Prof. Dr. Matthias Bäcker, LL.M.
...
... Mannheim

Mannheim, den 21. Mai 2019

Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Verfassungsbeschwerde

1. der Frau Ricarda Lang,
   ... München,
2. der Frau Franziska Nedelmann,
   ... Berlin,
3. der Frau Stephanie Dilba,
   ... München,
4. des Herrn Kerem Schamberger,
   ... München,
5. des Herrn S.,
   ... Bremen

g e g e n

§ 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1,

§ 16 Abs. 6 Nr. 2 (auch i.V.m. § 29 Abs. 4 Satz 2),

§ 18 Abs. 1, Abs. 2 und Abs. 5 (auch i.V.m. § 29 Abs. 4 Satz 2),

§ 45 Abs. 1 Satz 1 Nr. 4,

§ 49,

§ 51 Abs. 2

des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG) in der Fassung des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl I S. 1354).

Namens und in Vollmacht der Beschwerdeführerinnen und Beschwerdeführer **(Anlage 1)** erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen des Grundrechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Gliederung

A. Zusammenfassung

Die Verfassungsbeschwerde richtet sich gegen Vorschriften des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (im Folgenden: BKAG). Diese Vorschriften haben zum einen Ermächtigungen des Bundeskriminalamts (im Folgenden: BKA) zum Gegenstand, verdeckte Überwachungsmaßnahmen zum Zweck der Terrorismusabwehr durchzuführen. Zum anderen regeln sie die Bevorratung personenbezogener Daten im Datenbestand des BKA und die spätere Nutzung der bevorrateten Daten.

Soweit die angegriffenen Regelungen Überwachungsermächtigungen enthalten, rügt die Verfassungsbeschwerde zum einen, dass die Ermächtigung des BKA zum Einsatz besonderer Mittel der Datenerhebung (§ 45 BKAG) teilweise die verfassungsrechtlichen Anforderungen verfehlt, die das angerufene Gericht in seinem Urteil zum alten BKAG vom 20. April 2016 entwickelt hat. Denn sie erlaubt die Überwachung sogenannter Kontaktpersonen unter zu unbestimmten und weit gefassten Voraussetzungen. Zum anderen begründen die Ermächtigungen zu Online-Durchsuchungen (§ 49 BKAG) und zu sogenannten Quellen-Telekommunikationsüberwachungen (§ 51 Abs. 2 BKAG) schwerwiegende, nicht mehr hinnehmbare Risiken für die Informationssicherheit in der Bundesrepublik. Denn sie schließen es nicht aus, dass das BKA zur Durchführung solcher Überwachungen noch unbekannte Sicherheitslücken von Hard- und Software ausnutzt und geheimhält. Diese Sicherheitslücken können ebenso wie durch das BKA durch Dritte ausgenutzt werden, was schwere Schäden bis hin zum Tod von Menschen zur Folge haben kann. Die staatliche Ausnutzung und Geheimhaltung solcher Sicherheitslücken steht darum mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Dimension nicht in Einklang.

Hinsichtlich der angegriffenen Überwachungsermächtigungen beruft sich die Verfassungsbeschwerde auf verfassungsrechtliche Maßstäbe, die das angerufene Gericht bereits entwickelt hat oder die zumindest in seiner Rechtsprechung deutlich angelegt sind. Auf eine Fortentwicklung des Grundrechts auf informationelle Selbstbestimmung zielt die Verfassungsbeschwerde hingegen ab, soweit sie sich gegen die Regulierung des Datenbestands des BKA richtet.

Für die Bevorratung personenbezogener Daten in polizeilichen Datensammlungen und die spätere Nutzung der bevorrateten Daten fehlt es

bislang an konsolidierten verfassungsrechtlichen Maßstäben. Dieser Zustand ist nicht mehr haltbar. Die technischen Möglichkeiten zur Bevorratung und Nutzung großer Mengen personenbezogener Daten sind in den letzten Jahrzehnten in rasender Geschwindigkeit angestiegen und nehmen weiter zu. Polizeiliche Datensammlungen und gerade auch der Datenbestand des BKA erstrecken sich auf weite Kreise der Bevölkerung und begründen für die betroffenen Personen gewichtige Risiken. Die betroffenen Personen werden vielfach schon durch die Bevorratung ihrer Daten stigmatisiert. Komplexe Auswertungen des bevorrateten Datenbestands können tiefgreifende Einblicke in ihre Persönlichkeit und ihre sozialen Vernetzungen ermöglichen. Zudem drohen ihnen aufgrund späterer Nutzungen der bevorrateten Daten polizeiliche Anschlussmaßnahmen – von Befragungen über Reise- und Aufenthaltsbeschränkungen bis hin zum Freiheitsentzug –, denen sie zum Zeitpunkt der Anschlussmaßnahme häufig nicht mehr wirksam begegnen können. Diese Risiken werden durch die angegriffenen Regelungen, die Grundlage einer fundamentalen Umgestaltung und eines qualitativen Ausbaus der Informationsordnung des BKA sind, gegenüber dem früheren Rechtszustand noch erheblich verschärft. Es ist daher dringend erforderlich, dass das angerufene Gericht verfassungsrechtliche Maßstäbe entwickelt, an denen sich die Regulierung polizeilicher Datensammlungen orientieren kann.

Die Verfassungsbeschwerde unterbreitet mit Blick auf die Datensammlungen des BKA, die im Zentrum der polizeilichen Informationsordnung in Deutschland stehen, einen Vorschlag zur Konkretisierung der erforderlichen verfassungsrechtlichen Maßstäbe. Die vorgeschlagenen Maßstäbe haben zum einen die Bevorratung personenbezogener Daten in polizeilichen Datensammlungen, zum anderen die nachgelagerte Datennutzung zum Gegenstand. Ihr Ziel besteht darin, die durch groß angelegte polizeiliche Datensammlungen erzeugten Risiken auf ein zumutbares Maß zu begrenzen, ohne die Führung solcher Datensammlungen vollständig zu verhindern und damit die hinter ihnen stehenden legitimen öffentlichen Ziele zu vereiteln.

Die angegriffenen Regelungen genügen den vorgeschlagenen Maßstäben nicht annähernd. Sie sind in sich teils inkonsistent, in hohem Maße unbestimmt und hinsichtlich der regulierungsbedürftigen Stufen der Datenbevorratung und der späteren Datennutzung viel zu undifferenziert. Insgesamt ermöglichen sie es dem BKA, sensible personenbezogene Daten bereits aufgrund vager Anhaltspunkte, teils sogar aufgrund bloßer Vermutungen in weitem Umfang zu bevorraten und ohne weitere Voraussetzungen zu nutzen. Sie schirmen die aktuellen Risiken polizeilicher Datensammlungen damit nur völlig unzulänglich ab und bedürfen einer grundlegenden Korrektur.

B. Sachverhalt

I. Hintergrund der angegriffenen Regelungen

Die angegriffenen Regelungen waren Teil eines Gesetzes, welches das BKAG vollständig novelliert und inhaltlich teils erheblich verändert hat. Hierfür gab es eine Reihe von Gründen, die zusammen den Hintergrund der angegriffenen Regelungen bilden.

1. Das Urteil zum alten BKAG vom 20. April 2016

Einen Faktor der Novellierung des BKAG bildete das Urteil des angerufenen Gerichts vom 20. April 2016, das zahlreiche Ermächtigungen zu verdeckten Überwachungsmaßnahmen zum Gegenstand hatte, die dem BKA im Jahr 2009 zur Erfüllung seiner damals neuen Aufgabe der präventiven Terrorismusabwehr verliehen worden waren. Das Urteil bestätigte die seinerzeit angegriffenen Regelungen hinsichtlich ihrer Ziele und des regulativen Grundansatzes, stellte jedoch zugleich im Detail eine Vielzahl von materiellen und prozeduralen Defiziten fest,

BVerfGE 141, 220 (263 ff.).

Weiteren Änderungsbedarf erzeugten die in dem Urteil zum alten BKAG herausgearbeiteten verfassungsrechtlichen Maßstäbe für die Zweckbindung von personenbezogenen Daten, die durch eingriffsintensive Überwachungsmaßnahmen erlangt wurden. Diese Maßstäbe bündelten sich in den – die vorherige Rechtsprechung konsolidierenden und teils zurücknehmenden – verfassungsrechtlichen Figuren der weiteren Nutzung und der hypothetischen Datenneuerhebung. Auch diesen Maßstäben genügte das alte BKAG nicht in jeder Hinsicht,

BVerfGE 141, 220 (324 ff.).

Ein erklärtes Ziel der Novellierung des BKAG bestand darin, den durch das angerufene Gericht festgestellten Defiziten abzuhelfen und das Gesetz so an die verfassungsrechtlichen Anforderungen anzupassen,

vgl. BT-Drs. 18/11163, S. 1 und 73.

2. Die alte Informationsordnung des BKA

Da einige der angegriffenen Regelungen im Zentrum der Informationsordnung des BKA stehen, sind sie vor dem Hintergrund der Umgestaltung dieser Informationsordnung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes zu betrachten.

Als polizeiliche Informationsordnung wird im Folgenden die Gesamtheit der rechtlichen Regeln bezeichnet, die sich mit verfahrensexternen Datensammlungen der Polizei befassen. Eine verfahrensexterne Datensammlung enthält personenbezogene Daten, von denen die Polizei annimmt, dass sie zukünftig nützlich sein können, um polizeiliche Aufgaben zu erfüllen. Ein konkretes polizeiliches Verfahren, in dem die Daten genutzt werden sollen, muss hierfür weder schon begonnen haben noch auch nur absehbar sein. Hierin unterscheiden sich verfahrensexterne von verfahrensinternen Datensammlungen, die Informationsgrundlagen für ein bestimmtes polizeiliches Verfahren bereitstellen.

Das BKA führt seit jeher verfahrensexterne Datensammlungen insbesondere in seiner Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei (§ 2 BKAG). Diese Funktion umfasst als zentralen Baustein die informationelle Verklammerung und Versorgung der Landespolizeibehörden. Darüber hinaus unterhält das BKA verfahrensexterne Datensammlungen auch zur Erfüllung seiner sonstigen Aufgaben wie der Strafverfolgung oder der präventiven Terrorismusabwehr.

Der Datenbestand des BKA untergliederte sich nach altem Recht in Dateien. Dabei wurde zwischen Verbund-, Zentral- und Amtsdateien unterschieden, die in dem Informationssystem INPOL zusammengefasst wurden. Verbunddateien waren Dateien, die das BKA als Zentralstelle unter Beteiligung weiterer Polizeibehörden des Bundes und der Länder führte. In die Verbunddateien konnten alle Teilnehmer Daten eingeben. Zentraldateien unterfielen gleichfalls der Zentralstellenfunktion. Im Unterschied zu den Verbunddateien lag die Eingabeberechtigung jedoch allein beim BKA, das die eingegebenen Daten entweder selbst erhoben oder von anderen Polizeibehörden übermittelt bekommen hatte. Amtsdateien führte das BKA zur Erfüllung seiner eigenen Aufgaben außerhalb der Zentralstellenfunktion und in der Regel ohne Zugriffsberechtigung der anderen INPOL-Teilnehmer,

> Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. G 391.

Die Rechtsgrundlagen für die Dateien der Zentralstelle (also Verbund- und Zentraldateien) sowie teils (aufgrund von Verweisungen, etwa aus § 20 BKAG a.F.) auch für die Amtsdateien des BKA waren kaskadenartig gegliedert. Gesetzliche Regelungen fanden sich in §§ 7 ff. BKAG a.F. Zentrale Vorschrift war § 8 BKAG a.F., der regelte, über wen das BKA personenbezogene Daten in seinen Dateien bevorraten durfte. Die zulässigen Inhalte der Dateien sowie zumindest partiell auch die zulässigen Nutzungen

der bevorrateten Daten waren gemäß § 7 Abs. 11 BKAG a.F. in einer Rechtsverordnung zu konkretisieren, die eine konstitutive Voraussetzung für die Rechtmäßigkeit der Datenbevorratung darstellte,

vgl. BVerwG, Urteil vom 9. Juni 2010 – 6 C 5.09 –, juris, Rn. 20.

Die auf der Grundlage dieser Norm erlassene Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen (BKA-Daten-Verordnung – BKADV) zählte detailliert auf, welche Datenkategorien hinsichtlich welcher Personengruppen überhaupt in Dateien des BKA bevorratet werden durften. Außerdem definierte sie Grundtypen von Dateien mit unterschiedlichen abstrakten Zwecken (im Einzelnen: delikts- und phänomenbezogene Dateien, Kriminalaktennachweise, Gewalttäterdateien, erkennungsdienstliche Dateien sowie die DNA-Analyse-Datei) und ordnete ihnen unterschiedliche Datenkategorien zu. Die Verordnung wirkte damit als Baukasten, aus dem das BKA die Spezifikationen einzelner Dateien zusammenstellen konnte. Diese Spezifikationen waren für jede Datei gemäß § 34 BKAG a.F. in einer Errichtungsanordnung festzulegen, also einer Verwaltungsvorschrift. Der konkrete Zweck einer einzelnen Datei ergab sich dementsprechend aus einer Gesamtschau von Gesetz, Verordnung und Errichtungsanordnung.

Nach der Gesetzesbegründung bedurfte die in INPOL gebündelte alte Informationsordnung des BKA sowohl wegen des Urteils des angerufenen Gerichts zum alten BKAG als auch aufgrund praktischer Bedürfnisse einer grundlegenden Umstrukturierung. An die Stelle des in Dateien gegliederten Informationssystems des BKA solle ein einheitliches Verbundsystem mit zentraler Datenhaltung im BKA treten. Das BKA solle als Zentralstelle den Polizeibehörden von Bund und Ländern eine einheitliche Informationstechnik zur Verfügung stellen, deren Struktur deshalb zu modernisieren sei,

BT-Drs. 18/11163, S. 2 und 73 f.

3. Unionsrechtlicher Rahmen für die polizeiliche Informationsordnung

Weiterer Anlass für die Novellierung des BKAG ergab sich aus dem neuen europäischen Rechtsrahmen für das Datenschutzrecht, der neben der in den Mitgliedstaaten unmittelbar geltenden Datenschutz-Grundverordnung (im Folgenden: DSGVO) mit der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (im Folgenden: JI-RL) erstmals allgemeine Regelungen für den

Datenschutz in den Bereichen Strafjustiz und Kriminalitätsbekämpfung umfasst.

Da diese Richtlinie gemäß Art. 1 Abs. 3 JI-RL lediglich ein Mindestniveau für den Datenschutz errichtet, ist nicht unproblematisch, inwieweit sich aus ihr Änderungsbedarfe für das deutsche Polizeirecht einschließlich des BKAG ergaben. Für die Zwecke des vorliegenden Verfahrens kann diese Frage allerdings weitgehend auf sich beruhen. Bedeutsam sind hier vor allem die terminologischen Veränderungen, die der neue europäische Rechtsrahmen nahelegt und die das BKAG aufgriff,

vgl. BT-Drs. 18/11163, S. 75.

Das alte BKAG differenzierte – im Einklang mit § 3 Abs. 3 bis 5 BDSG a.F. – zwischen drei Phasen des Umgangs mit personenbezogenen Daten, die als Datenerhebung, Datenverarbeitung und Datennutzung bezeichnet wurden. Die Verarbeitungsphase war weiter ausdifferenziert und umfasste das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Als gemeinsamer Oberbegriff für die Phasen der Datenverarbeitung und der Datennutzung war der Begriff der Datenverwendung geläufig (vgl. beispielhaft § 10 Abs. 6 Satz 1 BKAG a.F.).

Demgegenüber ging das europäische Datenschutzrecht seit jeher von einem einheitlichen Begriff der Datenverarbeitung aus, der lediglich nach Bedarf in einzelnen Regelungen spezifiziert wurde. Mit der Ablösung des alten BDSG durch die DSGVO ergab sich in der Bundesrepublik ein Bedarf für eine terminologische Anpassung auch des bereichsspezifischen Datenschutzrechts, um eine begriffliche Zersplitterung zu vermeiden. Dementsprechend wurde das BKAG gleichfalls auf den einheitlichen Verarbeitungsbegriff umgestellt. Für das vorliegende Verfahren bedeutsam ist daneben der Begriff der Weiterverarbeitung, der in einigen der angegriffenen Regelungen verwandt wird. Er kennzeichnet bestimmte regulierungsbedürftige Verarbeitungsschritte, die der Datenerhebung nachgelagert sind. Die Gesetzesbegründung führt hierzu aus:

> „Der Gesetzentwurf führt, wie von der [JI-RL] gefordert, den neuen einheitlichen Begriff der Verarbeitung ein.
>
> Aus rechtssystematischen Gründen und aufgrund der weiteren europarechtlichen Vorgaben kann der einheitliche Begriff der Verarbeitung im Bundeskriminalamtgesetz allerdings nicht für die Datenerhebung, die Datenübermittlung, die Einschränkung der Datenverarbeitung und das Löschen der Daten Verwendung finden.

> Die übrigen Aspekte der Verarbeitung wie die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, den Abgleich oder die Verknüpfung (vgl. § 46 Nummer 2 des Bundesdatenschutzgesetzes (BDSG-E)) bezeichnet das Bundeskriminalamtgesetz zusammenfassend als ‚Weiterverarbeitung'."
>
> BT-Drs. 18/11163, S. 87 f.

Der Begriff der Weiterverarbeitung umfasst damit insbesondere die für die polizeiliche Informationsordnung relevanten Verarbeitungsschritte der Bevorratung personenbezogener Daten und der späteren Nutzung der bevorrateten Daten.

II. Gegenstände und Inhalte der angegriffenen Regelungen

Die mit der Verfassungsbeschwerde angegriffenen Regelungen lassen sich in zwei Regelungskomplexe untergliedern.

1. Überwachungsermächtigungen zur Terrorismusbekämpfung

Zum einen richtet sich die Verfassungsbeschwerde gegen einzelne Ermächtigungen des BKA, verdeckte Überwachungsmaßnahmen zum Zweck der präventiven Terrorismusabwehr (§ 5 BKAG) durchzuführen. Insoweit steht die Verfassungsbeschwerde in einer unmittelbaren Kontinuitätslinie zu den Verfassungsbeschwerden, die den Anlass für das Urteil des angerufenen Gerichts zum alten BKAG vom 20. April 2016 gaben.

Die Beschwerdeführerinnen und Beschwerdeführer erkennen an, dass die Ermächtigungen in Abschnitt 5 des BKAG den in diesem Urteil herausgearbeiteten verfassungsrechtlichen Maßstäben weitgehend Rechnung tragen. Gleichwohl finden sich noch immer verfassungsrechtliche Defizite. Die Verfassungsbeschwerde greift zwei davon auf.

Erstens richtet sich die Verfassungsbeschwerde gegen die in § 45 Abs. 1 Satz 1 Nr. 4 geregelte Ermächtigung des BKA, besondere Mittel der Datenerhebung (also längerfristige Observationen, technische Überwachungsmittel und menschliche Quellen) gezielt gegen sogenannte Kontaktpersonen einzusetzen. Insoweit wird eine unzureichende Umsetzung des Urteils zum alten BKAG gerügt.

Zweitens wendet sich die Verfassungsbeschwerde gegen die in § 49 BKAG enthaltene Ermächtigung zu Online-Durchsuchungen und die in § 51 Abs. 2 BKAG enthaltene Ermächtigung zu Quellen-Telekommunikationsüberwachun-

gen insoweit, als es an gesetzlichen Vorgaben für die Frage fehlt, ob und inwieweit IT-Sicherheitslücken für die Durchführung dieser Maßnahmen ausgenutzt werden dürfen. Hierbei geht es um eine objektiv-rechtliche Grundrechtswirkung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, die das angerufene Gericht in seinem Urteil zum alten BKAG nicht zu thematisieren hatte und deren Reichweite grundlegender Klärung bedarf.

2. Informationsordnung des BKA

Zum anderen hat die Verfassungsbeschwerde zentrale Regelungen der Informationsordnung des BKA zum Gegenstand, die durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes umgestaltet wurde. Insoweit wirft die Verfassungsbeschwerde verfassungsrechtliche Fragen auf, die das angerufene Gericht bislang weder in seinem Urteil zum alten BKAG noch in seiner sonstigen Rechtsprechung umfassend geklärt hat.

Das heute geltende Recht gibt die frühere Gliederung des Datenbestands des BKA in Dateien auf. Stattdessen errichtet § 29 BKAG einen polizeilichen Informationsverbund zwischen den Polizeibehörden von Bund und Ländern, dem technisch ein einheitliches Verbundsystem des BKA zugrunde liegt. Innerhalb dieses Verbundsystems stellen die daran teilnehmenden Behörden einander Daten zur Verfügung. Das BKA unterhält zudem für seine eigenen Informationsbestände gemäß § 13 BKAG ein Informationssystem, mit dem es zugleich – soweit vorgesehen – an dem polizeilichen Informationsverbund teilnimmt. Die gesetzlichen Vorgaben für die Datenverarbeitung im Informationssystem und im polizeilichen Informationsverbund sind weitgehend einheitlich in §§ 12 ff. BKAG geregelt, auf die § 29 Abs. 4 Satz 2 BKAG in weitem Umfang verweist.

Mit der Abschaffung der früheren Untergliederung in Dateien fallen die Zweckvorgaben des Dateiregimes weg. Zur Wahrung der verfassungs- und auch unionsrechtlich durch Art. 4 Abs. 1 lit. b JI-RL geforderten Zweckbindung orientiert sich das Gesetz stattdessen an den in dem Urteil zum alten BKAG entwickelten verfassungsrechtlichen Rechtsfiguren der weiteren Nutzung und der hypothetischen Datenneuerhebung, die nunmehr in § 12 BKAG positiviert sind. Diese Norm enthält selbst noch keine Ermächtigung zu Datenweiterverarbeitungen im Informationssystem und im polizeilichen Informationsverbund. Diese Ermächtigungen finden sich vielmehr in §§ 16 ff. BKAG. Sie werden flankiert durch Regelungen über die Kennzeichnung der weiterverarbeiteten Daten in § 14 BKAG und über die Zuweisung von Zugriffsrechten an die einzelnen Bearbeiter in § 15 BKAG. Für den

polizeilichen Informationsverbund zwischen Bund und Ländern treten hinzu Regelungen über die Verbundrelevanz personenbezogener Daten als weitere Verarbeitungsvoraussetzung in § 30 BKAG und über die Verteilung der datenschutzrechtlichen Verantwortlichkeit zwischen den teilnehmenden Behörden in § 31 BKAG. Schließlich enthält § 20 BKAG eine Ermächtigung des Bundesministeriums des Innern, durch Rechtsverordnung Näheres über Art und Umfang der im Informationssystem und im polizeilichen Informationsverbund weiterverarbeiteten Daten zu bestimmen. Diese Rechtsverordnung wurde bisher nicht erlassen. Ob einstweilen auf die alte BKADV zurückzugreifen ist, ist unklar und fragwürdig, da sich diese Verordnung an der alten Dateistruktur orientiert. In jedem Fall ergeben sich die tatbestandlichen Voraussetzungen von Datenbevorratung und Datennutzung abschließend aus §§ 16 ff. BKAG, die hinsichtlich dieser Fragen keinen Raum für eine Konkretisierung im Verordnungsrecht lassen.

Gegenstand der Verfassungsbeschwerde sind einige zentrale Ermächtigungen zu Datenweiterverarbeitungen im Informationssystem des BKA und im polizeilichen Informationsverbund von Bund und Ländern. Dabei beschränkt sich die Verfassungsbeschwerde teilweise auf bestimmte Anwendungsfälle der angegriffenen Regelungen.

Die Verfassungsbeschwerde richtet sich zunächst gegen die allgemeine Ermächtigung zu Datenweiterverarbeitungen § 16 Abs. 1 BKAG. Diese Vorschrift erlaubt dem BKA, nach Maßgabe von § 12 BKAG personenbezogene Daten im Informationssystem weiterzuverarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Gegenstand der Verfassungsbeschwerde ist diese Ermächtigung insoweit, als sie

- in Verbindung mit § 12 Abs. 1 Satz 1 BKAG dem BKA die weitgehend anlasslose Bevorratung von Daten erlaubt, die es im Rahmen seiner Aufgabe zur präventiven Terrorismusabwehr (§ 5 BKAG) mit eingriffsintensiven Überwachungsmaßnahmen wie den in § 45 Abs. 2 BKAG aufgezählten besonderen Mitteln der Datenerhebung erhoben hat und

- in Verbindung mit § 12 Abs. 1 Satz 1 BKAG dem BKA die spätere Nutzung der bevorrateten Daten zum Zweck der Terrorismusabwehr wiederum weitgehend anlasslos erlaubt.

Daneben richtet sich die Verfassungsbeschwerde gegen die Weiterverarbeitungsermächtigungen in § 18 Abs. 1, Abs. 2 und Abs. 5 BKAG, auch in Verbindung mit § 29 Abs. 4 Satz 2 BKAG. Diese Regelungen erlauben

dem BKA und den anderen am polizeilichen Informationsverbund teilnehmenden Behörden, im Rahmen der Zentralstellenaufgabe des BKA (§ 2 Abs. 1 bis 3 BKAG) personenbezogene Daten im Informationssystem bzw. im polizeilichen Informationsverbund zu bevorraten und die bevorrateten Daten später zu nutzen. Voraussetzung ist eine jeweils gesetzlich näher beschriebene Affinität der betroffenen Person zu Straftaten, die für die Zentralstellenaufgabe relevant sind.

Schließlich richtet sich die Verfassungsbeschwerde gegen die Ermächtigung in § 16 Abs. 6 Nr. 2 BKAG (auch in Verbindung mit § 29 Abs. 4 Satz 2 BKAG), im Informationssystem oder im polizeilichen Informationsverbund zu vorhandenen personenbezogenen Daten ohne weiteren Anlass zusätzliche Daten (sogenannte ermittlungsunterstützende Hinweise) hinzuzuspeichern und später zu nutzen.

III. Die Beschwerdeführerinnen und Beschwerdeführer

Die Beschwerdeführerin zu 1 ist Rechtsanwältin und Fachanwältin für Strafrecht. Sie hat seit 2006 immer wieder Angeklagte in Staatsschutzverfahren mit internationalem Bezug verteidigt, darunter zahlreiche Personen, denen Straftaten des islamistischen Terrorismus vorgeworfen wurden. Beispielsweise war sie ab 2009 Verteidigerin eines Angehörigen der sogenannten Sauerland-Gruppe, vertrat gleichfalls ab 2009 den Angeklagten in dem ersten deutschen Verfahren nach dem Völkerstrafgesetzbuch und verteidigte ab 2016 einen Mandanten, der in Syrien für den „Islamischen Staat“ Sprengfallen gebaut und zugleich deutschen Sicherheitsbehörden als Quelle gedient hatte,

> vgl. aus der umfangreichen Medienberichterstattung zu diesen exemplarischen Verfahren etwa https://www.merkur.de/lokales/muenchen/stadt-muenchen/frau-terroristen-sprechen-bringt-442055.html; http://www.taz.de/Nach-neun-Jahren-Haft-in-Deutschland/!5589026; https://www.spiegel.de/politik/deutschland/islamischer-staat-anwaelte-von-berliner-scheinterrorist-fechten-urteil-an-a-1145332.html (letzte Abrufe am 21. Mai 2019).

Da die meisten Staatsschutzverfahren, in denen die Beschwerdeführerin zu 1 mandatiert ist, einen weitreichenden Auslandsbezug aufweisen, ermittelt sie auch im Ausland, um Zeuginnen und Zeugen zu finden und zu befragen. Sie unterhält in der Folge Kontakte zu zahlreichen mutmaßlichen Angehörigen terroristischer Vereinigungen im In- und Ausland.

Die Beschwerdeführerin zu 2 ist Rechtsanwältin und Fachanwältin für Strafrecht. Ihre Tätigkeitsschwerpunkte liegen im Strafrecht und im Aufenthaltsrecht. Die Beschwerdeführerin ist wiederholt für Mandantinnen und Mandanten tätig geworden, denen die Mitgliedschaft in oder die Unterstützung einer terroristischen Vereinigung im Ausland vorgeworfen wurde, unter anderem der in Deutschland verbotenen Arbeiterpartei Kurdistans (Partiya Karkerên Kurdistanê – PKK). Gegenwärtig verteidigt sie zwei Personen in separaten Verfahren gegen solche Vorwürfe. Im Vorgang zu beiden Verfahren hat das BKA im Rahmen seiner Strafverfolgungsaufgabe (§ 4 BKAG) ermittelt. Frühere Mandate umfassten etwa ein strafrechtliches Verfahren wegen eines Verstoßes gegen das vereinsrechtliche Verbot der PKK sowie die Androhung einer aufenthaltsrechtlichen Ausweisung wegen einer Nähe zu der PKK.

Die Beschwerdeführerin zu 3 ist Mitglied des Ehrenrats des Sportvereins TSV 1860 München e.V., dessen Erste Herren-Fußballmannschaft derzeit in der bundesweiten 3. Liga spielt. Sie ist zudem Vorstandsmitglied des Football Supporters Europe e.V., eines europaweit tätigen Netzwerks von Fußballfans. Darüber hinaus engagiert sie sich seit mehreren Jahren ehrenamtlich in verschiedenen Faninitiativen wie den „Löwenfans gegen Rechts“, den „Freunden des Sechz‘ger-Stadions“ oder den „Fußballfans gegen Homophobie“. Die Beschwerdeführerin zu 3 ist seit 29 Jahren Fan des TSV 1860 München und besucht sowohl Heimspiele als auch Auswärtsspiele des Vereins. Durch ihre langjährigen Stadionbesuche, ihre Aktivität in verschiedenen Fangruppierungen und in der Vereinspolitik sowie ihre Tätigkeit im sozialpädagogischen Fanprojekt (2012-2013) sind viele persönliche Kontakte zu anderen Fans entstanden.

Gegen die Beschwerdeführerin zu 3 wurden in den Jahren 2007 und 2013 zwei strafrechtliche Ermittlungsverfahren im Zusammenhang mit Fußballspielen eingeleitet, die beide ohne Anklageerhebung eingestellt wurden. Laut einer Auskunft des Kriminalfachdezernats 10 der Münchner Polizei vom 11. Mai 2017 **(Anlage 2)** waren zu diesem Zeitpunkt in der „Informationsdatei Fußball“ der bayerischen Polizei über die Beschwerdeführerin zu 3 Angaben über ihre Vereins- und Fangruppenzugehörigkeit, Lichtbilder sowie „aufgrund einer Zurechnung zu gewalttätigen Gruppierungen oder deren engerem Umfeld“ 38 besuchte Sportveranstaltungen gespeichert. Die Beschwerdeführerin zu 3 legt Wert auf die Feststellung, dass sie Gewalt gegen andere Menschen kategorisch ablehnt, sofern sie nicht der verhältnismäßigen Verteidigung der eigenen

Person dient. Hierfür setzt sie sich im Rahmen ihrer Möglichkeiten auch ein und hat immer wieder den Dialog mit gewaltbereiten Fußballfans gesucht.

Der Beschwerdeführer zu 4 ist wissenschaftlicher Mitarbeiter und Doktorand an der Ludwig-Maximilians-Universität München. Er ist Mitglied verschiedener Organisationen aus dem linken politischen Spektrum. Der Beschwerdeführer besucht seit mehreren Jahren regelmäßig ein jährlich stattfindendes linkes Jugendfestival in Palästina. In diesem Zusammenhang sammelt er auch Spenden. So sind im Jahr 2018 etwa 5.000 Euro Spendengelder zusammengekommen,

> vgl. beispielhaft den Reisebericht des Beschwerdeführers auf seiner persönlichen Homepage, https://keremschamberger.de/2018/07/22/25-jahre-farkha-festival-25-jahre-widerstand-tag-1-2 (letzter Abruf am 21. Mai 2019).

Laut einem Schreiben des Bundespolizeipräsidiums vom 30. Januar 2019 **(Anlage 3)** sind personenbezogene Daten des Beschwerdeführers zu 4 sowohl im Vorgangsbearbeitungssystem der Bundespolizei als auch in INPOL gespeichert. Diesem Schreiben lässt sich entnehmen, dass die Spendensammlung durch den Beschwerdeführer im Jahr 2018 zu einer INPOL-Ausschreibung durch die Bundespolizei geführt hat. Diese Ausschreibung hat wiederum insbesondere zur Folge, dass der Beschwerdeführer immer dann, wenn er mit dem Flugzeug aus der Bundesrepublik ausreist oder in die Bundesrepublik einreist und dabei eine Grenzkontrolle durchläuft, angehalten und polizeilich befragt wird. Bei einer dieser Befragungen teilte der Polizeibeamte dem Beschwerdeführer ergänzend zu dem Auskunftsschreiben der Bundespolizei mündlich mit, er werde in INPOL als politisch motivierter potenzieller Gewalttäter (PMK-links) geführt.

Lediglich zur Abrundung sei zudem mitgeteilt, dass der Beschwerdeführer zu 4 auch in mindestens einer nachrichtendienstlichen Datensammlung des Bayerischen Landesamts für Verfassungsschutz geführt wird. Die Einstellung des Beschwerdeführers an der Ludwig-Maximilians-Universität verzögerte sich Ende 2016 aufgrund einer „Erkenntnismitteilung“ des Landesamts an die Universitätsverwaltung **(Anlage 4)**. In dieser Mitteilung waren zahlreiche Informationen über den Beschwerdeführer enthalten. Im Ergebnis brachte das Landesamt Bedenken gegen eine Einstellung vor. Über diesen Vorgang wurde seinerzeit auch in der überregionalen Presse berichtet,

vgl. etwa http://www.sueddeutsche.de/muenchen/trotz-einschaetzung-des-verfassungsschutzes-kommunist-darf-an-muenchner-universitaet-arbeiten-1.3308728; http://www.faz.net/aktuell/beruf-chance/recht-und-gehalt/politik-am-arbeitsplatz-wenn-dem-chef-das-parteibuch-nicht-passt-15061356.html (letzte Abrufe am 21. Mai 2019).

Der Beschwerdeführer zu 5 ist Fan des Fußballvereins SV Werder Bremen. Er gehört der sogenannten Ultra-Fanszene an und steht in dieser Eigenschaft mindestens seit 2007 unter ständiger polizeilicher Beobachtung. Personenbezogene Daten über ihn wurden mehrfach in landespolizeilichen Datensammlungen sowie im Verbundsystem des BKA bevorratet und im Rahmen imperativer polizeilicher Maßnahmen gegen ihn genutzt.

In einem Fall hat diese Nutzung zu einem verwaltungsgerichtlichen Urteil geführt, das einer Klage des Beschwerdeführers zu 5 stattgab: Der Beschwerdeführer war seit Januar 2010 in der Verbunddatei „Gewalttäter Sport“ mit dem Vermerk „Tatverdacht zur Sachbeschädigung/Graffiti in Göttingen im Rahmen der Busanreise zum Spiel Eintracht Frankfurt gegen SV Werder Bremen“ ausgeschrieben. Am 20. Oktober 2010 untersagte die Bundespolizei dem Beschwerdeführer, der sich zusammen mit anderen Fans in einem Reisebus auf dem Weg zu einem Champions-League-Spiel des SV Werder Bremen in Enschede (Niederlande) befand, die Ausreise. Zur Begründung verwies die Bundespolizei auf den oben erwähnten und einen weiteren, älteren Eintrag in der Datei „Gewalttäter Sport“ sowie auf den Umstand, dass sich in dem Reisebus noch drei weitere Personen befänden, zu denen Erkenntnisse als „Gewalttäter Sport“ vorlägen. Das Verwaltungsgericht Köln stellte mit Urteil vom 26. April 2012 die Rechtswidrigkeit der Ausreiseuntersagung fest **(Anlage 5)**.

Der Beschwerdeführer besucht weiterhin sowohl die Heim- als auch Auswärtsspiele seines Vereins und hält sich dabei in der Regel in der Nähe von anderen Mitgliedern der Bremer Ultraszene auf.

C. Zulässigkeit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist insgesamt zulässig. Die Beschwerdeführerinnen und Beschwerdeführer wenden sich in zwei Gruppen gegen überwiegend jeweils unterschiedliche Regelungen. Insoweit sind die Zulässigkeitsvoraussetzungen jeweils gewahrt.

I. Verfassungsrechtliche Rügen

Die Beschwerdeführerinnen zu 1 und 2 wenden sich zum einen gegen die Überwachungsermächtigungen aus § 45 Abs. 1 Satz 1 Nr. 4, § 49 und § 51 Abs. 2 BKAG. Insoweit rügen sie hinsichtlich von § 45 Abs. 1 Satz 1 Nr. 4 BKAG eine Verletzung des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), hinsichtlich von § 49 und § 51 Abs. 2 BKAG eine Verletzung des objektiv-rechtlich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme folgenden Gebots an die staatliche Gewalt der Bundesrepublik, übermäßige Risiken für informationstechnische Systeme und die informationstechnische Infrastruktur in Deutschland zu vermeiden.

Zum anderen wenden sich die Beschwerdeführerinnen zu 1 und 2 gegen § 16 Abs. 1 i.V.m. § 12 Abs. 1 BKAG, soweit diese Regelungen dem BKA erlauben, im Informationssystem personenbezogene Daten zu bevorraten und später zu nutzen, die es durch Überwachungsmaßnahmen nach den angegriffenen Überwachungsermächtigungen erlangt hat. Insoweit rügen die Beschwerdeführerinnen wiederum eine Verletzung des Grundrechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Beschwerdeführerin zu 3 und die Beschwerdeführer zu 4 und 5 wenden sich gegen die Ermächtigungen des BKA und der anderen am polizeilichen Informationsverbund teilnehmenden Polizeibehörden in § 18 Abs. 1, Abs. 2 und Abs. 5 BKAG, sie betreffende personenbezogene Daten im Informationssystem sowie (in Verbindung mit § 29 Abs. 4 Satz 2 BKAG) im polizeilichen Informationsverbund zu bevorraten und später zu nutzen. Die Beschwerdeführerin und die Beschwerdeführer rügen eine Verletzung des Grundrechts auf informationelle Selbstbestimmung.

Schließlich wenden sich alle Beschwerdeführerinnen und Beschwerdeführer gegen die in § 16 Abs. 6 Nr. 2 BKAG enthaltene Ermächtigung zur Hinzuspeicherung ermittlungsunterstützender Hinweise im Informationssystem sowie (in Verbindung mit § 29 Abs. 4 Satz 2 BKAG) im

polizeilichen Informationsverbund. Insoweit rügen sie wiederum eine Verletzung des Grundrechts auf informationelle Selbstbestimmung.

II. Anwendbarkeit der Grundrechte des Grundgesetzes

Die angegriffenen Regelungen sind vollumfänglich an den Grundrechten des Grundgesetzes zu messen, deren Wahrung das angerufene Gericht überprüft. Insbesondere steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen, dass die angegriffenen Regelungen auch der Umsetzung von Vorgaben der JI-RL dienen.

Nach der Rechtsprechung des angerufenen Gerichts sind Verfassungsbeschwerden gegen Regelungen des deutschen Rechts, die eine EU-Richtlinie umsetzen, nur insoweit grundsätzlich unzulässig, als die Richtlinie abschließende Vorgaben macht. Soweit eine Richtlinie hingegen den Mitgliedstaaten bei der Umsetzung Regelungsspielräume belässt, ist die deutsche hoheitliche Gewalt bei der Ausfüllung dieser Spielräume vollumfänglich an die Grundrechte des Grundgesetzes gebunden,

> vgl. BVerfGE 118, 79 (95 ff.); 122, 1 (20 f.); 125, 260 (308 f.); 129, 78 (90 f.); 140, 317 (335 f.).

So liegt es hier. Wie sich aus Art. 1 Abs. 3 JI-RL ergibt, errichtet diese Richtlinie für den Datenschutz im Polizeibereich lediglich Mindeststandards, über welche die Mitgliedstaaten hinausgehen dürfen. Der damit verbleibende Regelungsspielraum für eine Verschärfung der rechtlichen Anforderungen an polizeiliche Datenverarbeitungen ist im Einklang mit dem Grundgesetz auszufüllen.

III. Zulässigkeitsvoraussetzungen hinsichtlich der Beschwerdeführerinnen zu 1 und 2

1. Eigene, gegenwärtige und unmittelbare Beschwer

Die Beschwerdeführerinnen zu 1 und 2 sind als potenzielle Betroffene von Überwachungsmaßnahmen des BKA mit dem Ziel der Terrorismusabwehr sowie von nachfolgenden Datenweiterverarbeitungen beschwerdebefugt. Insbesondere sind sie durch die von ihnen angegriffenen Regelungen selbst, gegenwärtig und unmittelbar betroffen.

Zur Darlegung einer eigenen und gegenwärtigen Beschwer durch Ermächtigungen zu verdeckten Überwachungsmaßnahmen ist erforderlich, aber auch ausreichend, dass die Beschwerdeführerinnen darlegen, mit einiger

Wahrscheinlichkeit zukünftig von Maßnahmen auf der Grundlage der angegriffenen Ermächtigungen betroffen zu werden,

vgl. BVerfGE 141, 220 (262); stRspr.

Aufgrund ihrer beruflichen Tätigkeit als Rechtsanwältinnen und ihrer besonderen Spezialisierungen besteht für die Beschwerdeführerinnen zu 1 und 2 eine im Vergleich zum Bevölkerungsdurchschnitt weit erhöhte Wahrscheinlichkeit, von Überwachungsmaßnahmen des BKA zur Terrorismusabwehr erfasst zu werden.

Beide Beschwerdeführerinnen haben einen Tätigkeitsschwerpunkt im Strafrecht und haben in diesem Rahmen bereits wiederholt Personen verteidigt, denen Straftaten des internationalen Terrorismus vorgeworfen wurden. Die Beschwerdeführerin zu 2 hat im Rahmen ihres weiteren Tätigkeitsschwerpunkts im Aufenthaltsrecht gleichfalls bereits Mandanten vertreten, bei denen zumindest eine Nähebeziehung zum terroristischen Milieu vermutet wurde. Es ist davon auszugehen, dass die Beschwerdeführerinnen auch in Zukunft vergleichbare Mandate annehmen werden.

Aufgrund dieser beruflichen Spezialisierung unterhalten die Beschwerdeführerinnen zu 1 und 2 Kontakte zu zahlreichen Personen – etwa ihren Mandantinnen und Mandanten, deren Angehörigen oder potenziellen Zeuginnen und Zeugen –, die als Zielpersonen von Überwachungsmaßnahmen nach den angegriffenen Regelungen oder als deren Kontaktpersonen in Betracht kommen. Überwachungsmaßnahmen nach den angegriffenen Regelungen, die sich unmittelbar gegen diese Personen richten, werden in vielen Fällen die Beschwerdeführerinnen als Drittbetroffene miterfassen. Darüber hinaus könnten die Beschwerdeführerinnen aufgrund ihrer beruflichen Beziehungen zu Personen aus dem – mutmaßlich – terroristischen Milieu sogar selbst als Kontaktpersonen eingestuft und darum gezielt überwacht werden.

Der eigenen und gegenwärtigen Beschwer der Beschwerdeführerinnen zu 1 und 2 steht nicht entgegen, dass ihre berufliche Kommunikation gemäß § 62 Abs. 1 BKAG besonderen Schutz genießt. Denn dieser Schutz ist rechtlich und tatsächlich nicht lückenlos gewährleistet.

Zum einen ist der durch diese Norm gewährleistete Schutz des Berufsgeheimnisses durch die Verstrickungsregelung des § 62 Abs. 4 BKAG begrenzt. Obgleich sich die Beschwerdeführerinnen im Rahmen ihrer beruflichen Tätigkeit durchweg rechtstreu verhalten, ist nicht auszuschließen, dass das BKA – etwa aufgrund eines Irrtums oder einer ambivalenten

Indizienlage – eine mutmaßliche Verstrickung der Beschwerdeführerinnen annimmt und sich daher zu einer Überwachung ihrer Kommunikation entschließt.

Zum anderen greift der besondere Schutz aus § 62 Abs. 1 BKAG faktisch nur, wenn das BKA überhaupt erkennt, dass eine Überwachung sich auf das Berufsgeheimnis der Beschwerdeführerinnen erstreckt. Insbesondere bei einer Erfassung der Beschwerdeführerinnen als Drittbetroffene (§ 62 Abs. 1 Satz 6 BKAG) liegt nahe, dass dies nicht immer zuverlässig gewährleistet ist. Insbesondere kommunizieren die Beschwerdeführerinnen im Rahmen ihrer beruflichen Tätigkeit nicht nur mit ihren Mandantinnen und Mandanten, sondern auch mit Dritten – etwa Angehörigen oder potenziellen Zeuginnen und Zeugen –, die gleichfalls mitunter dem terroristischen Milieu zugeordnet oder als Kontaktpersonen überwacht werden könnten. Solche Kommunikationen sind zwar zumindest in aller Regel von ihrem Zeugnisverweigerungsrecht erfasst. Gerade bei der Kommunikation mit Dritten wird dies aber für das BKA nicht immer erkennbar sein.

Die eigene und gegenwärtige Beschwer der Beschwerdeführerinnen zu 1 und 2 erstreckt sich auf die angegriffene Ermächtigung zur Weiterverarbeitung von Daten, die auf der Grundlage der angegriffenen Überwachungsermächtigungen erhoben werden. Im Vergleich zum Bevölkerungsdurchschnitt ist wiederum die Wahrscheinlichkeit deutlich erhöht, dass das BKA personenbezogene Daten der Beschwerdeführerinnen, die es durch Überwachungsmaßnahmen nach den angegriffenen Überwachungsermächtigungen erlangt hat, in seinem Informationssystem bevorratet und sie später nutzt.

Die Beschwerdeführerinnen zu 1 und 2 sind durch die angegriffenen Regelungen auch unmittelbar beschwert. Zwar bedürfen diese sämtlich der Umsetzung durch Vollzugsakte des BKA. Eine unmittelbare Betroffenheit durch gesetzliche Eingriffsermächtigungen ist jedoch auch dann anzunehmen, wenn potenziell Betroffene gegen solche Umsetzungsakte nicht gerichtlich vorgehen können, weil sie keine Kenntnis von der Maßnahme erlangen oder eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann,

> BVerfGE 141, 220 (261); BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 2795/09, 1 BvR 3187/10 –, Rn. 35.

Danach ist eine unmittelbare Beschwer der Beschwerdeführerinnen zu 1 und 2 durch die von ihnen angegriffenen Regelungen zu bejahen. Die durch die angegriffenen Überwachungsermächtigungen ermöglichten Maßnahmen werden grundsätzlich heimlich durchgeführt. Die in § 74 BKAG vorgesehenen Benachrichtigungspflichten fangen dies nur teilweise auf. Je nach den Umständen des einzelnen Verfahrens greifen sie potenziell erst spät. Unter bestimmten Voraussetzungen kann von einer Benachrichtigung sogar ganz abgesehen werden. Eine Benachrichtigung von Drittbetroffenen ist zudem bei Überwachungsmaßnahmen nach § 45 BKAG gemäß § 74 Abs. 1 Nr. 1 und 2 BKAG nicht immer vorgesehen. Keine gesonderte Benachrichtigung erfolgt zudem bei einer Weiterverarbeitung der erhobenen personenbezogenen Daten im Informationssystem des BKA. Die Beschwerdeführerinnen können daher insgesamt nicht darauf verwiesen werden, Vollzugsakte des BKA abzuwarten und gegen diese vorzugehen.

2. Rüge der Verletzung objektiv-rechtlicher Grundrechtsgehalte

Die Verfassungsbeschwerde ist hinsichtlich der Beschwerdeführerinnen zu 1 und 2 auch insoweit zulässig, als sie hinsichtlich der Ermächtigungen zu Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen in § 49 und § 51 Abs. 2 BKAG (allein) eine Verletzung objektiv-rechtlicher Vorgaben rügen, die sich aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergeben.

Aus den Darlegungen zur eigenen und gegenwärtigen Beschwer der Beschwerdeführerinnen zu 1 und 2 ergibt sich, dass sie mit gesteigerter Wahrscheinlichkeit als Drittbetroffene Grundrechtseingriffen aufgrund von § 49 und § 51 Abs. 2 BKAG ausgesetzt sein können. Diese Grundrechtseingriffe sind nur gerechtfertigt, wenn die Eingriffsermächtigung in jeder Hinsicht mit dem Grundgesetz übereinstimmt,

> stRspr seit BVerfGE 6, 32 (41).

Dies schließt die Wahrung objektiv-rechtlicher Grundrechtsgehalte ein. Das angerufene Gericht hat dementsprechend in seiner jüngeren Rechtsprechung zum Sicherheitsrecht im Rahmen von Verfassungsbeschwerdeverfahren Eingriffsermächtigungen wiederholt an verfassungsrechtlichen Maßstäben gemessen, die zumindest nicht ausschließlich dem Schutz einzelner Eingriffsadressaten, sondern (auch) überindividuellen Zielen dienten,

> vgl. etwa BVerfGE 125, 260 (325 ff.) – Datensicherheit; BVerfGE 133, 277 (369 ff.) – rechtsstaatliche Kontrolle durch

> Datenschutzaufsichtsbehörden; BVerfGE 141, 220 (285) – demokratische Kontrolle durch Parlament und Öffentlichkeit.

Es ist folgerichtig, dass die Beschwerdeführerinnen zu 1 und 2 als absehbare Betroffene von Eingriffen auf der Grundlage der angegriffenen Ermächtigung auch ausschließlich die Verletzung objektiv-rechtlicher Grundrechtsgehalte rügen können.

Darüber hinaus haben die Beschwerdeführerinnen zu 1 und 2 ein im Vergleich zum Bevölkerungsdurchschnitt erheblich gesteigertes Interesse an der Sicherheit informationstechnischer Systeme in der Bundesrepublik, die Gegenstand ihrer objektiv-rechtlichen Rüge ist. Als Berufsgeheimnisträgerinnen sind sie auf eine sichere informationstechnische Infrastruktur zur vertraulichen Kommunikation mit ihren Mandantinnen und Mandanten in besonderem Maße angewiesen. Darüber hinaus sind auf den von ihnen beruflich genutzten informationstechnischen Systemen höchst sensible Daten in großem Umfang gespeichert. Infolge der angegriffenen Regelungen droht eine Kompromittierung der Informationssicherheit in Deutschland dadurch, dass Sicherheitslücken von Hard- und Software nicht oder nicht unverzüglich nach Bekanntwerden geschlossen werden. Dies würde gerade die Beschwerdeführerinnen besonders stark belasten.

3. Subsidiarität der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist auch nicht wegen des Subsidiaritätsgrundsatzes unzulässig. Zwar hat das angerufene Gericht jüngst in seinem Beschluss zur automatisierten Kfz-Kennzeichenkontrolle in Baden-Württemberg und Hessen anscheinend auch für sicherheitsrechtliche Überwachungsermächtigungen grundsätzlich verlangt, dass vor Einlegung einer Verfassungsbeschwerde ein fachgerichtliches Rechtsschutzverfahren durchlaufen wird,

> BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 2795/09, 1 BvR 3187/10 –, Rn. 40 ff.

Ein fachgerichtlicher Rechtsschutz ist den Beschwerdeführerinnen zu 1 und 2 jedoch teils nicht zumutbar, teils ist er schon nicht eröffnet.

Die Beschwerdeführerinnen zu 1 und 2 können nicht darauf verwiesen werden, gegen Überwachungsmaßnahmen oder Datenweiterverarbeitungen des BKA nachträglich vor den Verwaltungsgerichten vorzugehen, da ihnen dieser Weg nicht zumutbar ist. Dies wurde oben unter dem Gesichtspunkt der unmittelbaren Betroffenheit begründet.

Ein vorbeugender Rechtsschutz in Gestalt einer vorbeugenden Unterlassungs- oder Feststellungsklage ist den Beschwerdeführerinnen zu 1 und 2 nicht eröffnet. Solche Klagen setzen nach gefestigter Rechtsprechung voraus, dass sich ein drohendes Verwaltungshandeln bzw. ein zukünftiges Rechtsverhältnis bereits hinreichend konkret abzeichnet und die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist,

> vgl. zur vorbeugenden Unterlassungsklage BVerwGE 45, 99 (105); BVerwG BeckRS 1981, 31248115; BVerwG, Urteil vom 13. Dezember 2017 – 6 A 6.16 –, juris, Rn. 12; Pietzcker, in: Schoch/Schneider/Bier, VwGO, § 42 Abs. 1 Rn. 163; zur Feststellungsklage BVerwGE 59, 310 (318); BVerwG NVwZ 1988, 430 (431); BVerwG NVwZ 2017, 791; BVerwG NVwZ 2018, 1476 (1482); Pietzcker, in: Schoch/Schneider/Bier, VwGO, § 43 Rn. 21.

Eine nähere Bestimmung drohender Überwachungsmaßnahmen und anschließender Datenweiterarbeitungen ist den Beschwerdeführerinnen jedoch nicht möglich. Hierzu müssten die Beschwerdeführerinnen ein konkretes behördliches Verfahren bezeichnen können, in dessen Rahmen ihnen eine Überwachung – sei es als Kontaktpersonen oder als Drittbetroffenen – droht. Aus ihrer Betroffenenperspektive lassen sich solche Verfahren im Voraus aber nicht absehen. Das BKA geht zur Terrorismusabwehr in aller Regel zunächst über einen längeren Zeitraum heimlich vor. Für die Betroffenen zeichnet sich dieses Vorgehen naturgemäß nicht ab. Kenntnis von einem laufenden Verfahren der Terrorismusabwehr können die Betroffenen frühestens erlangen, wenn das BKA offene Gefahrenabwehrmaßnahmen durchführt oder das Verfahren in ein offenes strafrechtliches Ermittlungsverfahren überleitet. Dies wird allerdings zum einen keineswegs in jedem Fall geschehen. Zum anderen werden zu diesem Zeitpunkt die verdeckten Überwachungsmaßnahmen bereits abgeschlossen sein, so dass ein vorbeugender Rechtsschutz zu spät käme.

Als Alternative bliebe den Beschwerdeführerinnen lediglich eine vorbeugende Klage gegen unbestimmte Überwachungsmaßnahmen in unbestimmten Verfahren. Eine solche Klage „ins Blaue hinein“ sprengte jedoch den in langjähriger Rechtsprechung entwickelten Rahmen des vorbeugenden Rechtsschutzes und wäre aller Voraussicht nach unzulässig. Selbst wenn dies anders zu sehen wäre, wäre ein solcher Rechtsschutz so inadäquat, dass der Subsidiaritätsgrundsatz nicht dazu zwänge, ihn vorrangig zu ergreifen. Soweit nämlich die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne

dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten sind, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht,

> BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 2795/09, 1 BvR 3187/10 –, Rn. 44.

So läge der Fall bei einer vorbeugenden Unterlassungs- oder Feststellungsklage gegen verdeckte Überwachungsmaßnahmen des BKA nach den angegriffenen Regelungen. Da die Beschwerdeführerinnen zu 1 und 2 konkrete Überwachungsanlässe im Voraus nicht absehen und nicht benennen können, müsste eine solche Klage darauf gerichtet sein, eine Überwachung der Beschwerdeführerinnen nach den angegriffenen Regelungen *generell* zu unterlassen. Diese Klage wäre nur begründet, wenn es *keinen* denkbaren Sachverhalt gäbe, in dessen Rahmen die Beschwerdeführerinnen einer solchen Überwachung ausgesetzt werden dürfen. Dies ließe sich nur annehmen, wenn die angegriffenen Regelungen auch bei restriktiver Interpretation und unabhängig von ihrer tatsächlichen Handhabung verfassungswidrig wären. Ausführungen zur Auslegung und Anwendung der Normen könnten die Fachgerichte daher allenfalls als obiter dicta machen, zu denen sie nicht gehalten sind und deren bloße Möglichkeit unter Subsidiaritätsgesichtspunkten keinen fachgerichtlichen Rechtsschutz gebieten kann. Vielmehr wäre eine Aufklärung der einfachrechtlichen Rechtslage und der tatsächlichen Gegebenheiten im Verwaltungsprozess nicht angezeigt. Das verwaltungsgerichtliche Verfahren wäre vielmehr materiell als reiner Verfassungsprozess zu führen, was der Subsidiaritätsgrundsatz gerade nicht verlangt.

IV. Zulässigkeitsvoraussetzungen hinsichtlich der Beschwerdeführerin zu 3 und der Beschwerdeführer zu 4 und 5

Die Beschwerdeführerin zu 3 und die Beschwerdeführer zu 4 und 5 sind durch die von ihnen angegriffenen Regelungen über Datenweiterverarbeitungen im Informationssystem des BKA und im polizeilichen Informationsverbund gleichfalls selbst, gegenwärtig und unmittelbar betroffen.

Zur Begründung der eigenen und gegenwärtigen Beschwer reicht es auch hinsichtlich der Beschwerdeführerin zu 3 und der Beschwerdeführer zu 4 und 5 aus, dass sie darlegen, mit einiger Wahrscheinlichkeit in der Zukunft durch die in den angegriffenen Regelungen vorgesehenen Datenbevorratungen und späteren Datennutzungen in ihren Grundrechten berührt zu werden,

> vgl. zur Antiterrordatei BVerfGE 133, 277 (312).

Nach diesem Maßstab ergibt sich eine eigene und gegenwärtige Betroffenheit der Beschwerdeführerin zu 3 und der Beschwerdeführer zu 4 und 5 daraus, dass sie aufgrund ihrer Zugehörigkeit zur aktiven Fußballfanszene beziehungsweise zum linken politischen Spektrum und aufgrund ihrer dadurch motivierten Handlungen mit einer im Vergleich zum Bevölkerungsdurchschnitt weit erhöhten Wahrscheinlichkeit Adressaten polizeilicher Datenerhebungen werden können. An diese Datenerhebungen können Datenbevorratungen in den Datensammlungen des BKA anschließen. Sowohl die Verhütung und Verfolgung von Ausschreitungen bei oberklassigen Fußballspielen als auch die Bekämpfung der länderübergreifenden politisch motivierten Kriminalität gehören zu den Tätigkeitsschwerpunkten des BKA in seiner Funktion als Zentralstelle, wie sich am bisherigen Dateibestand zeigt. Die Beschwerdeführerin und die Beschwerdeführer sind dementsprechend aktuell oder waren zumindest noch kürzlich in polizeilichen Datensammlungen erfasst, die Beschwerdeführer zu 4 und 5 sogar in Datensammlungen des BKA.

Die Beschwerdeführerin zu 3 und die Beschwerdeführer zu 4 und 5 sind durch die von ihnen angegriffenen Regelungen auch unmittelbar beschwert. Zwar bedürfen die angegriffenen Ermächtigungen zur Weiterverarbeitung personenbezogener Daten des behördlichen Vollzugs. Die Beschwerdeführerin und die Beschwerdeführer können jedoch auf einen Rechtsschutz gegen einzelne Vollzugsakte nicht verwiesen werden, da sie hiervon nicht zuverlässig Kenntnis erhalten. Eine Benachrichtigung ist bei der Bevorratung personenbezogener Daten in den Datensammlungen des BKA gesetzlich ebenso wenig vorgesehen wie bei der späteren Nutzung der bevorrateten Daten. Des Weiteren können die Beschwerdeführerin und die Beschwerdeführer zwar gemäß § 57 BDSG i.V.m. § 84 Abs. 1 Satz 1 BKAG beim BKA Auskunft über sie betreffende Datenspeicherungen im Informationssystem und im polizeilichen Informationsverbund beantragen und gegebenenfalls anschließend gegen eine Speicherung gerichtlich vorgehen. Auf diesem Weg können sie jedoch lediglich dagegen vorgehen, dass zu einem bestimmten Zeitpunkt Daten über sie tatsächlich gespeichert sind, nicht aber – wie es ihrem Rechtsschutzanliegen entspricht – dagegen, dass eine solche Speicherung jederzeit möglich ist, ohne dass sie hierauf Einfluss haben oder hiervon Kenntnis erlangen,

vgl. zur Antiterrordatei BVerfGE 133, 277 (312).

Im Übrigen sieht § 57 Abs. 4 i.V.m. § 56 Abs. 2 BDSG weitreichende Ausnahmen von dem Auskunftsrecht vor, die dazu führen können, dass sich

eine betroffene Person über lange Zeit kein zuverlässiges Bild von den sie betreffenden Datenbevorratungen und Datennutzungen machen kann. Angesichts dessen ist der Weg, über den Auskunftsanspruch gerichtlichen Rechtsschutz zu erlangen, der Beschwerdeführerin und den Beschwerdeführern mangels hinreichender Wirksamkeit nicht zumutbar.

Der Zulässigkeit der Verfassungsbeschwerde steht auch der Subsidiaritätsgrundsatz nicht entgegen. Ein vorgängiges fachgerichtliches Verfahren ist der Beschwerdeführerin zu 3 und den Beschwerdeführern zu 4 und 5 nicht zumutbar, soweit es um einen nachträglichen Rechtsschutz gegen Datenweiterverarbeitungen des BKA geht. Dies ergibt sich aus den oben zum Erfordernis einer unmittelbaren Betroffenheit angeführten Gründen. Ein vorbeugender Rechtsschutz gegen zukünftige Datenweiterverarbeitungen ist der Beschwerdeführerin und den Beschwerdeführern nicht möglich, da sie drohende Datenweiterarbeitungen im Voraus nicht näher bezeichnen können. Insoweit gelten die Ausführungen zur Subsidiarität der Verfassungsbeschwerde der Beschwerdeführerinnen zu 1 und 2 hier entsprechend.

V. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die angegriffenen Regelungen sind gemäß Art. 13 Abs. 1 Satz 1 des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes am 25. Mai 2018 in Kraft getreten.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet. Die angegriffenen Ermächtigungen des BKA zu bestimmten Überwachungsmaßnahmen (unten I) verletzen ebenso Grundrechte wie zentrale Bestandteile der neuen Informationsordnung des BKA (unten II).

I. Überwachungsermächtigungen zur Terrorismusabwehr

Die Ermächtigung zum Einsatz besonderer Mittel der Datenerhebung verstößt teilweise gegen das Übermaßverbot (unten 1). Die Ermächtigungen zu Online-Durchsuchungen und zu Quellen-Telekommunikationsüberwachungen stehen mit den objektiv-rechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht in Einklang (unten 2).

1. Besondere Mittel der Datenerhebung

Die Ermächtigung zum Einsatz besonderer Mittel der Datenerhebung verletzt das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete Recht auf informationelle Selbstbestimmung insoweit, als sie in § 45 Abs. 1 Satz 1 Nr. 4 BKAG einen gezielten Einsatz dieser Mittel gegen Kontaktpersonen ermöglicht.

Die besonderen Mittel der Datenerhebung können je nach den Einsatzmodalitäten einen intensiven Grundrechtseingriff bewirken. Sie müssen darum an einen für Eingriffe hohen Gewichts hinreichend restriktiven Eingriffstatbestand gebunden werden,

BVerfGE 141, 220 (286 f.).

Dies schließt eine gezielte Überwachung von Kontaktpersonen, gegen die selbst kein Verdacht terroristischer Aktivitäten besteht, nicht aus. Die gesetzliche Eingriffsschwelle muss allerdings gewährleisten, dass eine spezifische individuelle Nähe der betroffenen Person zu der aufzuklärenden Gefahr besteht,

BVerfGE 141, 220 (274 f.).

Dieses Erfordernis verfehlt § 45 Abs. 1 Satz 1 Nr. 4 BKAG. Die Vorschrift regelt die Eingriffsschwelle nicht selbst, sondern verweist auf die Generalklausel zur Datenerhebung in § 39 Abs. 2 Nr. 2 BKAG. Diese Regelung hat zwei Komponenten. Zum einen bestimmt sie durch einen Verweis auf § 39 Abs. 2 Nr. 1 BKAG, welche Anforderungen an die verdächtige Zielperson der

Datenerhebung bestehen. Zum anderen definiert sie selbst, in welchem Verhältnis die Kontaktperson zu dieser Zielperson stehen muss.

Während die in § 39 Abs. 2 Nr. 2 BKAG selbst enthaltene zweite Komponente den verfassungsrechtlichen Anforderungen an die Nähe der Kontaktperson zu der Zielperson genügt,

> vgl. zu der Vorgängerregelung in § 20g Abs. 1 Satz 1 Nr. 3 i.V.m. § 20b Abs. 2 Nr. 2 BKAG BVerfGE 141, 220 (291 ff.),

ist die Definition der Zielperson in § 39 Abs. 2 Nr. 1 BKAG unzulänglich, um eingriffsintensive Überwachungsmaßnahmen wie die schwerer wiegenden Modalitäten des Einsatzes besonderer Mittel der Datenerhebung zu legitimieren. Diese Vorschrift lässt es für eine Datenerhebung ausreichen, dass die Zielperson eine terroristische Straftat „begehen will“. Dies mag für die unmittelbar in § 39 Abs. 2 Nr. 1 BKAG enthaltene Ermächtigung zu Datenerhebungen von geringerer Eingriffsintensität ausreichen. Eine Ermächtigung zu schwerwiegenden Eingriffsmaßnahmen bedarf jedoch gehaltvollerer Prognoseanforderungen. Insbesondere schließt § 39 Abs. 2 Nr. 1 BKAG seinem Wortlaut nach nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt,

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

Die zu unkonkrete Beschreibung der Zielperson wirkt auf die in § 39 Abs. 2 Nr. 2 BKAG enthaltene Beschreibung der Kontaktperson zurück. Wenn die Zielperson allein aufgrund allgemeiner Erfahrungssätze bestimmt werden darf, löst sich der Eingriffsanlass in tatsächlicher Hinsicht weitgehend auf. In der Folge kann sich auch die Bestimmung der Kontaktperson auf solche Erfahrungssätze beschränken. Die Trennschärfe der gesetzlichen Beschreibung der Kontaktperson ist insoweit akzessorisch zu der Konkretisierung der Zielperson. Beispielsweise reicht es für eine Überwachung auf der Grundlage von § 39 Abs. 2 Nr. 1 und Nr. 2 lit. b BKAG aus, dass 1. die Zielperson eine terroristische Straftat begehen will und 2. die Kontaktperson aus der Verwertung der Tat Vorteile ziehen könnte. Nach dieser Formulierung muss weder eine konkrete Straftat zumindest ansatzweise konturiert prognostiziert werden noch muss eine gehaltvollere personenbezogene Tatprognose über die Zielperson abgegeben werden. Stattdessen würde es etwa ausreichen, dass der Zielperson aufgrund ihrer sozialen Einbindung in ein terroraffines Milieu terroristische Straftaten zugetraut werden und die Kontaktperson aufgrund allgemeiner

Erfahrungssätze – etwa aufgrund ihrer Stellung als Ehepartnerin der Zielperson – von diesen Straftaten profitieren könnte. Eine Ermächtigung zu einer so detailarmen Prognose verfehlt die verfassungsrechtlichen Anforderungen deutlich.

Dem Befund der Verfassungswidrigkeit von § 45 Abs. 1 Satz 1 Nr. 4 BKAG steht nicht entgegen, dass das angerufene Gericht in seinem Urteil vom 20. April 2016 die Vorgängerregelung zu dieser Vorschrift verfassungsrechtlich gebilligt hat,

vgl. BVerfGE 141, 220 (291 ff.).

Die seinerzeit untersuchte Regelung in § 20g Abs. 1 Satz 1 Nr. 3 BKAG a.F. nahm zwar – vermittelt über eine Legaldefinition – ebenfalls Bezug auf die Generalklausel zu Datenerhebungen in § 20b Abs. 2 Nr. 2 BKAG a.F. Anders als die hier angegriffene Regelung ermöglichte sie jedoch unmittelbar ausdrücklich die Überwachung von „Kontakt- und Begleitpersonen“. Es lag darum nahe, diese Vorschrift so zu verstehen, dass es um eine Überwachung von Kontakt- und Begleitpersonen der in § 20g Abs. 1 Satz 1 Nr. 1 und 2 BKAG a.F. bezeichneten Personengruppen ging. Diese Interpretation liegt ersichtlich auch dem Urteil vom 20. April 2016 zugrunde. Darin untersucht das angerufene Gericht ausschließlich die zweite Komponente der Ermächtigung zur gezielten Überwachung von Kontaktpersonen, also die gesetzliche Beschreibung des Verhältnisses von Kontakt- und Zielperson. Die vorgelagerte Beschreibung des Verhältnisses der Zielperson zu den drohenden Straftaten wird hingegen an dieser Stelle des Urteils nicht erörtert. Dies wird plausibel, wenn angenommen wird, dass die erste Komponente den in § 20g Abs. 1 Satz 1 Nr. 1 und 2 BKAG a.F. enthaltenen Eingriffstatbeständen zu entnehmen war, die das angerufene Gericht unmittelbar vor der Ermächtigung zur Überwachung von Kontakt- und Begleitpersonen verfassungsrechtlich würdigt.

Die heutige Regelung verweist hingegen unmittelbar auf § 39 Abs. 2 Nr. 2 BKAG, der seinerseits allein die unscharfe Beschreibung der Zielperson in § 39 Abs. 2 Nr. 1 BKAG in Bezug nimmt. Dieser Verweis lässt sich nicht auf die in § 45 Abs. 1 Satz 1 Nr. 1-3 BKAG enthaltenen Eingriffstatbestände beziehen.

2. Online-Durchsuchung und Quellen-Telekommunikationsüberwachung

Die Ermächtigungen zu Online-Durchsuchungen in § 49 BKAG und zu Quellen-Telekommunikationsüberwachungen in § 51 Abs. 2 BKAG stehen bei einer rein subjektiv-rechtlichen Betrachtung mit den verfassungsrechtlichen

Anforderungen, wie sie das angerufene Gericht in seinem BKAG-Urteil herausgearbeitet hat, in Einklang. Die gesetzlichen Eingriffsschwellen orientieren sich eng an dem in diesem Urteil formulierten grundrechtlichen Mindestmaß. Auch die einem effektiven Rechtsschutz dienenden Verfahrensregelungen und die Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung sind nicht zu beanstanden. Schließlich enthalten die Vorschriften die gebotenen Regelungen zum Schutz des Zielsystems, das zur Durchführung der Überwachung informationstechnisch infiltriert wird.

Gleichwohl sind § 49 und § 51 Abs. 2 BKAG verfassungswidrig. Grund hierfür ist ein Gesichtspunkt, den das angerufene Gericht in seiner bisherigen Rechtsprechung zu Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen nicht berücksichtigt hat. Hierbei handelt es sich um die objektiv-rechtlichen Anforderungen, die das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dem Gesetzgeber auferlegt. Dieses Grundrecht ist nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff der Gewährleistung zeigt – auch eine staatliche Pflicht dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau erreicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung,

> vgl. etwa Sachs/Krings, JuS 2008, 481 (486); Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Heckmann, in: FS Käfer, 2009, S. 129 (133 ff.); Hoffmann-Riem, JZ 2009, S. 165 ff.; ders., AöR 134 (2009), S. 513 ff.; ders., JZ 2014, S. 53 ff.; Becker, NVwZ 2015, 1335 (1339 f.).

Die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist praktisch hoch bedeutsam, weil solche Systeme strukturell bedingt stets eine Vielzahl von Sicherheitslücken aufweisen, die eigenständig zu Fehlfunktionen führen oder durch Dritte missbräuchlich ausgenutzt werden können. Die Sicherheit informationstechnischer Systeme ist daher als dauerhafte öffentliche Aufgabe anzusehen. Diese Aufgabe kann der Staat allerdings weitgehend nicht eigenhändig erfüllen, da es ihm hierfür sowohl an Ressourcen als auch an Expertise fehlt. In erster Linie obliegt es vielmehr den Herstellern von informationstechnischen Systemen und der darauf laufenden Software,

vermeidbare Sicherheitslücken nicht entstehen zu lassen und später erkannte Sicherheitslücken zeitnah zu schließen. Die staatliche Gewalt kann hierbei lediglich eine unterstützende Rolle einnehmen. Welche Beiträge sie dazu übernimmt, hängt von Gestaltungsentscheidungen ab, für die das Grundgesetz beträchtliche Spielräume lässt. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in seiner objektiv-rechtlichen Dimension erst verletzt, wenn die staatlichen Anstrengungen offenkundig unzureichend sind,

> vgl. zu aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89 (142); 77, 17 (214 f.); 88, 203 (251 ff.); 92, 26 (46); 106, 28 (37); 125, 39 (78 f.); 143, 313 (337 f.).

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen abhängig von dem genutzten Infiltrationsweg auftreten. Insbesondere ist dies der Fall, wenn für die Infiltration des Zielsystems eine noch unbekannte Sicherheitslücke von Hardware oder Software ausgenutzt wird (sogenannter Zero-Day).

Da ein Zero-Day dem Hersteller und den Nutzern des betroffenen informationstechnischen Systems noch unbekannt ist, gibt es gegen ihn aus Sicht dieser Personen keine wirksamen Gegenmaßnahmen. Soweit die Sicherheitslücke sich prinzipiell durch eine Anpassung des Systems (etwa ein Software-Update) schließen ließe, steht der dafür erforderliche technische Baustein noch nicht zur Verfügung. Für die ansonsten notfalls mögliche und gebotene vollständige oder partielle Außerbetriebnahme des Systems besteht aus Sicht der betroffenen Personen kein Anlass, solange die Sicherheitslücke nicht bekannt ist.

Sicherheitsbehörden können Zero-Days ausnutzen, um informationstechnische Systeme zu infiltrieren und so eine Online-Durchsuchung oder eine Quellen-Telekommunikationsüberwachung zu ermöglichen. Dieser Infiltrationsweg erzeugt jedoch einen Zielkonflikt zwischen den Sicherheitsbelangen, denen die Maßnahme dient, und dem durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität

gewährleisteten Anliegen, dass der Staat zur Sicherheit der informationstechnischen Infrastruktur in der Bundesrepublik beiträgt,

> vgl. bereits BVerfGE 120, 274 (326), wo jedoch dieser Zielkonflikt nicht näher analysiert und darum aus ihm keine weiteren Folgerungen gezogen werden. Dies war in dem damaligen Verfahren auch nicht angezeigt, da die seinerzeit angegriffene Eingriffsermächtigung bereits die subjektiv-rechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (weit) verfehlte.

Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Interesse daran, den Zero-Day weiterhin geheim zu halten, um ihn für weitere Online-Durchsuchungen oder Quellen-Telekommunikationsüberwachungen nutzen zu können.

Die Ausnutzung von Zero-Days durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen.

Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur.

Einen darüber hinausgehenden Beitrag zur Schwächung der Informationssicherheit in der Bundesrepublik leistet der Staat dann, wenn eine Behörde Informationen über eine Sicherheitslücke nicht selbst generiert, sondern von Dritten bezieht. Dies ist kein unrealistisches Szenario. Noch in jüngerer Zeit hat der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich („ZITiS“), einer neuen Einrichtung des Bundes, die Sicherheitsbehörden bei der Identifikation und Ausnutzung von Sicherheitslücken unterstützen soll, eingeräumt, seine Stelle verfüge bislang

nicht über die technische Expertise, um Sicherheitslücken im benötigten Umfang selbst aufzudecken,

> vgl. https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html (letzter Abruf am 21. Mai 2019).

Werden Zero-Days auf dem Markt eingekauft, so stützt die beschaffende staatliche Stelle diesen Markt aktiv. Schon wegen der strengen strafrechtlichen Regulierung des Umgangs mit Informationen und Software, die zum Ausspähen oder Abfangen von Daten bestimmt sind (vgl. § 202c StGB), ist anzunehmen, dass die Akteure auf diesem Markt regelmäßig zumindest in einem rechtlichen Graubereich agieren. Die staatliche Teilnahme an diesem Markt birgt darum das erhebliche Risiko, Straftaten zu begünstigen. Sie setzt zudem einen Anreiz für Expertinnen und Experten, ihr Wissen um Sicherheitslücken zu monetarisieren statt damit zur Stärkung der Informationssicherheit beizutragen. So kann die staatliche Marktteilnahme zur Stabilisierung auch des illegalen Marktes und zur Vermehrung der angebotenen Sicherheitslücken beitragen, die von Dritten aufgekauft und ausgenutzt werden können.

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Zero-Days verfügt, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen können. Hierbei handelt es sich nicht um ein weitgehend hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen. So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. Dieses Schadprogramm nutzte eine Sicherheitslücke des Betriebssystems Windows 7 aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte,

> vgl. etwa http://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung; http://faktenfinder.tagesschau.de/wanna-cry-cyberangriff-101.html (letzte Abrufe am 21. Mai 2019).

Chinesische Spione sollen diese Sicherheitslücke bereits im Jahr 2016 von der NSA erlangt und für eigene Angriffe genutzt haben,

vgl. https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html (letzter Abruf am 21. Mai 2019).

Es liegt fern, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass sich ein Verlust nie ausschließen lässt. Mit vergleichbaren Vorfällen infolge einer Sammlung von Sicherheitslücken bei deutschen Behörden wäre daher zu rechnen.

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von Zero-Days einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss.

Die durch die Nutzung und Geheimhaltung von Zero-Days eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.

Zum einen kann der kriminelle Missbrauch der geheim gehaltenen Sicherheitslücken hochrangige Rechtsgüter empfindlich bedrohen. Nahezu alle lebenswichtigen Leistungen werden heute mit informationstechnischer Unterstützung erbracht. Ebenso verfügen so gut wie alle staatlichen und gesellschaftlichen Einrichtungen, deren Ausfall oder Funktionsstörung schwere Schäden verursachen kann, über informationstechnische Komponenten. Werden solche informationstechnischen Komponenten gestört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen, die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. Beispielsweise hat das oben erwähnte Schadprogramm „WannaCry“ informationstechnische Systeme in britischen Krankenhäusern infiltriert. In der Folge mussten unter anderem geplante Operationen verschoben werden. Auch zahlreiche Rechner der Deutschen Bahn wurden infiziert, was unter anderem zum Ausfall einer regionalen Leitstelle führte. Ein weiterer Angriff, der auf von der NSA erbeuteter Technologie basierte, führte dazu, dass bei dem Arzneimittelunternehmen Merck ein kritischer Minderbestand eines Impfstoffs eintrat.

Zum anderen erstreckt sich die Bedrohung durch den Missbrauch von Zero-Days auf praktisch die gesamte Bevölkerung, also ganz überwiegend auf Menschen, die für sicherheitsbehördliche Überwachungsmaßnahmen keinen Anlass geben. Es fehlt mithin vollständig an einer Zurechnungsbeziehung zwischen diesen Menschen und den Belangen, die der Geheimhaltung von Sicherheitslücken zugrunde liegen. Angesichts dessen und wegen der

drohenden schweren Schäden ist die Grenze der Aufopferungspflicht des Einzelnen für das Gemeinwohl deutlich überschritten.

Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von Zero-Days für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Zwar haben die Belange, denen Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen des BKA dienen, schon wegen der grundrechtlich gebotenen restriktiven Fassung des Eingriffstatbestands durchweg hohes Gewicht. Jedoch können diese Belange zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Online-Durchsuchung bzw. einer Quellen-Telekommunikationsüberwachung eine psychische Einflussnahme auf die Nutzer des Zielsystems *(social engineering)*, eine physische Zugriffsmöglichkeit auf das Zielsystem (etwa im Rahmen einer Durchsuchung) oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf solchen Wegen nicht möglich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahmen hinzunehmen und auf andere, gegebenenfalls teurere Maßnahmen auszuweichen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen. Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das objektiv-grundrechtlich nicht hinzunehmende Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt. Dass es einer solchen Vorgabe bedarf, illustriert beispielhaft die Antwort der Bundesregierung auf eine parlamentarische Kleine Anfrage, in der die Bundesregierung eine Nutzung von Zero-Days zumindest nicht ausgeschlossen hat:

> „Ob und inwieweit im Spannungsfeld technischer Erfordernisse, rechtlicher Vorgaben, sicherheits- und rechtspolitischer Erwägungen sowie taktischer Einsatzrahmenbedingungen zukünftig eine Nutzung sog. ‚Zero-Day-Exploits' für die Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung durch Sicherheitsbehörden in Betracht kommt, ist durch die zuständigen Stellen der Bundesregierung in Abstimmung

mit den zu beteiligenden nationalen und ggf. internationalen Stellen und Gremien zu prüfen."

Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413; die Antwort auf diese Fragen ist eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD (letzter Abruf am 21. Mai 2019).

Selbst wenn entgegen der oben begründeten Auffassung eine staatliche Infiltration informationstechnischer Systeme mithilfe von noch unbekannten Sicherheitslücken verfassungsrechtlich überhaupt rechtfertigungsfähig wäre, müsste die gesetzliche Grundlage der Infiltration zumindest Vorgaben für ein behördliches Schwachstellen-Management enthalten. Nur aufgrund prozeduraler Sicherungen und materieller Kriterien für ein solches Schwachstellen-Management kann das enorme Risiko für die informationstechnische Infrastruktur der Bundesrepublik hinnehmbar sein. In diesem Rahmen wäre ein Bündel von maßstabsbildenden Faktoren zu beachten, etwa

- die Verbreitung der Sicherheitslücke:
    - in quantitativer Hinsicht: Zahl der betroffenen Nutzerinnen und Nutzer,
    - in qualitativer Hinsicht: Art der betroffenen Nutzerinnen und Nutzer,
- das Gewicht der Sicherheitslücke:
    - zur Ausnutzung erforderlicher Aufwand,
    - aus der Ausnutzung resultierender Schaden,
- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,
- die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen bei einer (zeitweisen) Geheimhaltung der Lücke,
- die Wahrscheinlichkeit, dass Dritte die Lücke finden.

vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf (letzter Abruf am 21. Mai 2019).

Da § 49 und § 51 Abs. 2 BKAG kein ausdrückliches Verbot einer Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration enthalten und auch keine Vorgaben für ein behördliches Schwachstellen-Management errichten, sind die Vorschriften in diesem Punkt verfassungswidrig und bedarf einer Ergänzung.

II. Ermächtigungen zur Bevorratung und späteren Nutzung personenbezogener Daten

Zentrale Bestandteile der Informationsordnung des BKA verletzen das Grundrecht auf informationelle Selbstbestimmung, da das Gesetz in zu weitem Ausmaß die verfahrensexterne Bevorratung und spätere Nutzung personenbezogener Daten im Informationssystem des BKA und im polizeilichen Informationsverbund erlaubt.

1. Verfassungsrechtliche Maßstäbe

Die verfassungsrechtlichen Grenzen der polizeilichen Informationsordnung wurden in der Senatsrechtsprechung des angerufenen Gerichts bislang nicht umfassend geklärt. Die Entscheidungen zur Bevorratung von Telekommunikationsdaten,

BVerfGE 125, 260; 131, 151,

und das Urteil zur Antiterrordatei,

BVerfGE 133, 277,

betrafen Datenbestände, die jeweils erhebliche Besonderheiten aufwiesen. Die bevorrateten Telekommunikationsdaten fielen nicht im Rahmen der polizeilichen Aufgabenerfüllung an, sondern waren anlasslos zu bevorraten. Darüber hinaus wurden diese Daten nicht bei der Polizei, sondern bei Telekommunikationsunternehmen gespeichert. Die Antiterrordatei unterscheidet sich als Indexdatei, die sich auf einen spezifischen Sachbereich beschränkt und primär Datenübermittlungen vorbereitet, beträchtlich von breiter angelegten, in erster Linie für unmittelbare Auswertungen vorgesehenen polizeilichen Datenbeständen.

Im Übrigen standen im Vordergrund der Senatsrechtsprechung zur Weiterverarbeitung von Daten, die eine Sicherheitsbehörde im Rahmen ihrer

Aufgabenerfüllung erhoben hat, die Anforderungen an die unmittelbar an die Erhebung anschließende zweckändernde Nutzung oder Übermittlung der Daten,

vgl. zuletzt BVerfGE 141, 220 (324 ff.).

Im Folgenden wird ein Vorschlag zur Konturierung der verfassungsrechtlichen Anforderungen an die polizeiliche Informationsordnung unterbreitet, der sich an Einzelaussagen aus der Senats- und Kammerrechtsprechung des angerufenen Gerichts und daneben – im Sinne von Rechtserkenntnisquellen – an der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK und des Gerichtshofs der Europäischen Union zu Art. 7 und Art. 8 GRCh sowie an der JI-RL orientiert.

a) Eigenständige Maßstabsbildung für die polizeiliche Informationsordnung

Um die Bevorratung polizeilicher Daten in verfahrensexternen Datensammlungen und die Nutzung der bevorrateten Daten in späteren polizeilichen Verfahren verfassungsrechtlich einzuhegen, bedarf es eigenständiger Maßstäbe. Insbesondere kann nicht ohne weiteres auf die grundrechtlichen Anforderungen an die unmittelbare Weiterverarbeitung erhobener Daten zurückgegriffen werden, die das angerufene Gericht in seinem Urteil zum alten BKAG konsolidiert hat. Zwar werden in beiden Fallkonstellationen Daten aus dem polizeilichen Verfahren, in dessen Rahmen sie erhoben wurden, in weitere Verfahren überführt. Jedoch unterscheiden sich die beiden Fallkonstellationen darin, dass bei der unmittelbaren Weiterverarbeitung ein konkretes Zielverfahren bereits läuft oder mit der Weiterverarbeitung in Gang gesetzt wird, während zum Zeitpunkt der Datenbevorratung noch nicht absehbar ist, ob, wann und in welchem Kontext die bevorrateten Daten einmal genutzt werden sollen.

Die Regulierung von polizeilichen Datensammlungen hat darum einen zeitlich gestreckten zweiaktigen Vorgang zum Gegenstand, der aus der Bevorratung und der späteren Nutzung von Daten besteht. Hieraus ergeben sich einerseits praktische Verarbeitungsbedürfnisse, die bei der unmittelbaren Weiterverarbeitung von Daten nicht auftreten und darum bei der verfassungsrechtlichen Maßstabsbildung nicht berücksichtigt werden müssen. Andererseits erzeugt die zeitliche Streckung von Datenbevorratung und Datennutzung besondere grundrechtliche Risiken, die durch besondere verfassungsrechtliche Anforderungen abgeschirmt werden müssen. Dass eine schematische Übertragung der Anforderungen, die das angerufene Gericht im

BKAG-Urteil für die unmittelbare Weiterverarbeitung entwickelt hat, verfehlt wäre, zeigt sich, wenn diese Anforderungen probeweise auf die Datenbevorratung und spätere Datennutzung angewandt werden.

Das angerufene Gericht hat in diesem Urteil zwischen zwei Weiterverarbeitungskonstellationen unterschieden, für die es unterschiedlich strenge verfassungsrechtliche Maßstäbe entwickelt hat. Eine Weiterverarbeitung erhobener Daten in einem Verfahren derselben Behörde im Rahmen derselben Aufgabe zum Schutz gleichwertiger Rechtsgüter wie im Ausgangsverfahren hält sich als weitere Nutzung im Rahmen der verfassungsrechtlichen Zweckbindung der Daten. Der Gesetzgeber darf eine solche weitere Nutzung unabhängig von weiteren gesetzlichen Voraussetzungen als bloßer Spurenansatz zulassen, der den Ausgangspunkt weiterer Ermittlungen bildet,

BVerfGE 141, 220 (324 ff.).

Hingegen ist eine Weiterverarbeitung durch eine andere Behörde oder durch dieselbe Behörde im Rahmen einer anderen Aufgabe als Zweckänderung besonders rechtfertigungsbedürftig. Der Gesetzgeber darf die zweckändernde Weiterverarbeitung nach dem Kriterium einer hypothetischen Datenneuerhebung zulassen, wenn der neue Verarbeitungszweck dem Erhebungszweck gleichwertig ist. In tatsächlicher Hinsicht setzt die Zweckänderung einen konkreten Ermittlungsansatz voraus,

BVerfGE 141, 220 (326 ff.).

Werden diese verfassungsrechtlichen Maßstäbe ohne weiteres auf die Bevorratung und spätere Nutzung von Daten in polizeilichen Datensammlungen übertragen, so ergeben sich teils dysfunktionale, teils unangemessene Ergebnisse.

Dysfunktional wäre es, die Datenbevorratung als Zweckänderung zu behandeln und von einem konkreten Ermittlungsansatz abhängig zu machen. Zwar hat das angerufene Gericht in seinem Urteil zum BKAG nicht näher ausgeführt, was unter einem konkreten Ermittlungsansatz zu verstehen ist und wie genau sich ein konkreter Ermittlungsansatz von den hergebrachten polizeilichen Eingriffsschwellen der konkreten Gefahr und des Anfangsverdachts einer Straftat unterscheidet. Aus dem Urteil geht aber immerhin hervor, dass dazu über einen „potenziellen Informationsgehalt“ bestimmter Daten hinaus ein einzelfallbezogener tatsächlicher Anlass für die Weiterverarbeitung vorliegen muss,

BVerfGE 141, 220 (336 f.).

Tragfähig erscheint daher die Umschreibung in der Gesetzesbegründung zu § 12 BKAG, nach der ein konkreter Ermittlungsansatz vorliegt, wenn

> „sich eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut darstellt."
>
> BT-Drs. 18/11163, S. 91.

Würde die Bevorratung von Daten in einer polizeilichen verfahrensexternen Datensammlung von Verfassungs wegen an einen solchen einzelfallbezogenen Anlass geknüpft, so wären derartige Datensammlungen hinfällig. Verfahrensexterne Datensammlungen sollen einen Informationsbestand für noch nicht konkret absehbare soziale Konflikte bereitstellen. Der Speicherung von Daten in einer solchen Datensammlung liegt darum in aller Regel gerade kein einzelfallbezogener Anlass zugrunde. Das Erfordernis eines konkreten Ermittlungsansatzes würde die polizeiliche Informationsordnung daher ohne nachvollziehbaren Grund weitgehend aushebeln. Insbesondere die Zentralstellenaufgabe des BKA würde dadurch erheblich beeinträchtigt. Dies kann nicht der Sinn einer verfassungsrechtlichen Maßstabsbildung sein.

Unangemessen wäre es demgegenüber, die Datenbevorratung und die spätere Nutzung der bevorrateten Daten durch die datenerhebende Behörde im Rahmen derselben Aufgabe als weitere Nutzung zu behandeln. In diesem Fall wären sowohl die Bevorratung als auch die spätere Nutzung an keinen tatsächlichen Anlass gebunden. Polizeibehörden könnten einmal erhobene Daten ohne Beschränkungen in einem umfassenden Datenpool speichern und zur Verfolgung hinreichend gewichtiger Zwecke im Rahmen derselben Aufgabe anlasslos jederzeit in jeder denkbaren Weise nutzen. Dies schlösse beispielsweise Datenverknüpfungen zur Erzeugung umfassender Sozialprofile verdächtiger Milieus oder zur Erzeugung weitreichender Persönlichkeitsprofile von Einzelpersonen ein. Die Einordnung der Datenbevorratung und der späteren Datennutzung als weitere Nutzung hätte damit zur Folge, dass die materiellen Sicherungen des Datenschutzrechts im Rahmen der betreffenden Aufgabe praktisch vollständig entfielen, sobald personenbezogene Daten einmal rechtmäßig erhoben wurden. Damit blieben die verfassungsrechtlichen

Anforderungen selbst hinter dem Mindestschutzstandard, den die JI-RL errichtet, deutlich zurück.

Allerdings lässt sich dem BKAG-Urteil zumindest mittelbar und andeutungsweise entnehmen, dass das angerufene Gericht die neue Rechtsfigur der weiteren Nutzung nur auf die unmittelbare Weiterverarbeitung erhobener Daten in einem weiteren behördlichen Verfahren, nicht aber auf die verfahrensexterne Bevorratung von Daten beziehen wollte. Dies legt schon der Begriff der weiteren Nutzung nahe. Nach dem seinerzeit noch geltenden alten Datenschutzrecht war die Nutzung von Daten als eigenständige Phase des Datenumgangs ausgestaltet (vgl. § 3 Abs. 5 BDSG a.F.). Die Speicherung von Daten war hingegen ein Unterfall der Datenverarbeitung und gerade keine Datennutzung (vgl. § 3 Abs. 4 Satz 1 BDSG a.F.). Es liegt nahe, die Ausführungen des angerufenen Gerichts so zu verstehen, dass sie sich terminologisch an das damals geltende einfache Recht anlehnen. Hierfür sprechen auch weitere Passagen des Urteils, die keinen Sinn ergäben, wenn die weitere Nutzung im verfassungsrechtlichen Sinne die Bevorratung von Daten in verfahrensexternen Datensammlungen für noch nicht konkret absehbare zukünftige Verfahren umfasste. So hat das angerufene Gericht betont, von der Befugnis zur weiteren Nutzung der Daten bleibe die Pflicht unberührt, die Daten nach Erreichung des mit der Erhebung verfolgten Zwecks zu löschen,

BVerfGE 141, 220 (332 f.).

Würde die weitere Nutzung die Datenbevorratung umfassen, so ginge es aber gerade um eine Datenbevorratung über den Erhebungszweck hinaus. Gleichläufig heißt es an anderer Stelle in dem Urteil, von der Löschung erhobener Daten über den unmittelbaren Anlassfall hinaus dürfe nur dann abgesehen werden, wenn sich aus den Daten konkrete Ermittlungsansätze ergäben,

BVerfGE 141, 220 (322 f.).

Diese Aussage wäre inkonsistent zu der Differenzierung zwischen weiterer Nutzung und Zweckänderung, die das angerufene Gericht im BKAG-Urteil entwickelt, wenn eine Datenbevorratung als weitere Nutzung anzusehen wäre, da die weitere Nutzung gerade keinen konkreten Ermittlungsansatz voraussetzen soll.

b) Parameter für Gestaltung und verfassungsrechtliche Bewertung der polizeilichen Informationsordnung

Um die grundrechtlichen Anforderungen an die polizeiliche Informationsordnung zu konturieren, müssen die einer gesetzlichen Regulierung zugänglichen Parameter geklärt werden, an die diese Anforderungen anknüpfen können. Hierzu sind im ersten Schritt zwei Grundrechtseingriffe zu differenzieren, die zusammengenommen eine polizeiliche Datensammlung konstituieren: die Bevorratung polizeilicher Daten und die spätere Nutzung der bevorrateten Daten. Hinsichtlich der Bevorratung sind für die materielle grundrechtliche Bewertung 1. der Inhalt der Datensammlung, der durch Art und Umfang der bevorrateten Daten bestimmt wird, sowie 2. die Voraussetzungen und zeitlichen Grenzen einer Datenspeicherung maßgeblich. Hinsichtlich der späteren Nutzung der bevorrateten Daten bilden 3. die Voraussetzungen und zulässigen Ziele einer Nutzung, und 4. die zulässigen Nutzungsarten die relevanten Faktoren,

> vgl. zur Antiterrordatei für die Parameter Voraussetzungen der Speicherung (=erfasster Personenkreis), Inhalt der Datensammlung sowie Nutzungsvoraussetzungen und Nutzungsarten BVerfGE 133, 277 (339 ff., 350 ff., 360 ff.); ferner EGMR (4. Sektion), Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 195; EGMR (1. Sektion), Urteil vom 24. Januar 2019, No. 43514/15 (Catt/Vereinigtes Königreich), Rn. 95.

Diese vier Parameter sind aus grundrechtlicher Sicht miteinander verflochten. Insbesondere handelt es sich zwar bei der Datenbevorratung und der späteren Datennutzung um zwei eigenständige Grundrechtseingriffe. Diese sind jedoch aufeinander bezogen, da die Anforderungen an die Datennutzung zugleich den Zweck der Datenbevorratung mitdefinieren. Die Eingriffsintensität der Datensammlung und die daraus folgenden grundrechtlichen Maßstäbe lassen sich darum nur in einer Gesamtschau von Datenbevorratung und Datennutzung ermitteln,

> vgl. ansatzweise EGMR (4. Sektion), Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 200.

Folglich stehen die Parameter der Regulierung polizeilicher Datensammlungen zueinander in einem partiellen wechselseitigen Kompensationsverhältnis. Wird einer von ihnen weit gefasst, so müssen restriktivere Anforderungen an die anderen gestellt werden, um die

Datensammlung insgesamt zu rechtfertigen. Die Kompensation hat allerdings Grenzen. Insbesondere darf keiner der Parameter vollständig entgrenzt werden.

Soll etwa eine Datensammlung in großem Umfang sensible Daten enthalten, die unter niedrigen Voraussetzungen bevorratet werden, und ermöglicht das Gesetz ein breites Spektrum von Datennutzungen, so sind an die Voraussetzungen und Ziele der Datennutzung besonders strenge Anforderungen zu stellen,

> vgl. für die Nutzung anlasslos bevorrateter Telekommunikations-Verkehrsdaten – insoweit hinsichtlich der Billigung einer anlasslosen Datensammlung allerdings mittlerweile überholt – BVerfGE 125, 260 (327 ff.); für eine merkmalbezogene Recherche in der Antiterrordatei und für die umfassende Auswertung dieser Datei in Eilfällen BVerfGE 133, 277 (363 f., 364 f.).

Wird die Nutzung solcher Daten eng auf weniger eingriffsintensive Nutzungsarten begrenzt, so können die Voraussetzungen und Ziele der Datennutzung offener formuliert werden,

> vgl. für die Auflösung einer dynamischen IP-Adresse mittels bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (340 ff.); für die Nutzung der Antiterrordatei als Indexdatei BVerfGE 133, 277 (360 ff.).

Daneben können großzügigere Regelungen für Art, Voraussetzungen und Ziele der Datennutzung gerechtfertigt werden, wenn sich der Inhalt einer Datensammlung auf einen begrenzten Bestand weniger sensibler Daten beschränkt,

> vgl. für die Nutzung bevorrateter Telekommunikations-Bestandsdaten BVerfGE 130, 151 (195 ff.),

oder wenn die Datenbevorratung an besonders strenge Voraussetzungen geknüpft wird.

Allerdings bestehen verfassungsrechtliche Untergrenzen für die Rechtfertigung polizeilicher Datensammlungen, die durch die wechselseitige Kompensation der Parameter nicht verschoben werden können.

Auf der Ebene der Datenbevorratung ist den spezifischen Risiken Rechnung zu tragen, welche die Bevorratung für die betroffenen Personen mit sich bringt. Die Bevorratung kann unabhängig von den Anforderungen an die spätere

Datennutzung eine Stigmatisierung der betroffenen Personen bewirken und Einschüchterungseffekte hervorrufen,

> vgl. EGMR (Große Kammer), Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 121 ff.

Zudem birgt die Bevorratung die nie auszuschließenden Risiken einer irrtümlich oder sogar missbräuchlich rechtswidrigen Nutzung der bevorrateten Daten und eines unbefugten Zugriffs auf die Daten durch Dritte,

> vgl. beispielhaft zu einem kürzlich aufgetretenen schwerwiegenden Missbrauchsfall bei einer Landespolizeibehörde https://www.zeit.de/politik/deutschland/2019-02/seda-basay-yildiz-drohbrief-frankfurter-rechtsanwaeltin-rechtsextremismus (letzter Abruf am 21. Mai 2019).

Insbesondere die anlasslose großflächige Speicherung sensibler Daten lässt sich deshalb unabhängig von den Modalitäten und Voraussetzungen der späteren Datennutzung nie rechtfertigen,

> vgl. EuGH (Große Kammer), Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 (Tele2 Sverige u.a.), Rn. 97 ff.; EuGH (Große Kammer), Gutachten 1/15 vom 26. Juli 2017, Rn. 204 ff.; tendenziell gleichläufig EGMR (Große Kammer), Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 119 ff.; EGMR (4. Sektion), Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 195 ff.; überholt ist insoweit BVerfGE 125, 260 (316 ff.).

Die Bevorratung sensibler polizeilicher Daten ist vielmehr stets an einen zumindest ansatzweise konturierten Anlass zu knüpfen, der das Ausmaß der Datenbevorratung auf hinreichend gewichtige Fälle begrenzt,

> vgl. EGMR (5. Sektion), Urteil vom 18. April 2013, No. 19522/09 (M.K./Frankreich), Rn. 38; aus der Kammerrechtsprechung des angerufenen Gerichts BVerfGE 103, 21 (34); BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 16. Mai 2002 – 1 BvR 2257/01 –, juris, Rn. 14 f.

Bloße Mutmaßungen über die betroffene Person oder lediglich vage Anhaltspunkte für ein Fehlverhalten reichen demgegenüber nicht aus, um solche Daten über einen längeren Zeitraum zu bevorraten,

vgl. EGMR (2. Sektion), Urteil vom 18. Oktober 2011, No. 16188/07 (Khelili/Schweiz), Rn. 63 ff.; aus der Kammerrechtsprechung des angerufenen Gerichts BVerfGE 103, 21 (37); BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 1. Juni 2006 – 1 BvR 2293/03 –, juris, Rn. 15.

Zudem muss zum Zeitpunkt der Bevorratung zumindest ansatzweise absehbar sein, dass die bevorrateten Daten zukünftig einen Beitrag zur polizeilichen Aufgabenerfüllung erbringen können. Ist dies nicht der Fall, so ist die – auch unionsrechtlich durch Art. 4 Abs. 1 lit. c und e JI-RL vorausgesetzte – Erforderlichkeit der Bevorratung nicht gewährleistet,

vgl. EGMR (1. Sektion), Urteil vom 24. Januar 2019, No. 43514/15 (Catt/Vereinigtes Königreich), Rn. 116 ff.

Schließlich muss die Bevorratungsermächtigung die Bevorratung zeitlich begrenzen. Dies ist insbesondere bedeutsam, wenn die Bevorratung an die Feststellung oder gar lediglich an den Verdacht oder die Prognose eines Fehlverhaltens der betroffenen Person anknüpft. Denn eine solche Datenbevorratung ist geeignet, stigmatisierende Wirkungen zu zeitigen, die gerade nach längerer Zeit die betroffene Person unangemessen belasten können,

vgl. EGMR (Große Kammer), Urteil vom 4. Dezember 2008, No. 30562/04 and 30566/04 (S. und Marper/Vereinigtes Königreich), Rn. 119; EGMR (4. Sektion), Urteil vom 13. November 2012, No. 24029/07 (M.M./Vereinigtes Königreich), Rn. 199.

Dementsprechend schreibt Art. 5 JI-RL vor, dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Zudem ist durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

Auf der Ebene der Datennutzung ist unabhängig von den Voraussetzungen der Datenbevorratung die grundrechtliche Zweckbindung zu beachten. Aus der zeitlichen Streckung der Weiterverarbeitung ergibt sich kein Grund, von diesem Maßstab zulasten der betroffenen Person abzurücken. Darf die Polizei personenbezogene Daten bevorraten, die sie mit eingriffsintensiven Mitteln erhoben hat, so darf die zweckändernde Nutzung der bevorrateten Daten darum nur zugelassen werden, wenn die Voraussetzungen einer hypothetischen Datenneuerhebung vorliegen, wie sie das angerufene Gericht in seinem Urteil zum alten BKA-Gesetz entwickelt hat.

Hingegen lässt sich die im selben Urteil entwickelte Rechtsfigur der weiteren Nutzung nicht bruchlos auf die Nutzung von Daten übertragen, die über einen längeren Zeitraum bevorratet werden. Ansonsten würde die Nutzung bevorrateter Daten während der potenziell langjährigen Bevorratungszeit im Rahmen der betreffenden behördlichen Aufgabe anlasslos ermöglicht und so ins Belieben der bevorratenden Behörde gestellt. Von der grundrechtlichen Zweckbindung bliebe im Rahmen der betreffenden Aufgabe ebenso wenig übrig wie von dem Gebot einer verhältnismäßigen Datenverarbeitung, obwohl beide durch Art. 4 Abs. 1 lit. b und c, Abs. 2 JI-RL auch unionsrechtlich vorgegeben sind. Die weitere Nutzung bevorrateter Daten im Rahmen derselben behördlichen Aufgabe bedarf daher eines tatsächlichen Anlasses, wenngleich dieser schwächer konturiert ausfallen kann als der im Rahmen einer hypothetischen Datenneuerhebung erforderliche konkrete Ermittlungsansatz. Mindesterfordernis der Datennutzung ist eine gegenüber dem jederzeit und überall drohenden allgemeinen Schadensrisiko herausgehobene Bedrohungslage, die es ermöglicht, die Datennutzung mithilfe des Gebots der Erforderlichkeit auf ein hinnehmbares Maß zu begrenzen.

2. Datenbevorratung und Datennutzung zum Zweck der Terrorismusabwehr

Nach diesen Maßstäben ist § 16 Abs. 1 BKAG insoweit verfassungswidrig, als diese Norm dem BKA in Verbindung mit § 12 Abs. 1 Satz 1 BKAG erlaubt, personenbezogene Daten, die es durch eingriffsintensive Überwachungsmaßnahmen zum Zweck der Terrorismusabwehr (§ 5 BKAG) erlangt hat, im Rahmen dieser Aufgabe im Informationssystem zu bevorraten und zu nutzen.

§ 16 Abs. 1 BKAG bildet in dieser Fallkonstellation im Ergebnis die alleinige Ermächtigung zur Bevorratung und Nutzung erhobener Daten. Eine weitere Vorschrift, die zusätzliche Voraussetzungen errichtete, existiert prinzipiell nicht. Insbesondere gelten § 18 und § 19 BKAG nur für Datenweiterverarbeitungen im Rahmen der Zentralstellenfunktion des § 2 BKAG. Da es sich bei der hier gegenständlichen Fallkonstellation um eine Weiterverarbeitung im Rahmen derselben Aufgabe handelt, bemisst sich die Weiterverarbeitung grundsätzlich nach § 12 Abs. 1 Satz 1 BKAG. Diese Norm errichtet keinen besonderen tatsächlichen Weiterverarbeitungsanlass, sondern verlangt lediglich, dass die Weiterverarbeitung dem Schutz von Rechtsgütern dient, die den Schutzgütern der Datenerhebung gleichwertig sind. Dies ist bei einer Weiterverarbeitung zum Zweck der Terrorismusabwehr

praktisch immer der Fall, da die Aufgabe aus § 5 BKAG ausschließlich den Schutz hochwertiger Rechtsgüter vor schwerwiegenden Bedrohungen zum Gegenstand hat,

vgl. zu § 4a Abs. 1 Satz 2 BKAG a.F. BVerfGE 141, 220 (331 f.).

§ 12 Abs. 1 Satz 1 BKAG läuft also im Rahmen der Terrorismusabwehr praktisch leer. Strengere Anforderungen errichtet § 12 Abs. 1 Satz 2 BKAG lediglich an die Weiterverarbeitung von Daten, die das BKA durch Wohnraumüberwachungen und Online-Durchsuchungen erlangt hat. Insoweit bestehen gegen die Weiterverarbeitungsermächtigung keine verfassungsrechtlichen Bedenken, so dass diese Vorschrift hier außer Betracht bleibt.

Die Bevorratung von Daten, die das BKA zum Zweck der Terrorismusabwehr erhoben hat, ist nach § 16 Abs. 1 BKAG zulässig, wenn sie zur Erfüllung der Aufgabe der Terrorismusabwehr erforderlich ist. Wenngleich die Interpretation dieses Eingriffstatbestands Schwierigkeiten aufwirft,

vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 233 f., 508,

liegt sprachlich am nächsten, dass damit ein konkreter tatsächlicher Bevorratungsanlass nicht vorausgesetzt wird. Grundlage der Bevorratung ist dann lediglich die Erwartung, dass die bevorrateten Daten möglicherweise zukünftig einmal für die Terrorismusabwehr benötigt werden. Da die Daten in der hier gegenständlichen Fallkonstellation im Zusammenhang mit der Terrorismusabwehr erhoben wurden, wird sich dies praktisch immer bejahen lassen, soweit die Datenerhebung nicht von vornherein ohne jeglichen Ertrag geblieben ist. So kann das BKA neben Daten über „Gefährder“ auch etwa Daten über Dritte ohne besonderen Anlass bevorraten, wenn sich nur irgendwie begründen lässt, dass diese Daten einmal zur Erfüllung der Aufgabe des § 5 BKAG beitragen können. Hierzu könnten schon lose und oberflächliche soziale Kontakte zwischen den betroffenen Dritten und mutmaßlichen Angehörigen des terroristischen Milieus ausreichen. § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG ermöglicht mithin eine nahezu umfassende Bevorratung der personenbezogenen Daten, die das BKA zum Zweck der Terrorismusabwehr erhoben hat, selbst wenn es hierzu eingriffsintensive Mittel wie die in § 45 Abs. 2 BKAG genannten eingesetzt hat. Die aus § 79 Abs. 1 Satz 1 BKAG folgende Vorgabe, dass die im Rahmen der Terrorismusabwehr erhobenen Daten nach Zweckerreichung grundsätzlich zu löschen sind, steht der Bevorratung nicht entgegen, da hiervon Daten ausgenommen sind, die

nach den Vorschriften des Abschnitts 2 Unterabschnitt 2, also namentlich auch gemäß § 16 Abs. 1 BKAG weiterverarbeitet werden.

Desweiteren erlaubt § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG die Nutzung der bevorrateten Daten zum Zweck der Terrorismusabwehr gleichfalls bereits dann, wenn sie zur Erfüllung dieser Aufgabe erforderlich ist. Das BKA darf die bevorrateten Daten damit anlassunabhängig auf jede erdenkliche Weise nutzen, etwa um mithilfe komplexer Analyseverfahren erste Verdachtsmomente zu generieren. Auf die Stellung der betroffenen Personen als potenzielle terroristische Straftäter oder Dritte kommt es auch insoweit nicht an. Die gesetzlich geforderte Erforderlichkeitsprüfung schließt im Wesentlichen nur weitgehend irrationale Datennutzungen „ins Blaue hinein“ aus. Ansonsten wird sich die Erforderlichkeit der Nutzung in aller Regel begründen lassen.

Insgesamt ermöglicht § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG damit dem BKA, die durch Datenerhebungen zur Terrorismusabwehr gewonnenen Informationen – mit Ausnahme der durch Wohnraumüberwachungen und Online-Durchsuchungen erlangten Erkenntnisse – in einem stetig größer werdenden Datenpool zusammenzuführen, den es im Rahmen dieser Aufgabe annähernd nach Belieben auswerten darf. Das differenzierte Gefüge von Eingriffsanlässen und persönlichen Inanspruchnahmegründen, das die gesetzlichen Datenerhebungsermächtigungen kennzeichnet, wird auf den nachgelagerten Stufen der Datenbevorratung und Datennutzung so gut wie vollständig nivelliert. Die gesetzliche Weiterverarbeitungsermächtigung zeigt damit exemplarisch auf, warum sich die von dem angerufenen Gericht entwickelte Rechtsfigur der weiteren Nutzung nicht auf die längerfristige verfahrensexterne Bevorratung von Daten übertragen lässt. Die Bevorratung insbesondere sensibler Daten, die durch eingriffsintensive Überwachungsmaßnahmen zur Terrorismusabwehr erhoben wurden, bedarf vielmehr eines hinreichenden Anlasses und einer zeitlichen Begrenzung. Zudem muss dem Eingriffsgewicht der Bevorratung auch durch einen hinreichend restriktiven Zuschnitt der Ermächtigung zur späteren Nutzung der bevorrateten Daten Rechnung getragen werden. § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG leistet dies nicht ansatzweise.

3. Datenbevorratung und Datennutzung im Rahmen der Zentralstellenfunktion

Die in § 18 Abs. 1 und Abs. 2 (auch in Verbindung mit § 29 Abs. 4 Satz 2) BKAG enthaltenen Ermächtigungen des BKA und der am polizeilichen Informationsverbund teilnehmenden Behörden, personenbezogene Daten

über bestimmte Personenkreise im Rahmen der Zentralstellenaufgabe zu bevorraten und zu nutzen, verfehlen gleichfalls in erheblichem Ausmaß die verfassungsrechtlichen Anforderungen.

a) Zu weitreichende Bevorratungsermächtigungen

Soweit § 18 BKAG das BKA und (in Verbindung mit § 29 Abs. 4 Satz 2 BKAG) die Teilnehmer am polizeilichen Informationsverbund ermächtigt, personenbezogene Daten zu bevorraten, ist die Norm zu weit gefasst. Die in dieser Norm enthaltenen Bevorratungsermächtigungen schreiben weitgehend die Tatbestände des § 8 BKAG a.F. fort und teilen die rechtsstaatlichen Defizite dieser Norm,

vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 508 ff.

Sie vertiefen diese Defizite allerdings sogar noch, da nach dem Wegfall der alten Dateistruktur die einengenden Zweckbestimmungen der Errichtungsanordnungen kein Pendant im geltenden Recht finden. Die bevorrateten Daten stehen vielmehr prinzipiell allen am Informationsverbund teilnehmenden Behörden für alle erdenklichen Auswertungszwecke zur Verfügung. Hierdurch erhöht sich die Eingriffsintensität der Datenbevorratung beträchtlich, ohne dass die gesetzlichen Bevorratungstatbestände dem Rechnung trügen.

Im Einzelnen bestehen gegen die gesetzlichen Bevorratungsermächtigungen die folgenden grundrechtlichen Einwände:

aa) Erforderlichkeitsanordnung: § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG

Gemäß § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG dürfen bestimmte Basisdaten verurteilter Straftäter bevorratet werden. Die Norm errichtet für die Bevorratung über die Verurteilung hinaus keine weiteren Tatbestandsvoraussetzungen. Der Gesetzgeber hat damit die nach allgemeinen datenschutzrechtlichen Grundsätzen (vgl. Art. 8 Abs. 1 JI-RL, § 3 BDSG) mindestens gebotene Prüfung, ob die in der Bevorratung liegende Datenverarbeitung zur Aufgabenerfüllung erforderlich ist, durch eine abstrakt-generelle Anordnung vorweggenommen. Erst recht setzt die Bevorratung keine polizeiliche Prognose eines zukünftigen Fehlverhaltens der betroffenen Person voraus.

Die Datenbevorratung steht allerdings im Ermessen der bevorratenden Behörde. Dieses Ermessen wird jedoch durch § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG nicht näher angeleitet. Da die Zentralstellenaufgabe des BKA gemäß § 2 Abs. 2 Nr. 1 BKAG auf eine möglichst vollständige Sammlung der für die

Aufgabenerfüllung erforderlichen Informationen ausgerichtet ist, liegt es nahe, von einem intendierten Ermessen auszugehen. Danach ist nur in atypischen Fällen von einer Datenbevorratung nach § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG abzusehen,

> in diese Richtung implizit auch Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 18 BKAG Rn. 31, mit Beispielen für Sonderfälle, in denen eine Speicherung nicht angezeigt ist.

Die in der angegriffenen Norm vorgesehene Datenbevorratung kann die betroffene Person erheblich belasten, auch wenn die Bevorratung sich auf Basisdaten beschränkt. Die aus dem Datenbestand des BKA ersichtliche Eigenschaft als verurteilter Straftäter kann bereits für sich genommen die betroffene Person stigmatisieren. Die Bevorratung kann zudem für die betroffene Person schwerwiegende Folgen haben, wenn eine Polizeibehörde in einer tatsächlichen oder vermeintlichen Krisensituation zur Lagebeurteilung auf die bevorrateten Daten zugreift,

> vgl. beispielhaft zur praktischen Verwendung der auf der Grundlage von § 8 BKAG a.F. 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; vgl. zudem den von dem Beschwerdeführer zu 5 ausgetragenen Rechtsstreit, der ein Ausreiseverbot aufgrund einer Datenspeicherung zum Gegenstand hatte **(Anlage 5)**.

Diese Risiken sind auch einer Person, die durch eine gerichtlich festgestellte Straftat einen zurechenbaren Anlass für die Speicherung gegeben hat, nicht unbegrenzt zumutbar. Vielmehr sind in zweierlei Hinsicht Begrenzungen der Bevorratungsbefugnis geboten, die das Gesetz nicht vorsieht.

Erstens steht die Datenbevorratung ohne einzelfallbezogene Erforderlichkeitsprüfung mit dem Verhältnismäßigkeitsgrundsatz nur in Einklang, wenn die Straftat, welche die betroffene Person begangen hat, hinreichend schwer wiegt,

> vgl. zur Bedeutung dieses Gesichtspunkts EGMR (5. Sektion), Urteil vom 22. Juni 2017, No. 8806/12 (Aycaguer/Frankreich), Rn. 43.

Zumindest eine Bevorratung von Angaben über Bagatelldelikte muss hingegen voraussetzen, dass es hierfür im Einzelfall einen hinreichenden Anlass gibt, etwa weil aufgrund konkreter Tatsachen mit weiteren Straftaten der betroffenen Person zu rechnen ist. Hingegen ermöglicht § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG die Bevorratung von Basisdaten über jegliche Straftaten, soweit die Zentralstellenaufgabe des BKA eröffnet ist. Dies ist gemäß § 2 Abs. 1 BKAG unter anderem der Fall, wenn eine Straftat eine länderübergreifende Bedeutung hat, ohne dass es auf das Gewicht der Tat ankäme. Das aus § 30 BKAG folgende Erfordernis einer Verbundrelevanz ändert hieran nichts. Insoweit reicht die Bevorratungsermächtigung von vornherein zu weit.

Zweitens muss die Bevorratung in zeitlicher Hinsicht begrenzt werden, um die betroffene Person nicht langfristig oder sogar lebenslang an einem vergangenen Fehlverhalten festzuhalten.

Das BKAG sieht eine feste zeitliche Grenze weder für die Datenbevorratung noch für die Nutzung der bevorrateten Daten vor. Stattdessen verpflichtet § 75 Abs. 2 BDSG das BKA, bevorratete Daten zu löschen, wenn deren Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Diese Vorgabe wird durch eine Verpflichtung zur Festsetzung von Prüffristen flankiert, die sich aus § 75 Abs. 4 BDSG i.V.m. § 77 Abs. 1 BKAG ergibt.

Die Verknüpfung einer erforderlichkeitsabhängigen materiellen Löschungspflicht mit einer prozeduralen Prüfpflicht steht im Allgemeinen mit den Grundrechten in Einklang. Denn sie gewährleistet grundsätzlich, dass der Datenbestand des BKA dauerhaft dem datenschutzrechtlichen Erforderlichkeitsgebot genügt,

> vgl. EGMR (5. Sektion), Entscheidung vom 4. Juni 2013, No. 7841/08 and 57900/12 (Peruzzo und Martens/Deutschland), Rn. 46.

Defizitär ist dieser Regelungsansatz hingegen, wenn die materielle Löschungspflicht wegen einer gesetzlichen Erforderlichkeitsanordnung weitgehend leerläuft. Die Prüfung, ob eine Datenlöschung geboten ist, weil die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist, beinhaltet eine Erforderlichkeitsprüfung, die auf die Ermächtigung zur Datenbevorratung zu beziehen ist. Liegen die Voraussetzungen der

Datenbevorratung weiterhin vor, so werden zumindest in aller Regel die bevorrateten Daten weiterhin benötigt und dürfen darum behalten werden. Indem der Gesetzgeber abstrakt-generell angeordnet hat, dass bestimmte Basisdaten verurteilter Straftäter für die Aufgabenerfüllung des BKA erforderlich sind, hat er mithin auch die spätere Überprüfung der Datenbevorratung präformiert. Lediglich in atypischen Fällen, wenn positiv festzustellen ist, dass Daten über die betroffene Person zukünftig nicht mehr benötigt werden können (etwa wegen des Todes oder einer zwischenzeitlich eingetretenen schweren Gebrechlichkeit der betroffenen Person), fällt die Ermessensprüfung negativ aus und sind die Daten zu löschen.

Im Zusammenwirken von § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG und § 75 Abs. 2, Abs. 4 BDSG i.V.m. § 77 Abs. 1 BKAG ermöglicht das Gesetz dem BKA somit eine weitgehend routinemäßige Weiterbevorratung. Dies ist grundrechtlich nicht hinnehmbar. Die gesetzliche Erforderlichkeitsanordnung müsste vielmehr durch eine angemessene gesetzliche Frist flankiert werden, nach deren Ablauf die bevorrateten Daten zu löschen sind, wenn nicht eine einzelfallbezogene prognostische Erforderlichkeitsprüfung ausnahmsweise ergibt, dass sie weiterhin benötigt werden.

bb) Erforderlichkeitsvermutung: § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1, Abs. 5 BKAG

Noch weitergehenden Bedenken unterliegt die Bevorratungsermächtigung in § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG. Diese Regelungen erlauben dem BKA und den am Informationsverbund teilnehmenden Behörden wiederum ohne weitere Voraussetzungen, bestimmte Basisdaten über Beschuldigte zu bevorraten. Ähnlich wie bei § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG geht das Gesetz also davon aus, dass sich schon aus der Stellung der betroffenen Person als Beschuldigte in einem Strafverfahren ein hinreichender Bevorratungsanlass ergibt.

Diese Bevorratungsermächtigung ist noch problematischer als die Ermächtigung zur Bevorratung von Basisdaten über Verurteilte, weil es hier an einem gerichtlich festgestellten Ereignis als Bevorratungsanlass fehlt, das der betroffenen Person zurechenbar ist und darum die Bevorratung für sie zumutbar macht. Vielmehr ist für die Bevorratung weitgehend irrelevant, ob die betroffene Person zu Recht beschuldigt wurde. Nicht einmal ein positiv festzustellender kriminalistischer Restverdacht wird gefordert, um die Bevorratung zu legitimieren. Stattdessen ist umgekehrt die (weitere) Bevorratung nach § 18 Abs. 5 BKAG nur dann unzulässig, wenn das Strafverfahren gegen die betroffene Person mit einer Entscheidung geendet

hat, aus der sich positiv ergibt, dass sie die Tat nicht oder nicht rechtswidrig begangen hat,

> vgl. zum gleichlautenden § 8 Abs. 3 BKAG a.F. 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.

Hiermit wird auf einen Entscheidungsinhalt abgestellt, der dem Strafverfahren tendenziell systemfremd ist. Für eine Verfahrenseinstellung oder einen Freispruch reicht aus, dass sich die Täterschaft des Beschuldigten oder Angeklagten nicht mit hinreichender Wahrscheinlichkeit belegen lässt. Hingegen ist es nicht Aufgabe des Strafverfahrens, die Unschuld einer Person zu erweisen. Aus strafprozessualer Sicht ist es darum eher ein Zufallsergebnis und nicht Verfahrensziel, wenn die Ermittlungen die Täterschaft eines Beschuldigten positiv widerlegen. Selbst wenn kein signifikanter Restverdacht gegen den Beschuldigten besteht, wird sich in der Folge aus der verfahrensabschließenden Entscheidung nicht immer ergeben, dass er die Tat nicht oder nicht rechtswidrig begangen hat. Der Beschuldigte hat auch keine prozessuale Möglichkeit, eine solche Feststellung zu erwirken, da er durch Verfahrenseinstellung oder Freispruch nicht beschwert ist. Eine Grenze der Bevorratungsbefugnis ergibt sich damit in der Regel lediglich aus einer normativ nicht weiter angeleiteten Verhältnismäßigkeitsprüfung,

> ähnlich zu § 8 Abs. 3 BKAG a.F. Spiecker gen. Döhmann/Kehr, DVBl 2011, S. 930 (934 f.); Henseler, NWVBl 2015, S. 53 (60 f.); kritisch auch Eisenberg/Singelnstein, GA 2006, S. 168 (177 ff.); Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 18 BKAG Rn. 50 f.

Gegen die Angemessenheit der Bevorratungsermächtigung aus § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG, die für bestimmte Beschuldigtendaten eine sehr weitreichende Erforderlichkeitsvermutung errichtet, spricht daher neben den schon gegen § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG angeführten Gründen die strukturelle Ungewissheit über die Tatsachengrundlage und Berechtigung der Beschuldigung. Es bedarf darum noch weitergehender Vorkehrungen, damit diese Ermächtigung verfassungsrechtlich tragfähig wird.

Hierfür liegt es nahe, auf der nachgelagerten Ebene der Datennutzung anzusetzen. Hinnehmbar ist die pauschale Bevorratung von Beschuldigtendaten ohne positiv festzustellende Verdachtsmomente, wenn sie nur dazu dient, polizeiliche Kriminalakten zu erschließen, an deren Kenntnis ein hinreichendes einzelfallbezogenes Interesse besteht. So könnte

die Datennutzung an die Voraussetzung geknüpft werden, dass gegen die betroffene Person Verdachtsmomente bestehen, die es angezeigt erscheinen lassen, die über sie geführten Kriminalakten einzusehen. Nicht mehr hinnehmbar ist es hingegen, wenn die bevorrateten Daten auch genutzt werden dürfen, um einen personengerichteten Verdacht erst zu gewinnen, etwa im Rahmen einer Analyse von Tatzusammenhängen oder anlässlich eines Ereignisses wie einer Demonstration oder eines Fußballspiels. Im Kontext einer solchen Nutzung wird die gesetzliche Erforderlichkeits- zu einer Gefährlichkeitsvermutung über den früheren Beschuldigten auf potenziell sehr unsicherer Tatsachengrundlage, ohne dass die betroffene Person dem etwas entgegensetzen könnte.

cc) Unangeleitete Kriminalprognose: § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 1 und 3 BKAG

Verfassungswidrig ist schließlich die in § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 1 und 3 BKAG enthaltene weitreichende Ermächtigung zur Bevorratung von Daten über „Anlasspersonen“. Nach diesen Regelungen dürfen das BKA und die am Informationsverbund teilnehmenden Behörden sowohl Basisdaten als auch weitere Daten bevorraten, wenn sie aufgrund tatsächlicher Anhaltspunkte davon ausgehen, dass die betroffene Person in naher Zukunft Straftaten von erheblicher Bedeutung begehen wird. Welche weiteren personenbezogenen Daten bevorratet werden dürfen, lässt das Gesetz offen. Eine nähere Bestimmung ist der in § 20 BKAG vorgesehenen Rechtsverordnung vorbehalten. Unter Zugrundelegung der auf der Grundlage von § 7 Nr. 11 BKAG a.F. erlassenen BKADV könnte es sich dabei um sensible Daten wie etwa Angaben über Vermögensverhältnisse und Finanztransaktionen (§ 2 Abs. 1 Nr. 6-9 i.V.m. § 4 BKADV), soziale und institutionelle Beziehungen (§ 2 Abs. 1 Nr. 12-14 i.V.m. § 4 BKADV) oder Angaben zur Religionszugehörigkeit (§ 2 Abs. 1 Nr. 17 i.V.m. § 4 BKADV) handeln. Darüber hinaus können als weitere personenbezogene Daten auch Informationen bevorratet werden, die die bevorratende Behörde durch eingriffsintensive verdeckte Überwachungsmaßnahmen erlangt hat. Die vorgesehene Datenbevorratung kann daher nach Inhalt und Umfang erhebliches Gewicht aufweisen.

Der gesetzliche Bevorratungsanlass trägt der potenziell hohen Eingriffsintensität der geregelten Datenbevorratung nicht annähernd Rechnung. § 18 Abs. 1 Nr. 4 BKAG ermöglicht die Datenbevorratung auf der Grundlage einer Kriminalprognose, die das Gesetz nicht näher anleitet.

Hierin unterscheidet sich diese Regelung fundamental von § 18 Abs. 1 Nr. 1-3, Abs. 2 Nr. 2 und 3 BKAG. Diese Bevorratungsermächtigungen knüpfen,

zumindest soweit sie die Bevorratung weiterer personenbezogener Daten ermöglichen, zwar gleichfalls an Kriminalprognosen an. Grundlage dieser Kriminalprognosen sind jedoch entweder eine strafgerichtliche Verurteilung, durch die ein bestimmtes Handeln der betroffenen Person verbindlich festgestellt wurde, oder zumindest ein kriminalistischer Restverdacht gegen den einer Straftat Beschuldigten oder Verdächtigen. Der Bezug auf ein feststehendes oder wenigstens zu einem gewissen Grad wahrscheinliches vergangenes Verhalten der betroffenen Person verleiht der Kriminalprognose zumindest ansatzweise Konturen und begrenzt die Prognosebefugnis auf bestimmte Typen und Kontexte von Straftaten. Hierdurch wird das verbleibende – durchaus hohe – Prognoserisiko für die betroffene Person zumutbar.

Demgegenüber benennt § 18 Abs. 1 Nr. 4 BKAG für die Kriminalprognose keinerlei Anknüpfungspunkte. Die Norm errichtet weder spezifische Anforderungen an das Vorverhalten der betroffenen Person als Prognosegrundlage noch an die Wissensbestände, mit deren Hilfe auf die zukünftige Straftatbegehung geschlossen werden soll. Sie ermöglicht damit etwa Prognosen, die im Wesentlichen auf allgemeine Erfahrungssätze, auf zulässiges Verhalten oder auf von der betroffenen Person nicht zu verantwortende äußere Umstände gestützt werden. Beispielsweise kann es für eine Datenbevorratung ausreichen, dass eine Person in räumlichem und zeitlichem Zusammenhang mit einer Gewalttat bei einer Demonstration oder einem Fußballspiel angetroffen und deshalb gegen sie ein Platzverweis ausgesprochen wurde,

> vgl. zu § 8 Abs. 5 BKAG a.F. Arzt/Eier, DVBl 2010, S. 816 (818).

Eine so weitreichende Bevorratungsermächtigung verfehlt die grundrechtlichen Anforderungen deutlich,

> wie hier zu § 8 Abs. 5 BKAG a.F. Arzt/Eier, DVBl 2010, S. 816 (823); kritisch auch Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 18 BKAG Rn. 10 f.

b) Nutzungsermächtigung und hypothetische Datenneuerhebung

Darüber hinaus stehen § 18 Abs. 1 und Abs. 2 BKAG insgesamt mit den verfassungsrechtlichen Anforderungen nicht in Einklang, soweit sie das BKA zur Nutzung der bevorrateten Daten ermächtigen.

Die angegriffenen Regelungen sind als einheitliche Weiterverarbeitungsermächtigungen ausgestaltet, die dem BKA im Rahmen

seiner Zentralstellenaufgabe sowohl die Bevorratung bestimmter Daten als auch die spätere Nutzung der bevorrateten Daten erlauben. Die Nutzung ist damit nicht an eigenständige Voraussetzungen gebunden, der Tatbestand der Nutzungsermächtigung also immer erfüllt, wenn die Bevorratung zulässig war. Grenzen der Nutzungsbefugnis des BKA ergeben sich nur im Rahmen der normativ nicht näher angeleiteten Ermessensausübung.

Insbesondere ist die Nutzung der bevorrateten Daten auch dann, wenn diese durch eingriffsintensive verdeckte Überwachungsmaßnahmen gewonnen wurden, nicht von der Prüfung einer hypothetischen Datenneuerhebung abhängig. § 18 Abs. 1 und Abs. 2 BKAG enthalten keinen Verweis auf § 12 BKAG. Ein solcher Verweis lässt sich auch nicht der allgemeinen Regelung des § 16 Abs. 1 BKAG entnehmen. Zwar könnte diese Vorschrift nach ihrem Wortlaut so interpretiert werden, dass sie auch im Rahmen des § 18 BKAG anzuwenden ist, da sie nur insoweit zurücktritt, als „dieses Gesetz… zusätzliche besondere Voraussetzungen vorsieht“. Man könnte § 18 BKAG als Regelung solcher „zusätzlicher“ Voraussetzungen ansehen, welche die Voraussetzungen des § 16 Abs. 1 BKAG ergänzt, aber nicht verdrängt. Hiergegen sprechen jedoch zwei Erwägungen:

Erstens geht die Gesetzesbegründung erkennbar davon aus, dass § 16 Abs. 1 BKAG nicht tatbestandsergänzend zu § 18 BKAG hinzutritt. Zu § 16 Abs. 1 BKAG heißt es dort – im Widerspruch zum Normwortlaut –, „dass speziellere Weiterverarbeitungsbefugnisse der Norm vorgehen“,

BT-Drs. 18/11163, S. 94.

In den Ausführungen der Gesetzesbegründung zu § 18 und § 19 BKAG werden § 12 und § 16 BKAG folgerichtig nicht erwähnt,

vgl. BT-Drs. 18/11163, S. 95 ff.

Zweitens – und vor allem – würde eine Anwendung von § 16 Abs. 1 i.V.m. § 12 BKAG auf die Weiterverarbeitungsermächtigungen des § 18 BKAG zu dysfunktionalen, vom Gesetzgeber offenkundig nicht intendierten Ergebnissen führen. Da § 18 BKAG sämtliche Weiterverarbeitungsschritte einheitlich reguliert, müsste zwingend neben der Datennutzung auch die vorgelagerte Datenbevorratung den Anforderungen von § 16 Abs. 1 i.V.m. § 12 BKAG genügen. Eine unterschiedliche Behandlung beider Verarbeitungsschritte ist im Gesetz gerade nicht angelegt. Jedoch stellt eine Datenbevorratung im Rahmen der Zentralstellenaufgabe des BKA fast immer eine Zweckänderung dar, da die Daten aus dem ursprünglichen Verfahrenszusammenhang in einen verfahrensexternen und aufgabenübergreifenden Datenbestand überführt

werden, der sowohl für Zwecke der Gefahrenabwehr als auch der Strafverfolgung offensteht. Wären bereits auf die Bevorratung § 16 Abs. 1 i.V.m. § 12 BKAG anzuwenden, so müsste in diesem Zeitpunkt ein konkreter Ermittlungsansatz vorliegen. Damit wäre der Sinn des polizeilichen Informationsverbunds, der Informationen gerade für noch nicht konkret absehbare zukünftige Verfahren bereithalten soll, zunichte gemacht.

Es ist verfassungsrechtlich nicht zu beanstanden, dass § 18 Abs. 1 und Abs. 2 BKAG die Datenbevorratung nicht von der Prüfung einer hypothetischen Datenneuerhebung abhängig macht. Indem die Norm jedoch Datenbevorratung und Datennutzung gemeinsam reguliert, stellt sie auch die Datennutzung von diesem Erfordernis frei. Hierfür gibt es keinen rechtfertigenden Grund. Insbesondere können die Weiterverarbeitungstatbestände in § 18 Abs. 1 und Abs. 2 BKAG dieses Defizit nicht kompensieren. Weder gewährleisten sie, dass die Datennutzung durchweg dem Schutz eines hinreichend gewichtigen Rechtsguts oder der Verfolgung einer hinreichend schwerwiegenden Straftat dient, noch stellen sie in jedem Fall sicher, dass der Datennutzung ein konkreter Ermittlungsansatz zugrunde liegt.

c) Fehlen einer Benachrichtigungspflicht

Verfassungsrechtlich unzureichend sind auch die gesetzlichen Vorgaben zur Gewährleistung der Transparenz der aufgrund von § 18 Abs. 1 und Abs. 2 (auch in Verbindung mit § 29 Abs. 4 Satz 2) BKAG angelegten Datensammlung,

vgl. BVerfGE 133, 277 (365 ff.).

Zu beanstanden ist insbesondere, dass weder das BKAG noch das BDSG eine Pflicht des BKA oder der anderen Verbundteilnehmer begründen, eine betroffene Person über die Bevorratung von auf sie bezogenen Daten zu benachrichtigen. Die betroffene Person kann eine (partielle) Transparenz der beim BKA über sie vorhandenen Datenbestände daher nur erlangen, indem sie selbst aktiv wird und von ihrem Auskunftsrecht aus § 57 BDSG Gebrauch macht. Das Auskunftsrecht allein gewährleistet jedoch aus zwei Gründen nicht durchweg ein verfassungsrechtlich hinreichendes Transparenzniveau und muss darum durch eine Benachrichtigungspflicht flankiert werden.

Erstens können Datenbevorratungen gemäß § 18 Abs. 1, Abs. 2 BKAG in der Folge von verdeckten Überwachungsmaßnahmen erfolgen, von denen die betroffene Person erst nach geraumer Zeit oder sogar überhaupt nicht erfährt. Insbesondere gilt dies für Datenbevorratungen über Verdächtige und

Anlasspersonen, denen gegenüber auch das Strafprozessrecht keine Verfahrenstransparenz durch eine Vernehmungspflicht gewährleistet. In einem solchen Fall hat die betroffene Person keinen Anlass, von ihrem Auskunftsrecht Gebrauch zu machen, so dass dieses Recht leerläuft.

Zweitens ist selbst dann, wenn aus Sicht der betroffenen Person Anhaltspunkte für eine Datenbevorratung bestehen, für die betroffene Person nicht durchweg abschätzbar, gegenüber welcher Behörde sie ihr Auskunftsrecht geltend machen sollte. Insbesondere ist es für Außenstehende nicht immer ersichtlich, ob bestimmte Daten (allein) in einer landespolizeilichen Datensammlung oder (auch) im polizeilichen Informationsverbund des BKA bevorratet werden. Ein Auskunftsbegehren gegenüber dem BKA schafft in einem solchen Fall keine Transparenz über den landespolizeilichen Datenbestand. Ein Auskunftsbegehren gegenüber der Landespolizeibehörde schafft zumindest nicht stets Transparenz über den Bestand des BKA, da zum einen die angefragte Landesbehörde gemäß § 84 Abs. 1 Satz 2 BKAG auf eine zusätzliche eigene Bevorratung im Informationsverbund des BKA hinweisen kann, aber nicht muss, und da zum anderen ein Auskunftsbegehren gegenüber einer Landespolizeibehörde generell keine Transparenz hinsichtlich von Speicherungen im Informationsverbund durch das BKA oder durch andere Landespolizeibehörden erbringt.

Für das vollständige Fehlen einer Benachrichtigungspflicht ist kein rechtfertigender Grund ersichtlich. Zwar hat das angerufene Gericht das Fehlen einer solchen Pflicht in Bezug auf die Antiterrordatei gebilligt. Es hat hierzu jedoch auf die Zwecksetzung dieser Datei verwiesen, Ermittlungen im Bereich des internationalen Terrorismus zu unterstützen, die grundsätzlich nicht offen erfolgen könnten,

BVerfGE 133, 277 (369).

Diese Begründung lässt sich auf den polizeilichen Informationsverbund bei dem BKA nicht generell übertragen. Der Informationsverbund dient der Unterstützung der polizeilichen Aufgabenerfüllung auch auf Kriminalitätsfeldern, die – wie etwa die Verhütung und Verfolgung von Straftaten bei Großveranstaltungen – nicht generell ein verdecktes Vorgehen der Polizei erfordern. Datenbevorratungen im Zusammenhang mit solchen Kriminalitätsfeldern können den betroffenen Personen vorbehaltlich besonderer Umstände im Einzelfall durchaus mitgeteilt werden, ohne die polizeiliche Aufgabenerfüllung übermäßig zu beeinträchtigen.

4. Hinzuspeicherung ermittlungsunterstützender Hinweise

Schließlich verfehlt auch die in § 16 Abs. 6 Nr. 2 BKAG enthaltene Ermächtigung zur Hinzuspeicherung sogenannter ermittlungsunterstützender Hinweise die verfassungsrechtlichen Anforderungen. Diese Norm erlaubt dem BKA und den anderen Verbundteilnehmern, bereits vorhandene bevorratete Daten über eine Person durch Hinweise zu ergänzen, „die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen."

Diese Formulierung ist sehr offen gefasst und reicht darum potenziell sehr weit. Je nach Kriminalitätsfeld und (mutmaßlicher) Verstrickung der betroffenen Person können auch höchstpersönliche oder stigmatisierende Angaben den Schutz Dritter oder die Gewinnung von Ermittlungsansätzen erleichtern. Ermittlungsunterstützende Hinweise können daher sensible Informationen zum Gegenstand haben, deren Bevorratung das Persönlichkeitsrecht der betroffenen Person in erheblichem Ausmaß beeinträchtigen und die das Verhalten der Polizei ihr gegenüber maßgeblich beeinflussen können. So nennt zum früheren Recht § 2 Abs. 1 Nr. 16 BKADV beispielhaft für solche Hinweise die Angaben „Sexualstraftäter", „Straftäter politisch links motiviert" oder „Straftäter politisch rechts motiviert". Auch etwa Angaben zur Obdachlosigkeit einer Person oder zu ihrer mutmaßlichen Tätigkeit als Prostituierte ließen sich durchaus unter § 16 Abs. 6 Nr. 2 BKAG subsumieren. Die Vorschrift schließt es nicht einmal aus, diskriminierende Hinweise etwa zur Religionszugehörigkeit oder zum ethnischen Hintergrund zu speichern.

Wegen der potenziell erheblichen Eingriffsintensität der Hinzuspeicherung ermittlungsunterstützender Hinweise muss diese an eine hinreichend restriktive Eingriffsschwelle gebunden werden. § 16 Abs. 6 Nr. 2 BKAG leistet dies nicht ansatzweise. Insbesondere schlägt sich die in der Gesetzesbegründung enthaltene Maßgabe, ermittlungsunterstützende Hinweise müssten

> „auf der Grundlage von objektiven Erkenntnissen und von möglichst umfassenden Informationen zur betreffenden Person gewonnen werden",
>
> BT-Drs. 18/11163, S. 95,

im Wortlaut der Norm nicht nieder. Diese Regelung stellt vielmehr die Bevorratung und die spätere Nutzung solcher Wertungen ohne konkrete Voraussetzungen ins Belieben des jeweiligen Sachbearbeiters,

vgl. zu der teils erheblich defizitären Handhabung in der Praxis etwa https://amp.zdf.de/nachrichten/heute/sicherheitsdateien-des-bundes-bundesdatenschuetzer-kelber-will-aufraeumen-100.html (letzter Abruf am 21. Mai 2019).

Das verfassungsrechtliche Defizit von § 16 Abs. 6 Nr. 2 BKAG verschärft sich noch dadurch, dass die Norm die Bevorratung und Nutzung ermittlungsunterstützender Hinweise zu allen Personen erlaubt, zu denen bereits Daten vorhanden sind. Dies schließt Verurteilte und Beschuldigte ein, deren Basisdaten gemäß § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG ohne weitere Voraussetzungen gespeichert werden können. Damit ermöglicht das Gesetz, ohne jeglichen konkreten Anlass über diese Personen potenziell sehr sensible Daten zu bevorraten. Jedenfalls insoweit ist die Bevorratungsermächtigung grundrechtlich nicht haltbar.

(Prof. Dr. Bäcker, LL.M.)

Anlagen:

1. Verfahrensvollmachten
2. Auskunft des Kriminalfachdezernats 10 der Münchner Polizei vom 11. Mai 2017
3. Schreiben des Bundespolizeipräsidiums vom 30. Januar 2019
4. Erkenntnismitteilung des Bayerischen Landesamts für Verfassungsschutz vom 27. Oktober 2016
5. Urteil des Verwaltungsgerichts Köln vom 26. April 2012 – 13 K 3980/11