Leitsätze

zum Urteil des Ersten Senats vom 1. Oktober 2024

- 1 BvR 1160/19 -

Bundeskriminalamtgesetz II

1. Voraussetzung einer heimlichen Überwachung von Kontaktpersonen mit eingriffsintensiven Maßnahmen zum Zweck der Datenerhebung ist jedenfalls, dass eine Überwachung der polizeirechtlich verantwortlichen Person mit entsprechenden Mitteln zulässig wäre.

2. Im Rahmen einer zweckwahrenden Verarbeitung zuvor erhobener personenbezogener Daten sind diese grundsätzlich zu löschen, nachdem der unmittelbare Anlassfall abgeschlossen und damit der der Erhebungsmaßnahme zugrundeliegende konkrete Zweck erfüllt ist. Ein Absehen von einer Löschung über den unmittelbaren Anlassfall hinaus kommt in Betracht, soweit sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – zwischenzeitlich ein konkreter Ermittlungsansatz ergeben hat und damit die Voraussetzungen einer zweckändernden Nutzung vorliegen.

3. Eine vorsorgende Speicherung personenbezogener Grunddaten zur Identifizierung und zu einem bestimmten strafrechtlich relevanten Verhalten von Beschuldigten durch das Bundeskriminalamt auf einer föderalen polizeilichen Datenplattform erfordert jedenfalls die Festlegung angemessener Speicherschwellen sowie die Bestimmung einer angemessenen Speicherdauer:

   a) Die vorsorgende Speicherung muss auf einer Speicherschwelle beruhen, die den Zusammenhang zwischen den vorsorgend gespeicherten personenbezogenen Daten und der Erfüllung des Speicherzwecks in verhältnismäßiger Weise absichert und den spezifischen Gefahren der vorsorgenden Speicherung angemessen begegnet. Dies ist bei der Speicherung von Daten für die Verhütung und Verfolgung von Straftaten nur gegeben, wenn eine hinreichende Wahrscheinlichkeit dafür besteht, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen werden und gerade die gespeicherten Daten zu deren Verhütung und Verfolgung angemessen beitragen können. Diese Prognose muss sich auf zureichende tatsächliche Anhaltspunkte stützen.

   b) Es bedarf der gesetzlichen Regelung einer angemessenen Speicherdauer. Diese wird insbesondere geprägt durch das Eingriffsgewicht, die Belastbarkeit der Prognose

in der Zeit sowie durch andere sich aus dem Grundsatz der Verhältnismäßigkeit ergebende Gesichtspunkte. Die Prognose verliert ohne Hinzutreten neuer relevanter Umstände grundsätzlich an Überzeugungskraft über die Zeit.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 1160/19 -

Verkündet
am 1. Oktober 2024
Uhr
Amtsinspektorin
als Urkundsbeamtin
der Geschäftsstelle

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerde

1. der Frau (...),

2. der Frau (...),

3. der Frau (...),

4. des Herrn (...),

5. des Herrn (...),

- Bevollmächtigte:
  1. Prof. Dr. Matthias Bäcker, LL.M.,
     (...),
  2. Rechtsanwalt Dr. Bijan Moini,
     (...),
     (zu 2., 3.) -

gegen § 16 Absatz 1 in Verbindung mit § 12 Absatz 1 Satz 1, § 16 Absatz 6 Nummer 2 auch in Verbindung mit § 29 Absatz 4 Satz 2, § 18 Absatz 1, 2 und 5 in Verbindung mit § 13 Absatz 3, § 29, § 45 Absatz 1 Satz 1 Nummer 4, § 49, § 51 Absatz 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 (Bundesgesetzblatt I Seite 1354)

hat das Bundesverfassungsgericht - Erster Senat -

unter Mitwirkung der Richterinnen und Richter

Präsident Harbarth,

Ott,

Christ,

Radtke,

Härtel,

Wolff,

Eifert,

Meßling

aufgrund der mündlichen Verhandlung vom 20. Dezember 2023 durch

U r t e i l

für Recht erkannt:

1. § 18 Absatz 1 Nummer 2 in Verbindung mit § 18 Absatz 2 Nummer 1, soweit dieser in Verbindung mit § 13 Absatz 3, § 29 die Speicherung von Daten durch das Bundeskriminalamt in seiner Funktion als Zentralstelle erlaubt sowie § 45 Absatz 1 Satz 1 Nummer 4 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 (Bundesgesetzblatt I Seite 1354) sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes nicht vereinbar.

2. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Juli 2025, gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften nach Maßgabe der Gründe zu D II 2 b fort.

3. Soweit sich die Beschwerdeführerinnen zu 1) und 2) gegen § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG gewandt haben, wird die Verfassungsbeschwerde zurückgewiesen. Im Übrigen wird die Verfassungsbeschwerde verworfen.

4. Die Bundesrepublik Deutschland hat den Beschwerdeführenden ein Drittel ihrer notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

Gründe:

A.

Die Beschwerdeführenden wenden sich mit ihrer Verfassungsbeschwerde gegen Regelungen des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz, im Folgenden: BKAG) in der Fassung des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl I S. 1354), die zum 25. Mai 2018 in Kraft getreten sind (BGBl I S. 1354). Angegriffen ist zum einen die Ermächtigung des Bundeskriminalamts zum Einsatz besonderer Mittel der Datenerhebung zur Abwehr von Gefahren des internationalen Terrorismus, soweit diese eine Überwachung von Kontaktpersonen erlaubt (§ 45 Abs. 1 Satz 1 Nr. 4 i.V.m. § 39 Abs. 2 Nr. 2 BKAG). Zum anderen rügen die Beschwerdeführenden Regelungen zur Weiterverarbeitung bereits erhobener personenbezogener Daten im Informationssystem des Bundeskriminalamts und im polizeilichen Informationsverbund (§ 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG; § 18 Abs. 1 Nr. 1, 2 und 4, Abs. 2 Nr. 1 und 3 und Abs. 5 i.V.m. § 13 Abs. 3, § 29 BKAG) sowie zu polizeilichen Hinweisen (§ 16 Abs. 6 Nr. 2 auch i.V.m. § 29 Abs. 4 Satz 2 BKAG). 1

I.

Mit dem Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 beabsichtigte der Bundesgesetzgeber insbesondere die Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220) und die der Richtlinie (EU) 2016/680 vom 27. April 2016 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl EU, L 119 vom 4. Mai 2016, S. 89-131; JI-Richtlinie; im Folgenden: JI-RL; vgl. BTDrucks 18/11163, S. 1). Im Zuge dieser Reform sollte unter anderem die IT-Architektur des Bundeskriminalamts neu strukturiert werden, um so die Effizienz und Effektivität der kriminalpolizeilichen Arbeit zu verbessern. In Reaktion auf die Erfahrungen aus der Aufklärung der NSU-Mordserie im November 2011 wurde gefordert, dass die informationstechnischen Grundlagen für die notwendige Vernetzung aller an einer Ermittlung beteiligten Dienststellen jederzeit sofort verfügbar sein müssten. Es dürfe nicht nochmals vorkommen, dass Zeit und Kraft dafür verloren gingen, unterschiedliche Systeme während einer laufenden Ermittlung zu verknüpfen. Zugleich sollte den Datenschutzanforderungen Rechnung getragen werden (vgl. BTDrucks 18/11163, S. 76). 2

Die neuen Regelungen im Bundeskriminalamtgesetz zur Einrichtung einer föderalen Datenplattform („polizeilicher Informationsverbund“) stehen im Zusammenhang mit der für notwendig erachteten digitalen Transformation der Polizei. So verständigten sich im 3

November 2016 die Innenminister des Bundes und der Länder auf die „Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit“. Zur Umsetzung dieser Agenda stellte der Bund das Programm Polizei 2020 auf (vgl. Bundesministerium des Innern, Polizei 2020 - White Paper -, 2018). Auf seiner Grundlage trafen Bund und Länder im Dezember 2019 die „Verwaltungsvereinbarung über die Errichtung eines Polizei-IT-Fonds und über die Grundlagen der Zusammenarbeit bei der Modernisierung des polizeilichen Informationswesens von Bund und Ländern – Vereinbarung zur Ausführung von Artikel 91c Absatz 1 und Absatz 2 Satz 1 und Satz 4 GG“. Alleinige Regelungsgegenstände sind die Einrichtung eines Polizei-IT-Fonds zur Finanzierung und die Entscheidungsstrukturen bei der Zusammenarbeit bei der Modernisierung des polizeilichen Informationswesens.

In der föderalen Informationsordnung der Polizei gab es auch schon zuvor eine IT-Verbundarchitektur. Vorgänger des neuen „polizeilichen Informationsverbunds“ ist das bestehende Informationssystem Polizei (INPOL), das solange weiterbetrieben und gepflegt werden soll, bis die phasenweise Übernahme durch die neuen Komponenten sichergestellt ist (vgl. Bundesministerium des Innern, Polizei 2020 - White Paper -, 2018, S. 16). INPOL ist ein Verbundsystem, das von den Polizeien der Länder und des Bundes gemeinsam genutzt wird. Es enthält die Datenbanken für die polizeiliche Fahndung sowie allgemeine Auskunftszwecke (INPOL-Z). Zudem werden auch verbundrelevante Daten aus den Fallbearbeitungssystemen zur Analyse komplexer Sachverhalte gespeichert (INPOL-Fall). Dabei werden die Daten in verschiedenen Dateien gespeichert (vgl. § 9 der Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen <BKA-Daten-Verordnung – BKADV> vom 4. Juni 2010 <BGBl I S. 716>, die zuletzt durch Art. 6 Abs. 12 des Gesetzes zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 <BGBl I S. 872> geändert worden ist), so unter anderem in Delikts- und phänomenbezogene Dateien, in Kriminalaktennachweisen, in Gewalttäterdateien und erkennungsdienstlichen Dateien sowie in der DNA-Analyse-Datei und der Haftdatei. Das alte System der Dateien hat allerdings zur Folge, dass eine Person je nach Ermittlungskontext in mehreren Datenbanken gespeichert sein kann. Mangels übergreifender Verknüpfung zwischen den unterschiedlichen Datenbanken können eine Verbindung zwischen den Daten oder Abweichungen (etwa Eingabefehler) nicht systemunterstützt festgestellt werden (vgl. Bundesministerium des Innern, Polizei 2020 - White Paper -, 2018, S. 5). Deswegen ist mit der Gesetzesreform die Vorgabe zur Gliederung des Datenbestands des Bundeskriminalamts in Dateien aufgegeben worden (vgl. BTDrucks 18/11163, S. 2 und 75 f.). An deren Stelle soll als Ausdruck des kooperativen Föderalismus ein polizeilicher Informationsverbund zwischen den Polizeibehörden von Bund und Ländern treten, dem technisch ein einheitliches Verbundsystem des Bundeskriminalamts und ein System differenzierter Kennzeichnungen der Daten zugrunde liegt. Innerhalb dieses Verbundsystems stellen die daran teilnehmenden Behörden einander Daten zur Verfügung. 4

Das Bundeskriminalamt unterhält zudem für seine eigenen Informationsbestände ein Informationssystem, mit dem es zugleich – soweit vorgesehen – an dem polizeilichen Informationsverbund teilnimmt. Dementsprechend hat der Gesetzgeber die zuvor verstreut geregelten Datenverarbeitungsbefugnisse neu geordnet und zentral normiert. Dabei hat er sich für einen einheitlichen Begriff der Weiterverarbeitung entschieden, an den die Ermächtigungen anknüpfen (vgl. unten Rn. 120). 5

II.

Die für das Verfahren relevanten Normen haben in den hier maßgeblichen Fassungen folgenden Inhalt und Wortlaut: 6

1. § 45 BKAG regelt die besonderen Datenerhebungsbefugnisse des Bundeskriminalamts unter anderem zur Abwehr von Gefahren des internationalen Terrorismus. Die Vorschrift erlaubt dem Bundeskriminalamt zur Erhebung personenbezogener Daten den Einsatz besonderer in Absatz 2 aufgeführter Mittel, so zum Beispiel die längerfristige Observation und den Einsatz von Vertrauenspersonen und von verdeckt Ermittelnden. Der allein angegriffene § 45 Abs. 1 Satz 1 Nr. 4 BKAG ermächtigt dazu, personenbezogene Daten mit diesen besonderen Mitteln bei Kontaktpersonen nach § 39 Abs. 2 Nr. 2 BKAG zu erheben. § 45 Abs. 3 BKAG ordnet dabei für den überwiegenden Teil der Maßnahmen einen Richtervorbehalt an. Nach § 45 Abs. 1 Satz 2 BKAG darf eine Maßnahme auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. 7

§ 45 BKAG hat auszugsweise folgenden Wortlaut: 8

§ 45 BKAG - Besondere Mittel der Datenerhebung

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

1. den entsprechend § 17 oder § 18 des Bundespolizeigesetzes Verantwortlichen oder entsprechend den Voraussetzungen des § 20 Absatz 1 des Bundespolizeigesetzes über die dort bezeichnete Person zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,
2. eine Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird,
3. eine Person, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird, oder
4. eine Person nach § 39 Absatz 2 Nummer 2,

wenn die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. [2]Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besondere Mittel der Datenerhebung sind

1. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden dauern oder an mehr als zwei Tagen stattfinden soll (längerfristige Observation),
2. der Einsatz technischer Mittel außerhalb von Wohnungen in einer für die betroffene Person nicht erkennbaren Weise
   a) zur Anfertigung von Bildaufnahmen oder -aufzeichnungen von Personen oder Sachen, die sich außerhalb von Wohnungen befinden, oder
   b) zum Abhören oder Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes,
3. sonstige besondere für Observationszwecke bestimmte technische Mittel zur Erforschung des Sachverhalts oder zur Bestimmung des Aufenthaltsortes einer in Absatz 1 genannten Person,
4. der Einsatz von Privatpersonen, deren Zusammenarbeit mit dem Bundeskriminalamt Dritten nicht bekannt ist (Vertrauensperson), und
5. der Einsatz einer Polizeivollzugsbeamtin oder eines Polizeivollzugsbeamten unter einer ihr oder ihm verliehenen und auf Dauer angelegten Legende (Verdeckter Ermittler).

(3) [1]Maßnahmen nach
1. Absatz 2 Nummer 1,
2. Absatz 2 Nummer 2 Buchstabe a, bei denen durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen,
3. Absatz 2 Nummer 2 Buchstabe b,
4. Absatz 2 Nummer 3, bei denen für Observationszwecke bestimmte technische Mittel durchgehend länger als 24 Stunden oder an mehr als zwei Tagen zum Einsatz kommen und
5. Absatz 2 Nummer 4 und 5, die sich gegen eine bestimmte Person richten oder bei denen die Vertrauensperson oder der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist,

dürfen nur auf Antrag der zuständigen Abteilungsleitung oder deren Vertretung durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung einer Maßnahme nach Satz 1 durch die zuständige Abteilungsleitung oder deren Vertretung getroffen werden. [3]In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. [5]Die übrigen Maßnahmen nach Absatz 2 Nummer 1 bis 5 dürfen, außer bei Gefahr im Verzug, nur durch die zuständige Abteilungsleitung oder deren Vertretung angeordnet werden.

(4) bis (8) [...]

Der in Bezug genommene § 5 BKAG lautet auszugsweise wie folgt: 9

§ 5 BKAG - Abwehr von Gefahren des internationalen Terrorismus

(1) [1]Das Bundeskriminalamt kann die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus in Fällen wahrnehmen, in denen
1. eine länderübergreifende Gefahr vorliegt,
2. die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder
3. die oberste Landesbehörde um eine Übernahme ersucht.

[2]Gefahren des internationalen Terrorismus sind Gefahren der Verwirklichung von Straftaten, die in § 129a Absatz 1 und 2 des Strafgesetzbuchs bezeichnet und dazu bestimmt sind,

1. die Bevölkerung auf erhebliche Weise einzuschüchtern,
2. eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder
3. die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können. [3]Das Bundeskriminalamt kann in den in Satz 1 bezeichneten Fällen auch zur Verhütung von Straftaten nach Satz 2 tätig werden.
(2) [...]

Der weiter in Bezug genommene § 39 BKAG hat auszugsweise folgenden Wortlaut: 10

§ 39 BKAG - Erhebung personenbezogener Daten

(1) [...]
(2) Zur Verhütung von Straftaten nach § 5 Absatz 1 Satz 2 ist eine Erhebung personenbezogener Daten nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass
1. die Person eine Straftat nach § 5 Absatz 1 Satz 2 begehen will und die erhobenen Daten zur Verhütung dieser Straftat erforderlich sind oder
2. die Person mit einer Person nach Nummer 1 nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und
   a) von der Vorbereitung einer Straftat nach § 5 Absatz 1 Satz 2 Kenntnis hat,
   b) aus der Verwertung der Tat Vorteile ziehen könnte oder
   c) die Person nach Nummer 1 sich ihrer zur Begehung der Straftat bedienen könnte

und die Verhütung dieser Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre.
(3) [...]

2. § 16 Abs. 1 BKAG ermächtigt das Bundeskriminalamt zur internen Weiterverarbeitung 11
personenbezogener Daten in seinem eigenen Informationssystem, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und das Bundeskriminalamtgesetz keine zusätzlichen besonderen Voraussetzungen vorsieht. Die Verarbeitung geschieht nach Maßgabe des § 12 BKAG, der das Kriterium der hypothetischen Datenneuerhebung für die Weiterverarbeitung umsetzen soll, und zwar unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme (vgl. BTDrucks 18/11163, S. 92).

Aus dem weiten tatbestandlichen Anwendungsbereich des § 16 Abs. 1 BKAG ist vorliegend 12
nur ein spezifischer Fall verfahrensgegenständlich. Die Beschwerdeführerinnen zu 1) und 2) wenden sich allein gegen die Weiterverarbeitung von personenbezogenen Daten, die das Bundeskriminalamt im Rahmen der Abwehr von Gefahren des internationalen Terrorismus (vgl. § 5 BKAG) mit besonders eingriffsintensiven Mitteln erhoben hat, und wenn die Weiterverarbeitung nach Maßgabe des § 12 Abs. 1 Satz 1 BKAG zur Erfüllung derselben Aufgabe geschieht.

§ 16 BKAG hat auszugsweise folgenden Wortlaut: 13

§ 16 BKAG - Datenweiterverarbeitung im Informationssystem

(1) Das Bundeskriminalamt kann personenbezogene Daten nach Maßgabe des § 12 im Informationssystem weiterverarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht.
(2) bis (6) [...]

Der in Bezug genommene § 12 BKAG lautet auszugsweise wie folgt: 14

§ 12 BKAG - Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

(1) [1]Das Bundeskriminalamt kann personenbezogene Daten, die es selbst erhoben hat, weiterverarbeiten
1. zur Erfüllung derselben Aufgabe und
2. zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten.

[...]
(2) [1]Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn
1. mindestens
   a) vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder
   b) vergleichbar bedeutsame Rechtsgüter geschützt

   werden sollen und
2. sich im Einzelfall konkrete Ermittlungsansätze
   a) zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder
   b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

   [...]

(3) bis (5) [...]

3. § 18 BKAG ermächtigt das Bundeskriminalamt dazu, näher bezeichnete personenbezogene Daten bestimmter Personengruppen weiterzuverarbeiten. Anders als in § 16 Abs. 1 BKAG ist hier nicht nur die interne Weiterverarbeitung von Daten im eigenen Informationssystem erfasst, sondern auch die Weiterverarbeitung von Daten in der Zentralstellenfunktion des Bundeskriminalamts. 15

In Umsetzung des Art. 6 JI-RL unterscheidet der Gesetzgeber zwischen den Personenkategorien der Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen (vgl. BTDrucks 18/11163, S. 99, auch zur Vorgängervorschrift des § 8 Abs. 1 BKAG a.F., die nach altem Recht die zentrale Rechtsgrundlage für das Bundeskriminalamt als Zentralstelle bildete). Verfahrensgegenständlich sind vorliegend nur die Personengruppen der Verurteilten, Beschuldigten und sonstigen Anlasspersonen. 16

Als personenbezogene Daten können nach § 18 Abs. 2 Nr. 1 BKAG nur weiterverarbeitet werden: (a) die Grunddaten und (b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale, (c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer, (d) die Tatzeiten und Tatorte und (e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten. Der ebenfalls angegriffene § 18 Abs. 2 Nr. 3 BKAG erlaubt die Weiterverarbeitung weiterer personenbezogener Daten unter anderem zu sonstigen Anlasspersonen. Nach § 20 Satz 1 BKAG soll durch Rechtsverordnung das Nähere über die Art und den Umfang der Daten bestimmt werden, die insbesondere nach § 18 BKAG weiterverarbeitet werden dürfen. 17

§ 18 Abs. 1 BKAG erlaubt die Weiterverarbeitung dieser spezifischen personenbezogenen Daten durch das Bundeskriminalamt nur zur Erfüllung seiner Aufgaben nach § 2 Absätze 1 bis 3 BKAG. Gemäß § 2 Abs. 1 BKAG unterstützt das Bundeskriminalamt zunächst als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. Es hat alle hierfür erforderlichen Informationen zu sammeln und auszuwerten (§ 2 Abs. 2 Nr. 1 BKAG) und die Strafverfolgungsbehörden des Bundes und der Länder unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten zu unterrichten (§ 2 Abs. 2 Nr. 2 BKAG). Das Bundeskriminalamt unterhält überdies als Zentralstelle einen einheitlichen polizeilichen Informationsverbund nach Maßgabe des Bundeskriminalamtgesetzes (vgl. § 2 Abs. 3, § 29 Abs. 1 BKAG). Als Betreiber der föderalen Datenplattform stellt das Bundeskriminalamt die IT-Infrastruktur zur Verfügung, die auf einer einheitlichen Informationstechnik basiert (vgl. BTDrucks 18/11163, S. 81). Gleichzeitig gewährleistet es durch organisatorische und technische Maßnahmen, dass Eingaben von und Zugriffe auf Daten im polizeilichen Informationsverbund nur möglich sind, soweit die jeweiligen Behörden hierzu berechtigt sind (vgl. § 29 Abs. 4 Satz 1 BKAG). Die Berechtigung richtet sich nach den Zugriffsrechten (§ 15 BKAG) und setzt eine Kennzeichnung der weiterverarbeiteten Daten nach § 14 BKAG voraus. Das Bundeskriminalamt tritt nicht nur als Plattformbetreiber auf, sondern ist auch selbst zur Teilnahme am polizeilichen Informationsverbund berechtigt (vgl. § 29 Abs. 3 Satz 1 BKAG). Im Zuge dessen nimmt das Bundeskriminalamt mit seinem Informationssystem nach Maßgabe der §§ 29 und 30 BKAG am polizeilichen Informationsverbund nach § 29 BKAG teil (§ 13 Abs. 3 BKAG). Nach § 29 Abs. 4 Satz 2 BKAG gilt bei Eingaben von und Zugriffen auf Daten im polizeilichen Informationsverbund 18

für die teilnehmenden Behörden, die in § 29 Abs. 3 BKAG aufgezählt werden, unter anderem § 18 Absätze 1, 2, 4 und 5 BKAG entsprechend. § 31 Abs. 2 BKAG enthält Anforderungen zur datenschutzrechtlichen Verantwortung im polizeilichen Informationsverbund, während § 31 Abs. 3 BKAG die datenschutzrechtliche Kontrolle normiert. Zudem enthält der neunte Abschnitt des Bundeskriminalamtgesetzes (§§ 69 ff. BKAG) ergänzende Vorgaben zum Datenschutz und zur Datensicherheit.

§ 18 BKAG hat auszugsweise folgenden Wortlaut: 19

§ 18 BKAG - Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen

(1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Absatz 1 bis 3 personenbezogene Daten weiterverarbeiten von

1. Verurteilten,
2. Beschuldigten,
3. Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und
4. Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

(2) Das Bundeskriminalamt kann weiterverarbeiten:

1. von Personen nach Absatz 1 Nummer 1 bis 4
   a) die Grunddaten und
   b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
   c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,
   d) die Tatzeiten und Tatorte,
   e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten;
2. von Personen nach Absatz 1 Nummer 1 und 2 weitere personenbezogene Daten, soweit die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind;
3. von Personen nach Absatz 1 Nummer 3 und 4 weitere personenbezogene Daten.

(3) bis (4) [...]

(5) Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Weiterverarbeitung unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

Der in Bezug genommene § 2 BKAG lautet auszugsweise wie folgt: 20

§ 2 BKAG - Zentralstelle

(1) Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.
(2) Das Bundeskriminalamt hat zur Wahrnehmung dieser Aufgabe
1. alle hierfür erforderlichen Informationen zu sammeln und auszuwerten,
2. die Strafverfolgungsbehörden des Bundes und der Länder unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten zu unterrichten.

(3) Das Bundeskriminalamt unterhält als Zentralstelle einen einheitlichen polizeilichen Informationsverbund nach Maßgabe dieses Gesetzes.
(4) bis (7) [...]

Die für den polizeilichen Informationsverbund maßgeblichen Normen lauten auszugsweise: 21

§ 29 BKAG - Polizeilicher Informationsverbund, Verordnungsermächtigung

(1) bis (3) [...]
(4) [1]Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt sicherzustellen, dass Eingaben von und Zugriffe auf Daten im polizeilichen Informationsverbund nur möglich sind, soweit die jeweiligen Behörden hierzu berechtigt sind. [2]§ 12 Absatz 2 bis 5, die §§ 14, 15 und 16 Absatz 1, 2, 5 und 6, § 18 Absatz 1, 2, 4 und 5, § 19 Absatz 1 und 2 sowie die §§ 20 und 91 gelten entsprechend.
(5) bis (8) [...]

§ 30 BKAG - Verbundrelevanz

(1) Die am polizeilichen Informationsverbund teilnehmenden Stellen verarbeiten im polizeilichen Informationsverbund ausschließlich
1. personenbezogene Daten, deren Verarbeitung für die Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung erforderlich ist;
2. personenbezogene Daten, deren Verarbeitung im Informationsverbund erforderlich ist
   a) zu erkennungsdienstlichen Zwecken, soweit das Bundeskriminalamt diese Daten nach § 16 Absatz 5 auch im Informationssystem weiterverarbeiten dürfte oder
   b) zu Zwecken der Fahndung nach Personen und Sachen, soweit das Bundeskriminalamt diese Daten nach § 16 Absatz 2 auch im Informationssystem weiterverarbeiten dürfte

   (Verbundrelevanz).

(2) [...]

4. § 16 Abs. 6 Nr. 2 BKAG ermächtigt das Bundeskriminalamt zur Weiterverarbeitung näher bestimmter weiterer Hinweise zu Personen, zu denen bereits Daten vorhanden sind. Nach § 29 Abs. 4 Satz 2 BKAG (vgl. Rn. 21) gilt die Vorschrift entsprechend für die am polizeilichen Informationsverbund teilnehmenden Behörden bei Eingaben von und Zugriffen auf Daten. 22

§ 16 BKAG - Datenweiterverarbeitung im Informationssystem

(1) bis (5) [...]
(6) Das Bundeskriminalamt kann in den Fällen, in denen bereits Daten zu einer Person vorhanden sind, zu dieser Person auch weiterverarbeiten:
1. [...]
2. weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen.

5. Für die angegriffenen Befugnisse sind weiterhin übergreifende Anforderungen relevant. Pflichten in Bezug auf die Löschung der erhobenen Daten finden sich speziell für den Bereich der Terrorismusabwehr in § 79 Abs. 1 BKAG sowie allgemeiner in § 77 BKAG in Verbindung mit § 75 Abs. 2 BDSG. Nach § 79 Abs. 1 BKAG sind insbesondere die nach dem Abschnitt zur Terrorismusabwehr erlangten Daten unverzüglich zu löschen, wenn sie zur Erfüllung des der Maßnahme zugrunde liegenden Zwecks und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich sind. Eine Löschung unterbleibt, soweit eine „zulässige“ Weiterverarbeitung der Daten nach den Vorschriften des Abschnitts 2 Unterabschnitt 2, also insbesondere auch nach § 16 Abs. 1 und § 18 BKAG, erfolgt. § 77 Abs. 1 BKAG in Verbindung mit § 75 Abs. 2 BDSG enthält die allgemeineren Löschungsvorgaben und erstreckt sich damit auch auf die Befugnisse im Rahmen der Zentralstellenfunktion. Personenbezogene Daten sind insbesondere unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Löschungspflichten werden durch Aussonderungsprüffristen flankiert. 23

Die Löschungsvorschriften des Bundeskriminalamtgesetzes lauten auszugsweise wie folgt: 24

§ 77 BKAG - Aussonderungsprüffrist; Mitteilung von Löschungsverpflichtungen

(1) [1]Das Bundeskriminalamt prüft nach § 75 des Bundesdatenschutzgesetzes bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. [2]Die Aussonderungsprüffristen nach § 75 Absatz 4 des Bundesdatenschutzgesetzes dürfen bei im Informationssystem des Bundeskriminalamtes verarbeiteten personenbezogenen Daten bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. [3]Die Beachtung der Aussonderungsprüffristen ist durch geeignete technische Maßnahmen zu gewährleisten.
(2) bis (6) [...]

§ 79 BKAG - Löschung von durch Maßnahmen zur Abwehr von Gefahren des internationalen Terrorismus oder vergleichbaren Maßnahmen erlangten personenbezogenen Daten

(1) [1]Sind die durch eine in Abschnitt 5 genannte Maßnahme oder durch Maßnahmen nach § 34 oder § 64 erlangten personenbezogenen Daten, die nicht dem Kernbereich privater Lebensgestaltung zuzuordnen sind, zur Erfüllung des der Maßnahme zugrunde liegenden Zwecks und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, sind sie unverzüglich zu löschen, soweit keine Weiterverarbeitung der Daten nach den Vorschriften des Abschnitts 2 Unterabschnitt 2 erfolgt. [...]
(2) Absatz 1 gilt entsprechend für personenbezogene Daten, die
1. dem Bundeskriminalamt übermittelt worden sind und
2. durch Maßnahmen erlangt wurden, die den Maßnahmen nach § 34, Abschnitt 5 oder § 64 entsprechen.

Des Weiteren ist folgende Vorschrift aus dem Bundesdatenschutzgesetz von Bedeutung: 25

§ 75 BDSG - Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) [...]
(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.
(3) [...]
(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

III.

Die Beschwerdeführenden haben ihre Verfassungsbeschwerde am 22. Mai 2019 erhoben und mit Schriftsatz vom 29. September 2022 ergänzt. Soweit die Beschwerdeführerinnen zu 1) und 2) zunächst die Befugnisse des Bundeskriminalamts zu Online-Durchsuchungen (§ 49 BKAG) und Quellen-Telekommunikationsüberwachungen (§ 51 Abs. 2 BKAG) beanstandet hatten, haben sie mit Schriftsatz vom 27. April 2022 diesen Teil der Verfassungsbeschwerde zurückgenommen. 26

Die Beschwerdeführenden rügen eine Verletzung ihres Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Dabei wenden sich die Beschwerdeführerinnen zu 1) und 2) gegen die Befugnis des Bundeskriminalamts zur Datenerhebung zur Abwehr von Gefahren des internationalen Terrorismus (§ 45 Abs. 1 Satz 1 Nr. 4 BKAG), soweit diese eine Überwachung von Kontaktpersonen (§ 39 Abs. 2 Nr. 2 BKAG) er- 27

laubt. Zudem beanstanden sie die Befugnis des Bundeskriminalamts zur Weiterverarbeitung personenbezogener Daten in seinem eigenen Informationssystem, die durch derartige Überwachungsmaßnahmen erlangt wurden (§ 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG). Die Beschwerdeführenden zu 3) bis 5) wenden sich gegen die Weiterverarbeitungsbefugnis in § 18 Abs. 1 Nr. 1, 2 und 4, Abs.2 Nr. 1 und 3 und Abs. 5 auch in Verbindung mit § 29 Abs. 4 Satz 2 BKAG. Alle Beschwerdeführenden greifen die Ermächtigung zur Hinzuspeicherung ermittlungsunterstützender Hinweise im Informationssystem beziehungsweise Informationsverbund an (§ 16 Abs. 6 Nr. 2 auch i.V.m. § 29 Abs. 4 Satz 2 BKAG).

1. Die Verfassungsbeschwerde sei zulässig. Insbesondere seien die Beschwerdeführenden von den angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen. 28

Die Beschwerdeführerinnen zu 1) und 2) verträten als Rechtsanwältinnen Personen, die entweder selbst als terroristisch oder extremistisch eingestuft, oder die als Unterstützende terroristischer oder extremistischer Organisationen angesehen worden seien. 29

Die Beschwerdeführerin zu 3) sei (...) eines (...) von Fußballfans und engagiere sich in der Fanszene; in diesem Zusammenhang seien in der Vergangenheit zwei Ermittlungsverfahren gegen sie geführt worden. Der Beschwerdeführer zu 4) sei politisch in verschiedenen Organisationen aus dem linken politischen Spektrum aktiv und nehme regelmäßig an einschlägigen Veranstaltungen teil, was bereits zu einer polizeilichen Ausschreibung geführt habe. Der Beschwerdeführer zu 5) gehöre der sogenannten Ultra-Fußballfanszene an, in der er gut vernetzt sei. Über die Beschwerdeführenden zu 3) bis 5) seien personenbezogene Daten in polizeilichen Datensammlungen entweder aktuell gespeichert oder zumindest gespeichert gewesen. Als potenziell Betroffene könnten sie jedoch nicht ohne Weiteres gerichtlich gegen konkrete Umsetzungsakte vorgehen, weil sie davon keine Kenntnis erlangten und wegen weitreichender Ausnahmetatbestände eine nachträgliche Benachrichtigung nicht sichergestellt sei. 30

2. Die Verfassungsbeschwerde sei auch begründet. 31

a) § 45 Abs. 1 Satz 1 Nr. 4 BKAG ermögliche einen gezielten Einsatz eingriffsintensiver Überwachungsmittel gegen Kontaktpersonen unter unverhältnismäßig weiten Voraussetzungen. Der Verweis auf eine Person nach § 39 Abs. 2 Nr. 2 BKAG gewährleiste keine spezifische individuelle Nähe der betroffenen Person zur aufzuklärenden Gefahr. § 39 Abs. 2 Nr. 2 BKAG definiere zwar verfassungsrechtlich unbedenklich, in welchem Verhältnis die Kontaktperson zu einer verantwortlichen Person stehen müsse, verweise aber hinsichtlich dieser Person ihrerseits auf § 39 Abs. 2 Nr. 1 BKAG, der unter anderem ausreichen lasse, dass die verantwortliche Person eine terroristische Straftat begehen will. Diese weite Eingriffsschwelle könne indes eingriffsintensive Überwachungsmaßnahmen nach § 45 BKAG nicht rechtfertigen. Aufgrund der ausdrücklich geänderten Verweisungstechnik und des 32

eindeutigen Wortlauts könne die Vorschrift entgegen ihrer Vorgängernorm in § 20g Abs. 1 Satz 1 Nr. 3 BKAG a.F. nicht verfassungskonform ausgelegt werden.

b) Die Vorschriften zur reformierten polizeilichen Informationsordnung (§ 16, § 18 auch i.V.m. § 29 Abs. 4 Satz 2 BKAG) erlaubten eine Speicherung und spätere Nutzung personenbezogener Daten im Informationssystem des Bundeskriminalamts und im polizeilichen Informationsverbund unter unverhältnismäßig niedrigen Anforderungen. 33

aa) Polizeiliche Datensammlungen beträfen nicht die unmittelbare Weiterverarbeitung personenbezogener Daten, sondern beruhten auf einem zeitlich gestreckten Vorgang aus Datenspeicherung und späterer Nutzung. Die beiden aufeinander bezogenen Grundrechtseingriffe müssten getrennt gerechtfertigt werden. Zur Rechtfertigung der Speicherung bedürfe es eines hinreichenden Anlasses, der eine anlasslose Datenbevorratung ausschließe. Die Anforderungen bestimmten sich nach Art und Umfang der gespeicherten Daten. Eine zeitlich begrenzte Datenverfügbarkeit müsse durch gehaltvolle Löschungsregelungen gesichert werden. Höhere Anforderungen gälten für die an die Speicherung anschließende Nutzung der personenbezogenen Daten, wobei hierfür deren Ziele und Art maßgeblich seien. Auf Ebene der Datennutzung müssten unabhängig von den Voraussetzungen der Speicherung die grundrechtliche Zweckbindung und die Voraussetzungen einer hypothetischen Datenneuerhebung gewahrt werden. Daher sei es dysfunktional, beide Verarbeitungsschritte von einheitlichen Anforderungen abhängig zu machen. 34

bb) § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG sei unverhältnismäßig, soweit er das Bundeskriminalamt ermächtige, personenbezogene Daten, die es durch eingriffsintensive Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus erlangt habe, im Rahmen dieser Aufgabe in seinem Informationssystem zu speichern und anschließend zu nutzen. Da die Vorschrift auch eingriffsintensive Verarbeitungsmethoden ermögliche, könne das Eingriffsgewicht nicht allein durch die Schwelle der Erforderlichkeit zur Aufgabenerfüllung kompensiert werden. Der Verweis auf § 12 Abs. 1 Satz 1 BKAG schränke die Verarbeitung nicht maßgeblich ein. Bei einer Weiterverarbeitung zum Zweck der Terrorismusabwehr seien dessen Tatbestandsvoraussetzungen praktisch immer erfüllt. Die Vorgabe des § 79 Abs. 1 Satz 1 BKAG, im Rahmen der Terrorismusabwehr erhobene Daten nach Zweckerreichung grundsätzlich zu löschen, laufe weitgehend leer, da dieser Weiterverarbeitungen nach § 16 Abs. 1 BKAG nicht umfasse. 35

cc) Ebenso verfehlten die in § 18 Abs. 1 Nr. 1, 2 und 4, Abs. 2 Nr. 1 und 3 BKAG enthaltenen Ermächtigungen des Bundeskriminalamts, personenbezogene Daten über bestimmte Personenkreise im Rahmen der Zentralstellenaufgabe weiterzuverarbeiten, die verfassungsrechtlichen Anforderungen. Dies gelte gleichermaßen, soweit § 29 Abs. 4 Satz 2 BKAG die entsprechende Geltung der Vorschriften für die am polizeilichen Informationsverbund teilnehmenden Behörden anordne. 36

Schon die Ermächtigung zur Bevorratung (Speicherung) sei zu weitreichend. Nach § 18 Abs. 1 Nr. 1 und 2, Abs. 2 Nr. 1 BKAG dürften bestimmte Basisdaten verurteilter Straftäter und Beschuldigter ohne weitere Voraussetzungen gespeichert werden. So sei es verfassungsrechtlich zwar nicht zu beanstanden, dass § 18 Absätze 1 und 2 BKAG die Bevorratung personenbezogener Daten im Rahmen der Zentralstellenaufgabe – anders als im Rahmen von § 16 Abs. 1 BKAG – nicht von der Prüfung einer hypothetischen Datenneuerhebung abhängig mache. Der Gesetzgeber habe aber die nach allgemeinen datenschutzrechtlichen Grundsätzen gebotene Erforderlichkeitsprüfung im Einzelfall durch eine abstrakt-generelle Anordnung vorweggenommen. Dadurch laufe auch die Löschungspflicht nach § 77 Abs. 1 BKAG in Verbindung mit § 75 Abs. 2 BDSG weitgehend leer. § 18 Abs. 5 BKAG, nach dem die Weiterverarbeitung personenbezogener Daten von Beschuldigten unter engen Voraussetzungen unzulässig sei, schränke die Verarbeitungsbefugnis nicht maßgeblich ein. Unverhältnismäßig und unbestimmt sei ferner die in § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 1 und 3 BKAG enthaltene Ermächtigung zur Verarbeitung personenbezogener Daten über Anlasspersonen, die an eine unangeleitete Kriminalprognose anknüpfe. Die in § 67 Abs. 3 BDSG vorgesehene Datenschutzfolgenabwägung könne die verfassungsrechtlichen Verhältnismäßigkeits- und Bestimmtheitsmängel nicht heilen. Auch die transparenzschaffenden Regelungen genügten nicht den verfassungsrechtlichen Anforderungen. Eine Benachrichtigung der Betroffenen sei nicht vorgesehen, obwohl diese zumindest partiell im Rahmen der polizeilichen Aufgabenwahrnehmung möglich scheine. Das ebenfalls eingeschränkte Auskunftsrecht aus § 57 BDSG kompensiere diese Mängel nicht. 37

Die Ermächtigung in § 18 Absätze 1 und 2 BKAG zur Nutzung der bevorrateten Daten sei ebenfalls zu weitreichend. Anders als die Speicherung müsse die Nutzung von Daten, die durch eingriffsintensive verdeckte Überwachungsmaßnahmen gewonnen worden seien, von der Prüfung einer hypothetischen Datenneuerhebung abhängig gemacht werden. § 18 BKAG enthalte jedoch keinen Verweis auf den dies erfordernden § 12 BKAG. 38

dd) Die in § 16 Abs. 6 Nr. 2 BKAG enthaltene Ermächtigung zur Hinzuspeicherung sogenannter ermittlungsunterstützender Hinweise sei unverhältnismäßig weit und unbestimmt. Die Hinweise könnten höchstpersönliche oder stigmatisierende Angaben und sensible Informationen umfassen und damit eine erhebliche Eingriffsintensität aufweisen. Diese werde durch die weite Eingriffsschwelle der Eignung zum Drittschutz oder der Gewinnung von Ermittlungsansätzen nicht kompensiert. Die verfassungsrechtlichen Defizite könnten nicht durch eine restriktive Norminterpretation und sachgerechte Ermessensausübung im Einzelfall überwunden werden. 39

IV.

Zur Verfassungsbeschwerde haben die Bundesregierung, der Generalbundesanwalt beim Bundesgerichtshof und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Stellung genommen. 40

1. Die Bundesregierung hält die Verfassungsbeschwerde für unzulässig und unbegründet. 41

a) § 45 Abs. 1 Satz 1 Nr. 4 BKAG könne ebenso wie seine Vorgängervorschrift verfassungskonform ausgelegt werden. Die reine Wortlautauslegung möge zwar zu einem weiten Anwendungsbereich führen. Der Gesetzgeber habe aber allein eine redaktionelle Folgeänderung vornehmen wollen. Bei gebotener Auslegung solle der Verweis auf § 39 Abs. 2 Nr. 2 BKAG lediglich ein einheitliches Verständnis von Kontaktpersonen sicherstellen, nicht aber die niedrigeren Voraussetzungen des § 39 Abs. 2 Nr. 1 BKAG an die verantwortliche Person übernehmen. Das Bundeskriminalamt wende die Verweisung in der Praxis nur eingeschränkt an. Eine entsprechende Handhabung werde auch durch den Richtervorbehalt in § 45 Abs. 3 Satz 1 BKAG weitgehend sichergestellt. Im Übrigen sei § 39 Abs. 2 Nr. 1 BKAG nicht unbestimmt. 42

b) § 16 Abs. 1 BKAG normiere die Generalklausel des Bundeskriminalamts zur Weiterverarbeitung personenbezogener Daten und setze durch den Verweis auf § 12 BKAG konsequent das Konzept der hypothetischen Datenneuerhebung um. Eine anlasslose Bevorratung oder Nutzung personenbezogener Daten sei ausgeschlossen. Eine Überführung erhobener Daten in ein weiteres Verfahren richte sich entweder nach den §§ 18 und 19 BKAG oder aber nach strafprozessualen Normen. Soweit deren Voraussetzungen nicht gegeben wären oder die Daten weder für die Zentralstelle noch eine andere Aufgabe des Bundeskriminalamts oder für ein Strafverfahren erforderlich seien, würden sie unter den Voraussetzungen des § 79 BKAG und des § 77 Abs. 1 BKAG in Verbindung mit § 75 Abs. 2 BDSG gelöscht. Zudem sehe § 77 Abs. 1 BKAG in Verbindung mit § 75 Abs. 4 BDSG eine regelmäßige Überprüfung der Daten unter den Grundsätzen der Datensparsamkeit und Erforderlichkeit vor. Schließlich erfolgten Kontrollen durch den Datenschutzbeauftragten des Bundeskriminalamts und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. 43

c) Die Verarbeitungsvoraussetzungen personenbezogener Daten im Rahmen der Zentralstellenaufgabe ergäben sich nicht abschließend aus § 18 Absätze 1, 2 und 5 BKAG. Vielmehr grenze der ergänzend heranzuziehende § 12 BKAG die Verarbeitung maßgeblich ein. Ferner müsse das Bundeskriminalamt die in § 47 BDSG normierten allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten beachten, insbesondere, ob die Datenverarbeitung im Einzelfall erforderlich und angemessen sei. Der Gesetzgeber habe diese Prüfung nicht abstrakt-generell vorweggenommen. § 18 Abs. 1 Nr. 4 BKAG bedürfe verfassungsrechtlich keiner weitergehenden normierten Anknüpfungspunkte für die Anleitung der Kriminalprognose hinsichtlich der Anlasspersonen, sondern könne verfassungskonform ausgelegt werden. 44

Starre zeitliche Grenzen für eine Datenspeicherung oder -nutzung seien nicht geboten, da die Kombination aus festen Löschfristen und Aussonderungsprüffristen einen besseren 45

Ausgleich zwischen den betroffenen Grundrechten und der Sicherheit und Gefahrenabwehr gewährleiste. Ferner seien keine weitergehenden Benachrichtigungspflichten notwendig. Der Gesetzgeber könne innerhalb seines weiten Spielraums Geheimhaltungsaspekte einbeziehen und sich auf die Einräumung entsprechender Auskunftsrechte beschränken.

d) § 16 Abs. 6 Nr. 2 BKAG sei unter Berücksichtigung der Gesetzgebungsmaterialien hinsichtlich des Begriffs der Hinweise bestimmt genug. Einer potenziell erhöhten Eingriffsintensität könne durch eine verfassungskonforme Auslegung Rechnung getragen werden. Die verhältnismäßige Anwendung im Einzelfall sei durch entsprechende Verwaltungsvorschriften gewährleistet. 46

2. Der Generalbundesanwalt beim Bundesgerichtshof hält die Verfassungsbeschwerde jedenfalls für unbegründet. Er führt unter anderem aus, die Definition der verantwortlichen Person in § 39 Abs. 2 Nr. 1 BKAG stelle erkennbar nicht allein auf den subjektiven Wunsch des Betroffenen ab, sondern umfasse bei zutreffender Auslegung auch die konkrete Fähigkeit, terroristische Straftaten zu begehen. Zudem gewährleiste die Voraussetzung, dass die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtlos oder wesentlich erschwert wäre, eine strenge Verhältnismäßigkeitsprüfung aufgrund einer gehaltvollen Prognose. Soweit die Verfassungsbeschwerde die Weiterverarbeitung nach § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG rüge, verkenne sie die verfassungsrechtlich gefestigten Anforderungen an die Zweckbindung und Zweckänderung. Gerade um terroristische Strukturen zu verstehen und zu durchdringen, sei die von den Beschwerdeführenden kritisierte Sammlung und Auswertung relevanter Informationen notwendig. 47

3. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt im Ergebnis weithin die diesbezüglichen Bedenken der Beschwerdeführenden. Die Gesetzgebungsmaterialien ließen ein verkürztes Verständnis der Rechtsprechung des Bundesverfassungsgerichts erkennen. Während der Grundsatz der hypothetischen Datenneuerhebung zentral sei, werde nicht hinreichend gewichtet, dass jeder Verarbeitungsschritt als eigenständiger Grundrechtseingriff insoweit einer Rechtsgrundlage bedürfe, die orientiert am Eingriffsgewicht normenklare und verhältnismäßige Eingriffsschwellen festlege. Erschwerend komme hinzu, dass es sich bei dem Informationssystem und -verbund um Mischdateien für Zwecke der Strafverfolgung und der Gefahrenabwehr handele. 48

§ 16 Abs. 1 BKAG fasse die Eingriffsschwellen nicht bestimmt genug beziehungsweise zu weit. Die Vorschrift ermögliche durch den weiten Begriff der Weiterverarbeitung mitunter schwerwiegende Eingriffe. § 12 BKAG gewährleiste zwar einen Mindestmaßstab für jede weitere einzelne Verwendung polizeilich erhobener Daten, mache aber hinreichend bestimmte gesetzliche Voraussetzungen für die weiteren Verarbeitungsschritte nicht entbehrlich. Zudem sei unklar, welchen Personenkreis § 16 BKAG einbeziehe, der nicht an die 49

polizeirechtliche Verantwortlichkeit anknüpfe. Die subsidiäre Anwendung von § 16 Abs. 1 BKAG ermögliche indes eine einschränkende verfassungskonforme Auslegung. Insoweit seien insbesondere für das allgemeine Sammeln und Auswerten von Informationen § 18 und § 19 BKAG vorrangig. Der Wortlaut von § 16 Abs. 1 BKAG ermögliche indes darüber hinaus weitere Sammlungen, Analysen und Auswertungen. Bei verfassungskonformem Verständnis dürfe die umfassende Speicherung größerer Datenbestände zu Zwecken der Auswertung und Analyse nicht auf § 16 Abs. 1 BKAG gestützt werden.

Auch § 18 Absätze 1 und 2 BKAG verfehle angesichts des hohen Eingriffsgewichts der Datenverarbeitung die verfassungsrechtlichen Bestimmtheits- und Verhältnismäßigkeitsanforderungen und teile überwiegend die Mängel von § 16 Abs. 1 BKAG. Insbesondere sei nicht näher definiert, was unter den Begriff der Grunddaten zu fassen sei. Im Auslegungswege lasse sich für die Praxis aber eine verhältnismäßige Lösung finden. Allerdings sehe die Vorschrift keine Erforderlichkeitsprüfung vor; vielmehr genüge die „Relevanz“ der Daten, die voraussichtlich in der Praxis technisch anhand einer automatisierten Kategorisierung und nicht immer im Einzelfall geprüft werde. Dass die am Informationsverbund teilnehmenden Behörden nach § 30 BKAG nur verbundrelevante Daten erfassen dürften, führe mangels klarer festgelegter Kriterien zu keiner maßgeblichen Eingrenzung. § 18 Abs. 5 BKAG schränke die Weiterverarbeitung der Daten nicht hinreichend ein. In der Praxis fehle es regelmäßig an der Rückmeldung über die konkreten Verfahrensausgänge der Staatsanwaltschaften an die Polizeibehörden. Es bestünden erhebliche Probleme im Umgang mit der Negativprognose. 50

§ 16 Abs. 6 Nr. 2 BKAG ermögliche die Speicherung ermittlungsunterstützender Hinweise, die weitreichende Informationen enthalten könnten. Diese seien für die betroffenen Personen nicht nachvollziehbar, zumal der entsprechende Leitfaden als Verschlusssache eingestuft sei. 51

V.

Das Bundesverfassungsgericht hat am 20. Dezember 2023 eine mündliche Verhandlung durchgeführt. Geäußert haben sich dort die Beschwerdeführenden und die Bundesregierung. Als sachkundiger Dritter nach § 27a BVerfGG hat sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit geäußert. 52

B.

I.

Die Zuständigkeit des Bundesverfassungsgerichts für die Prüfung der Vereinbarkeit der angegriffenen Normen mit den Grundrechten des Grundgesetzes ist gegeben, obwohl die 53

angegriffenen Vorschriften Bezüge zu datenschutzrechtlichen Bestimmungen in Rechtsakten der Europäischen Union wie insbesondere der JI-Richtlinie haben. Es handelt sich bei den hier angegriffenen Befugnissen aber nicht um die Umsetzung zwingenden Unionsrechts. Rechtsvorschriften der Europäischen Union enthalten keine Bestimmungen, welche die hier angegriffenen Befugnisse erfordern oder gar abschließend regeln (vgl. dazu BVerfGE 155, 119 <162 ff. Rn. 83 ff.> m.w.N.; 156, 11 <35 ff. Rn. 63 ff.>; 158, 170 <183 Rn. 23> m.w.N.). Unberührt bleibt hiervon die vorliegend nicht zu klärende Frage, ob sich weitere rechtliche Anforderungen unmittelbar aus dem Sekundärrecht der Europäischen Union ergeben und ob die beanstandeten Vorschriften mit diesen vereinbar sind (vgl. BVerfGE 155, 119 <165 Rn. 88>; 163, 43 <76 f. Rn. 93> m.w.N.).

II.

Mit Schriftsatz vom 27. April 2022 haben die Beschwerdeführerinnen zu 1) und 2) den Teil der Verfassungsbeschwerde wirksam zurückgenommen, der sich gegen die Ermächtigungen des Bundeskriminalamts zu Online-Durchsuchungen (§ 49 BKAG) und Quellen-Telekommunikationsüberwachungen (§ 51 Abs. 2 BKAG) richtete. 54

III.

Die Verfassungsbeschwerde ist überwiegend zulässig. Soweit sich die Beschwerdeführerinnen zu 1) und 2) gegen § 45 Abs. 1 Satz 1 Nr. 4 in Verbindung mit § 39 Abs. 2 Nr. 2 BKAG sowie gegen § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG wenden, ist sie zulässig. Soweit die Beschwerdeführenden zu 3) bis 5) die Befugnis zur Datenweiterverarbeitung nach § 18 Abs. 1 Nr. 1, 2 und 4, Abs. 2 Nr. 1 und 3 und Abs. 5 auch in Verbindung mit § 29 Abs. 4 Satz 2 BKAG angreifen, ist sie dagegen nur teilweise zulässig. Unzulässig ist sie hinsichtlich aller Beschwerdeführenden, soweit sie sich gegen § 16 Abs. 6 Nr. 2 BKAG wendet. 55

1. Richtet sich eine Verfassungsbeschwerde wie vorliegend gegen ein Gesetz, das Sicherheitsbehörden zu heimlichen Maßnahmen ermächtigt, bestehen besondere Zulässigkeitsanforderungen bezüglich der Beschwerdebefugnis und der Subsidiarität der Verfassungsbeschwerde (vgl. BVerfGE 162, 1 <51 ff. Rn. 93 ff.> – Bayerisches Verfassungsschutzgesetz; 165, 1 <29 ff. Rn. 37 ff.> – Polizeiliche Befugnisse nach SOG MV). 56

a) Die Zulässigkeit einer Verfassungsbeschwerde setzt nach Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG die Behauptung voraus, durch einen Akt der öffentlichen Gewalt in Grundrechten oder grundrechtsgleichen Rechten verletzt zu sein (Beschwerdebefugnis) (vgl. BVerfGE 140, 42 <54 Rn. 47>; 162, 1 <51 f. Rn. 93>). Dazu müssen sowohl die Möglichkeit der Grundrechtsverletzung (aa) als auch die eigene, unmittelbare und gegenwärtige Betroffenheit (bb) den Begründungsanforderungen nach § 23 Abs. 1 Satz 2, § 92 BVerfGG entsprechend dargelegt sein (vgl. BVerfGE 125, 39 <73>; 159, 355 <375 Rn. 25> – Bundesnotbremse II). 57

aa) Der die behauptete Rechtsverletzung enthaltende Vorgang muss substantiiert und schlüssig vorgetragen sein, und der Vortrag muss die Möglichkeit einer Grundrechtsverletzung hinreichend deutlich erkennen lassen (vgl. BVerfGE 130, 1 <21>; 140, 229 <232 Rn. 9>). Eine genaue Bezeichnung des Grundrechts, dessen Verletzung geltend gemacht wird, ist nicht erforderlich. Dem Vortrag muss sich aber entnehmen lassen, inwiefern sich die Beschwerdeführenden durch den angegriffenen Hoheitsakt in ihren Rechten verletzt sehen (vgl. BVerfGE 115, 166 <180>). Ist die Verfassungsbeschwerde gegen gesetzliche Vorschriften gerichtet, müssen sich die Beschwerdeführenden genau mit der angegriffenen Norm befassen. Sie müssen auch weitere Regelungen des Fachrechts in ihre Darlegungen einbeziehen, wenn diese Bedeutung für die Verfassungsmäßigkeit der angegriffenen Norm haben können. Mit der verfassungsrechtlichen Beurteilung des vorgetragenen Sachverhalts müssen sich die Beschwerdeführenden im Einzelnen auseinandersetzen. Soweit das Bundesverfassungsgericht für bestimmte Fragen bereits verfassungsrechtliche Maßstäbe entwickelt hat, muss anhand dieser Maßstäbe aufgezeigt werden, inwieweit Grundrechte durch die angegriffene Maßnahme verletzt sein sollen (vgl. BVerfGE 101, 331 <345 f.>; 159, 223 <270 Rn. 89> m.w.N. – Bundesnotbremse I; stRspr). 58

bb) Für die Darlegung der unmittelbaren sowie der eigenen und gegenwärtigen Betroffenheit gelten bei einer Verfassungsbeschwerde gegen eine gesetzliche Ermächtigung zu heimlichen Maßnahmen besondere Anforderungen. 59

(1) Zwar werden die hier angegriffenen Vorschriften erst auf der Grundlage weiterer Vollzugsakte in Form von Datenerhebung oder -weiterverarbeitung wirksam. Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführende den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (vgl. BVerfGE 155, 119 <159 Rn. 73> – Bestandsdatenauskunft II). 60

(2) Zur Begründung der Möglichkeit eigener und gegenwärtiger Betroffenheit durch eine gesetzliche Ermächtigung zu heimlichen Maßnahmen, bei der die konkrete Beeinträchtigung zwar erst durch eine Vollziehung erfolgt, die Betroffenen in der Regel aber keine Kenntnis von Vollzugsakten erlangen, reicht es aus, wenn die Beschwerdeführenden darlegen, mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt zu werden (vgl. BVerfGE 155, 119 <160 Rn. 75>). Ein Vortrag, für sicherheitsgefährdende Aktivitäten verantwortlich zu sein, ist zum Beleg der Selbstbetroffenheit grundsätzlich ebenso wenig erforderlich wie Darlegungen, durch die sich Beschwerdeführende selbst einer Straftat bezichtigen müssten (vgl. BVerfGE 130, 151 <176 f.>; stRspr). 61

b) Besondere Zulässigkeitsanforderungen ergeben sich auch aus der Subsidiarität der Verfassungsbeschwerde. Zwar steht unmittelbar gegen Parlamentsgesetze kein ordentlicher Rechtsweg im Sinne des § 90 Abs. 2 BVerfGG zur Verfügung, der vor Erhebung der Verfassungsbeschwerde erschöpft werden muss. Die Verfassungsbeschwerde muss aber auch den Anforderungen der Subsidiarität im weiteren Sinne genügen. Diese beschränken sich nicht darauf, nur die zur Erreichung des unmittelbaren Prozessziels förmlich eröffneten Rechtsmittel zu ergreifen, sondern verlangen, alle Mittel zu nutzen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Damit soll erreicht werden, dass das Bundesverfassungsgericht nicht auf ungesicherter Tatsachen- und Rechtsgrundlage weitreichende Entscheidungen treffen muss, sondern zunächst die für die Auslegung und Anwendung des einfachen Rechts primär zuständigen Fachgerichte die Sach- und Rechtslage aufgearbeitet haben. Der Grundsatz der Subsidiarität erfordert deshalb grundsätzlich, vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen, um eine Korrektur der geltend gemachten Verfassungsverletzung zu erwirken oder eine Grundrechtsverletzung zu verhindern. Das gilt auch, wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und im konkreten Fall in zulässiger Weise eingelegt werden kann (vgl. zum Ganzen BVerfGE 150, 309 <326 ff. Rn. 42 ff.>; 162, 1 <54 ff. Rn. 100 ff.>; 165, 1 <29 ff. Rn. 37 ff.>; stRspr). 62

2. Die Verfassungsbeschwerde genügt diesen Anforderungen in weiten Teilen. 63

a) Die Verfassungsbeschwerde ist hinsichtlich der Beschwerdeführerinnen zu 1) und 2) zulässig, soweit sie geltend machen, die Befugnis des Bundeskriminalamts zur Datenerhebung mit besonderen Mitteln bei Kontaktpersonen (§ 45 Abs. 1 Satz 1 Nr. 4 i.V.m. § 39 Abs. 2 Nr. 2 BKAG) sei nicht an eine hinreichende Eingriffsschwelle gebunden. Insbesondere haben sie die Möglichkeit einer Verletzung in ihrem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG dargelegt. 64

Ihnen fehlt es auch nicht an einer unmittelbaren Betroffenheit. Zwar bedarf die angegriffene Befugnis einer Umsetzung durch weitere Vollzugsakte. Die streitgegenständlichen Überwachungsmaßnahmen werden jedoch grundsätzlich heimlich durchgeführt. Die im Gesetz vorgesehenen Benachrichtigungspflichten fangen dies nur teilweise auf, weil sie möglicherweise erst spät greifen und weitreichende Ausnahmen kennen. 65

Die Beschwerdeführerinnen zu 1) und 2) haben ferner hinreichend dargelegt, dass sie wegen ihrer spezifischen beruflichen Verbindungen zu Personen, die als Zielperson einer Maßnahme nach § 45 Abs. 1 Satz 1 Nr. 4 BKAG in Betracht kommen können, von den angegriffenen Überwachungsmaßnahmen jedenfalls mit hinreichender Wahrscheinlichkeit indirekt betroffen sein können. Sie verweisen insbesondere darauf, dass sie aufgrund ihrer beruflichen Tätigkeit als Rechtsanwältinnen auch mit Personen in Kontakt gerieten, die dem internationalen Terrorismus zugerechnet würden (vgl. auch BVerfGE 141, 220 <262 Rn. 84>; 165, 1 <37 f. Rn. 58 f.>). 66

b) Auch soweit sich die Beschwerdeführerinnen zu 1) und 2) gegen § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG wenden, ist die Verfassungsbeschwerde zulässig. Die Beschwerdeführerinnen haben die Möglichkeit einer Verletzung in ihrem Grundrecht auf informationelle Selbstbestimmung sowie ihre mögliche Betroffenheit hinreichend dargelegt. Gerügt ist die Weiterverarbeitung personenbezogener Daten, die zunächst zur Abwehr von Gefahren des internationalen Terrorismus nach § 5 BKAG mit besonders eingriffsintensiven Mitteln erhoben worden sind und in einem zweiten Schritt gemäß § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG zur Erfüllung derselben Aufgaben verwendet werden. 67

c) Soweit die Beschwerdeführenden zu 3) bis 5) die Befugnis zur Datenweiterverarbeitung nach § 18 Abs. 1 Nr. 1, 2 und 4, Abs. 2 Nr. 1 und 3 und Abs. 5 auch in Verbindung mit § 29 Abs. 4 Satz 2 BKAG angreifen, ist die Verfassungsbeschwerde nur teilweise zulässig. 68

aa) Die Möglichkeit einer Grundrechtsverletzung ist dargelegt, soweit die Speicherung zuvor erhobener personenbezogener Grunddaten von Beschuldigten durch das Bundeskriminalamt im polizeilichen Informationsverbund unter dem Gesichtspunkt einer unzureichenden Speicherschwelle beanstandet wird (§ 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1, soweit sein Anwendungsbereich durch § 13 Abs. 3, § 29 BKAG konkretisiert wird; im Folgenden vereinfachend: § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG). 69

In diesem Umfang haben die Beschwerdeführenden zu 3) bis 5) insbesondere auch hinreichend dargelegt, von der Weiterverarbeitungsbefugnis selbst betroffen zu sein. Hierzu verweisen sie auf ihre politischen und sonstigen Aktivitäten. Diese begründen eine erhöhte Wahrscheinlichkeit, zumindest von solchen polizeilichen Datenerhebungen betroffen zu werden, die in ihrer Intensität hinter einer Wohnraumüberwachung und Online-Durchsuchung zurückbleiben. Dies lässt auch eine anschließende Weiterverarbeitung der so erhobenen Daten wahrscheinlich erscheinen. Teilweise sind oder waren sie in polizeilichen Datensammlungen erfasst. 70

Unzulässig ist die Rüge mit Blick auf die Speicherung der personenbezogenen Daten allein im internen Informationssystem des Bundeskriminalamts. Insoweit fehlt es an einer hinreichenden Auseinandersetzung mit dem einschlägigen Fachrecht bezüglich der Trennung der Datenbestände im Informationssystem des Bundeskriminalamts und im polizeilichen Informationsverbund sowie der damit einhergehenden unterschiedlichen Gewichtung des Eingriffs und möglichen korrespondierenden Rechtfertigungsanforderungen. 71

Nicht zulässig gerügt ist weiter die sich der Speicherung anschließende weitere Nutzung der Daten durch das Bundeskriminalamt, da nicht hinreichend dargelegt wird, unter welchen Voraussetzungen diese erfolgt. Die Beschwerdeführenden zu 3) bis 5) behaupten, dass sämtliche Weiterverarbeitungsschritte einheitlich geregelt seien, setzen sich jedoch nicht damit auseinander, ob und wie § 12 Abs. 2 BKAG über den Verweis in § 29 Abs. 4 Satz 2 72

BKAG für die weitere Datennutzung im Informationsverbund zur Anwendung gelangen könnte, da das Bundeskriminalamt selbst teilnehmende Behörde im Informationsverbund ist (§ 13 Abs. 3, § 29 Abs. 3 BKAG).

Auch soweit eine Weiterverarbeitung durch die übrigen teilnehmenden Behörden des polizeilichen Informationsverbunds als verfassungswidrig gerügt wird, setzt sich die Verfassungsbeschwerde nicht hinreichend mit dem einschlägigen Fachrecht auseinander. Der knappe Verweis auf § 29 Abs. 4 Satz 2 BKAG kann insbesondere angesichts des differenzierten Regelungskonzepts des Bundesgesetzgebers und landesrechtlicher Vorgaben ein Vorbringen zu den Voraussetzungen für Speicherung und Zugriff durch die übrigen teilnehmenden Behörden nicht ersetzen. 73

bb) Unzulässig ist die Verfassungsbeschwerde, soweit sie sich gegen die Weiterverarbeitung personenbezogener Daten von Verurteilten nach § 18 Abs. 1 Nr. 1, Abs. 2 Nr. 1 BKAG wendet. Die Beschwerdeführenden zu 3) bis 5) haben zum einen nicht dargelegt, von der Regelung selbst betroffen zu sein. Sie haben insbesondere nicht mitgeteilt, bereits strafrechtlich verurteilt worden zu sein. Soweit sich den Anlagen der Verfassungsbeschwerde Hinweise auf Verurteilungen entnehmen lassen, kann dies hier einen entsprechenden Vortrag nicht ersetzen. 74

Zum anderen fehlt es mit Blick auf die Möglichkeiten verwaltungsgerichtlichen Rechtsschutzes hinsichtlich der Speicherung von Daten nach § 18 Abs. 1 Nr. 1 BKAG an Vortrag zur Wahrung der Anforderungen des Grundsatzes der Subsidiarität. In diesen Fällen hat die Person sichere Kenntnis von ihrer Verurteilung und damit vom Vorliegen der Voraussetzungen einer Speicherung ihrer Daten. 75

cc) Die Verfassungsbeschwerde ist ferner hinsichtlich der Rügen einer Weiterverarbeitung personenbezogener Daten von Anlasspersonen nach § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 1 und 3 BKAG sowie einer fehlenden Benachrichtigungspflicht unzulässig. Insoweit haben die Beschwerdeführenden zu 3) bis 5) die Möglichkeit einer Grundrechtsverletzung nicht ausreichend dargelegt. Sie führen aus, es gebe für die Kriminalprognose keine Anknüpfungspunkte aus dem Vorverhalten, setzen sich jedoch nicht mit den in § 18 Abs. 1 Nr. 4 BKAG anstelle eines Vorverhaltens zur Voraussetzung gemachten tatsächlichen Anhaltspunkten für eine Gefahr in naher Zukunft liegender Straftaten auseinander. Warum nur strafrechtlich relevantes Vorverhalten maßgeblich sein kann, erläutern die Beschwerdeführenden nicht. Hinsichtlich der Benachrichtigungspflichten fehlen eine konkretere Darlegung von und eine Auseinandersetzung mit den differenzierten verfassungsrechtlichen Transparenzanforderungen gerade auch mit Blick auf die Besonderheiten der Datenweiterverarbeitung im polizeilichen Informationsverbund. 76

dd) Nicht hinreichend substantiiert ist auch die Rüge von § 18 Abs. 5 BKAG, weil die Beschwerdeführenden insoweit eine eigene Beschwer nicht hinreichend dargelegt haben. 77

d) Der Rüge von § 16 Abs. 6 Nr. 2 BKAG fehlt es an hinreichenden Ausführungen zu den verfassungsrechtlichen Anforderungen einer Hinzuspeicherung. Allein der Hinweis auf eine fehlende hinreichend restriktive Eingriffsschwelle genügt insoweit nicht. 78

3. Die Verfassungsbeschwerde ist nach § 93 Abs. 3 BVerfGG fristgerecht eingelegt. Gemäß Art. 13 Abs. 1 Satz 1 des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes sind die gerügten Vorschriften am 25. Mai 2018 in Kraft getreten und mit der am 22. Mai 2019 eingegangenen Verfassungsbeschwerde innerhalb der Jahresfrist des § 93 Abs. 3 BVerfGG angegriffen worden. 79

C.

Die Verfassungsbeschwerde ist, soweit sie zulässig ist, teilweise begründet. Die angegriffenen Regelungen greifen in das Grundrecht der Beschwerdeführenden auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein (I). Sie sind zwar im zu prüfenden Umfang formell verfassungsgemäß (II), genügen aber den Vorgaben der Verhältnismäßigkeit (III) nicht durchgehend. So ist § 45 Abs. 1 Satz 1 Nr. 4 BKAG in seiner konkreten Ausgestaltung nicht mit der Verfassung vereinbar (IV). Demgegenüber greifen die gegen § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG erhobenen verfassungsrechtlichen Bedenken bei zutreffender Auslegung nicht durch (V). § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG hingegen wahrt die verfassungsrechtlichen Anforderungen nicht (VI). 80

I.

Die angegriffenen Befugnisse greifen in das als verletzt gerügte Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein. Nach ständiger Rechtsprechung umfasst das allgemeine Persönlichkeitsrecht als eigenständige Ausprägung auch das Grundrecht auf informationelle Selbstbestimmung (vgl. BVerfGE 65, 1 <42> – Volkszählung; 78, 77 <84>; 118, 168 <184>; 152, 152 <188 Rn. 83> – Recht auf Vergessen I). Danach setzt die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht gewährleistet damit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1 <42 f.>; 120, 274 <312>; zum unionalen Datenschutzgrundrecht als Ausprägung der Achtung des Privat- und Familienlebens aus Art. 7 GRCh und des Schutzes personenbezogener Daten aus Art. 8 GRCh vgl. EuGH, Urteil vom 8. April 2014, Digital Rights Ireland and Seitlinger u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 35, 47 und 54 f.; Urteil vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 47 sowie BVerfGE 152, 216 <254 ff. Rn. 99 ff.> – Recht auf Vergessen II m.w.N.). Es geht 81

damit über den Schutz der Privatsphäre hinaus. Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt (vgl. BVerfGE 120, 274 <312>).

Dies zugrunde legend stellt zunächst die Befugnis des Bundeskriminalamts zur heimlichen Erhebung von Daten nach § 45 Abs. 1 Satz 1 Nr. 4 BKAG einen Grundrechtseingriff dar (vgl. auch BVerfGE 141, 220 <286 f. Rn. 147 ff.>; zum Eingriffsgewicht sogleich unter Rn. 99). Aber auch die Befugnisse zur Weiterverarbeitung zuvor erhobener personenbezogener Daten – § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG und § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG – begründen jeweils eigenständige Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, deren Eingriffsintensität variieren kann (vgl. insbesondere BVerfGE 141, 220 <324 ff. Rn. 276 ff.>; 165, 363 <393 Rn. 61>). 82

II.

Soweit die angegriffenen Befugnisnormen zulässig gerügt sind, sind sie in formeller Hinsicht mit der Verfassung vereinbar. Insbesondere steht dem Bund insoweit die Gesetzgebungskompetenz zu. 83

1. § 45 Abs. 1 Satz 1 Nr. 4 in Verbindung mit § 39 Abs. 2 Nr. 2 BKAG sowie § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG im Rahmen der Aufgabenerfüllung nach § 5 BKAG sind in kompetenzrechtlicher Hinsicht verfassungsgemäß. Für den Bund besteht die ausschließliche Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 9a GG zur Regelung der Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um Übernahme ersucht. Der Begriff der Gefahrenabwehr schließt kompetenzrechtlich die Verhütung von Straftaten ein (vgl. zur Terrorismusabwehr nach dem Bundeskriminalamtgesetz i.d.F. vom 25. Dezember 2008 bereits BVerfGE 141, 220 <263 Rn. 88>). Der hier maßgebliche § 5 Abs. 1 Satz 1 BKAG beschränkt diese Befugnisse des Bundeskriminalamts ausdrücklich entsprechend den Vorgaben des Art. 73 Abs. 1 Nr. 9a GG. 84

2. Der Bund verfügt ferner über die Gesetzgebungskompetenz für die Regelungen der § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG hinsichtlich des polizeilichen Informationsverbundes und dem damit ermöglichten überbehördlichen Austausch personenbezogener Daten über bestimmte Personen. 85

a) Soweit die angegriffenen Vorschriften den Austausch von Informationen zwischen dem Bundeskriminalamt, den Landeskriminalämtern, sonstigen Polizeibehörden der Länder und der Steuerfahndung der Landesfinanzbehörden regeln, besteht für den Bund die Gesetzgebungskompetenz des Art. 73 Abs. 1 Nr. 10 Buchstabe a GG zur Zusammenarbeit 86

des Bundes und der Länder in der Kriminalpolizei (vgl. BVerfGE 133, 277 <317 Rn. 97>). Diese Zusammenarbeit umfasst insbesondere die laufende gegenseitige Unterrichtung und Auskunftserteilung und erlaubt funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und gemeinsame Informationssysteme (vgl. BVerfGE 133, 277 <317 f. Rn. 97>; 156, 11 <41 Rn. 76>; 163, 43 <79 Rn. 99>). Die Gesetzgebungskompetenz erstreckt sich dabei nicht nur auf die Zusammenarbeit des Bundes und der Länder, sondern ebenfalls auf die der Länder untereinander (BVerfGE 163, 43 <80 Rn. 101>). Der Begriff „Kriminalpolizei“ schließt nicht aus, dass der Bund eine Zusammenarbeit auch zur Verhinderung von Straftaten regeln kann, sondern dient lediglich der Beschränkung auf Regelungen, die sich auf bedeutsame Straftaten von Gewicht beziehen (vgl. BVerfGE 133, 277 <318 Rn. 98>; 156, 11 <41 f. Rn. 77>; 163, 43 <81 Rn. 104>). Dabei muss es sich um Straftatbestände handeln, bei denen es der durch Art. 73 Abs. 1 Nr. 10 GG erlaubten Zusammenarbeit bedarf oder eine solche naheliegt. Ausgeschlossen sind von vornherein die allgemeine Gefahrenabwehr oder die Bekämpfung von Kleinkriminalität, erst recht die Bekämpfung von Ordnungswidrigkeiten (BVerfGE 156, 11 <41 f. Rn. 77 f.>; 163, 43 <81 Rn. 104>).

Hiernach können § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG kompetenzrechtlich auf Art. 73 Abs. 1 Nr. 10 GG gestützt werden. Die angegriffenen Befugnisnormen ermächtigen das Bundeskriminalamt, dessen Aufgaben auf „kriminalpolizeiliche Angelegenheiten“ beschränkt sind (vgl. § 1 Abs. 1 BKAG), in seiner Funktion als Zentralstelle nach § 2 Absätze 1 bis 3 BKAG personenbezogene Daten weiterzuverarbeiten und insbesondere für den Zugriff der anderen am polizeilichen Informationsverbund teilnehmenden Behörden vorsorgend zu speichern. Der entsprechend dem Kompetenztitel in Art. 73 Abs. 1 Nr. 10 Buchstabe a GG verwendete Begriff „Kriminalpolizei“ dient der Beschränkung auf Regelungen, die sich auf bedeutsame Straftaten von Gewicht beziehen (vgl. BVerfGE 163, 43 <81 Rn. 104> m.w.N.). Dies gilt auch für die Zentralstellenaufgaben des Bundeskriminalamts, die gemäß § 2 Abs. 1 BKAG auf koordinierende und unterstützende Aufgaben bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung beschränkt sind (vgl. zu § 10 Abs. 2, Abs. 1 Satz 1 Nr. 1 BKAG a.F. BVerfGE 155, 119 <225 Rn. 241>). Straftaten, die aufgrund ihres grenzüberschreitenden Charakters die Belange eines anderen Bundeslandes oder eines anderen Staates (vgl. BTDrucks 13/1550, S. 21) betreffen, als auch solche, die den Rechtsfrieden empfindlich stören und die geeignet sind, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vgl. BVerfGE 109, 279 <344>; 124, 43 <64>), begründen ein Bedürfnis nach Zusammenarbeit von Bund und Ländern in der Kriminalpolizei. 87

b) Soweit als weitere Behörden die Bundespolizei, Zollbehörden und die Polizei beim Deutschen Bundestag in den Informationsverbund miteinbezogen werden, ergibt sich die Gesetzgebungskompetenz des Bundes aus Art. 73 Abs. 1 Nr. 5 GG sowie aus der Natur der Sache. Die Beteiligung der Bundespolizei und der Zollbehörden am Informationsverbund 88

kann der Bund auf Art. 73 Abs. 1 Nr. 5 GG stützen, der ihm die ausschließliche Gesetzgebungskompetenz für den Zoll- und Grenzschutz einräumt. Die angegriffenen Vorschriften weisen diesen keine neuen, durch Art. 73 Abs. 1 Nr. 5 GG nicht mehr gedeckten, auf die Verhinderung oder Verfolgung von Straftaten gerichteten Datenerhebungsbefugnisse zu, sondern knüpfen an die für die eigene Aufgabenerfüllung erhobenen Daten an und regeln lediglich die wechselseitige Zurverfügungstellung der Daten zwischen den teilnehmenden Behörden „zur jeweiligen Aufgabenerfüllung“ (§ 29 Abs. 3 Satz 2 BKAG; vgl. zum Datenaustausch nach dem Antiterrordateigesetz BVerfGE 133, 277 <319 f. Rn. 101, 102>; 156, 11 <43 Rn. 81 f.>). Hinsichtlich der Einbeziehung der Polizei beim Deutschen Bundestag folgt die Gesetzgebungskompetenz des Bundes aus der Natur der Sache (vgl. allgemein zu dieser ungeschriebenen Gesetzgebungskompetenz BVerfGE 12, 205 <251>; 22, 180 <216 f.>; 26, 246 <257>; vgl. zum Schutz von Verfassungsorganen auch BVerfGE 155, 119 <173 Rn. 112>).

c) Art. 91c Abs. 2 GG, der vorsieht, dass Bund und Länder die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen auf Grund von Vereinbarungen festlegen können, enthält insoweit keine spezielle Regelung, die der Annahme einer Gesetzgebungskompetenz des Bundes für die angegriffenen Vorschriften entgegensteht. Art. 91c GG trifft lediglich für die Kommunikation zwischen IT-Systemen von Bund und Ländern eine spezielle Regelung, um einen effizienten, schnellen und sicheren Austausch von Daten ohne System- und Medienbrüche zu gewährleisten (vgl. Wischmeyer, in: Huber/Voßkuhle, Grundgesetz, 8. Aufl. 2024, Art. 91c Rn. 21; s.a. Ruge, in: Schmidt-Bleibtreu/Hofmann/Henneke, Grundgesetz, 15. Aufl. 2022, Art. 91c Rn. 21, 27). 89

III.

1. a) Eingriffe in das Grundrecht auf informationelle Selbstbestimmung bedürfen einer gesetzlichen Ermächtigung, die einen legitimen Gemeinwohlzweck verfolgt und für die Zweckerreichung geeignet, erforderlich und verhältnismäßig im engeren Sinne ist (vgl. BVerfGE 65, 1 <44>; 100, 313 <359 f.>; 155, 119 <176 f. Rn. 123>; stRspr). Dabei ergeben sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne spezielle Anforderungen. Wie streng diese im Einzelnen sind, bestimmt sich nach dem Eingriffsgewicht der jeweiligen Befugnis zur Erhebung von oder dem weiteren Umgang mit personenbezogenen Daten (vgl. BVerfGE 141, 220 <269 Rn. 105>; 165, 363 <389 f. Rn. 54>; stRspr). Zur Konkretisierung der Rechtfertigungsanforderungen sind deshalb die grundsätzlich verschiedenen, aber aufeinander bezogenen Grundrechtseingriffe zu unterscheiden. Vorliegend ist insbesondere zwischen der gesondert geregelten Datenerhebung sowie der unter dem Oberbegriff der Weiterverarbeitung einheitlich normierten Speicherung personenbezogener Daten und deren weiterer Nutzung zu differenzieren (vgl. BVerfGE 65, 1 <43> – Volkszählung; 120, 351 <361> – Datensammlung über steuerliche Auslandsbeziehungen; sowie 90

BVerfGE 155, 119 <167 Rn. 93> – Bestandsdatenauskunft II). Eine Verwendung zuvor erhobener Daten über den ursprünglichen Anlass hinaus begründet dabei einen neuen Grundrechtseingriff und muss verfassungsrechtlich eigens nach dem Grundsatz der Zweckbindung gerechtfertigt werden (vgl. BVerfGE 141, 220 <324 Rn. 277, 327 Rn. 285>). Der Verhältnismäßigkeitsgrundsatz stellt – vorliegend mangels entsprechender Rügen nicht weiter zu prüfende – Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (vgl. BVerfGE 141, 220 <282 Rn. 134> m.w.N.; stRspr). Ebenfalls muss die Datensicherheit gewährleistet werden (vgl. BVerfGE 155, 119 <182 Rn. 135>).

b) Für die verfassungsrechtliche Prüfung der Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist die Aufgabe des Gesetzgebers in den Blick zu nehmen, einen Ausgleich zwischen der Schwere der hier zur Prüfung stehenden Eingriffe in das Grundrecht auf informationelle Selbstbestimmung potentiell betroffener Personen und der Pflicht des Staates zum Schutz der Grundrechte anderer zu schaffen (vgl. BVerfGE 141, 220 <267 Rn. 98>). Der Gesetzgeber hat dabei auf der einen Seite das – mitunter erhebliche – Eingriffsgewicht der durch die angegriffenen Vorschriften erlaubten Erhebungs- und Weiterverarbeitungsmaßnahmen in Rechnung zu stellen. Erhebungsmaßnahmen können teilweise tief in die Privatsphäre eindringen. Weiterverarbeitungsmaßnahmen können zeitlich über die ursprünglichen Anlasszwecke hinausgehende sicherheitsbehördliche Wissensbestände über Einzelne schaffen und Möglichkeiten ihrer Verknüpfung eröffnen. Hierdurch können für das Persönlichkeitsrecht sensible Zusammenhänge betroffen sein, und dem damit verbundenen potentiell hohen Eingriffsgewicht ist in der Abwägung Rechnung zu tragen. Auf der anderen Seite hat der Gesetzgeber einen wirksamen Schutz der Grundrechte und Rechtsgüter der Bürgerinnen und Bürger zu sichern. Dabei ist zu berücksichtigen, dass die verfassungsmäßige Ordnung, der Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person Schutzgüter von hohem verfassungsrechtlichen Gewicht sind. Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm – unter Achtung von Würde und Eigenwert des Einzelnen – zu gewährleistende Sicherheit der Bevölkerung sind Rechtsgüter von überragendem verfassungsrechtlichen Gewicht (vgl. BVerfGE 154, 152 <249 Rn. 163>), die mit anderen hochwertigen Verfassungsgütern im gleichen Rang stehen. Der Staat ist deshalb verpflichtet, das Leben, die körperliche Unversehrtheit und die Freiheit des Einzelnen zu schützen, das heißt vor allem, auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren (vgl. BVerfGE 141, 220 <267 f. Rn. 100>; stRspr; zum Verhältnis von Freiheit und Sicherheit vgl. BVerfGE 154, 152 <226 Rn. 108>). 91

2. Alle zulässig angegriffenen Befugnisse sind zudem am Grundsatz der Bestimmtheit und Normenklarheit zu messen, der der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Verwaltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient (vgl. BVerfGE 113, 348 <375 ff.>; 156, 11 <44 Rn. 85>; 162, 1 <95 Rn. 199>; stRspr). 92

Bei der Bestimmtheit geht es vornehmlich darum, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle vornehmen können. Der Gesetzgeber ist gehalten, seine Regelungen so bestimmt zu fassen, wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist (vgl. BVerfGE 145, 20 <69 f. Rn. 125> m.w.N.). Dabei reicht es aus, wenn sich im Wege der Auslegung der einschlägigen Bestimmung mit Hilfe der anerkannten Auslegungsregeln feststellen lässt, ob die tatsächlichen Voraussetzungen für die in der Rechtsnorm ausgesprochene Rechtsfolge vorliegen. Verbleibende Unsicherheiten dürfen nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Norm ermächtigten staatlichen Stellen gefährdet sind (vgl. BVerfGE 134, 141 <184 Rn. 126>; 156, 11 <44 f. Rn. 85 ff.> m.w.N.). 93

Bei der Normenklarheit steht die inhaltliche Verständlichkeit der Regelung im Vordergrund, insbesondere damit Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können (vgl. BVerfGE 145, 20 <69 f. Rn. 125>). Weil die Grundrechte hier ohne Wissen der Bürgerinnen und Bürger und oft ohne die Erreichbarkeit gerichtlicher Kontrolle durch die Verwaltung, durch Polizei und Nachrichtendienste eingeschränkt werden, muss der Inhalt der einzelnen Norm verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein. So mag eine Regelung durch Auslegung bestimmbar oder der verfassungskonformen Auslegung zugänglich und damit im verfassungsrechtlichen Sinne bestimmt sein, jedoch geht damit nicht zwingend auch ihre Normenklarheit für die Adressaten einher (vgl. BVerfGE 163, 43 <83 Rn. 111>; 165, 1 <53 f. Rn. 97>; stRspr). 94

Bei der heimlichen Datenerhebung und -verarbeitung sind an die Bestimmtheit und Normenklarheit besonders strenge Anforderungen zu stellen. Im Einzelnen unterscheiden sich die Anforderungen maßgeblich nach dem Gewicht des Eingriffs und sind insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden (vgl. BVerfGE 141, 220 <265 Rn. 94>; 155, 119 <181 Rn. 133>; 162, 1 <95 Rn. 200, 125 f. Rn. 273> jeweils m.w.N.; stRspr). Bei heimlichen Überwachungsmaßnahmen, die weit in die Privatsphäre hineinreichen können, sind die Bestimmtheitsanforderungen indessen hoch (vgl. BVerfGE 162, 1 <95 Rn. 200>). Dies trägt dem Umstand Rechnung, dass ein effektiver Schutz gegenüber staatlicher Datenerhebung und -verarbeitung nur auf Grundlage eines ausreichend spezifischen gesetzlichen Normprogramms möglich ist. Heimliche Überwachungsmaßnahmen gelangen den Betroffenen kaum zur Kenntnis und können daher von ihnen nur selten im Rechtsweg angegriffen werden. Der Gehalt der gesetzlichen Regelung kann so nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit der jeweiligen Normen auffangen muss (vgl. BVerfGE 162, 1 <95 f. Rn. 200, 125 f. Rn. 273> m.w.N.). 95

IV.

§ 45 Abs. 1 Satz 1 Nr. 4 BKAG genügt in seiner konkreten Ausgestaltung nicht diesen verfassungsrechtlichen Anforderungen. 96

Die Regelung ermächtigt das Bundeskriminalamt zu heimlichen Überwachungsmaßnahmen gegenüber Personen, gegen die selbst kein Verdacht terroristischer Aktivitäten besteht, die aber in einem Näheverhältnis zu einer verantwortlichen Person stehen (Kontaktpersonen). Dabei ist der Einsatz besonderer in § 45 Abs. 2 BKAG aufgeführter Mittel erlaubt, so zum Beispiel längerfristige Observationen oder der Einsatz von Vertrauenspersonen und von verdeckt Ermittelnden. Für die näheren Voraussetzungen der Überwachung verweist § 45 Abs. 1 Satz 1 Nr. 4 BKAG auf § 39 Abs. 2 Nr. 2 BKAG. Dieser normiert Kriterien des Näheverhältnisses zwischen der Kontaktperson und der eigentlichen verantwortlichen Person und nimmt hinsichtlich der verantwortlichen Person auf § 39 Abs. 2 Nr. 1 BKAG Bezug. 97

Die durch die Befugnisnorm gestatteten Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) können erhebliches Gewicht haben (1). Grundsätzlich kann der Einsatz besonderer Mittel der Datenerhebung auch gegenüber Kontaktpersonen zur Abwehr entsprechend gewichtiger Gefahren verfassungsrechtlich gerechtfertigt sein. Im Ergebnis erfüllt die in § 45 Abs. 1 Satz 1 Nr. 4 BKAG vorgesehene Eingriffsschwelle jedoch nicht die Anforderungen der Verhältnismäßigkeit im engeren Sinne (2). 98

1. § 45 Abs. 1 Satz 1 Nr. 4, Abs. 2 BKAG ermächtigt das Bundeskriminalamt zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), die unterschiedlich schwer wiegen können. Während der Eingriff beim Erstellen einzelner Fotos oder bei einer zeitlich begrenzten schlichten Beobachtung eher geringes Gewicht haben kann, ist etwa eine langfristig dauerhafte heimliche Aufzeichnung des gesprochenen Worts und Bilds einer Person regelmäßig ein Eingriff von erheblicher Schwere (vgl. BVerfGE 141, 220 <290 Rn. 160>; 165, 1 <48 Rn. 88>). Insbesondere wenn die in § 45 Abs. 2 BKAG zugelassenen Maßnahmen gebündelt durchgeführt werden und dabei darauf zielen, möglichst alle Äußerungen und Bewegungen zu erfassen und bildlich wie akustisch festzuhalten, können sie tief in die Privatsphäre eindringen und ein besonders schweres Eingriffsgewicht erlangen (vgl. BVerfGE 141, 220 <286 f. Rn. 149 ff.>; 162, 1 <160 f. Rn. 357>). Der Einsatz von Vertrauenspersonen und verdeckt Ermittelnden kann auch im Hinblick auf das durch diese ausgenutzte Vertrauen sehr schwerwiegend sein (vgl. BVerfGE 141, 220 <289 f. Rn. 160>; 162, 1 <153 f. Rn. 340 f., 158 Rn. 351>). Eingriffsmindernd wirkt, dass die Überwachungsbefugnisse nach § 45 BKAG zeitlich befristet sind. So sieht § 45 Abs. 5 Satz 3 BKAG bei einer richterlichen Anordnung nach § 45 Abs. 3 BKAG eine zeitliche Begrenzung auf höchstens einen beziehungsweise drei Monate vor. Diese Anordnung kann zwar unbegrenzt oft verlängert werden, dies bedarf aber jeweils erneut richterlicher Anordnung (§ 45 Abs. 5 Satz 4 BKAG). 99

2. Die diesem Eingriffsgewicht entsprechenden verfassungsrechtlichen Anforderungen wahrt § 45 Abs. 1 Satz 1 Nr. 4 BKAG nicht. Die Vorschrift dient zwar einem legitimen Ziel und ist geeignet und erforderlich, um dieses zu erreichen (a). Nicht zu vereinbaren ist die Norm aber mit den besonderen Anforderungen, die sich aus der Verhältnismäßigkeit im engeren Sinne an die hier erforderliche Eingriffsschwelle ergeben (b). Dem kann durch eine verfassungskonforme Auslegung nicht begegnet werden (c). An diesem Ergebnis ändert auch der Richtervorbehalt nichts (d). 100

a) Die Befugnis des § 45 Abs. 1 Satz 1 Nr. 4 BKAG dient einem legitimen Ziel. Sie gibt dem Bundeskriminalamt Überwachungsmaßnahmen an die Hand, mit denen dieses seine Aufgabe der Abwehr von Gefahren des internationalen Terrorismus wahrnehmen soll. Der Begriff des internationalen Terrorismus ist dabei durch die Aufgabenbeschreibung des § 5 Abs. 1 Satz 2 BKAG und dessen Verweis auf § 129a Absätze 1 und 2 StGB definiert und – in Übereinstimmung mit den Vorstellungen des verfassungsändernden Gesetzgebers bei Schaffung des Art. 73 Abs. 1 Nr. 9a GG (vgl. BTDrucks 16/813, S. 12) – auf spezifisch charakterisierte Straftaten von besonderem Gewicht begrenzt. Straftaten mit dem Gepräge des Terrorismus in diesem Sinne zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes (vgl. BVerfGE 141, 220 <266 f. Rn. 96 f.>). Die Bereitstellung von wirksamen Überwachungsmaßnahmen zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (vgl. BVerfGE 133, 277 <333 f. Rn. 133>). 101

Die Einräumung der hier angegriffenen Überwachungsbefugnis ist zur Erreichung dieses Ziels geeignet. Sie gibt dem Bundeskriminalamt Überwachungsmaßnahmen an die Hand, die dazu beitragen können, den Gefahren des internationalen Terrorismus entgegenzutreten. Sie ist auch erforderlich. Mildere Mittel, die gleichermaßen effektiv die Abwehr des internationalen Terrorismus ermöglichten, sind nicht ersichtlich. Dies lässt freilich unberührt, dass auch die Anwendung der Befugnisse im Einzelfall dem Grundsatz der Geeignetheit und Erforderlichkeit zu folgen hat (vgl. BVerfGE 141, 220 <266 f. Rn. 97>). 102

b) Nicht zu vereinbaren ist § 45 Abs. 1 Satz 1 Nr. 4 BKAG aber mit den besonderen Anforderungen, die sich aus der Verhältnismäßigkeit im engeren Sinne an die Rechtfertigung heimlicher Überwachungsmaßnahmen der Polizei ergeben. Denn schon die in § 39 Abs. 2 Nr. 1 BKAG für die polizeirechtlich verantwortliche Person normierte Eingriffsschwelle rechtfertigte deren heimliche Überwachung mit besonders eingriffsintensiven Mitteln nach § 45 Abs. 2 BKAG nicht. Erst recht darf dann die selbst nicht verantwortliche Kontaktperson, die in einem Näheverhältnis zu dieser verantwortlichen Person steht, nicht mit derart eingriffsintensiven Methoden überwacht werden. 103

aa) Die dem Eingriffsgewicht der heimlichen Erhebungsbefugnisse entsprechenden Anforderungen der Verhältnismäßigkeit im engeren Sinne richten sich sowohl an das mit der Datenerhebung zu schützende Rechtsgut als auch an die vorliegend allein gerügte sogenannte Eingriffsschwelle, also den Anlass der Überwachung (vgl. auch BVerfGE 141, 220 <269 Rn. 104, 270 f. Rn. 106 ff., 271 ff. Rn. 109 ff.>; 162, 1 <84 f. Rn. 174>). Der Einsatz einer eingriffsintensiven heimlichen Überwachungsbefugnis wie der vorliegenden setzt schon gegenüber der verantwortlichen Person eine wenigstens konkretisierte Gefahr für ein hinreichend gewichtiges Rechtsgut voraus (1). Sollen auch Kontaktpersonen aus dem Umfeld der verantwortlichen Person mit derartigen Mitteln überwacht werden, bedarf es einer hinzutretenden spezifischen individuellen Nähe der Betroffenen zu der aufzuklärenden Gefahr (2). 104

(1) Die Erhebung von Daten durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität ist im Bereich der Gefahrenabwehr grundsätzlich nur verhältnismäßig im engeren Sinne, wenn eine Gefährdung der zu schützenden Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist (vgl. BVerfGE 141, 220 <271 Rn. 109>). Die verfassungsrechtliche Rechtfertigung verlangt hier, dass entweder eine konkrete Gefahr oder eine wenigstens konkretisierte Gefahr für ein hinreichend gewichtiges Rechtsgut besteht (vgl. dazu BVerfGE 141, 220 <271 ff. Rn. 111 ff.>). 105

Eine konkretisierte Gefahr setzt zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter voraus. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus, um den Eingriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens tragen, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt. Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen (BVerfGE 141, 220 <272 f. Rn. 112>; 165, 1 <49 ff. Rn. 90 ff.>; stRspr). 106

Dafür müssen grundsätzlich zwei Bedingungen erfüllt sein: Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfGE 141, 220 <272 f. Rn. 112> m.w.N.). Speziell in Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können die Anforderungen an die Erkennbarkeit des Geschehens weiter abgesenkt werden, wenn dafür bereits genauere Erkenntnisse über die beteiligten Personen bestehen: Hier gilt, dass 107

Überwachungsmaßnahmen auch dann erlaubt werden können, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, dafür aber das individuelle Verhalten einer Person bereits die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (vgl. BVerfGE 141, 220 <272 f. Rn. 112>; 165, 1 <50 f. Rn. 91>). Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist (BVerfGE 141, 220 <272 f. Rn. 112>).

Hingegen wird dem Gewicht eines Eingriffs durch heimliche polizeirechtliche Überwachungsmaßnahmen nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weiter in das Vorfeld einer in ihren Konturen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird. Eine Anknüpfung der Eingriffsschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn zu diesem Zeitpunkt nur relativ diffuse Anhaltspunkte für mögliche Rechtsgutsgefahren bestehen. Die Bedeutung einzelner Beobachtungen ist dann häufig vieldeutig. Die Geschehnisse können harmlos bleiben, aber auch den Beginn eines Vorgangs bilden, der in eine konkrete Gefahr oder gar eine Verletzung der tatbestandlich geschützten Rechtsgüter mündet. Solche Offenheit genügt für die Durchführung von eingriffsintensiven heimlichen Überwachungsmaßnahmen nicht (vgl. BVerfGE 141, 220 <273 Rn. 113>; 165, 1 <51 Rn. 92>). 108

(2) Besondere zusätzliche Anforderungen bestehen für die heimliche Überwachung von Kontaktpersonen, die nicht selbst polizeirechtlich verantwortlich sind. Zwar ist auch der Einsatz einer eingriffsintensiven Überwachungsmaßnahme wie der vorliegend in Rede stehenden unmittelbar gegenüber Kontaktpersonen nicht schlechthin ausgeschlossen. Er steht aber unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der die Überwachung der verantwortlichen Person rechtfertigenden aufzuklärenden Gefahr voraus (vgl. BVerfGE 141, 220 <273 f. Rn. 114 ff., 291 ff. Rn. 167 ff.>). 109

Unabhängig von der hier nicht gerügten spezifischen individuellen Nähe ist Voraussetzung der Überwachung von Kontaktpersonen, dass jedenfalls eine Überwachung der verantwortlichen Person mit entsprechenden Mitteln zulässig wäre. Denn andernfalls fehlte es bereits an einer hinreichenden aufzuklärenden Gefahr. Wenn also bereits die verantwortliche Person nicht mit eingriffsintensiven Maßnahmen überwacht werden darf, darf erst recht nicht die Kontaktperson auf diese Weise überwacht werden. 110

bb) Diesen Anforderungen an die Eingriffsschwelle genügt § 45 Abs. 1 Satz 1 Nr. 4 BKAG bereits hinsichtlich der notwendigen Gefahrnähe der in Bezug genommenen verantwortlichen Person nicht; erst recht darf deshalb eine nicht verantwortliche Kontaktperson nicht überwacht werden. 111

Die Vorschrift erlaubt die Datenerhebung hinsichtlich einer Kontaktperson nach § 39 Abs. 2 Nr. 2 BKAG, wenn diese in einer spezifischen Nähebeziehung zu einer verantwortlichen Person steht und die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. § 39 Abs. 2 Nr. 2 BKAG nimmt dabei Bezug auf eine verantwortliche Person nach § 39 Abs. 2 Nr. 1 BKAG. Nach § 39 Abs. 2 Nr. 1 BKAG genügt für eine Erhebung personenbezogener Daten, dass Tatsachen die Annahme rechtfertigen, dass diese Person „eine Straftat nach § 5 Absatz 1 Satz 2 begehen will und die erhobenen Daten zur Verhütung dieser Straftat erforderlich sind“. Damit bleiben die Anforderungen weit hinter den in § 45 Abs. 1 Satz 1 Nummern 1 bis 3 BKAG normierten Anforderungen für besondere Mittel der Datenerhebung bei verantwortlichen Personen zurück und sollen schon nach der gesetzlichen Konzeption nur für weniger eingriffsintensive Erhebungen gelten. Insbesondere müssen hier hinsichtlich der verantwortlichen Person nach § 39 Abs. 2 Nr. 1 BKAG im Gegensatz zur verantwortlichen Person nach § 45 Abs. 1 Satz 1 BKAG weder „bestimmte Tatsachen die Annahme rechtfertigen, dass sie [die Person] innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird“ (Nr. 2), noch muss „deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründe[n], dass sie [die Person] innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird“ (Nr. 3). 112

c) Eine für derart eingriffsintensive Maßnahmen hinreichende Eingriffsschwelle kann § 45 Abs. 1 Satz 1 Nr. 4 BKAG auch nicht im Wege der verfassungskonformen Auslegung entnommen werden (zu deren allgemeinen Voraussetzungen und Grenzen BVerfGE 122, 39 <60 ff.>). Insbesondere kann der Verweis in § 45 Abs. 1 Satz 1 Nr. 4 BKAG entgegen der Auffassung der Bundesregierung nicht dergestalt gedeutet werden, dass er sich auf eine verantwortliche Person nach § 45 Abs. 1 Satz 1 Nummern 1 bis 3 BKAG bezieht und nur die Tatnähekriterien des § 39 Abs. 2 Nr. 2 Buchstaben a bis c BKAG übernimmt. Eine solche Auslegung setzte voraus, dass sämtliche Anforderungen der Verfassung eingehalten würden. Dazu gehört hier, dass der Norm unter Beachtung des Grundsatzes der Bestimmtheit und Normenklarheit eine verfassungskonforme Eingriffsschwelle entnommen werden kann. 113

aa) Der Annahme einer solchen Eingriffsschwelle steht schon der insoweit eindeutige Wortlaut entgegen. Nichts anderes ergibt sich aus der systematischen Auslegung. Dass die Adressatengruppen des § 45 Abs. 1 Satz 1 Nummern 1 bis 4 BKAG durch ein gemeinsames Tatbestandsmerkmal („wenn die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre“) „verklammert“ werden, lässt nicht die Folgerung zu, dass Nr. 4 als eine Adressatengruppe auch auf die anderen Adressatengruppen in Nummern 1 bis 3 Bezug nehmen soll. Auch das systematische Verhältnis von § 39 BKAG als allgemeiner Befugnis zur Erhebung personenbezogener Daten zu § 45 BKAG als spezieller Vorschrift für besondere Mittel der Datenerhebung vermag einen solchen Zusammenhang nicht herzustellen. Dies gilt umso mehr, als der Gesetzgeber an 114

anderer Stelle im Bundeskriminalamtgesetz den Bezug zur verantwortlichen Person unmissverständlich normiert hat (vgl. etwa § 47 Abs. 2 Nr. 3 BKAG sowie § 65 Abs. 1 Nr. 3 BKAG und § 19 Abs. 1 Satz 1 Nr. 3 BKAG).

Der Wille des Gesetzgebers, der im Vergleich zur Altfassung nur redaktionelle Folgeänderungen beabsichtigt hat (vgl. BTDrucks 18/11163, S. 113 f.), hat deshalb in der Vorschrift keinen hinreichenden Niederschlag gefunden (vgl. auch Schulenberg, in: Barczak, BKAG, 2023, § 45 Rn. 74). Es mag zwar zutreffen, dass die eingeschränkte Bedeutung des Verweises dem Bundeskriminalamt bekannt ist und die Vorschrift in der Praxis entsprechend angewendet wird. Jedoch ist für die verfassungsrechtliche Beurteilung einer Erhebungsbefugnis nicht die (derzeitige) Behördenpraxis maßgeblich, sondern die rechtliche Ausgestaltung (vgl. auch BVerfGE 162, 1 <147 Rn. 326>). Der Einsatz grundrechtsintensiver Überwachungsbefugnisse bedarf von Verfassungs wegen hinreichender Anbindung an Maßgaben des Rechts, die dem demokratischen Gesetzgebungsverfahren entspringen (vgl. BVerfGE 154, 152 <238 f. Rn. 139>; 162, 1 <97 Rn. 203 f.; 144 f. Rn. 322>). 115

bb) Im Wege der Auslegung der Norm eine den verfassungsrechtlichen Anforderungen genügende Eingriffsschwelle zu entnehmen, wäre hier jedenfalls mit dem Grundsatz der Bestimmtheit und Normenklarheit bei heimlichen Überwachungsmaßnahmen nicht zu vereinbaren. Da § 45 Abs. 1 Satz 1 Nr. 4 BKAG heimliche Datenerhebungen ermöglicht, die tief in die Privatsphäre einwirken können, gelten insoweit besonders strenge Anforderungen. Weil heimliche Überwachungsmaßnahmen den Betroffenen kaum zur Kenntnis gelangen und daher auch nur selten angegriffen werden, kann der Gehalt der gesetzlichen Regelung nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit auffangen muss (vgl. BVerfGE 162, 1 <126 Rn. 273>; oben Rn. 95). Dem genügte jedenfalls eine wie hier normtextkorrigierende Auslegung nicht. 116

d) Auch der in § 45 Abs. 3 BKAG überwiegend angeordnete Richtervorbehalt ist nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen (vgl. BVerfGE 110, 33 <67 f.>; 120, 274 <331 f.>). 117

V.

Soweit die Verfassungsbeschwerde sich gegen § 16 Abs. 1 BKAG wendet, bestehen keine durchgreifenden verfassungsrechtlichen Bedenken gegen die Vorschrift. 118

§ 16 Abs. 1 BKAG ermächtigt das Bundeskriminalamt zur Weiterverarbeitung personenbezogener Daten in seinem Informationssystem, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und das Bundeskriminalamtgesetz keine zusätzlichen besonderen Voraussetzungen vorsieht. 119

Der Begriff der Weiterverarbeitung wird im Bundeskriminalamtgesetz und auch in den allgemeinen datenschutzrechtlichen Normen im Gegensatz zum Begriff der Verarbeitung (vgl. § 46 Nr. 2 BDSG sowie Art. 3 Nr. 2 JI-RL) nicht legaldefiniert. Das Bundeskriminalamtgesetz unterscheidet innerhalb der allgemeinen Befugnisse zur Datenverarbeitung (Abschnitt 2) zwischen der Datenerhebung (§ 9 - § 11 BKAG), der Weiterverarbeitung von Daten (§ 12 - § 24 BKAG) und der Datenübermittlung (§ 25 - § 28 BKAG). Nach Wortlaut und Systematik erfasst der Begriff der Weiterverarbeitung die Datenerhebung und Datenübermittlung nicht, die jeweils speziell geregelt sind (vgl. auch Eichenhofer, in: Barczak, BKAG, 2023, § 16 Rn. 5). Dieses rechtssystematische Verständnis findet sich auch in der Begründung des Gesetzesentwurfs wieder. Da der einheitliche Begriff der Verarbeitung weit konzipiert sei und insbesondere die Datenerhebung, die Datenübermittlung, die Einschränkung der Datenverarbeitung und das Löschen der Daten umfasse (vgl. § 46 Nr. 2 BDSG), bedürfe es einer Einschränkung. Der Begriff der Weiterverarbeitung solle aus rechtssystematischen Gründen diese Verarbeitungsschritte nicht erfassen. Allerdings fielen unter ihn die übrigen Aspekte der Verarbeitung wie die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung von Daten (vgl. BTDrucks 18/11163, S. 90). 120

Diese Weiterverarbeitung geschieht im Rahmen des § 16 Abs. 1 BKAG nach Maßgabe des § 12 BKAG. Die Rüge bezieht sich allein auf die Weiterverarbeitung personenbezogener Daten, die das Bundeskriminalamt zuvor mit besonders eingriffsintensiven Mitteln nach § 45 BKAG erhoben hat und im Rahmen der Aufgabenerfüllung zur Abwehr von Gefahren des internationalen Terrorismus nach § 5 BKAG verarbeitet. Gerügt ist ohnehin nur die Weiterverarbeitung nach Maßgabe von § 12 Abs. 1 Satz 1 BKAG, also die Weiterverarbeitung der Daten im Rahmen ihrer ursprünglichen Zwecke. 121

In diesem Umfang erlaubt die Befugnis Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) von erheblichem Gewicht. Sie wahrt aber die verfassungsrechtlichen Vorgaben der Verhältnismäßigkeit im engeren Sinne an eine weitere Nutzung von Daten. 122

1. Soweit § 16 Abs. 1 BKAG gerügt ist, wirkt eingriffsverstärkend, dass die verarbeiteten Daten zuvor mit eingriffsintensiven Überwachungsmethoden nach § 45 Abs. 2 BKAG erhoben wurden (a). Das Eingriffsgewicht wird allerdings nicht dadurch weiter erhöht, dass besonders eingriffsintensive Verarbeitungsmethoden wie beispielsweise eine algorithmenbasierte automatisierte Datenanalyse gestattet wären; es wird vielmehr dadurch gemindert, dass vorliegend nur eine zweckwahrende Verarbeitung nach Maßgabe von § 12 Abs. 1 BKAG verfahrensgegenständlich ist (b). 123

a) Das Eingriffsgewicht von Datenweiterverarbeitungsbefugnissen richtet sich zunächst nach dem Gewicht der vorausgegangenen Datenerhebungseingriffe (vgl. BVerfGE 165, 363 124

<390 Rn. 54>). Dieses ist umso höher, je eingriffsintensiver die zugrundeliegende Erhebungsmaßnahme war (vgl. zur Abstufung anhand der Eingriffsintensität BVerfGE 141, 220 <269 f. Rn. 105 ff.>). Eingriffsintensivierend wirkt damit vorliegend, dass die personenbezogenen Daten in einem ersten Schritt durch das Bundeskriminalamt im Wege heimlich durchgeführter Befugnisse erhoben wurden, die dabei tief in die Privatsphäre hineinreichen können und berechtigte Vertraulichkeitserwartungen berühren können. Auch wenn sich das Eingriffsgewicht der Erhebungsbefugnisse im Einzelnen unterscheidet, wiegt dieses in der Regel jedenfalls schwer (vgl. BVerfGE 141, 220 <264 f. Rn. 92>; vgl. dazu bereits oben Rn. 99).

b) Für die Feststellung des Eingriffsgewichts ist überdies die Art der Datennutzung von Bedeutung, insbesondere, wie die gewonnenen personenbezogenen Informationen weiterverwendet werden und welche Folgen dies für die Betroffenen haben kann (vgl. BVerfGE 65, 1 <45 f.>; 155, 119 <178 f. Rn. 129>; 165, 363 <407 f. Rn. 99> m.w.N.). Insoweit ist das Eingriffsgewicht von § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG dadurch begrenzt, dass die Vorschrift allein die Weiterverarbeitung der Daten im Rahmen ihrer ursprünglichen Zwecke ermöglicht. 125

Die Vorschrift ermächtigt aber nicht zu besonders eingriffsintensiven Verarbeitungsmethoden, was das Eingriffsgewicht erhöhen könnte. Zwar schließt allein der Begriff der Weiterverarbeitung seinem Wortlaut nach auch besonders eingriffsintensive Auswertungsmethoden nicht von vornherein aus. Auch bestimmt allein die bloße Vorstellung des Gesetzgebers von der Reichweite der Befugnis nicht deren Eingriffsgewicht (vgl. BVerfGE 162, 1 <147 Rn. 326>). Allerdings hat der Gesetzgeber § 16 Abs. 1 BKAG erkennbar als Generalermächtigung formuliert (vgl. BTDrucks 18/11163, S. 97: „Grundnorm“; Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 16 BKAG Rn. 8), deren Anwendbarkeit durch ihren letzten Halbsatz auch ausdrücklich dahin eingeschränkt wird, dass spezielle Weiterverarbeitungsbefugnisse vorgehen, die ihrerseits an eigenständige Vorgaben geknüpft und durch diese begrenzt sein können. Eine solche Regelungstechnik ist aus dem allgemeinen Polizeirecht hinsichtlich der offen gefassten polizei- und ordnungsrechtlichen Generalermächtigungen bekannt und verfassungsrechtlich im Ausgangspunkt nicht zu beanstanden. 126

Auf eine solchermaßen formulierte Generalklausel dürfen jedoch grundsätzlich nicht solche Eingriffe gestützt werden, die eine erhöhte Eingriffsintensität aufweisen und daher die Schaffung einer speziellen Ermächtigungsgrundlage erfordern. Dies wäre bei einer automatisierten Datenanalyse und -auswertung der Fall, weil diese ein Eigengewicht aufweist, das schon wegen der spezifischen verfassungsrechtlichen Rechtfertigungsanforderungen einer speziellen Ermächtigungsgrundlage bedürfte (vgl. BVerfGE 165, 363 <389 f. Rn. 54, 395 ff. Rn. 66 ff., 400 Rn. 77>). Denn eine automatisierte Datenanalyse und -auswertung ermöglicht breitere und tiefere Erkenntnisse über Personen, kann eine spezifische Fehler- und Diskriminierungsanfälligkeit aufweisen und softwaregestützte Verknüpfungen 127

schwer nachvollziehbar werden lassen (vgl. zu Risiken, aber auch Potenzialen BVerfGE 165, 363 <400 ff. Rn. 77 ff.>). Es ist deshalb davon auszugehen, dass § 16 Abs. 1 BKAG keine Verarbeitungsmethoden mit derartigem potenziellen grundrechtlichen Eigengewicht umfasst.

2. § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG wahrt mit diesem Normverständnis die verfassungsrechtlichen Anforderungen. Die Befugnis dient einem legitimen Ziel und ist zu dessen Erreichung geeignet und erforderlich (a). Auch ist sie mit den Anforderungen der Verhältnismäßigkeit im engeren Sinne für eine zweckwahrende Weiterverarbeitung personenbezogener Daten vereinbar (b). 128

a) § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG dient einem legitimen Ziel. Die Vorschrift erlaubt dem Bundeskriminalamt eine Verwendung der von ihm zur Abwehr von Gefahren des internationalen Terrorismus im Sinne des § 5 Abs. 1 Satz 2 BKAG erhobenen personenbezogenen Daten zur Wahrnehmung derselben Aufgabe. Ebenso wie die Bereitstellung von wirksamen Aufklärungsmitteln dient auch die Möglichkeit der Datenweiterverarbeitung einem legitimen Ziel und ist für die demokratische und freiheitliche Ordnung von großem Gewicht (dazu oben Rn. 101 f.; vgl. BVerfGE 133, 277 <333 f. Rn. 133>). 129

Die Befugnis ist auch geeignet, da sie dazu beitragen kann, den Gefahren des internationalen Terrorismus wirkungsvoll entgegenzutreten, indem die gewonnenen Kenntnisse auch als Ausgangspunkt für weitere Ermittlungen genutzt werden können. Sie ist zudem erforderlich, weil durch die zweckwahrende Datenweiterverarbeitung relevante Erkenntnisse zur Abwehr des internationalen Terrorismus gewonnen werden können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu erlangen wären. 130

b) § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG ist auch mit dem Grundsatz der Verhältnismäßigkeit im engeren Sinne vereinbar. Dem Eingriffsgewicht für die Betroffenen steht das gewichtige öffentliche Interesse gegenüber, für die Aufklärung und Bekämpfung des internationalen Terrorismus eine effektive Datenweiterverarbeitung zu ermöglichen. 131

Die aus dem Eingriffsgewicht folgenden verfassungsrechtlichen Rechtfertigungsanforderungen der Weiterverarbeitung ergeben sich im Ausgangspunkt aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe; insoweit gelten die Grundsätze der Zweckbindung und Zweckänderung (vgl. BVerfGE 141, 220 <324 Rn. 276>; 165, 363 <390 Rn. 54>). Regelmäßig wird so die Verhältnismäßigkeit im engeren Sinne des in der Weiterverarbeitung bereits erhobener Daten liegenden Grundrechtseingriffs gesichert (vgl. BVerfGE 165, 363 <397 Rn. 70>). Vorliegend bedarf es keiner darüber hinausgehenden Rechtfertigungsanforderungen, die etwa für besonders eingriffsintensive Verarbeitungsbefugnisse zu fordern wären (vgl. BVerfGE 165, 363 <389 f. Rn. 54, 395 ff. Rn. 66 ff.>). 132

aa) Erlaubt der Gesetzgeber die Nutzung solcher Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus, muss er hierfür eine eigene Rechtsgrundlage schaffen (vgl. BVerfGE 141, 220 <324 Rn. 277>; stRspr). Dabei kann er insbesondere die weitere Nutzung der Daten im Rahmen der ursprünglichen Zwecke erlauben. Eine solche Nutzung kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung, sondern lediglich denen an die zweckwahrende Weiternutzung (vgl. BVerfGE 141, 220 <324 ff. Rn. 278 ff.> m.w.N.; 162, 1 <107 Rn. 227>; 165, 363 <390 f. Rn. 57>). 133

Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt die zur Datenerhebung ermächtigte Behörde, den Zweck und die Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine Zweckänderung eine weitergehende Nutzung erlaubt (vgl. BVerfGE 141, 220 <324 f. Rn. 279>; 165, 363 < 390 f. Rn. 57>). 134

Nicht zu den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten je neu beachtet werden müssen, gehören grundsätzlich die für die Datenerhebung maßgeblichen Anforderungen an Eingriffsschwellen, wie sie die hinreichend konkretisierte Gefahrenlage im Bereich der Gefahrenabwehr und ein qualifizierter Tatverdacht im Bereich der Strafverfolgung darstellen. Das Erfordernis einer hinreichend konkretisierten Gefahrenlage oder eines qualifizierten Tatverdachts bestimmt den Anlass, aus dem entsprechende Daten erhoben werden dürfen, nicht aber die erlaubten Zwecke, für die die Daten der Behörde dann zur Nutzung offenstehen (vgl. BVerfGE 141, 220 <325 Rn. 280>). Folglich widerspricht es nicht von vornherein dem Gebot einer dem ursprünglichen Erhebungszweck entsprechenden Verwendung, wenn die weitere Nutzung solcher Daten bei Wahrnehmung derselben Aufgabe auch unabhängig von weiteren gesetzlichen Voraussetzungen als Spurenansatz erlaubt wird. Die Behörde kann die insoweit gewonnenen Erkenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – allgemein und damit unabhängig von konkreten Gefahren oder konkreten Ermittlungsansätzen als Ausgangspunkt für weitere Ermittlungen nutzen. Dies trägt dem 135

Umstand Rechnung, dass sich die Generierung von Wissen – nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen geht – nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lässt. Damit ist keine Datennutzung ins Blaue hinein eröffnet. Vielmehr hat auch eine Verwendung der Daten als Spurenansatz durch die Bindung an die für die Datenerhebung maßgeblichen Aufgaben und die Anforderungen des Rechtsgüterschutzes einen hinreichend konkreten Ermittlungsbezug, den der Gesetzgeber nicht durch weitere einschränkende Maßgaben absichern muss (vgl. BVerfGE 141, 220 <325 f. Rn. 281>; 165, 363 <391 f. Rn. 58>). Die Einhaltung des verfassungsrechtlichen Grundsatzes der Zweckbindung sichert dabei, dass es einen hinreichenden Eingriffsanlass gibt (vgl. BVerfGE 165, 363 <412 Rn. 108>). Die Nutzung als Spurenansatz kann zwar bereits mit Blick auf einen nur potentiellen Informationsgehalt zugelassen werden (vgl. BVerfGE 141, 220 <336 f. Rn. 313>), muss aber immer auf einer Prüfung im Einzelfall basieren und darf nicht etwa dazu dienen, ins Blaue hinein sachliche Anhaltspunkte für eine künftige Begehung von Straftaten überhaupt erst zu generieren (vgl. BVerfGE 165, 363 <432 Rn. 158>). Diese Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung zu legitimieren (BVerfGE 141, 220 <326 Rn. 282>).

Weiter reicht die Zweckbindung allerdings für – vorliegend aufgrund der beschränkten Rüge nicht verfahrensgegenständliche – Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede weitere Nutzung der Daten, auch seitens derselben Behörde im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten, nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. dazu BVerfGE 162, 1 <134 Rn. 297> m.w.N.) oder im Einzelfall zumindest hinreichend konkretisierten Gefahr (vgl. dazu BVerfGE 141, 220 <272 f. Rn. 112>) erforderlich ist (vgl. BVerfGE 141, 220 <326 Rn. 282>; 165, 363 <392 Rn. 59>). 136

bb) Der Gesetzgeber kann eine weitere Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung); als Ermächtigung zu einer Datennutzung für neue Zwecke unterliegt sie den im Urteil des Bundesverfassungsgerichts vom 20. April 2016 formulierten verfassungsrechtlichen Anforderungen an die zweckändernde Weiternutzung von Daten (vgl. BVerfGE 141, 220 <326 ff. Rn. 284 ff.> m.w.N.; siehe auch BVerfGE 165, 363 <392 ff. Rn. 60 ff.>). 137

Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken genutzt werden. Als Maßstab der Verhältnismäßigkeitsprüfung gilt insoweit das Kriterium der hypothetischen Datenneuerhebung. Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften. Voraussetzung für eine Zweckänderung ist danach, dass die 138

neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrads der Gefahrenlage oder des Tatverdachts, also hinsichtlich der Eingriffsschwelle. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend ist insoweit, dass sich aus den Daten ein konkreter Ermittlungsansatz ergibt (vgl. BVerfGE 141, 220 <326 ff. Rn. 284 ff.>; 165, 363 <393 Rn. 61 f.>).

Der konkrete Ermittlungsansatz in diesem Sinne ist ein einzelfallbezogener tatsächlicher Anlass, der sich aus den Daten selbst oder in Verbindung mit weiteren Erkenntnissen der Behörde ergeben muss (vgl. BVerfGE 141, 220 <328 f. Rn. 289, 336 f. Rn. 313>). Allgemeine kriminologische Erwägungen oder Erfahrungssätze reichen daher für sich genommen nicht aus. Vielmehr müssen sich aus den Informationen zureichende tatsächliche Anhaltspunkte für eine Straftatenbegehung oder -aufdeckung ergeben (vgl. BVerfGE 141, 220 <349 Rn. 348>). Der tatsachengestützte Ermittlungsansatz muss hinreichend spezifisch sein, um Rückschlüsse auf eine Straftat von vergleichbarem Gewicht zu ermöglichen, wie sie der ursprünglichen Datenerhebung zugrunde lag, da andernfalls die Einhaltung der Grundsätze der Zweckänderung nicht überprüft werden könnte (vgl. BVerfGE 141, 220 <328 f. Rn. 289, 336 f. Rn. 313>). Dies entspricht für die Strafverfolgung im Wesentlichen dem Anfangsverdacht im strafprozessualen Sinne (vgl. BVerfGE 155, 119 <190 Rn. 153>; vgl. Schulenberg, in: Barczak, BKAG, 2023, § 12 Rn. 123 f.; Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 257). Im Bereich der Gefahrenabwehr müssen die Informationen im Einzelfall die Annahme einer zumindest auf mittlere Sicht drohenden Gefahr tragen (vgl. BVerfGE 141, 220 <328 f. Rn. 289 f.>; vgl. Schulenberg, in: Barczak, BKAG, 2023, § 12 Rn. 30). Anderes gilt allerdings wie bei der zweckwahrenden Weiterverarbeitung auch hier für Informationen aus Wohnraumüberwachungen oder aus dem Zugriff auf informationstechnische Systeme (siehe oben Rn. 136; vgl. BVerfGE 165, 363 <394 Rn. 64>). 139

cc) Besondere Bedeutung kommt den Löschungsvorgaben zu, mit deren Hilfe der Gesetzgeber die Zweckbindung der Weiterverarbeitungsbefugnisse sichert. Die Regelung von Löschungspflichten gehört zu den übergreifenden Verhältnismäßigkeitsanforderungen. Mit solchen Vorgaben wird gewährleistet, dass eine Verwendung personenbezogener Daten auf die die Datenverarbeitung rechtfertigenden Zwecke begrenzt bleibt und nach Erledigung nicht mehr möglich ist (vgl. BVerfGE 141, 220 <285 f. Rn. 144>). Grundsätzlich sind die erhobenen Daten zu löschen, sobald sie für die festgelegten Zwecke oder den gerichtlichen Rechtsschutz der Betroffenen nicht mehr benötigt werden (BVerfGE 150, 1 <108 Rn. 222>). Die Löschung der Daten ist zur Gewährleistung von Transparenz und Kontrolle zu protokollieren (vgl. BVerfGE 141, 220 <286 Rn. 144>; 154, 152 <265 Rn. 210>). 140

Auch im Falle einer zweckwahrenden Weiterverarbeitung sind die erhobenen Daten daher grundsätzlich zu löschen, nachdem der unmittelbare Anlassfall abgeschlossen und damit der der Erhebungsmaßnahme zugrundeliegende konkrete Zweck erfüllt ist. Danach ist eine zweckwahrende Verarbeitung nicht mehr zulässig. Dies sichern Löschvorschriften ab. Ein Absehen von einer Löschung über den unmittelbaren Anlassfall hinaus kommt nur in Betracht, soweit sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – zwischenzeitlich ein konkreter Ermittlungsansatz ergeben hat (vgl. BVerfGE 141, 220 <322 f. Rn. 270>) und damit die Voraussetzungen einer zweckändernden Nutzung vorliegen (siehe vorstehend Rn. 137 ff.; zur Ausnahme der vorsorgenden Speicherung unter engen Voraussetzungen, Rn. 152 ff.). 141

3. Ausgehend von den vorstehenden Maßstäben genügt die zweckwahrende Verarbeitung („weitere Nutzung“) personenbezogener Daten, die zuvor mit besonders eingriffsintensiven Mitteln des § 45 Abs. 2 BKAG erhoben worden sind, nach § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG in Zusammenschau mit den gesetzlichen Löschungsvorgaben den verfassungsrechtlichen Anforderungen. 142

a) Die Eingriffsbefugnis wahrt die verfassungsrechtlichen Anforderungen an eine zweckwahrende Nutzung. Denn soweit die Weiterverarbeitung personenbezogener Daten gerügt ist, die zuvor nach § 45 BKAG erhoben worden sind, sichern die Vorgaben des § 12 Abs. 1 Satz 1 BKAG neben der Identität der erhebenden und verarbeitenden Behörde (Bundeskriminalamt), dass die Weiterverarbeitung nur zur Erfüllung derselben Aufgabe (§ 5 Abs. 1 Satz 1 und 3 BKAG) und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten (§ 5 Abs. 1 Satz 2 BKAG) erfolgt. 143

Dass § 12 Abs. 1 Satz 1 BKAG nicht ausdrücklich im Sinne einer Mindestanforderung auf eine Nutzung der Daten als Spurenansatz verweist oder die Nutzung an eine anderweitige Verarbeitungsschwelle knüpft, ist unbedenklich. Denn § 16 Abs. 1 BKAG setzt voraus, dass die Weiterarbeitung „erforderlich“ sein muss, was gewährleistet, dass die Daten nicht unter der Schwelle im Sinne eines Spurenansatzes mit hinreichendem Ermittlungsbezug genutzt werden können (vgl. auch BVerfGE 165, 363 <432 Rn. 158>). Die in § 12 Abs. 1 Satz 1 BKAG niedergelegten Grenzen der zweckwahrenden Weiterverarbeitung gewährleisten zugleich, dass keine Datennutzung ins Blaue hinein eröffnet ist (vgl. BVerfGE 141, 220 <325 f. Rn. 281>; 165, 363 <412 Rn. 108>). 144

Die verfassungsrechtlichen Vorgaben werden auch gewahrt, soweit das Bundeskriminalamt im Rahmen dieser gesetzlichen Vorgaben die zur Abwehr des internationalen Terrorismus erhobenen personenbezogenen Daten so lange zweckwahrend weiterverarbeiten kann, wie der der Datenerhebung zugrundeliegende konkrete Gefahrenabwehrvorgang noch nicht abgeschlossen ist (vgl. zu den konkreten Löschungsvorgaben sogleich 145

Rn. 148 ff.). Denn auf diese Weise kann dem gewichtigen Bedürfnis einer effektiven Terrorismusabwehr durch eine adäquate Bestimmung des Zwecks der Maßnahme Rechnung getragen werden.

Der konkrete Zweck kann dabei in Abhängigkeit von der jeweiligen Aufgabe, dem Ermittlungsstand und der Abgrenzbarkeit der Verfahren festgelegt werden. Der Zweck eines Gefahrenabwehrvorgangs muss etwa nicht auf eine Tat im strafprozessualen Sinne (vgl. §§ 155, 264 StPO) beschränkt sein, sondern kann bei terroristischen Gefahren auch in der Bekämpfung einer komplexen kriminellen Struktur – etwa der Zerschlagung einer bestimmten terroristischen Gruppierung – bestehen, muss aber immer den Anforderungen der die Datenerhebung legitimierenden Ermächtigungsgrundlage gerecht werden. 146

Dementsprechend erfolgt nach den Ergebnissen der mündlichen Verhandlung und nach den schriftlichen Stellungnahmen der Abschluss eines Gefahrenabwehrvorgangs ebenso wie dessen Eröffnung durch einen formalen Akt. Ein laufender Vorgang im Rahmen der Abwehr des internationalen Terrorismus nach § 5 BKAG kann komplexe Sachverhalte umfassen und sich über einen gewissen Zeitraum erstrecken, was sich aus den Besonderheiten terroristischer Strukturen und dem praktischen Bedürfnis ergibt, diese aufzuklären (vgl. BVerfGE 141, 220 <325 f. Rn. 281>). Während des laufenden Gefahrenabwehrvorgangs können die insoweit gewonnenen Erkenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung als Ausgangspunkt für weitere Ermittlungen dienen, die insbesondere zu einem konkreten Ermittlungsansatz für die Eröffnung eines neuen Gefahrenabwehrvorgangs führen können, der die Voraussetzungen einer zweckändernden Weiterverarbeitung nach § 12 Abs. 2 BKAG erfüllen kann. 147

b) Der Gesetzgeber hat durch Löschungsvorgaben sichergestellt, dass bei einer Weiterverarbeitung nach § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG der Grundsatz der Zweckbindung gewahrt wird. 148

In Bezug auf die angegriffene Befugnisnorm ergeben sich die Vorgaben zur Löschung personenbezogener Daten gemäß § 1 Abs. 1 Satz 1 Nr. 1, Abs. 2 Satz 1 und 2 BDSG unmittelbar aus § 75 Abs. 2 BDSG, der wiederum durch § 77 BKAG ergänzt und konkretisiert wird (vgl. BTDrucks 18/11163, S. 131). § 79 BKAG hat daneben eine spezifisch klarstellende Auffangfunktion für personenbezogene Daten, die mit Maßnahmen zur Abwehr von Gefahren des internationalen Terrorismus oder vergleichbaren Maßnahmen erlangt wurden (vgl. Wilhelm-Robertson, in: Barczak, BKAG, 2023, § 79 Rn. 1-3; s.a. Ruthig, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BKAG, § 77 Rn. 2, § 79 Rn. 1). Bei § 77 BKAG und § 75 BDSG handelt sich um nationale Ausformungen der datenschutzrechtlichen Grundsätze der Datenminimierung und Speicherbegrenzung, die auf unionaler Ebene durch Art. 4 Abs. 1 Buchstaben c und d, Art. 16 JI-Richtlinie aufgestellt werden (vgl. BTDrucks 18/11325, S. 119; Burghardt/Reinbacher, in: BeckOK-DatenschutzR, 149

46. Ed. Stand: 01.05.2023, § 75 BDSG Rn. 1; Nolte/Werkmeister, in: Gola/Heckmann, DSGVO - BDSG, 3. Aufl. 2022, § 75 BDSG Rn. 1).

Gemäß § 77 Abs. 1 Satz 1 BKAG, § 75 Abs. 2 BDSG und § 79 Abs. 1 Satz 1 BKAG sind personenbezogene Daten unverzüglich zu löschen, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist beziehungsweise wenn sie zur Erfüllung des der Erhebungsmaßnahme zugrundeliegenden Zwecks nicht mehr erforderlich sind. Dies verweist auf die verfassungsrechtlichen Grundsätze zur Zweckbindung und genügt den verfassungsrechtlichen Anforderungen (vgl. BVerfGE 141, 220 <322 f. Rn. 270>; 155, 119 <231 f. Rn. 258 f.>). Entsprechend gibt § 77 Abs. 1 Satz 1 BKAG eine Erforderlichkeitsprüfung jedenfalls bei der Einzelfallbearbeitung, spätestens aber periodisiert nach Aussonderungsprüffristen (vgl. dazu BVerfGE 141, 220 <323 Rn. 270>) vor, deren Beachtung durch technische Maßnahmen zu gewährleisten ist (§ 77 Abs. 1 Satz 3 BKAG). 150

Der Grundsatz der Zweckwahrung wird durch § 79 Abs. 1 Satz 1 a.E. BKAG hinreichend gesichert. Danach sind die Daten ausdrücklich nur zu löschen, soweit keine Weiterverarbeitung der Daten nach den Vorschriften des Abschnitts 2 Unterabschnitt 2 erfolgt, zu denen § 16 Abs. 1 BKAG gehört. Die Ergänzung stellt klar, dass eine Löschung über den Anlassfall hinaus bei einer „zulässigen Weiterverarbeitung“ (BTDrucks 18/11163, S. 132; vgl. auch Ruthig, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BKAG, § 79 Rn. 2 f.; Wilhelm-Robertson, in: Barczak, BKAG, 2023, § 79 Rn. 3) unterbleibt, etwa unter Einhaltung der Voraussetzungen für die zweckändernde Weiterverarbeitung nach § 16 Abs. 1 in Verbindung mit § 12 Abs. 2 BKAG (vgl. zu § 20v Abs. 6 Satz 1 BKAG a.F. BVerfGE 141, 220 <322 f. Rn. 270>; vgl. BTDrucks 18/11163, S. 132). Mit Blick auf die zweckwahrende weitere Verwendung der Daten gemäß § 16 Abs. 1 in Verbindung mit § 12 Abs. 1 Satz 1 BKAG kommt ein Absehen von einer Löschung nach Erfüllung des der Erhebungsmaßnahme zugrundeliegenden konkreten Zwecks deshalb nur insoweit in Betracht, als sich aus den Daten konkrete Ermittlungsansätze für die Abwehr von Gefahren des internationalen Terrorismus ergeben (vgl. BVerfGE 141, 220 <322 f. Rn. 270>). 151

VI.

§ 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1, soweit dieser in Verbindung mit § 13 Abs. 3, § 29 BKAG die Speicherung zuvor erhobener personenbezogener Grunddaten durch das Bundeskriminalamt im polizeilichen Informationsverbund erlaubt, genügt dagegen nicht den verfassungsrechtlichen Anforderungen. 152

§ 18 Absätze 1 und 2 in Verbindung mit § 13 Abs. 3, § 29 BKAG erlaubt dem Bundeskriminalamt zur Erfüllung seiner Aufgaben nach § 2 Absätze 1 bis 3 BKAG im polizeilichen Informationsverbund, näher bestimmte personenbezogene Daten verschiedener Personenkategorien weiterzuverarbeiten (vgl. zum Begriff Rn. 120). Hier zur Prüfung steht nur die Bereitstellung der Daten in dem Informationsverbund, nicht aber der § 29 Abs. 4 Satz 2 BKAG 153

unterfallende Zugriff auf diese Daten. Nach § 2 Absätze 1 bis 3 BKAG unterstützt das Bundeskriminalamt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung und unterhält als Zentralstelle einen einheitlichen polizeilichen Informationsverbund als Grundlage für die Datenweiterverarbeitung (vgl. oben Rn. 18).

Ungeachtet des tatbestandlich weiten Anwendungsbereichs von § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG ist die Prüfung vorliegend beschränkt. Nicht gegenständlich ist die Weiterverarbeitung solcher personenbezogener Daten, die zuvor mittels einer Wohnraumüberwachung oder Online-Durchsuchung gewonnen worden sind. Inwieweit die verfassungsrechtlichen Anforderungen an eine der Speicherung nachfolgende Verwendung der personenbezogenen Daten hier eingehalten sind, muss offen bleiben, da dies nicht zulässig gerügt worden ist. 154

Die durch § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG eröffnete Befugnis zur Speicherung erlaubt Eingriffe in das Grundrecht auf informationelle Selbstbestimmung von mitunter erheblichem Gewicht (1). Die durch diese Vorschrift ermöglichte vorsorgende Speicherung ist unter engen Voraussetzungen, zu denen eine hinreichende Speicherschwelle gehört, rechtfertigungsfähig. Sie wahrt hier aber nicht die verfassungsrechtlichen Vorgaben der Verhältnismäßigkeit im engeren Sinne (2). 155

1. § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG erlaubt die Weiterverarbeitung von zuvor erhobenen oder in sonstiger Weise erlangten personenbezogenen Daten im polizeilichen Informationsverbund und damit Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) von erheblichem Gewicht. 156

a) Generell wird das Gewicht eines Eingriffs in die informationelle Selbstbestimmung vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt. Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden. Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme ebenso zur Erhöhung ihrer Intensität wie die faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist (vgl. BVerfGE 155, 119 <178 f. Rn. 129>; 165, 363 <399 f. Rn. 76> m.w.N.; stRspr). 157

Diese allgemeinen Kriterien bestimmen auch bei der hier vorliegenden Ermächtigung zur vorsorgenden Speicherung personenbezogener Daten das Eingriffsgewicht mit und erhalten bei einer solchen teilweise eine spezifische Prägung. Die Speicherung von Daten ist vorsorgend, weil sie nicht zu den Zwecken ihrer Erhebung oder Herstellung erfolgt, ohne dass eine neue Zweckbindung, die zu einer unmittelbaren weiteren Nutzung führt, an ihre Stelle gesetzt wird. Die neu gesetzten Zwecke liegen in der Bereithaltung der Daten für den Fall, dass sie für konkrete Zwecke künftig benötigt werden sollten. Das Besondere dieser Zweckänderung besteht in dem Fehlen einer unmittelbaren konkreten nutzungsorientierten Zwecksetzung zum Zeitpunkt der Speicherung. Zugleich teilt die vorsorgende Speicherung das allgemeine Charakteristikum jeder Speicherung, das darin liegt, dass die betroffenen Daten bereits zuvor durch Erhebung oder in sonstiger Weise in die staatliche Sphäre gelangt sind. 158

Auch das Eingriffsgewicht bei vorsorgenden Speicherungen personenbezogener Daten hängt zunächst ab vom Gewicht der vorausgegangenen Datenerhebungseingriffe und damit von der Herkunft der Daten. Es ist umso höher, je eingriffsintensiver die jeweils zugrundeliegende Erhebungsmaßnahme war (zur Abstufung anhand der Eingriffsintensität BVerfGE 141, 220 <269 f. Rn. 105 ff.>). 159

Maßgeblich geprägt wird die Eingriffsintensität ferner durch Art und Umfang der gespeicherten Daten. Die Art der Daten ist von Bedeutung, weil die Verwendung unterschiedlicher Daten direkt oder mittelbar unterschiedliche Persönlichkeitsrelevanz entfalten kann (vgl. zu einer Unterscheidung besonderer Kategorien personenbezogener Daten beispielsweise Art. 10 JI-RL). Je weniger die zu speichernden Daten der Art und ihrem Umfang nach eingeschränkt sind, umso größer ist die zur Verarbeitung gelangende Datenmenge und umso höher ist tendenziell das Eingriffsgewicht (vgl. BVerfGE 156, 11, <48 Rn. 96>; 165, 363 <401 Rn. 78>; parallel EuGH, Urteil vom 30. Januar 2024, Direktor na Glavna direktsia „Natsionalna politsia“ pri MVR - Sofia, C-118/22, EU:C:2024:97, Rn. 63; EGMR (GK), S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 103 f.). 160

Es ergibt einen wesentlichen Unterschied, welchen Anlass die betroffene Person zu einer Speicherung gegeben hat (vgl. BVerfGE 165, 363 <399 f. Rn. 76, 403 Rn. 84>). Werden etwa Informationen über (mögliche) Rechtsverstöße gespeichert, ist einzustellen, in welcher Beziehung die betroffenen Personen objektiv zu einem konkreten Fehlverhalten stehen und ob und inwiefern sie einen Eingriff durch ihr Verhalten zurechenbar veranlasst haben (vgl. BVerfGE 165, 363 <400 Rn. 77> m.w.N.). So stellt es für das Eingriffsgewicht einer Speicherung einen Unterschied dar, ob die betroffene Person hinsichtlich einer Straftat verurteilt oder aber lediglich beschuldigt oder verdächtigt wird (vgl. zu einer entsprechenden Unterscheidung anhand von Personenkategorien beispielsweise Art. 6 Buchstaben a und b JI-RL; vgl. unter dem Aspekt von Benachteiligungen auch EGMR (GK), S. and Marper v. The 161

United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 122; Peruzzo and Martens v. Germany, Entscheidung vom 4. Juni 2013, Kammer V, Nr. 7841/08 und 57900/12, § 43 f.).

Bedeutsam für das Eingriffsgewicht ist weiter, wie die gewonnenen personenbezogenen Daten weiterverwendet werden und welche Folgen dies für die Betroffenen haben kann (vgl. BVerfGE 65, 1 <45 f.>; 155, 119 <178 f. Rn. 129>; 165, 363 <407 f. Rn. 99> m.w.N.). Bei einer vorsorgenden Speicherung sind dabei nicht nur die möglichen künftigen Nutzungen zu berücksichtigen und wie viele und welche Grundrechtsträger dabei wie intensiven Beeinträchtigungen ausgesetzt sein können sowie unter welchen Voraussetzungen dies geschehen kann. Es sind darüber hinaus die mit einer vorsorgenden Speicherung verbundenen Besonderheiten einzustellen. Denn die vorsorgende Speicherung schafft einen Datenbestand, der nicht aus sich heraus auf konkrete Zwecke beschränkt ist, dabei aber Möglichkeiten der Verknüpfung von Daten eröffnet und personenbezogen auf potentiell sicherheitsrelevante Bezüge hinweisen kann. Dies wiederum kann zur Erstellung umfassenderer Persönlichkeitsbilder beitragen und erhöht die Wahrscheinlichkeit, von sicherheitsbehördlichen Maßnahmen adressiert zu werden. Die Regelung der Speicherzwecke hat deshalb Einfluss auf das Eingriffsgewicht. Je spezifischer die Zwecke, denen die Speicherung dient (Speicherzwecke), gefasst sind, umso geringer ist das Eingriffsgewicht. 162

Im Hinblick auf föderale polizeiliche Datenplattformen verschiedener Behörden ist einzustellen, welche und wie viele Akteure beteiligt sind und welchen Voraussetzungen der Datenzugriff unterliegt (vgl. BVerfGE 133, 277 <323 Rn. 112 f.>; 165, 363 <404 Rn. 89>; EGMR, Gardel v. France, Urteil vom 17. Dezember 2009, Kammer V, Nr. 16428/05, § 70). Insofern wirkt eine Speicherung in einem Informationsverbund, auf den viele Akteure zugreifen können, eingriffsverstärkend. 163

Die Eingriffsintensität bestimmt sich schließlich auch maßgeblich nach der Speicherdauer. Je länger die Speicherung und damit die weitere Nutzungsmöglichkeit der personenbezogenen Daten andauert, desto intensiver ist der Eingriff in das Grundrecht auf informationelle Selbstbestimmung (vgl. BVerfGE 125, 260 <322>). 164

b) Nach diesen Maßstäben ist das Eingriffsgewicht der Speicherung personenbezogener Daten nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG erheblich, bei fehlender Begrenzung von Speicherung und Verwendung schwerwiegend. 165

Eingriffsintensivierend wirkt sich aus, dass schon die vorsorgende Speicherung nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG regelhaft eine zweckändernde Weiterverarbeitung darstellt. Denn in den meisten Fällen werden personenbezogene Daten zum Zweck der Verhütung und Verfolgung von Straftaten gespeichert werden, die ursprünglich – zumeist von anderen Behörden oder Dritten – zu anderen konkreten Zwecken erhoben worden sind (vgl. zu 166

den diesbezüglichen Erhebungsbefugnissen des Bundeskriminalamts §§ 9 ff. BKAG). Dementsprechend wirkt eingriffsverstärkend, dass die Speicherung losgelöst vom ursprünglichen konkreten Erhebungszweck für noch nicht konkret bekannte künftige Zwecke erfolgt.

Die Speicherung hat vorliegend mit Blick auf die Herkunft der personenbezogenen Daten ein erhöhtes Eingriffsgewicht, soweit diese zuvor mittels besonders eingriffsintensiver Überwachungsmaßnahmen erhoben worden sind. Zwar dürfte ein Großteil der in § 18 Abs. 2 BKAG genannten Daten auch ohne eingriffsintensive Maßnahme gewonnen werden können. Dies ist jedoch nicht zwangsläufig der Fall. 167

Mit Blick auf die Art und den Umfang der zu speichernden personenbezogenen Daten wird das Eingriffsgewicht durch die Vorgaben in § 18 Abs. 2 Nr. 1 BKAG beschränkt. Gespeichert werden können im gerügten Umfang danach von Beschuldigten nur die Grunddaten und Informationen betreffend die kriminalaktenführende Polizeidienststelle, die Kriminalaktennummer, die Tatzeiten, die Tatorte sowie die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten. Die Grunddaten sollen der Identifizierung dienen und umfassen deswegen insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift der betroffenen Personen (vgl. § 20 Satz 2 Nr. 1 BKAG). Diesen Daten kommt eine nicht unerhebliche, aber beschränkt bleibende Persönlichkeitsrelevanz zu. 168

§ 18 Abs. 1 BKAG grenzt zudem den von einer Speicherung betroffenen Personenkreis ein und differenziert dabei zumindest im Ausgangspunkt nach verschiedenen Personenkategorien. Die Eigenschaft als Beschuldigter nach § 18 Abs. 1 Nr. 2 BKAG setzt in Anlehnung an das strafprozessuale Verständnis in der Regel voraus, dass gegen den Betroffenen eine Strafverfolgungsbehörde formal ein strafrechtliches Ermittlungsverfahren eingeleitet hat. Die Beschuldigteneigenschaft kann aber auch durch einen anderen Willensakt der Strafverfolgungsbehörden begründet werden (vgl. Schmitt, in: Meyer-Goßner/Schmitt, StPO, 67. Aufl. 2024, Einl. Rn. 76). Demgegenüber knüpft der Begriff des Verurteilten in § 18 Abs. 1 Nr. 1 BKAG an Art. 6 Buchstabe b JI-RL an und entspricht den in § 4 des Bundeszentralregistergesetzes geregelten Verurteilungen, die eine gerichtliche Feststellung eines Fehlverhaltens voraussetzen. Ausgehend hiervon ist eingriffsintensivierend bei § 18 Abs. 1 Nr. 2 BKAG zu berücksichtigen, dass es im Gegensatz etwa zu Verurteilten bei Beschuldigten an einem gerichtlich festgestellten Anlass einer Speicherung fehlen kann. Zudem können Beschuldigte einem erheblichen Informationsdefizit unterliegen, da sie nicht notwendigerweise von gegen sie gerichteten Erhebungsmaßnahmen, entsprechenden Weiterverarbeitungen und dem Status als Beschuldigter erfahren (vgl. § 170 Abs. 2 Satz 2 StPO). 169

Aufgrund der Heimlichkeit der vorsorgenden Speicherung ist die Erlangung nachträglichen Rechtsschutzes erheblich eingeschränkt, was das Eingriffsgewicht erhöht. 170

Für die Beurteilung der Eingriffsintensität zu gewichten sind auch die weitreichenden Verwendungsmöglichkeiten der gespeicherten Daten durch eine Vielzahl von Behörden (vgl. § 29 Abs. 3 BKAG). Zwar ist das Bundeskriminalamt als Zentralstelle im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben beschränkt (vgl. BVerfGE 110, 33 <51>). Polizeiliche Aufgaben der Gefahrenabwehr und Strafverfolgung sind insoweit nicht übertragen, sondern werden dort nur koordiniert und informationell verklammert (vgl. BVerfGE 155, 119 <212 Rn. 209>). Neben der Auswertung durch das Bundeskriminalamt im Rahmen seiner Zentralstellenaufgabe (vgl. § 2 Abs. 2 Nr. 1 BKAG) und einer entsprechenden Unterrichtung der Strafverfolgungsbehörden (vgl. § 2 Abs. 2 Nr. 2 BKAG) kann die Weiterverarbeitung aber auch auf eine Kooperation im Rahmen des polizeilichen Informationsverbunds gerichtet sein. Im Rahmen dieses Datenaustauschs, an dem das Bundeskriminalamt nach Maßgabe der §§ 29 und 30 BKAG teilnimmt (§ 13 Abs. 3 BKAG), erhalten aber weitere Sicherheitsbehörden unter den Anforderungen des § 29 Abs. 4 Satz 2 BKAG – insbesondere spezifischer Kennzeichnungspflichten (§ 14 BKAG) und Zugriffsberechtigungen (§ 15 BKAG) – auf einen mitunter erheblichen Teil der personenbezogenen Daten Zugriff. Hier erhöhen die erleichterten Zugriffsmöglichkeiten der teilnehmenden Behörden die Eingriffsintensität. Dabei sind nach § 29 Abs. 3 BKAG außer dem Bundeskriminalamt und Landeskriminalämtern zur Teilnahme berechtigt: sonstige Polizeibehörden der Länder, die Bundespolizei, die Polizei beim Deutschen Bundestag, mit der Wahrnehmung grenzpolizeilicher Aufgaben betraute Behörden der Zollverwaltung, die Zollfahndungsämter, das Zollkriminalamt und die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden. Nicht teilnahmeberechtigt sind die Nachrichtendienste. 171

In diesem Rahmen kann bereits die Speicherung im polizeilichen Informationsverbund als Beschuldigter mit seinen Grunddaten nachteilige Konsequenzen haben. Die Speicherung kann auf den unmittelbaren Austausch von Erkenntnissen gerichtet sein und entsprechende Einträge können gegenüber den teilnehmenden Behörden auf sicherheitsrelevante Bezüge hinweisen. Damit kann die Speicherung in letzter Konsequenz auf operative Maßnahmen gerichtet sein oder jedenfalls die Wahrscheinlichkeit sicherheitsbehördlicher Maßnahmen gegen die Betroffenen deutlich erhöhen. 172

Eingriffsverstärkend wirkt zudem in der konkreten Ausgestaltung, dass der Gesetzgeber auch angesichts der Zweckbestimmung einer künftigen Verhütung und Verfolgung bestimmter Straftaten neben den allgemeinen Löschungsvorgaben keine weitergehenden ausdifferenzierten Begrenzungen hinsichtlich der Speicherdauer der Daten getroffen hat. Damit können Daten mitunter über sehr lange Zeiträume gespeichert werden, ohne dass dabei deutlicher anhand des Gewichts der zu verhütenden oder aufzuklärenden Straftaten differenziert würde. 173

2. Angesichts dieses erheblichen Eingriffsgewichts wahrt § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG nicht die verfassungsrechtlichen Anforderungen. Zwar dient die Vorschrift einem legitimen Ziel und ist zu dessen Erreichung geeignet und 174

erforderlich (a). Auch ist die ermöglichte vorsorgende Speicherung der von ihr umfassten Daten im polizeilichen Informationsverbund unter engen Voraussetzungen rechtfertigungsfähig. In ihrer konkreten Ausgestaltung ist sie indes mit Anforderungen der Verhältnismäßigkeit im engeren Sinne unvereinbar, da es an einer hinreichend normierten Speicherungsschwelle und den gebotenen Vorgaben zur Speicherdauer fehlt (b).

a) Die vorsorgende Speicherung muss einem legitimen Ziel dienen, geeignet und erforderlich sein (vgl. dazu Rn. 90). 175

§ 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG dient einem legitimen Ziel. Die Befugnis ermöglicht dem Bundeskriminalamt die sachgerechte Erfüllung seiner Aufgaben als Zentralstelle nach § 2 Absätze 1 bis 3 BKAG, die ihrerseits auf eine effektive und zügige Strafverfolgung und Gefahrenabwehr durch die Sicherheitsbehörden gerichtet sind (vgl. auch BTDrucks 18/11163, S. 2, 76). Im Rahmen dieser Zentralstellenaufgaben unterstützt das Bundeskriminalamt die Polizeibehörden bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung (§ 2 Abs. 1 BKAG). Zur Wahrnehmung dieser Aufgabe hat es insbesondere alle hierfür erforderlichen Informationen zu sammeln und auszuwerten (§ 2 Abs. 2 Nr. 1 BKAG) sowie die Strafverfolgungsbehörden des Bundes und der Länder unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten zu unterrichten (§ 2 Abs. 2 Nr. 2 BKAG). Gleichzeitig unterhält es als Zentralstelle den einheitlichen polizeilichen Informationsverbund, an dem das Bundeskriminalamt nach Maßgabe der §§ 29 und 30 BKAG teilnimmt (§ 13 Abs. 3 BKAG). Die Schaffung eines Informationsverbundes der Polizeien von Bund und Ländern gewährleistet einen zielführenden und zügigen Austausch der Erkenntnisse zwischen den Sicherheitsbehörden (vgl. auch BTDrucks 18/11163, S. 2, 76). Die vorsorgende Speicherung dient im Rahmen dieses Zwecks dazu, die Möglichkeit zu schaffen, Zusammenhänge zwischen solchen Straftaten im Sinne von § 2 Abs. 1 BKAG bei ihrem zeitlich gestaffelten Auftreten zu erkennen. 176

Zur Erreichung dieses legitimen Zwecks ist die Befugnis zur Datenweiterverarbeitung nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG auch geeignet und erforderlich. Die Regelung ist zur Zweckerreichung geeignet, da die Verhütung und Verfolgung von Straftaten erleichtert wird, wenn Daten und Erkenntnisse gesammelt, verdichtet und effektiv unter den berechtigten Sicherheitsbehörden ausgetauscht werden können. Auf diese Weise kann differenziert Informationsproblemen unter Wahrung der gebotenen Organisationsordnung entgegengetreten werden, die in einem föderalen Staat jedenfalls nicht vollständig auf organisatorischer Ebene gelöst werden können und sollen (vgl. BVerfGE 133, 277 <332 f. Rn. 131>). Die vorsorgend zu speichernden Grunddaten der Beschuldigten bilden dabei die entscheidenden Faktoren für die zweifelsfreie, schnelle und effektive Identifizierung der betreffenden Person (vgl. BTDrucks 18/11163, S. 99). Die Befugnis ist auch erforderlich, da die Zusammenarbeit der Polizeien von Bund und Ländern mithilfe der Datenweiterverarbeitung durch das Bundeskriminalamt im Rahmen der Zentralstellenaufgaben auf andere, 177

grundrechtsschonendere Weise nicht gleichermaßen wirksam zu erreichen wäre. Insbesondere ist im Vergleich zu dem geschaffenen polizeilichen Informationsverbund kein milderes, gleich geeignetes Mittel ersichtlich. Die ebenfalls ermöglichte Datenübermittlung im Einzelfall oder der Zugriff auf andere partielle Datenbanken (beispielsweise das Bundeszentralregister) sind nicht gleich wirksam. Vor allem sind die eigenen Zugriffs- und Verarbeitungsrechte der teilnehmenden Behörden für eine schnelle Verfügbarkeit der Daten und damit effektive Kriminalitätsbekämpfung notwendig. Da gerade Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung aufgrund der verflochtenen Handlungszusammenhänge mitunter schwer zu erfassen sind, hängt der Erfolg einer wirksamen Aufgabenwahrnehmung der Sicherheitsbehörden in besonderer Weise davon ab, dass wichtige Informationen, die bei einer Behörde anfallen, auch für andere Behörden erschlossen werden und durch das Zusammenführen und Abgleichen der verschiedenen Daten aus diffusen Einzelerkenntnissen aussagekräftige Informationen und Lagebilder werden (vgl. BVerfGE 133, 277 <333 Rn. 132>).

b) Nicht zu vereinbaren ist die Speicherung nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG in ihrer konkreten Ausgestaltung hingegen mit den Anforderungen der Verhältnismäßigkeit im engeren Sinne. 178

aa) Die Verhältnismäßigkeit im engeren Sinne verlangt, dass die Schwere der gesetzgeberischen Grundrechtsbeschränkung bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der sie rechtfertigenden Gründe steht (vgl. BVerfGE 141, 220 <267 Rn. 98>; 148, 40 <57 f. Rn. 49>). Dabei ist ein angemessener Ausgleich zwischen dem Eingriffsgewicht der Regelung und dem verfolgten gesetzgeberischen Ziel, zwischen Individual- und Allgemeininteresse herzustellen (vgl. BVerfGE 100, 313 <375 f.>; 133, 277 <322 Rn. 109>; stRspr). Geboten hierfür ist eine Ausgestaltung, die dem Eingriffsgewicht differenzierend und hinreichend Rechnung trägt. 179

Die vorsorgende Speicherung stellt eine Zweckänderung dar (1). Sie muss an eine eindeutig erkennbare Zweckbestimmung geknüpft sein (2). Weiter sind Anforderungen an die Eingriffsschwellen, hier in Form von Speicherschwellen, zu stellen (3). Aufgrund der weiten Zielsetzung bedarf es spezifischer Begrenzungen der Speicherdauer (4). Schließlich muss der Gesetzgeber klare Verwendungsregeln und differenzierte organisatorische und verfahrensrechtliche Anforderungen sowie adäquate Kontrollmöglichkeiten vorsehen (5). 180

(1) Die vorsorgende Speicherung stellt eine Zweckänderung dar. Eine solche bedarf als Grundrechtseingriff einer verfassungsrechtlichen Rechtfertigung, insbesondere ihrerseits einer gesetzlichen Grundlage (vgl. BVerfGE 141, 220 <324 Rn. 277>). Sie darf allerdings nicht zu einer Umgehung der verfassungsrechtlichen Vorgaben für eine Datenübermittlung führen, auf die die Grundsätze der hypothetischen Datenneuerhebung Anwendung finden. 181

Für eine verfassungsrechtliche Rechtfertigung der vorsorgenden Speicherung erforderlich sind jedenfalls die Festlegung angemessener Speicherzwecke und Speicherschwellen sowie die Bestimmung einer angemessenen Speicherdauer. 182

(2) Die Entkoppelung der vorsorgenden Speicherung von den konkreten Zweckbestimmungen der Erhebung und einer späteren konkreten Nutzung (Rn. 158) erfordert die Festlegung hinreichend gewichtiger, konkret benannter Zwecke für die Speicherung selbst. Diese Speicherzwecke müssen der künftigen Nutzung einen festen Rahmen vorgeben. Der Staat darf nicht etwa alle Daten, die er rechtmäßig erhoben oder geschaffen hat, über den primären Zweck hinaus mit der Begründung vorsorgend speichern, die Daten könnten künftig noch einmal benötigt werden und der gebotene Schutz könne in die Ausgestaltung der zulässigen künftigen Nutzung verlagert werden. Unzulässig wäre es daher, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenvorrats würde den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck aufheben und damit auch die zentrale datenschutzrechtliche Freiheitssicherung durch die Zweckbindung. Auch wäre die Tragweite für die Bürgerinnen und Bürger nicht vorhersehbar (vgl. BVerfGE 125, 260 <345 f., 355 f.>; 155, 119 <180 Rn. 131>). 183

(3) Für die Bestimmung der Speicherschwelle muss der Gesetzgeber neben Herkunft, Art und Umfang der Daten insbesondere berücksichtigen, dass sich die Speicherung auch im Einzelfall an den festgelegten Speicherzwecken messen lassen muss. Die Speicherschwelle muss den Zusammenhang zwischen den vorsorgend gespeicherten personenbezogenen Daten und der Erfüllung des Speicherzwecks in verhältnismäßiger Weise absichern und den spezifischen Gefahren der vorsorgenden Speicherung angemessen begegnen. 184

Bei ihrer Bestimmung sind daher zunächst die Herkunft, also etwa die Erhebungsmethoden, aber auch Art und Umfang der Daten zu berücksichtigen und in Relation zu den mit der Speicherung letztlich verfolgten Zwecken zu setzen. Deren Angemessenheit muss die Besonderheit der vorsorgenden Speicherung einbeziehen. Dies erfordert insbesondere das Bestehen einer hinreichenden Wahrscheinlichkeit dafür, dass die vorsorgend gespeicherten Daten zur Erfüllung der mit der Speicherung letztlich verfolgten Zwecke benötigt werden. 185

Bei der Speicherung von Daten für die Verhütung und Verfolgung vom Speicherzweck erfasster Straftaten ist dies bei personenbezogenen Daten nur gegeben, wenn eine hinreichende Wahrscheinlichkeit dafür besteht, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen werden und gerade die gespeicherten Daten zu deren Verhütung und Verfolgung angemessen beitragen können. Diese Prog- 186

nosen müssen sich auf zureichende tatsächliche Anhaltspunkte stützen. Als taugliche Prognosekriterien können insbesondere die Art, Schwere und Begehungsweise der vormaligen Tat sowie die Persönlichkeit des Betroffenen und sein bisheriges strafrechtliches Erscheinungsbild in Frage kommen. Von Bedeutung wird angesichts der allgemeinen fachwissenschaftlichen Erkenntnisse zu Kriminalprognosen regelmäßig sein, ob die Person wiederholt und in welchem Ausmaß sie straffällig geworden ist. Relevant wird auch der Zeitraum sein, während dessen sie strafrechtlich nicht (mehr) in Erscheinung getreten ist (vgl. auch EGMR, P. N. gegen Deutschland, Urteil vom 11. Juni 2020, Kammer V, Nr. 74440/17, u.a. §§ 76 ff.; EuGH, Urteil vom 30. Januar 2024, Direktor na Glavna direktsia „Natsionalna politsia“ pri MVR - Sofia, C-118/22, EU:C:2024:97, Rn. 60 f., 67). Die Wahrscheinlichkeit kann personenbezogen, phänomenbezogen oder tatbezogen begründbar sein. So könnte etwa eine Ausrichtung an Delikts-/Phänomenbereichen erfolgen, wie beispielsweise Terrorismus, Organisierte Kriminalität, Schleusung, Menschenhandel, Ausbeutung, Waffen- und Sprengstoffkriminalität, Gewaltdelikte/gemeingefährliche Straftaten, Rauschgiftkriminalität, Cyberkriminalität, Eigentumskriminalität/Vermögensdelikte, Sexualdelikte, Arzneimittelkriminalität, Falschgeldkriminalität, Geldwäsche, Korruption, Wirtschafts- und Umweltkriminalität und politisch motivierte Kriminalität.

(4) Für die verfassungsrechtliche Rechtfertigung der vorsorgenden Speicherung personenbezogener Daten bedarf es zudem der gesetzlichen Regelung einer angemessenen Speicherdauer. 187

Grundsätzlich müssen personenbezogene Daten gelöscht werden, sobald sie für die zuvor festgelegten Zwecke oder den gerichtlichen Rechtsschutz der Betroffenen nicht länger benötigt werden (vgl. oben Rn. 140 f.). Dies gewährleistet im Ausgangspunkt, dass die Daten nicht länger gespeichert werden, als es für die Zwecke, für die sie gespeichert wurden, erforderlich ist (vgl. auch EuGH, Urteil vom 30. Januar 2024, Direktor na Glavna direktsia „Natsionalna politsia“ pri MVR - Sofia, C-118/22, EU:C:2024:97, Rn. 43; Art. 4 Abs. 1 Buchstabe e JI-RL; EGMR (GK), S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 107) und die Speicherdauer der Daten auf ein verfassungsrechtlich zulässiges Maß beschränkt bleibt. 188

Die Dauer der zulässigen Speicherung wird insbesondere geprägt durch das Eingriffsgewicht (Rn. 157 ff.), die Belastbarkeit der Prognose in der Zeit sowie durch andere sich aus dem Grundsatz der Verhältnismäßigkeit ergebende Gesichtspunkte. Die Prognose verliert über die Zeit ohne Hinzutreten neuer relevanter Umstände grundsätzlich an Überzeugungskraft (vgl. auch EuGH, Urteil vom 30. Januar 2024, Direktor na Glavna direktsia „Natsionalna politsia“ pri MVR - Sofia, C-118/22, EU:C:2024:97, Rn. 60 f.; EGMR, Catt v. the United Kingdom, Urteil vom 24. Januar 2019, Kammer I, Nr. 43514/15, §§ 119 f.). Die verfassungsrechtlich gebotene kompensatorische Einhegung einer Befugnis zur vorsorgenden Speicherung gebietet daher ein Regelungskonzept, das entsprechend diesen Gesichtspunkten 189

differenzierte Prüfungs- und Aussonderungsfristen setzt. Auch muss die vorsorgende Speicherung grundsätzlich zeitlich begrenzt sein.

Es obliegt dem Gesetzgeber, unter Berücksichtigung seiner Delegationsbefugnisse (vgl. BVerfGE 150, 1 <96 ff. Rn. 190 ff.> m.w.N.) die entsprechenden Regelungen einschließlich der notwendigen prozeduralen Sicherungen hierfür zu treffen. 190

(5) Unerlässliche Voraussetzung für die Verfassungsmäßigkeit der Speicherbefugnis sind weiterhin klar normierte Verwendungsregeln (vgl. BVerfGE 155, 119 <179 f. Rn. 130 f.>; 125, 260 <327 f.>), die insbesondere den im Urteil des Bundesverfassungsgerichts vom 20. April 2016 formulierten verfassungsrechtlichen Anforderungen an die zweckändernde Weiternutzung personenbezogener Daten genügen müssen (vgl. BVerfGE 141, 220 <326 ff. Rn. 284 ff.> m.w.N.). 191

Der Verhältnismäßigkeitsgrundsatz stellt zudem insbesondere auch bei der Speicherung personenbezogener Daten Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (siehe bereits Rn. 90; vgl. BVerfGE 141, 220 <282 Rn. 134> m.w.N.; stRspr) sowie an die Gewährleistung der Datensicherheit (vgl. BVerfGE 155, 119 <182 Rn. 135>). Für die vorsorgende Speicherung im polizeilichen Informationsverbund gehören dazu klare Zugriffsregeln, die sicherstellen, dass nur für den Speicherzweck zuständige Mitarbeiterinnen und Mitarbeiter der Polizei Zugriff haben (vgl. hierzu etwa § 15 Abs. 3 Satz 2 und 3 BKAG, BTDrucks 18/11163, S. 97). 192

bb) § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG genügt diesen verfassungsrechtlichen Anforderungen nicht. Die Befugnis ist mit dem Grundsatz der Verhältnismäßigkeit im engeren Sinne unvereinbar. Es fehlt an einer hinreichend normierten Speicherschwelle und den gebotenen Vorgaben zur Speicherdauer. Ob darüber hinaus den Gefahren der vorsorgenden Speicherung von mit besonders eingriffsintensiven Methoden erhobenen personenbezogenen Daten hinreichend begegnet wurde (vgl. dazu BVerfGE 133, 277 <373 f. Rn. 226>; 141, 220 <323 Rn. 274>), bedarf deshalb hier keiner Entscheidung. 193

(1) § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG erlaubt eine vorsorgende Speicherung personenbezogener Daten ohne Bindung an ihren vorherigen Zweck. Für die darin liegende Zweckänderung bildet die Vorschrift eine gesetzliche Grundlage. Soweit sie die Speicherung regelt, führt sie für sich genommen auch nicht zu einer Umgehung der Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung; der verfassungsrechtlichen Beurteilung anderer Weiterverarbeitungen bedarf es hier nicht. 194

(2) § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG enthält für die Speicherung personenbezogener Daten zu Zwecken künftiger Straftatenverhütung 195

und -verfolgung keine hinreichende Speicherschwelle. Die Norm lässt für die vorsorgende Speicherung allein die Beschuldigteneigenschaft genügen. Insbesondere ist eine Negativprognose fachrechtlich nicht vorgesehen. Der Status des Beschuldigten ist auch jenseits der Fälle des § 18 Abs. 5 BKAG schon mit Unsicherheiten hinsichtlich der Beziehung zur vorgeworfenen Straftat verbunden und vermag deshalb für sich allein erst recht keinen belastbaren Schluss auf die hinreichende Wahrscheinlichkeit einer relevanten Beziehung zu anderen zukünftig zu verfolgenden oder zu verhütenden Straftaten zu tragen.

Zwar hat der Gesetzgeber einzelne Aspekte einer solchen Prognose sowohl für die Tatverdächtigen und Anlasspersonen im Sinne des § 18 Abs. 1 Nr. 3 und 4 BKAG hinsichtlich ihrer Grunddaten berücksichtigt als auch nach § 18 Abs. 2 Nr. 2 BKAG für Beschuldigte hinsichtlich ihrer weiteren personenbezogenen Daten. Eine Übertragung dieser Speicherschwelle für den vorliegenden Anwendungsfall scheidet aber aufgrund des in dem eindeutigen Wortlaut zum Ausdruck gekommenen gesetzgeberischen Willen aus (vgl. dazu BVerfG, Beschluss des Ersten Senats vom 21. November 2023 - 1 BvL 6/21 -, Rn. 67 ff.). Auch wenn die Praxis des Bundeskriminalamts prognostische Elemente vor einer Speicherung berücksichtigt, ist für die verfassungsrechtliche Beurteilung der Befugnis deren rechtliche Reichweite und nicht eine Behördenpraxis maßgeblich (vgl. BVerfGE 162, 1 <147 Rn. 326>). 196

(a) Den verfassungsrechtlichen Anforderungen wird auch nicht dadurch entsprochen, dass eine Speicherung nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG die Prüfung der Erforderlichkeit im Einzelfall voraussetzt. Eine derartige Prüfung gebietet § 47 Nr. 3 BDSG, nach dem personenbezogene Daten für das Erreichen des Verarbeitungszwecks unter anderem erforderlich sein müssen. Die Erforderlichkeitsprüfung im Einzelfall gehört zu den in § 47 BDSG normierten allgemeinen Grundsätzen für die Verarbeitung personenbezogener Daten, die auch das Bundeskriminalamt bei Weiterverarbeitungsschritten wie der Speicherung von Daten grundsätzlich zu beachten hat. Ausgeschlossen wäre seine Anwendung nur, soweit das Bundeskriminalamtgesetz eine Vollregelung zur bereichsspezifischen Verarbeitung personenbezogener Daten enthielte. Eine solche Vollregelung hat das Bundeskriminalamtgesetz für die Datenweiterverarbeitung aber nicht getroffen (vgl. auch Wolf-Rüdiger Schenke/Graulich/Ruthig, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Einführung Rn. 27). 197

Auch die danach vorzunehmende Prüfung der Erforderlichkeit im Einzelfall kann aber mangels näher bestimmter Vorgaben nicht hinreichend gewährleisten, dass den Anforderungen einer spezifischen Negativprognose Rechnung getragen wird. Denn eine nicht näher angeleitete Prüfung der Erforderlichkeit genügt in ihrer Offenheit nicht dem verfassungsrechtlich gebotenen Differenzierungsgrad. 198

(b) Eine hinreichende Schwelle für die Speicherung nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG lässt sich auch nicht durch Rückgriff auf die Vorgaben des § 12 Abs. 2 BKAG gewinnen. 199

Denn dem Bundeskriminalamtgesetz kann nicht im Wege der anerkannten Auslegungsmethoden entnommen werden, dass die Voraussetzungen von § 12 Abs. 2 BKAG bei der vorliegenden Speicherung zu prüfen sind. Im Gegensatz zum Wortlaut des § 16 Abs. 1 BKAG soll nach § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG eine Weiterverarbeitung, also insbesondere eine Speicherung zuvor erhobener personenbezogener Daten, nicht ausdrücklich „nach Maßgabe des § 12“ BKAG erfolgen. Auch systematische Erwägungen streiten nicht für eine Anwendbarkeit der Vorschrift. Überdies wird § 12 BKAG nicht in den Ausführungen der Begründung des Gesetzesentwurfs zu § 18 BKAG erwähnt (vgl. BTDrucks 18/11163, S. 99 ff.). Dass das Kriterium der hypothetischen Datenneuerhebung in § 12 Abs. 2 BKAG als allgemeiner Grundsatz formuliert sein soll, der bei jeder Datenverarbeitung durch das Bundeskriminalamt – unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme – zu beachten sei (vgl. BTDrucks 18/11163, S. 92), rechtfertigt kein anderes Ergebnis. Insbesondere ist nicht zu erkennen, dass der Gesetzgeber bereits jede zweckändernde Speicherung personenbezogener Daten im Rahmen der Zentralstellenaufgaben vom Erfordernis des Vorliegens konkreter Ermittlungsansätze abhängig machen wollte.

(3) Überdies fehlt es an einem hinreichend ausdifferenzierten Regelungskonzept zur Speicherdauer. Die vorhandenen Regelungen in § 75 Absätze 2 und 4 BDSG und § 77 Abs. 1 BKAG genügen diesen Anforderungen nicht. Nach § 75 Abs. 2 BDSG sind personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Zudem enthält § 75 Abs. 4 BDSG die Pflicht, angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden. Ob gespeicherte personenbezogene Daten zu löschen sind, überprüft das Bundeskriminalamt danach zuvörderst im Rahmen einer durch Gesetz oder Verordnung nicht hinreichend angeleiteten Einzelfallbearbeitung. 200

An diesem Defizit vermögen auch etwaige Vorgaben aus dem als „Verschlusssache - nur für den Dienstgebrauch“ eingestuften und im hiesigen Verfahren nicht vorgelegten Leitfaden des Bundeskriminalamts für ein Löschkonzept nichts zu ändern. 201

Zwar sieht § 77 Abs. 1 Satz 1 BKAG zeitlich festgelegte Fristen für die Prüfung der Löschungspflichten vor. Diese Aussonderungsprüffristen dürfen bei Erwachsenen zehn Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist (vgl. § 77 Abs. 1 Satz 2 BKAG). 202

Allerdings genügt dies allein nicht den Anforderungen an ein durch den Gesetzgeber auszugestaltendes Regelungskonzept. Es bleibt hier weiterhin dem Bundeskriminalamt überlassen, durch eigene innerbehördliche Vorgaben die Prüfungs- und Aussonderungsfristen zu konkretisieren. Es kann deshalb offenbleiben, ob die verfassungsrechtlichen Kriterien zur Bemessung der Fristen (vgl. Rn. 189) angemessen abgebildet sind. 203

D.

I.

Im Ergebnis genügen die zulässig angegriffenen Normen den verfassungsrechtlichen Anforderungen teilweise nicht. Die Verfassungsbeschwerde ist insoweit begründet. 204

§ 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1, soweit dieser in Verbindung mit § 13 Abs. 3, § 29 BKAG die Speicherung von Daten durch das Bundeskriminalamt in seiner Funktion als Zentralstelle erlaubt, ist verfassungswidrig, weil es für die Speicherung an der Normierung einer angemessenen Speicherschwelle und ausreichenden Vorgaben zur Speicherdauer fehlt. 205

§ 45 Abs. 1 Satz 1 Nr. 4 BKAG ist verfassungswidrig, weil die vorgesehene Eingriffsschwelle nicht den Anforderungen der Verhältnismäßigkeit im engeren Sinne genügt. 206

II.

1. Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Sätze 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären. Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist. Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustands durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (BVerfGE 141, 220 <351 Rn. 355> m.w.N.; stRspr). 207

2. a) Danach sind § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1, soweit dieser in Verbindung mit § 13 Abs. 3, § 29 BKAG die Speicherung von Daten durch das Bundeskriminalamt in seiner Funktion als Zentralstelle erlaubt, sowie § 45 Abs. 1 Satz 1 Nr. 4 BKAG lediglich für mit der Verfassung unvereinbar zu erklären. Die Gründe für die Verfassungswidrigkeit dieser Vorschriften betreffen nicht den Kern der mit ihnen eingeräumten Befugnisse, sondern einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung. Der Gesetzgeber kann in diesen Fällen die verfassungsrechtlichen Beanstandungen nachbessern und damit den Kern der mit den Vorschriften verfolgten Ziele auf verfassungsmäßige Weise verwirklichen. 208

Die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung bis zum Ablauf des 31. Juli 2025 zu verbinden. Angesichts der Bedeutung, die der Gesetzgeber § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG für die staatliche Aufgabenwahrnehmung beimessen darf und wegen ihrer Bedeutung für die Verhütung und Verfolgung bestimmter Straftaten durch die Sicherheitsbehörden, ist eine befristete Fortgeltung zu bestimmen. Gleiches gilt für § 45 Abs. 1 Satz 1 Nr. 4 BKAG wegen der großen Bedeutung einer wirksamen Bekämpfung des internationalen Terrorismus für den freiheitlichen und demokratischen Rechtsstaat (vgl. BVerfGE 141, 220 <352 Rn. 357>). 209

b) Die befristete Anordnung der Fortgeltung bedarf jedoch einschränkender Maßgaben. § 45 Abs. 1 Satz 1 Nr. 4 BKAG gilt mit der Maßgabe fort, dass er lediglich dann zur Anwendung gelangt, wenn in der Person, zu der die von der Maßnahme nach § 45 Abs. 1 Satz 1 BKAG betroffene Person nicht nur flüchtig oder in zufälligem Kontakt steht (§ 39 Abs. 2 Nr. 2 BKAG), eine der in § 45 Abs. 1 Satz 1 Nr. 2 bis 3 BKAG geregelten Voraussetzungen vorliegt. 210

§ 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG gilt mit der Maßgabe fort, dass eine Speicherung der von der Regelung erfassten personenbezogenen Daten nur dann gestattet ist, wenn eine spezifische Negativprognose in der Weise gestellt worden ist, dass eine hinreichende Wahrscheinlichkeit dafür besteht, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen werden und gerade die gespeicherten Daten zu deren Verhütung und Verfolgung angemessen beitragen können. Diese Prognosen müssen sich auf zureichende tatsächliche Anhaltspunkte stützen. 211

Die Negativprognose und die sie tragenden Anknüpfungstatsachen sind durch das Bundeskriminalamt zu dokumentieren. Einer Übergangsregelung zur angemessenen Dauer der Speicherung auf der Grundlage von § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 in Verbindung mit § 13 Abs. 3, § 29 BKAG bedarf es wegen der bis zu einer Neuregelung durch den Gesetzgeber zeitlich begrenzten Fortgeltung nicht. 212

Eine Neuregelung durch den Gesetzgeber wird durch die getroffenen Übergangsregelungen nicht präjudiziert. 213

III.

Die Auslagenentscheidung beruht auf § 34a Abs. 2 BVerfGG. Die Beschwerdeführerinnen zu 1) und 2) sowie die Beschwerdeführenden zu 3) bis 5) haben jeweils nur teilweise obsiegt. 214

Harbarth Ott Christ

Radtke Härtel Wolff

Eifert Meßling