strafprozessrechts grundsätzlich den Ländern zu. Der Bund hat insoweit nur bereichsspezifische Vollzugskompetenzen. Gleichwohl bestehen föderale Spielräume für eine partielle Zentralisierung gerade der Terrorismusbekämpfung, die das geltende Recht nicht in jeder Hinsicht ausschöpft. Dies wird im Folgenden für das BKA und den GBA als Hauptakteure der Terrorismusbekämpfung auf Bundesebene näher ausgeführt. Die Darstellung orientiert sich an den hierfür relevanten Aufgaben dieser Behörden, die aus verfassungsrechtlicher Sicht auf unterschiedlichen Kompetenztiteln beruhen.

Hinsichtlich der nachrichtendienstlichen Aufklärung ist zu differenzieren. Die Auslandsaufklärung durch den BND und die – im Rahmen dieser Stellungnahme nicht näher zu behandelnde – militärspezifische Aufklärung verfassungsfeindlicher Bestrebungen durch den MAD unterfallen der Vollzugskompetenz des Bundes. Demgegenüber obliegt der nachrichtendienstliche Verfassungsschutz wiederum in erster Linie den Ländern. Anders als bei Gefahrenabwehr und Strafverfolgung hat der Bund die verfassungsrechtlichen Grenzen einer Zentralisierung dieser Aufgabe nicht nur ausgeschöpft, sondern sogar überschritten.

a) Zentralstellenaufgabe des BKA

Die Aufgabe des BKA als Zentralstelle für die innerstaatliche² und internationale³ kriminalpolizeiliche Zusammenarbeit findet ihre kompetenzrechtliche Grundlage in Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG. Nach diesen Normen hat der Bund zum einen die ausschließliche Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei, die Einrichtung eines Bundeskriminalpolizeiamtes und die internationale Verbrechensbekämpfung. Zum anderen steht ihm die Verwaltungskompetenz zu, Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei einzurichten.

Die Auslegung dieser Kompetenztitel ist schwierig, weil sie sich in die übliche Systematik von Gesetzgebungs- und Verwaltungskompetenzen nicht ohne weiteres einfügen: Die Befugnis, die „Zusammenarbeit“ von Bund und Ländern in der Kriminalpolizei zu regeln, setzt implizit voraus, dass auch der Bund kriminalpolizeilich tätig werden kann. Zudem erscheint die Bundeskompetenz, ein Bundeskriminalpolizeiamt einzurichten, nur dann sinnvoll, wenn der Bund dieses Amt auch mit Aufgaben und Befugnissen ausstatten darf. Jedoch enthält das Grundgesetz nirgendwo eine klare Aussage dazu, um welche Aufgaben und Befugnisse es sich handeln darf. Das systematische Problem lässt sich nur bewältigen, indem beide Kompetenzregelungen zusammen betrachtet werden. Das Bundeskriminalpolizeiamt darf danach (nur) als Zentralstelle Aufgaben in den Bereichen der kriminalpolizeilichen Zusammenarbeit von Bund und Ländern sowie der internationalen Verbrechensbekämpfung wahrnehmen.⁴ Jedoch ist es bislang nicht

² § 2 BKAG.

³ § 3 BKAG.

⁴ Insoweit wie hier die h.M. in der Literatur, etwa Burgi, in: von Mangoldt/Klein/Starck, Grundgesetz, Art. 87 Rn. 44 ff.; Ibler, in: Maunz/Dürig, Grundgesetz, Art. 87 Rn. 131; Gärditz, Strafprozeß und Prävention, S. 264.

gelingen, allgemein anerkannte Interpretationen der Begriffe Zentralstelle und Zusammenarbeit zu finden, welche die Gesetzgebungs- und Verwaltungskompetenz des Bundes trennscharf begrenzen könnten.

Die Rechtsprechung ist hierzu wenig ergiebig. Das BVerfG hat zwar ausgeführt, Zentralstellen seien nach Art. 87 Abs. 1 Satz 2 GG „im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben beschränkt“.⁵ Das Gericht hatte jedoch über die Grenzen dieser Koordinationsaufgaben nicht zu entscheiden und hat den Begriff der Zentralstelle dementsprechend nicht näher konkretisiert. In einer weiteren Entscheidung hat das Gericht den Begriff der Zusammenarbeit in Art. 73 Abs. 1 Nr. 10 GG auf eine Kooperation der beteiligten Stellen „in den Grenzen der je eigenen Befugnisse“ bezogen.⁶ Auch diese Aussage war jedoch in dem entschiedenen Fall nicht zu vertiefen. Zuletzt hat das BVerfG die Verwaltungskompetenz des Bundes für die operative Terrorismusabwehr „jedenfalls“ einer Zusammenschau von Art. 73 Abs. 1 Nr. 9a und Art. 87 Abs. 1 Satz 2 GG entnommen, ohne den Gehalt des Zentralstellenbegriffs zu erörtern. Das Verhältnis von Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG ließ das Gericht ausdrücklich offen.⁷

In der Literatur werden die Begriffe der Zentralstelle und der Zusammenarbeit teils sehr weit verstanden. Danach soll es kompetenzrechtlich zulässig sein, das Bundeskriminalamt mit originären Befugnissen zu außenwirksamen Maßnahmen (insbesondere zu eigenen Ermittlungen)⁸ sowohl zur repressiven Strafverfolgung als auch zur präventiven Straftatenverhütung⁹ auszustatten. So wird dem Bund im Ergebnis eine partielle Verfügungsbefugnis über die allgemein anerkannte Polizeihochheit der Länder eingeräumt, für die keine trennscharfen Grenzen genannt werden.

Gegen diese weite Interpretation spricht, dass die Begriffe Zentralstelle und Zusammenarbeit gerade nicht erkennen lassen, dass das Bundeskriminalamt eigenständig wahrzunehmende Aufgaben der Gefahrenabwehr oder Strafverfolgung erhalten soll. Vielmehr verweisen diese Begriffe auf eine Aufgabe, die sich in Kooperation und Koordination erschöpft. Zudem wäre es überflüssig gewesen, für die präventive Terrorismusbekämpfung durch das Bundeskriminalamt mit Art. 73 Abs. 1 Nr. 9a GG einen eigenständigen Kompetenztitel zu schaffen, wenn das weite Verständnis von Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG zuträfe. Daher ist eine restriktivere Interpretation angezeigt. Auf der Grundlage dieser Kompetenzregelungen darf der Bund das Bundeskriminalamt nur mit der Aufgabe und entsprechenden Befugnissen ausstatten, das Handeln der Landespolizeibehörden informationell zu verklammern, fachlich zu unterstützen und zu koordinieren, soweit die Landesbehörden sich abstimmen müssen. Dies schließt neben der Koordinierung im Einzelfall auch fortlaufende Serviceleistungen wie die kriminalistische Forschung, die Erstellung von Statistiken oder Fortbildungsangebote ein. Hingegen ist

⁵ BVerfGE 110, 33 (51).

⁶ BVerfGE 133, 277 (317 f.).

⁷ BVerfGE 141, 220 (263 f.).

⁸ Burgi, in: von Mangoldt/Klein/Starck, Grundgesetz, Art. 87 Rn. 47; Hermes, in: Dreier, Grundgesetz, Art. 87 Rn. 48; Abbühl, Der Aufgabenwandel des Bundeskriminalamtes, S. 93 ff.; Ahlf, Das Bundeskriminalamt als Zentralstelle, S. 59 ff.; Dittmann, Die Bundesverwaltung, S. 233; Gusy, DVBl 1993, S. 1117 (1122 ff.).

⁹ Der Begriff der Kriminalpolizei umfasst neben der Verfolgung auch die Verhütung von Straftaten, BVerfGE 133, 277 (318); vgl. zu der früheren Diskussion Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, S. 20, m.w.N. in Fn. 9.

es dem Amt kompetenzrechtlich verwehrt, in seiner Zentralstellenfunktion operative polizeiliche Verfahren aus eigener Initiative einzuleiten und mit eigenständig wahrzunehmenden Eingriffsbefugnissen zu betreiben.¹⁰

Die gegenwärtige Zentralstellenaufgabe des BKA hält sich im Rahmen der so verstandenen Bundeskompetenz.¹¹ Für einen Ausbau lässt die Kompetenzordnung nur partiell Raum.

Aufgaben zur eigenhändigen Auflösung sozialer Konflikte und die zugehörigen Überwachungs- und imperativen Befugnisse können dem BKA nicht auf der Grundlage von Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG übertragen werden. Hierzu bedarf es anderer kompetenzrechtlicher Grundlagen, die noch zu erörtern sind.

Hingegen könnten die Verklammerungs- und Koordinierungsaufgaben des BKA weiter ausgebaut werden. So könnten dem BKA im Rahmen dieser Aufgaben auch Weisungsbefugnisse gegenüber den Landespolizeibehörden eingeräumt werden.¹² Diese Weisungsbefugnisse könnten sich zwar nicht auf konkrete außenwirksamen Maßnahmen im Einzelfall beziehen. Dem BKA könnte jedoch etwa ermöglicht werden, bestimmte Feststellungen oder Bewertungen – etwa über das von einer bestimmten Person ausgehende Bedrohungspotenzial – für die Landespolizeibehörden verbindlich vorzugeben. Soweit eine länderübergreifende Bedrohungslage besteht, für deren Bewältigung mehrere Landespolizeibehörden zuständig sind, könnte das BKA zumindest in Konfliktfällen auch ermächtigt werden, allgemeine verfahrenstaktische Fragen verbindlich zu entscheiden. Solche Befugnisse könnten die Risikomanagement- und Monitoringfunktionen verstärken, die dem BKA bei der Zusammenarbeit gerade in der Terrorismusbekämpfung vermehrt zgedacht werden.¹³

b) Präventive Terrorismusbekämpfung durch das BKA

Art. 73 Abs. 1 Nr. 9a GG vermittelt dem Bund eine Gesetzgebungskompetenz für die präventive Terrorismusbekämpfung. Danach darf der Bund das BKA mit der Aufgabe betrauen, Gefahren des internationalen Terrorismus¹⁴ abzuwehren. Dieser Kompetenztitel impliziert eine parallele Verwaltungskompetenz des Bundes, die das Grundgesetz nicht ausdrücklich enthält.¹⁵ Die Bundeskompetenz für die präventivpolizeiliche Terrorismusbekämpfung ist allerdings in zweifacher Hinsicht begrenzt.

Erstens darf das Bundeskriminalamt nur Gefahren des *internationalen* Terrorismus abwehren. Für terroristische Phänomene, die auf Deutschland begrenzt sind, bleiben allein die Länder zuständig.¹⁶ Allerdings wird dieses Erfordernis überwiegend weit verstanden. So soll es nach der Begründung der Novelle des BKAG von 2009 ausreichen, wenn eine lediglich in Deutschland

¹⁰ Ähnlich Becker, DÖV 1978, S. 551 (553 ff.).

¹¹ Näher, insbesondere auch zu Grenzfällen Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. B 133.

¹² Wie hier für eine Weisungskompetenz etwa Burgi, in: von Mangoldt/Klein/Starck, Grundgesetz, Art. 87 Rn. 47; Abbühl, Der Aufgabenwandel des Bundeskriminalamtes, S. 100 ff.; Dittmann, Die Bundesverwaltung, S. 232 f.; a.A. etwa Hermes, in: Dreier, Grundgesetz, Art. 87 Rn. 49; Gärditz, Strafprozeß und Prävention, S. 373; Becker, DÖV 1978, S. 551 (554); Gusy, DVBl 1993, S. 1117 (1121).

¹³ Vgl. die Stellungnahme des Sachverständigen Maurer, S. 11.

¹⁴ Näher zum Terrorismusbegriff des Art. 73 Abs. 1 Nr. 9a GG Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. B 141.

¹⁵ Für eine Gesamtschau von Art. 73 Abs. 1 Nr. 9a und Art. 87 Abs. 1 Satz 2 GG BVerfG 141, 220 (263 f.).

¹⁶ Heintzen, in: von Mangoldt/Klein/Stark, Grundgesetz, Art. 73 Rn. 105.

tätige Gruppe in „international propagierte ideologische Strömungen“ wie etwa den „weltweiten Jihad“ eingebunden ist. Sogar eine Einzelperson, die allein handele, ihre Tätigkeit auf Deutschland beschränke und lediglich durch allgemein gehaltene ideologische Botschaften aus dem Ausland motiviert werde, könne dem internationalen Terrorismus zugerechnet werden.¹⁷

Zweitens darf der Bund die Gefahrenabwehr gemäß Art. 73 Abs. 1 Nr. 9a GG nur in drei Fallkonstellationen an sich ziehen, in denen eine Gefahrenabwehr (allein) durch Landesbehörden nicht effektiv genug zu sein droht.¹⁸ Auch insoweit wird der Kompetenztitel vielfach weit ausgelegt. Insbesondere gilt dies für die Fallkonstellation einer länderübergreifenden Gefahr (Art. 73 Abs. 1 Nr. 9a Alt. 1 GG), die nach einer extremen Position bei einer drohenden Straftat des internationalen Terrorismus in aller Regel vorliegen soll.¹⁹

Auf der Grundlage dieser weiten Interpretationen reicht die Bundeskompetenz für die präventive Terrorismusabwehr sachlich durchaus weit. § 4a Abs. 1 Satz 1 BKAG übernimmt die Voraussetzungen des Kompetenztitels wörtlich, um die Zuständigkeit des BKA zu beschreiben. Damit schöpft das Gesetz die Vollzugskompetenz des Bundes vollständig aus, soweit es um die eigenhändige operative Gefahrenabwehr geht.

Darüber hinaus umfasst die Gesetzgebungskompetenz des Bundes neben unmittelbaren Exekutivbefugnissen des Bundeskriminalamts auch Regelungen über das Zusammenwirken von Bundeskriminalamt und Landespolizeibehörden bei der Terrorismusabwehr. Insoweit schöpft das BKAG die Grenzen des kompetenzrechtlich Zulässigen bislang nicht aus.

Die Gesetzgebungs- und Verwaltungskompetenz des Bundes lässt die Zuständigkeit der Länder zur Abwehr terroristischer Gefahren unberührt. Es kommt daher regelmäßig zu Mehrfachzuständigkeiten,²⁰ die rechtsstaatliche und verwaltungspraktische Risiken bergen.²¹ Um diese Risiken abzuschirmen, muss durch rechtliche Regelungen gewährleistet werden, dass die zuständigen Polizeibehörden zügig und kontinuierlich kooperieren und ihre Tätigkeit koordinieren.

Der Bund kann daher Bundeskriminalamt und Landespolizeibehörden verpflichten, einander darüber zu informieren, dass sie die Gefahrenabwehr im konkreten Fall übernommen haben, und ihre Ermittlungsergebnisse auszutauschen. Eine entsprechende Informationspflicht des Bundeskriminalamts findet sich in § 4a Abs. 2 Satz 2 BKAG (ebenso § 5 Abs. 2 Satz 2 BKAG-neu). Eine Informationspflicht in umgekehrter Richtung findet sich nicht, allerdings dürfte das BKA ohnehin über seine Zentralstellenfunktion und die in diesem Rahmen bestehende Informationspflicht der Landespolizeibehörden aus § 13 BKAG die benötigten Informationen erhalten.

Darüber hinaus könnte der Bund das Bundeskriminalamt auch mit Weisungsbefugnissen gegenüber den Landesbehörden ausstatten, um Auseinandersetzungen zwischen den beteiligten Behörden zu vermeiden oder zumindest rasch beizulegen.²² Anders als im Rahmen der allge-

¹⁷ BT-Drucks. 16/10121, S. 21; dem folgend etwa Abbühl, Der Aufgabenwandel des Bundeskriminalamtes, S. 315; kritisch etwa Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. B 142.

¹⁸ Näher Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. B 144 ff.

¹⁹ Degenhart, in: Sachs, Grundgesetz, Art. 73 Rn. 48.

²⁰ BVerfGE 141, 220 (263).

²¹ Näher Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, S. 39 ff.

²² Mit Einschränkungen auch Uhle, in: Maunz/Dürig, Grundgesetz, Art. 73 Rn. 225; a.A. Heintzen, in: von Mangoldt/Klein/Starck, Grundgesetz, Art. 73 Rn. 106; Wittreck, in: Dreier, Grundgesetz, Art. 73 Rn. 66.

meinen Zentralstellenfunktion könnten diese Weisungsbefugnisse sich auch auf konkrete operative Entscheidungen im Einzelfall erstrecken. Von dieser Regelungsbefugnis hat der Bund keinen Gebrauch gemacht. Stattdessen ordnet § 4a Abs. 2 Satz 3 BKAG (ebenso § 5 Abs. 2 Satz 3 BKAG-neu) an, dass die zuständigen Polizeibehörden ihre Aufgaben in gegenseitigem Benehmen wahrnehmen.²³

c) Strafverfolgung durch GBA und BKA

Das Grundgesetz enthält keine Regelung, die Bundesbehörden ausdrücklich eine Strafverfolgungstätigkeit ermöglicht. Diese Tätigkeit lässt sich daher nur auf weniger spezifische Kompetenztitel stützen.

Nächstliegender Ausgangspunkt ist die Bundeskompetenz für die Rechtsprechung in Strafsachen. Art. 95 GG sieht die Errichtung oberster Gerichtshöfe des Bundes vor. Dieser Kompetenztitel erlaubt dem Bund, die Bundesgerichte neben ihrer Hauptfunktion als Rechtsmittelgerichte auch mit erstinstanzlichen Zuständigkeiten in Sachen von bundesweiter Bedeutung auszustatten.²⁴ Darüber hinaus benennt Art. 96 Abs. 5 GG ausdrücklich bestimmte Deliktsfelder, für die eine Gerichtsbarkeit des Bundes besteht. Hierzu zählt der Staatsschutz, der in einschränkender Auslegung nur solche Straftaten umfasst,

„die das staatliche Gefüge in länderübergreifender Weise treffen und die Rechtsgüter des Gesamtstaates in derart starkem Maße beeinträchtigen, dass ihre Ahndung durch die Landesjustiz der Bedeutung des in der jeweiligen Tat liegenden Angriffs auf die bundesstaatliche Gesamtordnung nicht gerecht würde.“²⁵

Da terroristische Gewalttaten sich gerade dadurch auszeichnen, dass sie zum einen eine spezifisch terroristische, auf die Destabilisierung des Gesamtstaates gerichtete Zielsetzung aufweisen und zum anderen geeignet sind, diese Zielsetzung signifikant zu fördern,²⁶ lässt sich meines Erachtens das gesamte Terrorismusstrafrecht dem so verstandenen Staatsschutz unterstellen.²⁷ Die von den Oberlandesgerichten wahrgenommene Strafgerichtsbarkeit des Bundes gemäß § 120 GVG könnte daher ausgebaut und insbesondere auf die in §§ 89a ff. StGB enthaltenen Straftatbestände erstreckt werden. Da andererseits der Staatsschutzbegriff einer einfachrechtlichen Ausgestaltung bedarf, bestehen auch keine kompetenzrechtlichen²⁸ Bedenken dagegen, die Bundesgerichtsbarkeit für bestimmte Staatsschutzdelikte von einer besonderen Bedeutung des Falles abhängig zu machen, wie dies § 120 Abs. 2 GVG vorsieht.

²³ Näher und kritisch Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, S. 59 f.

²⁴ Zur Verwaltungsgerichtsbarkeit BVerfGE 8, 174 (177); zur Sozialgerichtsbarkeit BVerfGE 92, 365 (410); zur Strafgerichtsbarkeit Welp, NStZ 2002, S. 1 (6); a.A. Gärditz, BRJ Sonderausgabe 1/2010, S. 11 (12).

²⁵ BGH NJW 2001, S. 1359 (1360); dem folgend etwa Voßkuhle, in: v. Mangoldt/Klein/Starck, GG, Art. 96 Rn. 24 mit Fn. 1.

²⁶ Vgl. zu dem Terrorismusbegriff des Art. 73 Abs. 1 Nr. 9a GG Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, S. 31 ff.

²⁷ Vgl. mit einem ähnlichen Interpretationsansatz Rebmann, NStZ 1986, S. 289 (292).

²⁸ Zum Recht auf den gesetzlichen Richter in diesem Zusammenhang Classen, in: von Mangoldt/Klein/Starck, GG, Art. 101 Rn. 36.

Nach meiner Auffassung richtet sich auch die Vollzugskompetenz des Bundes im strafprozessualen Ermittlungsverfahren primär nach den für die Strafjustiz maßgeblichen Kompetenzregelungen in Art. 95 und Art. 96 Abs. 5 GG. Dies gilt sowohl für den GBA²⁹ als auch für die Strafverfolgungstätigkeit des BKA.³⁰ Diese Behörden dürften daher gleichfalls umfassend mit der Verfolgung terroristischer Gewalttaten und der darauf bezogenen Vorfelddelikte betraut werden. Die Gegenauffassung, die die Vollzugskompetenz des Bundes auf Art. 87 Abs. 3 GG³¹ bzw. für das BKA auf Art. 87 Abs. 1 Satz 2 GG³² stützen will, führt hinsichtlich der Tatbestände des Terrorismusstrafrechts zum selben Ergebnis. Ob die Strafverfolgungszuständigkeiten des GBA und des BKA außerhalb des Terrorismusbereichs in jeder Hinsicht mit der Kompetenzordnung vereinbar sind, ist nicht Gegenstand dieser Stellungnahme.

Die Strafverfolgungskompetenz des Bundes setzt allerdings voraus, dass im Einzelfall der Verdacht eines Staatsschutzdelikts besteht. Sie erstreckt sich zudem nur auf die konkrete prozessuale Tat, auf die sich dieser Verdacht bezieht.³³ Mit der in den Leitfragen angesprochenen „Zusammenführung aller Verfahren zur gleichen Person auch bei unterschiedlichen Deliktgruppen“ über die einzelne prozessuale Tat hinaus könnte jedenfalls der GBA nicht betraut werden.

d) Nachrichtendienstliche Aufklärung durch die Nachrichtendienste des Bundes

Von den Nachrichtendiensten des Bundes werfen der BND und der MAD keine generellen³⁴ kompetenzrechtlichen Probleme auf. Sie beruhen auf den ausschließlichen Gesetzgebungs- und Verwaltungskompetenzen des Bundes für die Auslandsaufklärung (Art. 73 Abs. 1 Nr. 1, Art. 87 Abs. 1 Satz 1 GG)³⁵ sowie für den Schutz der Streitkräfte gegen verfassungsfeindliche Bestrebungen (Art. 73 Abs. 1 Nr. 1, Art. 87a Abs. 1 Satz 1 GG).³⁶

Kompetenzrechtlich problematisch ist hingegen die gegenwärtige Stellung des BfV. Das Grundgesetz konzipiert den allgemeinen Verfassungsschutz als geteilte Aufgabe von Bund und Ländern. Nach Art. 73 Abs. 1 Nr. 10 lit. b und c GG hat der Bund die Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder in diesem Bereich. Die zugehörige Verwaltungskompetenz des Bundes ergibt sich aus Art. 87 Abs. 1 Satz 2 GG, der den Bund ermächtigt, eine Zentralstelle für den Verfassungsschutz einzurichten. Im Übrigen ist der Verfassungsschutz Ländersache.

²⁹ Insoweit wie hier die überwiegende Auffassung, etwa Jarass/Pieroth, GG, Art. 96 Rn. 6; Rebmann, NStZ 1986, S. 289 (293); Gärditz, BRJ Sonderausgabe 1/2010, S. 11 (13 ff.); wohl auch Schulze-Fielitz, in: Dreier, GG, Art. 96 Rn. 34 f.; Voßkuhle, in: von Mangoldt/Klein/Starck, GG, Art. 96 Rn. 24 f.

³⁰ Insoweit wie hier etwa Jarass/Pieroth, GG, Art. 87 Rn. 6.

³¹ Für den GBA Wollweber, Die Zuständigkeit des Generalbundesanwalts in Staatsschutzsachen nach § 120 Abs. 1 und Abs. 2 GVG, S. 47 ff.; für das BKA Ibler, in: Maunz/Dürig, Grundgesetz, Art. 87 Rn. 134.

³² Etwa Uhle, in: Maunz/Dürig, Grundgesetz, Art. 73 Rn. 250; Hermes, in: Dreier, GG, Art. 87 Rn. 52.

³³ BGH NStZ-RR 2006, S. 303 (304 f.); grundsätzlich ebenso BGH NStZ 2009, 335 (338).

³⁴ Vgl. hingegen zu den kompetenzrechtlichen Anforderungen an die Gestaltung der Eingriffsermächtigungen des BND BVerfGE 100, 313 (368 ff.).

³⁵ Hinsichtlich der Verwaltungskompetenz in der Begründung, wenn auch nicht im Ergebnis streitig. Überwiegend wird stattdessen Art. 87 Abs. 3 GG herangezogen, so etwa Ibler, in: Maunz/Dürig, GG, Art. 87 Rn. 157; Werthebach/Droste, in: Bonner Kommentar zum GG, Art. 73 Rn. 266; Brenner, Bundesnachrichtendienst im Rechtsstaat, 1990, S. 40. Hiergegen spricht, dass es sich dann um eine fakultative Bundeskompetenz handelte, eine Auslandsaufklärung durch Landesbehörden aber faktisch wie auch angesichts von Art. 32 Abs. 1 GG verfassungsrechtlich schwerlich vorstellbar ist.

³⁶ Gröpl, Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung, S. 78 f.; Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 45.

Das Grundgesetz beschreibt damit die Kompetenzen des Bundes für den Verfassungsschutz parallel zu den polizeilichen Kompetenzen, die der Zentralstellenfunktion des Bundeskriminalamts zugrunde liegen. Es drängt sich auf, die entscheidenden Begriffe der Zusammenarbeit und der Zentralstelle hier ebenso auszulegen. Der Bund darf daher eine Verfassungsschutzbehörde unterhalten, die die Verfassungsschutzbehörden der Länder informationell verklammert, fachlich unterstützt und koordiniert, soweit die Länder sich abstimmen müssen. Bezogen auf diese Kooperations- und Koordinationsfunktion kann das BfV auch mit Weisungsbefugnissen ausgestattet werden. Hingegen ermöglicht die Kompetenzordnung dem Bund nicht, das BfV mit der Aufgabe zur eigenständigen Aufklärung verfassungsfeindlicher Bestrebungen und mit entsprechenden originären Überwachungsbefugnissen auszustatten.

Die Gesetzgebungspraxis ist – anders als bei der Zentralstellenfunktion des BKA – über diese beschränkte Bundeskompetenz seit jeher weit hinausgegangen. Insbesondere erlaubt § 5 Abs. 1 Satz 1 BVerfSchG dem BfV, aufgrund selbst festgelegter Erkenntnisziele eigenständig Informationen über bestimmte verfassungsfeindliche Bestrebungen zu sammeln. Das Bundesamt muss dabei zwar im Benehmen mit dem zuständigen LfV handeln, ein Vetorecht des betroffenen Landes besteht jedoch nicht.³⁷ Dementsprechend räumen §§ 8 ff. BVerfSchG sowie § 3 G 10 dem BfV zahlreiche eigenständig wahrzunehmende Datenerhebungsbefugnisse ein.

Eine kompetenzrechtliche Grundlage für diese weitreichenden originären Überwachungsbefugnisse des BfV ist nicht ersichtlich.³⁸ Insbesondere überzeugt es nicht, wenn in der Literatur hierfür allein auf Art. 87 Abs. 1 Satz 2 GG abgestellt wird.³⁹ Diese Position überspielt die getrennte Bestimmung von Gesetzgebungs- und Verwaltungskompetenzen, welche die Kompetenzordnung des Grundgesetzes kennzeichnet. Zudem nimmt sie dem Begriff der Zentralstelle jede Aussagekraft.

Entsprechend den allgemeinen Regeln sind daher die verfassungsrechtlichen Grenzen der Aufgaben und Befugnisse des BfV Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG in einer Gesamtschau zu entnehmen. Selbst bei einer weiten Interpretation dieser Normen, die entgegen der oben begründeten Position originäre Überwachungsaufgaben und -befugnisse des BfV überhaupt für verfassungsrechtlich möglich hält, ist wenigstens zu fordern, dass die Überwachungstätigkeit des BfV auf Sachverhalte mit einem spezifischen Bundesbezug begrenzt bleibt.⁴⁰ Zumindest die Zuständigkeitsregelung des § 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG, die allgemein eine Überwachung gewaltaffiner Bestrebungen zulässt, wahrt nicht mehr die Kompetenzordnung, da sie den erforderlichen Bundesbezug durch die Gefährlichkeit der Bestrebungen ersetzt. Dem lässt sich nicht entgegenhalten, gewaltorientierte Bestrebungen seien stets gesamtstaatlich bedeutsam.⁴¹ Es ist ohne weiteres vorstellbar, dass sich eine Bestrebung regional auf ein kleineres Gebiet beschränkt, auf diesem Gebiet aber äußerst aggressiv vorgeht. Eine gesamtstaatliche Relevanz ergibt sich in einem solchen Fall nicht schon daraus, dass von der Bestrebung erhebliche Schäden drohen mögen. Die bundesstaatliche Kompetenzordnung des

³⁷ Vgl. Roth, in: Schenke/Graulich/Ruthig, § 5 BVerfSchG Rn. 14.

³⁸ Vgl. mit Blick auf die Überwachungsbefugnisse nach dem G 10, aber verallgemeinerbar Bäcker, DÖV 2011, S. 840 ff.; ders., DÖV 2012, S. 560 ff.; dem folgend Pieroth, in: Jarass/Pieroth, GG, Art. 87 Rn. 5; a.A. Risse/Kathmann, DÖV 2012, S. 555 ff.; B. Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, Rn. 17 ff. vor § 1 G 10.

³⁹ So etwa Heintzen, in: von Mangoldt/Klein/Starck, GG, Art. 73 Rn. 116; Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 245; undeutlich Ibler, in: Maunz/Dürig, GG, Art. 87 Rn. 141.

⁴⁰ In diese Richtung Bergemann, NVwZ 2015, S. 1705 (1707).

⁴¹ So die Gesetzesbegründung zu § 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG, BT-Drs. 18/4654, S. 20.

Grundgesetzes beruht vielmehr auf der Annahme, dass die Länder in der Lage sind, auch erheblichen Gefahren zu begegnen. Dies zeigt sich neben dem Verfassungsschutz etwa an der Gesetzgebungs- und Verwaltungskompetenz der Länder für die allgemeine polizeiliche Gefahrenabwehr. Ein Schluss von Schadenspotenzialen auf Bundeskompetenzen ist ohne Verfassungsänderung nicht statthaft.

2. Horizontale Abgrenzungen und Schnittstellen zwischen den Aufgaben der Sicherheitsbehörden

Im horizontalen Verhältnis der unterschiedlichen Behörden und Aufgaben sind primär klärungsbedürftig zum einen das Verhältnis von polizeilicher Gefahrenabwehr und Strafverfolgung, zum anderen die Beziehungen zwischen Polizei und Nachrichtendiensten.

a) Polizeiliche Gefahrenabwehr und Strafverfolgung

Da die Polizei sowohl für die präventive Gefahrenabwehr als auch für die repressive Strafverfolgung zuständig ist, bedürfen beide Aufgaben einer Abgrenzung. Diese Abgrenzung wird gerade im Bereich der Terrorismusbekämpfung dadurch erschwert, dass einerseits das präventiv-polizeiliche Eingriffsinstrumentarium erheblich ausgebaut wurde, andererseits das strafrechtliche Sanktionsregime und das Strafverfahren zunehmend präventive Zielsetzungen verfolgen.

Nach herkömmlichem Verständnis lassen sich Gefahrenabwehr und Strafverfolgung grundsätzlich klar voneinander abgrenzen, selbst wenn diese Abgrenzung im Einzelfall Probleme aufwerfen mag. Danach ist das Strafrecht eine rein retrospektive Ordnung, die nicht laufende oder drohende soziale Konflikte bewältigen, sondern auf bereits abgeschlossene soziale Konflikte reagieren soll. Nach dieser Sichtweise erbringen strafrechtliche Sanktionen zwar auch mittelbare Präventionsleistungen, indem sie abschreckend und normstabilisierend auf die Allgemeinheit einwirken (Generalprävention) und eine individuelle Einwirkung auf Straftäter im Strafvollzug ermöglichen (Spezialprävention). Hingegen ist in diesem Verständnis das Anliegen, Risikofaktoren einzuhegen, bevor es zu einer Straftat überhaupt gekommen ist, dem Strafrecht als Sanktionsordnung kategorial fremd.⁴² Dieses Anliegen ist vielmehr Gegenstand des Gefahrenabwehrrechts. Die funktionale Unterscheidung von Strafverfolgung und Gefahrenabwehr wird normsystematisch dadurch unterstrichen, dass beide Aufgaben in unterschiedlichen Gesetzen geregelt werden.

Die funktionale Unterscheidung und normsystematische Trennung von Gefahrenabwehr und Strafverfolgung hat verfassungsrechtliche Wurzeln, ohne dass das Grundgesetz sie jedoch umfassend vorgäbe. Der Bund hat eine konkurrierende Gesetzgebungskompetenz für das materielle Strafrecht und das Strafverfahrensrecht. Hingegen ist das allgemeine Gefahrenabwehrrecht grundsätzlich Ländersache. Darüber hinaus enthält das Grundgesetz eine Reihe von strafrechtsspezifischen materiellen und prozeduralen Gewährleistungen wie etwa das Rückwirkungsverbot und den besonderen Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG oder das aus Art. 2 Abs. 1 i.V.m. Art. 20 Abs. 3 GG abzuleitende Recht auf ein faires Verfahren.

Die herkömmliche Sichtweise auf das Verhältnis von Strafverfolgung und Gefahrenabwehr trägt allerdings den Verschleifungen beider Ordnungen in der Praxis von Gesetzgebung und Verwaltung nicht vollständig Rechnung. Diese Verschleifungen gehen sowohl vom Polizeirecht als auch vom Strafrecht aus.

⁴² Bäcker, Kriminalpräventionsrecht, S. 8 f.

Auf der polizeirechtlichen Seite wurden die Ermächtigungen der Polizei, verdeckte Überwachungsmaßnahmen zu präventivpolizeilichen Zwecken durchzuführen, in den letzten Jahrzehnten stetig ausgebaut. Der präventivpolizeiliche Befugnisbereich steht heute nach vielen Landesgesetzen sowie auf Bundesebene insbesondere nach dem BKAG hinter dem strafprozessualen Überwachungsinstrumentarium nicht mehr zurück und geht teils – etwa bei der optischen Wohnraumüberwachung – sogar darüber hinaus. Darüber hinaus haben in der Vergangenheit viele Polizeigesetze präventivpolizeiliche Überwachungsmaßnahmen auch zu dem Ziel ermöglicht, die dadurch gewonnenen Erkenntnisse später in Strafverfahren einzuführen. Landesrechtliche Ermächtigungen mit dieser Zielsetzung sind allerdings kompetenzrechtlich nach einer Grundsatzentscheidung des BVerfG allenfalls in engen Grenzen zulässig.⁴³ Gleichwohl lassen sich gerade im Bereich der Terrorismusbekämpfung, wo es darum geht, drohende strafbare Schädigungshandlungen möglichst zuverlässig zu verhindern, Überwachungsmaßnahmen in der Regel auch mit rein präventiven Zielen begründen.

Parallel zu dieser Entwicklung wurden das strafrechtliche Sanktionsregime und das Strafverfahren in den letzten Jahren immer mehr in den Dienst einer unmittelbaren Kriminalprävention gestellt, die über die herkömmlichen mittelbaren Präventionsziele dieser Ordnung deutlich hinausgeht. Die präventive Indienstnahme des Strafrechts beruht auf dem Ausbau abstrakter Gefährdungsdelikte, die Handlungen unter Strafe stellen, welche teilweise weit im Vorfeld der Schädigung von Rechtsgütern angesiedelt sind. Gerade das Terrorismusstrafrecht zeichnet sich durch eine besonders weitreichende Vorfeldkriminalisierung aus. Zu nennen sind zum einen die auf die Beteiligung an terroristischen Vereinigungen oder die Unterstützung solcher Vereinigungen bezogenen Organisationsdelikte in §§ 129a f. StGB, zum anderen die nahezu flächendeckende Kriminalisierung von Vorbereitungs- und Unterstützungshandlungen zu terroristischen Gewalttaten durch §§ 89a ff. StGB.⁴⁴ Diese Tatbestände eines kriminalpräventiven Strafrechts ermöglichen frühzeitige strafprozessuale Ermittlungen in Situationen, in denen Schäden weder eingetreten sind noch unmittelbar bevorstehen. Zudem eröffnen sie den Anwendungsbereich des eingriffsintensiven strafrechtlichen Rechtsfolgenregimes unabhängig von eingetretenen Rechtsgutsverletzungen. Sie ermöglichen damit insbesondere, gefährliche Individuen mit strafrechtlichen Mitteln unschädlich zu machen.⁴⁵

Der parallele Ausbau präventivpolizeilicher Überwachungsermächtigungen und strafrechtlicher Vorfeldtatbestände führt gerade im Bereich der Terrorismusbekämpfung dazu, dass es häufig zu Gemengelagen zwischen Strafverfolgung und Gefahrenabwehr kommt. Eine solche Gemengelage entsteht, wenn ein strafprozessualer Anfangsverdacht besteht und zugleich die Voraussetzungen einer präventivpolizeilichen Eingriffsermächtigung erfüllt sind, weil von dem Verdächtigen weitere Straftaten erwartet werden. Es ist aus verschiedenen Gründen erforderlich, eine polizeiliche Eingriffsmaßnahme dem Polizei- oder dem Strafprozessrecht zuzuordnen. Prozessual entscheidet diese Abgrenzung darüber, welcher Rechtsweg gegen die Maßnahme eröffnet ist. Materiellrechtlich folgt aus ihr, welche Regelungen die Maßnahme anleiten und unter welchen Voraussetzungen sie zulässig ist. Institutionell bestimmt sie darüber, bei welcher Stelle die Verfahrensherrschaft liegt. Dieses Problem ist im Grundsatz seit langem be-

⁴³ BVerfGE 113, 348 (367 ff.).

⁴⁴ Näher Bäcker, Kriminalpräventionsrecht, S. 323 ff.

⁴⁵ Näher zu den strafprozessualen Funktionen des kriminalpräventiven Strafrechts Bäcker, Kriminalpräventionsrecht, S. 335 ff.

kannt und wird unter dem Schlagwort der doppelunktionalen Maßnahme erörtert. Die „klassische“ Diskussion um doppelunktionalen Maßnahmen der Polizei⁴⁶ befasst sich allerdings mit punktuellen Abgrenzungsproblemen in akuten Krisenlagen. Beim heutigen Stand der Rechtsgrundlagen der Terrorismusbekämpfung stellt die Abgrenzung von Strafprozessrecht und Polizeirecht in diesem Bereich hingegen ein Strukturproblem dar. In einer solchen strukturellen Gemengelage überlagern beide Regime einander nicht nur zeitlich, sondern auch sachlich. Dies gilt insbesondere für Überwachungsmaßnahmen. Solche Maßnahmen können einerseits dazu genutzt werden, die mutmaßlich bereits begangene Vorfeldstraftat aufzuklären. Dazu bedarf es einer Ermächtigung in der Strafprozessordnung. Andererseits können Überwachungsmaßnahmen gleichermaßen nützlich sein, um die drohenden Bezugstaten zu verhindern oder ihre spätere Strafverfolgung zu ermöglichen. Diese Erkenntnisziele lassen sich nach derzeitigem Rechtsstand nur auf der Grundlage polizeirechtlicher Eingriffsermächtigungen verfolgen. Oftmals werden dieselben Überwachungsmaßnahmen für alle denkbaren Erkenntnisziele nützlich sein. Gleichzeitig ist die Frage, nach welchem Rechtsregime sich eine Überwachungsmaßnahme richtet, auch für das institutionelle Verhältnis von Polizei und Staatsanwaltschaft bedeutsam.

Maßgebliches Abgrenzungskriterium ist im Ausgangspunkt das Ziel der einzelnen Überwachungsmaßnahme. Allerdings lassen sich gerade Überwachungen bei der Terrorismusbekämpfung vielfach nicht eindeutig zuordnen. Die Strafprozessordnung und die Polizeigesetze regeln keinen Vorrang der einen oder der anderen Ordnung. Auch das strafprozessuale Legalitätsprinzip zwingt nicht dazu, dem Strafverfahrensrecht den Vorrang einzuräumen, da es einer vorübergehenden Zurückstellung der Strafverfolgung mit strategischer Zielsetzung nicht entgegensteht.⁴⁷ In der Folge hat die Polizei ein Wahlrecht, auf welches Regime sie eine Überwachungsmaßnahme stützt, sofern die jeweils maßgeblichen Tatbestandsvoraussetzungen erfüllt sind.⁴⁸

Die partielle rechtliche Wahlfreiheit der Polizei zwischen Strafprozess- und Polizeirecht führt dazu, dass die Polizei ihr Verhältnis zu der Staatsanwaltschaft in erheblichem Umfang selbst definieren kann. Insbesondere kann sie entscheiden, wann und inwieweit sie das polizeirechtliche Verfahren in ein Ermittlungsverfahren nach der Strafprozessordnung überleitet.⁴⁹ Auch hinsichtlich der Informationen, die die Polizei in dieses Verfahren einbringt, genießt sie ein (zumindest partielles) Selektionsmonopol. Zudem kann der Rückgriff auf präventivpolizeiliche Überwachungsermächtigungen dazu führen, dass Schutzvorkehrungen des Strafverfahrensrechts wie Richtervorbehalte⁵⁰ oder Beschuldigtenrechte ganz oder vorübergehend unterlaufen werden.

⁴⁶ Zusammenfassend Schmidbauer, in: Manssen/Jachmann/Gröpl, Nach geltendem Verfassungsrecht, S. 735 (738 ff.).

⁴⁷ BGH, Urteil vom 26. April 2017 – 2 StR 247/16 –, juris, Rn. 32.

⁴⁸ Für einen (mehr oder weniger weitreichenden) Vorrang des Strafverfahrensrechts etwa Müller/Römer, NSTZ 2012, S. 543 (546 f.); Roggan, GSZ 2018, S. 52 (56).

⁴⁹ Ähnlich Roggan, ZRP 2017, S. 208 (209); vgl. ferner mit Blick auf Ermittlungen im Bereich der organisierten Kriminalität Kinzig, StV 2004, S. 560 (561).

⁵⁰ Vgl. als Beispiel den vom BGH entschiedenen Fall einer sogenannten legendierten Kontrolle zur Sicherstellung von Betäubungsmitteln, BGH, Urteil vom 26. April 2017 – 2 StR 247/16.

Auf der Grundlage des geltenden Rechts ist dieser Befund hinzunehmen. Solange die präventivpolizeilichen Überwachungsermächtigungen mit den grundrechtlichen Anforderungen übereinstimmen, gebietet das Grundgesetz nicht, die strukturelle Gemengelage zwischen Gefahrenabwehr und Strafverfolgung allgemeinverbindlich aufzulösen.

Eine Auflösung wäre allerdings verfassungsrechtlich zumindest teilweise zulässig, wenn der Bund von seiner Gesetzgebungsbefugnis für ein strafprozessuales Vorfeldrecht Gebrauch machte. Diese Gesetzgebungsbefugnis ergibt sich daraus, dass der Bund Überwachungsmaßnahmen mit dem Ziel der Strafverfolgung generell regeln darf. Die Bundeskompetenz setzt nicht voraus, dass die geregelten Maßnahmen vom Anfangsverdacht einer Straftat ausgehen. Der Bund könnte daher – soweit er die grundrechtlichen Grenzen wahrt – Überwachungsmaßnahmen auch im Vorfeld des Verdachts regulieren.⁵¹ Ein solches strafprozessuales Vorfeldrecht könnte bereichsspezifisch und darum trennschärfer als das allgemeine Polizeirecht auf die Eingriffsbedürfnisse der Terrorismusbekämpfung zugeschnitten werden und unmittelbar an das hergebrachte Recht des Ermittlungsverfahrens angeschlossen werden. In diesem Rahmen könnten auch Verfahrensregelungen geschaffen werden, um der drohenden partiellen Entkernung der Schutzvorkehrungen des Strafprozessrechts und der Verfahrensherrschaft der Staatsanwaltschaft zu begegnen.⁵²

b) Polizei und Nachrichtendienste

Die eigenhändige Tätigkeit der Nachrichtendienste erschöpft sich nach geltendem Recht darin, Informationen zusammenzutragen und auszuwerten. Sie sollen als „Frühwarnsystem“ potentiell staatsgefährdende Strukturen aufklären und die Regierung über sie informieren. Zur unmittelbaren Sicherheitsgewähr mit Befehl und Zwang sind sie nicht berufen. Vielmehr sind die Nachrichtendienste organisatorisch von den dafür zuständigen Polizeibehörden zu trennen⁵³ und dürfen diese auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen sie selbst nicht befugt sind.⁵⁴

Die Trennung von Polizei und Nachrichtendiensten entspricht ständiger Gesetzgebungspraxis. Verfassungsrechtlich wäre entgegen einer verbreiteten Position⁵⁵ eine Verschmelzung beider Behördentypen zwar teilweise möglich. Sie wäre jedoch weitgehend sinnlos.

Eine Zusammenlegung von Polizeibehörden und Nachrichtendiensten müsste im ersten Schritt die Kompetenzordnung wahren. Der Bund verfügt jedoch für die Gefahrenabwehr mit Befehl und Zwang nur über bereichsspezifische Gesetzgebungs- und Verwaltungskompetenzen. Er kann diese Kompetenzen nicht dadurch erweitern, dass er seine Nachrichtendienste mit der Aufgabe zur Gefahrenabwehr und entsprechenden Befugnissen ausstattet. Dies ist bereits praktisch relevant geworden für die Auslandsaufklärung durch den BND. Hierzu hat das BVerfG ausgeführt, Art. 73 Abs. 1 Nr. 1 GG erlaube dem Bund zwar, eine Stelle zur umfassenden Auslandsaufklärung einzurichten. Die Aufgabe dieser Stelle müsse jedoch auf die politische Aufklärung bezogen bleiben. Der Bundesgesetzgeber dürfe dem BND daher keine Befugnisse ein-

⁵¹ Vgl. BVerfGE 113, 348 (369 ff.).

⁵² Näher Bäcker, Kriminalpräventionsrecht, S. 379 ff., dort mit Blick vor allem auf die Bekämpfung der organisierten Kriminalität.

⁵³ § 2 Abs. 1 Satz 3 BVerfSchG; § 1 Abs. 1 Satz 2 BNDG.

⁵⁴ § 8 Abs. 3 BVerfSchG; § 2 Abs. 3 BNDG.

⁵⁵ Vgl. zu den Ansätzen zu einer verfassungsrechtlichen Fundierung des Trennungsgebots Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, S. 64 f., m.w.N.

räumen, die auf die Verhütung, Verhinderung oder Verfolgung von Straftaten als solche gerichtet seien.⁵⁶ Hingegen stünde die Kompetenzordnung insbesondere einer Ausstattung der Verfassungsschutzbehörden der Länder mit imperativen Befugnissen nicht entgegen.

Die Trennung von Polizei- und Verfassungsschutzbehörden ist jedoch mittelbar im grundrechtlichen Informationsschutz durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 und Art.13 GG verankert.⁵⁷ Diese Grundrechte errichten Anforderungen an behördliche Überwachungen und Datenweiterverarbeitungen, die sich mit zunehmender Eingriffsintensität verschärfen. Um die Eingriffsintensität einer solchen Maßnahme zu ermitteln, kommt es unter anderem auf ihre absehbaren Folgen an.⁵⁸ Denn der grundrechtliche Informationsschutz ist auch ein vorgelagerter Schutz gegen Grundrechtsgefährdungen.⁵⁹ Überwachungen durch Verfassungsschutzbehörden sind für den Betroffenen weniger nachteilträchtig als Überwachungsmaßnahmen anderer Behörden. Grund hierfür ist der politische Beobachtungsauftrag dieser Behörden und das daraus folgende Fehlen imperativer Befugnisse.

Der besondere Aufgaben- und Befugnisbereich der Verfassungsschutzbehörden begründet somit ein verfassungsrechtliches Privileg.⁶⁰ Der Gesetzgeber darf diesen Behörden Überwachungen teils unter niedrigeren Voraussetzungen erlauben als anderen Behörden.⁶¹ Dieses verfassungsrechtliche Privileg verlöre seine Berechtigung, wenn die Verfassungsschutzbehörden mit der Aufgabe zur unmittelbaren eigenhändigen Sozialgestaltung und mit zugehörigen imperativen Befugnissen ausgestattet würden. Die Verfassungsschutzbehörden dürften daher zwar mit solchen Aufgaben und Befugnissen betraut werden, etwa indem sie mit dem polizeilichen Staatsschutz zusammengelegt werden. Ihre informationellen Befugnisse wären dann jedoch an dem grundrechtlichen Standard zu messen, der für polizeiliche Überwachungen und Datenweiterverarbeitungen maßgeblich ist. Eine Sicherheitsbehörde, die zugleich weitreichende Überwachungsbefugnisse im Vorfeld konkreter sozialer Konflikte und schlagkräftige Eingriffsbefugnisse zur Bewältigung solcher Konflikte hat, kann deshalb in der Bundesrepublik nicht errichtet werden. Durch eine Zusammenlegung von Verfassungsschutz und Polizei entstünde also letztlich nur eine größere Polizei, die den verfassungsrechtlichen Anforderungen an die polizeiliche Tätigkeit ohne Abstriche genügen müsste.

Das verfassungsrechtliche Privileg für Überwachungen des Verfassungsschutzes ist nur dann gerechtfertigt, wenn gewährleistet ist, dass diese Überwachungen tatsächlich auf das Ziel der politischen Vorfeldaufklärung bezogen bleiben. Die Verfassungsschutzbehörden dürfen einerseits nicht zu ständigen Informations Helfern der Polizei werden. Andererseits dürfen sie sich der Polizei nicht bedienen, um ihren Befugnisbereich um imperative Eingriffe zu erweitern. Hierzu bedarf es organisatorischer und prozeduraler Sicherungen.

Verfassungsschutz und Polizei sind daher organisatorisch und befugnisrechtlich voneinander zu trennen. Zudem lässt sich aus dem grundrechtlichen Informationsschutz ein informationelles

⁵⁶ BVerfGE 100, 313 (368 ff.).

⁵⁷ Grundlegende Bedeutung für das Folgende hat insbesondere das Urteil des BVerfG zur Antiterrordatei (BVerfGE 133, 277).

⁵⁸ So etwa BVerfGE 100, 313 (376); 109, 279 (353); 115, 320 (347).

⁵⁹ Deutlich BVerfGE 118, 168 (184 f.); 120, 378 (397).

⁶⁰ Ähnlich Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, S. 407; mit kritischer Stoßrichtung auch Wegener, VVDStRL 75 (2016), S. 293 (312 ff.).

⁶¹ Näher unten III. 1. d).

Trennungsprinzip ableiten.⁶² Zumindest schief ist deshalb die Charakterisierung der Nachrichtendienste als informationelle Dienstleister für andere Sicherheitsbehörden, die insbesondere von Autoren aus dem Umfeld der Dienste vertreten wird.⁶³ Verfassungsschutzbehörden dürfen zwar ihre Erkenntnisse an operativ tätige Behörden wie die Polizei übermitteln, wenn ein hinreichender Übermittlungsanlass vorliegt. Hierbei handelt es sich jedoch nicht um einen Teil ihrer Aufgabe, sondern um eine Änderung des Verarbeitungszwecks der übermittelten Daten.

III. Eingriffsbefugnisse der Sicherheitsbehörden

Hinsichtlich der Eingriffsbefugnisse der Sicherheitsbehörden stehen hier nicht einzelne Eingriffsmaßnahmen, sondern die tatbestandlichen Regelungsmuster von Eingriffsermächtigungen und deren verfassungsrechtliche Grenzen im Vordergrund. Die Anforderungen an die gesetzlichen Eingriffstatbestände bestimmen, wie weitreichend der Befugnisbereich der Sicherheitsbehörden für den Umgang mit noch konturenarmen und typischerweise ambivalenten Bedrohungslagen geöffnet werden kann. Insbesondere stellt sich die Frage, ob und inwieweit Eingriffsmaßnahmen bereits im Vorfeld hergebrachter Eingriffsschwellen ermöglicht werden dürfen. Dies wird im Folgenden vor allem für Überwachungsermächtigungen (unten 1.), ferner cursorisch auch für imperative Eingriffe mit präventivpolizeilicher Zielsetzung (unten 2.) erörtert.

1. Tatbestandsmuster sicherheitsbehördlicher Überwachungsermächtigungen

Die grundrechtlichen Anforderungen an die tatbestandlichen Mindestschwellen von Überwachungsermächtigungen ergeben sich aus dem Gebot, Grundrechtseingriffe im angemessenen Rahmen zu halten, als letzter Komponente des Verhältnismäßigkeitsgrundsatzes.⁶⁴ Damit kommt es maßgeblich darauf an, wie intensiv eine Überwachungsmaßnahme in Grundrechte eingreift. Darüber hinaus hängen die konkreten Anforderungen von den spezifischen Regelungsmodellen und Regelungsmöglichkeiten der unterschiedlichen Regime des Sicherheitsrechts ab und sind daher für die unterschiedlichen Aufgabenbereiche der Sicherheitsbehörden separat zu entwickeln.

a) Intensität von Überwachungseingriffen

Wie streng der verfassungsrechtliche Maßstab ausfällt, hängt von der Eingriffsintensität einer Überwachungsmaßnahme ab. Um diese zu bemessen, zieht das BVerfG ein Bündel von Kriterien heran. Zu ihnen zählen Inhalt und Umfang der Erkenntnisse, die durch eine Überwachungsmaßnahme erlangt werden können, die Überwindung von Wahrnehmungshürden, die Enttäuschung berechtigten persönlichen Vertrauens, die verdeckte Durchführung einer Maßnahme, ihre Streubreite in persönlicher Hinsicht sowie ihre absehbaren Folgen für den Betroffenen.⁶⁵ Es bietet sich an und ist in der jüngeren Rechtsprechung des BVerfG angelegt,⁶⁶ auf der Grundlage dieser Kriterien Intensitätsstufen zu bilden, auf denen grundsätzlich jeweils gleichartige Anforderungen gelten.

Im Folgenden wird dementsprechend ein vierstufiges Modell zugrunde gelegt, das zwischen Eingriffen geringer, mittlerer, hoher und höchster Intensität unterscheidet. Auf der niedrigsten

⁶² BVerfGE 133, 277 (329).

⁶³ Vgl. etwa Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, V § 1 Rn. 7 f.; für die Terrorismusabwehr anscheinend auch Wolff, DVBl 2015, S. 1076 (1078).

⁶⁴ Deutlich BVerfGE 141, 220 (268).

⁶⁵ Näher Bäcker, Kriminalpräventionsrecht, S. 267 ff.

⁶⁶ Vgl. insbesondere BVerfGE 141, 220 (268 ff.).

Intensitätsstufe sind etwa Identitätsfeststellungen oder die Erhebung und Sichtung öffentlich zugänglicher Daten ohne Einsatz komplexer Analysetechnik anzusiedeln. Beispiele für Maßnahmen mittlerer Eingriffsintensität bilden einzelne Bildaufnahmen im öffentlichen Raum und kurzfristige Observationen. Eine hohe Eingriffsintensität weisen etwa Telekommunikationsüberwachungen, der gezielt gegen bestimmte Personen gerichtete Einsatz von verdeckten Ermittlern oder längere Bild- und Tonaufzeichnungen außerhalb von Wohnungen auf. Auf der höchsten Intensitätsstufe sind Wohnraumüberwachungen und „Online-Durchsuchungen“ zu verorten.

Welche Folgerungen aus der Eingriffsintensität von Überwachungsmaßnahmen für deren gesetzliche Regulierung zu ziehen sind, ist getrennt nach Rechtsregimen zu erörtern.

b) Tatbestandsmuster im Polizeirecht

Hergebrachte Eingriffsschwelle des Polizeirechts ist die konkrete Gefahr für ein polizeiliches Schutzgut. Dabei handelt es sich um die situationsbezogene Prognose eines zumindest ansatzweise konturierten Schadensereignisses, in die alle zum Prognosezeitpunkt erkennbaren Umstände aufzunehmen sind.⁶⁷ Um eingriffsintensivere polizeiliche Maßnahmen zu rechtfertigen, kann der hergebrachte Gefahrtatbestand qualifiziert werden. Anknüpfungspunkte hierfür sind die bedrohten Rechtsgüter, der Wahrscheinlichkeitsgrad des polizeilichen Prognoseschlusses und die zeitliche Nähe des drohenden Schadens.

Die verfassungsrechtliche Diskussion der letzten Jahrzehnte hat sich primär darum gedreht, ob und inwieweit polizeiliche Eingriffsmaßnahmen, insbesondere Überwachungsmaßnahmen auch im Vorfeld einer konkreten Gefahr zugelassen werden dürfen. Auf der Grundlage der jüngeren Rechtsprechung des BVerfG stehen Leitlinien für die Antwort auf diese Frage zur Verfügung.

Polizeiliche Überwachungsmaßnahmen geringer und mittlerer Eingriffsintensität lassen sich im Gefahrvorfeld rechtfertigen. Allerdings sind völlig anlasslose Maßnahmen nicht legitimierbar.⁶⁸ Tragfähig sind hingegen insbesondere Eingriffsermächtigungen, die solche Maßnahmen lediglich von einer grob konturierten allgemeinen Bedrohungslage oder von einer unspezifischen personenbezogenen Kriminalprognose abhängig machen. Bei Maßnahmen mittlerer Eingriffsintensität ist darüber hinaus zumindest das Gewicht der Rechtsgüter zu steigern, zu deren Schutz die Überwachung dienen darf.

Demgegenüber bestehen für Maßnahmen hoher und höchster Eingriffsintensität strengere Anforderungen an den tatsächlichen Eingriffsanlass. Das BVerfG hat in seinem Urteil zum BKAG diese Anforderungen präzisiert und konsolidiert. Neben der hergebrachten Eingriffsschwelle einer polizeilichen konkreten Gefahr nennt das Gericht zwei weitere Schadensprognosen, die auch einen intensiven Überwachungseingriff legitimieren können:

Erstens sei dies der Fall, wenn

„sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf,

⁶⁷ Eingehend Bäcker, Kriminalpräventionsrecht, S. 78 ff.

⁶⁸ Näher Bäcker, Kriminalpräventionsrecht, S. 217 f.

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“.⁶⁹

Hierbei geht es anscheinend um eine situationsbezogene Schadensprognose, bei der jedoch noch Informationslücken bestehen. Entgegen der erkennbaren Intention des Bundesverfassungsgerichts wird damit der Handlungskreis der Polizei gegenüber den hergebrachten Regelungsmustern des Polizeirechts nicht erweitert. Dieses Kriterium lässt sich vielmehr als Beschreibung des Gefahrverdachts in herkömmliche polizeirechtliche Terminologie „übersetzen“.

Zweitens dürften

„[i]n Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, [...] Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird.“⁷⁰

Hierdurch wird die verfassungsrechtliche Mindesteingriffsschwelle gegenüber dem hergebrachten polizeilichen Gefahratbestand wesentlich erweitert. In dieser Fallkonstellation knüpft der Überwachungseingriffe an eine nicht situationsbezogene, sondern personenbezogene Prognose an.⁷¹ Statt einer Gefahr bildet also ein „Gefährder“ den Anlass der Überwachung. So werden längerfristige Überwachungen gefahrträchtiger Individuen oder krimineller Strukturen ermöglicht.

Anzumerken bleibt, dass das BVerfG diese Erweiterung der Mindesteingriffsschwelle – anders als die vorausgegangene Reformulierung des Gefahrverdachts – ausdrücklich auf die Terrorismusbekämpfung und die auf diesem Feld bestehenden besonderen Ermittlungsschwierigkeiten bezieht. Daraus lässt sich folgern, dass auf anderen präventivpolizeilichen Tätigkeitsfeldern – beispielsweise bei der Bekämpfung der organisierten Kriminalität – Überwachungseingriffe hoher und höchster Intensität nicht an eine lediglich personenbezogene Prognose geknüpft werden dürfen. Die in der Landesgesetzgebung erkennbare Tendenz, darüber hinaus personenbezogene Prognosen allgemein zur Grundlage polizeilicher Überwachungseingriffe zu machen,⁷² steht mit der Rechtsprechung des BVerfG nicht in Einklang.

Die Überwachungsermächtigungen des neu gefassten BKAG, die sich eng an die Formulierungen des BKAG-Urteils anlehnen, genügen hingegen den verfassungsrechtlichen Anforderungen im Wesentlichen.

⁶⁹ BVerfGE 141, 220 (272).

⁷⁰ BVerfGE 141, 220 (272 f.).

⁷¹ Insoweit wie hier, wenngleich mit abweichenden Konkretisierungen und Folgerungen Darnstädt, DVBl 2017, S. 88 (92 ff.).

⁷² Vgl. insbesondere den 2017 in Art. 11 Abs. 3 Satz 1 Nr. 1 bayPAG aufgenommenen Begriff der „drohenden Gefahr“ und zu Recht kritisch dazu Löffelmann, BayVBl 2018, S. 145 (146 ff.).

c) Tatbestandsmuster im Strafprozessrecht

Weniger große Regelungsprobleme als im Polizeirecht stellen sich nach aktuellem Stand für strafprozessuale Überwachungsermächtigungen. Grund hierfür ist, dass das geltende Strafverfahrensrecht Überwachungsmaßnahmen praktisch durchweg an den hergebrachten strafprozessualen Verdachtstatbestand bindet. Die Überwachung setzt danach den Verdacht einer Straftat voraus und muss dem Ziel dienen, diese Straftat aufzuklären.⁷³

Der strafprozessuale Verdachtstatbestand kann hinsichtlich des tatsächlichen Eingriffsanlasses grundsätzlich auch Maßnahmen hoher und höchster Eingriffsintensität verfassungsrechtlich rechtfertigen. Gesteigerte Anforderungen je nach Eingriffsintensität ergebe allerdings an die Straftaten, die mit einer Überwachungsmaßnahme aufgeklärt werden sollen. Denn eingriffsinensitive Überwachungsmaßnahmen lassen sich nur legitimieren, wenn das staatliche Strafverfolgungsinteresse hinreichend schwer wiegt. Um das Gewicht des Strafverfolgungsinteresses zu bemessen, knüpft das Bundesverfassungsgericht insbesondere an die Systematik der gesetzlichen Strafrahmen an.⁷⁴

Darüber hinaus wäre es vorstellbar, in einem strafprozessualen Vorfeldrecht für Überwachungsmaßnahmen mit dem Ziel der Strafverfolgung von dem hergebrachten Verdachtstatbestand abzurücken, insbesondere um frühzeitige Überwachungen von gefährlichen Individuen oder die breit angelegte Ausleuchtung komplexer Strukturen des internationalen Terrorismus zu ermöglichen.⁷⁵ Denkbar wäre etwa, an dem Erfordernis eines Tatverdachts festzuhalten, die Überwachung aber für Erkenntnisziele zu ermöglichen, die über die Aufklärung dieses Verdachts hinausgehen. Daneben könnten die für präventivpolizeiliche Überwachungsmaßnahmen entwickelten Regelungsmuster genutzt und mit dem Ziel der Strafverfolgung verknüpft werden.

d) Tatbestandsmuster im Nachrichtendienstrecht

Noch weitgehend ungeklärt sind die verfassungsrechtlichen Anforderungen an Überwachungsermächtigungen im Nachrichtendienstrecht. Zwar hat sich das BVerfG mit einzelnen Ermächtigungen bereits befasst.⁷⁶ Die bisherige Rechtsprechung bildet jedoch noch kein kohärentes Ganzes und bedarf im Licht des BKAG-Urteils teils einer kritischen Evaluation, um die Anforderungen zu präzisieren und zu konsolidieren, wie es dieses Urteil für das Polizeirecht geleistet hat.

Die nachrichtendienstliche Aufklärung verfolgt – insoweit wie polizeiliche Überwachungsmaßnahmen – präventive Ziele. Sie dient der Früherkennung verfassungsfeindlicher Bestrebungen und Strukturen und der politischen Information der Regierung darüber. Dementsprechend wird die Aufklärungstätigkeit der Nachrichtendienste weiter im Vorfeld verortet als die der Polizei. Im Gegenzug verfügen die Nachrichtendienste nicht über Befugnisse zu imperativen Befehls- und Zwangsmaßnahmen. Daher verwenden die Nachrichtendienstgesetze zur Beschreibung von Eingriffsanlässen und -zielen offenere Begriffe als im herkömmlichen Polizeirecht üblich. Insbesondere beruhen nachrichtendienstliche Aufklärungsmaßnahmen überwiegend nicht auf einer Schadensprognose im Einzelfall, sondern auf einem personen- oder strukturbezogenen Verdacht nachrichtendienstrelevanter Bestrebungen. Dies schließt Bestrebungen ein, die zumindest gegenwärtig mit legalen Mitteln verfolgt werden.

⁷³ Näher Bäcker, Kriminalpräventionsrecht, S. 104 ff., 301 ff.

⁷⁴ BVerfGE 109, 279 (347); 125, 260 (329); 129, 208 (243).

⁷⁵ Siehe zur Kompetenzrechtslage oben II. 2. a).

⁷⁶ Vgl. BVerfGE 100, 313; 120, 274; 125, 260 (331 f.); 130, 151 (206).

Für Überwachungsmaßnahmen geringer und mittlerer Eingriffsintensität bestehen gegen diese offene Fassung des Eingriffsanlasses keine verfassungsrechtlichen Bedenken. Bei Maßnahmen mittlerer Intensität sind allerdings gehobene Anforderungen an das Gewicht der diagnostizierten Bestrebungen zu stellen. Darüber hinaus liegen den Nachrichtendienstgesetzen teilweise Fehleinschätzungen über die Eingriffsintensität bestimmter Maßnahmen zugrunde. Beispielsweise machen § 8 Abs. 2 i.V.m. § 9 Abs. 1 BVerfSchG sowie § 9a und § 9b BVerfSchG Maßnahmen wie längerfristige Ton- und Filmaufnahmen außerhalb von Wohnungen sowie den längerfristig gegen bestimmte Einzelpersonen gerichteten Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern lediglich davon abhängig, dass überhaupt Anknüpfungstatsachen bestehen. Dabei handelt es sich um die niedrigste Eingriffsschwelle, die der hohen Eingriffsintensität dieser Überwachungsmaßnahmen⁷⁷ bei weitem nicht Rechnung trägt.

Für Überwachungsmaßnahmen hoher und höchster Eingriffsintensität gleichen sich die Anforderungen an nachrichtendienstliche Überwachungseingriffe stärker den Anforderungen an polizeiliche Maßnahmen an. Für bestimmte Überwachungsmaßnahmen höchster Eingriffsintensität hat das BVerfG dies bereits ausdrücklich ausgeführt.⁷⁸ Auch ansonsten ist eine partielle Konvergenz der verfassungsrechtlichen Anforderungen sachgerecht. Zum einen steht bei der Beurteilung der Eingriffsintensität von Maßnahmen, die tiefgreifend in die informationelle Privatheit der betroffenen Personen eindringen, die Maßnahme selbst stärker im Vordergrund als die drohenden Folgen der Maßnahme, die für die grundrechtliche Privilegierung der nachrichtendienstlichen Aufklärung den Ausschlag geben.⁷⁹ Zum anderen ermöglicht das präventivpolizeiliche Vorfeldrecht der Polizei, gerade eingriffsintensive Überwachungsmaßnahmen für längerfristige, strategisch ausgerichtete Überwachungen krimineller Strukturen zu nutzen. Hierdurch hat sich die polizeiliche Überwachungstätigkeit partiell der nachrichtendienstlichen Aufklärung angenähert. Dieser Prozess wurde bereits als „Vernachrichtendienstlichung“ der Polizeiarbeit bezeichnet.⁸⁰ Das BVerfG hat hiergegen keine generellen Einwände erhoben, für die „nachrichtendienstnahe“ polizeiliche Überwachungstätigkeit jedoch zuletzt im BKAG-Urteil Mindestanforderungen an die gesetzlichen Eingriffsschwellen formuliert. Es liegt nahe, diese Anforderungen auf die Nachrichtendienste zu übertragen. Eine Lockerung der verfassungsrechtlichen Anforderungen erscheint (nur noch) insoweit angezeigt, als den Nachrichtendiensten Überwachungen aufgrund personenbezogener Schadensprognosen auch außerhalb der Terrorismusbekämpfung ermöglicht werden sollten, wenn hinreichend konkrete Tatsachen auf einen hinreichend gewichtigen Schaden hindeuten.

Demgegenüber ermächtigt das gegenwärtige Recht die Nachrichtendienste zu eingriffsintensive Überwachungsmaßnahmen teils weit im Vorfeld konkreter Gefahren. Ein Beispiel bildet die Ermächtigung zu Telekommunikationsüberwachungen im Einzelfall in § 3 G 10, nach der bereits der Verdacht der Planung einer terroristischen Vorbereitungsstraftat für eine Überwachung ausreicht. Hierdurch wird der Eingriffsanlass in tatsächlicher Hinsicht fast vollständig entgrenzt.⁸¹ Eine so weit reichende Überwachungsermächtigung lässt sich auch im Nachrichtendienstrecht verfassungsrechtlich nicht legitimieren.

⁷⁷ Vgl. zu Film- und Tonaufnahmen BVerfGE 141, 220 (287); zum Einsatz von Vertrauenspersonen BVerfGE 141, 220 (294).

⁷⁸ BVerfGE 120, 274 (329 ff.); 125, 260 (331 f.).

⁷⁹ Siehe oben II. 2. b).

⁸⁰ Etwa von Paeffgen, StV 2002, S. 336.

⁸¹ Näher meine Stellungnahme zu der Anhörung des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages am 22. Mai 2014.

2. Imperative präventivpolizeiliche Maßnahmen im Gefahrstofffeld?

Das BKAG-Urteil des BVerfG hat die verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsmaßnahmen weitgehend geklärt und insbesondere das schwierig zu fassende Vorfeld der konkreten Gefahr konturiert. Gegenwärtig stellt sich demgegenüber die Frage, ob und inwieweit auch Ermächtigungen zu imperativen polizeilichen Maßnahmen den Eingriffsanlass in das Gefahrstofffeld verlagern dürfen. Problematisch ist insbesondere, ob die vom BVerfG für Überwachungsmaßnahmen gebilligte personenbezogene Gefährlichkeitsprognose auch solchen Ermächtigungen zugrunde gelegt werden darf, damit die Polizei mit Befehl und Zwang die Schadensneigung gefährlicher Individuen oder Gruppierungen eindämmen kann.

Eine Tendenz zur Ausweitung des präventiven Befugnisbereichs der Sicherheitsbehörden findet sich sowohl in der Rechtsprechung als auch in der Polizeigesetzgebung. Beispiele bilden zum einen die Umdeutung des Gefahrstoffbegriffs in § 58a AufenthG durch das BVerwG,⁸² zum anderen die Ermächtigungen des BKA zu Aufenthaltsvorgaben und Kontaktverboten in § 20y Abs. 1 Nr. 2 und Abs. 2 BKAG (ebenso § 55 Abs. 1 Nr. 2 und Abs. 2 BKAG-neu) sowie die Ermächtigung der bayerischen Polizei zur längerfristigen präventiven Ingewahrsamnahme von „Gefährdern“ in Art. 17 Abs. 1 Nr. 5 bayPAG.

Eine Übertragung der personenbezogenen Gefährlichkeitsprognose auf imperative Maßnahmen ist allerdings problematisch. Zum einen erhöht die Vorverlagerung des Eingriffsanlasses das Prognoserisiko. Soweit die Gefährlichkeitsprognose zur Grundlage von Überwachungsmaßnahmen gemacht wird, lassen sich falsch positive Prognosen in vielen Fällen korrigieren. Bei imperativen Maßnahmen ist dies nicht anzunehmen, da diese Maßnahmen gerade keine Erkenntnisse über die betroffene Person erbringen. Hier fallen die Betroffenen falsch positiver Gefährlichkeitsprognosen im schlimmsten Fall nie auf, selbst wenn sie langfristige intensive Grundrechtseingriffe erleiden. Wenn zum anderen der Prognosegegenstand von einer schadensträchtigen Situation auf ein gefährliches Individuum verlagert wird, verändern gerade imperative Maßnahmen ihren Charakter. Sie werden von einer punktuellen Intervention auf die tendenziell längerfristige Eindämmung eines Risikofaktors umgestellt. Hierdurch erhöht sich ihre typische Eingriffsintensität erheblich.

Angesichts dieser Bedenken können zumindest imperative Maßnahmen hoher und höchster Eingriffsintensität nicht ohne weiteres auf eine personenbezogene Gefährlichkeitsprognose gestützt werden.⁸³ Zumindest müssen Vorgaben an die Grundlage des polizeilichen Prognose-schlusses errichtet werden, die das Risiko einer Fehlprognose abschirmen. Als beispielhaftes Vorbild sei das strafrechtliche Maßregelrecht genannt, das bestimmte präventiv ausgerichtete Eingriffsmaßnahmen im Zusammenhang einer strafrechtlichen Verurteilung ermöglicht, wenn zudem eine hinreichend fundierte Kriminalprognose erstellt wird. Die Vordelinquenz als gerichtlich festgestelltes zurechenbares Verhalten macht das verbleibende – durchaus hohe – Prognoserisiko für den Betroffenen zumutbar. Problematisch ist es hingegen, wenn erhebliche Beeinträchtigungen des Persönlichkeitsrechts wie ein Kontaktverbot oder wenn vielfach irreversible Eingriffe wie die aufenthaltsrechtliche Abschiebung ohne nähere Spezifizierung an die

⁸² Seit BVerwG, Beschluss vom 21. März 2017 – 1 VR 1/17 –, BVerwGE 158, 225.

⁸³ Vgl. für Aufenthaltsgebote Löffelmann, BayVBl 2018, S. 145 (149).

Gefährlichkeit des Betroffenen anknüpfen.⁸⁴ Weder mit Art. 2 Abs. 2 GG⁸⁵ noch mit Art. 5 EMRK⁸⁶ vereinbar sind Ermächtigungen zu einer längerfristigen Ingewahrsamnahme psychisch gesunder „Gefährder“, wenn sie nicht an eine strafrechtliche Verurteilung anknüpfen.⁸⁷

IV. Sicherheitsbehördliche Informationsordnung

Die Informationsordnung der Sicherheitsbehörden befasst sich mit der Weiterverarbeitung personenbezogener Daten, nachdem eine Behörde diese Daten erlangt hat. Die verfassungsrechtlichen Anforderungen an sie entscheiden insbesondere darüber, in welchem Ausmaß die Sicherheitsbehörden Informationen, die sie in einem konkreten behördlichen Verfahren erlangt haben, in andere Verfahren überführen oder an andere Behörden übermitteln dürfen, damit diese sie in weiteren Verfahren einsetzen können. Derartige Datenüberführungen ändern in der Regel den Verarbeitungszweck der überführten Daten im Verhältnis zu dem Zweck, zu dem die Daten ursprünglich erlangt wurden. Solche Zweckänderungen sind verfassungsrechtlich grundsätzlich möglich, unterliegen jedoch grundrechtlichen Anforderungen. Um diese Anforderungen zu konkretisieren, bietet es sich an, von unterschiedlichen Zweckänderungskonstellationen auszugehen, denen teils unterschiedliche Regulierungsmöglichkeiten und verfassungsrechtliche Regulierungserfordernisse entsprechen. Im Folgenden werden dementsprechend getrennt voneinander untersucht Datenüberführungen in ein konkretes einzelnes Zielverfahren derselben oder einer anderen Behörde (unten 1.), komplexere verfestigte informationelle Kooperationen zwischen mehreren Sicherheitsbehörden mit unterschiedlichen Aufgaben (unten 2.) sowie Datensammlungen, welche die Sicherheitsbehörden des Bundes für die Zwecke noch nicht konkret absehbarer zukünftiger Verfahren unterhalten (unten 3.).

1. Datenüberführung in ein einzelnes Zielverfahren

Den Grundfall einer zweckändernden Weiterverarbeitung personenbezogener Daten bildet die Überführung von Daten aus dem Ursprungsverfahren, in dessen Rahmen sie erhoben wurden, in ein einzelnes Zielverfahren, in dem sie weiterverarbeitet werden sollen. Dabei kann es sich um ein Verfahren derselben Behörde handeln, oder die für das Ursprungsverfahren zuständige Behörde übermittelt die Daten an eine andere Behörde, die das Zielverfahren betreibt. Das geltende Sicherheitsrecht errichtet für solche Datenüberführungen keine Voraussetzungen, an denen eine wirksame Terrorismusbekämpfung scheitern könnte. Im Gegenteil stehen die relevanten Regelungen des Bundesrechts nicht in vollem Umfang mit den Grundrechten in Einklang, da sie Datenüberführungen teilweise unter zu niedrigen Voraussetzungen erlauben.

a) Verfassungsrechtlicher Rahmen

Eine Datenüberführung von einem sicherheitsbehördlichen Verfahren in ein anderes ist datenschutzrechtlich als zweigliedriger Vorgang zu konzipieren. Die Daten werden zunächst aus dem Ursprungsverfahren als ihrem bisherigen Verarbeitungskontext gelöst und sodann in das Zielverfahren durch eine Weiterverarbeitung eingebettet. Beide Schritte lassen sich in einer einheitlichen Weiterverarbeitungsermächtigung zusammenfassen, wenn derselbe Gesetzgeber für das

⁸⁴ Unterkomplex ist daher die zu § 58a AufenthG ergangene Kammerrechtsprechung des BVerfG seit BVerfG, Beschluss der 1. Kammer des Zweiten Senats vom 24. Juli 2017 – 2 BvR 1487/17 –, juris; berechtigte Kritik hingegen bei Kießling, NVwZ 2017, S. 1019 (1020 f.).

⁸⁵ Vgl. BVerfGE 109, 190 (220); Müller, Präventive Freiheitsentziehung als Instrument der Terrorismusbekämpfung, S. 72 ff.

⁸⁶ Vgl. EGMR (Große Kammer), Urteil vom 19. Februar 2009, A. u.a. gegen Vereinigtes Königreich, No. 3455/05; ferner EGMR (Fünfte Sektion), Urteil vom 7. März 2013, Ostendorf gegen Deutschland, No. 15598/08; eingehend Müller, Präventive Freiheitsentziehung als Instrument der Terrorismusbekämpfung, S. 86 ff

⁸⁷ Vgl. zu Art. 17 Abs. 1 Nr. 4 und 5 bayPAG Löffelmann, BayVBl 2018, S. 145 (153).

Ursprungs- und das Zielverfahren zuständig ist. Ansonsten bedarf es zweier separater Ermächtigungen. Sofern unterschiedliche Gesetzgeber für die Regelung beider Verfahren zuständig sind, trifft zudem den Gesetzgeber des Ursprungsverfahrens eine grundrechtliche Regelungsverantwortung für die Weiterverarbeitung der Daten, die er aus seinem Regelungsbereich entlässt. Die Überführungsermächtigung im Recht des Ursprungsverfahrens muss daher durch geeignete Tatbestandsvoraussetzungen gewährleisten, dass eine Datenüberführung nur ermöglicht wird, wenn sie mit den materiellen Anforderungen des höherrangigen Rechts übereinstimmt.⁸⁸ Diese Anforderungen ergeben sich aus den Grundrechten des Grundgesetzes sowie auch aus dem europäischen Datenschutzrecht, das seinerseits im Lichte der Unionsgrundrechte auszulegen ist.

Regelmäßig liegt in der Datenüberführung eine Zweckänderung, die besonders gerechtfertigt werden muss. Klärungsbedürftig sind hingegen die materiellen Anforderungen an zweckändernde Weiterverarbeitungen. Das europäische Datenschutzrecht gibt vor, dass Erhebungszweck und Weiterverarbeitungszweck miteinander vereinbar sein müssen,⁸⁹ spezifiziert diese Vorgabe jedoch für den Bereich der Gefahrenabwehr und Strafverfolgung nicht.⁹⁰ Demgegenüber hat das BVerfG in seinem BKAG-Urteil konkretere grundrechtliche Anforderungen an Zweckänderungen entwickelt. Allerdings ist das Urteil in diesem Punkt weniger klar geraten, als es wünschenswert wäre. Zudem dürfte es unionsrechtlich nur teilweise anschlussfähig sein.

Nach dem BKAG-Urteil sind zweckändernde Weiterverarbeitungen verfassungsrechtlich gerechtfertigt, wenn sie dem Kriterium einer hypothetischen Datenneuerhebung genügen. Hierzu muss die Weiterverarbeitung „dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dien[en], die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten“. Hingegen sollen für den tatsächlichen Anlass der Weiterverarbeitung niedrigere Anforderungen gelten als für eine Datenerhebung. Ausreichend sei, dass sich aus den Daten ein „konkreter Ermittlungsansatz“ ergebe. Lediglich wenn die Daten mit Überwachungsmaßnahmen höchster Eingriffsintensität gewonnen wurden, gälten für die Weiterverarbeitung auch in tatsächlicher Hinsicht dieselben Anforderungen wie für die Datenerhebung.⁹¹ Nicht klar ist, was genau das BVerfG unter einem „konkreten Ermittlungsansatz“ versteht. Das Urteil legt verschiedentlich nahe, dass es um ein Wahrscheinlichkeitsurteil über eine begangene Straftat oder eine schadensträchtige Situation geht.⁹² In dieser Interpretation erschließt sich jedoch nicht der Unterschied zum strafprozessualen Anfangsverdacht oder zur präventivpolizeilichen konkreten Gefahr, gegen die das BVerfG das Erfordernis eines „konkreten Ermittlungsansatzes“ ausdrücklich abgrenzt.⁹³

Darüber hinaus führt das BKAG-Urteil eine weitere Kategorie ein, die dem Datenschutzrecht und dem Sicherheitsrecht zuvor fremd war. Der Zweck einer Datenerhebung bestimmt sich

⁸⁸ Vgl. BVerfGE 125, 260 (346); 130, 151 (201); 141, 220 (324).

⁸⁹ Art. 4 Abs. 1 lit. b RL (EU) 2016/680.

⁹⁰ Vgl. zum gleichlautenden Art. 5 Abs. 1 lit. b DSGVO beispielhaft Herbst, in: Kühling/Buchner, DSGVO, Art. 5 Rn. 44: „Der Begriff der Vereinbarkeit oder Kompatibilität ist für sich genommen wenig geeignet, konkrete Maßstäbe für die vorzunehmende Wertung vorzugeben.“ Unklar ist, ob auch im Anwendungsbereich der RL 2016/680 die spezifizierenden Kriterien für die Zweckkompatibilität aus Art. 6 Abs. 4 DSGVO herangezogen werden können, die allerdings ohnehin wesentliche Fragen offen lassen.

⁹¹ BVerfGE 141, 220 (326 ff.).

⁹² Etwa BVerfGE 141, 220 (329).

⁹³ BVerfGE 141, 220 (328).

danach – entsprechend dem für sicherheitsbehördliche Verfahren bislang überwiegenden Verständnis⁹⁴ – zwar nach dem konkreten behördlichen Verfahren, in welchem die Daten erhoben werden. Eine Weiterverarbeitung in anderen Verfahren durch dieselbe Behörde im Rahmen derselben Aufgabe und zum Schutz gleichwertiger Rechtsgüter soll gleichwohl keine Zweckänderung sein, sondern sich als „weitere Nutzung“ im Rahmen des Erhebungszwecks halten. Es soll daher verfassungsrechtlich zulässig sein, die Weiterverarbeitung „unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz“ zu erlauben.⁹⁵ Wiederum ist der – anscheinend zentrale – Begriff des Spurenansatzes wenig klar. Er ist zwar als rechtsdogmatischer Begriff aus dem Strafverfahrensrecht bekannt,⁹⁶ lässt sich insoweit aber nicht auf präventiv ausgerichtete Weiterverarbeitungen übertragen. Möglicherweise handelt es sich überhaupt nicht um eine Voraussetzung der Weiterverarbeitung. Eine Ermächtigung zur völlig anlasslosen Weiterverarbeitung einmal erhobener Daten im Rahmen einer bestimmten behördlichen Aufgabe reicht allerdings potenziell extrem weit und dürfte dem unionsrechtlichen Kriterium der Zweckkompatibilität kaum genügen.⁹⁷ Sollte der Begriff des Spurenansatzes ein rechtliches Erfordernis beschreiben, das die verfassungsrechtlich zulässigen Weiterverarbeitungen durch eine tatsächliche Verarbeitungsschwelle begrenzt, so bleiben sein Gehalt wie auch der Unterschied zu dem für Zweckänderungen erforderlichen konkreten Ermittlungsansatz undeutlich.

b) Zweckänderungen zwischen Gefahrenabwehr und Strafverfolgung

Eine Zweckänderung erhobener Daten, die an dem Kriterium der hypothetischen Neuerhebung zu messen ist, liegt bei der polizeilichen Tätigkeit insbesondere vor, wenn die Polizei Daten, die sie auf der Grundlage einer präventivpolizeilichen Überwachungsermächtigung erlangt hat, in einem strafprozessualen Ermittlungsverfahren weiterverarbeitet oder umgekehrt.

Eine umfassende Regelung solcher Datenüberführungen, die den im BKAG-Urteil errichteten grundrechtlichen Anforderungen entspricht, enthält § 12 BKAG-neu, der Zweckänderungen zwischen den Aufgabenbereichen des BKA ermöglicht und begrenzt.⁹⁸ Anpassungsbedarf besteht hingegen neben den Polizeigesetzen der Länder auch in der Strafprozessordnung.

§ 481 Abs. 1 Satz 1 StPO erlaubt der Polizei, personenbezogene Daten aus Strafverfahren zweckändernd nach Maßgabe der Polizeigesetze weiterzuverarbeiten.⁹⁹ Diese Norm verfehlt die grundrechtliche Regelungsverantwortung des Bundes als Strafprozessgesetzgeber, soweit sie die zweckändernde Weiterverarbeitung strafprozessual erlangter Daten in das Regelungsermessens der Länder als Polizeigesetzgeber stellt. Es ist vielmehr Aufgabe des Bundes, eine grundrechtskonforme Zweckänderungsschwelle zu formulieren. Eine solche Schwelle findet sich immerhin für eingriffsintensivere Überwachungsmaßnahmen, welche die StPO nur bei dem Verdacht bestimmter Straftaten zulässt, in § 477 Abs. 2 Satz 3 Nr. 1 StPO. Das darin enthaltene Erfordernis einer erheblichen Gefahr für die öffentliche Sicherheit gewährleistet jedoch nicht durchweg, dass die zweckändernde Weiterverarbeitung dem Kriterium einer hypothetischen Datenneuerhebung genügt. Hierzu bedürfte es einer einengenden Aufzählung von

⁹⁴ Müllmann, NVwZ 2016, S. 1692 (1694 f.), m.w.N. aus der Rechtsprechung des BVerfG; allgemein zum datenschutzrechtlichen Zweckbegriff etwa Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts, § 22 Rn. 123 ff.

⁹⁵ BVerfGE 141, 220 (324 ff.).

⁹⁶ Vgl. etwa Eisenberg, Beweisrecht der StPO, Rn. 359.

⁹⁷ Anscheinend a.A. Müllmann, NVwZ 2016, S. 1692 (1695).

⁹⁸ Albers, in: BeckOK DSR, § 49 BDSG Rn. 9.

⁹⁹ Zur Einstufung der Norm als Zweckänderungsermächtigung wie hier Gieg, in: Karlsruher Kommentar zur StPO, § 481 Rn. 1; Wittig, in: BeckOK StPO, § 481 Rn. 1.

Schutzgütern, wie sie die für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen geltende Sonderregelung in § 100e Abs. 6 Nr. 2 Satz 1 StPO enthält.¹⁰⁰ Darüber hinaus gewährleistet § 477 Abs. 2 Satz 3 Nr. 1 StPO den verfassungsrechtlich gebotenen Schutz sensibler Daten auch deshalb nicht umfassend, weil die Strafprozessordnung teilweise eingriffssintensive Überwachungsmaßnahmen, deren präventivpolizeiliche Weiterverarbeitung nur nach Maßgabe einer hypothetischen Datenneuerhebung zugelassen werden darf, ohne Bindung an den Verdacht bestimmter Straftaten zulässt. Beispiele bilden die Erhebung von Telekommunikations-Verkehrsdaten (§ 100g Abs. 1 StPO) oder längerfristige Observationen mit technischen Mitteln (§ 100 Abs. 1 Satz 1 Nr. 2 StPO).

Darüber hinaus lässt die Strafprozessordnung die Weiterverarbeitung von Daten, die mit einer strafprozessualen Überwachungsmaßnahme gewonnen wurden, in zu weitem Umfang für die Zwecke weiterer strafrechtlicher Verfahren zu. Bei einer solchen Weiterverarbeitung handelt es sich zwar nach dem BKAG-Urteil des BVerfG um eine weitere Nutzung, die nicht von einem konkreten Ermittlungsansatz abhängt. Voraussetzung ist jedoch, dass die Weiterverarbeitung hinreichend gewichtigen Zwecken dient, die den verfassungsrechtlichen Mindestschwellen für die Datenerhebung entsprechen. Diese Anforderungen verfehlt § 477 Abs. 2 Satz 2 StPO, der zwar eine Weiterverarbeitung von Daten aus eingriffssintensiven Überwachungsmaßnahmen zu Beweis Zwecken beschränkt, eine Weiterverarbeitung als bloßer Spurenansatz jedoch generell zulässt.¹⁰¹

c) Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden¹⁰²

Besondere Bedeutung für die Terrorismusbekämpfung kommt Datenübermittlungen zwischen Nachrichtendiensten und Polizei- und Strafverfolgungsbehörden zu. Grundrechtlich problematisch sind insbesondere Datenübermittlungen, die von den Nachrichtendiensten ausgehen. Durch eine solche Übermittlung werden die weitreichenden Überwachungsbefugnisse der Nachrichtendienste mit den weitreichenden imperativen Eingriffsbefugnissen der Polizei und der Staatsanwaltschaft verknüpft. Das BVerfG hat daher in seinem Urteil zum ATDG aus dem grundrechtlichen Informationsschutz das Prinzip einer informationellen Trennung dieser Behördentypen abgeleitet.¹⁰³ Auf der Grundlage des später ergangenen BKAG-Urteils lässt sich dieses Prinzip an die allgemeinen Anforderungen für Zweckänderungen anschließen. Auch eine Übermittlung personenbezogener Daten von einem Nachrichtendienst an eine Polizei- oder Strafverfolgungsbehörde ist daher an dem allgemeinen Kriterium einer hypothetischen Datenneuerhebung zu messen. Dieses Kriterium ist immer dann anzuwenden, wenn der Nachrichtendienst die übermittelten Daten mit nachrichtendienstlichen Mitteln gewonnen hat.¹⁰⁴ Die Übermittlungsermächtigungen im geltenden Recht der Nachrichtendienste des Bundes genügen dem

¹⁰⁰ Vgl. zu den insoweit maßgeblichen Anforderungen an die Schutzgüter bei eingriffssintensiven präventivpolizeilichen Überwachungsmaßnahmen BVerfGE 141, 220 (287 f.). Zu weit gefasst und zumindest restriktiv auszulegen ist danach auch § 100e Abs. 6 Nr. 2 Satz 2 StPO.

¹⁰¹ Vgl. Eisenberg, Beweisrecht der StPO, Rn. 359, m.w.N. zur Rechtsprechung.

¹⁰² Außer Acht bleiben in der folgenden exemplarischen Darstellung die besonderen Datenübermittlungsermächtigungen des G 10, wenngleich diese ebenfalls teilweise mit den verfassungsrechtlichen Anforderungen nicht in Einklang stehen. Die verfassungsrechtlichen Defizite dieser Vorschriften ähneln den hier erörterten Defiziten des Verfassungsschutzrechts, vgl. beispielhaft zu § 7 Abs. 4 G 10 meine Stellungnahme zu dem Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 2. Juni 2015, BT-Ausschussdr. 18(4)328 A.

¹⁰³ BVerfGE 133, 277 (329).

¹⁰⁴ Näher Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, S. 249 ff.

nicht vollständig. Zugleich begünstigen einige Regelungen im Nachrichtendienstrecht eine übermäßig restriktive Übermittlungspraxis.

Grundvorschrift für Datenübermittlungen der Nachrichtendienste des Bundes an Polizei- und Strafverfolgungsbehörden, die Erkenntnisse aus nachrichtendienstlichen Mitteln umfassen, ist § 19 Abs. 1 Satz 1 BVerfSchG. Diese Vorschrift gilt unmittelbar für das BfV, ist jedoch aufgrund von Verweisungen auch für den BND¹⁰⁵ und den MAD¹⁰⁶ maßgeblich. Sie bindet solche Übermittlungen an besondere Tatbestandsvoraussetzungen, die jedoch teilweise zu weit gefasst sind und darum mit den grundrechtlichen Anforderungen nicht übereinstimmen.

Bedenklich ist zunächst, dass § 19 Abs. 1 Satz 1 Nr. 4 BVerfSchG eine Übermittlung pauschal zur Verfolgung von Straftaten von erheblicher Bedeutung zulässt. Der unscharfe Begriff der Straftat von erheblicher Bedeutung begrenzt insbesondere Übermittlungen von Daten, die durch Überwachungsmaßnahmen hoher Eingriffsintensität wie längerfristige, technisch unterstützte Observationen außerhalb von Wohnungen¹⁰⁷ oder den längerfristigen personengerichteten Einsatz einer Vertrauensperson¹⁰⁸ oder eines Verdeckten Mitarbeiters¹⁰⁹ erlangt wurden, nicht hinreichend, um den grundrechtlichen Anforderungen Rechnung zu tragen.

Noch weitergehende verfassungsrechtliche Bedenken bestehen gegen den in § 19 Abs. 1 Satz 1 Nr. 3 BVerfSchG enthaltenen Übermittlungstatbestand zur Verhinderung oder sonstigen Verhütung von Straftaten von erheblicher Bedeutung.

Erstens wird dieser präventiv ausgerichtete Tatbestand durch den strafprozessualen Begriff der Straftat von erheblicher Bedeutung tendenziell entgrenzt. Soweit durch eine Straftat Schäden für besonders bedeutsame Rechtsgüter drohen, ist ohnehin bereits der Übermittlungstatbestand des § 19 Abs. 1 Satz 1 Nr. 2 BVerfSchG verwirklicht. Allerdings finden sich gerade im Terrorismusstrafrecht zahlreiche Vorfeldtatbestände.¹¹⁰ Viele dieser Straftaten sind schon wegen hoher Strafandrohungen¹¹¹ ohne weiteres als Straftaten von erheblicher Bedeutung anzusehen, die im strafrechtlichen Ermittlungsverfahren eingriffsintensive Überwachungsmaßnahmen rechtfertigen können, wenn ein Tatverdacht besteht. Allerdings führt der materiell-strafrechtliche Vorfeldansatz dazu, dass in beträchtlichem Umfang Handlungen weniger wegen ihres unmittelbaren Schadenspotenzials als deswegen verboten werden, weil sich in ihnen der Wille des Handelnden manifestiert, weitere Straftaten zu begehen. Wenn präventivpolizeiliche Ermächtigungen an solche Vorfeldtatbestände anknüpfen, dehnen sie die strafrechtliche Vorverlagerung noch aus. Sie ermöglichen dann Eingriffsmaßnahmen in weitgehend diffusen und zumeist höchst ambivalenten Bedrohungslagen, in denen Schäden für hochrangige Rechtsgüter allenfalls mittelbar und in geraumer Zeit zu besorgen sind. Mit den verfassungsrechtlichen Geboten der Bestimmtheit und Verhältnismäßigkeit ist dies nicht zu vereinbaren. Präventivpolizeiliche

¹⁰⁵ § 24 Abs. 1 Satz 2 BNDG.

¹⁰⁶ § 11 Abs. 1 Satz 1 MADG.

¹⁰⁷ § 8 Abs. 2, § 9 Abs. 1 BVerfSchG

¹⁰⁸ § 9b BVerfSchG

¹⁰⁹ § 9a BVerfSchG

¹¹⁰ Siehe oben II. 2. a).

¹¹¹ Vgl. beispielhaft § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) – Freiheitsstrafe von sechs Monaten bis zu zehn Jahren; § 129a Abs. 1 und 2 StGB (Bildung einer terroristischen Vereinigung) – Freiheitsstrafe von einem Jahr bis zu zehn Jahren.

Eingriffsermächtigungen dürfen daher grundsätzlich nicht auf strafrechtliche Vorfeldtatbestände verweisen.¹¹² Für Übermittlungsermächtigungen zu präventivpolizeilichen Zwecken gilt dies ebenso.

Zweitens ermöglicht § 19 Abs. 1 Satz 1 Nr. 3 BVerfSchG Datenübermittlungen auch, um Straftaten zu verhüten. Der Begriff der Straftatverhütung soll nach der Gesetzesbegründung dieser Vorschrift – die sich mit Teilen der Gesetzgebungspraxis, Rechtsprechung und Literatur zum Polizeirecht deckt¹¹³ – auf Bedrohungslagen im Vorfeld konkreter Gefahren verweisen.¹¹⁴ Es fehlt damit an dem verfassungsrechtlich gebotenen Erfordernis eines konkreten Ermittlungsansatzes. Besonders deutlich wird dies, wenn die Übermittlung dazu dient, ein strafrechtliches Vorfelddelikt zu verhüten, sodass es zu einer doppelten (materiell-strafrechtlichen und prozedural-nachrichtendienstrechtlichen) Vorverlagerung des Übermittlungsanlasses kommt.

Mit den grundrechtlichen Anforderungen nicht vollständig zu vereinbaren ist auch die weitere Übermittlungsermächtigung in § 20 Abs. 1 Satz 1 BVerfSchG.¹¹⁵ Diese Norm enthält eine Übermittlungspflicht zur Verhinderung und Verfolgung von Staatsschutzdelikten. Jedoch reicht der in § 20 Abs. 1 Satz 2 BVerfSchG definierte Begriff des Staatsschutzdelikts außerordentlich weit. Bei entsprechender Motivation des Täters umfasst er auch Straftaten von geringem Gewicht wie Beleidigungen oder Sachbeschädigungen, deren Verhinderung oder Verfolgung eine Übermittlung von Daten aus eingriffsintensiven Überwachungsmaßnahmen nicht legitimieren kann.

Insgesamt ermöglichen die Übermittlungsermächtigungen des Nachrichtendienstrechts auch dann, wenn sie auf ihre grundrechtskonformen Gehalte reduziert werden, zum Zweck der Terrorismusbekämpfung alle angezeigten Datenübermittlungen an Polizei- und Strafverfolgungsbehörden. Ein Ausbau dieser Ermächtigungen selbst ist weder zulässig noch erforderlich. Hingegen liegen in zwei Punkten aus sicherheitspolitischer Sicht Korrekturen nahe, um einen reibungslosen Informationstransfer zu gewährleisten.

Erstens ist die in § 20 Abs. 1 Satz 1 BVerfSchG vorgesehene Übermittlungspflicht teils zu eng gefasst. Eine solche Pflicht besteht nach dieser Norm ausschließlich bei Staatsschutzdelikten. Im Übrigen steht die Übermittlung auf der Grundlage von § 19 Abs. 1 Satz 1 BVerfSchG im Ermessen des handelnden Nachrichtendienstes. Dies ist schwer nachvollziehbar, soweit es um besonders schwere Straftaten ohne Staatsschutzbezug geht.

Zweitens erscheint § 23 Nr. 2 BVerfSchG korrekturbedürftig.¹¹⁶ Diese Norm verbietet eine Datenübermittlung, wenn ihr überwiegende Sicherheitsinteressen entgegenstehen. Hierzu zählen insbesondere Anliegen des Quellen- und Methodenschutzes.¹¹⁷ Es spricht viel dafür, dass diese Regelung in der Vergangenheit teils vorschnell herangezogen wurde, um nachrichtendienstliche Informationsbestände auch in schwerwiegenden Fällen gegen Polizei- und Strafver-

¹¹² Näher Bäcker, in: Festschrift für Schenke, S. 331 (343 ff.); noch weitergehend BVerfGE 125, 260 (329).

¹¹³ Vgl. etwa Denninger, in: Lisken/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. D 1 ff.

¹¹⁴ BT-Drs. 18/4654, S. 34.

¹¹⁵ Eingehend zu den Defiziten von § 20 BVerfSchG Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, S. 318 ff.

¹¹⁶ Näher Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, S. 361 ff.; wie hier auch Bergemann, NVwZ 2015, S. 1705 (1708).

¹¹⁷ Siems, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 7 Rn. 30.

folgungsbehörden abzuschotten. Daher sollte das Übermittlungsverbot tatbestandlich spezifiziert¹¹⁸ und ein Verfahren eingerichtet werden, um die Anwendung dieser Norm zu kontrollieren. Denkbar wäre etwa, die Entscheidung darüber, ob die Voraussetzungen des Übermittlungsverbots vorliegen, auf die oberste Dienstbehörde zu verlagern.¹¹⁹

2. Verfestigte informationelle Kooperationen von Sicherheitsbehörden

Neben dem punktuellen Informationsaustausch durch Datenübermittlungen unterhalten die Sicherheitsbehörden des Bundes und der Länder im Bereich der Terrorismusbekämpfung verfestigte Kooperationsverhältnisse zum Austausch und zur (teils gemeinsamen) Analyse relevanter Informationen. Diese Kooperationsverhältnisse werfen aus verfassungsrechtlicher Sicht teilweise spezifische Regelungsfragen auf, die das geltende Recht nicht vollständig bewältigt. In den Grundzügen, wenn auch nicht in allen Einzelheiten verfassungskonform ausgestaltet sind die Rechtsgrundlagen für gemeinsame Dateien der Sicherheitsbehörden. Für die praktisch wohl noch bedeutsameren gemeinsamen Zentren fehlt es hingegen bisher an der erforderlichen Rechtsgrundlage.

a) Gemeinsame Dateien

Als ständige gemeinsame Datei zahlreicher Sicherheitsbehörden von Bund und Ländern – darunter sowohl Polizei- und Strafverfolgungsbehörden als auch Nachrichtendienste – hat das ATDG für die Bekämpfung des internationalen Terrorismus die Antiterrordatei errichtet. Grundsätzlich ist diese Datei als bloße Indexdatei konzipiert, die einen Informationsaustausch zwischen den teilnehmenden Behörden auf der Grundlage der jeweils maßgeblichen Übermittlungsermächtigungen vorbereiten soll. Insoweit ist sie, nachdem der Gesetzgeber auf ein Urteil des BVerfG hin einige verfassungsrechtliche Defizite weitgehend abgestellt hat, im Wesentlichen mit dem Grundgesetz vereinbar.¹²⁰

Verfassungsrechtlichen Bedenken unterliegt hingegen die erst nach dem ATDG-Urteil des BVerfG geschaffene Ermächtigung zu einer erweiterten Nutzung der in der Antiterrordatei bevorrateten Daten aus § 6a ATDG.

Bei der erweiterten Nutzung handelt es sich gemäß § 6a Abs. 5 ATDG um eine komplexe – typischerweise informationstechnisch unterstützte – Auswertung der gespeicherten Datenbestände, um aus ihnen neue Informationen etwa über geografische oder soziale Zusammenhänge zu gewinnen. Sie geht über die prinzipielle Indexfunktion der Antiterrordatei weit hinaus und überschreitet auch den Rahmen einer punktuellen Eilfallnutzung, die als Verfahren für eine vereinfachte und beschleunigte Datenübermittlung in § 5 Abs. 2 ATDG verfassungskonform geregelt ist.¹²¹ Im Rahmen einer erweiterten Nutzung dient die Antiterrordatei der nutzenden Behörde als Datenpool, aus dem sie mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse schöpfen kann. Dies schließt etwa mehrstufige Analysen ein, die zunächst Verdachtsmomente überhaupt erst hervorbringen sollen, auf denen dann weitere Analyseschritte aufbauen. Eine teilnehmende Behörde kann so mittels einer erweiterten

¹¹⁸ In Betracht kommen insbesondere Rückausnahmen von dem Übermittlungsverbot und präzisere Abwägungsregeln, vgl. beispielhaft den Regelungsvorschlag im Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus, Rn. 721.

¹¹⁹ Hierfür Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, S. 594 ff., der insgesamt acht Regelungsmodelle für die Zuständigkeit erörtert.

¹²⁰ Vgl. zu einigen durch die Gesetzesänderung nicht behobenen Defiziten des ATDG meine Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 17. September 2014, BT-Ausschussdr. 18(4)144 B.

¹²¹ Vgl. BVerfGE 133, 277 (364 f.).

Nutzung Informationen erzeugen, die sie mit Hilfe gezielter Übermittlungsersuchen oder einzelner Suchabfragen nicht beschaffen könnte, weil sie im Voraus nicht genau angeben könnte, welche Daten sie benötigt. Die Ermächtigung zu erweiterten Nutzungen hebt damit das vom BVerfG formulierte informationelle Trennungsprinzip zwischen Nachrichtendiensten und Polizeibehörden¹²² bereichsspezifisch auf und ersetzt es durch ein informationelles Verfügbarkeitsprinzip.

Diese weitreichende Nutzungsermächtigung ermöglicht einen besonders schweren Grundrechtseingriff,¹²³ dessen Gewicht über eine Datenübermittlung noch erheblich hinausgeht.¹²⁴ Zur Legitimation dieses Eingriffs kann daher nicht auf das für Datenübermittlungen maßgebliche Kriterium der hypothetischen Datenneuerhebung zurückgegriffen werden. Es bedarf vielmehr eines deutlich restriktiveren Eingriffstatbestands, der sich an den Anforderungen für Überwachungseingriffe hoher Intensität orientiert.

Die Eingriffsschwellen, die das ATDG für erweiterten Nutzungen vorsieht, erfüllen diesen Maßstab durchweg nicht. § 6a Abs. 1 ATDG ermöglicht eine erweiterte Nutzung zur Analyse terroristischer Bestrebungen. Tatbestandlich setzt die Norm lediglich eine grob konturierte Bedrohungslage voraus, nicht aber eine konkrete situationsbezogene Schadens- oder personenbezogene Gefährlichkeitsprognose. Die Beschränkung der Ermächtigung auf ein einzelndfallbezogenes Projekt ändert hieran nichts, wie die sehr pauschale Definition des Projektbegriffs in § 6a Abs. 4 ATDG zeigt. Die Norm verlagert den Eingriffsanlass damit erheblich ins Vorfeld konkreter Gefahren.¹²⁵ Dies ist selbst bei Analyseprojekten von Nachrichtendiensten – auf welche die Ermächtigung ihrem Wortlaut nach nicht beschränkt ist – nicht mehr hinnehmbar. § 6a Abs. 2 ATDG lässt eine erweiterte Nutzung zur Strafverfolgung zu, beschränkt diese jedoch nicht durchweg auf hinreichend gewichtige Straftaten. Insbesondere gilt dies für die im Katalog des § 6a Abs. 2 Satz 2 ATDG genannten § 89b und § 91 StGB. Schließlich ermöglicht § 6a Abs. 3 ATDG eine erweiterte Nutzung zur Verhinderung von Straftaten, wenn Anhaltspunkte dafür bestehen, dass eine terroristische Straftat begangen werden „soll“. Der Eingriffstatbestand dieser Norm ist hinsichtlich der tatsächlichen Eingriffsschwelle zu unspezifisch gefasst.¹²⁶ Zudem verweist § 6a Abs. 3 Satz 2 ATDG hinsichtlich der drohenden Straftaten auch auf die strafrechtlichen Vorfeldtatbestände in § 89a, § 89b, § 91 und § 129a StGB. Die Kombination von materiell-strafrechtlicher und prozedural-polizeirechtlicher Vorverlagerung lässt den tatsächlichen Eingriffsanlass nahezu vollständig entgrenzen.

Die temporäre Errichtung projektbezogener gemeinsamer Dateien mehrerer Sicherheitsbehörden von Bund und Ländern ermöglichen § 9a BKAG (§ 17 BKAG-neu), § 22a BVerfSchG und § 25 BNDG. Wegen der Eingabe und Weiterverarbeitung der in der Datei enthaltenen Daten verweisen diese Vorschriften auf die Verarbeitungsermächtigungen des jeweiligen behördlichen Fachrechts. Die Ermächtigungen regeln zudem jeweils qualifizierte, an die Aufgaben der dateiführenden Behörde angepasste Voraussetzungen für die Errichtung einer gemeinsamen Datei. Wenn daneben das Erfordernis eines Projektbezugs restriktiv verstanden und auf einen

¹²² BVerfGE 133, 277 (329).

¹²³ Vgl. zu der erheblich weniger weitreichenden Ermächtigung zu einer durch die Antiterrordatei vermittelten Datenübermittlung in Eilfällen BVerfGE 133, 277 (332).

¹²⁴ Roggan, ZRP 2017, S. 208 (210).

¹²⁵ Kutzschbach, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 6 Rn. 159.

¹²⁶ Vgl. zu dem ähnlich gefassten Eingriffstatbestand in § 20g Abs. 1 Satz 1 Nr. 2 BKAG a.F. BVerfGE 141, 220 (291).

konturierten Errichtungsanlass bezogen wird, genügen diese Regelungen den verfassungsrechtlichen Anforderungen.¹²⁷

b) Gemeinsame Zentren

Über die ausdrücklich gesetzlich geregelten Formen einer verstetigten informationellen Kooperation zwischen mehreren Sicherheitsbehörden hinaus arbeiten Sicherheitsbehörden von Bund und Ländern in den sogenannten Gemeinsamen Zentren themenbezogen zusammen. Für den Bereich des internationalen Terrorismus ist das Gemeinsame Terrorismusabwehrzentrum in Berlin zu nennen. Neben täglichen Lagebesprechungen ist die Kooperation dort in mehrere Arbeitsgruppen gegliedert, die teils regelmäßig, teils bedarfsabhängig zusammentreten.¹²⁸

Für die Zentren bestehen – anders als für die sachlich und zeitlich erheblich enger begrenzten projektbezogenen gemeinsamen Dateien – keine besonderen Rechtsgrundlagen. Die Kooperation in den Zentren stützt sich prinzipiell vielmehr auf die allgemeinen Ermächtigungen zu Datenübermittlungen in den Fachgesetzen der beteiligten Behörden. Diese Regelungen reichen jedoch nicht aus, um den Informationsaustausch in den Zentren verfassungsrechtlich zu legitimieren.¹²⁹ Die allgemeinen Übermittlungsermächtigungen sind auf punktuelle informationelle Kontakte und primär auf Übermittlungen zugeschnitten, denen ein Ersuchen der Empfangsbehörde zugrunde liegt. Eine ständige informationelle Kooperation, bei der die beteiligten Behörden einander personenbezogene Informationen überwiegend proaktiv zur Verfügung stellen, hat eine andere Qualität.¹³⁰ Zudem übermitteln die teilnehmenden Behörden in den Zentren einander nicht lediglich Informationen, die sie anschließend je für sich weiterverarbeiten. Vielmehr erstellen sie in den Arbeitsgruppen teils gemeinsame situations- oder personenbezogene Auswertungen. Auf diese Weise bündeln die teilnehmenden Behörden ihre analytischen Fähigkeiten und erzeugen aus den bis dahin verstreuten Einzeldaten neue Informationen, über die bislang keine von ihnen verfügt hat und die so auch keine hätte zusammenstellen können. Dieser Vorgang begründet eigenständige grundrechtliche Risiken, die durch spezifische gesetzliche Ermächtigungsgrundlagen für die Zentren abgeschirmt werden müssen.

Die gebotenen Regelungen müssen die Zentren konstituieren, indem sie ihnen Themen (etwa Kriminalitätsfelder oder Gefahrbereiche) zuweisen und festlegen, welche Behörden an ihnen teilnehmen. Darüber hinaus müssen sie die Informationsverarbeitung in den Zentren durch hin-

¹²⁷ Vgl. den Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, S. 197 f.; a.A. Roggan/Bergemann, NJW 2007, S. 876 (878 f.).

¹²⁸ Vgl. die eingehende Darstellung von Vorgeschichte und Organisation des Gemeinsamen Terrorismusabwehrzentrums bei Sommerfeld, Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), S. 154 ff.

¹²⁹ Vgl. zum Folgenden den Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, S. 172 ff.; zur Gegenauffassung ebd., S. 180 ff. Im Ergebnis wie hier aus der juristischen Literatur Fremuth, AöR 139 (2014), S. 32 (67 ff.); Sommerfeld, Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), S. 258 ff.; Berger, Die Ordnung der Aufgaben im Staat, S. 160 f.; a.A. Rathgeber, DVBl 2013, S. 1009 (1012 f.); Dombert/Räuker, DÖV 2014, S. 414 (416 f.); T. Linke, DÖV 2015, S. 128 (134 f.); ferner Weisser, NVwZ 2011, S. 142 (145 f.), der allerdings eine gesetzliche Grundlage für das GTAZ rechtspolitisch für angezeigt hält.

¹³⁰ Vgl. zur Antiterrordatei selbst in ihrer Grundfunktion als bloße Indexdatei BVerfGE 133, 277 (331); ferner zu der problematischen organisationsrechtlichen Einordnung der Zentren Sommerfeld, Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), S. 217 ff.

reichende Eingriffsschwellen anleiten. Schließlich müssen die Rechtsgrundlagen für die Zentren auch spezifische Kontrollmechanismen schaffen.¹³¹ Die allgemeinen Kontrollen, insbesondere durch die Datenschutzbehörden, beschränken sich zumeist auf einen Teil der Tätigkeit in den Zentren. Denn an den Zentren sind in aller Regel Bundes- und Landesbehörden beteiligt, die Kontrollzuständigkeiten beschränken sich hingegen auf den Bund oder ein Land. Eine solchermaßen föderal beschränkte Kontrolle läuft jedoch Gefahr, die spezifischen grundrechtlichen Risiken, die gerade aus der Bündelung der Informationsbestände und Verarbeitungskapazitäten von Bundes- und Landesbehörden resultieren, nicht vollständig in den Blick zu nehmen.¹³²

3. Verfahrensübergreifende Datensammlungen der Sicherheitsbehörden des Bundes

Verfahrensübergreifende Datensammlungen der Sicherheitsbehörden sollen behördliches Wissen für zukünftige, noch nicht konkret absehbare Verfahren bewahren. Sie sind kein neues Phänomen, ihre praktische Bedeutung und ihr potenzieller Aussagewert haben sich aber mit dem informationstechnischen Fortschritt und dem Vordringen einzelfallübergreifender sicherheitsbehördlicher Handlungskonzepte erhöht. Die verfassungsrechtlichen Anforderungen an solche Datensammlungen sind in der Rechtsprechung bisher nicht umfassend geklärt, lassen sich jedoch auf der Grundlage der Rechtsprechung zu einzelfallbezogenen Datenüberführungen erarbeiten. Auf dieser Grundlage weisen die Rechtsgrundlagen der bei dem BKA und dem BfV geführten Datensammlungen deutliche verfassungsrechtliche Mängel auf.

a) Regulierungsbausteine für und verfassungsrechtliche Anforderungen an sicherheitsbehördliche Datensammlungen

Verfahrensübergreifende Datensammlungen werfen besondere Regelungsprobleme auf, weil zum Zeitpunkt der Speicherung von Daten in einer solchen Sammlung in der Regel noch nicht konkret absehbar ist, zu welchem Zweck genau die Daten einmal genutzt werden sollen. Die Regulierung verfahrensübergreifender Datensammlungen kann darum nicht schlicht Regelungsmuster zugrunde legen, die für die Überführung von Daten in ein einzelnes Zielverfahren entwickelt wurden. Dies gilt auch für die verfassungsrechtlichen Anforderungen an diese Regulierung, die das BVerfG bislang nicht im Einzelnen auszuführen hatte. Die bisherige Rechtsprechung zu Zweckänderungen kann allerdings eine Orientierungshilfe bieten, solange die Unterschiede zwischen einer einzelnen Datenüberführung und der verfahrensübergreifenden Datenbevorratung beachtet werden.

Auf verfahrensübergreifende Datensammlungen übertragen lässt sich die jüngere Rechtsprechung zu den Regelungskompetenzen für die sicherheitsbehördliche Informationsordnung. Die Speicherung erhobener Daten in einer solchen Datensammlung ist grundsätzlich von dem Gesetzgeber der Datenerhebung zu regeln. Wegen seiner grundrechtlichen Regelungsverantwortung muss dieser Gesetzgeber abschließend festlegen, für welche Verarbeitungszwecke die gespeicherten Daten zur Verfügung stehen. Die Gesetzgebungskompetenz für die spätere Weiter-

¹³¹ Näher hierzu der Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, S. 175 f.; ebenso Fremuth, AöR 139 (2014), S. 32 (68); Sommerfeld, Verwaltungsnetze am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), S. 251 ff.; für eine parlamentarische Kontrolle Dombert/Räuber, DÖV 2014, S. 414 (419 f.); a.A. Rathgeber, DVBl 2013, S. 1009 (1014 f.).

¹³² Für die Antiterrordatei hat das Bundesverfassungsgericht deshalb eine Kooperationspflicht der Datenschutzbehörden begründet, BVerfGE 133, 277 (370). Für die wesentlich weitreichendere sicherheitsbehördliche Kooperation in den Zentren erscheint dieser Ansatz nicht ausreichend.

verarbeitung der Daten, durch die diese in ein konkretes behördliches Verfahren überführt werden, richtet sich nach der Kompetenz für dieses Verfahren. Darüber hinaus erlauben die in Art. 73 Abs. 1 Nr. 10 GG enthaltenen Kompetenztitel dem Bund, die zentrale verfahrensübergreifende Bevorratung bestimmter Daten der Polizei- und Verfassungsschutzbehörden von Bund und Ländern bei BKA und BfV anzuordnen und den so gebildeten Datenbestand für Abrufe durch bestimmte Behörden zu öffnen.¹³³

Teils noch ungeklärt sind die grundrechtlichen Anforderungen an verfahrensübergreifende Datensammlungen. Die Ausführungen zu Zweckänderungen im BKAG-Urteil des BVerfG sind ersichtlich auf die unmittelbare Überführung von Daten in ein konkretes Zielverfahren zugeschnitten. Würden sie ohne weiteres auf die Datenbevorratung angewandt, würde dies zu befremdlichen Ergebnissen führen: Eine Datenbevorratung im Rahmen derselben behördlichen Aufgabe wäre danach als weitere Nutzung anlasslos und unbegrenzt zulässig, womit das – durch Unionsrecht verbindlich vorgegebene – datenschutzrechtliche Prinzip der Zweckkompatibilität praktisch ausgehebelt würde. Eine Datenbevorratung mit dem Ziel zweckändernder Weiterverarbeitungen hinge hingegen von einem konkreten Ermittlungsansatz ab. Wird darunter eine zumindest ansatzweise konturierte Verdachts- oder Bedrohungslage verstanden, so läuft dieses Kriterium im Kontext verfahrensübergreifender Datensammlungen leer. Denn solche Datensammlungen sollen gerade dazu dienen, Wissen für noch nicht absehbare Verfahren bereitzustellen.

Angesichts dessen müssen für die verfahrensübergreifende Bevorratung eigenständige grundrechtliche Maßstäbe entwickelt werden. Dabei ist zu beachten, dass die Regulierung verfahrensübergreifender Datensammlungen bei mehreren Parametern ansetzen kann. Im Einzelnen handelt es sich dabei um

1. den Inhalt der Datensammlung, der durch Art und Umfang der gespeicherten Daten bestimmt wird,
2. die Voraussetzungen, unter denen Daten in der Datensammlung gespeichert werden, sowie
3. die Voraussetzungen und die zulässigen Arten einer Nutzung der gespeicherten Daten.

Die Regulierung einer Datensammlung anhand dieser Parameter muss insgesamt gewährleisten, dass die Errichtung der Datensammlung grundrechtlichen Anforderungen genügt. Dabei stehen die Parameter partiell in einem wechselseitigen Kompensationsverhältnis. So sind etwa für inhaltlich weitreichende Datensammlungen, die aufgrund eines nur schwach konturierten Anlasses angelegt werden und aus denen sich sensible Informationen gewinnen lassen, grundsätzlich hohe Anforderungen an die Datennutzung zu stellen.¹³⁴ Die Voraussetzungen an den Anlass der Datennutzung können weiter gefasst werden, wenn die Nutzung der Art nach eng begrenzt wird.¹³⁵ Umgekehrt können offenere Nutzungsvoraussetzungen gerechtfertigt werden, wenn die Datensammlung nach ihrem Inhalt nur begrenzte Risiken für die Betroffenen birgt oder wenn hohe Anforderungen an eine Datenspeicherung bestehen.

¹³³ Vgl. zur Antiterrordatei BVerfGE 133, 277 (317 ff.).

¹³⁴ Vgl. für die umfassende Auswertung der Antiterrordatei in Eilfällen BVerfGE 133, 277 (364 f.).

¹³⁵ Vgl. für die Auflösung einer dynamischen IP-Adresse mittels bevorrateter Verkehrsdaten BVerfGE 125, 260 (340 ff.); für die Nutzung der Antiterrordatei als Indexdatei BVerfGE 133, 277 (360 ff.), anders aber für eine merkmalsbezogene Recherche ebd., S. 363 f.

Das vom BVerfG für zweckändernde Datenüberführungen in ein einzelnes Zielverfahren entwickelte Kriterium der hypothetischen Datenneuerhebung lässt sich heranziehen, um die grundrechtlichen Anforderungen zu konkretisieren, muss dafür allerdings auf den Gesamtprozess der Datenspeicherung und Datenweiterverarbeitung bezogen werden: Es ist insgesamt durch geeignete Speicherungs- und Weiterverarbeitungstatbestände zu gewährleisten, dass diesem Kriterium genügt wird, da es jedenfalls keinen Grund gibt, die zeitlich gestreckte zweckändernde Datenüberführung mittels einer behördlichen Datensammlung gegenüber der unmittelbaren Überführung in ein einzelnes Zielverfahren zu privilegieren.

Darüber hinaus muss die Datenspeicherung in jedem Fall an eine tatsächliche Mindestschwelle gebunden werden. Die völlig anlasslose großflächige Bevorratung sensibler Daten lässt sich unabhängig von den Vorgaben für die Datennutzung nicht rechtfertigen.¹³⁶

b) Informationssystem und Informationsverbund des BKA

Das in wenigen Tagen in Kraft tretende neue BKAG gestaltet die Informationsordnung des BKA fundamental um, indem es die bisher in Dateien gegliederte Informationsordnung des BKA in ein einheitliches Informationssystem¹³⁷ und einen allgemeinen Informationsverbund mit den Landespolizeien¹³⁸ überführt, die jeweils durch ein abgestuftes System von Zugriffsrechten erschlossen werden. Jedoch ist diese neue Ordnung konzeptionell nicht hinreichend fundiert.

Ausgangspunkt zum Verständnis der neuen Informationsordnung des BKA ist § 12 BKAG-neu, der allgemeine Anforderungen an die Weiterverarbeitung von Daten errichtet, die das BKA erlangt hat. Diese Vorschrift greift die Differenzierung zwischen weiterer Nutzung und hypothetischer Datenneuerhebung aus dem BKAG-Urteil des BVerfG¹³⁹ auf und errichtet für diese jeweils Anforderungen, die den Maßstäben des Urteils entsprechen. Die Norm eignet sich daher ohne weiteres dazu, die Überführung von Daten aus einem Ausgangsverfahren in ein einzelnes Zielverfahren anzuleiten. Hingegen bewältigt sie für sich genommen nicht die Regelungsprobleme, die eine Datenbevorratung in einer verfahrensübergreifenden Datensammlung aufwirft. Dementsprechend stellt § 12 BKAG-neu allein auch keine Rechtsgrundlage für eine solche Datenbevorratung dar. Die Norm wird vielmehr zumindest in einigen Verarbeitungsermächtigungen des Gesetzes in Bezug genommen. Das genaue systematische Verhältnis zwischen diesen Ermächtigungen und § 12 BKAG-neu ist schwierig zu bestimmen. Das neue BKAG lässt sich so verstehen, dass es für die verfahrensübergreifenden Datensammlungen des BKA kaum noch Grenzen enthält. Bemerkenswerterweise lässt sich das Gesetz auch gerade umgekehrt so interpretieren, dass es für die Informationsordnung des BKA überzogene und impraktikable Vorgaben errichtet.

Als Rechtsgrundlagen für verfahrensübergreifende Datenbevorratungen kommen zum einen die allgemeine Weiterverarbeitungsermächtigung in § 16 BKAG-neu, zum anderen die auf die Zentralstellenfunktion des BKA zugeschnittenen Ermächtigungen in § 18 und § 19 BKAG-neu in Betracht. Sie sind sämtlich sowohl auf das interne Informationssystem des BKA als auch

¹³⁶ Vgl. EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele2 Sverige u.a.; EuGH, Gutachten 1/15 vom 26. Juli 2017; EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. und Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04; anders noch, heute jedoch überholt BVerfGE 125, 260.

¹³⁷ §§ 13 ff. BKAG-neu.

¹³⁸ §§ 29 ff. BKAG-neu.

¹³⁹ Siehe oben IV. 1. a).

gemäß § 29 Abs. 4 BKAG-neu auf den polizeilichen Informationsverbund bei dem BKA anzuwenden.

Nach § 16 Abs. 1 BKAG-neu darf das BKA erhobene personenbezogene Daten weiterverarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Zudem müssen die Voraussetzungen von § 12 BKAG-neu vorliegen. Diese Regelung könnte dem BKA nahezu unbegrenzte Datenspeicherungen und Datenüberführungen in seinem internen Informationssystem als weitere Nutzungen im Sinne von § 12 Abs. 1 BKAG-neu ermöglichen, solange sich die Weiterverarbeitung im Rahmen derselben Aufgabe hält. Dies könnte sich insbesondere für die Aufgabe des BKA zur Terrorismusabwehr auswirken.

Eine so weitreichende Bevorratungsermächtigung stünde jedoch mit den Grundrechten nicht in Einklang. Sie lässt sich insbesondere nicht auf das BKAG-Urteil des BVerfG stützen. Das BVerfG hat zwar die mit § 16 Abs. 1 BKAG-NEU vergleichbare Vorschrift des § 20v Abs. 4 Satz 2 Nr. 1 BKAG grundsätzlich für verfassungskonform gehalten.¹⁴⁰ Das Gericht hatte jedoch bei der Prüfung dieser Norm ersichtlich nicht die hier erörterte Datenbevorratung, sondern allein eine Nutzung im Rahmen derselben Aufgabe vor Augen, die unmittelbar an die Datenerhebung oder zumindest an das dieser Datenerhebung zugrundeliegende polizeiliche Verfahren anschließt. Es ging dem Gericht also in gebräuchlicher Terminologie im Wesentlichen um Zufallsfunde. Stattdessen ist § 16 Abs. 1 BKAG-neu als Bevorratungsermächtigung an den hergebrachten Maßstäben zu messen, welche die Rechtsprechung an Datenbevorratungen für sicherheitsbehördliche Zwecke anlegt. Die Datenspeicherung muss daher an einen hinreichenden Anlass gebunden werden. Zudem ist die Überführung der bevorrateten Daten in ein weiteres Verfahren angemessen zu begrenzen.¹⁴¹ Die Verarbeitungsermächtigung in § 16 Abs. 1 BKAG-neu, die beide Verarbeitungsstufen weitgehend freigibt, leistet dies nicht ansatzweise.

Besondere Ermächtigungen zur Weiterverarbeitung von Daten im Rahmen der Zentralstellenaufgabe des BKA und zur Vorsorge für die Verfolgung von Straftaten finden sich in § 18 und § 19 BKAG-neu. Diese Regelungen entsprechen dem bisherigen § 8 BKAG und stimmen mit dieser Norm inhaltlich weitgehend überein.

Damit unterliegen § 18 und § 19 BKAG-neu zunächst den grundrechtlichen Bedenken, die gegen § 8 BKAG seit geraumer Zeit vorgebracht werden.¹⁴²

Problematisch ist die Ermächtigung in § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG-neu, über einen Beschuldigten bestimmte Identifikationsdaten sowie Angaben zu der ihm vorgeworfenen Straftat zu bevorraten. Diese Bevorratungsermächtigung erfordert keine personenbezogene Prognose zukünftiger Straftaten, sondern errichtet eine gesetzliche Vermutung, dass diese Daten allein aufgrund der Beschuldigtenstellung der betroffenen Person für die Zentralstellenaufgabe nützlich sind. Die (weitere) Bevorratung ist nach § 18 Abs. 5 BKAG-neu nur dann unzulässig, wenn das Verfahren gegen die betroffene Person mit einer Entscheidung geendet hat, aus der sich positiv ergibt, dass sie die Tat nicht oder nicht rechtswidrig begangen hat.¹⁴³ Eine solche

¹⁴⁰ BVerfGE 141, 220 (330 ff.).

¹⁴¹ Vgl. die hinsichtlich des konkreten Referenzfalls der Bevorratung von Telekommunikations-Verkehrsdaten mittlerweile überholten Ausführungen in BVerfGE 125, 260 (327 ff.).

¹⁴² Vgl. zur Beurteilung von § 8 BKAG im Einzelnen Bäcker, *Kriminalpräventionsrecht*, 2015, S. 508 ff.

¹⁴³ Vgl. zu § 8 BKAG BVerwG, Urteil vom 22. Oktober 2003 – 6 C 3/03 –, juris, Rn. 13 ff.; Urteil vom 9. Juni 2010 – 6 C 5/09 –, juris, Rn. 25 ff.

Entscheidung ergeht jedoch allenfalls in Ausnahmefällen, da es nicht Aufgabe des Strafverfahrens ist, die Unschuld einer Person zu erweisen.¹⁴⁴ Eine Grenze der Speicherungsbefugnis ergibt sich damit in aller Regel lediglich aus einer normativ nicht weiter angeleiteten Verhältnismäßigkeitsprüfung.¹⁴⁵ Diese sehr weitreichende Bevorratungsermächtigung ist grundrechtlich allenfalls dann hinnehmbar, wenn die Verwertung der gespeicherten Daten eng begrenzt wird. Nicht mehr hinnehmbar ist es insbesondere, wenn die Daten auch genutzt werden können, um einen personengerichteten Verdacht erst zu gewinnen. Im Kontext einer solchen Nutzung wird die gesetzliche Nützlichkeits- zu einer Gefährlichkeitsvermutung über den früheren Beschuldigten, ohne dass die betroffene Person dem etwas entgegensetzen könnte.¹⁴⁶

Offen ist daneben die Grundrechtskonformität von § 18 Abs. 1 Nr. 2 und Nr. 3, Abs. 2 Nr. 2 und Nr. 3 BKAG-neu. Diese Regelungen ermöglichen weitreichende Datenspeicherungen über Beschuldigte und Tatverdächtige, wenn von ihnen in Zukunft Straftaten erwartet werden. Damit knüpfen sie zwar an eine Kriminalprognose an, deren Grundlagen jedoch unsicher bleiben, weil eine positive Feststellung bereits begangener Straftaten nicht gefordert wird. Ausreichend ist ein kriminalistischer Restverdacht gegen die betroffene Person, aus dem auf zukünftiges Fehlverhalten geschlossen wird.¹⁴⁷ Das BVerfG hat zwar diesen Regelungsansatz im Rahmen verschiedener Bevorratungsermächtigungen grundsätzlich akzeptiert.¹⁴⁸ Fraglich ist allerdings, ob er auch Art. 6 RL (EU) 2016/680 i.V.m. Art. 7 und Art. 8 GRCh genügt. Für die Auslegung dieser Normen ist nach Art. 52 Abs. 3 GRCh die Rechtsprechung zu Art. 8 EMRK bedeutsam. Der EGMR hat jedoch die Bevorratung sensibler Daten von Tatverdächtigen, die nicht verurteilt wurden, für konventionswidrig gehalten.¹⁴⁹ Es ist denkbar, dass auch die Bevorratungsermächtigungen in § 18 Abs. 1 Nr. 2 und Nr. 3, Abs. 2 Nr. 2 und Nr. 3 BKAG-neu, die sich gleichfalls auf sensible und aussagekräftige Daten erstrecken, die konventionsrechtlichen Anforderungen und letztlich auch die unionsgrundrechtlichen Maßstäbe verfehlen.

Schließlich ist die in § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 3 BKAG-neu vorgesehene weitreichende Ermächtigung zur Datenspeicherung über „Anlasspersonen“ bedenklich. „Anlasspersonen“ zeichnen sich dadurch aus, dass sie bisher nicht einmal als Beschuldigte oder Tatverdächtige

¹⁴⁴ Ähnlich Spiecker gen. Döhm/Kehr, DVBl 2011, S. 930 (934 f.); Henseler, NWVBl 2015, S. 53 (60 f.); kritisch auch Eisenberg/Singelnstein, GA 2006, S. 168 (177 ff.); ansatzweise Kritik auch bei Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, § 8 BKAG Rn. 33 f.; Kugelmann, BKAG, § 8 Rn. 9.

¹⁴⁵ Vgl. zu dem weitgehend gleichlautenden § 484 Abs. 1 StPO Gieg, in: KK-StPO, § 484 Rn. 3; Wittig, in: BeckOK StPO, § 484 Rn. 1; beide m.w.N.

¹⁴⁶ Vgl. beispielhaft zur praktischen Verwendung der gegenwärtig geführten Gewalttäterdateien die Rechtsprechungsanalyse von Trute, Die Verwaltung 46 (2013), S. 537 (539 ff.), sowie die Sachverhalte von OVG Bremen, Beschluss vom 10. Februar 2010 – 1 B 30/10 –, juris; VG Hamburg, Urteil vom 2. Oktober 2012 – 5 K 1236/11 –, juris: Polizeiliche Platzverweise und Aufenthaltsverbote, die im Wesentlichen auf eine Speicherung der betroffenen Personen in polizeilichen Datenbanken als „Gewalttäter Sport“ beziehungsweise „Straftäterin links motiviert“ gestützt wurden.

¹⁴⁷ Näher und mit Nachweisen zur Rechtsprechung Bäcker, Kriminalpräventionsrecht, S. 510 ff.

¹⁴⁸ Vgl. etwa zu § 81g StPO BVerfGE 103, 21; zur Datenspeicherung in einer Kriminalakte BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 16. Mai 2002 – 1 BvR 2257/01 –, juris; zur Aufbewahrung erkennungsdienstlicher Unterlagen BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 1. Juni 2006 – 1 BvR 2293/03 –, juris, Rn. 11 f.

¹⁴⁹ EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. und Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04, §§ 105 ff.; auf derselben Linie EGMR (V. Sektion), Urteil vom 18. April 2013, M.K. gegen Frankreich, No. 19522/09, §§ 35 ff. Demgegenüber hat der Gerichtshof zwar in einem Fall gegen § 81g StPO keine Bedenken erhoben, dort waren die Beschwerdeführer jedoch wegen bestimmter Anlasstaten der Bevorratung verurteilt worden, so dass diese Entscheidung nichts über die Bevorratung von Daten über bloße Beschuldigte oder Verdächtige aussagt, vgl. EGMR (V. Sektion), Entscheidung vom 4. Juni 2013, Peruzzo und Martens gegen Deutschland, No. 7841/08, 57900/12, §§ 43 ff.

strafrechtlich in Erscheinung getreten sind. Die Datenspeicherung beruht bei ihnen damit auf einer Tatprognose, für die das Gesetz keine Anknüpfungspunkte benennt und die in weitem Umfang etwa auf zulässiges Verhalten oder von der betroffenen Person nicht zu verantwortende äußere Umstände gestützt werden kann.¹⁵⁰ Eine so weitreichende Bevorratungsermächtigung ist mit den Grundrechten nicht mehr zu vereinbaren,¹⁵¹ zumal die vorgesehene Regelung im Vergleich zum heutigen § 8 Abs. 5 BKAG als Grundlage für die Tatprognose nurmehr „tatsächliche Anhaltspunkte“ statt wie bisher „bestimmte Tatsachen“ fordert.¹⁵²

Darüber hinaus schaffen § 18 und § 19 BKAG-neu erhebliche neue Interpretationsprobleme, da ihr systematisches Verhältnis zu § 16 Abs. 1 BKAG-neu und mittelbar zu § 12 BKAG-neu unklar ist.¹⁵³ In der Folge stellt sich die Frage, ob Weiterverarbeitungen auf der Grundlage von § 18 und § 19 BKAG-neu an dem in § 12 BKAG-neu geregelten Kriterium einer hypothetischen Datenneuerhebung zu messen sind. Wird für jede Weiterverarbeitung nach § 18 und § 19 BKAG-neu die Prüfung einer hypothetischen Datenneuerhebung verlangt, so sind die Vorschriften nicht praktikabel. Denn dann hängt nicht nur die Datenüberführung in ein neues polizeiliches Verfahren, sondern bereits die Datenspeicherung davon ab, dass zum Speicherungszeitpunkt ein konkreter Ermittlungsansatz vorliegt. Sicherheitsbehördliche Datensammlungen sollen jedoch Wissen gerade unabhängig von einem solchen Ermittlungsansatz bevorraten. Werden hingegen § 18 und § 19 BKAG-neu so verstanden, dass für die Weiterverarbeitung nach diesen Normen nie eine hypothetische Datenneuerhebung zu prüfen ist, so sind die Vorschriften verfassungswidrig, da die in ihnen enthaltenen Weiterverarbeitungsschwellen für sich genommen nicht den verfassungsrechtlichen Anforderungen an zweckändernde Datenüberführungen genügen. Die in der Sache sinnvolle Lösung, nicht die Datenspeicherung, wohl aber die Datennutzung am Erfordernis einer hypothetischen Datenneuerhebung zu messen, gibt das Gesetz nicht her, da es diese Verarbeitungsformen nicht separat reguliert.

c) Datenverbund der Verfassungsschutzbehörden bei dem BfV

Zu offen gefasst sind die Regelungen über den bei dem BfV geführten Datenverbund der Verfassungsschutzbehörden. Diese Regelungen stehen im Zusammenhang mit der in § 6 Abs. 1 BVerfSchG enthaltenen Pflicht der Verfassungsschutzbehörden, sich wechselseitig die für ihre Aufgaben relevanten Informationen zu übermitteln. Zur Erfüllung dieser Pflicht errichtet § 6 Abs. 2 BVerfSchG einen automatisierten Datenverbund der Verfassungsschutzbehörden, die gemeinsame Dateien bei dem BfV zu führen haben. Diese Regelung gibt den Datenverbund nach allen für die Regulierung verfahrensübergreifender Datensammlungen maßgeblichen Parametern weitgehend frei und wahrt daher nicht mehr das Übermaßverbot.

Erstens enthält § 6 Abs. 2 BVerfSchG keine begrenzenden Vorgaben für den Inhalt der gemeinsamen Dateien. Auch eine Konkretisierung durch außenwirksames abgeleitetes Recht ist nicht vorgesehen. Die Dateien können daher aufgrund beliebig vieler Datenfelder mit jeglichen Daten befüllt werden. Dies schließt Daten ein, die mit eingriffsintensiven nachrichtendienstlichen Mitteln erhoben wurden und bereits deshalb sensibel sind. Zudem ermöglicht § 10 Abs. 2

¹⁵⁰ Vgl. Arzt/Eier, DVBl 2010, S. 816 (818).

¹⁵¹ Wie hier zu § 8 Abs. 5 BKAG Arzt/Eier, DVBl 2010, S. 816 (823); kritisch zu dieser Regelung auch Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, § 8 BKAG Rn. 52, 55f.

¹⁵² Diese Differenzierung ist in der Gesetzgebung verbreitet, wenngleich ihre Handhabbarkeit bezweifelt werden kann, vgl. für das Strafverfahrensrecht Bäcker, Kriminalpräventionsrecht, S. 133 ff.

¹⁵³ Näher meine Stellungnahme zu dem zu dem Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 16. März 2017, BT-Ausschussdr. 18(4)806 D.

BVerfSchG den Verfassungsschutzbehörden, zusätzlich zu den gespeicherten Daten auch Belegdokumente zu den gemeinsamen Dateien hinzu zu speichern. Zusammen genommen mit dem potenziell sehr weitreichenden Relevanzkriterium des § 6 Abs. 1 BVerfSchG¹⁵⁴ und dem gleichfalls extensiven Auswertungsauftrag des BfV aus § 5 Abs. 2 BVerfSchG erlaubt das Gesetz den Verfassungsschutzbehörden im Ergebnis, praktisch ihren gesamten Informationsbestand in digitaler Form in den Datenverbund einzustellen.¹⁵⁵

Zweitens enthält das Gesetz kaum begrenzende Anforderungen an den Anlass einer Speicherung in den gemeinsamen Dateien. Wegen der Speichervoraussetzungen verweist § 6 Abs. 2 Satz 2 BVerfSchG insbesondere auf § 10 Abs. 1 BVerfSchG. Eine Speicherung ist danach primär zulässig, wenn tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen oder Tätigkeiten vorliegen oder wenn sie für die Erforschung und Bewertung solcher Bestrebungen oder Tätigkeiten erforderlich ist. Damit fordert die Norm letztlich nur, dass sich die Speicherung im Rahmen der Aufgaben des Verfassungsschutzes hält.¹⁵⁶ Weitere Restriktionen hinsichtlich des Gewichts der jeweiligen Bestrebungen und Tätigkeiten, hinsichtlich des konkreten Speicherungsanlasses oder hinsichtlich der betroffenen Personen enthält § 10 Abs. 1 BVerfSchG nicht. Die Behördenpraxis mag restriktiver sein und insbesondere die Speicherung an eine bestimmte Beziehung des Betroffenen zu der Bestrebung knüpfen.¹⁵⁷ Dem Wortlaut der Norm lässt sich eine solche Einschränkung jedoch nicht entnehmen. § 10 Abs. 1 BVerfSchG ermöglicht seinem Wortlaut nach im Zusammenwirken mit § 6 Abs. 2 Satz 2 BVerfSchG vielmehr ohne weiteres, Informationen etwa über nicht-dolose Helfer („nützliche Idioten“), flüchtige Kontaktpersonen oder potenzielle Opfer der Angehörigen verfassungsfeindlicher Bestrebungen in die gemeinsamen Dateien aufzunehmen.¹⁵⁸

Drittens enthält das Gesetz kaum Beschränkungen für die Nutzung der gespeicherten Daten. Die Art der Nutzung ist in § 6 Abs. 2 BVerfSchG überhaupt nicht vorgegeben. Die gemeinsamen Dateien können daher für komplexe IT-gestützte Analysen genutzt werden, mit denen etwa Sozialprofile gebildet oder persönliche Eigenschaften und Vorlieben erschlossen werden können.¹⁵⁹ Zudem setzt eine Abfrage von Daten aus einer gemeinsamen Datei nach § 6 Abs. 2 Satz 6 BVerfSchG lediglich voraus, dass sie für die Aufgabenerfüllung des Abfragenden erforderlich ist. Ein besonderer Nutzungstatbestand wird damit nicht geregelt. Insbesondere muss weder ein konkreter Nutzungsanlass bestehen noch muss sich die Abfrage auf Personen beziehen, die in einem spezifischen Näheverhältnis zu einer verfassungsfeindlichen Bestrebung stehen. Die weiteren Regelungen über die Zugriffsberechtigung in § 6 Abs. 2 Sätze 7 und 8 BVerfSchG geben lediglich vor, welche Amtswalter innerhalb einer Behörde die Dateien inwieweit nutzen dürfen. Die weite Abfrageermächtigung des § 6 Abs. 2 Satz 6 BVerfSchG wird

¹⁵⁴ Bergemann, NVwZ 2015, S. 1705 (1706).

¹⁵⁵ Vgl. zur dahingehenden Praxis Kutzschbach, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 6 Rn. 87 ff.

¹⁵⁶ So im Ergebnis auch Kutzschbach, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, VI § 6 Rn. 20.

¹⁵⁷ So implizit die Gesetzesbegründung, vgl. BT-Drs. 18/4654, S. 29; einen Vorschlag für eine restriktivere Interpretation von § 10 Abs. 1 BVerfSchG unterbreitet Bergemann, in: Liskan/Denninger, Handbuch des Polizeirechts (im Erscheinen), Rn. H 97; keine nähere Erläuterung der Tatbestandsvoraussetzungen findet sich bei Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 10 Rn. 4.

¹⁵⁸ Bergemann, NVwZ 2015, S. 1705 (1706).

¹⁵⁹ So deutlich auch die Gesetzesbegründung, BT-Drs. 18/4654, S. 23 f., in Abgrenzung zu „archaischen Arbeitsmitteln“.

damit nicht beschränkt, sondern nur nach Maßgabe der innerbehördlichen Zuständigkeitsordnung verteilt.