18. Wahlperiode

Deutscher Bundestag
Innenausschuss

# Wortprotokoll
der 107. Sitzung

**Innenausschuss**
Berlin, den 20. März 2017, 11:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Ansgar Heveling, MdB

## Tagesordnung - Öffentliche Anhörung

**Einziger Tagesordnungspunkt**

a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

**Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes**

**BT-Drucksache 18/11163**

**Federführend:**
Innenausschuss

**Mitberatend:**
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss für Gesundheit
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss Digitale Agenda
Haushaltsausschuss (§ 96 GO)

**Berichterstatter/in:**
Abg. Clemens Binninger [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Martina Renner [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

b) Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes**

**BT-Drucksache 18/11326**

**Federführend:**
Innenausschuss

**Mitberatend:**
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss für Gesundheit
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss Digitale Agenda
Haushaltsausschuss (§ 96 GO)

**Gutachtlich:**
Parlamentarischer Beirat für nachhaltige Entwicklung

**Berichterstatter/in:**
Abg. Clemens Binninger [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Martina Renner [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

# Inhaltsverzeichnis

Unangeforderte Stellungnahmen

| | |
|---|---|
| Deutscher Richterbund | 18(4)749 |
| Bundespsychotherapeutenkammer | 18(4)781 |
| Deutsche Gesellschaft für Kinder- und Jugendpsychiatrie, Psychosomatik und Psychotherapie e. V. | 18(4)791 |
| Deutscher Anwaltverein | 18(4)863 |

Gutachterliche Stellungnahmen des Parlamentarischen Beirates für nachhaltige Entwicklung

| | |
|---|---|
| zu Bundestagsdrucksache 18/11326 | 18(4)793 |

ÖH

18. Wahlperiode

Deutscher Bundestag

**Sitzung des Innenausschusses (4. Ausschuss)**
Montag, 20. März 2017, 11:00 Uhr

## CDU/CSU

| Ordentliche Mitglieder | Unterschrift |
|---|---|
| Baumann, Günter | |
| Binninger, Clemens | |
| Bosbach, Wolfgang | |
| Frieser, Michael | |
| Hellmuth, Jörg | |
| Heveling, Ansgar | |
| Hoffmann (Dortmund), Thorsten | |
| Lindholz, Andrea | |
| Mayer (Altötting), Stephan | |
| Ostermann Dr., Tim | |
| Schäfer (Saalstadt), Anita | |
| Schuster (Weil am Rhein), Armin | |
| Veith, Oswin | |
| Warken, Nina | |
| Wendt, Marian | |
| Wichtel, Peter | |
| Woltmann, Barbara | |
| Zertik, Heinrich | |

04

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. März 2017, 11:00 Uhr

## SPD

| Ordentliche Mitglieder | Unterschrift |
|---|---|
| Castellucci Dr., Lars | |
| Fograscher, Gabriele | |
| Grötsch, Uli | |
| Gunkel, Wolfgang | |
| Hartmann, Sebastian | |
| Lischka, Burkhard | |
| Mittag, Susanne | |
| Özdemir (Duisburg), Mahmut | |
| Reichenbach, Gerold | |
| Schmidt (Berlin), Matthias | |
| Veit, Rüdiger | |

| Stellvertretende Mitglieder | Unterschrift |
|---|---|
| Esken, Saskia | |
| Fechner Dr., Johannes | |
| Gerster, Martin | |
| Högl Dr., Eva | |
| Juratovic, Josip | |
| Kolbe, Daniela | |

4

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. März 2017, 11:00 Uhr

## SPD

| Stellvertretende Mitglieder | Unterschrift |
|---|---|
| Lühmann, Kirsten | |
| Poschmann, Sabine | |
| Rix, Sönke | |
| Spinrath, Norbert | |
| Yüksel, Gülistan | |

## DIE LINKE.

| Ordentliche Mitglieder | Unterschrift |
|---|---|
| Jelpke, Ulla | |
| Korte, Jan | |
| Renner, Martina | M. Renner |
| Tempel, Frank | |

| Stellvertretende Mitglieder | Unterschrift |
|---|---|
| Dağdelen, Sevim | |
| Hahn Dr., André | |
| Karawanskij, Susanna | |

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 20. März 2017, 11:00 Uhr

## DIE LINKE.

| Stellvertretende Mitglieder | Unterschrift |
|---|---|
| Pau, Petra | |

## BÜ90/GR

| Ordentliche Mitglieder | Unterschrift |
|---|---|
| Amtsberg, Luise | |
| Beck (Köln), Volker | |
| Mihalic, Irene | |
| Notz Dr., Konstantin von | |

| Stellvertretende Mitglieder | Unterschrift |
|---|---|
| Haßelmann, Britta | |
| Künast, Renate | |
| Lazar, Monika | |
| Mutlu, Özcan | |

öff.

Tagungsbüro

Deutscher Bundestag

**Sitzung des Innenausschusses (4. Ausschuss)**
Montag, 20. März 2017, 11:00 Uhr

| | Fraktionsvorsitz | Vertreter |
|---|---|---|
| CDU/CSU | | |
| SPD | | |
| DIE LINKE. | | |
| BÜNDNIS 90/DIE GRÜNEN | | |

## Fraktionsmitarbeiter

| **Name** (Bitte in Druckschrift) | **Fraktion** | **Unterschrift** |
|---|---|---|
| Burczyk, Dirk | LINKE | |
| Wehrhahn, Sebastian | LINKE | |
| [illegible], [illegible] | Grün | |
| Ueckert, Stefan | SPD | |
| Elfadli, Daniel | B90/Grüne | |
| Hartmann, Johannes | Grüne | |
| Mellentin, Johanna | " | |
| Vera Eilers | CDU/CSU | |
| Felix Burzer | Grüne | |
| | | |
| | | |

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro | **Sitzung des Innenausschusses (4. Ausschuss)** Montag, 20. März 2017, 11:00 Uhr | Seite 3

## Bundesrat

| Land | Name (bitte in Druckschrift) | Unterschrift | Amts-bezeichnung |
|---|---|---|---|
| Baden-Württemberg | GIUENZL | | |
| Bayern | AFraz | | |
| Berlin | SULYOK | | Referend |
| Brandenburg | Dr. Langel | | Ref'in |
| Bremen | Krebsbach | Krebsbach | Hospitantin |
| Hamburg | | | |
| Hessen | | | |
| Mecklenburg-Vorpommern | PAUCH | | |
| Niedersachsen | TER UEGA | | |
| Nordrhein-Westfalen | | | |
| Rheinland-Pfalz | | | |
| Saarland | | | |
| Sachsen | Kühne | | RR'in |
| Sachsen-Anhalt | Strotenbecker | | ORin |
| Schleswig-Holstein | | | |
| Thüringen | | | |

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

9

Tagungsbüro

**Sitzung des Innenausschusses (4. Ausschuss)**
Montag, 20. März 2017, 11:00 Uhr



| **Ministerium bzw. Dienststelle** (bitte in Druckschrift) | **Name** (bitte in Druckschrift) | **Unterschrift** | **Amts-bezeichnung** |
|---|---|---|---|
| BMI | Bergmann | | RD |
| BMJV | Dr. Hempel | | ltd DGL |
| BMJV | Kraft | | RD |
| BMJV | Kall | | RL |
| BMI | Schokendorf | | RD |
| " | Gaitzsch | | RR |
| " | Zander | | KOK |
| BMJV | | | MI |

# Liste der Sachverständigen
Öffentliche Anhörung am Montag, 20. März 2017, 11.00 Uhr

**Prof. Dr. Matthias Bäcker**
Johannes Gutenberg-Universität Mainz

**Dr. iur. Ulf Buermeyer, LL.M.**
Richter am Landgericht Berlin

**Prof. Dr. Klaus Ferdinand Gärditz**
Rheinische Friedrich-Wilhelms-Universität Bonn

**MD Diethelm Gerhold**
Leitender Beamter
Bundesbeauftragte für den Datenschutz und
die Informationsfreiheit, Bonn

**Prof. Dr. Markus Möstl**
Universität Bayreuth

**Präsident Holger Münch**
Bundeskriminalamt, Wiesbaden

**Prof. Dr. Kyrill-A. Schwarz**
Universität Würzburg

# Sprechregister der Sachverständigen und Abgeordneten

**Einziger Tagesordnungspunkt**

a) Gesetzentwurf der Fraktionen der CDU/CSU und SPD

**Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes**

**BT-Drucksache 18/11163**

b) Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes**

**BT-Drucksache 18/11326**

Vors. **Ansgar Heveling** (CDU/CSU): Meine sehr geehrten Damen und Herren, liebe Kolleginnen und Kollegen, sehr geehrte Gäste, vor allem aber meine sehr geehrten Herren Sachverständige. Ich darf die 107. Sitzung des Innenausschusses eröffnen. Wir führen diese Ausschusssitzung heute als öffentliche Anhörung zu den Entwürfen eines Gesetzes zur Neustrukturierung des Bundeskriminalamtsgesetzes durch.

Ich danke Ihnen, sehr geehrte Herren Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss und aus den mitberatenden Ausschüssen zu beantworten. Die Ergebnisse dieser Anhörung dienen dazu, die Beratung zu diesen Gesetzentwürfen vorzubereiten.

Die heutige Sitzung wird im Parlamentsfernsehen des Deutschen Bundestages übertragen. Ich darf mich sehr herzlich für die schriftlichen Stellungnahmen der Sachverständigen bedanken. Sie sind an die Mitglieder des Innenausschusses und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über diese Sitzung auch beigefügt. Ich gehe davon aus, sehr geehrte Herren Sachverständige, dass Ihr Einverständnis zur öffentlichen Durchführung der Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Ich ernte damit keinen Widerspruch.

Von der heutigen Anhörung wird für ein Wortprotokoll eine Bandabschrift gefertigt. Das Protokoll wird Ihnen zur Korrektur übersandt. Im Anschreiben erhalten Sie dann auch Informationen und weitere Details zur Behandlung. Die Gesamtdrucksache, bestehend aus Protokoll und schriftlichen Stellungnahmen, wird im Übrigen auch ins Intranet-Angebot des Deutschen Bundestages eingestellt.

Zum zeitlichen Ablauf darf ich anmerken, dass insgesamt eine Zeit von 11.00 bis 13.00 Uhr für diese Anhörung vorgesehen ist. Einleitend sind die Sachverständigen um ein Eingangsstatement von längstens 5 Minuten gebeten. Sie sehen, hier läuft keine Uhr rückwärts. Maßgeblich ist also die Uhr des Vorsitzenden. Sollten Sie überziehen, beginne ich mit einem langsamen Hüsteln und werde irgendwann dann zu anderen Maßnahmen greifen, natürlich alles im Rahmen der Verhältnismäßigkeit.

Im Anschluss an die Eingangsstatements beginnt dann die Fragerunde durch die Berichterstatterinnen und Berichterstatter der Fraktionen sowie weitere Abgeordnete. Ich bitte jetzt schon die Fragesteller, grundsätzlich immer den Sachverständigen zu benennen, an den eine Frage gerichtet ist. Dabei dienen knapp gehaltene und limitierte Fragen natürlich dazu, dass auch mehr Kolleginnen und Kollegen zum Zuge kommen und Fragen stellen können.

Ich darf sehr herzlich für die Bundesregierung Herrn Staatssekretär Dr. Günter Krings begrüßen. Dann legen wir mit den Eingangsstatements los. Entsprechend der alphabetischen Reihenfolge darf ich deshalb Herrn Prof. Dr. Bäcker von der Universität Mainz das Wort für das Eingangsstatement erteilen. Bitte sehr Herr Prof. Dr. Bäcker.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Vielen Dank, Herr Vorsitzender, und vielen Dank für die Gelegenheit, heute Stellung zu nehmen. Ich möchte mein Eingangsstatement, genauso wie meine schriftliche Stellungnahme, auf einen kleinen Teil des Gesetzentwurfs beschränken, der allerdings besonders bedeutsam ist. Das sind die Regelungen über die Neustrukturierung der Informationsordnung des Bundeskriminalamts im Wege eines Informationssystems des Amtes selbst und eines Informationsverbunds mit den Landespolizeibehörden.

Das Ziel dieser Regelungen besteht in einer fundamentalen Umgestaltung der Informationsordnung beim Bundeskriminalamt. Bisher gliedert sich der Informationsbestand des Bundeskriminalsamts in mehrere Dateien, die

jeweils spezifische Gegenstände haben – zum Beispiel die Datei „Gewalttäter Sport“ oder die Datei „Politisch motivierte Kriminalität links“. Dieser spezifische Gegenstand trägt auch dazu bei, den Zweck der jeweiligen Datei und der darin erfolgenden Datenverarbeitungen festzustellen. Das wird in sogenannten Errichtungsanordnungen konkretisiert. Diese vertikale Gliederung fällt weg. Jetzt soll ein einheitlicher Informationsbestand des Bundeskriminalamts geschaffen werden, um das dort vorhandene Wissen leichter erschließbar zu machen und Querverbindungen zwischen Personen, Ereignissen usw. aufzufinden.

Auf der anderen Seite ist klar, dass eine völlig unterschiedslose Datenbevorratung in einem polizeilichen Datenpool zu unbestimmten Zwecken mit den Grundrechten nicht im Einklang stünde. Deswegen sind wirksame Regelungen erforderlich, die die Bevorratung von Daten im Informationsbestand und den Zugriff auf diese Daten gesetzlich strukturieren. Der Gesetzentwurf versucht eine solche gesetzliche Strukturierung unter Rückgriff auf das BKAG-Urteil des Bundesverfassungsgerichts und die darin enthaltenen Rechtsfiguren der sogenannten weiteren Nutzung und der hypothetischen Datenneuerhebung. Unter „weiterer Nutzung“ versteht man eine Nutzung von Daten im Rahmen derselben Aufgabe zum Schutz derselben Rechtsgüter oder zur Verhütung derselben Straftaten. Eine hypothetische Datenneuerhebung ist dann zu prüfen, wenn man den Verarbeitungszweck von Daten ändert. In diesem Fall bedarf es eines zumindest vergleichbar gewichtigen neuen Verarbeitungszwecks und außerdem eines konkreten Ermittlungsansatzes.

Das Problem bei dieser Regelungstechnik ist, dass die Rechtsfiguren der weiteren Nutzung und der hypothetischen Datenneuerhebung nicht auf komplexe Datenbevorratungen zugeschnitten sind, sondern auf Datennutzungen. Die Bevorratungsebene wird vom Bundesverfassungsgericht in seinem Urteil überhaupt nicht adressiert. Wenn man jetzt diese Rechtsfiguren auf die Bevorratung von Daten zu Zwecken, die man noch nicht konkret absehen kann, anwendet, ergibt sich folgendes: Soweit solche Bevorratungen als weitere Nutzung behandelt werden, wird die Bevorratung praktisch vollständig freigegeben. Das steht mit dem Urteil eindeutig nicht im Einklang, denn das Bundesverfassungsgericht hat ganz klar festgehalten, dass eine weitere Nutzung nichts daran ändert, dass nicht mehr benötigte Daten gelöscht werden müssen. Bei der hypothetischen Datenneuerhebung ist es genau umgekehrt: Wenn man die hypothetische Datenneuerhebung auf Datenspeicherungen in polizeilichen Datenbeständen anwendet, dann kann man diese Datenbestände eigentlich vergessen. Wenn Sie Daten für die Zukunft erschließbar machen sollen, brauchen Sie dann schon im Moment der Speicherung einen konkreten Ermittlungsansatz. Genau darum geht es bei solchen Datenbeständen aber nicht, sodass der Grundsatz der hypothetischen Datenneuerhebung sich schlicht nicht eignet, um solche Dateien anzuleiten.

Erforderlich ist demgegenüber eine differenziertere Regelung von Datenbevorratung auf der einen Seite und Verwertung der bevorrateten Daten auf der anderen Seite, für die jeweils unterschiedliche Anlässe geschaffen werden müssen. Dabei läge auch nahe, Differenzierungen auf beiden Ebenen – also Bevorratungs- und Verwertungsebene – zwischen den verschiedenen Aufgaben des Bundeskriminalamts und den jeweils betroffenen Personen einzuziehen. Das alles leistet der Gesetzentwurf nur ganz unzureichend. Auf der Ebene der Bevorratung finden sich bestimmte differenzierende Regelungen, die allerdings den bisherigen Rechtszustand fortschreiben, der schon seit Langem unter verschiedenen Gesichtspunkten rechtsstaatlich kritisiert wird. Die Nutzungsebene wird überhaupt nicht eigenständig adressiert, was insgesamt dazu führt, dass ich glaube: Wenn Sie den Entwurf so in Kraft setzen, kippt er entweder vor dem Bundesverfassungsgericht oder aber Sie kriegen vor irgendeinem Verwaltungsgericht irgendwann mal Entscheidungen, die dazu führen, dass das Bundeskriminalamt ohne jede Not ganz empfindlich in seiner Tätigkeit eingeschränkt wird. Beides wären, denke ich, keine wünschenswerten Ergebnisse, was mich zu dem Fazit bringt, dass hier noch erhebliche konzeptionelle Nacharbeit erforderlich ist. Wenn die in dieser Legislaturperiode aus Zeitgründen nicht zu leisten sein sollte, kann ich Ihnen nur dringend dazu raten, den Gesetzentwurf, so ambitioniert, wie er gerade ist, in dieser Form nicht in Kraft zu setzen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Bäcker. Als nächster erhält Herr Dr. Buermeyer das Wort.

SV **Dr. Ulf Buermeyer**, LL.M. (Richter am Landgericht Berlin): Herr Vorsitzender, meine sehr geehrten Damen und Herren, auch ich danke zunächst sehr herzlich für die Einladung und für die Gelegenheit, einige Aspekte zur Sprache zu bringen.

Der Gesetzentwurf, der hier zur Beratung vorliegt, bezweckt eine Systematisierung der Rechtsgrundlagen der Arbeit des Bundeskriminalamts und ist im Grundsatz natürlich begrüßenswert, denn in der Praxis waren nicht zuletzt die §§ 20a bis x letztlich schwer zu handhaben. Der Unterschied zwischen i und l ist jedenfalls in der Schriftform nicht immer ganz klar geworden – mit anderen Worten: Das halte ich für einen wesentlichen Schritt. Allerdings, so sinnvoll Systematisierung auch ist – man sollte sich, denke ich, immer überlegen, ob man tatsächlich überzeugende Lösungen gefunden hat. Insofern möchte ich zunächst die Analyse von Herrn Prof. Dr. Bäcker ausdrücklich unterstreichen. Die Datenverarbeitung durch das Bundeskriminalamt neu zu regeln und sie auch so, wie das der Entwurf vorsieht, gleichsam vor die Klammer zu ziehen, halte ich für eine sehr überzeugende Lösung, aber nicht die Details. Ich denke, das ist schon in dem angeklungen, was Prof. Dr. Bäcker gerade sagte: Die bisher das Datenschutzrecht leitenden Grundsätze, nämlich die Grundsätze der Datensparsamkeit und der Zweckbindung, werden durch das beabsichtigte Datenpooling beim Bundeskriminalamt in ihr Gegenteil verkehrt. Ich denke, auch der Kollege von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wird dazu nochmal Stellung nehmen. Daher auch von meiner Seite an dieser Stelle eine deutliche Warnung, den Gesetzentwurf so umzusetzen, wie er uns heute vorliegt.

Den Schwerpunkt meiner Ausführungen möchte ich aber auf den sogenannten Terrorismusteil des Entwurfs setzen. Das sind die polizeilichen Befugnisse für das Bundeskriminalamt in Abschnitt V des Entwurfs, also die §§ 38 ff. Hierbei handelt es sich in weiten Bereichen um eine nahezu wörtliche Übernahme von Passagen aus dem Urteil des Bundesverfassungsgerichts. Meine Damen und Herren, das ist eine Gesetzgebungstechnik, die uns in den vergangenen Jahren durchaus verschiedentlich untergekommen ist. Sie erweckt zunächst mal den Eindruck einer sehr akribischen Umsetzung der verfassungsgerichtlichen Vorgaben. Ich denke aber gleichwohl, dass der Gesetzgeber mit einer solchen Copy-and-Paste-Technik letztlich seine Aufgabe verfehlt. Aufgabe des Gesetzgebers ist es nämlich gerade nicht, Gesetze zu verfassen, die die maximalen äußersten Grenzen dessen in Gesetzesform gießen, was gerade noch von Verfassung wegen tragfähig ist. Aufgabe des Gesetzgebers ist – wie das immer so schön auf eine Kurzformel gebracht wird – eine Abwägung zwischen Freiheit und Sicherheit. Ich denke, insbesondere der Terrorismusteil dieses Gesetzes leistet eine solche Abwägung nicht. Er geht an die Grenzen dessen, was von Verfassung wegen gerade noch möglich sein mag. Um das einmal etwas bildhaft zu formulieren, bewegt sich der Gesetzgeber gerade nicht in der Mitte einer vorgegebenen Fahrspur möglicher Grundrechtseingriffe, sondern schrammt konsequent an der rechten Leitplanke entlang. Das ist in weiten Teilen zwar verfassungsgemäß – zu Ausnahmen, wo also auch die Grenzen dessen überschritten sind, was das Bundesverfassungsgericht vorgegeben hat, kommen wir vielleicht gleich noch – aber es ist jedenfalls aus der Perspektive der Rechtspolitik eine sehr eindeutige Priorisierung der Interessen des Bundeskriminalamts.

Ich möchte Ihnen jetzt noch ganz kurz zwei Beispiele nennen, bei denen das aus meiner Sicht besonders augenfällig wird. Das Eine sind die Befugnisse für den Einsatz von Staatstrojanern, das ist § 49 des Entwurfs. Hier hat das Bundesverfassungsgericht vergleichsweise wenig Vorgaben gemacht und der Gesetzentwurf schließt diese erhebliche rechtsstaatliche Lücke, die Karlsruhe an dieser Stelle gelassen hat, nicht. So fehlt es an jeden rechtsstaatlichen Mindestanforderungen, insbesondere technischen Anforderungen, an den Staatstrojaner. Natürlich soll sich das Bundeskriminalamtsgesetz nicht irgendwann wie ein Aufgabenheft, ein Pflichtenheft, für Software-Entwickler lesen, aber man muss doch zumindest die wesentlichen Vorgaben machen und auch ein Verfahrensrecht etablieren, das sicherstellt, dass die gesetzlichen Vorgaben auch eingehalten sind. Zum Beispiel

könnte man an eine Verordnungsermächtigung denken, die es dann beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik erlauben würde, genauere technische Vorgaben zu machen. Ich denke, das Bundesverfassungsgericht war an dieser Stelle vergleichsweise großzügig, hat sich dazu wenig geäußert, aber da ist der Gesetzgeber dringend aufgerufen einzugreifen, denn das wären letztlich auch Grundlagen für eine rechtssichere Anwendung von Staatstrojanern, wenn man das denn tatsächlich will.

Zweiter Punkt im Kontext Staatstrojaner ist die Cybersicherheit. Der Gesetzentwurf schafft Anreize für das Bundeskriminalamt, Sicherheitslücken zu sammeln – also das Bundeskriminalamt oder die Zentralstelle ZITiS, die sich ja zurzeit im Aufbau befindet. Sicherheitslücken sammeln bedeutet, Sicherheitslücken nicht schließen zu lassen. Wer ein Arsenal von Sicherheitslücken aufbaut, von sogenannten Zero-Day-Exploits, um mit Hilfe dieser Sicherheitslücken in Systeme von möglicherweise Gefährdern einzudringen, der nimmt dabei in Kauf, dass Millionen von Systemen auf der ganzen Welt unsicher bleiben, weil er die Sicherheitslücken eben nicht dem Hersteller melden kann, zum Beispiel der Firma Microsoft, damit diese Sicherheitslücken geschlossen werden. Ich denke, das ist eine Güterabwägung, die, jedenfalls aus der Perspektive eines Gesetzgebers, schlechthin untragbar ist, der sich ja eigentlich die Cybersicherheit auch auf die Fahne geschrieben hat. Ganz herzlichen Dank soweit.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Dr. Buermeyer. Dann erhält als nächstes Herr Prof. Dr. Gärditz das Wort.

SV **Prof. Dr. Klaus Ferdinand Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Vielen Dank Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete. Auch ich muss mich auf einige Stichpunkte beschränken. Das Gesetz ist sehr lang, eine Detailanalyse zu allen möglichen Fragen ist in diesem Rahmen nicht möglich.

Ich will ganz allgemein etwas zu dem Stil des Gesetzes und der Regelungstechnik sagen und dann vielleicht ein paar Punkte herausgreifen, die mir diskussionswürdig erscheinen. Mein Vorredner hat das bereits angedeutet: Das Gesetzt versucht hier letzten Endes eine eins-zu-eins-Umsetzung dessen vorzunehmen, was das Bundesverfassungsgericht in den Entscheidungsgründen ausgeführt hat. Ich will jetzt gar nicht die inhaltlichen Fragen bewerten – also etwa ob das an der rechten Leitplanke entlang schrammt, wie der Kollege gesagt hat. Mir geht es eigentlich eher um die Regelungstechnik, die ich für problematisch halte. Eigentlich ist das Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz von seinem Stil und seiner Detailierungsdichte an den Grenzen dessen, was eigentlich die Funktion von Verfassungsgerichtsbarkeit ausmacht, ob man das jetzt inhaltlich für richtig hält oder für nicht. Es wird also ganz stark in den Bereich der politischen Gestaltung eingegriffen. Jetzt haben Sie natürlich dieses Urteil auf dem Tisch und müssen irgendwie damit leben. Ich halte es aber für problematisch, wenn man diese Entwicklung einer extremen Konstitutionalisierung des Sicherheitsrechts noch katalysiert, indem man die Begrifflichkeiten des Bundesverfassungsgerichts übernimmt, eins-zu-eins in den Gesetzeswortlaut hineingießt, und dann später damit leben muss, dass jeder Interpret, der das Gesetz anwendet, gar nicht mehr nach dem politischen Regelungswillen, den Zwecken und den dahinter stehenden politischen Kompromissen fragt, sondern eigentlich sofort zur Anthrazitsammlung greift und fragt: Was hat das Bundesverfassungsgericht hier gewollt? Sie bringen sich als Parlament im Grunde genommen selbst aus dem Spiel, das halte ich für etwas unglücklich.

Inhaltlich möchte ich einfach willkürlich Punkte herausgreifen, die mir aus der Vielfalt der Regelungen aufgefallen waren. Erstens: Hypothetische Datenneuerhebung. Einige Kollegen haben in ihren Stellungnahmen auch darauf hingewiesen. Dieses Kriterium, was letzten Endes ein Leerlaufen der Ermächtigungen bei der Weiterverwendung verhindern soll, wurde vom Bundesverfassungsgericht – Zitat: „Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen gefordert.“ Hier soll es jetzt zu einem allgemeinen Grundsatz des Datenschutzrechts werden. Mir leuchtet das nicht recht ein, dass ich diese Anforderungen auch für Daten, die ich aus einer schlichten Befragung gewonnen habe, weiter beachten muss. Da wird eigentlich einer Engführung weiterer Vorschub geleistet.

Zwei Fragezeichen, die mir aufgefallen waren – vielleicht habe ich aber auch irgendetwas übersehen – die Regelung des § 12 behandelt zwei praktisch wichtige Probleme nicht. Zum einen stellt sich die Frage, was mit rechtswidrig erhobenen Daten ist, bei denen es aber ein legitimes Weiterverwendungsinteresse geben kann, ob die von den erhobenen Daten miterfasst sind oder ob die Regelung voraussetzt, dass die Daten im Primäreingriffsrecht rechtmäßig erhoben worden sind. Wir wissen aus der Rechtsprechung auch des Bundesverfassungsgerichts, dass es unter Umständen gerechtfertigt sein kann, rechtswidrig erlangte Daten trotzdem weiter zu verwenden. Zweite Frage, Zufallsfunde – kommen auch häufiger vor. Dieses Problem ist auch nicht eindeutig geregelt. Sind Zufallsfunde, die ich anlässlich eines Ermittlungseingriffs mache, eigentlich erhobene Daten, die ich dann im Rahmen des § 12 Absatz 1 bis 2 weiter verwenden darf?

Ein letzter Punkt vielleicht noch – damit wir heute nicht nur über Datenschutzrecht reden müssen, auch wenn das sicherlich im Mittelpunkt steht – die neue Befugnis der elektronischen Aufenthaltsüberwachung, § 56 Bundeskriminalamtsgesetz. Ich habe mir diese angesehen, weil in der politischen Diskussion im Vorfeld die Verhältnismäßigkeit in Frage gestellt worden ist. Ich bin zu der Auffassung gelangt, dass die Regelung, wie sie jetzt im Gesetz vorgesehen ist, den Anforderungen der Verhältnismäßigkeit genügt. Insbesondere lässt sich gegen die Regelung nicht einwenden, dass sie ohnehin nichts bringe. Natürlich kann ich einen zum Selbstmordanschlag entschlossenen Attentäter nicht von diesem Anschlag abhalten, indem ich ihm eine elektronische Fußfessel anlege. Das ist aber vielleicht das Extremszenario. Die geltende Regelung kann durchaus sinnvolle Anwendungsbereiche haben, zum Beispiel bei jemandem, der sich in einer Vereinigung nach §§ 129a, 129b StGB bewegt und vielleicht einen künftigen Anschlag plant. Die Vorbereitung, die kommunikative Abstimmung, die Beschaffung etwa von Waffen, von Sprengstoffen, kann erheblich erschwert werden, wenn er in der Zwischenzeit dieser Überwachung unterliegt. Die rechtsstaatliche Einhebung ist meines Erachtens ausreichend. Die Befristung auf 3 Monate auch. Ich darf zu guter Letzt darauf hinweisen, dass vielleicht auch diese Regelung ein sinnvoller Kompromiss ist, mit einer milderen Maßnahme einzusteigen, denn diese Überwachung ist ja auch der Versuch, nicht die Inhaftnahme regeln zu müssen, die in denkbaren Extremfällen für diese Zeiträume ja durchaus auch in Betracht käme. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Gärditz. Wir haben vereinbart, dass auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Gelegenheit zur Stellungnahme bekommt. Sie kann persönlich heute nicht da sein. Dafür ist Herr Gerhold aus ihrem Bereich heute anwesend und Ihnen darf ich jetzt das Wort geben.

SV **MD Diethelm Gerhold** (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Dankeschön Herr Vorsitzender. Ich darf mich dafür bedanken, dass wir Gelegenheit bekommen haben, für die BfDI heute hier Stellung zu nehmen und möchte vorab auf unsere schriftliche Stellungnahme verweisen, in der wir versucht haben, zu den für uns besonders wichtigen Punkten ausführlich Stellung zu nehmen.

Der Entwurf wird das polizeiliche Datenschutzrecht grundlegend verändern. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem aktuellen Urteil zum BKA-Gesetz umzusetzen, und auch nicht darauf, die Vorgaben, die die JI-Richtlinie der Europäischen Union gemacht hat, umzusetzen, sondern er geht teilweise weit darüber hinaus und ist in seinen Folgen, wenn er so verabschiedet wird, wie er eingereicht worden ist, noch gar nicht abzusehen.

Aus der Sicht des Datenschutzes sind deswegen eine Reihe von Änderungen dringend geboten. Das Ganze ist aber so umfangreich, dass ich mich heute nur auf einige Punkte beschränken möchte. Da geht es einmal, Herr Prof. Dr. Bäcker hat schon darauf hingewiesen, um das neue Informationssystem des BKA, das das bisherige Verfahren in grundlegender Hinsicht ablöst. Es ist dabei zu berücksichtigen, dass all das, was in den letzten Jahrzehnten seit dem Volkszählungsurteil als Verfahrenssicherung und überhaupt als datenschutzrechtliche Sicherungen im Zuge der Rechtsprechung des Bundesverfassungsgerichts eingeführt worden ist, jetzt abgelöst werden soll. Das ist ein

entscheidender Wechsel in den Verfahren und hat natürlich auch entscheidende Auswirkungen. Jeder muss damit rechnen, in diesem Informationssystem erstmal gespeichert werden zu können. Das geht mitunter ganz schnell. Da reicht es, dass Sie am falschen Ort gewesen sind, da reicht, dass Sie jemand völlig unbegründeter Weise anzeigt, da reicht, dass Sie bei irgendwelchen Überprüfungsmaßnahmen mit dabei gewesen sind, und Sie sind ganz schnell in dem System drin. Da sind dann entsprechende Schutzmechanismen erforderlich. Es genügt ein einfacher Verdacht für die Speicherung, aber das bisherige Regelungssystem schützt Sie davor, dass Sie dann auf Ewigkeiten in dem System gespeichert bleiben. Da wird sich in Zukunft einiges ändern. Es ist völlig klar, die Polizei muss jedem Verdacht nachgehen. Sie muss auch entsprechende Datenspeicherung vornehmen können. Das kann man als polizeiliche Vorratsdatenspeicherung bezeichnen. Das hat auch soweit durchaus seine Berechtigung, wenn es einen fairen Ausgleich zwischen den Allgemeininteressen und den Grundrechten der betroffenen Person gibt. Dieser Ausgleich ist aber jetzt in Gefahr, weil das künftige Informationssystem nicht mehr, wie bisher, in logische Dateien gegliedert ist. Es wird auch keine Errichtungsanordnung mehr geben, die die Rechtsgrundlage und vor allem die Zweckbindung der Speicherung festschreibt, die Zwecke müssen gar nicht mehr angegeben werden. Es kommen stattdessen alle Daten in einen großen Topf. Diese Methode des Datenabgleichs aus diesem Topf heraus ist nicht mehr eingegrenzt. Die Datenfelder und Daten sind beliebig miteinander verknüpfbar, personenübergreifend. Jeder Abgleich kann zu neuen Datenverknüpfungen führen, was – da komme ich gleich noch darauf zu sprechen – auch die Speicherdauer entsprechend verlängern wird und die Errichtungsanordnung wird es nicht mehr geben. Dies führt auch dazu – aber das nur am Rande –, dass unsere Kontrolle sehr erschwert wird: Muss die Zweckbindung gar nicht mehr angegeben werden, können wir natürlich auch nicht mehr prüfen, ob die Weiterverarbeitung zweckentsprechend stattfindet.

Ein weiteres Problem, auf das ich kurz eingehen will, ist die sogenannte Mitziehautomatik. Das bedeutet, dass künftig jede Zuspeicherung, aus welchem Anlass auch immer, dazu führt, dass die Daten weiterhin gespeichert bleiben können. Bisher gab es nach einem gewissen Zeitraum in den einzelnen Dateien sogenannte Aussonderungsprüffristen, das heißt, es musste kontrolliert werden, ob die Daten weiter dort gespeichert bleiben müssen oder ob sie gelöscht werden können. Das war ein Verfahren, was es der Polizei ermöglicht hat, wichtige Daten, die noch gebraucht werden, auch weiterhin zu speichern, aber eben all das, was mittlerweile überholt, nicht mehr aktuell ist, dann auch auszusondern. Durch dieses neue Verfahren wird dies so nicht mehr sein. Es reicht jede Zuspeicherung, um dann erst einmal ohne weitere Prüfung den gesamten Datenbestand weiter zu perpetuieren und das kann über Jahrzehnte gehen, ohne dass die betroffene Person – wir haben in unserer schriftlichen Stellungnahme ein kleines Beispiel dazu gebildet – etwas dagegen unternehmen kann.

Als Letztes noch ganz kurz zu den Begrifflichkeiten. Es wird jetzt der Begriff des Weiterverarbeitens in vielen Paragraphen eingeführt. Weiterverarbeiten ist undifferenziert. Bisher wurde zwischen Speicherung, Übermittlung, Nutzung und weiteren Begriffen unterschieden. Weiterverarbeiten ist alles. Dieser breite Begriff macht es aber unmöglich, für bestimmte Verarbeitungsformen bestimmte Kriterien und Voraussetzungen festzulegen. Das heißt, Sie können jetzt nicht mehr für das Speichern andere Regelungen, andere Sicherheitsmechanismen vorsehen als etwa für das Übermitteln an Dritte. Und auch darin sehen wir ein ziemliches Problem. Dabei möchte ich es bewenden lassen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Gerhold. Dann gehe ich jetzt auf die von mir aus gesehen linke Seite weiter. Herr Prof. Dr. Möstl.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): Vielen Dank Herr Vorsitzender, meine Damen und Herren. Der Gesetzentwurf dient unter anderem der Umsetzung der Vorgaben des Bundesverfassungsgerichts. Diese Vorgaben sind ungewöhnlich dicht und steigen tief ins Detail der einfachgesetzlichen Dogmatik hinab. Das Bundesverfassungsgericht ist nicht zu Unrecht dafür kritisiert worden, wie weit es sich in das Feld des Gesetzgebers vorgewagt hat. Dennoch ist der Entwurf von dem sichtlichen Bemühen geprägt, die vielen Detailvorgaben getreulich umzusetzen, bis hin zur Technik der wortwörtlichen Übernahme.

Dies ist unbedenklich, nicht aber ist es in jedem Fall zwingend. Bindung an die tragenden Gründe des Urteils bedeutet nicht die Pflicht zur wortwörtlichen Übernahme. Der Gesetzgeber bleibt zur eigenständigen Systembildung berufen. Auch hat er etwa im Lichte neuer Bewertungen zur Sicherheitslage durchaus einen gewissen Spielraum des Festhaltens am vom Bundesverfassungsgericht kritisierten Regelungsanliegen. Unbenommen ist es ihm schließlich, dogmatische Ansätze des Bundesverfassungsgerichts weiter zu denken und in anderen Kontexten anzuwenden.

Zunächst einige Gedanken zur Fassung der Eingriffstatbestände. Das Urteil des Bundesverfassungsgerichts führt zu einer gewissen Konsolidierung der tatbestandlichen Anforderungen an Informationseingriffe, die bereits im Gefahrenvorfeld ansetzen. Der Gesetzentwurf greift die diesbezüglichen Formulierungsvorschläge der Urteilsgründe in der Weise auf, dass sie quasi wortwörtlich übernommen werden. Dies ist einwandfrei, wenngleich vielleicht die Chance vertan wird, die Polizeirechtsdogmatik allgemein fortzuentwickeln, indem etwa eine vor die Klammer gezogene präzisierende Regelung zu dieser neuen Eingriffsschwelle geschaffen wird. Der bayerische Polizeigesetzgeber will die neue Schwelle nach derzeitigen Überlegungen zum Beispiel als drohende Gefahr definieren. Besonders erwähnenswert ist, dass der Entwurf die neue Eingriffsschwelle im Gefahrenvorfeld auch für die neuen Befugnisse des Aufenthalts- und Kontaktverbots und der elektronischen Aufenthaltsüberwachung verwenden will. Dies ist nicht ganz so selbstverständlich, wie es die Entwurfsbegründung vielleicht suggeriert. Denn ausdrücklich entwickelt hat das Bundesverfassungsgericht diese Vorfeldschwelle allein für reine Informationseingriffe. Bei den genannten Befugnissen handelt es sich aber nicht um reine Ermittlungseingriffe, sondern um aktionelle Anordnungen, mit denen auch bereits in den schadensrechtlichen Kausalverlauf eingegriffen wird und die Gefahrentstehung unterbunden werden soll. Aktionelle kausalverlaufsrelevante Eingriffe sind aber prinzipiell auch von Verfassung wegen an die Gefahrenschwelle gebunden. Ausnahmen von dieser Regel sind jedoch möglich und um eine solche zulässige Ausnahme handelt es sich auch hier. Denn jedenfalls im Bereich der Terrorismusbekämpfung darf der Gesetzgeber zu Recht davon ausgehen, dass es bisweilen zu riskant sein kann, die polizeilichen Aktivitäten im Gefahrenvorfeld auf reine Beobachtung zu beschränken, da zu befürchten steht, dass sich eine Gefahr vielleicht plötzlich und mit großem Schaden realisiert, noch bevor sie als solche erkannt und aufgeklärt werden konnte. In eben solchen Fällen kann es zulässig sein, vorgelagert bereits die weitere Entstehung einer Gefahr verhindern zu wollen. Die Überlegungen des Bundesverfassungsgerichts werden insoweit folgerichtig weiter gedacht.

Ein Wort ist schließlich zum horizontal wirkenden Datenschutzkonzept des Gesetzentwurfs zu sagen. Dass der Gesetzgeber zu einem die prinzipielle Vernetzung sicherstellenden, einheitlichen Verbundsystem, das von einem horizontal wirkenden Datenschutzkonzept beherrscht wird, übergehen will, entspricht einem legitimen Ziel, das in Artikel 87 Absatz 1 Satz 2 Grundgesetz – Zentralstellenfunktion für das polizeiliche Auskunft- und Nachrichtenwesen – überdies verfassungsrechtlich fundiert ist. Zur Wahrung des Datenschutzes soll in § 12 (neu) flankiert durch die Kennzeichnungspflicht in § 14 (neu) bei Zweckänderung generell auf den Grundsatz der hypothetischen Datenneuerhebung zurückgegriffen werden, wie ihn das Bundesverfassungsgericht entwickelt hat. Dies ist sicher zulässig, dennoch fällt auf, dass der Entwurf damit deutlich über das hinausgeht, was das Bundesverfassungsgericht zwingend verlangt hat. Denn es hat seine Rechtsprechung ausdrücklich allein auf Daten aus eingriffsintensiven Maßnahmen bezogen und den vergleichsweise strengen Grundsatz der hypothetischen Datenneuerhebung nicht zum allgemeinen Grundsatz des polizeilichen Datenverarbeitungsrechts erhoben. Wenn er dennoch zu einem solchen gemacht werden soll, steht zu befürchten, dass dies die Arbeit der Polizei stärker erschwert, als es verfassungsrechtlich zwingend ist und dass gegebenenfalls Schutzlücken entstehen. Die vom Bundesrat geäußerte Bitte zu prüfen, ob eine so ehrgeizige Regelung wirklich nötig ist, scheint mir vor diesem Hintergrund plausibel.

Ein letztes Wort vielleicht noch zu einem Einwand, den Herr Prof. Dr. Bäcker gebracht hat, der befürchtet hat, dass weder zum Zeitpunkt der

Speicherung noch zum Zeitpunkt des Abrufs sichergestellt wird, dass der Grundsatz der Zweckbindung eingehalten wird. Also nach meiner Lektüre des Gesetzes habe ich den Eindruck, dass sehr wohl jedenfalls auf der Ebene der Datennutzung diese Zweckbindung sichergestellt wird. Das ergibt sich, meines Erachtens, sowohl aus § 15 als auch aus § 29 Absatz 4, sodass ich insoweit einen Angriffspunkt für nicht gegeben erachte. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Möstl. Und nun Herr Münch, Präsident des Bundeskriminalamts.

SV Präsident **Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank Herr Vorsitzender. Sehr geehrte Abgeordnete, der Ihnen vorliegende Entwurf des neuen BKA-Gesetzes ist aus meiner Sicht mehr als eine partielle Ergänzung oder Anpassung des bestehenden Gesetzes. Er ist in weiten Teilen ein vollständig neues Regelwerk. Er ist nicht nur umfangreicher, sondern auch anders strukturiert. Er greift die Vorgaben des Bundesverfassungsgerichtes aus seiner Entscheidung vom 20. April 2016 auf, Stichwort „hypothetische Datenerhebung“, das ist hier mehrfach gefallen, ebenso wie die EU-Vorgaben im Hinblick auf die Stärkung des Datenschutzes. Darüber hinaus folgen moderne Regelungen, die die Zentralstellenfunktion des BKA stärken und die informationelle Verknüpfung im polizeilichen föderativen Verbund zukunftsweisend neu strukturieren sollen. Dabei gibt es dann noch maßvolle und zugleich fachlich gebotene Erweiterungen der Befugnisse zur Abwehr von Gefahren im Bereich des internationalen Terrorismus, Strichwort „elektronische Aufenthaltsüberwachung“. Lassen Sie mich kurz auf einige Punkte eingehen.

Das Bundesverfassungsgericht hat mit Urteil vom 20. April des letzten Jahres Klarheit geschaffen und zunächst grundsätzlich die Notwendigkeit und Zulässigkeit der 2009 dem BKA im Gesetz eingeräumten Aufgaben und Befugnisse bei der Abwehr von Gefahren des internationalen Terrorismus anerkannt. Die vom Bundesverfassungsgericht für notwendig erachteten konkreten Anpassungen werden mit dem vorliegenden Gesetzentwurf vorgenommen. So enthält er weitergehende Vorgaben für den Kernbereichsschutz. Das Verfassungsgericht hat umfangreiche zusätzliche Regelungen zum Kernbereichsschutz eingefordert, nicht nur für besonders schwere Eingriffe, sondern auch letztlich für viele weitere verdeckte Maßnahmen bis hin zur längerfristigen Observation. Die hieraus erwachsenen und nun zu regelnden Dokumentations-/Prüf- und Berichtspflichten bis hin zur Vorlage in Zweifelsfällen beim zuständigen Gericht werden natürlich auch zusätzliche Ressourcen in nicht unerheblichem Maße binden. Erst recht gilt das für die Vorgabe einer vollständigen Prüfung der erhobenen Daten aus Wohnraumüberwachung und Online-Durchsuchungen nach dem BKA-Gesetz, die durch eine externe Stelle auf Kernbereichsrelevanz zu prüfen sind. Das bedeutet eine 24/7-Betreuung der Maßnahmen auf Seiten von Polizei und Justiz, hier dem Amtsgericht Wiesbaden, mit einem entsprechend einzurichtenden Work-Flow. Dabei kommt es mir jetzt weniger auch auf die Frage der Ressourcen an, die das braucht, sondern, ich denke im Bereich der Online-Durchsuchung ist das eher unkritisch, weil wir nicht über Live-Daten reden. Im Bereich der Wohnüberwachung kommt es darauf an, diese Prozesse sehr gut zu gestalten, um hier nicht durch zusätzliche Beteiligte und zusätzliche Schritte in ein Risiko zu gehen.

Auch die grundsätzliche Beachtung des Prinzips der hypothetischen Datenneuerhebung und die Reform der polizeilichen IT-Architektur folgen aus dem Gesetzentwurf. Das Bundesverfassungsgericht hat, nach eigener Aussage, ein Grundsatzurteil zum polizeilichen Datenschutz gefällt. Es hat zwar keine technischen Vorgaben zur Umsetzung und Einhaltung des Prinzips der hypothetischen Datenneuerhebung aufgestellt, dennoch war das Urteil Anlass für uns, eine Reform der polizeilichen IT-Architektur zu beschließen und zügig mit der Umsetzung zu beginnen. Denn dieses Prinzip kann nach unserer Einschätzung nicht durch eine Nachbesserung der IT-basierten Rahmenbedingungen erreicht werden, denn das Ziel ist ja, die Vorgaben des Verfassungsgerichtes so umzusetzen, dass im Polizeialltag die befassten Akteure in einer praxisgerechten Lösung auch die Daten verfügbar haben, die der einzelne Polizeibeamte dann auch braucht. Dazu braucht es einen einheitlichen Rahmen in Bund und Land und letztendlich war das der Grund auch zu sagen: Wir brauchen jetzt auch eine neue IT-Infrastruktur, die die Schwächen der alten Struktur, nämlich eine

zu langsame Anpassungsfähigkeit, die auch ein Risiko darstellt, beseitigt.

Weiterhin erfolgt eine Modernisierung der Zentralstellenrolle des BKA. Der Gesetzentwurf sieht vor, dass das Bundeskriminalamt zur Unterstützung von Polizeien von Bund und Ländern bei der Verhütung und Verfolgung von Straftaten neben Koordination und Beratung einerseits und dem Angebot von sogenannten Special-Services andererseits, hier auch durch die Schaffung von Kompetenzzentren gemäß § 2 Absatz 5 Nr. 2 des Gesetzentwurfes eine neue Rolle schafft. Insbesondere in den Bereichen der Informations-, Einsatz- und Kriminaltechnik dürfen wir – das gilt für Polizei in Bund und Ländern – unsere wertvollen personellen und sachlichen Ressourcen nicht für Doppelarbeit oder Kooperationsmängel vergeuden. Hier ist durch diese, wenn Sie so wollen, Auftragszuschreibung das BKA in der Rolle, solche neuen Strukturen voranzutreiben. Außerdem soll eine Erleichterung des Informationsaustausches innerhalb der EU erreicht werden. Die Optimierung der Nutzung und Teilung vorhandenen polizeilichen Wissens im nationalen Bereich ist unabdingbar, muss aber auch im internationalen Bereich intensiviert werden. Ebenso wie organisierte Kriminalität und Terrorismus nicht an Landesgrenzen halt machen, darf der polizeiliche Informationsaustausch im Zeitalter der Globalisierung durch geografische Grenzen und nationalstaatliche Einzelregelungen nicht erschwert werden, solange es keine gerechtfertigten Gründe für Restriktionen gibt.

Mit dem Gesetzentwurf werden einzelne Befugnisnormen angepasst und vor allem die elektronische Aufenthaltsüberwachung, die sogenannte Fußfessel, wird eingeführt. Das war hier schon kurz ein Thema.

Anlässlich der ohnehin notwendigen Neustrukturierung wurde die Gelegenheit genutzt, die Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus sowie zur Wahrnehmung der Zentralstellenaufgabe und der Strafverfolgung über die Vorgaben des Bundesverfassungsgerichtes hinaus anzupassen und maßvoll zu erweitern. Novum ist die elektronische Aufenthaltsüberwachung. Die Regelung zur sogenannten Fußfessel soll ebenso wie die Ermächtigungsgrundlage zur Verhängung von Aufenthalts- und Kontaktverboten im BKA-Gesetz verankert werden. Für das BKA beschränkt sich diese Befugnis im neuen BKA-Gesetz auf Ausnahmefälle der eigenen originären Aufgabenwahrnehmung zur Abwehr von Gefahren des internationalen Terrorismus in Fällen, in denen die Zuständigkeit eines Landes noch nicht erkennbar ist, eine länderübergreifende Gefahr vorliegt oder ein Land um Übernahme ersucht. Vor allem die elektronische Aufenthaltsüberwachung zur Gefahrenabwehr steht im Fokus der öffentlichen Diskussion. Aufenthalts- und Kontaktverbote sind allerdings als weitere Maßnahmen im optionalen Instrumentenkasten zu verstehen, die uns zur Verfügung stehen müssen, um auch offene Maßnahmen gegen Gefährder ergreifen zu können und sie letztendlich auch dann mit der sogenannten Fußfessel überwachen zu können. Das Risiko eines Informationsverlustes, schon in Form der Unkenntnis über den Aufenthalt eines polizeilich detektierten sogenannten Gefährders, dürfen wir nicht eingehen. Dem staatlichen Schutzauftrag und der berechtigten Erwartungshaltung der Bevölkerungen würden wir dann nicht gerecht. Insofern halte ich auch aus der praktischen Erwägung heraus diese Erweiterungen für sinnvoll.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Münch. Herr Prof. Dr. Schwarz, Sie haben nun das Wort.

SV **Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Herr Vorsitzender, meine sehr geehrten Damen und Herren Abgeordnete, wenn man sich den vorliegenden Gesetzentwurf genauer anschaut, dann wird deutlich, dass das sehr viel mehr ist als nur der Versuch, die Vorgaben des Bundesverfassungsgerichts eins-zu-eins umzusetzen. Bisweilen hat man den Eindruck, es ist schon fast der Versuch, noch darüber hinaus zu gehen, was das Bundesverfassungsgericht bereits an engen Kautelen aufgestellt hat. Vor dem Hintergrund sollte man jedenfalls – das zunächst vielleicht auch noch zur Einleitung – davor warnen, den Sicherheitsbehörden noch engere Maschen aufzuerlegen.

Natürlich ist Sicherheitsrecht und Sicherheitspolitik ein Spiegel der gesellschaftlichen Entwicklung und natürlich kann man auch sagen, dass wir – jedenfalls wenn man sich die Rechtsprechung des Bundesverfassungsgerichts bis hin zur

Entscheidung vom April letzten Jahres anschaut – den Eindruck gewinnen können, dass Sicherheitspolitik als grundrechtschonende Sicherheitspolitik in den letzten 15 Jahren in Karlsruhe gemacht wurde, jedenfalls, wenn man sich die Anzahl der Entscheidungen und die in den Entscheidungen getroffenen Aussagen genauer anschaut. Natürlich ist vor dem Hintergrund der jetzige Gesetzentwurf auch erkennbar von dem Bemühen gekennzeichnet, ein weiteres Verfahren in Karlsruhe möglichst zu vermeiden, wobei auch das selbstverständlich nicht auszuschließen ist.

Ich möchte mich vor dem Hintergrund zunächst auf der Grundlage einiger ganz allgemeiner Ausführungen – die Sie zum Teil auch in meiner schriftlichen Stellungnahme haben, die aber auch nochmal darüber hinausgeht – zwei wesentlichen Bereichen zuwenden. Das ist zum einen die Problematik des sogenannten Staatstrojaners oder der Infiltration informationstechnischer Systeme. Das ist zum anderen – Herr Münch hat gerade darauf hingewiesen, dass das nun auch tatsächlich ein neues operatives Mittel im BKA-Gesetz ist – die elektronische Aufenthaltsüberwachung. Zu diesen beiden Bereichen möchte ich hier noch etwas Genaueres sagen.

Zunächst einmal – was man sicherlich feststellen kann, das ist ja auch einer der Gründe für das hier heute zu besprechende und zu begutachtende Gesetz – ist offensichtlich, dass das allgemeine Sicherheitsinstrumentarium in den letzten Jahren oder Jahrzehnten immer nur Reaktionen auf vorgefundene Veränderungen waren. Das heißt, das hat sich letzten Endes offensichtlich aus den Bedürfnissen der Praxis heraus nicht als ausreichend erwiesen. Nun kann man vor dem Hintergrund natürlich sagen: Wo bettet man das Ganze ein? Das Ganze ist klassischerweise in das Verhältnis von Freiheit und Sicherheit eingebettet und das ist etwas, worüber man lange sinnieren kann. Aber – und das wird in der gesamten Diskussion eigentlich ausgeblendet – dieses Verhältnis von Freiheit und Sicherheit auszutarieren ist in einer Hinsicht ganz einfach möglich. Denn Sicherheit ohne Freiheit ist sofort denkbar. Das ist nicht erstrebenswert, aber es ist zumindest denkbar. Aber umgekehrt ist Freiheit ohne Sicherheit undenkbar. Denn in einem freiheitlichen Gemeinwesen brauchen Sie auch die Sicherheit, um sich entsprechend frei verhalten zu können. Nun ist es – und das sollte man sich vielleicht auch einmal vor Augen führen – nicht so sehr der Gesetzgeber, der immer wieder die Verhältnisse von Freiheit und Sicherheit in die eine oder andere Richtung verschiebt, auch wenn das das Bundesverfassungsgericht letzten Endes dem Gesetzgeber genau zugebilligt hat. Ich will aus einer Entscheidung zitieren: „Die Balance zwischen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch nicht von ihm grundlegend verschoben werden.“ Wenn man sich das vor Augen führt, kann man sagen: Es ist schon fraglich, ob es wirklich der Gesetzgeber ist, oder ob nicht vielleicht Karlsruhe selber auch diese Gewichte nachhaltig verschoben hat, indem es nämlich auf der einen Seite mit dem Recht auf informationelle Selbstbestimmung und dann mit dem Zwillingsgrundrecht, nämlich dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, zwei neue große Abwägungspositionen grundrechtlicher Natur geschaffen hat. Aber wenn man sich die Entscheidung des Bundesverfassungsgerichts mit Blick auf die Aussagen zur Sicherheit anschaut, dann gewinnt man den Eindruck, diese Aussagen sind im wesentlichen Aussagen, die ein bisschen grundrechtliche Schutzpflichten in den Blick nehmen und artikulieren, aber sonst nicht weiter thematisieren. Das heißt, das was Karlsruhe gemacht hat, ist letzten Endes selbst ein Verschieben der Verhältnisse von Freiheit und Sicherheit. Das kann man so sehen, das kann man sicherlich auch anders sehen, aber es ist jedenfalls ein ganz zentraler Befund.

Wenn wir uns jetzt in einem weiteren Schritt dem Staatstrojaner, der in § 49 des Gesetzentwurfs geregelten Befugnis zur Infiltration informationstechnischer Systeme, zuwenden, so ist doch ganz bemerkenswert, dass die daran geäußerte Kritik, dass der Gesetzgeber hier nicht hinreichende Kautelen geschaffen hat für die Frage, was eigentlich informationstechnische Systeme sind bzw. unter welchen Voraussetzungen das in formeller und materieller Natur zum Einsatz kommen kann, so nicht zutreffend ist. Denn zum einen hat der Gesetzgeber letzten Endes die Aussagen des Bundesverfassungsgerichts in der Online-Durchsuchungsentscheidung zum nordrhein-westfälischen Verfassungsschutzgesetz nahezu eins-zu-eins umgesetzt. Jetzt darüber noch

hinausgehen zu wollen und noch weitere Anforderungen aufstellen zu wollen, ist meines Erachtens mehr ein Akt vorauseilenden Gehorsams, der Karlsruhe tatsächlich nicht geschuldet ist. Wenn Sie sich die Regelung des § 49 anschauen, dann werden Sie sehen, dass Sie dort entsprechende formelle Kautelen haben. Sie haben die entsprechenden Behördenleitervorbehalte, Sie haben die entsprechenden Richtervorbehalte und Sie haben darüber hinausgehend auch Kernbereichsschutzregelungen. Also all das, was Karlsruhe gefordert hat, ist im § 49 auch entsprechend geregelt.

Zur Frage der elektronischen Aufenthaltsüberwachung ist hier bereits einiges gesagt worden. Ich will es vielleicht noch etwas auf die Spitze treiben. Man könnte auch sagen, das ist ein Akt experimenteller Gesetzgebung.

Abg. **Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Das sehen wir auch so.

SV **Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Ja, aber wahrscheinlich aus anderen Gründen. Wahrscheinlich wird diese Maßnahme, wie auch Herr Prof. Dr. Gärditz gesagt hat, einen zu allem Entschlossenen nicht verhindern können. Aber was man sich überlegen kann ist, ob man in einem verhältnismäßig ausgestalteten System präventiver Maßnahmen nicht noch auf weitergehende Maßnahmen zurückgreifen könnte. Der bereits genannte Entwurf zur Änderung bayerischer Sicherheitsgesetze, der von einem selbstverständlich unter richterlichen Vorbehalt gestellten Präventivgewahrsam ausgeht, wäre aber doch eine deutlich weitgehendere Maßnahme und deutlich freiheitsbeschränkender, als die bloße elektronische Aufenthaltsüberwachung, die ja ihrerseits auch wiederrum an bestimmte tatbestandliche Voraussetzungen und rechtsstaatliche Kautelen geknüpft ist.

Insgesamt möchte ich zusammenfassend zu dem Ergebnis kommen, dass der jetzt hier vorliegende Gesetzentwurf die Karlsruher Vorgaben aus der Entscheidung vom April letzten Jahres detailgetreu umsetzt. Man kann zurecht auch als Kritik erheben, dass es eigentlich eine Art Copy-and-Paste-Verfahren ist. Aber das führt nicht zur Verfassungswidrigkeit, sondern das ist einfach eine Frage der Gesetzestechnik und vielleicht auch des Gehorsams gegenüber dem Verfassungsgericht. Man kann die Entscheidung durchaus kritisieren und sagen, dass sie von einer Grundrechtsrigidität ausgeht, die bisweilen weit über die Erfordernisse sowohl des Freiheitsschutzes als auch der praktischen Anforderungen hinausgeht. Das ist aber eine andere Frage, die hier nicht zu beantworten ist. Herzlichen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Schwarz. Damit sind wir durch die Eingangsstatements durch. Ganz herzlichen Dank nochmal für Ihre Beiträge. Wir kämen jetzt zur Berichterstatterrunde. Zunächst erteile ich Herrn Kollegen Binninger das Wort.

BE Abg. **Clemens Binninger** (CDU/CSU): Herr Vorsitzender, vielen Dank. Meine Herren Sachverständige, vielen Dank für die Ausführungen. Ich bin ja schon ein paar Jahre dabei, aber ich habe, glaube ich, noch nie erlebt, dass mehrere Sachverständige sagen: Der Gesetzgeber geht zu weit, soweit hätte er gar nicht gehen müssen. Das wird uns auf jeden Fall zum Nachdenken bringen, was das Thema § 12 im BKA-Gesetz betrifft.

Ich will ein paar Fragen stellen, mich aber für die erste Runde im Interesse der Kollegen auf zwei Fragen beschränken. Die erste ist eher grundsätzlicher Natur, aber sie wird in den politischen Debatten eine Rolle spielen. Es ist ja ein paar mal kritisiert worden, dass wir „Copy-and-Paste machen." Ich will einmal Herrn Prof. Dr. Gärditz und Herrn Prof. Dr. Bäcker fragen: Wie hätten Sie es denn gerne? Entschuldigung, wenn uns Karlsruhe detaillierte Vorgaben macht, und zwar so detailliert, dass man sie kaum noch anders umsetzen kann, als sie zu übernehmen, was wäre denn die Alternative? Herr Prof. Dr. Schwarz hat gerade darauf hingewiesen: Dort, wo wir es nicht gemacht haben, wird es einem wie bei der Online-Durchsuchung wieder vorgehalten, oder wo wir schon alles erfüllen ist es immer noch zu wenig. Ich will einen Satz kurz zitieren, wenn ich darf: „Den Gesetzgeber nun auch noch in dieser Weise mit zahlreichen Ausgestaltungsanforderungen zu Kontrolle, Transparenz und Rechtsschutz gleichsam an die Hand nehmen zu wollen" – eine Passage lasse ich weg – „engt die originäre Gestaltungsbefugnis des Gesetzgebers in meines Erachten verfassungsrechtlich nicht angezeigter Weise ein." Will sagen, so lese ich dieses Zitat, wir können doch gar nicht mehr anders. Dieses Zitat

stammt übrigens nicht von mir, es stammt von einem Mitglied des Senats, der das Urteil gefällt und es abgelehnt hat, Bundesverfassungsrichter Dr. h.c. Wilhelm Schluckebier, so wie auch Bundesverfassungsrichter Prof. Dr. Michael Eichberger, der das ein bisschen anders gesehen hat. Deshalb meine erste Frage: Wie sollen wir es denn überhaupt noch machen? Wir können doch gar nicht mehr anders. In dem Moment, in dem Karlsruhe so detailliert urteilt, sind wir fast gehalten, so detailliert umzusetzen. Wenn Sie uns einen anderen Weg aufzeigen können, bitte, daran hätte ich ein großes Interesse.

Die zweite Frage, dann stelle ich die anderen zurück, ist praktischer Natur: Die Fußfessel. Da wäre meine Frage an Herrn Münch und an Herrn Prof. Dr. Schwarz, einmal praktischer Natur, einmal rechtlicher Natur. Herr Prof. Dr. Schwarz, gilt die Passage aus § 56 BKA-Gesetz neu, da ist die Fußfessel ja geregelt, für alle sogenannten Gefährder, die irgendwo in der Bundesrepublik als Gefährder eingestuft sind, oder muss sich das BKA, das ja eigentlich sein eigenes Gesetz nur für seine Fälle anwendet und nicht für von Landesbehörden eingestufte Gefährder, diese Gefährder-Definition der jeweiligen konkreten Person erst zu Eigen machen? Oder können wir jetzt zum Beispiel für Nordrhein-Westfalen sagen – die haben am meisten, 70 eingestufte Gefährder, von denen die Hälfte eigentlich unser Land verlassen müsste und für die also die Fußfessel zumindest interessant wäre, um ihren Aufenthaltsort zu überwachen – wir, das BKA, übernehmen die alle. Ginge das rechtlich? Herr Präsident Münch, wie würde das praktisch ablaufen? Das wäre es mal für den Moment.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Binninger. Frau Kollegin Renner.

BE Abg. **Martina Renner** (DIE LINKE.): Danke Herr Vorsitzender und auch Dank von mir an die Sachverständigen für Ihre schriftlichen und auch heute mündlich vorgetragenen Stellungnahmen. Ich habe zuerst eine Frage an Herrn Prof. Dr. Bäcker zum § 26, der Datenübermittlung an EU-Staaten und Stellen. Ich denke, da müssen wir auch angesichts der zum Teil auseinanderlaufenden innenpolitischen Entwicklung in den verschiedenen EU-Staaten, durchaus die Frage stellen, ob wir tatsächlich überall dasselbe Datenschutzniveau vorfinden. Daran anschließend stellt sich die Frage: EU-Staaten kooperieren ja auch mit Dritten außerhalb der EU. Da findet möglicherweise dann auch ein Datenaustausch aus dieser Datenweitergabe an Staaten statt, die möglicherweise nicht über dasselbe Datenschutzniveau wie hier in Deutschland verfügen. Wie beurteilen Sie also vor diesem Hintergrund die Gleichbehandlung, also des innerstaatlichen mit dem europäischen Datenaustausch?

Dann würde ich gerne die Frage von Herrn Binninger nach diesem Copy-and-Paste-Verfahren etwas variieren und auch stellen wollen. Ich glaube, man darf jetzt nicht nur so abfällig sagen, man hätte ja gar keine andere Möglichkeit gehabt. Positiv gesprochen: Wir finden ja jetzt in dem entsprechenden Gesetzentwurf tatsächlich wortgleiche Übernahmen aus dem Urteil – „Konkrete Wahrscheinlichkeit“ zum Beispiel – die bisher im polizeilichen Gefahrenabwehrrecht so nicht bekannt sind. Hätte es denn eine sich enger an dem Kanon der Polizeirechtsformulierungen orientierende Formulierung geben können, die dann auch vor allem dem polizeilichen Handeln mehr Bestimmtheit und Auslegungsgewissheit geben könnte oder war man, wie hier suggeriert wird, gezwungen, sich so eng an das Urteil zu halten? Also die Frage, ob es eine normenklarere, enger ans Polizeirecht angelegte Formulierung hätte geben können. Vielleicht könnten Herr Dr. Buermeyer oder auch andere dazu nochmal Stellung nehmen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Renner. Herr Kollege Grötsch.

BE Abg. **Uli Grötsch** (SPD): Vielen Dank Herr Vorsitzender. Als erstes Herr Münch: Sie haben eben von Special Services gesprochen und von dem Kompetenzzentrum, wenn es um die Zentralstellenfunktion des Bundeskriminalamtes geht. Das klingt gut, aber ich frage mich, inwieweit schaffen Sie das denn mit den personellen und auch mit den materiellen Ressourcen, die durch dieses Gesetz für Sie vorgesehen sind. Diese Stärkung des BKA bringt eine enorme Aufgabenmehrung mit sich. Erst mal die Umsetzung der Regelungen, die im Gesetz enthalten sind, das halte ich schon für eine Mammutaufgabe, das zu bewerkstelligen. Gibt es denn in Ihrem Haus schon eine Schätzung oder Annahme, wie lange es überhaupt dauern würde?

Etwa das horizontale Datenschutzkonzept umzusetzen, das muss ja auch ein Riesenpool an Daten sein. Und wo sehen Sie denn den konkreten Mehrwert in der horizontalen Aufstellung des Datenschutzkonzeptes? Das ist meine nächste Frage.

Dann hätte ich an Sie eine Frage, Herr Prof. Dr. Schwarz, was die Regelungen im § 77 Absatz 3 angeht, nämlich die Aussonderungsfristregelung, die sogenannte Mitziehautomatik. Wie bewerten Sie denn diese Mitziehautomatik. Ich halte das für eine sehr sehr weitgehende Regelung. Und das würde ich auch Sie fragen wollen, Herr Buermeyer, wie Sie das bewerten, die Mitziehautomtik im § 77 Absatz 3.

Und dann noch eine letzte Frage. Die Thematik des absoluten Schutzes von Berufsgeheimnisträgern. Auch wieder an Sie, Herr Prof. Dr. Schwarz, gerne auch Sie dazu, Herr Buermeyer: Die Psychotherapeuten haben ein Anliegen an uns herangetragen, die sich auch als Seelsorger sehen, eben nicht als geistliche Seelsorger, was ja auf der Hand liegt. Wie bewerten Sie das denn hinsichtlich des fehlenden absoluten Schutzes für diese Berufsgruppe? Danke.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Grötsch. Für die Fraktion BÜNDNIS 90/DIE GRÜNEN hatte sich Herr Kollege Ströbele gemeldet.

Abg. **Hans-Christian Ströbele** (BÜNDNIS 90/DIE GRÜNEN): Erstmal eine kleine Vorbemerkung. Ich glaube, Herr Prof. Dr. Schwarz hat so etwas beklagt, dass das Bundesverfassungsgericht sehr häufig bemüht wurde im Bereich der inneren Sicherheit und eigentlich schon seit dem Volkszählungsurteil fast gesetzgeberisch tätig ist und immer wieder angerufen werden muss. Das kann man natürlich auch so sehen und ich erinnere mich an Äußerungen aus Regierungskreisen, aus Parlamentskreisen, dass man sich einfach nicht die Mühe machen will als Gesetzgeber oder auch als Bundesregierung, die ja meistens die Gesetze vorschlägt, die dann das Parlament beschließen soll, das wirklich verfassungsrechtlich bis zum Kern hin zu überprüfen. Es wurde immer gesagt: Naja, dann geht es eben zum Bundesverfassungsgericht und dann werden wir wieder nachbessern. So ähnlich sehe ich das hier auch. Man setzt jetzt was in die Welt und sagt: Na ok, wenn wir da oder da zu weit gegangen sind, da werden sich schon genügend Kläger finden und das Bundesverfassungsgericht… ich rede jetzt im Augenblick mal nicht mit Ihnen, Herr Binninger, aber vielleicht nachher wieder. Das finde ich deshalb eine Kritik. Man kann auch sagen, das ist ein Armutszeugnis für den Gesetzgeber, dass das Bundesverfassungsgericht immer wieder eingreifen muss, seit der Volkszählung und mit maßgeblichen Urteilen und auch so konkrete Vorgaben macht, wie das im April letzten Jahres geschehen ist.

Die zweite Vorbemerkung bezieht sich auf die Fußfessel. Also alles diskutiert über Fußfessel. Ich habe nachher noch eine weitere Anhörung zur Fußfessel im Rechtsausschuss. Nämlich Fußfessel als Maßregel, also was wird da gemacht. Aber wenn ich dann die Akten lese, Akten der Behörden, des Bundeskriminalamts, Strafverfolgungsbehörden, dann sehe ich immer, dass die eigentlich bemüht sind, möglichst die Gefährder nicht wissen zu lassen, dass sie ihnen auf der Spur sind. Also keine Fußfessel anzulegen, wo die natürlich dann wissen, dass sie im Zentrum des Interesses sind. Sondern eher das alles vermieden wird, wodurch die merken, dass man ihnen auf der Spur ist, dass man sie beobachtet – vielleicht hin und wieder – und sie als Gefährder erkannt hat oder führt. Also ich finde, das ist eine Diskussion, die irgendwas in den Raum stellt, dass die Fußfessel groß was nutzen würde, aber in der Anwendung wird gerade das BKA wahrscheinlich das äußerst selten machen; nur wenn es gar nicht anderes geht, weil die eh längst verstanden haben, dass sie ganz oben auf der Liste stehen der Gefährder.

Aber jetzt meine zwei Fragen. Die eine Frage schließt sich an das an, was der Kollege Grötsch gefragt hat. Da habe ich die Frage auch an Herrn Prof. Dr. Bäcker. Diese Mitziehautomatik bedeutet ja, dass Dateien aus allen Bereichen der Polizei erstmal zusammengeführt werden und dann ihrer Löschungsfristen entledigt werden. Bisher steht ja immer drin, da muss das nach 5 oder 10 Jahren oder sowas gelöscht werden. Jetzt stehen die hier drin. Es gibt eine Klausel, wonach jede weitere Erfassung in irgendeiner Datei dazu führt, dass keine Löschung mehr eintritt, sondern dass alles, was sich da gesammelt hat, in den verschiedensten Dateien dann zur Verfügung steht und das auf Dauer und das auch lebenslang und ohne, dass das zwischenrein kontrolliert wird. Was ist eigentlich

der Grund, warum man das so gemacht hat? Weil das riecht natürlich nach Vorratsdatenspeicherung, mindestens für diesen Bereich, und deshalb stellt sich die Frage, warum hat man die Löschungsfristen aus den einzelnen Gesetzen, aus den einzelnen Datenerhebungen jetzt einfach gestrichen? Was ist der Hintergrund? Ist das nicht notwendig? Ist die Datensicherheit jetzt so gegeben? Also da fehlt mir die Begründung dafür, warum man das macht. Warum man also diese ganzen Dateien von den Löschungen freimacht und damit natürlich eine Art von Vorratsdatenspeicherung macht? Das ist die erste Frage an Herrn Prof. Dr. Bäcker. Welche Alternativen gibt es dazu? Kann man nicht einfach diese Einzelfristen lassen, so wie sie sind? Die haben ja alle einen Sinn. Da hat sich ja damals der Gesetzgeber durchaus was bei überlegt. Der Vertreter der Datenschutzbeauftragten hat da ja auch auf diese Problematik hingewiesen. Da ist der erste Punkt.

Und der zweite Punkt ist das mit der – ist ja auch angesprochen worden – länderübergreifenden Gefahr. Also ich erinnere mich, dass es in einem anderen Sicherheitsbereich, nämlich bei den Nachrichtendiensten, ja sowas durchaus gibt und man sich aber dann fragt, wieso es immer noch vorkommt, dass verschiedene Landesämter, manchmal auch das Bundesamt für Verfassungsschutz, einfach daneben bei bestimmten Gefährdern weiterhin tätig sind und die Informationen nur, wenn überhaupt, sehr mangelhaft zusammengeführt werden. Also wie kann eine solche Vorschrift, die ja durchaus Sinn macht, erstens eingegrenzt werden, aber dann auch angewandt werden. Sie wird wahrscheinlich deshalb nicht angewandt werden, weil nicht nur bei den Geheimdiensten, sondern auch bei den Polizeibehörden so eine Tendenz besteht: Unsere Ermittlung, unsere Daten, die wir haben, die wollen wir auch gerne bei uns haben und die wollen wir ungern weiter geben und schon gar nicht an das BKA, das dann die ganzen Sachen übernimmt. Also, wie kann man eine solche Vorschrift auf der einen Seite im föderalen System verfassungsgemäß gestalten und auf der anderen Seite auch in den Fällen zur Anwendungen bringen, wo das erforderlich ist.

Vors. **Ansgar Heveling** (CDU/CSU): Von wem möchten Sie das denn wissen, Herr Kollege Ströbele? Dann kämen wir jetzt zur Antwortrunde. Es sind Fragen gerichtet an Herrn Prof. Dr. Schwarz, an Herrn Münch, an Herrn Prof. Dr. Gärditz, an Herrn Dr. Buermeyer und an Herrn Prof. Dr. Bäcker. Jetzt gehen wir im Alphabet anders herum. Herr Prof. Dr. Schwarz, Sie dürfen den Anfang machen.

SV **Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Herr Vorsitzender, ganz herzlichen Dank. Vielleicht zur ersten Frage. Erstreckung der elektronischen Fußfessel auf Gefährder nach § 56. Nach meinem Verständnis nur, soweit es in die Zuständigkeit auch des BKA fällt. Selbstverständlich nicht für alle Gefährder, die sozusagen bundesweit nach Maßgabe landesrechtlicher Regelung unter Umständen als Gefährder eingestuft werden. Wobei wir ja auch darauf hinweisen müssen, dass längst nicht alle Landesgesetzgeber entsprechende Regelungen für Gefährder bereits getroffen haben. Was aber nicht geht, ist meines Erachtens ein Automatismus, dass zunächst landesrechtlich, unter Umständen auch unterschiedlich, festgelegt werden kann, unter welchen Voraussetzungen jemand ein Gefährder ist und dann automatisch, gewissermaßen, auch die Zuständigkeit des BKA gegeben wäre.

BE Abg. **Clemens Binninger** (CDU/CSU): Sie wissen, wie viele eingestufte BKA-Gefährder wir haben? Null!

SV **Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Dann ist das eine Vorschrift, bei der man sich unter Umständen die Frage stellen kann, die wir auch in der Vergangenheit bei anderen Regelungen hatten, wie oft sie denn tatsächlich zur Anwendung kommen. Aber möglicherweise mag sich ja das BKA auch einer Einschätzung des Landesgesetzgebers anschließen, aber es muss immer eine eigene Entscheidung entsprechend sein. So würde ich die Vorschriften in jedem Fall verstehen wollen.

Die Frage, die ebenfalls angesprochen wurde, die Mitziehautomatik nach Maßgabe von § 77. Ich glaube, das lässt sich damit rechtfertigen, dass wir auf der einen Seite bereits für die entsprechenden Datensammlungen so hohe Anforderungen haben, dass wir dann hier auch in Ansehung der besonderen Aufgaben des BKA eben die Möglichkeit haben, unter Umständen die Löschungsfristen zu verlängern. Aber das Ganze

beruht eben auf der Tatsache, dass wir bereits vorher so hohe Kautelen haben für die entsprechende Datensammlung überhaupt, dass das hier jedenfalls bezüglich der weiteren Speicherungsmöglichkeit dann keinen weiteren verfassungsrechtlichen Bedenken begegnet.

Ihre zweite Frage Herr Grötsch, die Frage des fehlenden absoluten Schutzes für Psychotherapeuten. Wenn ich mir die Systematik von § 62 BKA-Gesetzentwurf anschaue, versucht er letzten Endes ja eine Deckungsgleichheit mit den Vorgaben der Strafprozessordnung herzustellen. Und ob man jetzt hier ein gewissermaßen darüber hinausgehenden Sondertatbestand schaffen müsste, da mag man darüber nachdenken, rechtlich geboten ist es nicht. Und ich glaube, es geht nicht darum, dass das jeweilige berufliche Selbstverständnis derjenigen, die gerne als Geheimnisträger darüber hinausgehen und einen absoluten Schutz haben möchten, maßgeblich wäre für die verfassungsrechtliche Einschätzung.

Ein letzter Punkt, auch wenn das gestattet ist, Herr Vorsitzender, mit Blick auf die Äußerungen von Herrn Ströbele, der mir zwar nicht unmittelbar eine Frage gestellt hat, oder möchten Sie, dass wir diesen rechtspolitischen Diskurs außerhalb des Raumes bei Gelegenheit fortsetzen.

Abg. **Clemens Binninger** (CDU/CSU): Eine Antwort wäre interessant.

Vors. **Ansgar Heveling** (CDU/CSU): Wenn Kollege Binninger diese Frage jetzt auch stellt, dann ist es ok, wenn es kurz ist.

SV **Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Ich mache es auch entsprechend kurz. Herr Ströbele, mitnichten ein Armutszeugnis nur für den Gesetzgeber. Sondern mir ging es darum deutlich zu machen, dass der Gesetzgeber auf vorgefundene Situationen reagiert hat und auch reagieren musste, dass aber Karlsruhe nach meiner Einschätzung dem Gesetzgeber weit über den Gestaltungsspielraum des Gesetzgebers hinausgehende, engmaschige Befugnisse gesetzt hat, die nicht zwingend indiziert waren. Also man hätte den gesetzgeberischen Gestaltungsspielraum auch deutlich mehr schonen können und das bisweilen jedenfalls, dass ist dann natürlich auch eine Frage der rechtspolitischen Einschätzung, die durchaus unterschiedlicher Natur sein kann. Die rechtliche Bewertung dessen, was Karlsruhe gemacht hat – zum Teil zwischen rechtspolitischer Rigidität aus grundrechtsschützendem Selbstverständnis heraus bis hin zu weltfremd changierend, das ist glaube ich uns beiden auch bekannt. Das ist dann eben die Frage der rechtlichen Bewertung.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Schwarz. Herr Münch, bitte.

SV Präs. **Holger Münch** (Bundeskriminalamt, Wiesbaden): Ich will auf zwei Themenkomplexe eingehen, die an mich gerichtet waren. Zum einen die praktische Umsetzung der elektronischen Aufenthaltsüberwachung. Es ist so, dass natürlich in den Ländern gerade auch die Diskussion über die rechtliche Normierung läuft. Wir gehen davon aus, das wird im Bund nicht die einzige Regelung bleiben zur elektronischen Aufenthaltsüberwachung von sogenannten Gefährdern. Insofern stellen wir uns jetzt darauf ein, das mit den Ländern gemeinsam umzusetzen. Es gibt auch schon entsprechende Arbeitsgruppen, die das ausarbeiten. Wir prüfen dazu zum einen die Nutzung der technischen Infrastruktur, die die Hessen bereits aufgebaut haben, aber auch, inwieweit diese vorhandene Infrastruktur für unseren speziellen Anwendungsbereich Gefährder möglicherweise auch angepasst werden muss in dem einen oder anderen Bereich.

BE Abg. **Uli Grötsch** (SPD): Darf ich dann eine Zwischenfrage stellen, Herr Vorsitzender? Wenn Sie jetzt sagen, Herr Münch, dass Sie das mit den Ländern gemeinsam umsetzen – ich würde es mir nur von der praktischen Arbeitsweise her vorstellen wollen. Stoßen Sie dann nicht auch auf das Problem, dass die Länder teilweise unterschiedliche EDV-Systeme anwenden als Sie oder ist das dann auf eine Art und Weise miteinander realisierbar, sodass die Länder Ihnen Daten zur Verfügung stellen?

SV Präs. **Holger Münch** (Bundeskriminalamt, Wiesbaden): Es würde ja darum gehen, die Daten an einer bestimmten Stelle auszuleiten und anderen verfügbar zu machen. Sie müssen sich das praktisch also so vorstellen: Wenn jemand verpflichtet ist, so eine Fußfessel zu tragen, dann stellen wir uns vor, dass wir ein zentrales Überwachungszentrum haben, in dem auch vorher klar ist, welche Vorgaben bestehen, worauf ist zu achten, wenn ein Alarm in irgendeiner Form

aufläuft, was ist dann zu tun, mit wem arbeite ich zusammen, welcher Sachbearbeiter im BKA oder auch in einem Bundesland. Diese Prozesse muss man möglichst einheitlich gestalten. Das gilt dann auch für die technische Ausleitung. Wie sorge ich dafür, dass dieses Signal auch bei dem Mitarbeiter ankommt, der am Ende auch die Entscheidung in der Praxis treffen kann, muss und soll. Daran arbeiten wir. Das Ziel ist, dass wir im BKA dann an einer Stelle auch für Gefährder, die auf Basis von Entscheidungen aus den Bundesländern eine solche Überwachungsmaßnahme erhalten, dort eine Amtshilfe für diese übernehmen, die Frage der Überprüfung, wo hält sich die Person auf und notfalls eine Alarmierung durchführen. Ähnlich wie das hier auch schon heute in Hessen läuft und zwar bundesweit. Das ist technisch nicht so anspruchsvoll. Das ist lösbar. Praktisch ist es so, dass wir sagen: Es ist schon etwas anderes, eine Gefährderüberwachung umzusetzen. Das geht hin bis möglicherweise – wenn Sie so wollen – einer digitalen Observation. Deshalb gehen wir davon aus, dass wir das in einem ersten Schritt mit den Hessen zusammen, in einem zweiten Schritt mit einer Zentrale der Polizei im BKA, umsetzen. Das ist auch die Einschätzung der Länder und aktueller Diskussionsstand. Was das genau bedeutet, ist noch nicht abschließend erhoben, sondern wir sind noch in der Arbeit. Zu der Bemerkung: Wie häufig kommt das vor? Wenn wir uns anschauen, wie jemand Gefährder wird: In der Regel bekommen wir eine Erstinformation aus verdeckten Maßnahmen bzw. aus weiteren Ermittlungen. Dann sind wir in der Regel bemüht, durch strafprozessuale oder gefahrenabwehrrechtliche Ermittlungen zunächst einmal auch einen Nachweis und weitere Ermittlungsansätze zu erbringen bzw. mit verdeckten Maßnahmen zu agieren. Aber am Ende ist es häufig so, dass Sie an Grenzen kommen und dann ist die Frage: Haben Sie ein offenes Maßnahmenkonzept? Nur eine Zahl dazu: Im Jahr 2015 – die 2016-Zahlen habe ich noch nicht im Kopf – hatten wir 38 Gefährder von etwa 500, die eine Meldeauflage hatten – eine klassische offene Maßnahme, d. h. unter 10 Prozent. Das ist etwas, wo Sie schon sagen: Wenn ich jetzt noch weitergehen will – Kontaktverbote, bestimmte Aufenthaltsverbote – dann ist das eine Klientel in etwa der Größenordnung, wo wir dieses Instrument einsetzen und dann ist es eine sinnvolle Ergänzung des Instrumentariums, das wir jetzt haben. Das noch einmal als Einschätzung aus der Praxis. Zu der zweiten Frage: Wie schaffen wir das eigentlich, was da alles im Gesetz steht bzw. was kommt ansonsten noch auf das BKA zu? Kompetenzzentrum war hier das Stichwort und wie wir uns den konkreten Mehrwert einer technischen Neugestaltung vorstellen. Ich will einmal bei der technischen Neugestaltung anfangen. Heute leben wir mit einem INPOL-System, was 19 Teilnehmersysteme und ein Zentralsystem hat. Diese 19 Teilnehmersysteme werden durch unterschiedliche Vorgangsbearbeitungssysteme bestückt. Wenn Sie eine kleine Veränderung vornehmen wollen, bspw. dass Sie die Foreign Fighter künftig an das Schengener Informationssystem weiterleiten – ganz praktisch – dann brauchen Sie zur Umsetzung einer solchen Veränderung in diesem Veränderungsprozess, der extrem komplex ist, 20 Monate. Das ist einfach nicht mehr zeitgemäß, wenn Sie schnell reagieren wollen, denn dann brauchen Sie eine IT-Struktur, die nicht wie ein Flickenteppich aufgebaut ist. Deshalb ist es ein wesentlicher Hebel, die Verbundsysteme, die der Bund für die Länder bereitstellt, auf eine einheitliche Plattform zu stellen. Der Mehrwert besteht darin, von den einzelnen Datentöpfen, die man alle anfassen muss, von den 19 Teilnehmersystemen wegzukommen und hin zu einem mandantenfähigen Zentralsystem, was natürlich auch hohe Datenschutzanforderungen erfüllen muss. Da haben wir gar keine Zweifel. Wenn wir das aber hinbekommen, dann haben wir damit einen wesentlichen Stellhebel, um auch die Informationsversorgung des Polizisten am Schreibtisch oder im Streifenwagen auf eine ganz andere Ebene zu bringen, was es heute schon praktisch gibt. Sie müssen nur nach Holland schauen. Dann sehen Sie dort eine mobile IT-Infrastruktur, wo der Polizeibeamte auf der Straße alle möglichen Zugangsmöglichkeiten hat bis hin zu der Tatsache, dass er einen Ausweis mit seiner Kamera am iPad für die Strafanzeige einlesen kann. All das kriegen Sie nur hin, wenn Sie weit weniger komplex sind, also für uns ein wesentlicher Hebel auch mittelfristig, um die IT-Struktur deutlich leistungsfähiger zu machen, ohne dabei den Datenschutz in Frage zu stellen. Was die Umsetzungszeit angeht: Wir bauen gerade eine Programmstruktur auf. Es sind mehrere Projekte, die betroffen sind, INPOL auf eine neue Plattform

zu bringen. Für den Polizeilichen Informations- und Analyseverbund gilt dann natürlich auch das Grundsatzurteil. Wir müssen auch hier schauen, wie wir die Datenstruktur künftig gestalten. Wir haben ein weiteres Projekt – nämlich ein einheitliches Fallbearbeitungssystem, das ist das, womit die Ermittler arbeiten – zu entwickeln und auch schrittweise auszurollen. Wir gehen von fünf bis sechs Jahren aus, die wir brauchen, diesen wesentlichen Schritt INPOL-neu – es gibt da noch keinen vernünftigen Begriff – mit einem sehr, sehr erheblichen Aufwand auch von internen und externen Kräften – eine dreistellige Personenzahl, die wir alleine im IT-Bereich bräuchten – zu schaffen. Daneben haben wir auch noch weiteren Umsetzungsaufwand durch das Gesetz und durch die Kompetenzzentren selbst, die wir auch schon schrittweise aufbauen. Ich will einmal an zwei Dinge erinnern. Die Software für die sog. Quellen-TKÜ: Die stellen wir den Bundesländern auch schon heute zur Verfügung. Wir sind da so etwas wie ein Kompetenzzentrum. Oder die Boston-Infrastruktur, die wir zur Entgegennahme von Bild- und Videomaterial aufgebaut haben. Auch das haben wir zentral entwickelt und stellen es den Ländern zur Verfügung. Da wollen wir weitermachen, z. B. auch mit einer einheitlichen Struktur für Kommunikationsüberwachung. Wenn wir das hinbekommen, dann werden wir insgesamt als polizeilicher Verbund leistungsfähiger. Für uns bedeutet das aktuell neun Personalprojekte, die wir parallel führen – von der Personalgewinnung vom Kriminalbeamten über Angestellte über den Umbau auch des Personalkörpers und eine Menge von Projekten, die wir parallel stemmen müssen. Das ist alles nicht einfach. Ich glaube aber, das ist der richtige Schritt. Das ist die richtige Antwort auf die Anforderungen der heutigen und der künftigen Zeit, die wir haben, d. h. wir brauchen einen leistungsfähigen Verbund und da hat das BKA nun einmal eine Schlüsselrolle. Soweit zu Ihren Fragen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Münch. Die nächsten Fragen richteten sich an Herrn Prof. Dr. Gärditz.

SV **Prof. Dr. Klaus Ferdinand Gärditz** (Rheinische Friedrich-Wilhelms-Universität Bonn): Vielen Dank. Ich habe eine Frage von Herrn Binninger. Wie hätten Sie es denn gerne bei der Kritik? Ich kann Ihren Standpunkt natürlich gut verstehen. Sie sind jetzt in einer reaktiven Situation. Sie haben dieses Urteil bekommen, das sich teilweise eher liest wie – ich sage einmal – ein Handbuch der guten Sicherheitspolitik und nicht wie eine richterliche Deduktion aus der Verfassung. Sie müssen damit leben. Ich würde mir wünschen, dass der Deutsche Bundestag eine vielleicht eher mittel- oder langfristige Strategie im Umgang mit dem Bundesverfassungsgericht verfolgt, die das Parlament auch als ein Akteur auf Augenhöhe ins Spiel bringt, der respektvoll aber selbstbewusst mit dem Gericht umgeht und auch zeigt, dass er sich eben nicht auf Vollzugsautomatismen einlässt. Ich habe kein Patentrezept dafür, meine aber durchaus, dass etwa eine sprachliche Abänderung der Frage, was Frau Renner durchaus mit Recht aufgeworfen hat, ob man in dem ein oder anderen Fall vielleicht eine bessere Einpassung in die polizeirechtliche Kategorien findet, ob der Deutsche Bundestag möglicherweise an der ein oder anderen Stelle präzisere oder andere Kategorien findet, allein schon abhelfen würde – unabhängig von der Qualität der einzelnen Formulierung. Weil das den Blick zurück auf das Parlament lenkt und nicht im Grunde genommen das Gesetz am Ende aussehen lässt, wie etwas, wo ich zum Verständnis sofort zur Anthrazitsammlung des Bundesverfassungsgerichts greife und nachlese, was denn das Gericht damit gemeint hat. Das betrifft aber nicht diesen Fall alleine, sondern das ist etwas, was mittelfristig in allen Bereichen notwendig wäre, dass man nicht zum Getriebenen wird, sondern dass man deutlicher die eigenen Gestaltungsansprüche zum Ausdruck bringt. Denn Sie haben natürlich auch das Bundesverfassungsgericht, was ein Stückweit Politik gemacht hat und das Gericht so wie es jetzt ist und wie es agiert und handelt, ist auch ein Produkt – ich sage mal – eines reaktiven Umgangs mit diesen Entscheidungen. Ich selber sehe das zugegeben aus einer wissenschaftlichen Sicht, die von diesen praktischen Bedürfnissen befreit ist – und ich will da deswegen mit meiner Kritik auch zurückhaltend sein. Ich habe gewisse Bedenken, dass so eine eins-zu-eins-Umsetzung im Wortlaut eigentlich diesen Prozess noch weiter beschleunigt. Das nächste Mal steigen wir ein. Die Regelungen werden irgendwie angegriffen. Das passiert immer. Da steigen wir bei der Frage ein: Hat der Deutsche Bundestag hier die Passage in Randnummer 264 des Bundesverfassungsgerichts richtig umgesetzt? Der Wortlaut ist schon derselbe und dann wird nur noch Bundesverfassungsgerichtdezisionismus bzw.

-deduktion aus einzelnen Urteilsgründen betrieben. Das überfrachtet die Urteilsgründe. Das überfordert im Übrigen auch das Bundesverfassungsgericht, weil es kein Sicherheitsgesetzgeber ist. Was ich mir wünschen würde, ist deswegen ein bisschen mehr Distanz zu den Urteilen. Vielleicht in der Semantik aber vielleicht auch – ich sage einmal – eine gewisse Widerspenstigkeit, dass Dinge, die einem nicht so gut einleuchten, vielleicht politisch auch einmal anders formuliert werden und dass man auch einmal das Risiko eingeht, dass das Bundesverfassungsgericht in fünf, sieben oder zehn Jahren dann sagt: Das akzeptieren wir nicht. Das wissen Sie heute nicht. Ich darf Sie da einfach ermutigen, damit ein bisschen selbstbewusster umzugehen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Gärditz. Herr Dr. Buermeyer, bitte.

SV **Dr. iur. Ulf Buermeyer, LL.M.** (Richter am Landgericht Berlin): Vielen Dank, Herr Vorsitzender. Eine ganze Reihe von Fragen sind aufgelaufen. Ich möchte zunächst ein Wort zu diesem Stichwort Gefährderbegriff, der ganz häufig gefallen ist, sagen, um das einfach zu verklaren. Jedenfalls – nach meinem Kenntnisstand – gibt es bislang bundesweit keine quasi feststellenden Verwaltungsakte, dass die Person XY Gefährder ist, was auch immer das heißen mag. Was es auf Bundes- und Landesebene teilweise im Entwurfsstadium gibt, teilweise im Gesetzesstadium, sind bestimmt tatbestandliche Voraussetzungen, an die sich dann Rechtsfolgen knüpfen und die tatbestandlichen Voraussetzungen werden im politischen Diskurs umschrieben als „Das ist ein Gefährder.“ Insofern wäre die Antwort auf die Frage von Herrn Binninger ganz kurz: Das BKA wird selber subsummieren müssen. Selbstverständlich kann es sich, soweit es Erkenntnisse, z. B. beim GTAZ erlangt hat, auch auf Erkenntnisse aus den Ländern stützen. Das wäre meine kurze Antwort dazu. Zweiter Punkt die Berufsgeheimnisträger: Das ist ja schon mehrfach angesprochen worden. Psychologische Psychotherapeuten, ja aber aus meiner Perspektive auch ganz wichtig Journalistinnen und Journalisten. Liest man dann in diesem Kontext unmittelbar die Entscheidung des Bundesverfassungsgerichts, dann macht sie relativ wenige Vorgaben. Als mit dem Gleichheitssatz nicht in Übereinstimmung stehend, hat das Gericht verworfen – die Differenzierung zwischen Rechtsanwälten und Strafverteidigern und damit den Schutz auf Rechtsanwälte insgesamt erstreckt. Das, denke ich, leuchtet unmittelbar ein. Gleichwohl hält das BKA-Gesetz ansonsten – also im Entwurfsstadium – fest an einem Schutzdualismus. Es gibt bestimmte absolut geschützte Berufsgruppen. Eben jetzt neu die Rechtsanwälte aber auch noch ein paar andere und dann gibt es relativ Geschützte, z. B. die psychologischen Psychotherapeuten aber auch Ärzte, Journalistinnen und Journalisten. Wie überzeugend dieser Dualismus aus rechtspolitischer Perspektive ist, da habe ich gewichtige Zweifel. Das Bundesverfassungsgericht macht da wenige Vorgaben und betont im Gegenteil den Einschätzungsspielraum des Gesetzgebers. Die Frage ist aber: Wie groß ist dieser Einschätzungsspielraum, wenn man einmal genau hinschaut? Wie gesagt, direkt aus der Perspektive Gleichheitssatz hat das Gericht keine Bedenken oder nur ganz wenige Bedenken. Ausnahme: Rechtsanwälte vs. Strafverteidiger. Aber es betont zugleich, dass Artikel 12, also die Berufsfreiheit, Akzente setzen und die Abwägung im Hinblick auf eine Unzulässigkeit einer Datenerhebung verschieben kann. Es betont in diesem Zusammenhang zugleich auch die Bedeutung des Kernbereichsschutzes. Wenn man das einmal zusammen nimmt, dann glaube ich, lässt sich mit Fug und Recht vertreten, dass es jedenfalls bestimmte Berufsgruppen gibt, wo im Ergebnis eine Datenerhebung in aller Regel nicht zulässig sein wird. Stichwort: Psychologische Psychotherapeuten, Ärzte. Ich kann mir kaum vorstellen, dass eine medizinische Behandlung nicht den Kernbereich der Persönlichkeit berührt. Wir schreiben hier – Sie schreiben, ich persönlich nicht – wenn Sie das so Gesetz werden lassen, einen Tatbestand, dessen Voraussetzungen fast immer vorliegen werden, fast immer wird es jedenfalls im Bereich Ärzte und psychologische Psychotherapeuten im Ergebnis – jedenfalls bei richtiger Anwendung des Gesetzes – dazu kommen, dass eine Überwachung nicht zulässig ist. Das lässt es doch aus meiner Sicht im Interesse eines Grundrechtsschutzes durch Verfahrensgestaltung und auch durch die Fassung von tatbestandlichen Voraussetzungen naheliegend erscheinen, auf die Differenzierung zu verzichten und zu sagen: Wir beziehen jedenfalls Ärzte und psychologische

Psychotherapeuten umfassend in den Schutz ein. Dann bleibt letztlich nur noch die Berufsgruppe der Journalisten. Da muss man sagen: Das ist eine rein rechtspolitische Frage. Das muss man so offen sagen. Da gibt es wohl wenige Vorgaben, aber ein Stichwort: Quellenschutz. Ich glaube, es würde sich lohnen, noch zwei Minuten darüber nachzudenken, ob ein relativer Schutz von der Pressefreiheit, insbesondere der Informantenschutz, überhaupt zielführend ist. Die Begründung dafür ist, dass ein Informant sich – wenn er z. B. ein Whistleblower ist – in aller Regel strafbar macht oder sich jedenfalls gravierenden arbeitsrechtlichen Folgen aussetzt. Dass ein solcher Informant natürlich nicht darauf vertrauen kann, wie eine solche Abwägung durch das Bundeskriminalamt – bei allem Respekt, Herr Münch, vor Ihren Mitarbeiterinnen und Mitarbeitern – ausfallen wird. Ein relativer Schutz ist eben ein relativer Schutz, der im Einzelfall versagt werden kann. Ein Whistleblower kann sich auf einen solchen relativen Schutz schlicht nicht verlassen. Mit anderen Worten: Eine solche Regelung ist aus meiner Sicht für den Quellenschutz und damit für die Pressefreiheit in unserem Lande verheerend und ich würde Sie deswegen sehr deutlich ermuntern wollen, noch einmal darüber nachzudenken, ob man sich nicht hier einen belastbaren Schutz für den Bereich der Informationsgewinnung durch die Presse rechtsstaatlich leisten kann. Ich glaube, das würde die Rechtsanwendung für das BKA sogar erleichtern, wenn auch in bestimmten Ausnahmesituationen natürlich dann eine Informationsgewinnung unzulässig ist und es würde – wie gesagt – die Pressefreiheit deutlich stärken. Stichwort: Mitziehautomatik. Ich sage Ihnen ganz offen, dass ich ein gewisses Verständnis für diese Mitziehautomatik habe und zwar deswegen, weil das BKA eine Gefahreneinschätzung leisten muss. Man kann eigentlich nie zu viele Daten haben, wenn man eine Gefährdereinschätzung zuverlässig treffen will. Da können auch lange zurückliegende Informationen von gewissem Wert sein. Insofern denke ich, kann man diese Regelungen nicht in Bausch und Bogen verdammen. Ich sehe durchaus einen sinnvollen Grundgedanken dahinter. Das eigentliche Problem aus meiner Sicht ist, wie eine solche Mitziehautomatik ausgelöst wird. Mit anderen Worten: Wie kommen denn eigentlich die Informationen in diese Datenbank? Da ist das Beispiel der Bundesbeauftragten für Datenschutz und Informationsfreiheit sehr eindrucksvoll. Da scheint mir darin ein Problem zu liegen, wenn es letztlich das BKA in der Hand hat, die Mitziehautomatik auszulösen, indem sie einfach bestimmte neue Speicherungen vornehmen, die den Betroffenen möglicherweise kaum zuzurechnen sind. Stichwort: Personenkontrollen, die keine näheren Erkenntnisse bringen als dass eine Person an einer bestimmten Kontrollstelle angetroffen wurde. Ich denke, da könnte man zumindest tatbestandlich nachsteuern und sich nämlich die Frage stellen, ob man nicht zumindest die Anforderungen stellt, dass die Mitziehautomatik nur dann ausgelöst wird, wenn die neuen Informationen tatsächlich zurechenbar auf die Personen zurückgehen und in irgendeiner Art und Weise tatsächlich die Vermutung begründen, dass die Informationen in Zukunft für die Arbeit des BKA erforderlich sein werden. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Dr. Buermeyer. Herr Prof. Dr. Bäcker, bitte.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Vielen Dank. Frau Renner und Herr Binninger haben nach der Copy-and-Paste-Regelungstechnik gefragt. Ich möchte zunächst einmal betonen, dass ich weder in meiner schriftlichen Stellungnahme noch in meinen mündlichen Äußerungen irgendwas gegen die Copy-and-Paste-Regelungstechnik gesagt habe. Das waren die anderen. Aber wenn Sie mich schon fragen, dann möchte ich das ein bisschen zweigestaltig beantworten.

Ich habe extrem große Empathie für sie. Wenn ich Sie wäre, würde ich es wahrscheinlich genauso machen. Das Bundesverfassungsgericht schreibt etwas in ein Urteil hinein. Sie wollen dem BKA gerne das, was ihm verfassungsrechtlich gegeben werden darf, auch geben. Da ist natürlich der sicherste Weg: Sie schreiben das Urteil ab. Ich finde das absolut nachvollziehbar und gleichwohl unschön.

Die Frage ist: Wie könnte man es schöner machen? Man könnte größere Risiken eingehen. Ich will mir einmal erlauben, einen solchen riskanten Weg aufzuzeigen, den ich persönlich für gangbar hielte. Leider denken allerdings nicht alle Menschen

genauso wie ich. Ich könnte nicht garantieren, dass auch jeder andere ihn mittragen würde. Wenn man sich einmal überlegt, von welchem Gedanken das Bundesverfassungsgericht mit seinen sehr erstaunlichen Formulierungen ausgeht, mit denen Neuland im BKAG-Urteil betreten wird, die ich im Übrigen auch für falsch halte, dann ist die grundlegende Idee, dass man zwischen situationsbezogenen und personenbezogenen Prognosen unterscheiden kann. Der klassische polizeiliche Begriff der konkreten Gefahr ist eine situationsbezogene Prognose eines Schadensereignisses, das sich irgendwie konturiert abzeichnen muss. Ich muss anhand der Parameter Art des Ereignisses, Ort des Ereignisses, Zeit des Ereignisses, Beteiligte des Ereignisses in der Lage sein, zumindest einigermaßen zu sagen, worum es mir geht und wogegen ich tätig werden möchte. Im Unterschied dazu steht eine personenbezogene Prognose über eine Einzelperson, von der ich annehme, dass die gefährlich ist. Ich weiß noch überhaupt nicht, was die irgendwann mal macht und wo sie das macht und wie sie das macht, aber ich kann sagen: Es gibt eine Gruppe von Straftaten, zu denen die Person eine besondere Affinität aufweist. Nehmen Sie das etwas platte Beispiel des Sexualdelinquenten, der aufgrund von Persönlichkeitsstörungen in bestimmten Situationen Gefahr läuft, bestimmte Sexualstraftaten zu begehen. Ich weiß noch nicht, ob der jemals in Zukunft in diese Situation gelangen wird, aber ich kann sagen, wenn er das unter geeigneten Randbedingungen tut, dann muss ich befürchten, dass solch eine Straftat im Verhältnis zum Großen und Ganzen der Bevölkerung mit erhöhter Wahrscheinlichkeit das Ergebnis sein wird. Zwischen diesen beiden Prognosen kann man unterscheiden. Das, was das Bundesverfassungsgericht machen will in seinem BKAG-Urteil ist, polizeiliche Überwachungsmaßnahmen auch aufgrund von personenbezogenen Prognosen zu ermöglichen, auch wenn es sich um sehr eingriffsintensive Überwachungsmaßnahmen handelt. Deswegen finden sich dort all diese schwammigen Formulierungen: Der verfassungsrechtliche Gefahrenbegriff, den man nicht versteht, weil der klassische situationsbezogene Begriff der polizeilichen konkreten Gefahr auf eine personenbezogene Prognose ausgeweitet werden soll. Ich persönlich glaube allerdings, dass die Leistungsfähigkeit der situationsbezogenen konkreten Gefahr auch deliktsbereichsspezifisch zu würdigen ist. Ich glaube, im Bereich der Organisierten Kriminalität, wo es um die Beteiligung an einem fortwährenden kriminellen Geschehen geht und die einzelne Straftat nur sowas wie ein Einzelereignis in einer Kette von Ereignissen ist, da brauchen Sie tatsächlich so einen personenbezogenen Gefahrenbegriff bzw. eine personenbezogene Prognose, weil es Ihnen nicht so sehr um die einzelne Straftat geht, sondern es geht Ihnen darum, kriminelle Strukturen auszuleuchten. Im Terrorismusbereich ist das ein bisschen anders, denn da wollen Sie ja unbedingt jeden einzelnen terroristischen Anschlag verhindern. Andererseits ist es so, dass aufgrund der hohen Schäden, die hier in Rede stehen, letztlich die Anforderungen an die Konturierung des Schadensereignisses und an die Wahrscheinlichkeit des Schadensereignisses ziemlich niedrig anzusetzen sind. Das führt dazu, dass sich im Terrorismusbereich eine konkrete Gefahr sehr schnell bejahen lässt. Dazu gibt es auch Rechtsprechung. Es gibt Rechtsprechung aus Terrorismusprozessen, wo präventivpolizeilich gewonnenes Material eingeführt wurde und wo gesagt wurde, dass eben in einer sehr ambivalenten Situation, wo sich gerade so etwas zusammenbraut, wo Leute anfangen, auffällig zu werden, konspirativ zu kommunizieren, sich häufiger zu treffen, das schon ausreichen kann, um eine konkrete Gefahr zu bejahen. Ich hätte, wenn ich das BKA-Gesetz hätte schreiben müssen und wenn ich sicher wäre, dass alle es so verstehen, wie ich es verstehen würde, schlicht alles von einer konkreten Gefahr abhängig gemacht. Ich glaube, damit wäre man auch gar nicht so schlecht gefahren, dass man sich auf gängige polizeirechtliche Argumentationsmuster hätte beziehen können, um das sinnvoll anzuwenden. Ich gestehe Ihnen sofort ein, vielleicht gibt es irgendein Verwaltungsgericht, dass das nicht schnallt, wie es in Wirklichkeit sein muss, und dann verlieren Sie. Das wäre natürlich misslich und darum habe ich – wie gesagt – volles Verständnis für Sie. Ich habe darüber ein gutes Buch geschrieben, dessen Lektüre ich Ihnen wärmstens empfehlen würde. Ich hoffe, dass das zumindest die Frage beantwortet. Jetzt habe ich meinen persönlichen Standpunkt einmal klar gemacht.

Die nächste Frage nach der Mitziehautomatik: Die Mitziehautomatik sehe ich erheblich skeptischer als mein Vorredner. Ich glaube allerdings auch, dass man ihren genauen Gehalt betrachten muss. Deswegen würde ich Sie gerne einmal zur Lektüre von § 77 des Entwurfs einladen. Im § 77 geht es ausweislich der Überschrift bereits um eine Aussonderungsprüffrist. § 77 Abs. 1 S. 1 sagt uns: Das BKA prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind, und der Abs. 3 regelt den Fristbeginn, also den Zeitpunkt ab dem diese Frist zu beachten ist. Es geht hier gar nicht um Löschungsfristen. Die Löschungsregelungen sind die ganz allgemeinen Löschungsregelungen. Personenbezogene Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Das gilt hier genauso wie anderswo auch. Das ergibt sich dann letztlich, wenn ich es richtig sehe – ich habe versucht, noch einmal zu blättern – nicht aus dem BKAG, sondern aus dem neuen BDSG, das Sie nächste Woche beraten. Es geht hier also nur um die Frage: Wann muss das BKA von sich aus turnusmäßig prüfen, ob es die Daten noch braucht oder ob es sie löschen muss? Da sagt jetzt die Mitziehautomatik: eigentlich nie, vorausgesetzt ab und zu finden sich mal wieder neue Speicherungsanlässe. Das halte ich für ein Problem und dafür sehe ich schlicht auch keinen Grund. Die Begründung des Gesetzentwurfs sagt: Es geht darum, eine polizeifachlich erforderliche Abbildung der Entwicklung einer betroffenen Person in kriminalistischer Hinsicht über aussagekräftige Zeiträume hinweg zu ermöglichen: Nur die bloße Prüfung, ob gelöscht werden muss, steht ja dieser polizeifachlich erforderlichen Abbildung gar nicht entgegen, sondern höchstens das Ergebnis der Prüfung, dass man nämlich die Daten nicht mehr braucht. Aber das ist eine ganz andere Frage, die vom § 77 mit seiner Mitziehautomatik unmittelbar gar nicht adressiert wird. Irgendwann könnte es auch dazu kommen, dass mal jemand Auskunft vom BKA aufgrund des datenschutzrechtlichen Auskunftsanspruchs begehrt und wissen will, welche Daten über ihn gespeichert sind und dann sagt: Ich will, dass diese Daten gelöscht werden. In dem Moment muss das BKA auch prüfen, ob es die Daten noch braucht. Dann muss es diese möglicherweise auch löschen, wenn es dann in diesem Zeitpunkt nicht substanziieren kann, warum es sie noch braucht – polizeifachlich erforderliche Abbildung hin oder her. Solange die polizeifachlich erforderlich ist, besteht ja ein Grund, die Daten zu behalten. Da müssen sie auch nicht gelöscht werden, auch nicht, wenn die Frist abgelaufen ist. D. h. aus polizeilicher Sicht ist aus meiner Sicht die Mitziehautomatik überhaupt nicht besonders wichtig. Die turnusmäßige Prüfung macht nur Aufwand, weil man sich ab und zu eben die Daten angucken muss. Andererseits aus bürgerrechtlicher Sicht, weil die meisten Leute eben von ihren Auskunftsrechten keinen Gebrauch machen, ist das ein wichtiger Baustein einer datenschutzkonformen Informationsordnung und deswegen meine ich, dass man die Regelung unbedingt ändern sollte.

Letzter Punkt von Frau Renner: Die Übermittlungsregelungen: Das ist wirklich eine fiese Frage. Ich habe auf sie auch keine wirklich befriedigende, gute Antwort. Es ist ja in der Tat so, dass der Gesetzentwurf vorsieht, das europäische Ausland oder ausländische Behörden hinsichtlich von Datenübermittlungen genauso zu behandeln, wie inländische Behörden. Wenn ich einer inländischen Behörde übermitteln darf, darf ich auch ins EU-Ausland übermitteln. Ist das jetzt sinnvoll, wenn wir davon ausgehen, dass vielleicht nicht in allen Mitgliedstaaten der Europäischen Union faktisch – rechtlich schon – aber faktisch dasselbe Datenschutzniveau besteht wie bei uns. Darüber kann man sich politisch sicherlich lange streiten. Aus rechtlicher Sicht haben wir natürlich das Problem, dass wir uns fragen müssen, ob die Datenschutzrichtlinie für Polizei und Justiz, die wir bis Mai 2018 umzusetzen haben, überhaupt ermöglicht, dem BKA eine solche Prüfung einzuräumen oder ob die nicht letztlich sagt: Wir müssen ohnehin Übermittlungen ins EU-Ausland so behandeln wie Übermittlungen ins Inland. Das ist eine außerordentlich schwierige Frage, auf die ich keine Antwort habe. Ich habe Vorträge über die Richtlinie gehalten. Ich habe jetzt gerade auch noch einmal versucht, in aller Hektik, nachdem Sie mir einen Herzinfarkt verursacht und diese Frage gestellt haben, das noch einmal zu erschließen und es ist wirklich nicht so einfach zu beantworten. Man kann die Richtlinie so verstehen, dass sie letztlich ein einheitliches Datenschutzniveau für die EU fingiert. Man kann sie aber auch so verstehen, dass sie eigentlich für Übermittlungen innerhalb der Europäischen Union gar keine Regelungen enthält, sondern nur sagt, dass, wenn

es anderswo Regelungen gibt, diese Regelungen eingehalten werden müssen. Da bewegen wir uns in einem Spannungsfeld. Ich würde mir da jetzt im Moment – im Rahmen dieser Stellungnahme – zu dieser Frage kein endgültiges Urteil zutrauen. Wenn Sie mir einen Gutachtenauftrag erteilen und 10.000 Euro geben – mit großem Vergnügen.

Vors. **Ansgar Heveling (**CDU/CSU): Vielen Dank, Herr Prof. Dr. Bäcker – zwischenzeitliche Werbeblöcke ausgenommen. Kommen wir jetzt zu einer zweiten Runde. Ich bitte um kurze und knappe Fragen, damit wir auch noch zur Beantwortung kommen. Herr Kollege Binninger, bitte.

BE Abg. **Clemens Binninger** (CDU/CSU): Vorneweg, Herr Bäcker: Zum Datenschutzniveau nur eine kurze Erinnerung von mir – Herr Kollege Dr. von Notz war ja dabei und hat auch tapfer gekämpft – aber da gab es diesen Satz, dass eben das Datenschutzniveau nicht der Maßstab ist, eben nicht in anderen Länder das gleiche Datenschutzniveau vorhanden sein muss, vielleicht auch gar nicht kann, selbst wenn es wünschenswert wäre. Das ist kein Hinderungsgrund. Jetzt meine Fragen an Herr Prof. Dr. Möstl und Herrn Prof. Dr. Schwarz. Von Herrn Prof. Dr. Schwarz würde ich gerne noch einmal ganz allgemein wissen, weil es heute gar nicht so sehr Thema war: Ausgangspunkt für die Gesetzesänderungen ist ja das Urteil, wo Karlsruhe gesagt hat: Das alte BKA-Gesetz hat beim Kernbereichsschutz bei sehr eingriffsintensiven Maßnahmen zu wenig vorgesehen. Es hat die Berufsgeheimnisträger – das Spannungsfeld war dort Rechtsanwälte/Strafverteidiger – das datenschutzrechtliche Kontrollregime und die Übermittelung an andere Sicherheitsbehörden, dort vor allem auch Ausland, gemeint. Das waren die Hauptkritikpunkte: Sind denn – jetzt einmal losgelöst davon, dass wir mit Neuordnung der Datenverarbeitung im BKA und im Verbund Bund-Länder natürlich große Felder aufmachen, Fußfesseln etc. – sind denn nach Ihrer Lesart des Gesetzentwurfs diese Kernpunkte, die Karlsruhe an den Anfang seines Urteils gestellt hat, erfüllt oder sehen Sie da noch Nachbesserungsbedarf? Die zweite Frage an Herrn Prof. Dr. Möstl: Zweierlei, auch noch einmal mit den Berufsgeheimnisträgern, weil da vorhin auch eine andere Auffassung anklang. Auch dort habe ich das Urteil so verstanden – und ich war ja bei beiden Verhandlungen dabei, beim mündlichen wie beim Urteilsverkünden – dass Karlsruhe nicht moniert hat, dass wir nicht alle Berufsgeheimnisträger aus der StPO ins BKA-Gesetz übernehmen und quasi vor diesen Maßnahmen schützen, sondern Karlsruhe hat nur moniert, was das für eine theoretische Unterscheidung ist – Strafverteidiger ja, Rechtsanwälte nein. Das haben wir jetzt korrigiert. Gibt es aus dem Urteil heraus – vom rechtspolitischen Diskurs mal abgesehen – überhaupt eine Notwendigkeit, den Kreis größer zu ziehen? Und reicht der relative Schutz, wie er im § 62 Abs. 2 formuliert ist für die anderen Berufsgeheimnisträger, nicht aus? Ganz davon abgesehen, dass es auch schwierig sein dürfte, jeden als solchen zu erkennen. Die zweite Frage auch an Herrn Prof. Dr. Möstl: Sie haben wie ich finde sehr anschaulich dargelegt, mit § 12 BKA-Gesetz schränkt sich der Gesetzgeber mehr ein, als er müsste. Jetzt könnten wir sagen: Der Gesetzgeber sind wir, wir halten das aus. Aber wir machen uns ein bisschen Sorge um die Polizeiarbeit. Was wäre für Sie der Punkt, wie müsste man ihn anders fassen? Müsste man ihn, so wie es Karlsruhe im Urteil getan hat, nur beziehen explizit auf die eingriffsintensiven Maßnahmen, nur dann gilt das, aber nicht auf alle Daten, die die Polizei im Rahmen irgendeines Strafverfahrens mal erhoben hat? Wir haben hier die zwei großen Felder. Einmal Terrorismusbekämpfung – aber was voransteht, gilt ja für jede polizeiliche Handlung, gilt bei jedem Datensatz, der beim Ladendiebstahl, bei der Sachbeschädigung, bei der Schlägerei, beim Raub erhoben wird. Das hat mit Terrorismus gar nichts zu tun. Wir haben das heute übrigens schon. Damit muss gearbeitet werden. Wie könnte man das klarer konturieren, damit wir am Ende nicht eine Regelung fassen, die über die Karlsruher Urteile hinausgeht und am Ende der Polizeibeamte im Revier im Kriminaldauerdienst nicht mal einfachste Datenabgleiche vornehmen kann, wenn er irgendeinem anderen Kriminellen auf der Spur ist?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege Binninger. Frau Kollegin Renner, bitte.

BE Abg. **Martina Renner** (DIE LINKE.): Von mir auch noch zwei Fragen: Die erste Frage richtet sich an Herrn Prof. Dr. Buermeyer. Es geht noch einmal

um einen Teilaspekt der Umsetzung des Urteils des Bundesverfassungsgerichts. Es ist ja aufgegeben, diese unabhängige Stelle zur Prüfung der Daten aus Wohnraumüberwachung und Online-Durchsuchung zu schaffen. Hier wird jetzt das Amtsgericht Wiesbaden vorgesehen. Jetzt die Frage: Sind denn dort die Kolleginnen und Kollegen tatsächlich überhaupt in der Lage, die Eingriffstiefe, z. B. beim Einsatz von Staatstrojanern, beurteilen zu können? Müsste es dort nicht auch technische Expertise geben? Wir sprachen vorhin über Zero-Day-Exploits und ähnliche Geschichten. Da kann man z. T. in den Systemen manipulativ tätig werden, also Daten verändern, Daten retrograd auswerten und Ähnliches mehr. Dazu braucht es doch an dieser Stelle umfängliche Fachkenntnis und zum Zweiten: Ist denn dort auch der Wille vorhanden, eben nicht nur einmal zu prüfen, sondern die Maßnahme zu begleiten oder müsste das nicht so sein, dass man sich dann eben auch im Verlauf der Überwachungsmaßnahme regelmäßig informieren lässt? Das wäre der erste Punkt. Der zweite Punkt geht an Herrn Gerhold: Die BfDI hat ja in der Stellungnahme geschrieben, dass sie die Gefahr sieht, dass durch die Struktur des zu schaffenden Datenpools und der Befugnisse der Weiterverarbeitung aber auch dem Austausch, insbesondere auch mit externen Stellen, die Möglichkeit geschaffen wird, dass Artikel 11 der Datenschutzrichtlinie für Polizei und Justiz unterlaufen würde und dass so etwas wie Personenprofile entstehen könnte. Die Frage: Können Sie das vielleicht noch einmal erläutern und sehen Sie sogar die Regelung verletzt, dass man automatisierte Entscheidungen nicht treffen darf, indem man z. B. durch diese Art des Datenpoolaufbaus eben auch Persönlichkeitsprofile, Personenprofile schafft, wo der Begriff der automatisierten Entscheidung sehr nahe kommt?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Kollegin Renner. Herr Kollege Grötsch, bitte.

BE Abg. **Uli Grötsch** (SPD): Vielen Dank, Herr Vorsitzender. Herr Dr. Buermeyer, Sie haben eben in Bezug auf die Mitziehautomatik gesagt: Die Frage ist doch, wie kommen die Daten in die Datenbank hinein? Für uns ist natürlich auch interessant, wie sie da wieder herauskommen, wenn sie einmal drinnen sind. Wenn ich das eben richtig verstanden habe – oder wenn ich die Regelung richtig verstehe – prüft dann am Ende, also wenn die Frist eintritt, ein Beamter des Bundeskriminalamts, ob die Daten unter den Voraussetzungen, die Sie gerade genannt hatten, noch gebraucht werden oder ob sie gelöscht werden können. Würden Sie, Herr Dr. Buermeyer, mir zustimmen, wenn ich sage, dass das auch letztendlich damit zu tun hat, welche Mentalität im BKA herrscht, was jetzt die Löschung der Daten angeht? Ich meine das so: Herr Münch, wenn Sie jetzt ein Präsident sind, der womöglich eher liberal ist und mehr Wert darauf legt, dass wirklich nur das weiter verwendet wird, was auch wirklich unter den Gesichtspunkten noch gebraucht wird und nach Ihnen kommt vielleicht ein Präsident – in ferner Zukunft – der das ganz anders sieht. Wer weiß, in ferner Zukunft habe ich angefügt. Verstehen Sie die Wertschätzung, wenn ich das sage? Wie gesagt, dann kommt vielleicht ein Präsident, der sieht das anders. Der ist der Meinung, dass das nur gelöscht werden soll, wenn es dann wirklich raus muss und dann entsteht da eine völlig andere Situation, wenn ich das richtig verstehe. Würden Sie mir da zustimmen, Herr Dr. Buermeyer, wenn ich das so sehe? Und dann nochmal an Herrn Prof. Dr. Bäcker zum Thema fehlende Legaldefinition des Begriffs Gefährder. Sehen Sie es als schädlich für die Anwendung des Gesetzes, dass es das nicht gibt? Es gibt wohl eine Definition des AK II der Innenministerkonferenz, die auch schon ziemlich alt ist. Wir reden hier im parlamentarischen Bereich jede Woche intensiv darüber, wie wir mit Gefährdern umgehen aber gesetzlich definiert ist es nicht, was ein Gefährder ist. Sehen Sie dahingehend einen Schaden durch diese fehlende Legaldefinition, was die Anwendung des Gesetzes angeht? Das sind meine Fragen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Kollege Grötsch. Frau Kollegin Mihalic, bitte.

Abg. **Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Vielleicht knüpfe ich gleich an die Frage von Herrn Grötsch an. Es betrifft die fehlende Legaldefinition „Gefährder“. Wie würde sich denn eine solche Legaldefinition ins Verhältnis zu anderen polizeilichen Begriffen wie den des Verhaltens- oder des Zustandshafters setzen lassen? Das müsste ja sozusagen irgendwie zusammenpassen. Wenn Sie da sozusagen anschließend an die Frage von

Herrn Grötsch noch zusätzlich zu ausführen könnten? Dann möchte ich jetzt noch einmal auf das Thema Fußfessel zu sprechen kommen und Herrn Münch fragen: Im Gesetzentwurf wird der Erfüllungsaufwand des BKA durch die Einführung der Fußfessel mit 170 Euro für das Überwachungsgerät und 500 Euro monatlich für die Überwachung der Personen angegeben. Schließt das Ihrer Ansicht nach auch die Kosten aller Einsätze ein, die dadurch ausgelöst werden, dass betroffene Auflagen verletzt werden, ohne dass es einen konkreten terroristischen Hintergrund gibt? Inwiefern haben Sie diesen zu erwartenden Mehraufwand, auch im Rahmen Ihrer Nützlichkeitsanalyse, mitberücksichtigt, die es ja vom BKA gibt? Vielleicht in dem Zusammenhang gefragt, Herr Münch: Also mal davon ausgehend, wir haben im Bereich des BKA null Gefährder aber einige bundesweit und Sie haben vorhin auch gesagt, dass wir bundesweit über 38 Fälle reden, die mit Meldeauflagen versehen sind, also bei denen ein offenes Maßnahmenkonzept in Betracht kommt. Wie viele Fälle würden Sie denn sozusagen für das BKA prognostizieren, bei denen ein solches offenes Maßnahmenkonzept mit Fußfesseln in Frage kommt? Würde sich Ihrer Ansicht nach auch aufgrund der neuen Möglichkeiten für eine offene Überwachung etwas an der Einordnung der jeweiligen Personen verändern? Wann könnte sozusagen ein offenes Maßnahmenkonzept gefahren werden und wann nicht? Rechnen Sie damit, dass durch die Möglichkeit der Fußfesseln mehr Fälle in der offenen Überwachung vorgesehen werden als bisher? Dann möchte ich noch eine Frage an das Thema Psychotherapeuten anschließen. Da hat mich vorhin ein bisschen die Aussage von Herrn Prof. Dr. Schwarz irritiert, dass § 62 im Gesetzentwurf angelehnt sei an die Regelung an die StPO, also in § 53 StPO sind die psychologischen Psychotherapeuten ja ausdrücklich erwähnt und das sind sie jetzt im Gesetzentwurf § 62 BKA-Gesetz eben nicht. Deswegen stellt sich schon die Frage – die möchte ich auch an Sie richten, Herr Prof. Dr. Schwarz, aber auch an Herrn Dr. Buermeyer und Herrn Prof. Dr. Bäcker – wenn sich eben strafprozessuale und präventive Ermittlungsmöglichkeiten annähern, muss dann nicht auch der Schutzstandard bei Berufsgeheimnisträgern gleichwertig ausgestaltet sein und müsste man dann nicht auch die psychologischen Psychotherapeuten extra in § 62 erwähnen, eben damit es sich auch an die Regelung der StPO annähert? Daran anschließend die Frage, welche Erwägungen – vielleicht kann man sagen, welche polizeilichen Erwägungen – sprechen denn dafür, Psychotherapeuten in § 62 nicht zu erwähnen, wenn deren Tätigkeit praktisch den Kernbereich privater Lebensführung betrifft? Wenn Sie dazu auch noch Stellung nehmen könnten? Dann hätte ich noch eine abschließende Frage an Herrn Gerhold. Wir haben vorhin die Einschätzung von Herrn Münch gehört, dass viele Probleme im Bereich des INPOL-Systems liegen. Wenn man dort also Veränderungen vornehmen möchte – im Hinblick auf einen Gefährder oder eine Person – und wenn man da weitere Dinge erfassen möchte, dann würde es 20 Monate dauern bis man sie sozusagen in dieses System einfügen könnte. Wie schätzen Sie diese Bewertung ein? Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Frau Kollegin Mihalic. Ich gehe davon aus, die erste Frage, die Sie im Anschluss an Herrn Grötsch gestellt haben, richtete sich an Herrn Prof. Dr. Bäcker. Dann beginnen wir auch mit Ihnen, Herr Prof. Dr. Bäcker und gehen durch. Wir haben noch etwa 13 Minuten Zeit. Es sind kurze und knappe Antworten mehr als erwünscht.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Vielen Dank. An mich sind zwei Fragen gerichtet worden. Einmal nach dem Gefährder, einmal nach dem psychologischen Psychotherapeuten.

Zu der Gefährderfrage und zum Verhältnis des Gefährders zur Polizeipflicht: Wenn man in meiner idealen Welt das BKA-Gesetz so umgestalten würde, dass im Terrorismusbereich eigentlich die konkrete Gefahr immer reicht, dann bräuchten wir eben als Adressatenregelung dazu in der Regel die Regelungen über die Polizeipflicht, die auch jetzt schon in Bezug genommen werden. Derjenige, von dem wir eine Straftat erwarten, ist ein Verhaltensstörer in klassischer polizeirechtlicher Terminologie. Jetzt ist es so, dass das Gesetz das nicht macht, sondern das Gesetz einen bunten Strauß von weiteren Tatbestandsfassungen enthält, die alle mehr oder weniger auf die Person bezogen sind. Das ist das, worüber wir eben geredet haben. Die sind aber unterschiedlich voneinander und auch mit gutem Grund, denn manche der Maßnahmen im Gesetz sind eingriffsintensiver und manche sind weniger eingriffsintensiv. Letztlich

steuert hier der Verhältnismäßigkeitsgrundsatz die Tatbestandsfassung. Eine einheitliche Gefährderdefiniton wäre in diesem Zusammenhang meiner Ansicht nach eher schädlich, denn dann würden wir ja diese Differenzierung aufgeben müssen. Das wäre, glaube ich, nicht klug. Jenseits der Tatbestände und jenseits auch von Bevorratungstatbeständen, wie § 18 des Entwurfs, sehe ich keinen Bedarf für eine besondere Regelung, was ein Gefährder im Rechtssinne ist. Was soll denn daraus folgen? Ich sehe da keine Konsequenz. Dann sollte man es aber auch lassen. Das wäre schlechte Gesetzgebung, den dann trotzdem zu definieren.

Abg. **Hans-Christian Ströbele** (BÜNDNIS 90/DIE GRÜNEN): Deshalb haben die ja auch die Stufen eingeführt.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Genau. Die Stufen des Gefährders als polizeipraktisches Instrument, um Gefährdungseinschätzungen zu rationalisieren, lassen sich ja ein stückweit in die gesetzlichen Tatbestandsfassungen übertragen, indem ich eben im § 39 in der Generalklausel zur Datenerhebung nur die Anforderung habe, eine Person will eine Straftat begehen und die erhobenen Daten sind zur Verhütung der Straftat erforderlich. Das ist sehr wenig. Im Unterschied dazu habe ich z. B. im § 51, der Vorschrift der Telekommunikationsüberwachung, die Anforderung, dass bestimmte Tatsachen die Annahme rechtfertigen, dass die Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird bzw. dass das individuelle Verhalten der Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat begehen wird. Was das alles so genau bedeutet, weiß ich auch nicht, aber es wird, glaube ich, offensichtlich: Hier soll mehr gefordert werden. Möglicherweise lässt sich da was draus machen, mit dem, was polizeifachlich intern an differenzierten Einstufungen gängig ist. Möglicherweise lässt sich das nachher ein stückweit auch auf diese Ermächtigungstatbestände spiegeln. Bestimmt nicht schematisch im Sinne von Stufe 4 ist § 51, aber vielleicht so im Sinne von Faustregeln oder ersten Annäherungen an diese Vorschriften. Ich beneide das BKA auch nicht um die Aufgabe, diese nachher anwenden zu müssen.

Die zweite Frage ist die nach dem Psychotherapeuten. Ich glaube schon, dass sich der § 62 BKAG an die Strafprozessordnung anlehnt, denn es geht ja hier nicht unmittelbar um die Frage von Zeugnisverweigerungsrechten, wenn jemand direkt gefragt wird, sondern es geht ja um die Frage, inwieweit Zeugnisverweigerungsberechtigte auch gegen verdeckte Überwachungsmaßnahmen geschützt werden. Da ist es aber jetzt so, dass grundsätzlich einmal, wenn wir Zeugnisverweigerungsberechtigte absolut schützen, das eigentlich zunächst eine überobligationsmäßige Wohltat ist. Eigentlich ist der Gesetzgeber dazu nicht unbedingt verpflichtet, das aus verfassungsrechtlicher Sicht zu tun. Sie dürfen das natürlich, aber sie müssen es nicht. Das Problem bei der alten Differenzierung zwischen Rechtsanwälten und Strafverteidigern war ja vor allem, dass diese nicht einleuchtet und dass die auch nicht trennscharf zu leisten war. Ich glaube deswegen: über die Frage, welche Berufsgruppen Sie konkret absolut schützen oder nicht, sollte genuin rechtspolitisch debattiert werden. Ich persönlich habe hohe Sympathien dafür, zumindest die Journalisten wieder mit einzubeziehen, aber das ist erst einmal keine Frage des Grundgesetzes. Letzter Punkt in diesem Zusammenhang: Unabhängig von dem Schutz der Berufsgeheimnisträger sind ja immer die Schutzregelungen für den Kernbereich der privaten Lebensgestaltung zu beachten. Wenn wir jetzt sagen, das Gespräch mit dem Psychotherapeuten – das würde ich sagen – unterfällt typischerweise dem Kernbereich, dann darf es aus diesem Grund nicht abgehört werden. Nicht also über den Hebel Berufsgeheimnisträger, sondern über den Kernbereich kommen wir letztlich zum erwünschten Ergebnis. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Bäcker. Herr Dr. Buermeyer, bitte.

SV **Dr. iur. Ulf Buermeyer, LL.M.** (Richter am Landgericht Berlin): Vielen Dank. Ich schließe meine Antwort direkt an das an, was Herr Prof. Dr. Bäcker gerade gesagt hat und würde aber unterstreichen wollen: Wenn es denn so ist, dass ein Gespräch mit einem psychologischen Psychotherapeuten in aller Regel unter Geltung des Kernbereichsschutzes ohnehin nicht abgehört werden darf, warum erweckt dann dieser Gesetzentwurf den Eindruck durch diesen nur

relativen Schutz in § 62 Abs. 2, dass das Gespräch doch abgehört werden könne? Jedenfalls nach Maßgabe einer Einzelfallentscheidung durch das BKA. Das war ja eben mein Punkt, dass die Gesetzesfassung einen falschen, unzutreffenden Eindruck erweckt, dass diese Gespräche wie gesagt nach Maßgabe einer Abwägungsentscheidung abgehört werden können. Damit leistet das Gesetz Fehlentscheidungen in der Praxis Vorschub. Wir wissen alle – jedenfalls die, die schon einmal in der Strafrechtspraxis oder polizeilich gearbeitet haben – dass es einfach häufig Entscheidungen sind, die unter großem Zeitdruck und unter dem Gewicht einer enormen Verantwortung für Menschenleben z. B. zu treffen sind. Da muss man einfach damit rechnen, dass im Einzelfall eine Fehlentscheidung getroffen wird. Dieser Fehlanwendung des Rechts kann man, denke ich, sehr schön vorbeugen, wenn man die Differenzierung zwischen relativen und absoluten Berufsgeheimnisträgern aufgibt. Da hinzu kommt natürlich, dass das Stichwort Vorratsdatenspeicherung in diesem Zusammenhang eine große Rolle spielt, denn da sind die Berufsgeheimnisträger auch nicht konsequent geschützt, wie wir wissen. Nächster Punkt: Stichwort: Unabhängige Stelle, Amtsgericht Wiesbaden, praktische Durchführung z. B. von Staatstrojanern. Frau Renner, ich stimme Ihnen absolut zu, dass natürlich ein Richter im Amtsgericht Wiesebaden per se nicht in der Lage ist, einzuschätzen, ob ein Staatstrojaner irgendwelche technischen Anforderungen erfüllt. Wie sollte er denn? Das hat er nicht gelernt. Zufälligerweise kann er privat entsprechende Kenntnisse haben. Das soll vorkommen, auch bei Richterinnen und Richtern, aber das kann man jedenfalls nicht erwarten und in diesem Zusammenhang war die mündliche Verhandlung in Karlsruhe, an der ich teilgenommen habe, ja auch sehr eindrucksvoll. Der Senat hatte einen Kollegen geladen als sachverständige Auskunftsperson, der über Staatstrojanereinsätze zu entscheiden hat und der hat ziemlich offen gesagt: „Ich hatte natürlich überhaupt keine Ahnung, worüber ich da eigentlich zu entscheiden habe, also habe ich die amtsrichterliche Kaffeerunde gefragt.“ Das ist eben die Notlösung, die man als Richter anwendet, wenn man nicht recht weiß, welches eigentlich die richtigen Vorgaben sind. Der Kollege hat sich völlig richtig verhalten. Aber was soll er denn auch tun, wenn ihm das Gesetz letztlich keine Prüfungsmaßstäbe vorgibt? Es sagt natürlich jetzt im Abs. 2, wenn das technisch sicherzustellen ist, dass z. B. nur die notwendigen Veränderungen an dem System vorgenommen werden, in das da eingedrungen wird und dass diese Änderungen wieder rückgängig gemacht werden müssen, aber wie soll der Richter das prüfen, ob diese eingesetzte Software diesen Anforderungen entspricht? Deswegen meine Forderung aus der ersten Runde, dass das Gesetz hier ein wirksames Prüfverfahren vorsehen muss – aus meiner Sicht, z. B. eben über eine Verordnungsermächtigung für das BSI. Die Darlegung, dass die technischen Voraussetzungen überhaupt erfüllt sind, müssten wenigstens in dem Antrag anzugeben sein. Im Abs. 5 ist ja ausführlich geregelt, welche Mindestinhalte ein solcher Antrag auf Einsatz eines Staatstrojaners zu enthalten hat – und wie dieses technische Mittel beschaffen ist, ist da nicht enthalten. Das müsste das BKA – streng genommen – dem Richter nicht einmal mitteilen. Ich denke so augenzwinkernd kann man eine Rechtsgrundlage für einen Staatstrojanereinsatz rechtsstaatlich überzeugend nicht fassen. Auf die Frage von Herrn Grötsch nur ganz kurz: Selbstverständlich hängt die Entscheidung darüber, welche Daten das BKA weiter speichert oder nicht speichert, davon ab, welche „Politik“ im BKA gerade herrscht. Es gibt – das hat Prof. Dr. Bäcker ausgeführt – Löschtatbestände, vermutlich im neuen Bundesdatenschutzgesetz, so es denn Gesetz wird, aber wie die dann in der Praxis angewendet werden, das weiß Herr Münch im Zweifel viel besser als ich. Das bestimmt sich letztlich durch Verwaltungsvorschriften. Natürlich auch durch die Organisation dieser Prüfung im Behördenaufbau und da werden immer Spielräume bestehen dafür, welche Daten man löscht oder auch noch nicht löscht. Insofern klar gibt es ein großes Einfallstor oder sagen wir gibt es viele Stellschrauben auch politischer Art. Letzter Punkt zu Frau Mihalic zum Berufsgeheimnisträger. In der Tat sehe ich es auch als großes Problem, wenn die Regelung im BKAG und in der Strafprozessordnung nicht deckungsgleich sind, denn dann stellt sich ja genau die Frage, ob die zunächst präventivpolizeilich erhobenen Daten nicht durch diese Hintertür dann auch im Strafverfahren Verwendung finden können? Oder ob es zumindest doch so ist, dass sie mehr oder weniger deutlich als Spurenansätze

Anwendung finden in der strafrechtlichen Ermittlungsarbeit und genau das will ja § 53 der Strafprozessordnung verhindern. Diesen Hintertüreffekt sehe ich hier auch sehr deutlich. Wie gesagt, die einzelnen Argumente für die Einbeziehung weiterer Berufsgruppen wurden schon genannt, aber ich denke, dieser Grund spricht dafür, auf die Differenzierung im § 62 des Entwurfs zu verzichten. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Dr. Buermeyer. Dann kommen wir nun zu Herrn Gerhold.

SV **MD Diethelm Gerhold** (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank. Zunächst zu der Frage der Persönlichkeitsprofile: In der Tat ist es so, dass durch dieses neue System die Möglichkeit geschaffen wird, nicht nur intern beim BKA aus verschiedenen Bereichen die Daten zusammenzuführen, abzugleichen, sondern auch mit externen Systemen. Nicht nur auf nationaler Ebene, sondern auch auf internationaler Ebene – Europol, SIS, VIS, PNR-Fluggastdaten – nur um einige zu nennen. Alle diese Dateien können abgeglichen werden. Es besteht auch die Möglichkeit dann zuzuspeichern, d. h. den Datensatz zu einer Person oder zu einem Ereignis entsprechend aus diesen anderen Dateien zu ergänzen, und das ohne jede Differenzierung. D. h., es ist nicht nur möglich, z. B. für den Bereich des internationalen Terrorismus, sondern es ist generell möglich und es gibt keine weiteren Voraussetzungen oder verfahrensmäßigen Absicherungen, um das in irgendeiner Art und Weise zu beschränken. Es gibt auch keine Schutzmechanismen, sodass im Ergebnis eine solche Persönlichkeitsprofilerstellung vom System her ohne weitere Einschränkung möglich wäre. Ob es getan wird, ist eine andere Frage, weil es ein Verstoß gegen die JI-Richtlinie wäre, aber es wäre möglich. Was die automatisierte Einzelentscheidung anbelangt, denke ich, muss man noch ein stückweit unterscheiden zwischen der rechtlichen Voraussetzung und der Praxis. Rein rechtlich gibt es da noch einen Mechanismus, wonach noch ein Mensch entscheiden müsste, aber ob das dann in der Praxis so eingehalten wird, ist eine Frage, die sich dann u. a. durch eine Kontrolle der BfDI zeigen wird. Zu der anderen Frage, was das System anbelangt, bestehen aktuell sicherlich die Schwierigkeiten, die der Präsident des BKA geschildert hat. Es geht auch nicht darum, dieses System, so wie es ist, aufrechtzuerhalten. Es gibt aber jetzt schon eine Lösung mit diesem PIAV. Das sind die neuen Dateiformen, die gerade etabliert wurden. PIAV steht für Polizeilicher Informations- und Analyseverbund, in dem viele dieser Probleme, die auch zu Schwierigkeiten und Langwierigkeiten führen, behoben werden. Dabei handelt es sich auch um kein Datenschutzproblem, um es ganz deutlich zu sagen. Diese Schwierigkeiten beruhen darauf, dass halt Bund und Länder zusammen kommen müssen, dass es unterschiedliche Systeme gibt, dass es Gremien gibt, die bei jeder Änderung gemeinsam entscheiden müssen. Das ist keine Frage, die vom Datenschutz ausgelöst wird und es geht auch nicht darum, dass der Datenschutz ein modernes System verhindern möchte – um das einmal ganz deutlich zu sagen. Wir sehen selber die Notwendigkeit, dass da IT-mäßig sehr viel getan werden muss. Die Frage ist nur, wie dies geschieht und welche Sicherungen künftig noch bestehen. Da geht aus unserer Sicht das, was jetzt geplant ist, darüber hinaus. Vor allen Dingen dadurch, dass die Dateianordnungen jetzt komplett wegfallen, fällt auch die bisherige Basis weg, weil weder der Erhebungszweck noch die Rechtsgrundlagen gespeichert werden müssen. Dadurch geht auch so ein bisschen die Grundlage für alles Weitere verloren, z. B. Zugriffsberechtigungen oder auch Löschfristen und Ähnliches – das hängt alles miteinander zusammen – dies wird alles ohne Not aufgegeben. Das ist das Problem bei den geplanten Änderungen und nicht, dass man jetzt generell eine moderne IT verhinden möchte. Dieser Hinweis ist mir ganz wichtig.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Gerold. Herr Prof. Dr. Möstl, bitte.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): An mich sind zwei Fragen gerichtet worden. Zu dem Berufsgeheimnisträger möchte ich mich jetzt kurz fassen, weil dazu schon mehrfach Stellung genommen worden ist. Ich habe das Bundesverfassungsgericht so verstanden, dass es das Regelungskonzept des Gesetzgebers eigentlich insgesamt gebilligt hat und eben nur Detailkorrekturen verlangt hat, sodass ich glaube, dass man da auf der sicheren Seite ist. Richtig ist allerdings, was auch betont worden ist, dass wir kumulativ immer noch das

Kernbereichsschutzkonzept haben, was eben sozusagen später vom Bundesverfassungsgericht erfunden worden ist und, dass es da gewisse Dopplungen geben kann.

BE Abg. **Clemens Binninger** (CDU/CSU): Ich will nur kurz dazwischenrufen. Dieser Berufsgeheimnisträgerschutz bezieht sich hier auf alle Maßnahmen aus dem Abschnitt. Nicht nur immer auf die Telefonüberwachung, wo es um den Kernbereich geht. Deshalb macht es schon Sinn.

Abg. **Hans-Christian Ströbele** (BÜNDNIS 90/DIE GRÜNEN): Es soll ja auch keiner wissen, wo man auf der Couch liegt.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): Zu § 12 und dem Zweckbindungsgrundsatz: Ich glaube, es ist offensichtlich aus dem Gesetz heraus, Begründung des Gesetzentwurfs, und wenn man das Bundesverfassungsgerichtsurteil anschaut, dass hier darüber hinausgegangen wird über das, was hier erforderlich war. Der relativ strenge Maßstab der hypothetischen Datenneuerhebung soll eben auf alle Daten erstreckt werden. Welche Auswirkungen das nun polizeipraktisch hat, kann ich als Wissenschaftler eigentlich nur beschränkt beurteilen, aber es hat mich schon stutzig gemacht, in der Stellungnahme des Bundesrates zu lesen, dass auf Seiten der Länder also doch befürchtet wird, dass es zu Erschwernissen kommt und, dass es eine große Herausforderung ist, durchgehend auch den damit verbundenen Protokollierungsanforderungen zu genügen. So gesehen, glaube ich, lohnt es sich schon darüber nachzudenken, ob man nicht zu einem differenzierten Regelungskonzept übergeht, dass die aus besonders eingriffsintensiven Maßnahmen erhobenen Daten diesem strengeren Konzept unterstellt und die übrigen Daten einem gelockerten Konzept, etwa wie das Bundesverfassungsgericht es früher judiziert hat, dass die Zwecke nicht unvereinbar sein dürfen oder dergleichen. Kehrseite ist evtl. – das muss man sich überlegen – dass dieses durchgehend strenge Konzept einen Vorteil dahingehend haben könnte, dass man sagt, wenn es die spätere Verwendung der Daten anbelangend so einen durchgehend strengen Maßstab gibt, sind die Maßstäbe andere als man es früher gedacht hat, was die Speicherung, die zwischenzeitliche Speicherung betrifft. Dass es vielleicht leichter möglich ist – was hier auch immer wieder angesprochen worden ist, z. T. auch kritisiert worden ist – Daten zu bevorraten, zu speichern, zu behalten, weil eben danach dieses strenge Konzept Anwendung findet. Das ist ein ganz gutes Beispiel dafür, dass selbst wenn das Bundesverfassungsgericht quasi lehrbuchartig sagt, wie man es machen muss, eben doch wieder Folgefragen offen bleiben. Und die Frage, welche Auswirkungen so ein neues Konzept auf die Frage der Zulässigkeit von Speicherung hat, ist eben sehr offen. Ich würde schon einmal sagen: Wenn sich der Gesetzgeber zum neuen Konzept durchringt, werden auch hinsichtlich der Frage der Zulässigkeit von Speicherungen die Karten neu gemischt.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Möstl. Herr Münch, bitte.

SV Präs. **Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank. Drei Vorbemerkungen kann ich mir nicht verkneifen. Erstens: Was die technischen Fähigkeiten angeht, die bei Gericht erforderlich sein sollten oder müssen. Nach dem Urteil des Bundesverfassungsgerichts 2008 haben wir eine standardisierte Leistungsbeschreibung entwickelt, an der muss sich die Software – egal ob eigenentwickelt oder fremdentwickelt – messen lassen. Das gilt auch für künftige Software, z. B. im mobilen Bereich. Das ist wahrscheinlich auch ein lebendes Instrumentarium, aber wir beauftragen externe Gutachter, die am Ende dann auch nachweisen helfen sollen, dass die Software, die wir einsetzen, den Grundlagen entspricht, die das Verfassungsgericht uns aufgegeben hat. Zweitens: Die Mitziehregel, die nicht vorhanden ist, hat uns in der Praxis erhebliche Schwierigkeiten gemacht. Spätestens nach einem entsprechenden Urteil aus Kassel im Jahre 2007, weil es uns gezwungen hat, an jedem zu speichernden Ereignis orientiert zu prüfen und nicht an der Frage der Historie einer Person, also einer kriminellen Entwicklung einer Person. Deshalb sind wir sehr froh, wenn es diese klare Befugnis im Gesetz wieder geben soll. Was die Auslegung angeht, bin ich sehr eng bei Herrn Dr. Buermeyer. Was die Frage angeht, was man letztendlich bei den Aussonderungsprüffristen beachten muss: Nicht nur die polizeiliche Maßnahme, sondern das Datum, das von den Personen ausgeht. Insofern haben wir da keinen Widerspruch. Drittens: Wir vermissen keine Legaldefinition eines Gefährders.

Wir kommen gut mit den Störerbegriffen und mit den tatbestandlichen Voraussetzungen von Ermächtigungsgrundlagen zurecht. Die jetzige Definition, die wir anwenden, erfüllt die Schwelle der Grundmaßnahmen, nämlich dass Tatsachen vorhanden sein müssen, die die Annahme rechtfertigen, dass die Person über einen überschaubaren Zeitraum zu einer erheblichen Tat möglicherweise ansetzt. D. h. mit dieser Definition erreichen wir die Schwelle, dass wir Grunddaten auch für die Person erheben können, um das bundeseinheitlich zu machen. Zu Ihrer konkreten Fragen, Frau Mihalic: Der Erfüllungsaufwand, der in der Begründung hinterlegt ist, ist zunächst einmal von den vorhandenen Prozessen adaptiert, die wir uns anschauen können. In Hessen kostet solch ein Gerät 170 Euro, 500 Euro wird man monatlich an pauschalen Kosten für eine Überwachung ausgeben. Ob das in praxi das ist, was wir bei dieser Aufgabe haben werden, da mache ich noch einmal ein Fragezeichen dran. Was die technische Umsetzung angeht: sicherlich. Aber praktisch, glaube ich, ist das nicht immer anwendbar, z. B. wird dort von Privaten die Fußfessel angelegt. Ob man das auf einen Gefährder übertragen kann, wage ich zu bezweifeln, wo die Mitwirkungsbereitschaft der Zielperson vielleicht eine andere ist. Das Zweite ist eben, dass wir auch bei dem Blick auf die Daten noch einmal anders herangehen müssen als bei einer Stelle, die nicht für diese Aufgabe geschult ist, d. h. wir sind noch nicht im Abschluss mit dieser Frage, was das kostet. Einsätze sind jedenfalls davon nicht umfasst. Diesen Mehraufwand, den wir insgesamt sehen, auch wenn wir eine solche Überwachungsstelle einsetzen – wenn man den Vergleich zu alternativen Konzepten zieht, da sind wir in der Regel auch bei der Frage von temporären Observationsmaßnahmen, dann sind wir sehr schnell wieder in einer Waagschale, wo wir sagen: Diese offene Maßnahme, wenn insgesamt ein Maßnahmenkonzept für den jeweiligen Betroffenen sich als geeignet herausstellt, dann glauben wir, ist die Fußfessel am Ende sogar wirtschaftlich als Alternativmaßnahme – auch einfacher insgesamt – umsetzbar. Weil die Ressourcen, wenn Sie einmal überlegen, wie viele mobile Einsatzkommandos und Observationstrupps wir in der Republik haben, gar nicht ausreichen, um insgesamt eine Überwachung sicherzustellen. Ob das Auswirkungen hat auf die Frage, wie wir am Ende Maßnahmenkonzepte in der Praxis umsetzen – das kann ich mir vorstellen, ich kann das aber noch nicht abschließend beurteilen. Wir sehen hier auch in der Nachbereitung Anis Amri, dass wir durchaus selbstkritisch sagen: Wir haben Lücken in der Frage von offenen Maßnahmenkonzepten, wie wir die ausgestalten werden, wenn wir erkennen, dass verdeckte Maßnahmen nicht mehr weiterführen. Wir entwickeln als nächste Stufe, nachdem wir RADAR-iTE als einheitliches Bewertungsinstrument entwickelt haben, nun auch mit wissenschaftlicher Unterstützung ein Instrument, weil wir sagen, dass wir ein einheitliches Risikomanagement in der Republik brauchen. Dabei wird die Frage auch eine Rolle spielen: Ist ein offenes oder ein verdecktes Maßnahmenkonzept - jeweils bezogen auf die Person und die Umstände - das geeignete? Insofern kann ich mir vorstellen, dass es noch einmal zu Verschiebungen kommt. In welchem Umfang kann ich aber nicht einschätzen. Ich denke, damit habe ich die Frage beantwortet. Wie viele Fälle für das BKA? Es bleibt die Ausnahme. Ich nehme einmal so ein Beispiel: Die Ermittlungen, die wir in Schleswig-Holstein zu drei Gefährdern geführt haben, die eine eins-zu-eins-Kopie der Attentäter zu Paris darstellen. In so einem Fall, wenn wir am Ende die Überwachung nicht mehr sicherstellen können, wenn es nicht zu einem Haftbefehl gekommen wäre, dann wären wir sicherlich bei der Frage der Fußfessel gewesen. Wie gesagt, es bleibt die Ausnahme.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Münch. Herr Prof. Dr. Schwarz, Sie haben jetzt das letzte Wort und die Gelegenheit, alles rund zu machen.

**SV Prof. Dr. Kyrill-A. Schwarz** (Universität Würzburg): Herr Vorsitzender, sehr geehrte Damen und Herren, auch mit Blick auf die fortgeschrittene Zeit versuche ich jetzt sehr kurz die entsprechenden Fragen zu beantworten. Frau Mihalic, mit Blick auf die Geheimnisträger: Ich glaube, dass wir hier einen Bereich haben, bei dem, wie meine Vorredner auch bereits gesagt haben, das Verfassungsgericht letzten Endes Randkorrekturen verlangt hat und einen gewissen gesetzgeberischen Gestaltungsspielraum eröffnet hat. Dass es Gründe geben mag, die unter Umständen für eine Erstreckung sprechen, will ich nicht ausschließen. Aber ich glaube, das ist eine wirklich originäre

Entscheidung, wo auch tatsächlich die Vorgaben von Karlsruhe nicht so zu verstehen sind, dass hier unmittelbar Handlungsbedürfnis besteht. Zweite Frage von Herrn Binninger: Wenn ich mir die Ausgangsposition des Bundesverfassungsgerichts anschaue: Wenn man ein wenig die Rechtsprechung des Verfassungsgerichts der letzten 15 Jahre Revue passieren lässt, dann kann man ja, nachdem auch viel Kritik am Verfassungsgericht bereits geäußert wurde, vielleicht eins doch sagen: Bisweilen bei Ansehung der Realitäten, auch der Kriminalitätsbekämpfung, der Terrorismusbekämpfung hat das Gericht etwas dazu gelernt. Und zwar nicht nur in den Sondervoten, sondern auch in den die Senatsmehrheit tragenden Ausführungen. Wenn man sich beispielsweise noch die Entscheidung zum großen Lauschangriff anschaut und sich dort das absolute Kernbereichsmodell vor Augen führt, dass eigentlich jegliche Ermittlungsmöglichkeiten in dem Bereich ausgeschlossen hat, soweit der Kernbereich auch nur berührt sein könnte, so sieht man ja, dass jetzt das Gericht durchaus ein abgestuftes Konzept vorsieht. Vor dem Hintergrund – das ist ja nicht nur Einsicht vielleicht in tatsächliche Notwendigkeiten, sondern wenn Sie sich jetzt eine Regelung, die noch einmal die Bestimmungen über die Online-Durchsuchungen betrifft, anschauen – ich glaube, mehr als das, was Sie in § 49 Abs. 7 BKAG-Entwurf gemacht haben, verlangt Karlsruhe auch nicht aber es ist ein Musterbeispiel dafür, dass wir tatsächlich ein abgestuftes Konzept von kernbereichsschützenden Elementen haben, nämlich einen absoluten Kernbereich, in dem auch das Gericht sagt: Maßnahmen, die alleine, so wie es auch im Gesetz steht, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangen würden, sind unzulässig. Im Übrigen kann ich mir nicht vorstellen, dass das BKA als seine zentrale Aufgabe ansehen würde, Maßnahmen zu treffen, durch die allein und ausschließlich Erkenntnis aus dem Kernbereich privater Lebensgestaltung gesammelt werden sollten. Von daher ist es eine Aussage, die gut klingt, sie dürfte aber wohl an den Realitäten völlig vorbeigehen. Danach finden Sie die genau abgestuften Konzepte, was man mit den entsprechenden Maßnahmen machen darf, was man mit den Erkenntnissen machen darf, wie letzten Endes zu löschen ist. All das entspricht aber genau den Vorgaben – auch jüngerer Rechtsprechung. Vor dem Hintergrund würde ich insgesamt sagen, dass Sie mit dem, was Sie hier gemacht haben – und ich glaube, das dürfte auch weitgehend, bis auf gewisse Randmodifikationen, hier heute der vorherrschenden Ansicht der Sachverständigen entsprechen – mit dem Gesetzentwurf, den Sie hier haben, auf der sicheren Seite sind. Danke schön.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank, Herr Prof. Dr. Schwarz. Meine sehr geehrten Herren Sachverständige, ganz herzlichen Dank für Ihre Darstellung und die Beantwortung der Fragen. Vielen Dank an die Kolleginnen und Kollegen. Sie haben uns eine Menge für die weiteren Beratungen mitgegeben. Das werden wir jetzt alles in die Erwägung mit einbeziehen. Ich darf mich ganz herzlich bedanken, schließe die 107. Sitzung, denn die 108. wirft schon ihre Schatten voraus. In einer Viertelstunde geht es weiter. Ganz herzlichen Dank.

Schluss der Sitzung: 13:15 Uhr

Ansgar Heveling, MdB
**Vorsitzender**

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 A

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 10.03.2017

# Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

## zum

## Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

**BR-Drucksache 109/17 (Regierungsentwurf)**
**BT-Drucksache 18/11163 (Fraktionsentwurf)**

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Das Volkszählungsurteil des Bundesverfassungsgerichts hat das Datenschutzrecht in der Bundesrepublik Deutschland maßgeblich geprägt. Die Bundesregierung hat nunmehr einen Gesetzentwurf vorgelegt, der in der Zeit danach die bislang umfangreichsten Änderungen des polizeilichen Datenschutzes zur Folge hat.

Positiv bewerte ich, dass bereits einige meiner Änderungsvorschläge in der Ressortabstimmung berücksichtigt worden sind. Gleichwohl empfehle ich dringend eine gründliche fachliche Beratung. Denn es verbleiben noch gravierende – verfassungsrechtliche – Risiken.

Der Entwurf beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil zum BKAG und aus der neuen JI-Richtlinie zum polizeilichen Datenschutz umzusetzen (Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016). Er gibt dem Bundeskriminalamt darüber hinaus umfangreiche neue Befugnisse. Entsprechendes gilt – mit dem Informationsverbund – für die weiteren Polizeibehörden in Bund und Ländern.

Kritisch zu überprüfen sind insbesondere die nachfolgend dargelegten datenschutzrechtlichen Punkte. Im Annex habe ich hierzu konkrete Änderungsvorschläge beigefügt.

## 1. Neuer Informationsverbund und Abschaffung aller Dateien

*Die gesetzliche **Neugestaltung der polizeilichen Datenbanksysteme** ist weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die Europäische Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Sie führt zu unverhältnismäßig weitreichenden Speicherungen.*

Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahme bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Gleichzeitig müssen Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufrechterhalten werden, mit deren Hilfe die breitenwirksamen Grundrechtsgefährdungspotentiale moderner Datenverarbeitung eingegrenzt werden sollen.

Der Entwurf gibt wesentliche dieser Sicherungen auf. Er schafft die Grundlagen für einen neuen bundesweiten polizeilichen Informationsverbund und ein neues Informationssystem des BKA (in §§ 13ff. und 29 ff. BKAG-E). Der künftige Informationsverbund und das Informationssystem werden nicht mehr wie INPOL und PIAV in logische Dateien gegliedert sein. Alle Daten kommen stattdessen ohne nähere Zweckbestimmung in einen „großen Topf“ und können miteinander abgeglichen werden. Die Methoden des Datenabgleichs sind nicht eingegrenzt. Alle Daten und Datenfelder sind personenübergreifend beliebig miteinander verknüpfbar. Jeder Abgleich

kann zu weiteren Datenverknüpfungen führen und damit wiederum die Speicherdauer perpetuieren.

### 1.1. Grundsatz der Zweckbindung – Vorgaben des Bundesverfassungsgerichts

*Das Urteil des Bundesverfassungsgerichts ist ein Grundsatzurteil zur Zweckbindung. Damit legt es zusätzliche Anforderungen für Daten aus heimlichen bzw. eingriffsintensiven Ermittlungsmaßnahmen fest. Es stellt klar, wie diese Daten verwendet werden können. Es legitimiert nicht, die bestehenden* ***datenschutzrechtlichen Sicherungen für die elektronische Datenverarbeitung*** *der Polizeibehörden weitgehend aufzugeben.*

Das Bundesverfassungsgericht hat in seiner Entscheidung zum BKAG zu der Frage Stellung genommen, mit welchen Mitteln personenbezogene Daten im Gefahrenvorfeld heimlich erhoben werden dürfen und für welche Zwecke die Behörden diese Daten weiter verwenden und übermitteln dürfen (BVerfG vom 20. April 2016, Az. BvR 966/09 u.a., NJW 2016, 1781). Das Bundesverfassungsgericht hat in seinem Urteil den Grundsatz der Zweckbindung dogmatisch umrissen. Dabei hat es höhere Maßstäbe angelegt, wenn die Datenverarbeitung besonders intensiv in Grundrechte eingreift. Gleichzeitig hat das Gericht für die Anwendungspraxis einige Klarstellungen vorgenommen. Nach Ansicht des Gerichts darf eine Einzelerkenntnis aus einer heimlichen und eingriffsintensiven Ermittlungsmaßnahme innerhalb derselben Behörde, derselben Aufgabe und zum Schutz derselben Rechtsgüter als Anknüpfungstatsache für weitere Ermittlungen genutzt werden.

> ***Beispiel:*** *Der Ermittler für den Bereich der Betäubungsmittelkriminalität wertet das Protokoll einer Telekommunikationsüberwachung aus. Dort findet er die Aussage, nach der Person X nicht nur mit Betäubungsmitteln handelt, sondern auch Terrorismus finanziert. Diese Erkenntnis darf der Ermittler an seine Kollegen aus dem Bereich der Verfolgung von Staatsschutzdelikten und Terrorismus weitergeben.*

Die Bundesregierung zieht hieraus den Schluss, alle Daten könnten pauschal und ohne weitere Differenzierungen in einer großen Datenbank gespeichert werden. Sie behauptet, das Bundesverfassungsgericht habe das bisherige Datenschutzrecht durch ein **„horizontal wirkendes“ Datenschutzkonzept** ersetzt. **Diese Auffassung ist unzutreffend.**

Der Entwurf verzichtet darauf, die Behörden zu verpflichten, nähere Einzelheiten zum jeweiligen Zweck der Speicherung festzulegen**. Ohne diese Festlegungen ist – auch bei Datenschutzkontrollen – kaum noch prüf- und beurteilbar, ob die jeweilige Speicherung erforderlich ist.** Dies war bislang durch die Errichtungsanord-

nungen gemäß § 34 BKAG sichergestellt, die der Entwurf aber ersatzlos streicht (siehe dazu unten 3.1.).

Intensive Grundrechtseingriffe können sich nicht nur aus dem jeweiligen Ermittlungseingriff selbst (z.B. heimliche Telekommunikationsüberwachung), sondern auch aus der weiteren Verwendung dieser Daten im Einzelfall ergeben. Eine **eigenständige Eingriffswirkung** entfaltet auch ihre Speicherung in **elektronischen Dateien**. Dies betrifft die spezifisch breitenwirksamen Grundrechtsgefährdungspotenziale, insbesondere solche der elektronischen Datenverarbeitung. Das Bundesverfassungsgericht hat hierzu in zahlreichen Entscheidungen Stellung genommen, auf die es in der aktuellen Entscheidung verweist (Abs. Nr. 103; vgl. BVerfGE 100, 313, 358 ff.; 115, 320, 341 ff.; 125, 260, 316 ff.; 133, 277, 335 ff.). Es verweist auf seine ständige Rechtsprechung zur Zweckbindung und Zweckänderung (Abs. Nr. 276, beginnend mit einem Verweis auf BVerfGE 65, 1 – Volkszählung). Es spricht nichts dafür anzunehmen, das Bundesverfassungsgericht wolle die wesentlichen für die elektronischen Datenbanksysteme der Polizeien entwickelten Grundsätze zurücknehmen. Im Gegenteil. In der aktuellen Entscheidung weist das Gericht auf Folgendes hin:

> *„Dabei hat der Gesetzgeber in seine Abwägung auch die Entwicklung der Informationstechnik einzustellen, die die Reichweite von Überwachungsmaßnahmen zunehmend ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen.“ (BVerfG NJW 2016, 1781, Abs. Nr. 99).*

### 1.2. Struktur der neuen polizeilichen Informationsverarbeitung

*Nach dem bisherigen Datenschutzrecht sind Informationssysteme und Informationsverbünde bei der Polizei **in (logische) Dateien gegliedert**. Dies hindert nicht daran, die polizeilichen Datenbanksysteme zu modernisieren. Die Dateien können nach Zweckmäßigkeit und Erforderlichkeit angepasst werden. Die Ursache für die bisherigen Defizite haben zum Teil technisch bedingte Ursachen und liegen in einer unübersichtlichen und schwerfälligen polizeilichen Gremienstruktur. Es gibt also keinen Grund, das bisherige Recht aufzugeben.*

**Änderungsvorschlag BfDI:**

- **Beibehaltung des §§ 34**
- **Inhaltliche Beibehaltung der §§ 11 Absatz 1 Satz 2, Absatz 2 Satz 3 BKAG, Aufnahme des Dateibegriffs in §§ 18, 19 BKAGE**
- **Siehe Änderungsvorschläge im Annex**

Viele der bislang bestehenden Probleme liegen in der **unübersichtlichen und schwerfälligen Struktur der polizeilichen Gremien**. Diese sind jedoch nicht durch

das bisherige Recht, durch die Pflicht zu Errichtungsanordnungen oder durch „den Datenschutz“ verursacht. Dateien könnten auch nach bestehendem Recht neu zugeschnitten und strukturiert werden. Beispielsweise zeigen dies die neuen Dateien in PIAV. Die Datenschutzbeauftragten in Bund und Ländern haben den Prozess konstruktiv begleitet. An veralteten Strukturen festzuhalten, war nicht das Ziel der Datenschutzbeauftragten.

Die vollständige Abkehr vom bisherigen System der Dateien ist nicht notwendig, zu undifferenziert und daher abzulehnen. Dies sollte zunächst fachlich erörtert werden, sobald das BKA konkrete Planungen in belastbarer Form vorlegen kann. Erst wenn die Planungen einen höheren Konkretisierungsgrad erreicht haben, kann darüber gesprochen werden, ob und welche gesetzlichen Änderungen ggf. dafür notwendig sind. Gerne bin ich bereit, diese Diskussion zu begleiten.

Der Gesetzentwurf verzichtet an zentralen Stellen auf bislang geltende tatbestandliche Eingrenzungen. Es ist nicht mehr festzulegen, zu welchem Zweck und auf welcher Rechtsgrundlage eine Datei zu führen ist. Vielmehr sollen nur noch Kategorien der Datenverarbeitung „beschrieben“ werden. Die Polizeibehörden sind dann nicht mehr verpflichtet, konkret festzulegen, welchem Zweck eine solche „Kategorien von innerhalb seines Informationssystems durchgeführten Tätigkeiten der Datenverarbeitungen“ dienen soll. Deshalb sind die tatsächlichen Folgen derzeit kaum abschätzbar.

Zudem begrenzt der Entwurf nicht, die zu unterschiedlichen Zwecken gespeicherten Daten (beliebig) zu verknüpfen (siehe auch unten 1.3.). Die bisherigen Errichtungsanordnungen setzen insoweit Grenzen, als Verknüpfungen grundsätzlich nur innerhalb der jeweiligen (logischen) Dateien zulässig sind.

Der Entwurf verwendet nunmehr der Begriff der „**Kategorien**“ (§ 80 BKAG-E). Dies ist begrifflich gegenüber der in einem Vorentwurf verwendeten Formulierung der „abgrenzbaren Elemente“ des Informationssystems eine Verbesserung. Es ist aber begrifflich **nicht klar**, was darunter zu verstehen ist, wie die Kategorien genau gebildet werden sollen und wie sie voneinander abzugrenzen sind (siehe dazu ausführlich zu den Errichtungsanordnungen unten 3.2.). Zudem ist der Begriff der „Kategorien“ auch sprachlich noch nicht ausgereift. Das Gesetz verwendet ihn in § 80 offenbar in einem anderen Zusammenhang als in § 14 Abs. 1 Nr. 2 BKAG-E.

Die neue Struktur ergibt sich aus folgenden Vorschriften:

| ***Bisheriges Recht:*** | |
|---|---|
| § 34 BKAG | Die Vorschrift wird ersatzlos gestrichen. Aus ihr ergibt sich derzeit, dass für jede Datenverarbeitung mit einer Errichtungsanordnung eine Datei einzurichten ist. Zu Funktion |

| | |
|---|---|
| | und Notwendigkeit der Errichtungsanordnungen ausführlich unten 3. |
| § 11 Absatz 1 Satz 2 BKAG | Danach ist festzulegen, welche Dateien in das Informationssystem einzufügen sind. |
| § 11 Abs. 2 S. 3 BKAG | Anwendung der inhaltlichen Vorgaben des BKAG für alle Verbunddateien durch Verweis auf §§ 7 – 9 BKAG. |
| §§ 8, 9 BKAG | Regelungen zu Dateien der Zentralstelle und sonstigen Dateien. |
| ***Geplante Vorschriften:*** | |
| - | § 34 wird ersatzlos gestrichen |
| § 14 BKAG-E | Enthält Kennzeichnungspflichten, die Rechtsgrundlage und Zweck der Speicherung außer Acht lassen. |
| § 80 | Verzeichnis der Verarbeitungstätigkeiten sieht keine Dateien mehr vor, sondern nur noch<br><br>*„Kategorien von innerhalb seines Informationssystems durchgeführten Tätigkeiten der Datenverarbeitungen, Datenverarbeitungen, einschließlich derer, die es im Rahmen seiner Teilnahme am polizeilichen Informationsverbund nach § 29 Absatz 3 durchführt“*<br><br>und<br><br>*„Die nach § 70 Absatz 1 Satz 2 Nummer 2 des Bundesdatenschutzgesetzes geforderte Darstellung der Zwecke der im Informationssystem des Bundeskriminalamtes und in Erfüllung der Aufgabe nach § 2 Absatz 3 durchgeführten Kategorien an Verarbeitungen richtet sich nach den in den §§ 2 bis 8 genannten Aufgaben des Bundeskriminalamtes.“*<br><br>Für die Länderdaten fehlt anders als bisher jede Vorgabe.“<br><br>[Das Verarbeitungsverzeichnis wird offenbar keine bindende, sondern nur eine beschreibende Wirkung haben.] |

## 1.3. Funktionalität

*Der Gesetzentwurf sollte sich der Frage annehmen, welche Funktionalitäten das Informationssystem und der Informationsverbund enthalten dürfen. Welche Verknüpfungen und welche Methoden zum Datenabgleich sollen erlaubt sein?*

**Änderungsvorschlag BfDI:**

- **auf den zu weitreichenden Begriff *„weiterverarbeiten“* verzichten**
- **Stattdessen §§ 16, 18, 19 als Befugnisse zum *„speichern“* ausgestalten**
- **Regelung zu der Frage, in welchem Umfang Daten dateiübergreifend miteinander abgeglichen werden dürfen** (bislang müssen die durch den Entwurf gestrichenen Errichtungsanordnungen dazu Grenzen setzen, ermöglichen der Polizei aber die nötige Flexibilität).

Das Bundesverfassungsgericht hat auf die verfassungsrechtlichen Risiken der Informationstechnik hingewiesen, wenn diese umfangreiche Verknüpfungen bis hin zur Erstellung von Persönlichkeitsprofilen erlauben (BVerfG NJW 2016, 1781, Abs. Nr. 99).

Diesen verfassungsrechtlichen Risiken begegnet der Entwurf nicht ausreichend. Er führt im Gegenteil dazu, dass sich diese noch verschärfen.

Der Gesetzentwurf wird es umfangreich erlauben, die im Informationssystem und im Informationsverbund gespeicherten Daten abzugleichen und mit technischen Analyseverfahren auszuwerten.

Den **Begriff des Weiterverarbeitens** verwendet der Entwurf überaus zahlreich.

Dieser Begriff ist nach der Gesetzesbegründung als **Auffangbegriff weit zu verstehen**. Demnach fallen darunter die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung von Daten zu verstehen (BR-Drs. 109/17, S. 104).

Konkret verwendet der Entwurf den Begriff des Weiterverarbeitens etwa in den **wichtigen Vorschiften der §§ 18, 19 BKAG**. Diese enthalten die zentralen Vorgaben, welche Daten zu welchem Personenkreis das Bundeskriminalamt im Informationssystem speichern darf. Über den Verweis in § 29 Abs. 5 BKAG-E gelten diese für den bundesweiten Informationsverbund entsprechend. Ebenso bestimmt z.B. **§ 16 Abs. 1 BKAG-E,** das BKA dürfe die gespeicherten Daten zur Erfüllung seiner Aufgaben **„weiterverarbeiten“.** Dort ist die Weiterverarbeitung nur durch den Grundsatz

der hypothetischen Datenneuerhebung (§ 12 BKAG-E) und die Aufgaben des BKA begrenzt.

Ergänzt wird dies durch **§ 13 Abs. 2 BKAG-E**, nach dem das Bundeskriminalamt ausdrücklich zur „polizeilichen Informationsverdichtung“ durch Abklärung von Hinweisen und Spurenansätzen, zur Durchführung von Abgleichen von personenbezogenen Daten und zur Unterstützung bei der Erstellung von strategischen Analysen und Statistiken ermächtigt wird.

Daraus ergibt sich also, dass das Bundeskriminalamt **alle Daten im Informationssystem und im Informationsverbund umfassend verknüpfen, abgleichen und mit technischen Verfahren auswerten und analysieren darf**. Dies korrespondiert mit den weiten und teilweise erweiterten Aufgaben des BKA in § 2 BKAG-E.

Dies ermöglicht Systeme, die nicht mehr personenorientierte Datensätze speichern, sondern unabhängig von Dateigrenzen ereignisorientiert arbeiten: Die Daten zu einer Person werden mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft wird. Die Zahl der Verknüpfungsebenen ist nicht begrenzt. Damit diffundieren die zu einer Person gespeicherten Daten zunehmend.

Zusätzlich erlaubt **§ 16 Abs. 4 BKAG-E** dem BKA, die Daten aus dem Informationssystem mit anderen Daten abzugleichen, auf die es zur Erfüllung seiner Aufgaben „zugreifen“ darf. Dies setzt lediglich einen Grund zu der Annahme voraus, dies sei zur Erfüllung einer Aufgabe erforderlich.

Damit ist nicht nur der interne Abgleich innerhalb der polizeilichen Systeme zulässig. Vielmehr können auch **externe Systeme einbezogen** werden, auf die das Bundeskriminalamt Zugriff hat (z.B. Europol, SIS, VIS ggf. künftige Systeme, die auf europäischer Ebene diskutiert oder geschaffen werden, wie etwa PNR zu Flugpassagieren, Entry-Exit-System, ETIAS).

Im Zusammenhang ist noch zu sehen, dass das Bundeskriminalamt **Datenabgleiche zum Anlass nehmen** kann, **vorhandene Daten zu einer Person zu ergänzen**. Dazu kann es ohne nennenswerte Eingriffsschwelle – unterhalb der Schwelle des Anfangsverdachts – ergänzende Informationen erheben (§§ 9, 10 BKAG-E, siehe dazu unten 5.1).

Ich wende mich nicht pauschal dagegen, in bestimmten Fällen ggf. weitreichende Möglichkeiten des Datenabgleichs vorzusehen. Das Gesetz müsste dann aber **stärker nach dem jeweiligen Anlass und Umfang differenzieren**. Die Gefahr des internationalen Terrorismus und die umfassende Reisetätigkeit der dafür verantwortlichen Personen können umfangreichere Abgleiche notwendig machen. Nach solchen Gefahrenlagen differenziert der Entwurf aber nicht. Vielmehr lässt er weitgehende

Verknüpfungs- und Analysemöglichkeiten für alle in den Datenbanksystemen gespeicherten Personen und Sachverhalte zu.

Im Ergebnis können das Bundeskriminalamt und ggf. die Teilnehmer am Informationsverbund künftig

- sämtliche Daten innerhalb des Informationssystems und des Informationsverbundes prinzipiell miteinander verknüpfen und
- alle Daten miteinander abgleichen.
- Die Methoden des Datenabgleichs sind nicht eingegrenzt.
- Jeder Abgleich kann zu weiteren Datenverknüpfungen führen und damit wiederum die Speicherdauer perpetuieren.

Soweit hier in der Konsequenz die Möglichkeit geschaffen wird, ohne weitere Voraussetzungen und verfahrensmäßige Absicherungen in automatisierten Verfahren **Persönlichkeitsprofíle** zu erstellen, widerspricht dies auch der Vorgabe in Art. 11 der Datenschutzrichtlinie für Polizei und Justiz (Richtlinie EU 2016/680). Danach sind Prozesse einer automatisierten Entscheidungsfindung – einschließlich Profiling –, die eine nachteilige Rechtsfolge für den Betroffenen haben, grundsätzlich verboten. Sie sind nur ausnahmsweise zulässig, wenn das Recht der Union oder der Mitgliedstaaten dies vorsieht und geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet.

### 1.4. Personenkreis und gespeicherte Daten

*Zum **Umfang und Inhalt** der zu speichernden Daten sowie zu den Voraussetzungen der Datenspeicherung sollte der Entwurf dringend angepasst werden.*

**Änderungsvorschlag BfDI:**

- **Engere Fassung der Grunddaten**
- **Engere Fassung der Regelungen zu den Prüffällen (§§ 18 Abs. 3, 19 Abs. 3 BKAG-E**
- **Änderung des § 16 BKAG-E**

**Siehe Änderungsvorschläge zu § 18 BKAG-E im Annex**

#### 1.4.1. Grunddaten (Beschuldigte, Verdächtige)

In § 18 Abs. 1 Nr. 1 BKAG-E erweitert der Entwurf die zu speichernden „Grunddaten“ und erlaubt die Verknüpfung der Daten zu allen gespeicherten Beschuldigten.

**Die Regelung entspricht –** anders als die Begründung dies darstellt **– nicht der bisherigen Regelung in § 8 BKAG.**

Hier geht es – in Abgrenzung zu § 18 Abs. 2 Nr. 2 BKAG – um Fälle, in denen **keine sogenannte Negativprognose** gestellt werden kann. Betroffen sind i.V.m. § 2 Abs. 1 alle Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.

Bislang sind die **„Grunddaten“** in § 8 Abs. 1 BKAG geregelt. Der neue § 18 Abs. 1 BKAG-E enthält denselben Datenkranz, nimmt aber als zusätzlichen Aufzählungspunkt den Begriff „Grunddaten“ auf. Grunddaten sind also nicht mehr die im bisherigen § 8 Abs. 1 genannten Daten, sondern alle darüber hinausgehenden „Grunddaten“. Welche das sind, definiert der Entwurf nicht. Unklar ist insoweit die Formulierung zur Verordnungsermächtigung in § 20 Abs. 1 BKAG-E. Diese kann zwar auf der einen Seite so verstanden werden, sie ermögliche innerhalb der Grunddaten nur, Merkmale zur Identifizierung zu regeln. Sie kann aber auch so verstanden werden, sie ermögliche zwar dem Verordnungsgeber nur, „weitere zur Identifizierung dienende Merkmale“ zu regeln, darüber hinausgehend aber weitere Daten als Grunddaten zu speichern. Für die zweite Variante könnte sprechen, dass es ansonsten zu einer Überschneidung mit der Aufzählung nach Buchstabe b) kommt. Damit bleibt unklar, was unter „Grunddaten“ zu verstehen ist. Daher rege ich an, die Begrenzungen des § 20 Satz 2 Nr. 1 BKAG-E bereits in § 18 Abs. 2 Nr. 1 BKAG-E zu nennen (siehe Vorschlag im Annex).

Wesentlicher Unterschied ist vor allem die bereits oben dargestellte Möglichkeit, die Daten mit anderen im Informationssystem gespeicherten Daten umfassend zu **verknüpfen**. Damit werden die Daten mit den zu anderen Personen, Institutionen, Ereignissen, Objekten oder Sachen verbunden und damit ergänzt oder in einen anderen Zusammenhang gestellt. Denn die neue Vorschrift erlaubt es, die Daten **„weiterzuverarbeiten“** (siehe oben 1.3.; die frühere Fassung lautete „speichern, verändern und nutzen“). Dadurch erhalten die Daten einen erhöhten Aussagegehalt. So lassen sich über längere Zeiträume tiefgreifende Aussagen zu den betroffenen Personen generieren. Nach bisherigem Recht ist die Zuspeicherung weitergehender Informationen nur bei Personen gemäß § 8 Abs. 2 BKAG möglich, der eine sogenannte Negativprognose voraussetzt.

Zudem wird in § 18 BKGE-E auch der Inhalt der zu speichernden „Grunddaten“ erweitert (siehe unten 1.5.).

> *Beispiel: A wird erstmalig gespeichert, weil er bei seiner Rückreise aus den Niederlanden eine geringe Menge Betäubungsmittel mit sich führte (einen Joint). Es handelt sich um eine staatenübergreifende Straftat. Eine sog. Negativprognose ist bei solchen Fällen in der Regel nicht möglich. Bislang können allenfalls die „Grunddaten“ nach dem geltenden § 8 Abs. 1 BKAG gespeichert werden. Künftig können diese Daten mit allen weiteren Daten im Informationssys-*

*tem verknüpft werden. Zum Beispiel mit Verkehrsmitteln, einem größeren Ereigniskomplex, anderen Personen etc. Nach bisherigem Recht wären diese Verknüpfungen nicht zulässig.*

### 1.4.2. Anlasspersonen

Es wurde meine Anregung aufgenommen, den Begriff der „Anlasspersonen“ in § 18 Abs. 1 Nr. 4 BKAG-E jedenfalls enger zu fassen. Diese Personen entsprechen dem Personenkreis gemäß dem geltenden § 8 Abs. 5 BKAG. Diese geltende Vorschrift ist aber nicht hinreichend normenklar und –bestimmt (Graulich in: Sicherheitsrecht des Bundes, 1. Auflage 2015, § 8 BKAG Rn. 52; ebenso Ruthig § 34 BKAG Rn. 4; Arzt NJW 2011, 352, 354 m.w.N.). Zudem enthält sie die vom Bundesverfassungsgericht im Zusammenhang mit § 20g Abs. 1 Nr. 2 BKAG für nicht hinreichend normenklar erachtete Formulierung einer Vorfeldkompetenz (BVerfG NJW 2016, 1781, Abs. 162 ff., 165). Diese wird durch die neue Fassung zumindest auf Fälle beschränkt, in denen die zu begehende Straftat „in naher Zukunft“ erwartet wird. Das ist insoweit eine Verbesserung.

### 1.4.3. Prüffälle

Nach den §§ 18 Abs. 3, 19 Abs. 3 BKAG-E dürfen künftig Daten zu Personen in Vorsorgedateien gespeichert werden, gegen die rechtlich im Zeitpunkt der Speicherung nichts „Handfestes“ vorliegt. Insbesondere muss danach kein Verdacht einer Straftat bestehen. Die Speicherung soll möglich sein, um zu prüfen, ob jemand als Beschuldigter, Verdächtiger, Opfer oder Zeuge „in Betracht kommt“. Die „Anreicherung“ der Daten ist ausdrückliches Ziel.

Es geht also weitgehend um **voraussetzungslose Speicherungen** unterhalb der Schwelle des einfachen Tatverdachts. Diese lehne ich ab. Die Daten werden im Ergebnis zur **Verdachtsgenerierung** gespeichert. Eingriffsschwellen, die dem Eingriffsgewicht Rechnung tragen, wären datenschutzrechtlich der richtige Weg. Eine bloß befristete Speicherung löst das Problem nicht. Die geplanten §§ 14 Abs. 3, 15 Abs. 3 BKAG-E sind also zu weitgehend.

Sie sind auch nicht durchgängig erforderlich. Dies gilt etwa für die Befugnis, Personen für ein Jahr zu speichern, um zu überprüfen, ob sie „Beschuldigte“ sind. Der Beschuldigtenstatus lässt sich schnell durch eine Abfrage des Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStV) klären, ohne die betroffene Person als Prüffall zu speichern.

Zu akzeptieren sind vorübergehende Speicherungen von Personen, wenn das Bundeskriminalamt konkreten Fragen nachgegangen ist. Beispielsweise bei Anfragen eines LKA oder einer internationalen Behörde, die weitere Recherchen des BKA erforderlich machen. Problematisch wären aber die Fälle, in denen zunächst keine wei-

teren Aufgaben zu erfüllen sind und in denen die betroffene Person gespeichert wird, damit sie sich mehr oder weniger zufällig mit weiteren Daten „anreichert“.

Allenfalls denkbar wäre, Beschuldigte oder Verdächtige in den im Entwurf festgelegten Grenzen in einer gesonderten Prüfdatei kurzfristig zu speichern. Ziel muss dann sein, konkret zu untersuchen, ob zusammen mit weiteren Umständen eine Negativprognose gemäß § 18 Abs. 2 Nr. 2 BKAG-E erstellt werden kann oder ob ein Fall des § 18 Abs. 1 Nr. 3 oder 4 BKAG-E vorliegt.

Daher schlage ich Änderungen in §§ 18 Abs. 3, 19 Abs. 3 BKAG-E vor (siehe Annex).

Diese Fallgruppe ist seit langem Gegenstand von Diskussionen zwischen dem Bundeskriminalamt und der Datenschutzaufsicht. Die Speicherung sogenannter Prüffälle ohne Rechtsgrundlage habe ich in der Vergangenheit immer wieder kritisiert (z.B. mein 24. TB Nr. 7.4.4; 22. TB Nr. 4.2.4).

### 1.4.4. „Ermittlungsunterstützende Hinweise“

Die Regelung zu weiteren Hinweise ist zu weitgehend (§ 16 Abs. 6 Nr. 2 BKAG-E). Sie betrifft auch Personen nach § 18 Abs. 1 Nr. 2 BKAG-E, zu denen keine Negativprognose vorliegt. Damit können die ermittlungsunterstützenden Hinweise auch zu Personen gespeichert werden, die lediglich wegen Bagatelldelikten verdächtigt werden (z.B. „Drogenkonsument“). Das **Gesetz bestimmt nicht näher, welcher Art die Hinweise sein dürfen**. Ebenfalls bestimmt es **keine konkreten Voraussetzungen**, unter denen diese Hinweise vergeben werden dürfen. Die Vorschrift ist daher unverhältnismäßig.

Diese Hinweise sollen nach der Gesetzesbegründung schon dann möglich sein, um einen **„polizeilichen Kontext“** zu erläutern (BR-Drs. 109/17, S. 113). Das öffnet die Tür zu Speicherungen ins Blaue hinein, weil sie sich in ihren tatbestandlichen Voraussetzungen immer mehr vom konkreten Ereignis – insbesondere einer Straftat oder einer Gefahrenlage – entfernen. Hinreichend klare tatbestandliche Voraussetzungen fehlen. Dies kann zur **Stigmatisierung** der betroffenen Person führen, wenn sie etwa einer „Szene“ zugeordnet, also quasi in eine **„Schublade“** einsortiert wird.

Die personengebundenen Hinweise nach § 7 Abs. 8 BKAG sind wegen Erforderlichkeit für die Eigensicherung oder die Sicherheit der betroffenen Person zu vergeben. Das sind zumindest klarere tatbestandliche Voraussetzungen. Diese sind aber für die neuen „ermittlungsunterstützenden Hinweise“ gerade nicht vorgesehen.

In der derzeitigen praktischen Diskussion zeigt sich zudem, dass sich Probleme bei den Kriterien für die Fristenvergabe ergeben. So ist unklar, ob und ggf. an welches

Ereignis jeweils ein „ermittlungsunterstützender Hinweis“ geknüpft werden muss. Werden „ermittlungsunterstützende Hinweise“ losgelöst von konkreten Ereignissen vergeben, ergeben sich ebenso losgelöste Löschungsfristen. Das kann zu langen, von konkreten Ereignissen losgelösten Speicherungen führen. Im Angesicht der neuen Mitziehautomatik besteht nun erst recht die Gefahr langfristiger Stigmatisierungen (siehe unten 2.).

## 2. Mitziehautomatik – Abschaffung der bisherigen Aussonderungsprüffristen

*Mit Nachdruck lehne ich die neue „Mitziehautomatik“ bei den Speicherungsfristen ab (§ 77 Abs. 3 BKAG-E). Sie ist ein erheblicher Grundrechtseingriff, für den es keine Rechtfertigung gibt. Er ist unverhältnismäßig und europarechtlich unzulässig.*

**Änderungsvorschlag BfDI:**

- **Beibehaltung des bisherigen § 32 Abs. 5 (statt § 77 Abs. 3 BKAG-E)**

Die geplante Vorschrift in § 77 Abs. 3 BKAG-E ist nicht erforderlich und außerdem unverhältnismäßig. Sie wird in vielen Fällen zu zeitlich praktisch unbegrenzten Speicherungen führen. Siehe dazu das bereits mit Schreiben vom 22. Februar übersandte Beispiel.

Tatbestandlich knüpft § 77 Abs. 3 BKAG-E an „alle zu einer Person gespeicherten Daten“ an. Bei jeder neuen Speicherung werden also alle mit einer Person verknüpften Daten weitergespeichert. Dies gilt unabhängig von der Personenrolle, vom Anlass und vom Zweck der neuen Speicherung. Jede neue Anzeige – auch eines Bagatelldelikts – zieht alle alten Speicherungen mit. Gerade dann, wenn Speicherungen nur auf einem leichten „Restverdacht“ beruhen, kann dies erhebliche Grundrechtseingriffe zur Folge haben.

### 2.1. Inhalt der Regelung

*Jede neue Speicherung zieht alle alten Speicherungen mit.*

***Was sind Aussonderungsprüffristen?*** *Das Gesetz sieht keine Löschungsfristen für gespeicherte Daten vor. Es bestimmt sog. Aussonderungsprüffristen. Nach diesen Fristen muss geprüft werden, ob die jeweiligen gespeicherten Daten noch zulässig gespeichert und weiterhin erforderlich sind. Nach der neuen Regelung ist nur die neueste Speicherung zu prüfen, die alten Daten werden ungeprüft weiter gespeichert.*

Nach § 77 Abs. 3 BKAG-E sollen die Aussonderungsprüffristen *„für alle zu einer Person gespeicherten Daten einheitlich“* an dem Tag beginnen, an dem „*die betroffene Person letztmalig zur Speicherung nach diesem Gesetz Anlass gegeben hat“*.

**„Anlass zur Speicherung nach diesem Gesetz“**

Der in § 77 Abs. 3 BKAG-E genannte „Anlass“ bezieht sich nicht auf eine Straftat oder eine Gefahr, für die die betroffene Person verantwortlich ist, sondern auf einen Anlass, den diese Person „zur Speicherung nach diesem Gesetz“ gegeben hat. Einen solchen Anlass gibt die Person auch, wenn sie als **Kontaktperson, Zeuge, Hinweisgeber etc.** gemäß § 19 BKAG-E in Erscheinung tritt. Darüber hinaus gibt die Person einen Anlass, wenn sie nur in den **Verdacht einer länderübergreifenden oder internationalen Bagatellstraftat** gerät. Der **„Anlass“** bezieht sich zudem nur auf die aktuell gespeicherten Daten, ist aber **von den weiteren „mitgezogenen“ Daten gerade unabhängig**. In der Ressortberatung ist die Formulierung etwas enger gefasst worden. Dies beseitigt aber nicht die immer noch weitreichenden Folgen.

**„Alle zu der Person gespeicherten Daten“**

Die Formulierung „alle zu der Person gespeicherten Daten“ ist der Kern der sog. **„Mitziehautomatik“**. Ausgelöst wird sie, wenn die Polizeibehörde ein weiteres Datum hinzuspeichert (z.B. die betroffene Person wird als Zeuge oder als Verdächtiger gespeichert). Dies zieht dann alle älteren Speicherungen mit, für die dann die neue Aussonderungsprüffrist gilt.

> *Beispiel: A wurde vor acht Jahren der Nötigung und des Landfriedensbruchs verdächtigt. Das Verfahren wurde eingestellt, weil ihm die Tat nicht nachgewiesen werden konnte. Es wurde gleichwohl im Informationsverbund gespeichert (vgl. § 18 Abs. 5 BKAG-E, dazu unten 4.). A fährt nun gemeinsam mit B und C als Mitfahrer in einem Auto auf der Rückreise aus den Niederlanden nach Deutschland. An der Grenze werden sie kontrolliert. Im Kofferraum des Fahrzeugs ist in einer Tasche ein „Joint“ versteckt. Es ist unklar, welcher Person die Tasche zuzuordnen ist. A wird im Informationsverbund erneut gespeichert. Es wird eine Aussonderungsprüffrist von 10 Jahren festgelegt (§ 77 Abs. 1 S. 2 BKAG-E). Die alte acht Jahre alte Speicherung wird pauschal „mitgezogen“, da die neue Prüffrist für „alle zur Person gespeicherten Daten“ gilt. Es muss also nicht einmal mehr geprüft werden, ob die älteren Daten noch erforderlich sind. Die alte Speicherung erhält damit ungeprüft eine Aussonderungsprüffrist von 18 Jahren, obwohl sie nur auf einer Verdachtslage beruht und das Verfahren eingestellt wurde.*

## 2.2. Neue Datenbanksysteme als geänderter Kontext

Der Begriff „alle zu der Person gespeicherten Daten“ erhält seine besondere Eingriffstiefe auch durch die weiteren im Entwurf vorgesehenen Änderungen. Die grundrechtliche Eingriffswirkung ist im neuen Zusammenhang zu sehen, weil die **IT-Strukturen sich erheblich ändern**. Wie oben dargelegt, grenzen die neuen Daten-

banksysteme die darin gespeicherten Daten nicht mehr nach Dateien ab und sie verknüpfen die in ihnen gespeicherten Daten umfassend miteinander.

Rechtlich stellt sich deshalb die Frage:

> **Welche der mit der gespeicherten Person verknüpften Daten gehören zu „allen mit einer Person gespeicherten Daten“?**

Der Entwurf ist zwar in der Ressortabstimmung nach meiner Kritik geändert worden, indem auf den besagten „Anlass“ abgestellt wurde, statt allgemein alle Speicherungen einzubeziehen. Das ändert aber nichts daran, dass alle Daten im Informationssystem und im Informationsverbund künftig umfassend miteinander verknüpft werden dürfen. Deshalb bleiben durch die „Mitziehklausel“ auch alle verknüpften Daten erhalten.

Der Anlass für eine neue Speicherung kann insofern auch gerade durch Datenabgleiche und Verknüpfungen entstehen. Dies etwa dann, wenn sich aus den Abgleichen ergibt, dass mit unterschiedlichen Ereignissen in Zusammenhang stehende Personen miteinander in Kontakt stehen und deshalb entweder jeweils dem anderen Ereignis zugeordnet werden oder als Kontaktpersonen gespeichert werden. In solchen Fällen kann die Zuspeicherung und damit auch die Verlängerung der Aussonderungsprüffrist für alle (!) Daten sogar ohne Kenntnis der Betroffenen geschehen. Daran ändert es auch nichts, dass während der Ressortberatung der Hinweis aus der Begründung zu § 77 Abs. 3 BKAG-E gestrichen wurde, wonach hinzugespeicherte Daten dazu beitragen können, die betroffene Person in einen anderen Kontext des Informationssystems zu überführen.

Weder der Gesetzeswortlaut noch die Begründung bieten **ausreichend sachhaltige Kriterien**, welche Daten der Person in einem derartigen Speicherkonzept noch **zurechenbar** sind und welche nicht.

### 2.3. Keine Orientierung an der Erforderlichkeit

Das Bundeskriminalamt hat schon nach geltendem Recht die Möglichkeit, die Daten länger aufzubewahren, sofern ein sachlicher Grund die längere Speicherung rechtfertigt. Die geplante Regelung ändert dies nur für die Fälle, in denen ein solcher sachlicher Grund gerade nicht vorliegt. Das ist unverhältnismäßig.

> **Die neue Regelung orientiert sich nicht daran, was für die Aufgabenerfüllung erforderlich ist und aus welchen Gründen die älteren Daten noch benötigt werden.**

Es ist insgesamt nicht nachvollziehbar, pauschal ältere Daten aufzubewahren. Wenn eine Polizeibehörde in einem aktuellen Betrugsfall ermittelt, kann sie mit einem dreißig Jahre alten Eintrag in der Regel nur wenig anfangen. Welche aktuellen Erkenntnisse will sie daraus gewinnen? Wie soll der alte Eintrag dazu beitragen, im aktuellen Fall nachzuweisen, dass dieser Mensch einem anderen Menschen aktuell falsche Tatsachen vorgespiegelt hat, um sich aktuell zu bereichern? Dem Gesetzgeber obliegen eine Beobachtungspflicht und eine Darlegungslast. Er muss jetzt und heute aktuell nachweisen, wozu die Polizei die Daten konkret benötigt. Das Bundeskriminalamt hat den Nachweis zu erbringen, dass es für das Informationssystem und den Informationsverbund gerade solche Daten benötigt, die nicht mehr aktuell sind.

### 2.4. Grundlage: Verdachtsspeicherungen

Die Behörden speichern in polizeilichen Informationssystemen Daten auch über solche Personen, die bislang **nur unter einem Verdacht** standen, aber nicht verurteilt wurden.

> Dies betrifft deshalb auch einen Anteil von Personen, die **tatsächlich keine Straftaten begangen** haben.

Deshalb bilden die Dateien nicht nur die „kriminelle Karriere“ ab, sondern ebenso die nur *vermeintliche* „kriminelle Karriere“. Diese Daten sind Grundlage und „Anknüpfungspunkt“ neuer Ermittlungen.

> Wer „polizeibekannt“ ist, muss eher damit rechnen, Gegenstand polizeilicher Ermittlungen zu werden. Dies stellt für die betroffene Person eine **potentiell erhebliche Belastung** dar.

Bislang mildern diese Belastung an der jeweils vorgeworfenen Tat orientierte Aussonderungsprüffristen ab. Ereignisse, die längere Zeit – also in der Regel mehr als 10 Jahre zurückliegen – werden im Normalfall gelöscht. Damit werden den Betroffenen nach der bisherigen Regelung **ältere Verdachtsmomente** nicht mehr entgegen gehalten. Das wird sich künftig ändern.

### 2.5. Unzutreffende Gesetzesbegründung

Die Gesetzesbegründung ist irreführend. Sie gibt vor, einen Gleichklang mit der Strafprozessordnung herbeizuführen. Sie erwähnt aber nicht, dass nach der Strafprozessordnung keine Dateien der Strafverfolgungsvorsorge geführt werden.

> **Der Gesetzentwurf nimmt damit eine gesetzliche Regelung als Vorbild und Anlass, die sich in der Praxis nicht bewährt hat und somit leerläuft**.

Der Hinweis auf die bestehende Regelung in § 489 Abs. 6 StPO ist nicht sachhaltig. Die Vorschrift findet in der Praxis in vergleichbarem Zusammenhang keine Anwendung. Hinsichtlich der Vorsorgespeicherungen findet sich in der StPO allein in § 484 Abs. 2 eine Regelung. Hierzu haben aber weder die Länder noch der Bund bislang eine nach § 484 Abs. 3 StPO notwendige Rechtsverordnung erlassen. Wie daraus zu schließen ist, wird kein Bedarf für Speicherungen nach dieser Vorschrift gesehen (vgl. Schmitt in: Meyer-Goßner/Schmitt, StPO, 58. Auflage 2015, § 484 Rn. 4). Das letzte Schreiben des BMJV in meinen Akten zu dieser Frage stammt aus dem Jahre 2002. Darin teilt es in wenigen Zeilen den fehlenden Bedarf mit. Deshalb läuft § 489 Abs. 6 StPO für den Bereich der Strafverfolgungsvorsorge praktisch leer.

Die Dateien der Staatsanwaltschaften betreffen in der Praxis einen völlig anderen Kontext. Es handelt sich in der Regel um Dateien der Vorgangsverwaltung, die eine Übersicht über die geführten Verfahren ermöglichen. Es handelt sich hingegen nicht um große präventive Mischdatenbestände. Die nach der StPO geführten Datenbanken sind nicht mit den Polizeidatenbanken vergleichbar. Die Polizeibehörden führen – abgesehen von Dateien nach § 483 Abs. 1 StPO – keine Dateien nach der Strafprozessordnung. Denn die Kollisionsregeln führen dazu, dass in der Praxis stets das Polizeirecht eingreift (§§ 483 Abs. 3, 484 Abs. 4, 485 S. 3 StPO). Die Staatsanwaltschaften sind bildlich gesprochen „Herrin des Verfahrens“, nicht jedoch „Herrin der Daten(banken)“.

Den Änderungsbedarf für das BKAG nur mit dem Hinweis auf eine leerlaufende und praktisch wenig bedeutsame Vorschrift zu begründen, ist nicht überzeugend.

Die Abbildung einer „kriminellen Historie“ kann ebenfalls kein tauglicher Zweck sein. Polizeilichen Datenbanken enthalten in erster Linie Verdachtsspeicherungen, keine Verurteilungen. Für letztere existiert das Bundeszentralregister.

### 2.6. Verstoß gegen Art. 7 Abs. 2 JI-Richtlinie

Gemäß Art. 7 Abs. 2 der JI-Richtlinie muss der Gesetzgeber alle angemessenen Maßnahmen vorsehen, damit personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht übermittelt oder bereitgestellt werden. Die Daten aus dem Informationssystem können übermittelt werden. Die Daten, die das Bundeskriminalamt in den Informationsverbund speichert, stehen zur Übermittlung im automatisierten Abrufverfahren bereit. Es handelt sich insofern um eine Übermittlung bzw. Bereitstellung im Sinne des Art. 7 Abs. 2 der JI-Richtlinie. Weil aber pauschal auch solche Daten übermittelt bzw. bereitgestellt werden dürfen, die nur gemäß § 77 Abs. 3 BKAG-E „mitgezogen“ wurden, sind dies Daten, die nicht mehr geprüft und damit nicht mehr aktuell i.S.d. Art. 7 Abs. 2 der JI-Richtlinie sind.

**§ 77 Abs. 3 BKAG-E verstößt damit gegen Art. 7 Abs. 2 der JI-Richtlinie.**

### 2.7. Fazit

Die vorgesehene Regelung in § 77 Abs. 3 ist nicht erforderlich und unverhältnismäßig. Sie verstößt gegen europäisches Recht.

## 3. Verfahrenssicherungen, insb. Abschaffung der Errichtungsanordnungen

### 3.1. Errichtungsanordnungen

*Errichtungsanordnungen dienen als wesentlicher Maßstab, um zu beurteilen, welchem Zweck gespeicherte Daten im Einzelnen dienen sollen und ob sie dafür erforderlich sind. Damit sind sie gleichzeitig wesentliche Grundlage für die Selbstkontrolle der Polizeibehörden und für die Datenschutzkontrolle (bisheriger § 34 BKAG, der durch den Gesetzesentwurf gestrichen wird).*

**Änderungsvorschlag BfDI:**

**Beibehaltung des § 34**
**Hilfsweise: Änderungsvorschlag zu § 80 BKAG-E, äußerst hilfsweise zu § 14 BKAG-E im Annex**

Durch die neue geplante Struktur und durch den Wegfall des bisherigen § 34 BKAG werden die gespeicherten Daten nicht mehr einzelnen Dateien zugeordnet. Damit enthalten die zusammengefassten Daten keine spezifischen Vorgaben mehr zum Zweck der jeweiligen Speicherung, zu Aussonderungsprüffristen und den jeweils im Zusammenhang gespeicherten Daten. Dies ist jedoch weiterhin verfassungsrechtlich notwendig (siehe oben 1.1.).

Speichert eine Polizeibehörde personenbezogene Daten, muss sie im Einzelfall prüfen, dokumentieren und angeben können, zu welchen Zwecken sie dies tut und aus welchem Grund dies geeignet und erforderlich ist. **Bislang** wird insbesondere der Zweck der in einer Datei gespeicherten Daten spezifisch festgelegt. In der **Errichtungsanordnung** werden diese abstrakt festgelegt und können zuvor im Anhörungsverfahren diskutiert werden. Dies dient als **Maßstab für die Datenschutzkontrolle** und für die **Selbstkontrolle der Polizeibehörden**. All dies fällt künftig weg.

Verfassungsrechtlich ist entscheidend, dass der Verwendungszusammenhang jedes gespeicherten Datums spezifisch festgelegt wird. Dies stellt bislang § 34 BKAG sicher. Die Vorschrift ist seinerzeit eingefügt worden, um die verfahrensrechtlichen und organisatorischen Vorgaben des Bundesverfassungsgerichts aus dem Volkszählungsurteil umzusetzen (BT-Drs. 13/1550, S. 19; Kugelmann, BKAG, 1. Aufl. 2014, § 34 Rn. 1):

> *„Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.“ BVerfGE 65, 1 (45)*

Die verfassungsrechtlich begründeten Vorgaben des § 34 BKAG fallen künftig weg. Sein Regelungsinhalt wird nicht anderweitig ersetzt oder kompensiert. Es fehlt also eine Regelung, die spezifisch für jedes Datum den Zweck der Speicherung festlegt (nicht nur der Erhebung). Orientiert an diesem jeweils spezifisch festgelegten Zweck – und nicht nur abstrakt für das gesamte BKA oder den gesamten Informationsverbund (!) – ist darüber hinaus festzulegen:

- Der Personenkreis, über den Daten gespeichert werden,
- die Art der zu speichernden personenbezogenen Daten,
- die Arten der personenbezogenen Daten, die der Erschließung der Datei dienen – einschließlich Analyse – und Verknüpfungsmöglichkeiten,
- die Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden,
- Prüffristen und Speicherungsdauer.

Das Volkszählungsurteil ist immer noch gültig. Es verbietet insoweit, alle Daten über einen Kamm zu scheren. Genau dies aber sieht der Entwurf vor, sowohl für das Informationssystem des BKA als auch für den bundesweiten Informationsverbund.

### 3.2. Zugriffsberechtigungen

Insbesondere die in der letzten Entwurfsfassung ergänzten §§ 14, 15 BKAG-E zur Kennzeichnung von Daten und zur Regelung der Zugriffsberechtigungen kompensieren das Fehlen der Errichtungsanordnungen nicht. So ist nach § 14 BKAG-E nicht zu kennzeichnen, welchem Zweck die Speicherung dient.

> Vor allem **fehlt** es **an hinreichend klaren Kriterien**, nach denen die Zugriffsberechtigungen vergeben werden. Diese lassen sich jederzeit nahezu beliebig ändern.

§ 15 BKAG-E enthält in der neuen Entwurfsfassung zwar Regelungen dazu, wie Zugriffsberechtigungen vergeben werden können. Diese orientieren sich aber nur an

den Vorgaben des § 12 BKAG und daran, dass die jeweiligen Sachbearbeiter nur innerhalb der „dienstlichen Pflichten“ zugreifen dürfen.

Nicht mehr entscheidend sollen aber die Zwecke der jeweils gespeicherten Daten sein. In § 13 Absatz 3 fehlt eine Bezugnahme darauf. Hierfür müsste geklärt sein, welche Zweckbindung gilt und nach welchen Kriterien die Berechtigungen vergeben werden. Künftig finden sich keinerlei Anhaltspunkte mehr zu den spezifischen Zwecken der jeweiligen Datei bzw. „Kategorie von Daten“, wie dies derzeit noch wegen der Errichtungsanordnungen der Fall ist.

Die gesetzliche Regelung sollte also festlegen:

- In einem ersten Schritt ist für das jeweilige Datum oder für „eine Kategorie von Daten“ bzw. für eine Datei ein spezifischer Verarbeitungszweck vorzusehen.
- Erst dann kann geklärt werden, welche Personen für diesen spezifischen Zweck Zugriff auf das Datum, die Datei oder die „Kategorie von Daten“ benötigen.

### 3.3. Protokollierung und Datensicherheit

Ich begrüße die Festlegung in § 81 Abs. 1 BKAG-E, nach der die Protokolldaten der BfDI in elektronisch auswertbarer Form zur Verfügung gestellt werden müssen.

Ich weise im Hinblick auf den Parallelentwurf zum Datenschutzanpassungsgesetz auf Folgendes hin (BR-Drs. 110/17): Protokollierung ist eine Verfahrenssicherung, die den Grundrechtseingriff der Datenverarbeitung abmildern soll. Sie darf deshalb nicht ihrerseits zu zusätzlichen Grundrechtseingriffen führen. Dies schließt die Verwertung für die Strafverfolgung aus.

> *Beispiel: Eine Person ist rechtswidrig zur Beobachtung ausgeschrieben. Dann wird ihr Datensatz nach einem aufhebenden Gerichtsbeschluss gelöscht. Aus den Protokolldaten ergeben sich dann aber weiter die vollen Daten und zusätzlich ggf. wann der Betroffene an welchem Ort angetroffen wurde. Problematisch ist weiterhin, dass die „Eigenkontrolle“ auch die Verhaltens- und Leistungskontrolle innerhalb der Polizeibehörden umfasst.*

Hinsichtlich der Datensicherheit berücksichtigt der Entwurf, dass hinsichtlich der Datensicherheit auf den Stand der Technik abgestellt werden muss.

## 4. Unschuldsvermutung in polizeilichen Dateien

*Ein Kernanliegen des Datenschutzes ist, die Unschuldsvermutung in polizeilichen Dateien zur Geltung zu bringen. Jeder muss die Chance haben, aus einem Ermittlungsverfahren am Ende als Unschuldiger herauszukommen, wenn er keine Straftat*

*begangen hat. Das muss dann auch in Polizeidateien wirken. Datenschutz ist rechtsstaatlicher Beschuldigtenschutz. Jeder Mensch kann in die Situation kommen, diesen zu benötigen.*

**Änderungsvorschlag BfDI:**

**Änderung und Ergänzung des § 18 Abs. 5 BKAG-E, siehe Annex**

Ein Kernanliegen des Datenschutzes ist es, die Unschuldsvermutung auch in polizeilichen Dateien zur Geltung zu bringen. Datenschutz ist rechtsstaatlicher Beschuldigtenschutz. Jeder muss die Chance haben, aus einem Ermittlungsverfahren als Unschuldiger herauszukommen, wenn er die vorgeworfene Straftat nicht begangen hat. Bislang müssen Daten erst gelöscht werden, wenn die Unschuld erwiesen ist. Anderenfalls bedeutet das für die Betroffenen: Die Daten bleiben weiter gespeichert. *Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um* und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Bundesverfassungsgerichts. Das Gesetz sollte daher die Pflicht der Behörden klarstellen, bei der Negativprognose den Grad des Tatverdachts zu berücksichtigen. Jeder gerichtliche Freispruch sollte zur Löschung führen. Einen „Freispruch zweiter Klasse“ darf es bei der Polizei nicht mehr geben.

Es handelt sich insoweit nicht nur um eine allgemeine datenschutzpolitische Forderung. Vielmehr liegt sie auch in der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs für Menschenrechte begründet.

### 4.1 Vorgaben des BVerfG und des EGMR

Das **Bundesverfassungsgericht** hat entschieden, „nach einem Freispruch bedarf es für die Annahme eines fortbestehenden Tatverdachts aber besonderer, von der speichernden Polizeibehörde darzulegender Anhaltspunkte, die sich insbesondere aus den Gründen des freisprechenden strafgerichtlichen Urteils selbst ergeben können.“ (BVerfG NJW 2002, 3231). Damit dürfen Polizeibehörden personenbezogene Daten nach einem **Freispruch** nur in **Ausnahmefällen** zur Gefahrenvorsorge speichern. Die bisherige Regelung kehrt aber den Tenor dieser Entscheidung des Bundesverfassungsgerichts in ihr Gegenteil um (Petri in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Auflage 2012, Kap. G Rn. 403). Entsprechendes gilt für Verfahrenseinstellungen.

**Der Europäische Gerichtshof für Menschenrechte legt sogar noch strengere Maßstäbe an.** Nach dessen neueren Entscheidungen darf insbesondere in Urteilen überhaupt nicht zwischen Freisprüchen „erster“ und „zweiter Klasse“ unterschieden werden. „Tatsächlich gilt die Unschuldsvermutung nicht nur während eines laufenden Strafverfahrens. Damit sie praktisch und wirksam ist, dürfen Behörden und Gerichte im Fall der Einstellung eines Strafverfahrens oder des Freispruchs in den Gründen

ihrer Entscheidung keinen Schuldvorwurf gegenüber dem Betroffenen äußern.“ (EGMR, Urteil vom 15.01.2015 - EGMR Aktenzeichen 48144/09, ‚BeckRS 2016, 09502). Wenn eine Person nicht verurteilt wurde, ist dies auch bei der Speicherung in polizeilichen Dateien besonders zu berücksichtigen (so bereits EGMR NJOZ 2010, 696 – Marper).

Der **verbleibende Tatverdacht** kann **verschieden stark ausgeprägt** sein, was nicht zuletzt die im Bereich der StPO vorgesehenen und anerkannten verschiedenen Arten des Tatverdachts belegen. Insbesondere muss die speichernde Stelle deshalb die Gründe für den fortbestehenden Tatverdacht und für dessen Gewicht bzw. den verbleibenden Verdachtsgrad besonders darlegen. Wie Ergebnisse datenschutzrechtlicher Kontrollen gezeigt haben, liegen oftmals nicht einmal Rückmeldungen zum Verfahrensausgang vor. Unabhängig davon haben sich – unabhängig von der Frage des bestehenden Restverdachts – teilweise erhebliche Dokumentationsdefizite hinsichtlich der Negativprognose gezeigt (so die Ergebnisse der Kontrolle der FDR in mehreren Bundesländern und im Bereich der Zollfahndung). Bei datenschutzrechtlichen Kontrollen habe ich trotz der Rechtsprechung des BVerfG und des EGMR – abgesehen von gerichtlich geprüften Fällen der DNA-Analyse – noch keinen Fall gefunden, in dem die datenverarbeitende Stelle sich mit dieser Frage befasst und dies dokumentiert hatte.

Auch im Falle einer Einstellung nach §§ 153, 153a StPO ist zu berücksichtigen, dass das Gewicht der Straftat ein anderes ist als bei einer Verurteilung. § 153 StPO verlangt nicht, alle entlastenden Umstände auszuermitteln. Ebenfalls nicht erforderlich ist ein hinreichender Tatverdacht, also die überwiegende Wahrscheinlichkeit einer Verurteilung (Peters in: Münchener Kommentar zur StPO, 1. Auflage 2016, § 153 Rn. 17). Ähnliches gilt für § 153a StPO, der allerdings einen stärkeren Verdachtsgrad voraussetzt. In all diesen Fällen kann also nicht von vornherein von einem ausreichenden Verdachtsgrad ausgegangen werden, der die weitere Speicherung zulassen würde.

Soweit in der Ressortberatung auf die mögliche Wiederaufnahme eines abgeschlossenen Verfahrens zuungunsten des Verurteilten gemäß § 362 StPO hingewiesen wurde, verfängt dies ebenfalls nicht. Dieser Hinweis vermischt die verschiedenen polizeiinternen Zwecke der Speicherung, die nach Aufgabenerfüllung, Vorsorge und Dokumentation zu differenzieren sind. Für die Wiederaufnahme genügt es, die Verfahrensakte aufzubewahren. Abgesehen davon ist die Wiederaufnahme der Ausnahmefall. Die Annahme, für den Fall einer Wiederaufnahme seien Daten stets in einer Vorsorgedatei zu speichern, findet im geltenden Recht keine Stütze und wäre auch mit der Funktion des Strafklageverbrauchs und dem daraus resultierenden Ausnahmecharakter der Wiederaufnahme nicht zu vereinbaren.

### 4.2. Richtlinienvorgabe

Artikel 6 Buchst. a der JI-Richtlinie fordert eine Differenzierung zwischen Verdächtigen, Verurteilten, Opfern und anderen Parteien. Dem bisherigen Recht fehlt ebenso wie dem Gesetzentwurf eine Unterscheidung zwischen Verurteilten und Verdächtigten Personen. Zwar erwähnt der neue § 18 Abs. 1 BKAG-E in Nr. 1 und 2 beide Personengruppen. Er knüpft daran aber dieselben Speichervoraussetzungen, differenziert also nur begrifflich zwischen beiden Personengruppen, nicht hinsichtlich der Voraussetzungen der Speicherungen bzw. der Rechtsfolgen. Das verletzt die Richtlinienvorgabe.

Artikel 6 Buchst. a der JI-Richtlinie lautet:

> *„Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter:*
> *a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden,*
> *b) verurteilte Straftäter,*
> *c) Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und*
> *d) andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a und b genannten Personen in Kontakt oder in Verbindung stehen“*

### 4.3. Mögliche Regelung

Ich schlage deshalb vor, die zu enge Regelung des bisherigen § 8 Abs. 3 BKAG zu ändern. Hierzu verweise ich auf meinen Vorschlag zu § 18 Abs. 5 BKAG-E im Annex zu dieser Stellungnahme. Nach diesem Vorschlag wäre auch weiterhin eine Regelung vorhanden, nach der auch solche Personen gespeichert werden, bei denen das Verfahren mit einem „Restverdacht“ eingestellt wurde. Dies bedürfte aber einer eingehenden Prüfung des Einzelfalls.

## 5. Datenerhebungen in der Zentralstellenfunktion als weitere Befugnis des BKA

*Das Urteil des Bundesverfassungsgerichts zwingt dazu, die Vorfeldbefugnisse zur Terrorismusbekämpfung zu überarbeiten. Daneben geraten allerdings leicht andere mit dem Entwurf verfolgten Befugnisse aus dem Blick. Die Regelungen in §§ 9 Abs. 1, 10 Abs. 1 BKAG-E ermöglichen es, ohne einen Anfangsverdacht Daten zu einer Person zu erheben. Voraussetzung ist lediglich, dass diese Daten „zur Ergänzung vorhandener Sachverhalte" oder sonst „zu Zwecken der Auswertung" erhoben werden und dies für die „Zentralstellenfunktion" des BKA erforderlich ist. Dies entspricht teilweise dem geltenden Recht (§ 7 Abs. 2 BKAG). Die Befugnis bringt erhebliche verfassungsrechtliche Risiken mit sich.*

Die in §§ 9 Abs. 1, 10 Abs. 1 BKAG-E enthaltenen Nachfolgeregelungen des § 7 Absätze 2 bis 7 BKAG sehe ich als zu weitgehend an. Der Wortlaut dieser Vorschriften enthält praktisch nur eine tatbestandliche Eingrenzung, nämlich den Verweis auf die Aufgabe als Zentralstelle. Der Begriff der Zentralstellenaufgabe ist weit. Deshalb begrenzen diese Vorschriften kaum, welche Daten das Bundeskriminalamt erheben darf. Damit kann dieses unabhängig von den Voraussetzungen der §§ 161, 163 StPO Ermittlungen durchführen und Daten zu Personen erheben, gegen die aktuell kein Strafverfahren geführt wird. Es kann **ohne ausreichende tatbestandliche Begrenzungen** beliebig Daten zu Personen „anreichern", die nur aus Vorsorgegründen gespeichert sind. Dies umfasst im Zusammenwirken mit den übrigen Vorschriften auch Personen, bei denen die gegen sie geführten Strafverfahren eingestellt oder sie freigesprochen worden sind. Eine solche Regelung wirft aus meiner Sicht erhebliche verfassungsrechtliche Fragen auf (zu Recht kritisch etwa Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Mannheim 2009, S. 23).

Wer also einmal wegen eines Verdachts im Informationssystem oder im Informationsverbund gespeichert ist, lebt mit dem Risiko, dass ohne einen strafrechtlichen Anfangsverdacht weitere Daten zu ihm „hinzugespeichert" werden. Diese Daten können ggf. „Anlass" für die weitere Speicherung aller Daten sein (Mitziehautomatik, siehe oben 2.).

Das Bundeskriminalamt kann die Daten ohne Wissen des Betroffenen erheben, wenn sonst die Erfüllung der dem Bundeskriminalamt obliegenden Aufgaben nach Satz 1 gefährdet oder erheblich erschwert würde (§ 9 Abs. 2 S. 3 BKAG-E). Dies bezieht sich aber nicht auf die Abwehr einer konkreten Gefahr, sondern auf die Zentralstellenaufgabe, die in der bloßen routinemäßigen Anreicherung von Daten zu einer zu Vorsorgezwecken gespeicherten Person bestehen kann. Die Vorschrift ist also mitnichten mit den Generalklauseln der Landespolizeigesetze zu vergleichen, bei denen es um die Abwehr konkreter Gefahren geht. Es handelt sich hier um eine

kaum begrenzte heimliche Vorfeldbefugnis, die nicht den Vorgaben des aktuellen Urteils des Bundesverfassungsgerichts entspricht.

Möglich sind künftig unter denselben weiten Voraussetzungen Datenerhebungen bei ausländischen privaten Stellen. Dazu verweist § 9 Abs. 1 S. 2 Nr. 3 BKAG-E auf den künftigen § 81 BDSG. Dieser Verweis ist aber nicht passend, weil § 81 BDSG die Voraussetzungen einer Datenübermittlung regelt, nicht die einer Datenerhebung. Die Vorschrift arbeitet also mit einer Verweistechnik, die eine gedankliche Umkehrung erforderlich macht und ihrerseits auf weitere Verweise verweist (Mehrfachverweistechnik). Das ist nicht hinreichend normenklar.

§ 10 Abs. 2 BKAG-E erlaubt es nach seinem Wortlaut, permanent zu allen gespeicherten Personen die IP-Adressen abzurufen und fortlaufend für die gesamte Speicherdauer hinzu zu speichern. Dies betrifft alle Daten und alle Personen, die im Informationssystem und im Informationsverbund gespeichert sind. Das Bundesverfassungsgericht hat entschieden, dass die Zuordnung dynamischer IP-Adressen ein Eingriff in Artikel 10 GG ist. Insoweit bedarf es einer hinreichend klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen der Eingriff erlaubt werden soll (BVerfG NJW 2012, 1419, 1428).

Eine Benachrichtigungspflicht für heimliche Erhebungen nach § 9 BKAG-E fehlt gänzlich.

Selbst wenn das BKA von diesen Vorschriften in der Praxis nur restriktiven Gebrauch machen würde, würde dies die fehlenden gesetzlichen Begrenzungen nicht kompensieren. Für ausreichende tatbestandliche Grenzen zu sorgen, ist allein Aufgabe des Gesetzgebers.

## 6. Datenschutzkontrolle

*Für die Datenschutzkontrolle bietet der Entwurf aufgrund der Vorgaben des Bundesverfassungsgerichts und der Richtlinie durchaus Verbesserungen, die grundsätzlich zu begrüßen sind, in der Ausgestaltung aber ergänzt werden sollten.*

Dies gilt etwa für die in § 69 Abs. 2 BKAG-E gegen Ende der Ressortabstimmung eingefügte Anordnungsbefugnis der BfDI. Diese ist aber auf erhebliche Datenschutzverstöße beschränkt und enthält z.B. nicht die ausdrückliche Klarstellung, ggf. auf die Löschung einzelner Daten hinwirken zu können.

## 7. Fazit

Im Ergebnis erhalten die Polizeibehörden in Bund und Ländern erheblich erweiterte Befugnisse, personenbezogene Daten in Datenbanksystemen zu verarbeiten. Wesentliche Verfahrenssicherungen fallen weg. Weder einer Modernisierung der polizeilichen IT noch des Polizeirechts stelle ich mich entgegen. Dafür ist der vorgelegte Entwurf aber nicht notwendig. Zudem geht er in vielen Punkten zu weit. Er sollte deshalb nachgebessert werden.

Andrea Voßhoff

**Annex**

**zur Orientierungshilfe der BfDI zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes**

# Änderungsvorschläge

| Text des Entwurfs: | Änderungsvorschlag BfDI: | Vorgeschlagen wird eine Änderung des § 80 BKAG-E. Sofern dem nicht gefolgt wird, ist mindestens die nebenstehende Änderung notwendig. |
|---|---|---|
| § 14 **Kennzeichnung**<br><br>(1) Bei der Speicherung im Informationssystem sind personenbezogene Daten wie folgt zu kennzeichnen:<br>1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,<br>2. Angabe der Kategorie nach den §§ 18 und 19 bei Personen, zu denen Grunddaten angelegt wurden,<br>3. Angabe der<br>a) Rechtsgüter, deren Schutz die Erhebung dient oder<br>b) Straftaten, deren Verfolgung oder Verhütung die Erhebung dient,<br>4. Angabe der Stelle, die sie erhoben hat, sofern nicht das Bundeskriminalamt die Daten erhoben hat.<br>Die Kennzeichnung nach Absatz 1 Nummer 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden.<br><br>(2) (…) | § 14 **Kennzeichnung**<br><br>(1) Bei der Speicherung im Informationssystem sind personenbezogene Daten wie folgt zu kennzeichnen:<br>1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,<br>2. Angabe der Kategorie nach den §§ 18 und 19 bei Personen, zu denen Grunddaten angelegt wurden,<br>3. Angabe der<br>a) Rechtsgüter, deren Schutz die Erhebung dient oder<br>b) Straftaten, deren Verfolgung oder Verhütung die Erhebung dient,<br>*4. Angabe der Rechtsgrundlage und des Zwecks der Speicherung*<br>*5. Angabe, für welche Datenabgleiche das Datum zur Verfügung steht*<br>*6. Voraussetzungen, unter denen das Datum an welche Empfänger und in welchem Verfahren übermittelt werden darf*<br>7. Angabe der Stelle, die sie erhoben hat, sofern nicht das Bundeskriminalamt die Daten erhoben | |

| | | |
|---|---|---|
| | hat.<br>Die Kennzeichnung nach Absatz 1 Nummer 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden.<br><br>(2) (…) | |
| Entwurfstext:<br><br>§ 16<br><br>Datenweiterverarbeitung im Informationssystem<br><br>(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.<br><br>(2) Das Bundeskriminalamt kann personenbezogene Daten im Informationssystem weiterverarbeiten, soweit dies erforderlich ist zur Fahndung und polizeilichen Beobachtung oder gezielten Kontrolle, wenn das Bundeskriminalamt oder die die Ausschreibung veranlassende Stelle nach dem für sie geltenden Recht befugt ist, die mit der Ausschreibung für Zwecke der Strafverfolgung, des Strafvollzugs, der Strafvollstreckung oder der | Änderungsvorschlag BfDI<br><br>§ 16<br><br>Datenweiterverarbeitung im Informationssystem<br><br>(1) Das Bundeskriminalamt kann personenbezogene Daten nach Maßgabe des § 12 im Informationssystem *speichern, verändern und nutzen*, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht.<br><br>(2) Das Bundeskriminalamt kann personenbezogene Daten im Informationssystem *speichern, verändern und nutzen*, soweit dies erforderlich ist zur Fahndung und polizeilichen Beobachtung oder gezielten Kontrolle, wenn das Bundeskriminalamt oder die die Ausschreibung veranlassende Stelle nach dem für sie geltenden Recht befugt ist, die mit der Ausschreibung für Zwecke der Strafverfolgung, des Strafvollzugs, der Strafvollstreckung oder der | |

| | | |
|---|---|---|
| Abwehr erheblicher Gefahren vorgesehene Maßnahme vorzunehmen oder durch eine Polizeibehörde vornehmen zu lassen. Satz 1 gilt entsprechend für Ausschreibungen zur Durchführung aufenthaltsbeendender oder einreiseverhindernder Maßnahmen. Die veranlassende Stelle trägt die Verantwortung für die Zulässigkeit der Maßnahme. Sie hat in ihrem Ersuchen die bezweckte Maßnahme sowie Umfang und Dauer der Ausschreibung zu bezeichnen. Nach Beendigung einer Ausschreibung nach Satz 1 oder Satz 2 sind die zu diesem Zweck gespeicherten Daten unverzüglich zu löschen.<br><br>(3) Das Bundeskriminalamt kann personenbezogene Daten, die es bei der Wahrnehmung seiner Aufgaben auf dem Gebiet der Strafverfolgung erlangt hat, unter den Voraussetzungen der §§ 18 und 19 im Informationssystem für Zwecke künftiger Strafverfahren weiterverarbeiten.<br><br>(4) Das Bundeskriminalamt kann im Informationssystem personenbezogene Daten mit Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, abgleichen, wenn Grund zu der Annahme besteht, dass dies zur Erfüllung einer Aufgabe erforderlich ist. Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.<br><br>(5) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Absatz 4 im Informationssystem personenbezogene Daten, die bei der Durchführung erkennungsdienstlicher Maßnahmen erhoben worden | Abwehr erheblicher Gefahren vorgesehene Maßnahme vorzunehmen oder durch eine Polizeibehörde vornehmen zu lassen. Satz 1 gilt entsprechend für Ausschreibungen zur Durchführung aufenthaltsbeendender oder einreiseverhindernder Maßnahmen. Die veranlassende Stelle trägt die Verantwortung für die Zulässigkeit der Maßnahme. Sie hat in ihrem Ersuchen die bezweckte Maßnahme sowie Umfang und Dauer der Ausschreibung zu bezeichnen. Nach Beendigung einer Ausschreibung nach Satz 1 oder Satz 2 sind die zu diesem Zweck gespeicherten Daten unverzüglich zu löschen.<br><br>(3) Das Bundeskriminalamt kann personenbezogene Daten, die es bei der Wahrnehmung seiner Aufgaben auf dem Gebiet der Strafverfolgung erlangt hat, unter den Voraussetzungen der §§ 18 und 19 im Informationssystem für Zwecke künftiger Strafverfahren *speichern, verändern und nutzen*.<br><br>(4) Das Bundeskriminalamt kann im Informationssystem personenbezogene Daten mit Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, abgleichen, wenn Grund zu der Annahme besteht, dass dies zur *Abwehr einer Gefahr* erforderlich ist. Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.<br><br>(5) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Absatz 4 im Informationssystem personenbezogene Daten, die bei der Durchführung erkennungsdienstlicher Maßnahmen erhoben worden | |

| | | |
|---|---|---|
| sind, weiterverarbeiten,<br><br>1. wenn eine andere Rechtsvorschrift dies erlaubt oder<br><br>2. dies erforderlich ist,<br><br>a) weil bei Beschuldigten und Personen, die einer Straftat verdächtig sind, wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen sie Strafverfahren zu führen sind, oder<br><br>b) um eine erhebliche Gefahr abzuwehren.<br><br>§ 18 Absatz 5 gilt entsprechend.<br><br>(6) Das Bundeskriminalamt kann in den Fällen, in denen bereits Daten zu einer Person vorhanden sind, zu dieser Person auch weiterverarbeiten<br><br>1. personengebundene Hinweise, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind, oder<br><br>2. weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen. | sind, *speichern, verändern und nutzen*,<br><br>1. wenn eine andere Rechtsvorschrift dies erlaubt oder<br><br>2. dies erforderlich ist,<br><br>a) weil bei Beschuldigten und Personen, die einer Straftat verdächtig sind, wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen sie Strafverfahren zu führen sind, oder<br><br>b) um eine erhebliche Gefahr abzuwehren.<br><br>§ 18 Absatz 5 gilt entsprechend.<br><br>(6) Das Bundeskriminalamt kann in den Fällen, in denen bereits Daten zu einer Person vorhanden sind, zu dieser Person auch personengebundene Hinweise *speichern und nutzen*, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind. | |
| Text des Entwurfs: | Änderungsvorschlag BfDI: | |

| | | |
|---|---|---|
| § 18 Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen<br><br>(1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Absatz 1 bis 3 personenbezogene Daten weiterverarbeiten von<br>1. Verurteilten,<br>2. Beschuldigten,<br>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<br>4. Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).<br>(2) Das Bundeskriminalamt kann weiterverarbeiten<br><br>1. von Personen nach Absatz 1 Nummer 1 bis 4<br>a) die Grunddaten und<br>b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale;<br>c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,<br>d) die Tatzeiten und Tatorte,<br>e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere | § 18 Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen<br><br>(1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Absatz 1 bis 3 personenbezogene Daten *in Dateien speichern, verändern und nutzen* von<br>1. Verurteilten,<br>2. Beschuldigten,<br>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<br>4. Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).<br>(2) Das Bundeskriminalamt kann *speichern, verändern und nutzen*<br><br>1. von Personen nach Absatz 1 Nummer 1 bis 4 *[Streichung des ersten Aufzählungspunktes]*<br>a) zur Identifizierung geeignete Merkmale *(Grunddaten i.S.d. § 20 Satz 2 Nr. 1)*;<br>b) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,<br>c) die Tatzeiten und Tatorte,<br>d) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere | |

| | | |
|---|---|---|
| Bezeichnung der Straftaten,<br>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;<br>3. von Personen nach Absatz 1 Nummer 3 und 4 weitere personenbezogen Daten.<br>(3) Das Bundeskriminalamt kann personenbezogene Daten weiterverarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 1 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden und sind im Informationssystem gesondert zu speichern. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.<br>(4) Das Bundeskriminalamt kann personenbezogene Daten weiterverarbeiten, soweit dies erforderlich ist zum Zwecke des Nachweises von Personen, die wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen. Die Löschung von Daten, die allein zu diesem Zweck weiterverarbeitet werden, erfolgt nach zwei Jahren.<br>(5) Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig | Bezeichnung der Straftaten,<br>2. von Personen nach Absatz 1 Nummer 1 und 2 weitere personenbezogene Daten, soweit die *Speicherung* 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;<br>3. von Personen nach Absatz 1 Nummer 3 und 4 weitere personenbezogen Daten.<br>(3) Das Bundeskriminalamt kann personenbezogene Daten zu *Beschuldigten speichern und nutzen*, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 1 *Nummer 4* erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck *genutzt* werden und sind im Informationssystem gesondert zu speichern. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.<br>(4) Das Bundeskriminalamt kann personenbezogene Daten *speichern und nutzen*, soweit dies erforderlich ist zum Zwecke des Nachweises von Personen, die wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen. Die Löschung von Daten, die allein zu diesem Zweck weiterverarbeitet werden, erfolgt nach zwei Jahren.<br>(5) *Wird der Beschuldigte rechtskräftig freigesprochen oder wird die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt, ist die weitere Speicherung unzulässig.*<br>*(6) Wird das Verfahren nicht nur vorläufig eingestellt, so* | |

| | | |
|---|---|---|
| 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. | *ist die Speicherung, Veränderung und Nutzung nur zulässig, wenn weiterhin ein erheblicher Tatverdacht besteht. Daten nach Absatz 2 Nummer 1 dürfen in diesem Fall nur unter den Voraussetzungen der Nummer 2 gespeichert werden, Die Daten sind zu löschen, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.* | |
| ***Zur Streichung des bisherigen § 34 BKAG*** | Vorschlag für eine geänderte Formulierung<br><br>Vorschlag: **Beibehaltung des § 34 BKAG.** Hilfsweise änderung in § 80. Äußerst hilfsweise Änderung in § 14: | |
| Entwurfstext:<br><br>§ 77 **Aussonderungsprüffrist; Mitteilung von Löschungsverpflichtungen**<br><br>(3) Die Fristen beginnen für alle zu einer Person gespeicherten Daten mit dem Tag, an dem die betroffene Person letztmalig zur Speicherung nach diesem Gesetz Anlass gegeben hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Die Speicherung kann über die in Absatz 1 Satz 2 genannten Fristen hinaus auch allein für Zwecke der Vorgangsverwaltung aufrechterhalten werden, sofern dies erforderlich ist; in diesem Falle können die Daten nur noch für diesen Zweck oder zur Behebung einer bestehenden Beweisnot verwendet werden. | Änderungsvorschlag BfDI:<br><br>§ 77 **Aussonderungsprüffrist; Mitteilung von Löschungsverpflichtungen**<br><br>(3) Die Fristen beginnen mit dem Tag, an dem *das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat,* jedoch nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Die Speicherung kann über die in Absatz 3 Satz 2 genannten Fristen hinaus auch allein für Zwecke der Vorgangsverwaltung aufrechterhalten werden; in diesem Falle können die Daten nur noch für diesen Zweck oder zur Behebung einer bestehenden Beweisnot verwendet werden. | Nr. 2 der Stellungnahme („Mitziehautomatik“) |

| | | |
|---|---|---|
| Text des Entwurfs:<br><br>§ 80 **Verzeichnis von Verarbeitungstätigkeiten**<br><br>(1) Das Bundeskriminalamt nimmt in das Verzeichnis nach § 70 des Bundesdatenschutzgesetzes Angaben auf zu<br><br>1. Kategorien von innerhalb seines Informationssystems durchgeführten Tätigkeiten der Datenverarbeitungen, einschließlich derer, die es im Rahmen seiner Teilnahme am polizeilichen Informationsverbund nach § 29 Absatz 3 durchführt,<br>2. Kategorien von Tätigkeiten der Datenverarbeitungen, die es in Erfüllung seiner Aufgabe nach § 2 Absatz 3 durchführt.<br>(2) Die nach § 70 Absatz 1 Satz 2 Nummer 2 des Bundesdatenschutzgesetzes geforderte Darstellung der Zwecke der im Informationssystem des Bundeskriminalamtes und in Erfüllung der Aufgabe nach § 2 Absatz 3 durchgeführten Kategorien an Verarbeitungen richtet sich nach den in den §§ 2 bis 8 genannten Aufgaben des Bundeskriminalamtes.<br>(3) Die nach § 70 Absatz 1 Satz 2 Nummer 3 des Bundesdatenschutzgesetzes geforderte Darstellung der Kategorien von Empfängern enthält auch Angaben dazu, ob die Übermittlung im Wege eines nach § 25 Absatz 7 eingerichteten automatisierten Abrufverfahrens erfolgt.<br>(4) Die nach § 70 Absatz 1 Satz 2 Nummer 4 des Bundesdatenschutzgesetzes geforderte Beschreibung | Artikel 1, § 80 wird wie folgt gefasst:<br><br>§ 80 **Verzeichnis von Verarbeitungstätigkeiten**<br><br>(1) Das Bundeskriminalamt legt in dem Verzeichnis nach § 70 des Bundesdatenschutzgesetzes Kategorien *der* innerhalb seines Informationssystems *und des Informationsverbundes* durchgeführten Datenverarbeitungen fest. *Für die jeweilige Kategorie bestimmt es:*<br><br>*1. Zweck und Rechtsgrundlage der innerhalb der Kategorie durchgeführten Datenverarbeitung,*<br>*2. Personenkreis, über den Daten gespeichert werden,*<br>*3. Art der zu speichernden personenbezogenen Daten,*<br>*4. Arten der personenbezogenen Daten, die für einen Datenabgleich zur Verfügung stehen,*<br>*5. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden,*<br>*6. Prüffristen und Speicherungsdauer.*<br><br>(2) Der Personenkreis und die Art der personenbezogenen Daten *ist gemäß der* §§ 18 und 19 *und* gemäß der Rechtsverordnung nach § 20 *zu bestimmen*.<br>*(3) Der oder die Bundesbeauftragte für den Datenschutz ist hierzu vorher anzuhören.* | Siehe dazu Nr. 1 und Nr. 3 der Stellungnahme.<br><br>Sofern dieser Änderung nicht gefolgt wird, müssen mindestens die zu § 14 vorgeschlagenen Änderungen eingefügt werden.<br><br>Die Änderung führt auch zu sprachlichen Verbesserungen, da die mehrfach gestaffelte Verweisungstechnik sehr unübersichtlich ist. |

| | | |
|---|---|---|
| 1. der Kategorien betroffener Personen richtet sich insbesondere nach den in den §§ 18 und 19 genannten Personen,<br>2. der Kategorien personenbezogener Daten richtet sich insbesondere nach den in der Rechtsverordnung nach § 20 aufgeführten Datenarten.<br>(5) Die im Verzeichnis enthaltenen Angaben zu Kategorien von Datenverarbeitungen nach Absatz 1 Nummer 2 enthalten Aussagen zu den Kriterien nach § 30.<br>(6) Das Bundeskriminalamt stellt das Verzeichnis und dessen Aktualisierungen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Verfügung. | | |
| | | |

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 A - Erg.

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

**Andrea Voßhoff**
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

**POSTANSCHRIFT** Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

An den
Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn Ansgar Heveling, MdB

An die
Vorsitzende des Ausschuss für
Recht und Verbraucherschutz
des Deutschen Bundestages
Frau Renate Künast, MdB

Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL arbeitsgruppe22@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 17.03.2017
GESCHÄFTSZ. **22-642/041#1204**

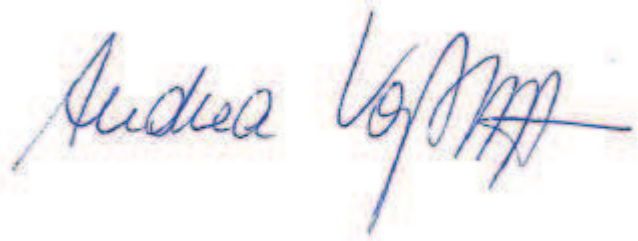
**Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.**

BETREFF **Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes, BT-Drs. 18/11163 und 18/11326**
HIER Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
BEZUG Öffentliche Anhörung am 20. März 2017
ANLAGEN 1

Sehr geehrter Herr Vorsitzender,
sehr geehrte Frau Vorsitzende,

in Ergänzung zu meiner Stellungnahme vom 10. März 2017 sende ich Ihnen anbei eine Entschließung der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder zum o.g. Gesetzentwurf.

Mit freundlichen Grüßen



Andrea Voßhoff

Die Landesbeauftragte für den
Datenschutz Niedersachsen

Hannover, 16.03.2017

**Entschließung der**
**Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder**

**Neues Bundeskriminalamtgesetz - Informationspool beschneidet Grundrechte**

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.
Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.
Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.
Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 B

UNIVERSITÄT BAYREUTH

Lehrstuhl für Öffentliches Recht II
Prof. Dr. Markus Möstl

**Stellungnahme im Rahmen der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (BT-Drs. 18/11163 und 11326) am 20.3.2017**

Ich beschränke meine Stellungnahme – meiner Rolle als Hochschullehrer des öffentlichen Rechts entsprechend – im Wesentlichen auf einige grundlegende Aspekte zum vorliegenden Gesetzentwurf, die aus wissenschaftlicher Sicht bemerkenswert erscheinen. Im Zentrum steht dabei die Prüfung des Entwurfs auf seine Vereinbarkeit mit den Maßstäben, die das BVerfG in seinem BKAG-Urteil vom 20.4.2016 (1 BvR 866/09 und 1140/09) entwickelt hat, deren Umsetzung der vorliegende Entwurf dient. Fragen der korrekten Umsetzung der Richtlinie (EU) 2016/680 vom 27.4.2016 sollen dagegen nur am Rande und nur, soweit sie im bisherigen Gesetzgebungsverfahren hervorgetreten sind, gestreift werden, denn ihre Beantwortung würde eine umfassende Einbeziehung auch der parallel stattfindenden Novellierung des BDSG (DSAnpUG-EU) voraussetzen, die in diesem Rahmen nicht geleistet werden kann. Zur Anhörung wurde kein Fragenkatalog vorgelegt, so dass eine eigenständige Schwerpunktsetzung unumgänglich ist.

Zur Frage der Umsetzung der vom BVerfG im BKAG-Urteil entwickelten Maßstäbe erscheint eine Vorbemerkung nötig: Das BKAG-Urteil setzt den vorläufigen Schlusspunkt einer Rechtsprechungsreihe, in der das BVerfG dem Polizeirechtsgesetzgeber ungewöhnlich dichte und bis ins Detail der einfachgesetzlichen Dogmatik hinabsteigende Vorgaben gemacht hat, die bisweilen geradezu ersatzgesetzgeberische Züge tragen bzw. in Funktionen des einfachen Gesetzgebers übergreifen; die Senatsmehrheit hat hierfür auch Kritik einstecken müssen, sowohl in den Sondervoten als auch in der Literatur. Wenn der Gesetzgeber vor der Aufgabe steht, solchermaßen dichte Vorgaben umzusetzen, wird er versucht sein, dies Punkt für Punkt möglichst getreulich zu tun, bis hin zu der Technik, Aussagen der Urteilsgründe mehr oder weniger wortwörtlich in gesetzliche Tatbestände zu gießen. Ein solches Vorgehen ist selbstverständlich zulässig und es minimiert zweifelsohne verfassungsrechtliche Risiken. Es ist verständlich, dass auch der vorliegende Gesetzentwurf eben diesen Weg der getreulichen Übernahme weit überwiegend zu gehen versucht – zur Konsequenz hat dies, dass der Entwurf, um ein Ergebnis vorweg zu nehmen, auch in der Tat kaum größere verfassungsrechtliche Probleme aufwirft. Dennoch erscheint es angebracht – und gerade für diejenigen (verhältnismäßig wenigen) Bereiche ist dies wichtig, wo der vorliegende Gesetzentwurf in dem vom BVerfG behandelten Bereich einmal doch abweichende oder eigenständige Akzente setzt –, darauf hinzuweisen, dass der Gesetzgeber auch bei dichten Vorgaben nicht gezwungen ist, stets diesen Weg der „eins-zu-eins"-Umsetzung zu gehen:

- Denn auch bei dichten Vorgaben in den Ausführungen des Gerichts heißt „Bindung an die tragenden Urteilsgründe" im Sinne des § 31 Abs. 1 BVerfGG nicht, dass der Gesetzgeber Einzelaussagen des BVerfG sozusagen wortwörtlich übernehmen müsste; auf der Linie der tragenden Erwägungen ist er vielmehr auch zu eigenständigen dogmatischen Systembildungen in der Lage und berufen. Er darf seine originäre gesetzgeberisch-gestalterische Aufgabe auch verteidigen.

**Prof. Dr. Markus Möstl** I Lehrstuhl für Öffentliches Recht II, RW II, Zi. 1.64, Universitätsstr. 30, 95447 Bayreuth,
Tel: 0921 55-6211 (Sekretariat), Fax: 0921 55-6212, markus.moestl@uni-bayreuth.de
www.oer2.uni-bayreuth.de

- Der Gesetzgeber hat – gerade in einem Bereich, der auch im Gericht selbst so umstritten war wie der vorliegende (vgl. Sondervoten) – trotz § 31 Abs. 1 BVerfG, wenn er entsprechende sachliche Gründe anführen kann, einen gewissen Spielraum des Festhaltens an eigenen Regelungsanliegen, der äußerstenfalls bis zur Wiederholung der verworfenen Norm reichen kann, in jedem Fall aber eine Norm nicht schon deswegen als verfassungswidrig erscheinen lässt, weil u.U. einzelne Teilaspekte eines vom BVerfG kritisierten Regelungsansatzes in modifizierter Form oder anderem Kontext wiederaufgegriffen werden (vgl. Heusch, in Burkiczak/Dollinger/Schorkopf, BVerfGG, § 31, Rn. 61 ff.; BVerfGE 135, 259/281 f.).
- Unbenommen ist es dem Gesetzgeber schließlich, dogmatische Ansätze des BVerfG weiterzudenken und auch in anderen Kontexten anzuwenden, insbesondere auch, soweit sich neue Bedrohungslagen und Regelungsbedürfnisse ergeben, die das BVerfG nicht thematisieren konnte. Von Bedeutung ist dies im hiesigen Kontext, weil die terroristischen Anschläge des vergangenen Jahres und namentlich der Anschlag in Berlin im vorliegenden Entwurf auch zu neuen Befugnissen (Aufenthalts- und Kontaktverbot, Elektronische Aufenthaltsüberwachung, §§ 5 f. BKAG-E) geführt haben, die teilweise an (in anderem Kontext entwickelte) Systembildungen des BVerfG (z.B. hinsichtlich der Eingriffsschwelle) anknüpfen.

## 1. Strukturelle Bemerkungen zur Fassung der Eingriffstatbestände

### a) Eingriffsschwelle im Gefahrenvorfeld

Das BKAG-Urteil des BVerfG führt zu einer gewissen Konsolidierung hinsichtlich der Anforderungen, die an die Fassung von Eingriffsschwellen zu stellen sind, welche Informationseingriffe bereits im Gefahrenvorfeld ermöglichen wollen (die früheren Entscheidungen hatten diesbezüglich noch keine Klarheit gebracht, vgl. Möstl, DVBl. 2010, 808/809). Gerade in Bezug auf terroristische Gefahren scheint es unumgänglich, polizeiliche Gefahraufklärung bereits im Gefahrenvorfeld ansetzen zu lassen (und dies ggf. auch mittels eingriffsintensiver Maßnahmen), um überhaupt in der Lage zu sein, etwaige Gefahren rechtzeitig entdecken und ggf. bekämpfen zu können. Das BVerfG konzediert dies ausdrücklich und entwickelt v.a. in Rn. 112 eine – auf eingriffsintensive Maßnahmen zum Schutz gewichtiger Rechtsgüter zugeschnittene – Eingriffsschwelle, die einerseits darauf abstellt, dass bestimmte Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes Geschehen sowie eine Begrenzung auf einen bestimmten Personenkreis zulassen, oder aber andererseits darauf, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie bestimmte Straftaten begehen wird. Gemeinsam ist diesen Fallgruppen, dass es weniger um eine Absenkung der Wahrscheinlichkeitsschwelle geht (dass überhaupt eine Rechtsgutsverletzung/Straftatenbegehung droht, ist durchaus hinreichend wahrscheinlich), sondern dass der genaue Kausalverlauf (wann, wo und wie wird sich die Gefahr möglicherweise realisieren?) noch nicht in der Weise konkret vorhersehbar ist, wie dies sonst für eine konkrete Gefahr erforderlich ist. Ermöglicht wird damit eine gewisse – begrenzte (vgl. die Einschränkungen in Rn. 113) –, aber doch wichtige Vorverlagerung der Eingriffsmöglichkeit selbst in Bezug auf tiefgreifende Informationseingriffe (bzgl. weniger tiefgreifenden Ermittlungseingriffen ist eine weitergehende Vorverlagerung zulässig, vgl. Rn. 104).

Der vorliegende Gesetzentwurf greift die Aussagen des Urteils in der Weise auf, dass diese quasi wortwörtlich in die Fassung der jeweiligen Eingriffstatbestände übernommen werden (§ 45 I Nr. 2, 3; § 49 I 2, § 50 I Nr. 2, 3; § 51 I Nr. 2, 3; § 52 I Nr. 2, 3 etc. BKAG-E). Dies ist eine zweifelsohne zulässige und bedenkenfreie gesetzgeberische Technik. Etwaige Chancen zu einer generellen gesetzgeberischen Fortentwicklung der polizeirechtlichen Systembildung, indem etwa eine vor die Klammer gezogene Regelung zu dieser neuen Eingriffsschwelle geschaffen und für diese ein neuer übergreifender Gefahr- bzw. Gefahrverdachtsbegriff definiert wird, werden jedoch nicht aufgegriffen (anders z.B. die derzeitigen Überlegungen zur Novellierung des BayPAG; hier soll die vom BVerfG beschriebene Eingriffsschwelle vor der Klammer in einem neuen Art. 11

III BayPAG-E als „drohende Gefahr" definiert werden; siehe https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwuerfe/gesetzentwurf_-_gesetz_zur_effektiveren_Überwachung_gefährlicher_personen.pdf). Auch bleibt die Interpretation dessen, was genau mit der neuen Schwelle gemeint ist, ganz der Rechtsanwendung überlassen, ohne dass eigenständige Präzisierungs- oder Formulierungsversuche unternommen werden (so solchen Versuchen vgl. z.B. Darnstädt, DVBl. 2017, 88). Dies ändert freilich nichts daran, dass gegen die wortwörtliche Übernahme der vom BVerfG getroffenen Aussagen verfassungsrechtlich nichts zu erinnern ist.

Die neue Eingriffsschwelle verwendet der Gesetzesentwurf auch für die im BKAG neuartigen Befugnisse des Aufenthalts-/Kontaktverbots (§ 55 BKAG-E) und der elektronischen Aufenthaltsüberwachung (§ 56 BKAG-E). Die Entwurfsbegründung merkt hierzu an (BT-Drs. 18/11163, S. 116, 117), hierdurch solle auf die vom BVerfG „entwickelten Voraussetzungen für gefahrenabwehrrechtliche Maßnahmen zurückgegriffen" werden, „die auch für die übrigen Maßnahmen des Bundeskriminalamtes gelten". Damit füge sich „die neue in den Kanon der bestehenden Befugnisse ein".

Übergangen wird durch diese Begründung allerdings der Umstand, dass das BVerfG die neue Gefahrenvorfeldschwelle ausdrücklich allein für (reine) Informationseingriffe (vgl. Rn. 103 ff. „Ermittlungs- und Überwachungsbefugnisse"), nicht dagegen für in Kausalverläufe eingreifende aktionelle Befugnisse entwickelt hat. Jedenfalls das Aufenthalts- und Kontaktverbot ist jedoch eine Anordnung, mithilfe derer sehr wohl in Kausalverläufe eingegriffen und das (weitere) Entstehen einer drohenden Gefahr verhindert werden soll (um reine Ermittlung geht es hier gerade nicht, vielmehr werden Konsequenzen aus vorhandenen Erkenntnissen gezogen). Und auch die elektronische Aufenthaltserfassung, mag diese im Schwerpunkt durchaus eine informationelle (auf Erkenntnisgewinn gerichtete) Zielrichtung haben, kann (gerade, wenn sie in Verbindung mit einem Aufenthalts-/Kontaktverbot angeordnet wird, vgl. § 56 II Nr. 2 BKAG) durchaus (auch) verhaltensbeeinflussende Wirkung haben, so dass sie im Grenzbereich zwischen rein informationeller und aktioneller Maßnahme anzusiedeln ist (vgl. Brodmerkel, https://bayrvr.de/2017/03/09/der-gesetzentwurf-zur-effektiveren-ueberwachung-gefaehrlicher-personen-gelungen-mit-einschraenkungen/, unter 5.).

Der Unterschied zwischen aktionellen und rein informationellen Befugnissen ist für das Polizeirecht jedoch systemprägend (zum Folgenden mwN: Möstl, in Möstl/Schwabenbauer, BeckOK PolSichR Bayern, Systematische Vorbemerkungen, Rn. 37): Aktionelle (d.h. verhaltenssteuernde, in den potentiell schadensträchtigenden Kausalverlauf eingreifende und diesen unterbrechen wollende) Befugnisse hat die Polizei regelmäßig erst ab der Schwelle der konkreten Gefahr (systembildend: die polizeiliche Generalklausel). Rein informationelle, der Gefahraufklärung dienende Befugnisse dagegen können, ja müssen typischerweise bereits im Gefahrenvorfeld ansetzen, denn sie dienen der Gewinnung von Erkenntnissen, die nötig sind, um das Entstehen und Bestehen von Gefahren zu erkennen und dann – nach erkannter Gefahr – mittels aktioneller Befugnisse gegen sie einzuschreiten (vgl. Gusy JA 2011, 641: „Gefahrenabwehr setzt Gefahraufklärung voraus"); allenfalls wie weit die Vorverlagerung je nach Gewicht des Eingriffs reichen darf, kann verfassungsrechtlich problematisch sein. Deutlich wird, dass es (entgegen dem in der Gesetzesbegründung erweckten Eindruck) keineswegs selbstverständlich ist, dass eine aktionelle Befugnis im Gefahrenvorfeld ansetzen darf und dass eine vom BVerfG allein für Informationseingriffe entwickelte Vorfeldschwelle auch auf aktionelle Befugnisse übertragen werden darf.

Dennoch sind gegen die neuen Befugnisse, was die Fassung ihrer Eingriffsschwellen anbelangt, im Ergebnis keine verfassungsrechtlichen Bedenken zu erheben. Denn die Gefahrenschwelle als Regelschwelle für aktionelle Gefahrbeseitigungseingriffe entspricht nur einer verfassungsrechtlichen Normalvorstellung des verhältnismäßigen Ausgleichs von Freiheits- und Sicherheitsinteressen in Ungewissheitslagen (Möstl, Die

staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, S. 195 ff.), die nicht für alle denkbaren Fallkonstellationen zwingend ist. Seit jeher ist anerkannt, dass der Gesetzgeber bei entsprechender sachlicher Notwendigkeit der Polizei oder den Sicherheitsbehörden auch (aktionelle) Befugnisse einräumen darf, die in besonderen Fällen auch einmal vor der Normaleingriffsschwelle der konkreten Gefahr ansetzen. Eine solche Vorverlagerung ist verfassungsrechtlich rechtfertigungsbedürftig, u.U. aber sehr wohl rechtfertigbar. Genau so liegt der Fall hier: Denn die zu bekämpfenden terroristischen Gefährdungslagen, bei denen es (gemäß der neuen Vorfeldschwelle) zwar hinreichend wahrscheinlich erscheint, dass es überhaupt zu einer terroristischen Straftat kommen kann, sich aber (für eine konkrete Gefahr) noch nicht hinreichend konkret absehen lässt, wie, wann und wo sich diese Gefahr realisieren wird, zeichnen sich gerade dadurch aus, dass es oftmals als unzureichend erscheint, im Gefahrenvorfeld allein auf Gefahrbeobachtung zu setzen, da das Risiko, dass sich die Gefahr vielleicht plötzlich realisiert, noch bevor sie aufgeklärt ist, angesichts der auf dem Spiele stehenden Rechtsgüter zu hoch ist (terroristische Gefährdungslagen, die sich verdeckt entwickeln, können sehr schnell in eine Gefahr und einen Schaden umschlagen); gleichermaßen kann reine Gefahraufklärung (zB in Gestalt permanenter Beobachtung) auch zu aufwändig sein, um eine realistische und praktisch durchführbare Alternative zu einer (auch) aktionellen Vorgehensweise darstellen zu können. In genau diesen Fällen sollen die neuen Befugnisse der Polizei ein Mittel an die Hand geben, mittels Aufenthalts- und Kontaktverboten und ggf. flankiert durch elektronische Aufenthaltsüberwachung präventiv das weitere Entstehen der drohenden Gefahr abzuwenden. Die neuen Befugnisse basieren – sicherlich auch infolge der Erfahrungen aus dem Anschlag von Berlin – also auf der Erkenntnis, dass es für die Bekämpfung terroristischer Gefahren nicht immer ausreicht, auf die klassische Systembildung „(rein informationelle) Gefahraufklärung im (je nach Eingriffstiefe zu begrenzenden) Gefahrenvorfeld, aktionelle Kausalverlaufseingriffe jedoch erst ab der Schwelle der konkreten Gefahr" zu setzen, da eine verlässliche und rechtzeitige Gefahrerkennung durch rein informationelle Vorfeldmaßnahmen oftmals nicht möglich ist, so dass auch gewisse aktionelle Maßnahmen im Gefahrenvorfeld unvermeidlich erscheinen (vgl. Brodmerkel, https://bayrvr.de/2017/03/09/der-gesetzentwurf-zur-effektiveren-ueberwachung-gefaehrlicher-personen-gelungen-mit-einschraenkungen/, unter 7.). Wenn der Gesetzgeber hierbei auf die vom BVerfG (in anderem, nämlich rein informationellen Kontext) entwickelte Vorfeldschwelle des BKAG-Urteils zurückgreift, so erscheint dies als eine zulässige und verfassungsrechtlich rechtfertigbare Erstreckung einer Systembildung des BVerfG auf einen anders gelagerten Befugnistypus (siehe auch meine Vorbemerkung unmittelbar vor 1.).

b) Straftatenbezogene Eingriffstatbestände

Noch ein letztes sei allgemein zur Fassung der Eingriffstatbestände angemerkt: Einwandfrei sind diese auch, soweit sie (wie z.B. §§ 45 I Nr. 2, 3, 51 I Nr. 2, 3, 55 I, 56 I BKAG-E) tatbestandlich auf die (drohende) Gefahr der Begehung bestimmter Straftaten (nach § 5 I 2 BKAG-E) statt auf die (drohende) Gefahr einer Verletzung bestimmter Rechtsgüter (so zB § 49 I 2 BKAG-E) abstellen. Dies zu betonen besteht deswegen Anlass, weil das BVerfG mehrfach den Eindruck erweckt hat, als sei es für das Polizeirecht generell keine geeignete Regelungstechnik, Eingriffstatbestände statt rechtsgutsbezogen straftatenbezogen (d.h. auf die Verhütung bestimmter Katalogstraftaten bezogen) auszuformen (BVerfGE 122, 120/142; 125, 260/329; in diese Richtung auch BKAG-Urteil Rn. 108; kritisch dazu Möstl DVBl. 2010, 808/811 ff.; Möstl, in: Möstl/Schwabenbauer, BeckOK PolSichR Bayern, Systematische Vorbemerkungen, Rn. 12.1.). Für eine solche Sichtweise ist jedoch keinerlei verfassungsrechtlich tragfähiger Grund ersichtlich. Denn das deutsche Polizeirecht ist – unter der Überschrift des Schutzes der öffentlichen Sicherheit – bereits seit langem nicht allein auf den Schutz bestimmter Rechtsgüter (Leib, Leben, Gesundheit, Freiheit, Eigentum, Ehre etc. - Rechtsgüterschutz), sondern auch (und sogar zuallererst) auf den Schutz der Unversehrtheit der Rechtordnung bezogen (Rechtsdurchsetzung), so dass polizeiliche Befugnisnormen ganz selbstverständlich (und oftmals mit dem Vorzug

größerer Bestimmtheit) auch auf die Verhütung bestimmter Straftaten abstellen dürfen. Es ist vor diesem Hintergrund zu begrüßen, dass das BVerfG im BKAG-Urteil – trotz seiner erneut missverständlichen Äußerungen in Rn. 108 – mehrfach implizit anerkennen musste, dass Eingriffsbefugnisse auf die Verhütung bestimmter Straftaten abzielen dürfen (dies jedenfalls dann, wenn sie, wie die Straftaten des § 5 I 2 BKAG-E, ihrerseits dem Schutz derjenigen Rechtsgüter dienen, die das BVerfG gemäß Rn. 108 als für die Rechtfertigung tiefgreifende Ermittlungseingriffe im terroristischen Kontext maßgeblich ansieht); siehe insbesondere Rn. 108 „solche Straftaten", „Straftatenverhütung"; s.a. Rn. 164; zuvor bereits Rn. 88, 96.). Der Gesetzentwurf greift dies zu Recht auf, und zwar nicht allein dadurch, dass er die einzelnen Eingriffsbefugnisse straftatenbezogen ausgestaltet, sondern in einwandfreier Weise auch dadurch, dass er bereits die aufgabeneröffnende terroristische Gefahr gemäß § 5 I 2 BKAG-E auf die Verhütung bestimmter Straftaten bezogen definiert (dazu auch Entwurfsbegründung S. 86).

## 2. Horizontal wirkendes Datenschutzkonzept und Grundsatz der hypothetischen Datenneuerhebung

Der Gesetzentwurf will – statt der bisherigen vertikalen Aufspaltung Einzeldateien – zu einem horizontal wirkenden Datenschutzkonzept im Rahmen eines einheitlichen (die prinzipielle wechselseitige Vernetzung sicherstellenden) Verbundsystems übergehen. Das entsprechende gesetzgeberische Ziel wird auf den S. 73 f. der Entwurfsbegründung plausibel dargelegt. Der Legitimität des gesetzgeberischen Ziels tut es keinen Abbruch, dass das auf S. 73 in Bezug genommene Zitat aus Rn. 281 des BVerfG-Urteils einer Passage entstammt, in der es zunächst nur um die Verwendung von Spurenansätzen und noch nicht um (ggf. zweckändernde) Übermittlungen im Allgemeinen ging (vgl. den Hinweis in Punkt 1. der Stellungnahme des Bundesrates, BT-Drs. 109/17). Denn erstens dürfte sich der in Bezug genommene Gedanke des BVerfG (dass sich die Generierung von Wissen nicht auf die Addition von je getrennten Einzeldaten reduzieren lässt) verallgemeinern lassen. Zweitens bedarf der demokratische Gesetzgeber für die Verfolgung eines vernünftigen Ziels keiner verfassungsrechtlichen/verfassungsgerichtlichen Ermächtigung (er darf selbst legitime Ziele setzen). Drittens und überdies lässt sich (soweit es hierauf ankäme) sogar eine verfassungsunmittelbare Rechtfertigung für die Verfolgung des gesetzgeberischen Ziels finden: Das Ziel eines einheitlichen, eine effektive wechselseitige Vernetzung sicherstellenden Datenverbundsystems sieht sich in Art. 87 Abs. 1 Satz 2 GG (Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen) nämlich auf eine verfassungsrechtliche Basis gestellt, auf die sich der Gesetzgeber (im Rahmen einer grundrechtlichen Rechtfertigungsprüfung) berufen kann.

Freilich muss sich die Weiterverwendung und Übermittlung von Daten ggf. an den Grundrechten der hiervon Betroffenen messen lassen. Als dogmatisches Kernstück des neuen horizontal wirkenden Datenschutzkonzepts, mithilfe dessen die Grundrechtskonformität der Datenverwendung im Rahmen des neuen Verbundsystem gewährleistet werden soll, fungiert im Gesetzentwurf der Grundsatz der hypothetischen Datenneuerhebung, wie er vom BVerfG im BKAG-Urteil ausgeformt wurde. An der Normierung dieses Grundsatzes in § 12 BKAG-E fällt auf, dass er als allgemeiner Grundsatz für die prinzipiell gesamte Weiterverarbeitung von Daten durch das BKA Anwendung finden soll (vgl. die systematische Stellung im Allgemeinen Teil des Abschnittes 2); auch der Gesetzentwurf sagt ausdrücklich, der Grundsatz gelte bei jeder Datenverarbeitung durch das BKA – unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme (S. 89, siehe auch S. 91: „allgemeiner Grundsatz"). Dies wirkt sich auch aus auf im Allgemeinen (d.h. bzgl. aller Daten) entsprechend gesteigerte Kennzeichnungspflichten (§ 14 BKAG-E). Der Gesetzentwurf geht hierbei bewusst deutlich über das hinaus, was das BVerfG zwingend gefordert hat, denn dieses hat den (vergleichsweise strengen) Grundsatz der hypothetischen Datenneuerhebung ausdrücklich allein für Daten gefordert, die aus „eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen" entstammen (vgl. Rn.

287 des Urteils). Bzgl. der aus nicht besonders eingriffsintensiven Ermittlungsmaßnahmen gewonnen Daten hat es zumindest offen gelassen, ob hier nicht ein milderer Maßstab (z.B. keine Unvereinbarkeit der Zwecke, vgl. dazu auch Art. 4 Abs. 1 b) der Richtlinie 2016/680) in Betracht kommt, wenn diesbezüglich nicht sogar ein zwingender Umkehrschluss zu bilden ist.

Dem Gesetzgeber ist es grundrechtlich freilich nicht verwehrt, den vergleichsweise strengen Maßstab der hypothetischen Datenneuerhebung (zur Kritik hieran vgl. die Sondervoten des BKAG-Urteils) über das grundrechtlich zwingende Maß hinaus allgemein zu statuieren. Er nimmt hierdurch aber ggf. Schutzlücken in Kauf und erschwert die Arbeit der Polizei über das verfassungsrechtlich erforderliche Maß hinaus. In diesem Kontext erscheint es gut nachvollziehbar, dass die Stellungnahme des Bundesrates (vgl. Punkt 6. der BR-Drs. 109/17) zu bedenken gibt, dass eine so weit gezogene Fassung des Grundsatzes der hypothetischen Datenneuerhebung (samt entsprechenden durchgehenden Kennzeichnungspflichten) die Sachbearbeitung in den Ländern vor schwerwiegendste Probleme stellen würde (vgl. S. 4 des BR-Beschlusses). Erwägenswert erscheint auch, dass vom Bundesrat (a.a.O.) Übergangsregelungen (auch für Altdaten) angeregt werden. Es ist mir, der ich keinen besonderen Praxiseinblick habe, nicht möglich, aus dem Stegreif verlässlich zu beurteilen, welche Praxiskonsequenzen eine so umfassende Normierung des Grundsatzes der hypothetischen Datenneuerhebung (samt verfahrensrechtlicher Flankierung durch entsprechende Kennzeichnungspflichten) haben würde. Es scheint mir aber doch, dass ein sehr ehrgeiziger Ansatz gewählt wird, der die vom BVerfG aufgestellten anspruchsvollen Anforderungen (die an sich schon im Senat umstritten waren, vgl. die Sondervoten) noch zusätzlich perfektioniert, und was als Sonderrecht für Daten aus eingriffsintensiven Maßnahmen konzipiert war, unnötig zu einem allgemeinen Grundsatz des polizeilichen Datenschutzrechts erhebt.

Noch eine letzte Überlegung sei in diesem Zusammenhang gestattet (sie betrifft speziell die zweckändernde Verwendung von aus präventivpolizeilichen Gründen erhobenen Daten zu Repressivzwecken und umgekehrt): Der Grundsatz der hypothetischen Datenneuerhebung, wie ihn das BVerfG entwickelt hat, passt diesbezüglich gut, soweit es um Daten geht, die aus einem eindeutig präventivpolizeilichen Kontext stammen, wie dies im Kontext der BKA-Aufgabe „Abwehr von Gefahren des internationalen Terrorismus" (über die allein das BVerfG zu befinden hatte) auch klar der Fall ist. Ich habe jedoch Zweifel, ob es sachlich richtig ist, diesen Grundsatz – wie in § 12 BKAG-E geplant – auf die gesamte Tätigkeit des BKA, insbesondere auch seine Zentralstellentätigkeit zu erstrecken. Denn als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen hat das BKA schon bislang (und ich vermute, das soll so bleiben), wie die Praxis so genannter „Mischdateien" zeigt, Aufgaben der Zurverfügungstellung von Daten wahrgenommen, die das Präventiv-Repressiv-Schema bewusst übersteigen und sich diesbezüglich nicht eindeutig zuordnen lassen (vgl. § 2 Abs. 1 und Abs. 4 BKAG und BKAG-E, § 9 Abs. 1 BKAG: „Verhütung und Verfolgung von Straftaten", z.B. im Rahmen der Fahndung nach Personen und Sachen; zu solchen Mischdateien siehe auch § 483 Abs. 3 StPO; BVerfGE 120, 378/421 f. ). Dass dies so ist, ist auch kein rechtsstaatliches Manko, sondern verfassungsrechtlich legitimiert, da die Normierung der einheitlichen übergreifenden Aufgabe „polizeiliches Auskunfts- und Nachrichtenwesen" in Art. 87 Abs. 1 Satz 2 GG ein Stück weit anerkennt, dass sich kriminalpolizeiliche Datensammlungen nicht stets eindeutig nach dem Präventiv-Repressiv-Schema zuordnen lassen, sondern ggf. multifunktional einsetzbar sein müssen (vgl. Ibler, in Maunz/Dürig, Art. 87, Rn. 129: keine „strikte Trennung" von Gefahrenabwehr und Strafverfolgung in diesem Rahmen; siehe auch Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 2 BKAG, Rn. 7). Es wäre wünschenswert, dass der Gesetzgeber klarstellte, in welchem Verhältnis der Grundsatz der hypothetischen Datenneuerhebung bei Zweckänderungen in § 12 BKAG-E zu dieser (multifunktionellen) Eigenart der Zentralstellenaufgabe des BKAG stehen soll (es sei denn man versteht die wiederholte Bezugnahme auf „Verhütung oder Verfolgung" von Straftaten

in § 12 BKAG-E so, dass bereits damit klargestellt werden soll, dass allein die präventiv-repressive Zweckänderung innerhalb des BKA wegen der einheitlich zu begreifenden Zentralstellenaufgabe kein Problem sein soll; eventuell spricht dafür auch die Kennzeichnungsregelung des § 14 Abs. 1 Nr. 2 und 3 BKAG-E, die zwar die Kennzeichnung der Rechtsgüter, deren Schutz die Erhebung dient, bzw. der Straftaten, deren Verfolgung oder Verhütung die Erhebung dient, verlangt, nicht aber eindeutig auch eine Kennzeichnung, ob der diesbezügliche ursprüngliche Erhebungszweck präventiv oder repressiv war). Die streng nach präventiven und repressiven Zwecken unterscheidende Logik der Lehre von der Zweckbindung und des Grundsatzes der hypothetischen Datenneuerhebung steht insoweit in einer nicht ganz klar aufgelösten Spannung zu einer spezifischen Eigenart des BKA als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen, die diesen Unterschied traditionell gerade nicht besonders betont, sondern bewusst überschreitet.

## 3. Einzelfragen der Verfassungs- und Unionsrechtskonformität

- Erwägenswert erscheint die Anregung des Bundesrates, die §§ 18, 19 BKAG-E stärker an den Personenkategorien des Art. 6 der Richtlinie (EU) 2016/680 zu orientieren (vgl. Punkt 7. der BR-Drs. 109/17).

- Erwägenswert erscheint auch die in Punkt 8. der Stellungnahme des Bundesrates (BR-Drs. 109/17) geäußerte Prüfbitte zu § 28 BKAG-E.

- Aus meiner Sicht im Ergebnis zu Recht nicht übernommen hat das Plenum des Bundesrates eine vom Rechtsausschuss des Bundesrates noch vorgeschlagene Kritik an § 45 Abs. 3 Satz 1 Nr. 5 BKAG-E (vgl. Empfehlungen 109/1/17, Punkt 11; in BR-Drs. 109/17 fehlt dieser Punkt). Er betrifft die Frage, ob der dort vorgesehene Richtervorbehalt für Maßnahmen nach Abs. 2 Nr. 4 und 5 (Vertrauensperson und Verdeckter Ermittler) an die Bedingung geknüpft werden kann, dass sich die Ermittlung gegen eine bestimmte Person richtet oder dass eine nicht allgemein zugängliche Wohnung betreten werden soll. Denn zwar ist richtig, dass das BVerfG im Rahmen seiner Anordnung zur übergangsweisen Weiteranwendung des § 20g BKAG den Richtervorbehalt nicht mit dieser Einschränkung versehen hat. Andererseits hat es sich in den Gründen zur Frage der Zulässigkeit dieser Einschränkung nicht ausdrücklich geäußert, sondern andere Probleme thematisiert (Fokus auf das Problem, ob der Richtervorbehalt bereits für die erstmalige Anordnung oder nur für die Verlängerung der Maßnahme vorgesehen werden muss; vgl. Rn. 172 ff.; eher positive Äußerung zum – eingeschränkten – Richtervorbehalt dagegen in Rn. 173). Vor dem Hintergrund dieser nicht eindeutigen Äußerung spricht nichts dagegen, dass der Gesetzgeber auch weiterhin an einer Regelung festhalten will, die offensichtlich an die Parallelregelung der StPO (§ 110b Abs. 2) angelehnt ist.

Bayreuth, den 14.3.2017

Prof. Dr. Markus Möstl

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)806 C

# Anhörung des Präsidenten des Bundeskriminalamtes

# Holger Münch

# vor dem Innenausschuss des Bundestages

# am 20. März 2017

# zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

## (Drs. 18/11163, 18/11326)

Einleitung

Im Jahre 2009 hat der Gesetzgeber dem Bundeskriminalamt für bestimmte Fallkonstellationen die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus übertragen, um praktische Hindernisse in der Aufspaltung der Kompetenzen zwischen dem Bund und den Ländern in Fällen hoher terroristischer Bedrohung zu vermeiden; diese Aufgabe hat seitdem aufgrund der weiteren Entwicklung des islamistischen Terrorismus in Deutschland und in unseren europäischen Nachbarländern eher an Bedeutung zugenommen als eingebüßt.

Die dieser Aufgabenwahrnehmung entsprechenden Befugnisse nach §§ 20a ff. BKAG - im Gesetzentwurf nunmehr §§ 38 ff. - wurden seit Einführung im Jahre 2009 sowohl im Allgemeinen als auch im Einzelnen kontrovers diskutiert. Das Bundesverfassungsgericht hat mit Urteil vom 20. April 2016 Klarheit geschaffen und grundsätzlich die Notwendigkeit und Zulässigkeit dieser Aufgaben- und Befugnisnormen anerkannt. Das Bundesverfassungsgericht hat weder die dem Bundeskriminalamt zugewiesene Gefahrenabwehraufgabe im Bereich internationaler Terrorismus an sich, noch eine der zahlreichen, insbesondere verdeckten Befugnisse in Gänze für verfassungswidrig erklärt.

Lediglich wird bei einzelnen Vorschriften die im Tatbestand formulierte Vorgabe für ihre Umsetzung und der fehlende Umfang der Einrichtung von Schutzmechanismen beanstandet, es sind Verfahrensregelungen einschließlich Vorgaben für die Datenverwendung vom Gesetzgeber zu schaffen. Diese verfassungsrechtlich notwendigen Anpassungen werden durch den vorliegenden Gesetzentwurf vorgenommen.

Hypothetische Datenneuerhebung und Reform der polizeilichen IT-Architektur

Das Bundesverfassungsgericht hat nach eigener Aussage ein Grundsatzurteil zum polizeilichen Datenschutz gefällt. Die verfassungsrechtlichen Vorgaben zur Verwendung und Weiterverwendung von Daten aus polizeilichen Maßnahmen werden im Gesetzentwurf insbesondere durch die §§ 12 und 14 konkretisiert. Das Prinzip der sogenannten hypothetischen Datenneuerhebung gilt nach den Ausführungen des Bundesverfassungsgerichts explizit für verdeckte Maßnahmen mit erheblicher Eingriffstiefe wie für die Wohnraumüberwachung, Onlinedurchsuchung, Telekommunikationsüberwachung oder längerfristige Observation im Zusammenhang mit der Weiterverwendung von durch solche Maßnahmen gewonnenen Daten. Der vorliegende Gesetzentwurf erstreckt die Anwendung dieses Grundsatzes zur Stärkung des Datenschutzes in § 12 auf alle gewonnen Daten, ungeachtet dessen, aus welcher Maßnahme sie erwachsen.

Die Vorgaben des Bundesverfassungsgerichts waren Anlass, eine Reform der polizeilichen IT-Architektur zu beschließen und zügig mit deren Umsetzung zu beginnen. Diese grundlegende Entscheidung findet sich im § 2 Abs. 3 des Gesetzentwurfs wieder, nach dem das Bundeskriminalamt als Zentralstelle einen *einheitlichen* polizeilichen Informationsverbund unterhält.

Das Bundesverfassungsgericht hat keine Vorgaben zur Umsetzung und Einhaltung des Prinzips der hypothetischen Datenneuerhebung aufgestellt, auch nicht in technischer Hinsicht, jedoch ist es Aufgabe des Gesetzgebers und der mit diesen Vorgaben letztlich im Polizeialltag befassten Akteure eine praxisgerechte Lösung für diese Anforderungen zu entwickeln. Die tägliche Information und Kommunikation im Rahmen des nationalen und internationalen polizeilichen Dienstverkehrs - das Herzstück unserer Zentralstellenaufgabe ! - darf durch unpraktikable Anforderungen nicht erschwert oder gar vereitelt werden. Trotz Übergangsfrist bis zum 30. Juni 2018 stellte sich daher für das Bundeskriminalamt in Abstimmung mit dem Bundesinnenministerium unmittelbar

nach Urteilsverkündung die Frage nach gangbaren Lösungen zur Umsetzung und Implementierung dieser Vorgaben. Dabei kamen wir sehr schnell zu dem Schluss, dass dieses Ziel nur durch Anpassung IT-basierter Rahmenbedingungen erreicht werden kann, denn die Gewährleistung dafür, dass die jeweilig Eingriffstiefe der Datenerhebungsmaßnahme nach den Grundsätzen der hypothetischen Datenneuerhebung bei der weiteren Datenverwendung umfassend in die Entscheidung über eine Datenverwendung einfließt, kann nur mit einer einheitlichen Kennzeichnungspflicht und Systematik bei allen Polizeien des Bundes und der Länder erfolgen.

Darüber hinaus ist eine grundlegende und vor allem einheitliche Neukonzeption der polizeilichen IT-Architektur dringend geboten, um die bisherigen Schwierigkeiten, die durch die zersplitterte IT-Landschaft mit ihren nur teilweise kompatiblen Systemen bei den Polizeien des Bundes und der Länder bedingt sind, zu beheben. Die effektive und grundrechtsschonende Verknüpfung bereits vorhandener Daten ist für die polizeiliche Arbeit und damit der Gewährleistung der inneren Sicherheit nicht weniger ausschlaggebend, als die Befugnisse zur originären Erhebung dieser Daten selbst. Das diesem Gesetzentwurf zugrundeliegende Bekenntnis zur Schaffung eines übergreifenden Informationssystems ist aus polizeilicher Sicht alternativlos.

Weiterer Modernisierung der Zentralstelle

Über diese spezifische Anpassung der Zentralstellenaufgabe hinaus verfolgt der Gesetzentwurf das Ziel der Modernisierung der Zentralstellenfunktion des Bundeskriminalamts insgesamt. Nicht zuletzt aufgrund der steten Herausforderungen, die das föderale System in unserem Land mit sich bringt, sind zeitgemäße und praxisgerechte Regelungen notwendig, welche die erforderliche Koordinierungs- und Unterstützungsaufgaben für die Polizeien von Bund und Länder bei der Verhütung und Verfolgung von Straftaten durch das Bundeskriminalamt gewährleisten. Diese befinden sich im Gesetzentwurf vor allem in § 2 für die Zentralstellenaufgabe des BKA:

Neben der Abgrenzung zwischen Koordination und Beratung einerseits und dem Angebot sogenannter „Spezial-Services“ andererseits ist hier vor allem die gesetzliche Grundlage zur Schaffung sogenannter Kompetenzzentren gem. § 2 Abs. 5 Nr. 2 des Gesetzentwurfs zu erwähnen. Insbesondere in den Bereichen der Informations-, Einsatz- und Kriminaltechnik, deren Grundlagen und Entwicklungen grundsätzlich für alle Polizeien gleichermaßen von Bedeutung sind, dürfen unsere wertvollen personellen

und sachlichen Ressourcen nicht für Doppelarbeit oder Kooperationsmängel vergeudet werden. Durch eine Regelung zur Errichtung von Kompetenzzentren beim Bundeskriminalamt wird nunmehr eine rechtssichere Form der Zusammenarbeit eröffnet, die durch Nutzung von Synergieeffekten einen effektiven und effizienten Ansatz zur Bewältigung übergeordneter polizeilicher Herausforderungen bietet.
Wesentlicher Teil der Zentralstelle bleibt indes die allgemeine Auswertung und Analyse gesammelter Informationen in operativer und strategischer Hinsicht. Diese Tätigkeit ist notwendige Bedingung zur Erlangung von unverzichtbarem Hintergrundwissen zu unterschiedlichsten Kriminalitätsfeldern und dient als elementare Grundlage für daraus resultierende kriminalstrategische Überlegungen. Die Hervorhebung der Bedeutung und die Stärkung dieses Aufgabengebiets durch § 2 Abs. 6 Nr. 1 des Gesetzentwurfs wird daher uneingeschränkt begrüßt. Auch hier gilt das bereits oben erwähnte Gebot, aus bereits vorhandenen Daten die größtmögliche Aussagekraft für die polizeiliche Arbeit zu extrahieren und dieses Wissen mit anderen Polizei- und Sicherheitsbehörden zu teilen.

Erleichterung des Informationsaustausches innerhalb der EU

Die Optimierung der Nutzung und Teilung vorhandenen polizeilichen Wissens im nationalen Bereich ist unabdingbar, muss aber auch im internationalen Bereich intensiviert werden. Ebenso wie organisierte Kriminalität und Terrorismus nicht an den Landesgrenzen Halt machen, darf der polizeiliche Informationsaustausch im Zeitalter der Globalisierung durch geographische Grenzen und nationalstaatlichen Einzelregelungen erschwert werden, solange es keine gerechtfertigten Gründe für Restriktionen gibt. Bezüglich des Datenaustauschs mit der Europäischen Union als einer Werte- und Rechtsgemeinschaft, die die Einhaltung der Grund- und Menschenrechte und ein einheitliches Datenschutzniveau gewährleistet, sind keine solchen Gründe ersichtlich. Somit ist der § 26 des vorliegenden Gesetzentwurfs, der eine Gleichstellung der Voraussetzungen der Datenübermittlung im Inland mit der Datenübermittlung an das EU-Ausland vorsieht, wesentliche Grundlage für die Erfüllung unserer Aufgaben sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung.

Anpassung und Erweiterung einzelner Befugnisnormen, elektronische Aufenthaltsüberwachung

Anlässlich der ohnehin notwendigen Neustrukturierung des Bundeskriminalamtgesetzes wurde die Gelegenheit genutzt, unsere Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus sowie zur Wahrnehmung der Zentralstellenaufgabe und der Strafverfolgung über die Vorgaben des Bundesverfassungsgerichts hinaus anzupassen und maßvoll zu erweitern. Die Bewältigung unserer Aufgaben und somit auch die Gewährleistung der inneren Sicherheit hängen nicht zuletzt vom Vorhandensein eines angemessenen polizeilichen Instrumentenkastens ab. Die Ausweitung unserer Befugnisse beschränkt sich im Wesentlichen auf Maßnahmen, die anderen Polizeibehörden überwiegend schon lange zur Verfügung stehen - beispielsweise die Befugnis zur nationalen und internationalen Ausschreibung von Personen zur gezielten Kontrolle (als offene Maßnahme im Unterschied zur „polizeilichen Beobachtung“, einer verdeckten Maßnahme) gem. § 33 des Gesetzentwurfs - , oder die bereits zum festen Bestandteil der Strafprozessordnung gehören - wie die Postbeschlagnahme, eingefügt in § 50 des Gesetzentwurfs.

Ein Novum hingegen ist die elektronische Aufenthaltsüberwachung zur Verhütung und Abwehr von Gefahren des internationalen Terrorismus. Die Regelung zur sogenannten „Fußfessel“ (§ 56 BKAG-E) soll ebenso wie die Ermächtigungsgrundlage zur Verhängung von Aufenthalts- und Kontaktverboten (§ 55 BKAG-E) bereits am Tag nach der Verkündung des Gesetzes bis 25. Mai 2018 - dem vorgesehenen Zeitpunkt des Inkrafttretens des Gesetzes im Übrigen - als §§ 20y/20z in Kraft treten. Für das BKA beschränkt sich diese Befugnis im neuen BKAG auf Ausnahmefälle der eigenen, originären Aufgabenwahrnehmung zur Abwehr von Gefahren des internationalen Terrorismus in Fällen, in denen die Zuständigkeit eines Landes noch nicht erkennbar ist, eine länderübergreifende Gefahr vorliegt oder ein Land um Übernahme ersucht (§ 4a BKAG, künftig § 5 BKAG-neu).

Vor allem die elektronische Aufenthaltsüberwachung zur Gefahrenabwehr steht im Fokus der öffentlichen Diskussion. Immer wieder werden Stimmen laut, die die Verhütung und Verhinderung von Anschlägen durch die elektronische Aufenthaltsüberwachung bezweifeln und daher den Sinn der Maßnahme als Ganzes in Frage stellen oder als pure Gesetzessymbolik zur Erzeugung eines trügerischen Sicherheitsgefühls ansehen. Aus diesem Grund möchte ich erneut betonen, dass sowohl Aufenthalts- und Kontaktverbote als auch die elektronische Aufenthaltsüberwachung schlicht als weitere Maßnahmen zu verstehen sind, die unseren polizeilichen Instrumentenkasten vervoll-

ständigen, aber keinesfalls als Patentlösungen - schon gar nicht isoliert betrachtet - zur Verhinderung von Anschlägen dargestellt werden dürfen. Dennoch bieten uns diese Maßnahmen wertvolle Ansätze zur Verhütung und Abwehr von Gefahren des internationalen Terrorismus, in einem derart sensiblen Aufgabenbereich, in dem wir das Risiko von Informationsverlusten allein schon in Form der Unkenntnis über den Aufenthalt eines polizeilich detektierten sog. Gefährders nicht eingehen dürfen. Dem staatlichen Schutzauftrag und der berechtigten Erwartungshaltung der Bevölkerung würden wir nicht gerecht. Neben der Möglichkeit, Personen, von denen die Gefahr der Begehung einer terroristischen Straftat im Sinne des § 5 Abs. 1 S. 2 BKAG-E ausgeht, Betretungsverbote für potentielle Anschlagsziele - regelmäßig durch richterliche Anordnung - aufzuerlegen, kann durch Einsatz der „Fußfessel“ sichergestellt werden, dass ein solcher „Gefährder“ sich den Blicken der Sicherheitsbehörden nicht generell entziehen kann und bei Bedarf ein schnelles Eingreifen der Polizei realisierbar ist.

FAZIT:

Die Neustrukturierung des Bundeskriminalamtsgesetz und der damit einhergehenden Aufgaben des Bundeskriminalamts, insbesondere die Schaffung einer zukunftsfähigen, polizeifachgemäßen Neugestaltung der polizeilichen IT-Architektur, stellen derzeit eine der größten Herausforderungen im Bundeskriminalamt dar. Die dazu nötigen Änderungen und Prozesse eröffnen gleichzeitig die Chance, das Bundeskriminalamt zu einer modernen, zukunftsfähigen Zentralstelle zu entwickeln. Der vorliegende Gesetzentwurf stellt eine grundlegende Basis zur Erreichung dieses Zieles dar. Zudem wird durch teilweise Änderung der Gefahrenabwehrbefugnisse der polizeiliche Instrumentenkasten bedarfsgerecht angepasst.

Der Aufwand zur Erfüllung der gesetzgeberischen bzw. verfassungsrechtlichen Vorgaben kann indes keinesfalls als gering bezeichnet werden. Dies gilt zwar vor allem für die Ausrichtung der polizeilichen IT-Architektur an den Grundsatz der hypothetischen Datenneuerhebung, beschränkt sich aber nicht auf dieses Aufgabenfeld. Nicht zuletzt die durch das Bundesverfassungsgericht erheblich ausgeweiteten Dokumentations-, Statistik- und Berichtspflichten werden zukünftig personelle Ressourcen spürbar in Anspruch nehmen. Auch die Durchführung einzelner Maßnahmen wird partiell auf-

wändiger. Dies gilt etwa für die strengeren Vorgaben zur Gewährleistung des Kernbereichsschutzes privater Lebensgestaltung. Während Regelungen zum Kernbereichsschutz sich nach Maßgabe des Bundesverfassungsgerichts auf weitere verdeckte Maßnahmen erstrecken, also quantitativ ausgeweitet wurden - z.B. auf die längerfristige Observation - , erfolgte auch eine qualitative Steigerung der Anforderungen darüber hinaus für die Maßnahmen der Wohnraumüberwachung und Onlinedurchsuchung: Hier ist die unverzügliche Prüfung **sämtlicher** Daten aus diesen beiden Maßnahmen auf Kernbereichsrelevanz durch eine „unabhängige Stelle“ (im Aufgabenfeld des Bundeskriminalamtes zur Abwehr von Gefahren des internationalen Terrorismus ist dies gemäß BKAG das AG Wiesbaden) gefordert, bindet weitere zusätzliche Ressourcen, nicht nur auf Seiten des Bundeskriminalamtes, sondern auch auf Seiten der Justiz.

Voraussetzung für die polizeiliche Arbeit ist Rechtssicherheit. Die Vorschriften zur Neustrukturierung des Bundeskriminalamtgesetzes gewährleisten die Ausübung unserer Arbeit in verfassungskonformer und datenschutzfreundlicher Weise. Die Umsetzung der verschiedenen Zielrichtungen des Gesetzentwurfs gewährt dem Bundeskriminalamt zukünftig die notwendige Basis für eine verfassungsgemäße, moderne Aufgabenwahrnehmung.

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 D

Prof. Dr. Matthias Bäcker, LL.M.

Johannes Gutenberg-Universität Mainz
Abt. Rechtswissenschaft

Jakob-Welder-Weg 9
55128 Mainz

Mainz, den 16. März 2017

# Stellungnahme

zu dem Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

(BT-Drs. 18/11163)

## Gliederung

**Ergebnisse**

1. Die geplanten Ermächtigungen zur Weiterarbeitung erhobener Daten in § 16 Abs. 1, § 18 und § 19 BKAG-E weisen grundlegende konzeptionelle Defizite auf. Der Gehalt dieser Normen ist in wesentlichen Punkten unklar. Je nach Interpretation geben sie die Bevorratung erhobener Daten und deren weitere Nutzung in verfassungswidrig großem Ausmaß frei, sie könnten jedoch – gerade umgekehrt – auch zu einer verfassungsrechtlich nicht erforderlichen und kaum praktikablen Einschränkung der Informationsverwaltung bei dem Bundeskriminalamt führen.

2. Diese Defizite lassen sich nicht durch punktuelle Anpassungen beheben. Vielmehr bedarf es einer weitaus differenzierteren Regulierung unterschiedlicher Verarbeitungsphasen (insb. weitere Nutzung erhobener Daten im unmittelbaren Anschluss an das Ausgangsverfahren, Bevorratung erhobener Daten über das Ausgangsverfahren hinaus, Verwertung bevorrateter Daten) und unterschiedlicher Personenkategorien, als sie der Entwurf vorsieht.

3. Der Entwurf droht sein Ziel, die durch Dateien strukturierte Informationsordnung bei dem Bundeskriminalamt auf einen einheitlichen Informationsbestand umzustellen, sowohl in verfassungsrechtlicher als auch in polizeipraktischer Perspektive zu verfehlen. Die rechtliche Strukturierung des vorgesehenen einheitlichen Informationsbestands ist als überaus komplexe, bislang nicht bewältigte Aufgabe anzusehen. Ich rate daher dringend dazu, diesen Teil des Entwurfs vorerst zurückzustellen und zunächst eine die praktischen Bedürfnisse, verfassungsrechtlichen Anforderungen und gesetzgebungstechnischen Regelungsoptionen eingehend zu analysieren.

4. Darüber hinaus weisen die Regelungen über die Weiterverarbeitung von Daten weitere weniger grundlegende, aber gleichwohl erhebliche praktische und verfassungsrechtliche Defizite auf.

    a) § 12 BKAG-E beschränkt die weitere Nutzung erhobener Daten sowie die Zweckänderung von Daten, die mit „Online-Durchsuchungen“ gewonnen wurden, über das verfassungsrechtlich erforderliche Maß hinaus. Insbesondere die Einschränkung der weiteren Nutzung dürfte schwierig zu handhaben sein und sollte behoben werden.

    b) Die Ermächtigungen zu Datenbevorratungen in § 18 und § 19 BKAG-E lehnen sich an § 8 BKAG an und sind ebenso wie diese Norm teils zu unbestimmt und unverhältnismäßig.

    c) Die neue Ermächtigung zur anlasslosen Hinzuspeicherung ermittlungsunterstützender Hinweise in § 16 Abs. 6 Nr. 2 BKAG-E steht so mit dem Verhältnismäßigkeitsgrundsatz nicht in Einklang.

    d) Die Regelung über die Aussonderungsprüffrist in § 77 Abs. 3 BKAG-E ermöglicht dem Bundeskriminalamt, einmal erhobene Daten ohne Prüfung über sehr lange Zeiträume gespeichert zu halten. Ein rechtfertigender Grund hierfür ist nicht erkennbar.

**Stellungnahme**

Eine umfassende Stellungnahme zu einem 131 Seiten umfassenden, inhaltlich sehr komplexen Gesetzentwurf erfordert mehr Zeit, als den Sachverständigen zur Verfügung gestellt wurde. Meine Stellungnahme beschränkt sich daher – ohne dass damit eine Aussage zur Praktikabilität oder zur Verfassungskonformität des Entwurfs im Übrigen verbunden wäre – auf einen kleinen, allerdings bedeutsamen Teil des Entwurfs:[1] die Regelungen über die Weiterverarbeitung erhobener Daten in §§ 12 ff. BKAG-E, die sowohl dem in § 13 BKAG-E vorgesehenen Informationssystem des Bundeskriminalamts als auch dem durch §§ 29 ff. BKAG-E errichteten polizeilichen Informationsverbund[2] zugrunde liegen. Diese Regelungen stellen den wohl anspruchsvollsten Teil des Entwurfs dar, da sie die Informationsordnung bei dem Bundeskriminalamt grundlegend umgestalten sollen.[3] Jedoch werden sie dieses Ziel aufgrund konzeptioneller Defizite nicht erreichen (unten I). Darüber hinaus werfen die vorgesehenen Regelungen zur Weiterverarbeitung erhobener Daten weitere weniger fundamentale, aber gleichwohl erhebliche verfassungsrechtliche und praktische Probleme auf (unten II).

**I. Konzeptionelle Defizite der Weiterverarbeitungsregelungen**

Von zentraler Bedeutung für das Informationssystem und den polizeilichen Informationsverbund sind die Weiterverarbeitungsermächtigungen in § 16, § 18 und § 19 BKAG-E. Diese Regelungen weisen grundlegende konzeptionelle Mängel auf und drohen schwerwiegende Fehlsteuerungen zu bewirken: Die allgemeine Weiterverarbeitungsermächtigung in § 16 Abs. 1 BKAG-E ist viel zu weit gefasst und so verfassungsrechtlich nicht haltbar (unten 1). Die besonderen Ermächtigungen in § 18 und § 19 BKAG-E sind unklar. Sie können einerseits so verstanden werden, dass sie gleichfalls zu weit reichen und Grundrechte verletzen. Andererseits ist auch eine Interpretation möglich und naheliegend, nach der diese Normen für die Informationsordnung des Bundeskriminalamts praktisch nicht umsetzbare und verfassungsrechtlich nicht geforderte Hürden errichten (unten 2). Die Mängel dieser Regelungen lassen sich nicht mit punktuellen Änderungen des Entwurfs abstellen. Dieser Befund berührt allerdings die beabsichtigte Neugliederung der Informationsordnung des Bundeskriminalamts fundamental. Dieses Vorhaben sollte daher zurückgestellt werden, bis die derzeit offene Frage geklärt ist, ob sich hierfür grundrechtskonforme und praktikable Rechtsgrundlagen finden lassen (unten 3).

**1. Reichweite und Anforderungen von § 16 Abs. 1 BKAG-E als eigenständiger Verarbeitungsermächtigung**

Die allgemeine Ermächtigung zur Weiterverarbeitung erhobener Daten in § 16 Abs. 1 BKAG-E wirft Fragen hinsichtlich ihrer genauen Reichweite und der in ihr enthaltenen Anforderungen auf.

Nach der Entwurfsbegründung soll § 16 Abs. 1 BKAG-E der bisherigen Rechtslage entsprechen. Die Begründung verweist auf die derzeitigen Regelungen in § 7 Abs. 10 und § 13 Abs. 1,

[1] Vgl. zu den vorgesehenen Befugnissen zur Terrorismusabwehr die Stellungnahme von Ulf Buermeyer.

[2] Vgl. § 29 Abs. 4 Satz 2 BKAG-E.

[3] Vgl. zu diesem Ziel des Entwurfs BT-Drs. 18/11163, S. 73.

Abs. 4 BKAG, die es erlauben, Daten zwischen der Zentralstellenaufgabe und den anderen Aufgaben des Bundeskriminalamts zu verschieben.[4]

Der Anwendungsbereich von § 16 Abs. 1 BKAG reicht jedoch über diese spezifischen Zweckänderungen nach dem Wortlaut der vorgesehenen Norm weit hinaus. Insbesondere erwähnt die Begründung nicht, dass das Bundeskriminalamt auf der Grundlage dieser Regelung personenbezogene Daten auch im Rahmen der ursprünglichen Aufgabe weiterverarbeiten kann. Diese Verarbeitungsbefugnis reicht potenziell sehr weit, wie im Folgenden anhand der Aufgabe zur Terrorismusabwehr (§ 5 BKAG-E) gezeigt werden soll.

Im Rahmen dieser Aufgabe handelt das Bundeskriminalamt durchweg zur Verhütung und Abwehr von Gefahren für besonders gewichtige Rechtsgüter. Ist die Aufgabe des § 5 BKAG-E eröffnet, sind daher zumindest in aller Regel die Rechtsgüter bedroht, die in den Ermächtigungen zu eingriffsintensiven Datenerhebungsmaßnahmen (wie Telekommunikationsüberwachungen oder Bild- und Tonaufzeichnungen außerhalb von Wohnungen) genannt werden.[5] Will das Bundeskriminalamt Daten weiterverarbeiten, die es zur Erfüllung dieser Aufgabe erhoben hat, unterfällt die Weiterverarbeitung deshalb grundsätzlich[6] § 12 Abs. 1 Satz 1 BKAG-E.[7] Die Weiterverarbeitung hängt also nicht davon ab, dass ein konkreter Ermittlungsansatz i.S.v. § 12 Abs. 2 BKAG vorliegt. § 16 Abs. 1 BKAG-E verlangt darüber hinaus lediglich, dass die Weiterverarbeitung für die Erfüllung der Aufgabe aus § 5 BKAG erforderlich ist. Dies ist eine niedrigschwellige Voraussetzung.[8]

Auf der Grundlage von § 16 Abs. 1 BKAG-E könnte das Bundeskriminalamt daher insbesondere nahezu alle personenbezogenen Daten, die es im Rahmen seiner Aufgabe zur Terrorismusabwehr erhoben hat, dauerhaft bevorraten, um sie später einmal im Rahmen dieser Aufgabe zu verwerten. Lediglich hinsichtlich der Frage, welche Daten genau das Bundeskriminalamt speichern darf, wären einschränkende Vorgaben in der von § 20 BKAG-E vorgesehenen Verordnung zu regeln.[9] Einen besonderen Speicherungsanlass, der über die – praktisch in der Regel bejahbare – Erforderlichkeit zur Aufgabenerfüllung hinausginge, sieht der Entwurf hingegen nicht vor. So könnte das Bundeskriminalamt neben Daten über „Gefährder“ auch Daten über Dritte ohne besonderen Anlass und in weitem Umfang bevorraten, soweit dies zur Aufgabenerfüllung beizutragen verspricht. Die aus § 79 Abs. 1 Satz 1 BKAG-E folgende Vorgabe, dass die im Rahmen der Terrorismusabwehr erhobenen Daten nach Zweckerreichung grundsätzlich zu löschen sind, stünde der Bevorratung nicht entgegen, da hiervon Daten ausgenommen sind, die nach den Vorschriften des Abschnitts 1 Unterabschnitt 2, also auch nach § 16 Abs. 1 BKAG-E, weiterverarbeitet werden. Schließlich wäre auch die Verwertung der bevorrateten

[4] BT-Drs. 18/11163, S. 94.

[5] Vgl. zum geltenden Recht BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 299 f.

[6] Eine Ausnahme bilden die unter § 12 Abs. 1 Satz 2 BKAG-E fallenden besonders eingriffsintensiven Datenerhebungsmaßnahmen, die in diesem Abschnitt außer Betracht bleiben.

[7] Vgl. zu der missverständlichen, aber leicht korrigierbaren Formulierung dieser Norm unten II. 1. a).

[8] Vgl. zur problematischen Interpretation dieses Eingriffstatbestands Bäcker, Kriminalpräventionsrecht, 2015, S. 233 f., 508.

[9] Der Erlass dieser Verordnung ist daher als Voraussetzung der Datenweiterverarbeitung anzusehen, vgl. für das geltende Recht BVerwG, Urteil vom 9. Juni 2010 – 6 C 5/09 –, juris, Rn. 20.

Daten, die wiederum auf § 16 Abs. 1 BKAG-E zu stützen wäre, dem Bundeskriminalamt weitgehend freigestellt.

Eine so weitreichende Bevorratungsbefugnis steht mit den Grundrechten nicht in Einklang. Sie lässt sich insbesondere nicht auf das BKAG-Urteil des Bundesverfassungsgerichts stützen. Das Bundesverfassungsgericht hat zwar die mit § 16 Abs. 1 BKAG-E vergleichbare Vorschrift des § 20v Abs. 4 Satz 2 Nr. 1 BKAG grundsätzlich für verfassungskonform gehalten.[10] Das Gericht hatte jedoch bei der Prüfung dieser Norm ersichtlich nicht die hier erörterte Datenbevorratung, sondern allein eine Nutzung im Rahmen derselben Aufgabe vor Augen, die unmittelbar an die Datenerhebung oder zumindest an das dieser Datenerhebung zugrundeliegende polizeiliche Verfahren anschließt. Es ging dem Gericht also in gebräuchlicher Terminologie im Wesentlichen um Zufallsfunde. Ob das Gericht damit den Regelungsgehalt von § 20v Abs. 4 Satz 2 Nr. 1 BKAG zutreffend bzw. vollständig erfasst hat, ist insofern unerheblich.

Dass das Bundesverfassungsgericht sich lediglich mit der unmittelbaren Anschlussnutzung befasst hat, ergibt sich zum einen daraus, dass es den in § 20v Abs. 4 Satz 2 Nr. 1 BKAG vorgesehenen Datenumgang als weitere Nutzung bezeichnet hat.[11] Nach der damit in Bezug genommenen Terminologie des noch geltenden Datenschutzrechts ist eine Datenspeicherung gerade keine Datennutzung.[12] Zum anderen betont das Bundesverfassungsgericht, dass von der Befugnis zur weiteren Nutzung der Daten die Pflicht unberührt bleibe, die Daten nach Erreichung des mit der Erhebung verfolgten Zwecks zu löschen.[13] Dieser Hinweis ergäbe keinen Sinn, wenn das Gericht § 20v Abs. 4 Satz 2 Nr. 1 BKAG als Ermächtigung zur Datenspeicherung verstanden hätte, da dann die Norm gerade eine Datenbevorratung über den Erhebungszweck hinaus vorsähe. Dementsprechend heißt es an anderer Stelle in dem Urteil, dass von der Löschung erhobener Daten über den unmittelbaren Anlassfall hinaus nur dann abgesehen werden kann, wenn sich aus den Daten konkrete Ermittlungsansätze ergeben.[14]

Stattdessen ist § 16 Abs. 1 BKAG-E als Bevorratungsermächtigung an den Maßstäben zu messen, die sich aus der Rechtsprechung zur Bevorratung von Daten für sicherheitsbehördliche Zwecke ergeben. Die Eingriffsintensität der durch die vorgesehene Norm ermöglichten Datenbevorratung ist als hoch anzusehen, da die Bevorratungsermächtigung sachlich sehr weit reicht und Daten aus eingriffsintensiven Ermittlungsmaßnahmen einschließt. Die Daten können somit weitreichende Schlüsse über die betroffenen Personen ermöglichen und Einblicke in besonders schutzwürdige Rückzugsbereiche der Privatheit eröffnen.[15] Die Datenbevorratung bedarf daher eines hinreichenden Anlasses,[16] zudem muss dem Eingriffsgewicht der Bevorratung auf der

[10] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 294 ff.

[11] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 296.

[12] Vgl. § 3 Abs. 4 Satz 1, Abs. 5 BDSG.

[13] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 301.

[14] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 270.

[15] Vgl. zu den maßgeblichen Intensitätskriterien BVerfGE 125, 260 (318 ff.); 130, 151 (188 ff.).

[16] Vgl. BVerfGE 133, 277 (339 ff.); EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele2 Sverige u.a., Rn. 96 ff.; EGMR, Urteil vom 4. Dezember 2008, No. 30562/04 und 30566/04 – S. und Marper gegen Vereinigtes Königreich, §§ 101 ff.

Ebene der Datenverwertung Rechnung getragen werden.[17] Die vorgesehene Regelung in § 16 Abs. 1 BKAG-E, welche sowohl die Datenspeicherung als auch die Datenverwertung weitgehend freigibt, leistet dies nicht ansatzweise.[18]

**2. Verhältnis der Verarbeitungsermächtigungen in § 18 und § 19 BKAG-E zu § 16 Abs. 1 und § 12 BKAG-E**

In § 18 und § 19 BKAG-E finden sich Ermächtigungen zur Weiterverarbeitung von Daten im Rahmen der Zentralstellenaufgabe des Bundeskriminalamts sowie (aufgrund des Verweises aus § 16 Abs. 3 BKAG-E) zur Vorsorge für die Verfolgung von Straftaten. Inhaltlich lehnen sich diese Ermächtigungen an § 8 BKAG an, so dass auf den ersten Blick ihr Gehalt klar zu sein scheint, wenngleich damit auch die rechtsstaatlichen Bedenken bestehen bleiben, die gegen einige der Regelungen in § 8 BKAG seit geraumer Zeit erhoben werden.[19]

Bei näherer Betrachtung werfen § 18 und § 19 BKAG-E allerdings erhebliche neue Auslegungsprobleme auf. Unmittelbarer gesetzessystematischer Grund hierfür ist, dass das Verhältnis dieser Normen zu § 16 Abs. 1 und mittelbar zu § 12 BKAG-E unklar ist. Die Unklarheiten von § 18 und § 19 BKAG-E verweisen zugleich auf das tiefer liegende Problem, dass sich die von dem Bundesverfassungsgericht erarbeiteten Anforderungen an die zweckändernde Weiterverarbeitung von Daten nicht bruchlos auf die längerfristige Bevorratung von Daten übertragen lassen, wie es der Gesetzentwurf versucht. Zur rechtlichen Steuerung eines über längere Zeit bevorrateten Informationsbestands bedarf es vielmehr differenzierterer Regelungen.

Die in § 16 Abs. 1 BKAG-E enthaltenen Tatbestandsvoraussetzungen für eine Weiterverarbeitung von Daten sind zu beachten, „soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht." Aus § 18 und § 19 BKAG-E ergeben sich für die Weiterverarbeitung von Daten spezifische Anforderungen, die über die Anforderungen aus § 16 Abs. 1 BKAG-E insoweit hinausgehen, als die Erforderlichkeit für die Aufgabenerfüllung nicht ausreicht, um die Weiterverarbeitung zu legitimieren. Vielmehr enthalten diese Regelungen ein Gefüge von Anlässen für eine Weiterverarbeitung im Informationssystem bzw. im Informationsverbund. Insofern enthalten § 18 und § 19 BKAG-E im Vergleich mit § 16 Abs. 1 BKAG-E eindeutig „zusätzliche besondere Voraussetzungen".

Allerdings verweist § 16 Abs. 1 BKAG-E wegen der Voraussetzungen einer Datenweiterverarbeitung auch auf § 12 BKAG-E, während § 18 und § 19 BKAG-E keinen solchen Verweis enthalten. Da eine Weiterverarbeitung im Rahmen der Zentralstellenaufgabe in aller Regel eine Zweckänderung bewirkt,[20] stellt sich insbesondere die Frage, ob diese Weiterverarbeitung an das Erfordernis einer hypothetischen Datenneuerhebung gemäß § 12 Abs. 2 BKAG-E geknüpft ist. Der Wortlaut von § 16 Abs. 1 BKAG, demzufolge diese Norm nur insoweit als subsidiär zurücktritt, als eine andere Regelung *zusätzliche* Voraussetzungen errichtet, spricht eher dafür,

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

[18] Vgl. zur Speicherung in der Antiterrordatei BVerfGE 133, 277 (340).

[19] Zu ihnen unten II. 2.

[20] Eine Ausnahme bildet die Weiterverarbeitung von Daten, die das Bundeskriminalamt auf der Grundlage von § 9 Abs. 1 oder § 10 BKAG-E von vornherein im Rahmen seiner Zentralstellenaufgabe erhoben hat – jedenfalls wenn man die Zentralstellenaufgabe als *eine* einheitliche Aufgabe des Bundeskriminalamts begreift.

dass § 12 BKAG-E auch im Rahmen von § 18 und § 19 BKAG-E zu prüfen ist. Die Entwurfsbegründung scheint eher vom Gegenteil auszugehen. Zu § 16 Abs. 1 BKAG-E heißt es dort, „dass speziellere Weiterverarbeitungsbefugnisse der Norm vorgehen."[21] In den Ausführungen zu § 18 und § 19 BKAG-E wird § 12 BKAG-E nicht erwähnt.

Damit sind aufgrund von Wortlaut und Systematik des Gesetzentwurfs zwei Auslegungsvarianten denkbar: In der ersten Variante sind bei jeder Weiterverarbeitung auf der Grundlage von § 18 und § 19 BKAG-E zusätzlich zu den Tatbestandsvoraussetzungen dieser Normen auch die Voraussetzungen von § 12 BKAG-E zu prüfen. In der zweiten Variante ist § 12 BKAG-E in den Fällen der § 18 und § 19 BKAG-E nicht zu prüfen.

Misslich ist, dass keine der beiden Auslegungsvarianten zu befriedigenden Ergebnissen führt. Die gesetzlichen Weiterverarbeitungsermächtigungen sind in der ersten Auslegungsvariante nicht praxisgerecht, in der zweiten Auslegungsvariante sind sie verfassungswidrig.

*Auslegungsvariante 1: Anwendung von § 16 Abs. 1 i.V.m. § 12 BKAG-E*

Kaum praktikabel sind § 18 und § 19 BKAG-E, wenn die Weiterverarbeitung von Daten durchweg von der Prüfung einer hypothetischen Datenneuerhebung gem. § 12 Abs. 2 BKAG-E abhängig gemacht wird. Denn § 18 und § 19 BKAG-E dienen – ebenso wie der heutige § 8 BKAG – dazu, dass das Bundeskriminalamt im Rahmen seiner Zentralstellenfunktion Datenbestände für zukünftige, noch nicht konkret absehbare soziale Konflikte und daran anknüpfende polizeiliche Verfahren anlegen kann. Dementsprechend knüpfen diese Regelungen die Weiterverarbeitung an die strafprozessuale Stellung der betroffenen Person als Verurteilte oder Beschuldigte oder an ein prognostisches Urteil über die betroffene Person. Hingegen verlangen sie keine situationsbezogene Schadensprognose im Einzelfall.

Demgegenüber setzt nach § 12 Abs. 2 BKAG-E die zweckändernde Weiterverarbeitung von Daten einen konkreten Ermittlungsansatz voraus. Dies steht im Einklang mit dem BKAG-Urteil des Bundesverfassungsgerichts. Das Bundesverfassungsgericht führt zwar nicht näher aus, was genau ein konkreter Ermittlungsansatz ist. Aus dem Urteil geht jedoch hervor, dass dazu über einen „potenziellen Informationsgehalt" bestimmter Daten hinaus ein einzelfallbezogener tatsächlicher Anlass für die Weiterverarbeitung vorliegen muss.[22] Tragfähig erscheint insoweit die Entwurfsbegründung, nach der ein konkreter Ermittlungsansatz vorliegt, wenn „sich eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut darstellt."[23]

Ein konkreter Ermittlungsansatz müsste bei einer Anwendung von § 16 Abs. 1 i.V.m. § 12 BKAG-E auf § 18 und § 19 BKAG-E, die allgemein die Weiterverarbeitung von Daten im Rahmen der Zentralstellenaufgabe regeln, bei jeder einzelnen Weiterverarbeitungshandlung

[21] BT-Drs. 18-11163, S. 94.

[22] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 313.

[23] BT-Drs. 18/11163, S. 91.

und damit *bereits bei der Datenspeicherung* vorliegen. Die von § 18 und § 19 BKAG-E teilweise geforderten personenbezogenen Prognosen stellen für sich genommen nicht sicher, dass ein konkreter Ermittlungsansatz vorliegt. Erst recht folgt ein konkreter Ermittlungsansatz für die Zukunft nicht schon daraus, dass die betroffene Person einmal wegen einer Straftat verurteilt oder einer Straftat beschuldigt wurde. Die Datenspeicherung hinge also über die tatbestandlichen Voraussetzungen von § 18 und § 19 BKAG-E hinaus von einer situationsbezogenen Schadensprognose ab.

Daten, die durch eine Wohnraumüberwachung oder durch eine „Online-Durchsuchung" erlangt wurden, dürften darüber hinaus gem. § 12 Abs. 3 BKAG-E sogar nur gespeichert werden, wenn bereits zum Zeitpunkt der Speicherung eine konkrete Gefahr vorliegt.

Damit würden insgesamt die Speicherungsvoraussetzungen gegenüber der heutigen Rechtslage deutlich verschärft. In der Sache erscheint es kontraproduktiv, eine situationsbezogene Schadensprognose in Form eines konkreten Ermittlungsansatzes oder sogar einer konkreten Gefahr bereits zum Zeitpunkt der Datenspeicherung zu verlangen. Hierdurch würde das Ziel verfehlt, einen verfahrensübergreifenden Informationsbestand für noch nicht zwangsläufig absehbare zukünftige soziale Konflikte anzulegen. Die Zentralstellenaufgabe des Bundeskriminalamts würde erheblich beeinträchtigt.

*Auslegungsvariante 2: Keine Anwendung von § 16 Abs. 1 i.V.m. § 12 BKAG-E*

Andererseits sind § 18 und § 19 BKAG-E verfassungswidrig, wenn davon ausgegangen wird, dass sie § 16 Abs. 1 BKAG-E vollständig verdrängen, so dass auch § 12 BKAG-E nie zu prüfen ist.

In diesem Fall käme es bei der Weiterverarbeitung von Daten im Rahmen der Zentralstellenaufgabe überhaupt nicht auf die Voraussetzungen einer hypothetischen Datenneuerhebung an. Nicht nur die Speicherung, sondern auch die Verwertung der gespeicherten Daten hinge allein von den in § 18 und § 19 BKAG-E geregelten personenbezogenen Prognosen ab. Im Ergebnis dürften Daten, die einmal gespeichert werden dürfen, ohne weiteren Anlass in beliebiger Weise miteinander verknüpft und ausgewertet werden.

Wenn das Bundesverfassungsgericht aber für eine Datennutzung, die unmittelbar an die Erhebung anschließt, die Prüfung einer hypothetischen Datenneuerhebung verlangt,[24] muss dies (erst recht) auch für eine Nutzung gelten, die an eine zwischenzeitliche Datenspeicherung anschließt.

*Keine dritte Auslegungsvariante*

Nicht möglich ist es, § 18 und § 19 BKAG-E so auszulegen, dass eine hypothetische Datenneuerhebung nicht schon bei der Speicherung erhobener Daten, sondern erst bei der Verwertung der gespeicherten Daten zu prüfen ist. Dies wäre zwar am ehesten ein sinnvolles Regelungsmodell, das im Gesetzentwurf jedoch nicht angelegt ist, da die vorgesehenen Normen unterschiedslos die Weiterverarbeitung von Daten[25] und nicht lediglich ihre Speicherung oder Verwertung

[24] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 285, 303.

[25] Vgl. zur Definition dieses Begriffs BT-Drs. 18/11163, S. 87 f.

regeln. Dementsprechend kann für § 18 und § 19 BKAG-E nur einheitlich bestimmt werden, ob für die Weiterverarbeitung die Voraussetzungen auch von § 12 BKAG vorliegen müssen oder nicht.

**3. Fazit**

Die aufgezeigten Mängel von § 16, § 18 und § 19 BKAG-E sind struktureller Art und lassen sich nicht mit punktuellen Änderungen oder Ergänzungen des Entwurfs beheben. Vielmehr bedürfen die Weiterverarbeitungsermächtigungen einer Entflechtung und stärkeren Differenzierung.

Zunächst muss der Anwendungsbereich der in § 12 Abs. 1 BKAG-E geregelten weiteren Nutzung verkleinert werden. Als weitere Nutzung können nur solche Weiterverarbeitungen (nach bisheriger datenschutzrechtlicher Terminologie neben Nutzungen i.e.S. auch Datenveränderungen) zugelassen werden, die unmittelbar an das polizeiliche Verfahren anschließen, in dessen Rahmen die Daten erhoben wurden. Nach Abschluss dieses Verfahrens sind die erhobenen Daten hingegen zu löschen, wenn bis dahin kein konkreter Anlass für eine weitere Nutzung entstanden ist. Längerfristige, über den Zeitraum des Ausgangsverfahrens hinausgehende Datenspeicherungen im Informationssystem für die Zwecke zukünftiger Verfahren sind daher nicht als weitere Nutzung darstellbar.

Darüber hinaus müssen die Regelungen über die Datenbevorratung im Rahmen der Zentralstellenaufgabe stärker differenzieren. Datenspeicherung und Datenverwertung im Informationssystem lassen sich nicht einheitlich regeln, da sonst entweder praktische Erfordernisse oder verfassungsrechtliche Vorgaben verfehlt werden. Geboten ist eine getrennte Regulierung beider Verarbeitungsphasen:

Die Datenspeicherung ist danach an eine personenbezogene Prognose zu binden. Eines situationsbezogenen konkreten Ermittlungsansatzes bedarf es hingegen nicht. So hat das Bundesverfassungsgericht noch in jüngerer Zeit die Speicherungsregelungen des ATDG im Grundsatz akzeptiert, ohne als Grundlage der Datenspeicherung einen solchen Ermittlungsansatz zu fordern.[26]

Der Grundsatz der hypothetischen Datenneuerhebung ist jedoch bei der Verwertung der gespeicherten Daten zu beachten. Die personenbezogene Prognose, die der Datenspeicherung zugrunde liegt, legitimiert daher noch nicht die nachgelagerte Verwertung. Es bedarf hierfür vielmehr einer eigenständigen Ermächtigung, die einen von den Speicherungsvoraussetzungen unabhängigen Verwertungsanlass normiert.

Speicherungs- und Verwertungsermächtigung bedingen einander.[27] Je niedriger die gesetzlichen Anforderungen an die Datenspeicherung ausfallen, desto enger ist die Datenverwertung zu begrenzen.[28] Umgekehrt führen hohe Anforderungen an die Datenspeicherung dazu, dass

[26] Vgl. BVerfGE 133, 277 (339 ff.).

[27] Näher Bäcker, Kriminalpräventionsrecht, 2015, S. 502 ff.

[28] Vgl. zum Extremfall der anlasslosen und flächendeckenden Datenbevorratung BVerfGE 125, 260 (325 ff.).

die Datenverwertung in größerem Ausmaß erlaubt werden darf. Allerdings sind auf beiden Ebenen Minimalanforderungen zu beachten.[29]

Auch wegen dieser Wechselwirkung von Speicherung und Verwertung liegt es nahe, dass sich einheitliche Speicherungs- und Verwertungsermächtigungen für alle Aufgaben des Bundeskriminalamts (in ihren unterschiedlichen Facetten) und alle betroffenen Personenkreise nicht finden lassen. Dieser Befund stellt den grundlegenden konzeptionellen Ansatz des Gesetzentwurfs in Frage, die hergebrachte Gliederung des Informationsbestands in Dateien aufzugeben und durch ein einheitliches Informationssystem bzw. einen einheitlichen Informationsverbund zu ersetzen, in die alle polizeilich relevanten Daten einfließen und die rechtlich primär durch den Grundsatz der hypothetischen Datenneuerhebung gesteuert werden. Für mich ist derzeit nicht absehbar, ob und wie sich diese Neugliederung erreichen lässt, ohne entweder Grundrechte zu verletzen oder polizeipraktisch unerwünschte, verfassungsrechtlich nicht gebotene Verarbeitungsbarrieren zu errichten.

Abweichend von meiner Gewohnheit, meine Stellungnahmen für parlamentarische Anhörungen auf die verfassungsrechtliche Würdigung der vorgesehenen Neuregelungen zu beschränken, möchte ich daher dringend empfehlen, die Neugliederung der Informationsordnung des Bundeskriminalamts zurückzustellen, da eine tragfähige rechtliche Fundierung ersichtlich zumindest bislang nicht gefunden wurde. Stattdessen sollte der Entwurf auf die Regelungen zur Neuordnung der Terrorismusabwehr reduziert werden, die allein unmittelbar durch das BKAG-Urteil des Bundesverfassungsgerichts berührt werden. Alle weiteren Vorhaben, die der Entwurf verfolgt, lassen sich gegebenenfalls noch in der nächsten Legislaturperiode abarbeiten. Insbesondere trifft die in der Entwurfsbegründung vertretene Auffassung nicht zu, aufgrund des BKAG-Urteils des Bundesverfassungsgerichts müsse die hergebrachte Informationsordnung des Bundeskriminalamts zwingend aufgelöst und neu strukturiert werden.[30] Die Begründung nennt keine konkrete Passage des Urteils, aus der sich eine so weitreichende Aussage ableiten ließe; eine solche Passage gibt es auch nicht. Zutreffend ist, dass die gegenwärtigen Regelungen über die Informationsordnung des Bundeskriminalamts nicht in jeder Hinsicht den grundrechtlichen Anforderungen genügen. Sie müssen an die jüngere Rechtsprechung des Bundesverfassungsgerichts wie auch anderer Höchstgerichte angepasst werden. Diese Aufgabe könnte aber auch im Rahmen der bisherigen Dateistruktur gelöst werden. Welcher Weg vorzugswürdig ist, sollte in einer vertieften Analyse geklärt werden, die polizeipraktische, verfassungsrechtliche und gesetzgebungstechnische Aspekte umfassend einbezieht.

[29] So lässt sich eine anlasslose und flächendeckende Bevorratung sensibler Daten entgegen dem BVerfG auch durch strenge Verwertungsvoraussetzungen nicht rechtfertigen, so nunmehr EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele2 Sverige u.a., Rn. 97 ff.

[30] BT-Drs. 18/11163, S. 2.

## II. Weitere verfassungsrechtliche und praktische Probleme der Weiterverarbeitungsregelungen

Über ihre grundlegenden konzeptionellen Mängel hinaus werfen die vorgesehenen Regelungen zur Weiterverarbeitung erhobener Daten weitere, eher punktuelle verfassungsrechtliche und praktische Probleme auf. Diese Probleme betreffen die Vorgaben für weitere Nutzung und Zweckänderung (unten 1), die Voraussetzungen einer Datenspeicherung im Rahmen der Zentralstellenaufgabe des Bundeskriminalamts (unten 2), die Ermächtigung zur Speicherung sogenannter ermittlungsunterstützender Hinweise (unten 3) sowie die Regelung über den Beginn der Frist zur Löschung gespeicherter Daten (unten 4).

### 1. Zweckbindung und hypothetische Datenneuerhebung (§ 12 BKAG-E)

Die Regelungen in § 12 BKAG-E sind ersichtlich an das BKAG-Urteil des Bundesverfassungsgerichts angelehnt. In zweifacher Hinsicht sind sie jedoch restriktiver, als es das Bundesverfassungsgericht fordert: Erstens fasst § 12 Abs. 1 BKAG die sogenannte weitere Nutzung erhobener Daten sehr eng und unterwirft damit die Weiterverarbeitung dieser Daten in weiterem Umfang als nötig den Anforderungen an eine Zweckänderung. Daraus dürften sich auch praktische Anwendungsprobleme ergeben. Zweitens beschränkt die Norm die Zweckänderung von Daten, die durch „Online-Durchsuchungen“ gewonnen wurden, über das verfassungsrechtlich gebotene Maß hinaus, indem sie eine strafprozessuale Verwertung solcher Daten vollständig ausschließt. Diese Restriktion ist verfassungsrechtlich zulässig und praktikabel, aber nach meiner Vermutung nicht intendiert.

#### a) Abgrenzung von weiterer Nutzung (§ 12 Abs. 1 BKAG-E) und Zweckänderung (§ 12 Abs. 2 BKAG-E)

Der Gesetzentwurf unterscheidet zwischen der weiteren Nutzung erhobener Daten (§ 12 Abs. 1 BKAG-E) und ihrer zweckändernden Weiterverarbeitung (§ 12 Abs. 2 BKAG-E). Dieser Unterschied ist bedeutsam, weil danach – im Einklang mit dem BKAG-Urteil des Bundesverfassungsgerichts[31] – die weitere Nutzung von Daten grundsätzlich ohne besonderen Anlass zulässig ist, während es für die Zweckänderung eines konkreten Ermittlungsansatzes bedarf.

Nach § 12 Abs. 1 BKAG-E besteht die weitere Nutzung in der Weiterverarbeitung erhobener Daten „zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten“. Diese Formulierung wirft die Frage auf, worauf sich das Wort „derselben“ jeweils bezieht.

Nach dem Wortlaut der vorgesehenen Norm läge es am nächsten, dass nur die Weiterverarbeitung im Rahmen des konkreten polizeilichen Verfahrens erlaubt wird, in dem die Daten erhoben wurden. Diese Auslegung liegt allerdings sachlich fern, da § 12 Abs. 1 BKAG-E so leerliefe, weil diese Weiterverarbeitung schon von der Ermächtigung zur Datenerhebung gedeckt wird.

Eine durchaus sinnvolle und nach dem Wortlaut naheliegende Interpretation ginge hingegen dahin, dass eine weitere Nutzung (nur) dann vorliegt, wenn das Bundeskriminalamt erhobene Daten zum Schutz von Rechtsgütern oder zur Bekämpfung von Straftaten weiterverarbeitet, die ihrer Art nach mit den Rechtsgütern oder Straftaten identisch sind, die den Anlass der Datener-

[31] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 276 ff.

hebung gebildet haben. Dies lässt sich an dem in der Gesetzesbegründung enthaltenen Fallbeispiel veranschaulichen:[32] Erhebt das Bundeskriminalamt im Rahmen seiner Aufgabe zur Terrorismusabwehr (§ 5 BKAG-E) durch eine Telekommunikationsüberwachung Daten, um eine Gefahr für das Leben von Menschen abzuwehren, so handelt es sich um eine weitere Nutzung, wenn das Amt die erhobenen Daten weiterverarbeitet, um im Rahmen derselben Aufgabe eine an einem anderen Ort, zu einer anderen Zeit und durch andere Personen drohende Gefahr für das Leben anderer Menschen abzuwehren. Hingegen handelt es sich um eine Zweckänderung, wenn die Daten ebenfalls im Rahmen der Terrorismusabwehr weiterverarbeitet werden sollen, um eine an einem anderen Ort, zu einer anderen Zeit und durch andere Personen drohende Gefahr für die Freiheit von Menschen abzuwehren. Diese Zweckänderung bedarf daher gemäß § 12 Abs. 2 BKAG-E eines konkreten Ermittlungsansatzes.

Diese Konzeption der weiteren Nutzung ist restriktiver, als es das Bundesverfassungsgericht verlangt. § 12 BKAG-E unterwirft also Datenverarbeitungen dem Erfordernis einer hypothetischen Datenneuerhebung, die von Verfassungs wegen als weitere Nutzung zugelassen werden könnten. Grund hierfür ist eine Auslassung im Gesetzentwurf. Nach dem Urteil des Bundesverfassungsgerichts ist eine weitere Nutzung die Nutzung „seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter […] *wie für die Datenerhebung maßgeblich*“ (Hervorhebung nur hier). Das Gericht fügt konkretisierend an: „Ist [die Datenerhebung] nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt.“[33] Aus dem Zusatz und der anschließenden Konkretisierung ergibt sich, dass es nach dem Bundesverfassungsgericht nicht darauf ankommt, ob die Schutzgüter der Datenerhebung und der weiteren Nutzung identisch sind, sondern ob beide Schutzgüter (zulässigerweise) in der Ermächtigung für die Datenerhebung aufgeführt sind. In dem Beispielsfall läge also in beiden Varianten eine weitere Nutzung im verfassungsrechtlichen Sinne vor, da § 51 Abs. 1 Satz 1 Nr. 1 BKAG-E eine Telekommunikationsüberwachung zur Abwehr sowohl einer Lebens- als auch einer Freiheitsgefahr zulässt.

Es liegt nahe, den gesetzlichen Begriff der weiteren Nutzung an den verfassungsrechtlichen Begriff heranzuführen, um Wertungswidersprüche und Rechtsunsicherheit zu vermeiden. Dies bereitet auch keine Schwierigkeiten, da lediglich der bislang ausgelassene Zusatz aus dem Urteil des Bundesverfassungsgerichts in den Gesetzestext aufgenommen werden muss.

**b) Zweckänderung bei Daten aus „Online-Durchsuchungen“ (§ 12 Abs. 3 BKAG-E)**

Restriktiver als verfassungsrechtlich erforderlich fällt auch die in § 12 Abs. 3 BKAG-E enthaltene Regelung über die Zweckänderung von Daten aus, die mittels „Online-Durchsuchungen“ oder Wohnraumüberwachungen gewonnen wurden. Eine solche Regelung ist erforderlich, da nach dem Bundesverfassungsgericht Daten, die mit diesen besonders eingriffsintensiven Überwachungsmaßnahmen gewonnen wurden, nur unter den Voraussetzungen weiterverarbeitet werden dürfen, unter denen sie von Verfassungs wegen auch erhoben werden dürften. Daher muss zum einen die Weiterverarbeitung dem Schutz besonders bedeutsamer Rechtsgüter oder

[32] BT-Drs. 18/11163, S. 91.

[33] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 279.

der Verhütung oder Verfolgung besonders schwerer Straftaten dienen.[34] Zum anderen muss als Verarbeitungsanlass eine konkrete Gefahr oder ein konkreter Tatverdacht bestehen.[35] Ein unterhalb dieser Eingriffsschwellen anzusiedelnder konkreter Ermittlungsansatz reicht hier – anders als ansonsten für eine zweckändernde Weiterverarbeitung – nicht aus. Aufgrund von Art. 13 Abs. 3 GG dürfen schließlich Bilddaten, die bei einer optischen Wohnraumüberwachung gewonnen wurden, nicht für Zwecke eines Strafverfahrens weiterverarbeitet werden.[36]

Um diese verfassungsrechtlichen Vorgaben umzusetzen, verweist § 12 Abs. 3 Satz 1 BKAG-E wegen der Voraussetzungen der Zweckänderung auf § 12 Abs. 2 Satz 1 Nr. 2 lit. b BKAG-E und modifiziert diese Regelung durch ein Gefahrerfordernis. Damit enthält die Norm eine positive Regelung nur für die Weiterverarbeitung zu präventiven Zwecken der Gefahrenabwehr. Eine Regelung für die Weiterverarbeitung zu Strafverfolgungszwecken fehlt. Eine positive Regelung wird jedoch auch hierzu benötigt, um die Weiterverarbeitung als eigenständigen Grundrechtseingriff zu rechtfertigen.[37]

Eine positive Weiterverarbeitungsermächtigung für diese Daten findet sich im Gesetzentwurf auch nicht an anderer Stelle. Für Daten, die aus akustischen Wohnraumüberwachungen stammen, kann allerdings auf § 100d Abs. 5 Nr. 3 StPO zurückgegriffen werden. Hingegen fehlt es an einer Weiterverarbeitungsermächtigung für Daten, die das Bundeskriminalamt mit „Online-Durchsuchungen“ erlangt hat. Insbesondere kann die Weiterverarbeitung nicht auf § 161 Abs. 2 Satz 1 StPO gestützt werden. Diese Norm beschränkt lediglich die Weiterverarbeitung zu Beweiszwecken und erlaubt eine Weiterverarbeitung als Spurenansatz einschränkungslos.[38] Sie genügt damit nicht den vom Bundesverfassungsgericht errichteten Anforderungen an die Weiterverarbeitung von Daten aus besonders eingriffsintensiven Ermittlungsmaßnahmen.[39]

Damit darf das Bundeskriminalamt nach der vorgesehenen Regelung Daten, die es durch eine „Online-Durchsuchung“ erlangt hat, nicht zu Strafverfolgungszwecken weiterverarbeiten. Verfassungsrechtlich geboten ist diese strenge Beschränkung nicht. Die Daten dürften vielmehr unter denselben Voraussetzungen wie Daten, die durch eine akustische Wohnraumüberwachung erlangt wurden, zur strafprozessualen Weiterverarbeitung freigegeben werden.[40] Sollte dies gewünscht sein, so sollte § 12 Abs. 3 Satz 1 BKAG-E als eigenständige Zweckänderungsermächtigung ausgestaltet werden, die statt des – ohnehin schwer zu lesenden – Verweises auf

[34] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 316.

[35] Missverständlich insoweit BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 291, wo nur Zweckänderungen zur Gefahrenabwehr angesprochen werden. Dass eine Änderung des Verarbeitungszwecks zur Verfolgung von Straftaten grundsätzlich zulässig sein kann, ergibt sich aber aus Rn. 316 f.

[36] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 317.

[37] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 284.

[38] Vgl. etwa Sackreuther, in: BeckOK StPO, § 161 Rn. 12; Griesbaum, in: KK-StPO, § 161 Rn. 36.

[39] So ausdrücklich BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 283: „Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht.“

[40] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 316.

§ 12 Abs. 2 BKAG-E die Anforderungen an die zweckändernde Weiterverarbeitung von Daten aus Wohnraumüberwachungen und Online-Durchsuchungen abschließend regelt.

**2. Voraussetzungen einer Speicherung (§ 18 und § 19 BKAG-E)**

Es wurde bereits dargelegt, dass eine längerfristige Speicherung im Informationssystem eines hinreichenden Anlasses bedarf. Für Datenbevorratungen im Rahmen der Zentralstellenaufgabe enthalten § 18 und § 19 BKAG-E Anlässe, die weitgehend dem heutigen § 8 BKAG entsprechen. Generell können diese Regelungen nur die Datenspeicherung, nicht aber die gleichfalls erfasste Datenverwertung legitimieren.[41] Einige von ihnen werfen darüber hinaus auch in ihrer Funktion als Bevorratungsermächtigungen grundrechtliche Probleme auf.[42]

Problematisch ist die Ermächtigung in § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG-E, über einen Beschuldigten bestimmte Identifikationsdaten sowie Angaben zu der ihm vorgeworfenen Straftat zu bevorraten. Diese Bevorratungsermächtigung erfordert keine personenbezogene Prognose zukünftiger Straftaten, sondern errichtet eine gesetzliche Vermutung, dass diese Daten allein aufgrund der Beschuldigtenstellung der betroffenen Person für die Zentralstellenaufgabe nützlich sind. Diese Vermutung lässt sich in der Praxis in der Regel kaum widerlegen. Insbesondere ist weitgehend irrelevant, ob die betroffene Person zu Recht beschuldigt wurde. Nicht einmal ein festzustellender kriminalistischer Restverdacht wird gefordert, um die Bevorratung zu legitimieren. Vielmehr ist umgekehrt die (weitere) Bevorratung nach § 18 Abs. 5 BKAG-E nur dann unzulässig, wenn das Verfahren gegen die betroffene Person mit einer Entscheidung geendet hat, aus der sich positiv ergibt, dass sie die Tat nicht oder nicht rechtswidrig begangen hat.[43] Eine solche Entscheidung ergeht jedoch allenfalls in Ausnahmefällen, da es nicht Aufgabe des Strafverfahrens ist, die Unschuld einer Person zu erweisen.[44] Eine Grenze der Speicherungsbefugnis ergibt sich damit in aller Regel lediglich aus einer normativ nicht weiter angeleiteten Verhältnismäßigkeitsprüfung.[45]

Diese sehr weitreichende Bevorratungsermächtigung ist grundrechtlich allenfalls dann hinnehmbar, wenn die Verwertung der gespeicherten Daten eng begrenzt wird. Akzeptabel ist § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG-E, soweit die Beschuldigtendaten nur zu dem Zweck bevorratet werden, polizeiliche Kriminalakten zu erschließen. Der Datenabruf muss dementsprechend voraussetzen, dass gegen die betroffene Person Verdachtsmomente bestehen, die es angezeigt erscheinen lassen, die über sie geführten Kriminalakten einzusehen. Nicht mehr hinnehmbar ist es hingegen, wenn die Daten auch genutzt werden können, um einen personengerichteten Verdacht erst zu gewinnen, etwa im Rahmen einer Analyse von Tatzusammenhängen oder anlässlich eines Ereignisses wie einer Demonstration oder eines Fußballspiels. Im Kontext einer solchen Nutzung wird die gesetzliche Nützlichkeits- zu einer Gefährlichkeitsvermutung

---

[41] Siehe oben I. 3.

[42] Vgl. zur Beurteilung von § 8 BKAG im Einzelnen Bäcker, Kriminalpräventionsrecht, 2015, S. 508 ff.

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

[44] Ähnlich Spiecker gen. Döhmann/Kehr, DVBl 2011, S. 930 (934 f.); Henseler, NWVBl 2015, S. 53 (60 f.); kritisch auch Eisenberg/Singelnstein, GA 2006, S. 168 (177 ff.); ansatzweise Kritik auch bei Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2014, § 8 BKAG Rn. 33 f.; Kugelmann, BKAG, 2014, § 8 Rn. 9.

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

über den früheren Beschuldigten, ohne dass die betroffene Person dem etwas entgegensetzen könnte.[46]

Offen ist daneben die Grundrechtskonformität von § 18 Abs. 1 Nr. 2 und Nr. 3, Abs. 2 Nr. 2 und Nr. 3 BKAG-E. Diese Regelungen ermöglichen weitreichende Datenspeicherungen über Beschuldigte und Tatverdächtige, wenn von ihnen in Zukunft Straftaten erwartet werden. Damit knüpfen sie zwar an eine Kriminalprognose an, deren Grundlagen jedoch unsicher bleiben, weil eine positive Feststellung bereits begangener Straftaten nicht gefordert wird. Ausreichend ist ein kriminalistischer Restverdacht gegen die betroffene Person, aus dem auf zukünftiges Fehlverhalten geschlossen wird.[47]

Das Bundesverfassungsgericht hat diesen Regelungsansatz im Rahmen verschiedener Bevorratungsermächtigungen grundsätzlich akzeptiert.[48] Fraglich ist allerdings, ob er auch Art. 6 RL 2016/680 i.V.m. Art. 7 und Art. 8 GRCh genügt. Für die Auslegung dieser Normen ist nach Art. 52 Abs. 3 GRCh die Rechtsprechung zu Art. 8 EMRK bedeutsam. Der Europäische Gerichtshof für Menschenrechte hat jedoch die Bevorratung sensibler Daten von Tatverdächtigen, die nicht verurteilt wurden, für konventionswidrig gehalten.[49] Es ist denkbar, dass auch die Bevorratungsermächtigungen in § 18 Abs. 1 Nr. 2 und Nr. 3, Abs. 2 Nr. 2 und Nr. 3 BKAG-E, die sich gleichfalls auf sensible und aussagekräftige Daten erstrecken, die konventionsrechtlichen Anforderungen und letztlich auch die unionsgrundrechtlichen Maßstäbe verfehlen.

Schließlich ist die in § 18 Abs. 1 Nr. 4, Abs. 2 Nr. 3 BKAG-E vorgesehene weitreichende Ermächtigung zur Datenspeicherung über „Anlasspersonen“ bedenklich. „Anlasspersonen“ zeichnen sich dadurch aus, dass sie bisher nicht einmal als Beschuldigte oder Tatverdächtige strafrechtlich in Erscheinung getreten sind. Die Datenspeicherung beruht bei ihnen damit auf einer Tatprognose, für die das Gesetz keine Anknüpfungspunkte benennt und die in weitem Umfang etwa auf zulässiges Verhalten oder von der betroffenen Person nicht zu verantwortende äußere Umstände gestützt werden kann. Beispielsweise kann es ausreichen, dass eine Person in räumlichem und zeitlichem Zusammenhang mit einer Gewalttat bei einer Demonstration oder einem Fußballspiel angetroffen und deshalb gegen sie ein Platzverweis ausgesprochen wurde.[50]

---

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

[47] Näher und mit Nachweisen zur Rechtsprechung Bäcker, Kriminalpräventionsrecht, 2015, S. 510 ff.

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

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

[50] Beispiel von Arzt/Eier, DVBl 2010, S. 816 (818).

Eine so weitreichende Bevorratungsermächtigung ist mit den Grundrechten nicht mehr zu vereinbaren,[51] zumal die vorgesehene Regelung im Vergleich zum heutigen § 8 Abs. 5 BKAG als Grundlage für die Tatprognose nurmehr „tatsächliche Anhaltspunkte“ statt wie bisher „bestimmte Tatsachen“ fordert.[52]

**3. Speicherung ermittlungsunterstützender Hinweise (§ 16 Abs. 6 BKAG-E)**

Die vorgesehene Ermächtigung in § 16 Abs. 6 BKAG-E zur Speicherung sogenannter ermittlungsunterstützender Hinweise erweitert die heutige Regelung in § 7 Abs. 8 BKAG um weitere Hinweise, die bislang nur in der auf der Grundlage von § 7 Abs. 11 BKAG erlassenen BKADV erwähnt wurden.

Insbesondere die in § 16 Abs. 6 Nr. 2 BKAG-E genannten ermittlungsunterstützenden Hinweise können sensible Informationen zum Gegenstand haben, die das Persönlichkeitsrecht der betroffenen Person in erheblichem Ausmaß beeinträchtigen und das Verhalten der Polizei ihr gegenüber prägen können. So nennt § 2 Abs. 1 Nr. 16 BKADV beispielhaft für solche Hinweise die Angaben „Sexualstraftäter“, „Straftäter politisch links motiviert“ oder „Straftäter politisch rechts motiviert“.

Es ist daher grundrechtlich bedenklich, dass § 16 Abs. 6 Nr. 2 BKAG-E die Speicherung und Verwertung solcher Hinweise an keine besonderen Anforderungen knüpft. Insbesondere schlägt sich die in der Entwurfsbegründung enthaltene Maßgabe, ermittlungsunterstützende Hinweise müssten „auf der Grundlage von objektiven Erkenntnissen und von möglichst umfassenden Informationen zur betreffenden Person gewonnen werden“,[53] im Wortlaut der vorgesehenen Norm nicht nieder. Diese Regelung stellt vielmehr die Speicherung solcher Wertungen ohne besondere Anforderungen weitgehend ins Belieben des jeweils handelnden Sachbearbeiters.

Die Bedenken verschärfen sich noch dadurch, dass § 16 Abs. 6 Nr. 2 BKAG-E die Speicherung und Nutzung ermittlungsunterstützender Hinweise zu allen Personen erlaubt, zu denen bereits Daten vorhanden sind. Dies schließt insbesondere Beschuldigte ein, deren Grunddaten gemäß § 18 Abs. 1 Nr. 2, Abs. 2 Nr. 1 BKAG-E ohne weitere Voraussetzungen gespeichert werden können. Damit fordert der Entwurf keine individuelle Kriminalprognose, um potenziell sehr sensible Daten über diese Personen zu bevorraten. Jedenfalls insoweit ist die Bevorratungsermächtigung grundrechtlich nicht haltbar.

§ 16 Abs. 6 Nr. 2 BKAG-E sollte daher um einen besonderen Speicherungsanlass ergänzt werden. Zumindest aber müssen – wie es derzeit § 2 Abs. 1 Nr. 16 BKADV vorsieht – bloß Beschuldigte, hinsichtlich derer die Voraussetzungen von § 18 Abs. 2 Nr. 2 BKAG-E nicht festgestellt wurden, von der Bevorratungsermächtigung ausgenommen werden.

---

[51] Wie hier zu § 8 Abs. 5 BKAG Arzt/Eier, DVBl 2010, S. 816 (823); kritisch zu dieser Regelung auch Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2014, § 8 BKAG Rn. 52, 55 f.

[52] Diese Differenzierung ist in der Gesetzgebung verbreitet, wenngleich ihre Handhabbarkeit bezweifelt werden kann, vgl. für das Strafverfahrensrecht Bäcker, Kriminalpräventionsrecht, 2015, S. 133 ff.

[53] BT-Drs. 18/11163, S. 95.

**4. Beginn der Aussonderungsprüffrist (§ 77 Abs. 3 BKAG-E)**

Bedenklich ist schließlich § 77 Abs. 3 BKAG-E, der den Beginn der Frist regelt, nach der das Bundeskriminalamt zu prüfen hat, ob gespeicherte Daten zu berichtigen oder zu löschen sind. Die in dieser Regelung enthaltene „Mitführungsklausel“[54] verschiebt den Fristbeginn hinsichtlich aller über eine Person gespeicherter Daten auf den Zeitpunkt des letzten Speicherungsanlasses. Gerade für das Informationssystem des Bundeskriminalamts und den polizeilichen Informationsverbund kann dies zu sehr langen Datenspeicherungen ohne hinreichenden Anlass führen, da mit der beabsichtigten Neugliederung der Informationsordnung des Bundeskriminalamts die dort vorhandenen Datenbestände nicht mehr nach inhaltlichen Gesichtspunkten untergliedert werden.[55]

Ein rechtfertigender Grund hierfür ist nicht ersichtlich. Die vorgesehene Regelung verletzt daher sowohl die Grundrechte des Grundgesetzes als auch Art. 5 RL 2016/680, den sie in erheblichem Maße leerlaufen lässt. Soweit sie sich auch auf den polizeilichen Informationsverbund erstreckt, steht sie darüber hinaus mit Art. 7 Abs. 2 RL 2016/680 nicht in Einklang.

Insbesondere die von der Entwurfsbegründung angeführte „polizeifachlich erforderliche Abbildung der Entwicklung einer betroffenen Person in kriminalistischer Hinsicht über aussagekräftige Zeiträume hinweg“[56] kann diese Regelung nicht legitimieren. Der Ablauf der Aussonderungsprüffrist verpflichtet gemäß § 77 Abs. 1 BKAG-E i.V.m. § 75 Abs. 4 BDSG-E das Bundeskriminalamt nicht automatisch zur Datenlöschung, sondern lediglich zur Prüfung, ob eine Löschungspflicht besteht. Es ist nicht erkennbar, warum diese Prüfpflicht berechtigten Dokumentationsanliegen des Bundeskriminalamts zuwiderlaufen soll. Wenn sich bei Fristablauf herausstellt, dass bestimmte Daten gelöscht werden müssen, so ergibt sich die Löschungspflicht gerade daraus, dass berechtigte Dokumentationsanliegen nicht mehr bestehen.

[54] Vgl. zum gleichartigen, praktisch allerdings irrelevanten § 489 Abs. 6 StPO Wittig, in: BeckOK StPO § 489 Rn. 4.

[55] Vgl. hierzu das von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Anhang ihres Schreibens vom 22. Februar 2017 gebildete Fallbeispiel.

[56] BT-Drs. 18/11163, S. 126.

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 E

# Gutachterliche Stellungnahme

## zur Öffentlichen Anhörung des Gesetzentwurfs der Fraktionen der CDU/CSU und der SPD zur Neustrukturierung des Bundeskriminalamtgesetzes

**BT-Drucksache 18/11163**

im Innenausschuss des Deutschen Bundestages
am 20. März 2017

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin
Vorsitzender der Gesellschaft für Freiheitsrechte e.V. (GFF)

ulf@buermeyer.de

Berlin, den 16. März 2017

**Wesentliche Ergebnisse**

1. Der Gesetzentwurf auf BT-Drucksache 18/11163 (im Folgenden: der Gesetzentwurf) bezweckt eine Systematisierung der Rechtsgrundlage der Arbeit insbesondere des Bundeskriminalamts und eine Umsetzung der Entscheidung des BVerfG zum BKA-Gesetz[1]. Dieses Anliegen ist im Grundsatz begrüßenswert.

2. Dies gilt aus systematischer Perspektive auch für den Ansatz, die Rechtsgrundlagen der Datenverarbeitung durch das BKA „vor die Klammer zu ziehen“[2]. Gleichwohl gibt das konkrete Regelungskonzept[3] zu verfassungsrechtlichen Bedenken Anlass[4], da wesentliche Grundsätze des Datenschutzrechts – namentlich die Gebote der Datensparsamkeit und der Zweckbindung – mit der Idee eines umfassenden BKA-Datenpools in ihr Gegenteil verkehrt werden, ohne die Vorgaben der Verfassung hinreichend in Rechnung zu stellen. Dieser Paradigmenwechsel soll hier indes nicht vertieft werden, da er Gegenstand der Stellungnahme des Sachverständigen Prof. Dr. Matthias Bäcker ist.

3. Der Gesetzentwurf setzt in Abschnitt 5 des BKAG-E (§§ 38 ff., „Terrorismusteil“) vielfach wortgetreu die Entscheidung des BVerfG zum BKA-Gesetz um. Die Übernahme von Formulierungen und ganzen Passagen aus dem Urteil in den Gesetzesentwurf erweckt auf den ersten Blick den Eindruck einer sehr akribischen Umsetzung der verfassungsgerichtlichen Vorgaben. In Gesetzesform gegossene Urteilsgründe führen jedoch oft zu Auslegungsschwierigkeiten, weil sich Gesetzestechnik und Urteilsbegründungstechnik grundlegend unterscheiden. Zudem würde der Gesetzgeber durch diese „Copy & Paste“ – Technik seine Aufgabe verfehlen, einen Ausgleich zwischen kollidierenden Gütern von Verfassungsrang zu schaffen: Das BKAG in der Fassung des Entwurfs markiert infolge der Orientierung an den vom BVerfG gezogenen äußersten Grenzen das Maximum an Grundrechtseingriffen zur Gefahrenabwehr, das noch verfassungsgemäß sein mag, in Details geht es über diese Grenzen sogar noch hinaus.

---

[1] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09.
[2] Abschnitt 2 des BKAG-E, §§ 9 ff.
[3] Insbesondere §§ 12, 16, 18, 19 BKAG-E.
[4] Vgl. insoweit nur die Stellungnahme des Bundesrats auf BR-Drucks. 109/1/17, Seite 2.

Damit würde der Gesetzgeber aber gerade keine Balance zwischen „Freiheit und Sicherheit“ schaffen, sondern Interessen der Sicherheitsbehörden umfassend den Vorrang geben. Bildhaft gesprochen würde sich der Gesetzgeber nicht in der Mitte der ihm von Verfassungs wegen vorgegebenen „Fahrspur“ möglicher Grundrechtseingriffe zum Zwecke der Gefahrenabwehr durch das Bundeskriminalamt bewegen, sondern konsequent an der rechten Leitplanke entlangschrammen – und an einigen Stellen gar von der Fahrbahn abkommen.

4. Daraus folgt zugleich eine wesentliche Konsequenz für die Landesgesetzgeber: Es wäre verfehlt, den „Terrorismusteil“[5] als Muster-Polizeigesetz anzusehen. Die hier vorgesehenen Eingriffe mögen angesichts der spezifischen Gefahr besonders schwerer Rechtsgutsbeeinträchtigungen, wie sie der internationale Terrorismus mit sich bringen kann[6], im Wesentlichen zu rechtfertigen sein[7]. Bei der Abwehr „normaler“ Gefahren, wie sie sich im Alltag der Polizeibehörden überwiegend stellen, fällt die anzustellender Güterabwägung hingegen anders aus. Die Aufgabeneröffnung des § 5 Abs. 1 BKAG-E muss in sämtliche Befugnisnormen des Terrorismusteils mit hineingelesen werden; allein im Rahmen dieser Aufgabe können die Befugnisse nach Maßgabe des BKAG-Urteils gerechtfertigt werden.

5. Die gravierendsten Bedenken im Hinblick auf die Befugnisse des „Terrorismusteils“ bestehen gegen die Ausgestaltung der Ermächtigung zum Einsatz von Staatstrojanern: § 49 BKAG-E stellt in keiner Weise verfahrensrechtlich sicher, dass die vom BKA einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit erfüllen. Hier fehlen Regelungen sowohl über die an Staatstrojaner zu stellenden technischen Anforderungen, die wenigstens im Verordnungswege erlassen werden sollten, als auch über eine obligatorische unabhängige Prüfung, dass ein Staatstrojaner diese Anforderungen auch erfüllt.

---

[5] § 38 ff. BKAG-E.
[6] Vgl. die Aufgabenzuweisung in § 5 Abs. 1 BKAG-E.
[7] Vgl. aber die unten zu übende Kritik.

6. Zudem schafft § 49 BKAG-E in seiner derzeitigen Form ein erhebliches Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen (!), um Systeme von Zielpersonen gegebenenfalls „hacken“ zu können. Diese Fehlanreize sollten durch ein Verbot der Ausnutzung von Sicherheitslücken verhindert werden, die auch den Herstellern noch unbekannt sind.

7. Schließlich enthält der Gesetzentwurf in § 41 Abs. 3 und § 62 Abs. 1 und 2 BKAG-E unzureichende Regelungen zum Schutz bestimmter Gruppen von Berufsgeheimnisträgern, insbesondere von Ärzten, Psychologischen Psychotherapeuten und Journalisten. Denn er schließt Eingriffe ihnen gegenüber nicht zuverlässig aus, sondern überlässt solche Maßnahmen einer im Einzelfall nicht zu prognostizierenden Abwägungsentscheidung.

**Einzelaspekte des Gesetzentwurfs**

Eine erschöpfende Stellungnahme zu einem 131 Seiten umfassenden, inhaltlich sehr komplexen Gesetzentwurf würde deutlich mehr Zeit erfordern, als den Sachverständigen zur Verfügung stand. Meine Stellungnahme konzentriert sich daher auf die Befugnisnormen des „Terrorismusteils“[8].

Hingewiesen werden kann aber auch insoweit angesichts des Umfangs des Vorhabens und der Kürze der Vorbereitungszeit nur auf ausgewählte rechtlich bedenkliche Vorschläge oder sonst änderungsbedürftige Aspekte des Entwurfs. Ist eine Regelung in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies nicht dahingehend zu verstehen, dass sie als unbedenklich anzusehen wäre.

### *1.) Erhebung personenbezogener Daten, § 39 BKAG-E*

Die Norm definiert, über welche Personen zur Erfüllung der Aufgabe der Abwehr des internationalen Terrorismus Daten erhoben werden dürfen, sofern die besonderen Erhebungsbefugnisse des Terrorismusteils nichts Abweichendes regeln. Bedenken begegnet die beabsichtigte Regelung im Hinblick auf die Befugnis zur Datenerhebung über die derzeit noch so genannten Kontakt- und Begleitpersonen (§ 20b Abs. 2 Nr. 2 lit. c BKAG). Nach der alten wie der neuen Fassung soll eine Datenerhebung auch über eine selbst in keiner Weise verantwortliche Person möglich sein, wenn *„die Person mit einer [terrorverdächtigen Person] nicht nur flüchtig oder in zufälligem Kontakt in Verbindung steht und die [terrorverdächtige Person] sich ihrer zur Begehung der Straftat bedienen könnte“* (§ 39 Abs. 2 Nr. 2 lit. c BKAG-E). Dies umfasst erkennbar einen potentiell weiten Kreis von gutgläubigen Umfeldpersonen, gegen die selbst keinerlei Verdachtsmomente vorliegen. Das BVerfG hat die inhaltsgleiche derzeitige Regelung nur im Zuge einer verfassungskonformen Reduktion hingenommen[9], indem es nämlich verlangt: *„Freilich dürfen die Merkmale von Verfassungs wegen nicht entgrenzend weit verstanden werden.“* Diesen Hinweis nimmt der Gesetzentwurf jedoch nicht auf, indem er keinerlei Versuch

[8] Abschnitt 5, §§ 38 ff. BKAG-E.
[9] BVerfG, BKAG-Urteil (oben Fn. 1), Rn. 169.

unternimmt, einer „entgrenzenden“ Interpretation durch entsprechend engere Formulierung der Eingriffsermächtigung vorzubeugen. Auch der bereits vom BVerfG monierten Gefahr einer zirkelschlüssigen Anwendung der Norm begegnet der Gesetzentwurf derzeit nicht: Das BVerfG hat ausdrücklich verlangt, dass bei der Anwendung der Vorschrift die Voraussetzungen des § 20b Abs. 2 Nr. 2 BKAG – nunmehr: § 39 Abs. 2 Nr. 2 BKAG-E – nicht ihrerseits aus dem bloßen Kontakt oder der bloßen persönlichen Nähe des Betreffenden zur Zielperson hergeleitet werden[10]. § 39 BKAG-E lässt dies derzeit gleichwohl zu.

Durch die Schaffung eines neuen polizeilichen Informationsverbundes, in dem alle Daten in einem „großen Topf“ für eine etwaige spätere Nutzung gespeichert werden[11], wird die Intensität des mit der Datenerhebung verbundenen Grundrechtseingriffs für Kontakt- und Begleitpersonen, die weitgehend unbeteiligte Dritte sein können, noch weiter intensiviert. Dabei ist auch zu berücksichtigen, dass das BVerfG diese erhebliche Vertiefung der sich an eine Datenerhebung knüpfenden Folgen für die informationelle Selbstbestimmung noch nicht in Rechnung stellen konnte, sodass die Abwägung insoweit heute durchaus anders ausfallen könnte.

### *2.) Schutz von Berufsgeheimnisträgern, § 41 Abs. 3 und § 62 BKAG-E*

§ 62 beschränkt Maßnahmen aus dem Terrorismusteil des BKAG in der Fassung des Gesetzentwurfs, sofern sie sich gegen Berufsgeheimnisträger richten würden bzw. gegen Dritte richten, aber dabei Erkenntnisse von Berufsgeheimnisträgern erlangt würden, über die sie das Zeugnis verweigern dürften. Der Entwurf folgt weitgehend der Vorgängernorm des § 20u BKAG und übernimmt insbesondere die Zweiteilung in umfassend (§ 62 Abs. 1 BKAG-E) und lediglich relativ (§ 62 Abs. 2 BKAG-E) geschützte Berufsgeheimnisträger.

Absolut geschützt sind nach der Konzeption des Entwurfs Seelsorger (§ 53 Abs. 1 Satz 1 Nr. 1 StPO), Verteidiger (§ 53 Abs. 1 Satz 1 Nr. 2 StPO), Rechtsanwälte und

[10] BVerfG a.a.O, Rn. 168 a.E.
[11] Vgl. insbesondere §§ 12, 16 BKAG-E.

Kammerrechtsbeistände (§ 53 Abs. 1 Satz 1 Nr. 3 StPO) sowie Parlamentarier (§ 53 Abs. 1 Satz 1 Nr. 4). Insoweit sind Maßnahmen unzulässig, sofern die Berufsgeheimnisträger nicht selbst für die Gefahr verantwortlich sind.

Lediglich relativ geschützt sind hingegen weitere in § 53 Abs. 1 Satz 1 Nr. 3 StPO geschützte Berufsgruppen, insbesondere Ärzte, Zahnärzte und Psychologische Psychotherapeuten, sowie Journalisten (§ 53 Abs. 1 Satz 1 Nr. 5 StPO): Hier ist lediglich die Tatsache, dass Berufsgeheimnisträger betroffen wären und Informationen erlangt würden, die einem Schweigerecht unterliegen, *„im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen."*

Zwar hat das BVerfG diesen Schutz-Dualismus grundsätzlich als verfassungsgemäß akzeptiert[12] und auch die konkrete Zuordnung einzelner Berufsgruppen zu dem einen oder anderen Schutzniveau als im Rahmen des *„erheblichen Einschätzungsspielraums"* des Gesetzgebers liegend noch hingenommen[13]. Die vom BVerfG monierte Differenzierung zwischen Verteidigern einerseits und anderen Rechtsanwälten andererseits[14] enthält § 62 Abs. 1 BKAG-E nicht mehr.

Indes hat das BVerfG ausdrücklich darauf verwiesen, dass sich Einschränkungen bei Maßnahmen gegenüber nur relativ geschützten Berufsgeheimnisträgern aus Art. 12 GG sowie unter dem Gesichtspunkt des Schutzes des unantastbaren Kernbereichs der privaten Lebensgestaltung ergeben können. Auf diese wesentlichen, die Prüfung der Verhältnismäßigkeit von Verfassungs wegen leitenden Gesichtspunkte sollte der Tatbestand des § 62 BKAG-E ausdrücklich verweisen.

Dass die Unterscheidung zwischen absolut und nur relativ geschützten Berufsgeheimnisträgern nicht zwingend gegen das Grundgesetz verstößt, besagt im

[12] BVerfG a.a.O., Rn. 256.
[13] BVerfG a.a.O., Rn. 258.
[14] BVerfG a.a.O., Rn. 257.

Übrigen für sich noch nicht, dass sie auch sachlich gerechtfertigt wäre. In der Tat erscheint die Binnendifferenzierung zwischen den Berufsgeheimnisträgern nach § 53 Abs. 1 Satz 1 Nr. 3 StPO wenig überzeugend: Es ist kein hinreichender Grund erkennbar, warum etwa gegenüber Psychologischen Psychotherapeuten oder Ärzten, die regelmäßig intimste Kenntnisse über ihre Patienten erlangen, die Eingriffsbefugnisse des 5. Abschnitts des BKAG-E grundsätzlich eingesetzt werden können, gegenüber Strafverteidigern – etwa wegen eines vergleichsweise banalen Verkehrsdelikts – hingegen nicht. Gerade im Lichte der oben bereits zitierten und vom BVerfG in diesem Kontext ins Feld geführten Kernbereichs-Rechtsprechung liegen im Falle der in § 53 Abs. 1 Satz 1 Nr. 3 StPO genannten Berufsgeheimnisträger insgesamt Erhebungs- und Verwertungsverbote sehr nahe. Indem die derzeitige Fassung des BKAG-E in Konstellationen (scheinbar) eine Abwägung erlaubt, in denen in aller Regel das Ermessen auf null reduziert sein wird, leistet sie der Gefahr von Fehlentscheidungen Vorschub. Auf die Differenzierung des Entwurfs sollte daher im Interesse der Rechtsklarheit und eines effektiven Schutzes des Kernbereichs der privaten Lebensgestaltung verzichtet werden. § 62 Abs. 1 Satz 7 und Abs. 2 Satz 3 BKAG-E sollten dementsprechend ersatzlos entfallen.

Ebenso wenig überzeugend ist die Benachteiligung von Journalistinnen und Journalisten[15]. In Bezug auf diese Berufsgruppe berücksichtigt der Gesetzentwurf nicht hinreichend, dass für die – nach der ständigen Rechtsprechung des BVerfG von Art. 5 Abs. 1 GG geschützte[16] – journalistische Recherche ein *absolutes* Vertrauen in den Informantenschutz erforderlich ist. Ein Schutz von Informantinnen und Informanten allein nach Maßgabe einer im Einzelfall nicht zu prognostizierenden Abwägung (vgl. § 62 Abs. 2 Satz 2 BKAG-E) kommt aus der Sicht eines potentiellen Informanten einem insgesamt fehlenden Schutz gleich, weil er sich nicht darauf verlassen kann, dass seine Kommunikation mit einer Journalistin nicht ausgespäht werden darf. Dies wiegt im Bereich der journalistischen Recherche umso schwerer, als potentielle Informanten –

[15] § 62 Abs. 1 und 2 BKAG-E i.V.m. § 53 Abs. 1 Satz 1 Nr. 5 StPO.

[16] Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten (vgl. BVerfGE 100, 313 <365> m.w.N.). „Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann." (BVerfGE 117, 244 <259>, vgl. bereits BVerfGE 20, 162 <176, 187>; 36, 193 <204>).

anders als etwa Menschen, die medizinische Behandlung benötigen – auf den Kontakt zur Presse im Zweifel verzichten werden.

Dabei ist auch in Rechnung zu stellen, dass Informanten brisante Informationen auch vergleichsweise risikolos ins Netz stellen können, wobei die Kollateralschäden für die von Leaks betroffenen Personen typischerweise erheblich höher sind als bei verantwortlichem „Durchstechen" von Informationen an die Presse, die Persönlichkeitsrechte zu schützen versucht. Daraus folgt ein erhebliches öffentliches Interesse daran, dass Leaks an verantwortungsbewusste Journalistinnen und Journalisten und nicht etwa an Plattformen wie Wikileaks erfolgen. Gerade angesichts dessen erscheint der nur relative – und damit im Ergebnis nicht hinreichend belastbare– Schutz der Presse nach dem Gesetzentwurf anachronistisch. Berufsgeheimnisträger gem. § 53 Abs. 1 Satz 1 Nr. 5 StPO sollten daher ebenfalls in den Katalog des § 62 Abs. 1 BKAG-E aufgenommen werden.

### *3.) Besondere Mittel der Datenerhebung, § 45 BKAG-E*

§ 45 BKAG-E regelt den Einsatz „besonderer Mittel" der Datenerhebung, nämlich Observationen (Abs. 2 Nr. 1), auch unter Einsatz von technischen Mitteln wie etwa Kameras und Richtmikrofonen (Nr. 2) oder GPS-Sendern (Nr. 3), Vertrauenspersonen (Nr. 4) und Verdeckten Ermittlern (Nr. 5). Bedenken ergeben sich hier zunächst wieder aus der Verweisung des Abs. 1 Nr. 4 auf die Kontakt- und Begleitpersonen (§ 39 Abs. 2 Nr. 2 BKAG-E)[17]. Vor allem aber dürfte die Umsetzung des vom BVerfG angemahnten Richtervorbehalts misslungen sein[18]: Gemäß § 45 Abs. 3 Nr. 5 soll ein Richtervorbehalt vor Einsatz einer Vertrauensperson oder eines Verdeckten Ermittlers nicht schlechthin, sondern nur bei Maßnahmen erforderlich sein, die sich *„gegen eine bestimmte Person richten oder bei denen die Vertrauensperson oder der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist*".

[17] Vgl. oben Seite 4 zu § 39 BKAG-E.

[18] Im Ergebnis ebenso die Stellungnahme des Bundesrats, BR-Drucks. 109/1/17, Seite 10.

Das BVerfG[19] verlangt hingegen *„eine unabhängige Kontrolle ..., wenn Observationen ... längerfristig - zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender - durchgeführt werden, wenn nichtöffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss. Insoweit reicht es nicht, die Anordnung der Maßnahmen zunächst der Sicherheitsbehörde selbst zu überlassen und die disziplinierende Wirkung wegen des Erfordernisses einer richterlichen Entscheidung erst für deren Verlängerung - möglicherweise auf der Grundlage der so gewonnenen Erkenntnisse - vorzusehen. Soweit für diese Maßnahmen eine erstmalige Anordnung ohne richterliche Entscheidung vorgesehen ist, genügt [dies] einer verhältnismäßigen verfahrensrechtlichen Ausgestaltung nicht."*

Im Lichte dieser eindeutigen Aussage ist die Beschränkung des Richtervorbehalts auf ausgewählte Fälle des Einsatzes von VP / VE nicht haltbar.

### *4.) Staatstrojaner, § 49 BKAG-E*

Aus verfassungsrechtlicher wie rechtspolitischer Perspektive besonders bedenklich erscheint § 49 BKAG in der Fassung des Entwurfs. Die Regelung weist zwei Defizite auf, die miteinander verzahnt sind: Sie überlässt es dem Bundeskriminalamt und dem Gericht, die technischen Anforderungen an Software zu definieren, die in informationstechnische Systeme eingreift („Staatstrojaner"), obwohl von ihnen – ebenso wie von den verfahrensrechtlichen Vorkehrungen, um ihre Einhaltung sicherzustellen – das Gewicht des Grundrechtseingriffs maßgeblich bestimmt wird. Dies ist mit dem Gebot des Grundrechtsschutzes durch Verfahrensgestaltung ebenso wie mit dem Wesentlichkeitsgrundsatz unvereinbar. Außerdem lässt die Norm dem BKA und dem Gericht Raum für den Missbrauch von Sicherheitslücken in informationstechnischen Systemen (sog. *Zero Day Exploits* oder kurz *0days*[20]) zum Zwecke der Infiltration. Dies schafft fatale Fehlanreize, weil deutsche Behörden damit ein Interesse daran haben

[19] BVerfG, BKAG-Urteil (a.a.O.), Rn.
[20] Gesprochen: Oh-Days.

könnten, Sicherheitslücken in informationstechnischen Systemen nicht an die Hersteller zu melden, sodass sie geschlossen werden können, sondern sie vielmehr zu horten.

*a) Mangelhafte verfahrensrechtliche Sicherung*

Die Eingriffsbefugnis enthält in § 49 Abs. 2 BKAG-E zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des „Eingreifens“, etwa eine Beschränkung von Veränderungen auf das Notwendige oder einen Schutz von Zugriffen durch Dritte. Diese begrüßenswerten Regelungen finden indes keinerlei verfahrensrechtliche Absicherung. In der Aufzählung des § 49 Abs. 5 BKAG-E zum notwendigen Inhalt eines Antrags ist das technische Mittel, dessen Einsatz beabsichtigt ist, nicht einmal zu benennen, geschweige denn in seinen technischen Spezifikationen näher zu bezeichnen. Dies ermöglicht nach dem Wortlaut des Gesetzes den Einsatz beliebiger Staatstrojaner nach Gutdünken des Bundeskriminalamts, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann.

Die Verantwortung für die Prüfung der technischen Beschaffenheit des einzusetzenden Staatstrojaners kann auch nicht auf den Vorbehaltsrichter abgewälzt werden. Zum einen müsste er über den gesetzlich vorgegebenen Inhalt des Antrags (§ 49 Abs. 5 BKAG-E) hinaus Rückfragen stellen, um überhaupt zu erfahren, welches technische Mittel eingesetzt werden soll. Zum anderen kann vom zuständigen Richter des Amtsgerichts Wiesbaden nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwenigen Zeit – wenigstens Tage, wohl eher Wochen –in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird in „Terror-Fällen“ kaum ein Richter auf sich nehmen wollen, sodass er sich im Zweifel auf Beteuerungen der antragstellenden Behörde verlassen wird, mit dem Staatstrojaner habe schon alles seine Ordnung. Im Ergebnis ist daher zu besorgen, dass die Einhaltung der in § 49 Abs. 2 BKAG-E genannten, aber auch weiterer aus der Perspektive der Informationssicherheit gebotener technischer Anforderungen an Staatstrojaner allenfalls vom BKA geprüft werden wird.

Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ist ein derart blindes Vertrauen in die vom Bundeskriminalamt einzusetzenden Staatstrojaner ohne einen rechtsstaatlich gebotenen ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Dies gilt insbesondere angesichts des Umstands, dass die Software nach dem Wortlaut des Gesetzes durchaus von einem externen Anbieter stammen kann, sodass das Bundeskriminalamt mitunter selbst nicht mit Sicherheit einzuschätzen vermöchte, welche Funktionen die einzusetzende Software ausführt. Ausdrücklich zu begrüßen ist in diesem Kontext, dass sich das BKA nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-Telekommunikationsüberwachung soll diese einsatzbereit sein[21]. Der vorliegende Gesetzentwurf schließt aber gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind.

Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Die durch einen Staatstrojaner zu erfüllenden Spezifikationen könnten etwa im Verordnungswege durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben werden. Der Gesetzentwurf sollte hierzu um eine entsprechende Verordnungsermächtigung ergänzt werden. Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Dies darzulegen sollte in den Katalog der obligatorischen Inhalte des Antrags (§ 49 Abs. 5 BKAG-E) aufgenommen werden.

*b) Fehlanreize, die die Datensicherheit insgesamt schwächen*

Zumindest ebenso schwer wie die geschilderten rechtlichen Bedenken gegen die fehlende Prüfung der Staatstrojaner wiegen indes die fatalen Fehlanreize, die die Norm für die Arbeit der Bundesbehörden – namentlich die im Aufbau befindliche „ZITIS“

[21] https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html

(Zentrale Stelle für Informationstechnik im Sicherheitsbereich) – mit sich bringt. Nach § 49 Abs. 1 BKAG-E soll das BKA in informationstechnische Systeme „eingreifen“ dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen einer hoheitlichen Software, die Daten ausliest und an das BKA übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Der Entwurf definiert indes nicht weiter, wie der Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege[22]:

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle
- Aufspielen durch Hoheitsträger durch heimliches Betreten der Räumlichkeiten, in denen sich das System befindet
- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen EMail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde
- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*)

Es erschließt sich unmittelbar, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Artikel 13 Abs. 1 des Grundgesetzes ohne eine (bisher fehlende) spezifische Ermächtigungsgrundlage hierzu schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden eine E-Mail mit einem getarnten Staatstrojaner (kriminalistische List), soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken – wiewohl vom Wortlaut des § 49 Abs. 1 BKAG-E gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Bundesbehörden solche Lücken ausnutzen dürfen, so haben sie ein

[22] Vertiefend zu den technischen Grundlagen *Buermeyer* HRRS 2007, S. 154 ff.

als solches durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle eines Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, gefundene oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Bundesbehörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu horten.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur Bundesbehörden diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für *0days* kauft, die Lücken zur Infiltration informationstechnischer Systeme missbrauchen – insbesondere auch Cyber-Kriminelle, die es beispielsweise darauf anlegen könnten, die betroffenen Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen. Im Ergebnis würden Bundesbehörden mitunter viele Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von der jeweiligen Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aussetzen, um Sicherheitslücken im Einzelfall selbst für Maßnahmen nach § 49 BKAG-E ausnutzen zu können.

Eine solche aus der Sicht einer Gefahrenabwehrbehörde noch nachvollziehbare Güterabwägung verbietet sich indes aus der Perspektive des Gesetzgebers, der das Wohl der Allgemeinheit in den Blick zu nehmen hat. Nicht zuletzt hat sich die Bundesregierung politisch zur Förderung der IT-Sicherheit bekannt[23]. Damit sind Anreize für Bundesbehörden, die Cyber-Sicherheit in Deutschland und weltweit im Interesse einer möglicherweise einmal erforderlichen Gefahrenabwehr zu schwächen, schlechthin unvereinbar.

[23] Vgl. die sog. Cyber-Sicherheitsstrategie für Deutschland 2016, abzurufen auf http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html

§ 49 BKAG-E sollte daher um ein explizites Verbot des Einsatzes von dem Hersteller eines informationstechnischen Systems bisher unbekannten Sicherheitslücken (sog. *0days*) ergänzt werden, um sicherzustellen, dass sich alle Bundesbehörden darum bemühen, ihnen bekannte Sicherheitslücken durch die Hersteller der Systeme so schnell wie möglich schließen zu lassen.

### *5.) Datenerhebungsermächtigung in § 64 Abs. 1 Nr. 1 BKAG-E*

Insoweit wird auf die Erörterungen zu § 45 BKAG-E verwiesen.

### *6.) Benachrichtigungen, § 74 BKAG-E*

Die Benachrichtigungsregelungen begegnen im Lichte des BKAG-Urteils ebenfalls Bedenken[24], sofern sie ein endgültiges Absehen von der Benachrichtigung nach fünf Jahren vorsehen, dabei aber die seitens des BVerfG vorgenommene verfassungskonforme Auslegung der Norm nicht aufgreifen[25]: Das endgültige Absehen ist als solches zwar verfassungsrechtlich zulässig, setzt aber *„voraus, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden"*. Dies ist durch § 74 Abs. 3 BKAG-E bisher nicht sichergestellt.

Nach dem Neuerlass einer Norm in zur Umsetzung einer hierzu ergangenen Entscheidung des BVerfG, aber ohne Berücksichtigung einzelner Monita des Gerichts würde sich indes eine (neuerliche) verfassungskonforme Auslegung verbieten: Der Verzicht auf eine Umsetzung würde insoweit auf einen entgegenstehenden Willen des Gesetzgebers hindeuten. § 74 Abs. 3 Satz 5 BKAG-E wäre also insoweit verfassungswidrig, als nicht sichergestellt ist, dass eine weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht wurden[26].

---

[24] Vgl. auch die Stellungnahme des Bundesrats (a.a.O.), Seite 14.
[25] BVerfG a.a.O., Rn. 262.
[26] Vgl. auch die Stellungnahme des Bundesrats (a.a.O).

**Schlussbemerkung**

Angesichts des Änderungsbedarfs in dem in dieser Stellungnahme erörterten Teilen des Entwurfs, vor allem aber aufgrund der grundsätzlichen Bedenken gegen die Konzeption der Datenverarbeitung durch das BKA[27] sollte der Gesetzentwurf überarbeitet werden. Dies gilt insbesondere, führt man sich vor Augen, dass die Stellungnahmen der Sachverständigen schon aus Zeitgründen nur einen Abriss der verfassungsrechtlichen, aber auch rechtspolitischen Probleme des vorliegenden Entwurfs wiedergeben können.

Die seitens des BVerfG im Urteil zum BKA-Gesetz gesetzte Umsetzungsfrist (30. Juni 2018) lässt auch unter Berücksichtigung der Diskontinuität eine rechtzeitige Beschlussfassung durch den 19. Deutschen Bundestag durchaus zu, während sich die Schwächen des Entwurfs in dieser Legislaturperiode kaum rechtzeitig dürften beheben lassen. Insofern sollte von der Novelle einstweilen abgesehen werden.

Berlin, den 16. März 2016

Dr. Ulf Buermeyer, LL.M. (Columbia)[28]

[27] Vgl. §§ 12 ff. BKAG-E.

[28] Für wertvolle Hinweise dankt der Verfasser Herrn Univ.-Prof. Dr. Matthias Bäcker (Mainz) sowie Herrn Rechtsanwalt Dr. Nikolaos Gazeas (Köln).

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)806 F

Prof. Dr. Klaus F. Gärditz, Adenauerallee 24-42,· 53113 Bonn

An den Innenausschuss des
Deutschen Bundestages

**Prof. Dr. Klaus F. Gärditz**
Lehrstuhl für Öffentliches Recht

Postanschrift:
Adenauerallee 24-42
53113 Bonn
Tel.: 0228/73-9176
Email: gaerditz@jura.uni-bonn.de

Bonn, den 19. März 2017

***Stellungnahme zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamt-Gesetzes v. 14.2.2017 (BT-Drs. 18/11163)***

Der vorliegende Gesetzentwurf beschränkt sich nicht darauf, einzelne Regelungen, die vom BVerfG in seiner Entscheidung vom 20. April 2016 (BvR 966/09 u.a., NJW 2016, 1781) für unvereinbar mit der Verfassung erklärt wurden, nach Maßgabe der Entscheidungsgründe „nachzubessern". Vielmehr verfolgt der Gesetzentwurf eine vollständige Neuregelung des BKAG und geht damit oftmals über das hinaus, was im Lichte des Urteils des BVerfG vordringlich geboten wäre. Dies ist einerseits demokratiepolitisch zu begrüßen, weil der Deutsche Bundestag insoweit nicht nur als vom BVerfG Getriebener agiert. Angesichts des Umfanges des Entwurfs und der begrenzten Zeit, die für eine Stellungnahme zur Verfügung stand, muss ich meine Stellungnahme aber andererseits auch auf übergreifende Erwägungen und selektiv ausgewählte Problemfelder beschränken.

## I. Zur allgemeinen Umsetzungsstrategie

Zur allgemeinen Umsetzungsstrategie sei Folgendes angemerkt:

- *Bundesverfassungsgerichtsschematismus*: Der gesamte Entwurf ist von dem Willen getragen, das Urteil des BVerfG „eins zu eins" umzusetzen. Insoweit spiegeln die einzelnen Regelungen teils beinahe wortlautgleich die Urteilsgründe des Gerichts. Die damit einhergehende Engführung des Gesetzgebers wirft vor allem die – hier nicht zu diskutierende – Frage auf, inwiefern der – in einer längeren Entscheidungskette angewachsene (vgl. etwa *Gärditz*, JZ 2013, 633 ff.; *Möstl*, DVBl. 2010, 808 ff.), nicht erst im Urteil zum BKAG entwickelte – ausladende Stil bundesverfassungsgerichtlicher Begründungstechnik im Bereich des Sicherheitsverfassungsrechts und die damit einhergehende Überbeanspruchung der Angemessenheitsprüfung zur richterlichen Detailsteuerung (rechtsstaatlicher „Overkill") noch

funktionsadäquat ist (kritisch etwa *Durner*, DVBl. 2016, 780, 782, 784; *Gärditz*, in: Menzel/Müller-Terpitz, Verfassungsrechtsprechung, 3. Aufl. 2017, S. 988, 955 f.).

Dass der Gesetzgeber hierauf nur noch schematisch reagieren will, ist nachvollziehbar und verfassungsrechtlich gewiss unbedenklich. Notwendig wäre eine solche urteilsnahe Umsetzung freilich nicht immer. Dort wo abweichende Konzepte politisch sinnvoll erscheinen, könnte der Gesetzgeber durchaus gestaltend tätig werden und andere Formulierungen oder Regelungsstrategien wählen (zutreffend die Stellungnahme von *Möstl* zu dieser Anhörung). Im Übrigen ist die Bindung an tragende Urteilsgründe (§ 31 Abs. 1 BVerfGG) ihrem Rechtsgrund nach einfachgesetzlich und kann den parlamentarischen Gesetzgeber nicht daran hindern, im konstruktiven Dialog mit dem BVerfG abweichende politische Konzepte zu formulieren, zumal es vorliegend vor allem um Details geht, die sich nur auf einfachgesetzlicher Ebene sinnvoll austarieren lassen. Der vorliegend gewählte Umsetzungsschematismus birgt hingegen das Risiko, die beständige Verfeinerung und Ausdifferenzierung der verfassungsrechtlichen Standards zusätzlich zu katalysieren, weil künftige Gesetzesinterpretation mit Verfassungs- bzw. Verfassungsgerichtsinterpretation zusammenfällt; die Frage nach gesetzlichen Regelungszwecken und politischen Zielen wird verdrängt von der Frage, was das BVerfG entschieden hat bzw. künftig entscheidet wird.

- *Verzicht auf Verallgemeinerung:* Dass der Gesetzgeber vorliegend die Vorgaben des BVerfG zu den Eingriffsschwellen nicht durchweg in einem „vor die Klammer" gezogenen Allgemeinen Teil regelt, sondern sektoral ausdifferenziert, erscheint sinnvoll. Denn eine sektorale Gesamtstruktur des BKAG, die Eingriffsschwellen möglichst vollständig innerhalb der einzelnen Eingriffsbefugnisse formuliert, trägt zur Verständlichkeit der Einzelregelungen bei und vermeidet unnötige Verweisungen, die die neuere Sicherheitsgesetzgebung bisweilen durchziehen und unlesbar machen.

- *Verständlichkeit*: Ungeachtet dessen würde es sich an den Stellen, an denen auf andere Bestimmungen des Gesetzes verwiesen wird (und dies sind immer noch viele), gelegentlich legistisch anbieten, wenigstens den Regelungsgehalt der in Bezug genommenen Norm (etwa durch Klammerzusatz) zu umschreiben. Angesichts der Länge des Gesetzes leidet bei Verweisungen (wie etwa in § 12 I 2 BKAG-E) die Lesbarkeit und Übersichtlichkeit.

  *Ressourcenfaktor*: Das vom BVerfG entwickelte Datenschutzregime ist nicht nur anspruchsvoll, sondern bindet absehbar auch nicht unerhebliche Ressourcen (zutreffend die Stellungnahme von *Münch*). Dies gilt namentlich für die Operationalisierung der §§ 12-14 und §§ 74-80 BKAG-E. Die wichtige und konsequente materiell-rechtliche Regelung, die eine verfassungs(gerichts)konforme Rechtslage herstellt, muss mit Sach- sowie Personalmitteln umgesetzt werden, und zwar sowohl im Interesse der Grundrechtsbetroffenen, da Schutzmechanismen bei heimlichen Eingriffen ganz wesentlich von der Professionalität und Sorgfalt der betrauten Beamtinnen und Beamten abhängen, als auch im Interesse wirksamer Terrorismus- und Kriminalitätsbekämpfung. Der Gesetzgeber wird den notwendigen Folgekosten der Reform daher haushaltsrechtlich Rechnung zu tragen haben.

## II. Kompetenz

Die Regelungen des BKAG-E lassen sich insbesondere auf die Gesetzgebungskompetenztitel nach Art. 73 I Nr. 9a, Nr. 10 Halbs. 2 GG und auf die Verwaltungskompetenz des Art. 87 I 2 GG stützten.

Soweit § 2 V 1 Nr. 2 BKAG-E allerdings vorsieht, Kompetenzzentren für informationstechnische Systeme und Infrastrukturen sowie Einsatztechnik, technische Einsatzmittel und kriminaltechnische Untersuchungsmethoden im kriminalpolizeilichen Bereich aufzubauen, zu unterhalten und deren Entwicklungen und Ergebnisse den Polizeien des Bundes und der Länder zur Verfügung zu stellen, ist bei der Umsetzung dieser – in der Sache gewiss sinnvollen – Regelung auf Folgendes zu achten: Art. 87 I 2 GG i. V. mit Art. 73 I Nr. 9a, Nr. 10 Halbs. 2 GG spezifiziert die notwendige Verwaltungskompetenz des Bundes auf die Errichtung des „Bundeskriminalpolizeiamtes". Dies lässt es richtigerweise nicht zu, das BKA als Bundesoberbehörde mit einem eigenen – dezentralen – Verwaltungsunterbau zu versehen. „Kompetenzzentren" können daher keine selbstständigen Einrichtungen sein, sondern müssen abhängige Organisationsformate innerhalb des BKA bleiben. Eine fachliche Segmentierung (ggf. auch innerhalb von Außenstellen) erscheint insoweit möglich, eine territoriale Dezentralisierung, etwa zur regionalen und ortsnahen Unterstützung der Polizeibehörden der Länder hingegen unzulässig.

## III. Inhaltliches

### 1. Datenschutzkonzept

Herzstück des Datenschutzkonzepts des BKAG-E bilden die §§ 12 ff. BKAG-E. Die Regelungen sind insgesamt als verfassungskonform zu bewerten. Stichpunktartig sei hierbei auf Folgendes hingewiesen:

- Zwar fällt die *Generalklausel des § 12 I 1 BKAG-E* weit aus und wird lediglich durch einen Verweis auf die Aufgaben des BKA eingegrenzt. Sie ist jedoch insoweit verfassungskonform, als die darin liegende Befugnis durch die detaillierten Aufgabenzuweisungen nach §§ 4, 5 BKAG-E konkretisiert wird, die ihrerseits an Tatbestände anknüpfen, die nicht nur die interföderale Zuständigkeit (vgl. Art. 73 I Nr. 9a, 10 GG) tangieren, sondern zugleich tatbestandlich eine gewisse Gravität der Sicherheitsbeeinträchtigungen vorgeben.
- Auch soweit es bei den §§ 12, 18, 19 BKAG-E um eine Weiterverarbeitung im *Vorfeld* konkreter Gefahren oder Verdachtslagen geht, ist dies nach Maßgabe der Rechtsprechung des BVerfG (E 133, 277, 339) zulässig. Eine rein spekulative Speicherung, die verfassungsrechtlich unzulässig wäre, ist gesetzlich ausgeschlossen, weil auch ohne konkrete Eingriffsschwellen in jedem Fall konkret und nachvollziehbar zu begründen ist, inwiefern die – in jedem Fall an der der Verhältnismäßigkeit zu messende – Weiterverarbeitung zur Erfüllung einer konkreten Aufgabe erforderlich ist.
- Die Anwendungsvoraussetzung des § 12 I 1 BKAG-E, dass das BKA zur Erfüllung *derselben* Aufgabe und zum Schutz *derselben* Rechtsgüter oder zur Verfolgung oder Verhütung *derselben* Straftaten handeln darf, ist unklar (zutreffend die Stellungnahme von *Bäcker*). Ich verstehe diese Regelung so, dass die geforderte Zweckidentität nicht personal oder fallbezogen eingeschränkt wird, sondern sich auf die Aufgabenprofile der §§ 4, 5 BKAG-E bezieht. Was unter eine gesetzlich normierte Aufgabe fällt, darf dann – sollte diese Auslegung zutreffen – auch in anderen Verfahren weiterverwendet werden, die denselben Zweck verfolgen und

den gleichen Schutzgütern oder Verfolgungsinteressen dienen. Z. B. Daten aus einer Telefonüberwachung gemäß § 51 BKAG zur Aufklärung einer Straftat nach § 129a StGB (rechtsterroristische Vereinigung in Paderborn) gegen den Beschuldigten A führen zu belastenden Erkenntnissen über den zuvor nicht Beschuldigten B (linksterroristische Vereinigung nach § 129a StGB in Traunstein) und dürften entsprechend § 12 I BKAG-E – also ohne Prüfung des § 12 II BKAG-E – grundsätzlich weiterverwendet werden. Sieht man die besonderen Anforderungen an eine Zweckänderung als Schutzbarriere, damit die primären Eingriffsvoraussetzungen nicht nur abstrakt, sondern auch *fallbezogen* nicht unterlaufen werden (vgl. BVerfGE 133, 277, 324), ist unklar, ob ein solches weites Verständnis der Weiterverwendung eine verhältnismäßige Rechtsanwendung hinreichend sicherstellt.

- § 12 II BKAG-E normiert als allgemeine – somit wohl auch für die §§ 18, 19 BKAG-E zur Anwendung kommende – Regelung für eine Zweckänderung die Schwelle des hypothetischen Ersatzeingriffs (*hypothetische Datenneuerhebung*). Das ist konsequent, in sich stimmig und entspricht fraglos den verfassungsrechtlichen Anforderungen, schießt aber insoweit über das Ziel hinaus. Das BVerfG hat eine solche Prüfung nur bei Zweckänderungen von „Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen" gefordert (Urteil vom 20. April 2016, Rn. 287). Die allgemeine Regelung des § 12 BNDG-E erfasst aber auch Daten, die im Rahmen der Aufgaben des BKA auf andere Weise und ohne entsprechend intensive Grundrechtseingriffe erlangt wurden (vgl. auch die Stellungnahmen von *Bäcker*, *Möstl* und *Münch*). Es erscheint angesichts des ohnehin engen Korsetts grundrechtlicher Datenverwendungsschranken wenig überzeugend, hier zusätzliche Hürden aufzubauen.

- Unklar bleibt, inwiefern § 12 I, II BKAG-E (und entsprechend auch §§ 18, 19 BKAG-E) auch Regelungen für *rechtswidrig erhobene Daten* trifft. Die Normen stellen nur darauf ab, dass die Daten erhoben wurden. Es ist anzunehmen (obgleich nicht expliziert), dass damit nur eine Erhebung im Rahmen des Gesetzes gemeint ist. Es kann aber durchaus ein Bedarf bestehen, rechtswidrig erlangte Daten zu demselben bzw. zu einem anderen Zweck weiterzuverwenden, etwa wenn ein Eingriff, der unterhalb der Eingriffsschwelle und damit rechtswidrig vorgenommen wurde, zu Erkenntnissen führt, die eine hypothetische Datenneuerhebung nunmehr rechtfertigen würden (z. B. ein verdeckter Eingriff in informationstechnische Systeme nach § 49 BKAG gründet auf keiner hinreichend plausibilisierten Gefahr, führt aber zur Aufdeckung von terroristischen Anschlagsplänen). Auch solche Erkenntnisse können – in den Grenzen der Verhältnismäßigkeit und der Fairness des Verfahrens – ggf. verfassungskonform verwertet werden (BVerfGE 130, 1, 27 ff.). Sachgerecht erscheint daher eine Klarstellung in § 12 BKAG-E, um auszuschließen, dass sich das BKA im Konfliktfall an einer Verwertung gehindert sieht bzw. eine solche gerichtlich für unzulässig erklärt wird, weil es an einer hinreichenden Rechtsgrundlage fehle.

- Ein entsprechendes Problem stellt sich in Bezug auf *Zufallsfunde*: Deren Verwertung ist grundsätzlich – jedenfalls unter den Konditionen einer hypothetischen Datenneuerhebung – verfassungskonform möglich (vgl. für schwerwiegende Eingriffe BVerfGE 67, 157, 182; 115, 320, 359; *Huber*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 1 G 10 Rn. 29, § 4 G 10 Rn. 22). Es wird aber nicht deutlich, ob diese unter die nach § 12 BKAG-E (bzw. §§ 18, 19 BKAG-E) erhobenen Daten fallen. Eine Klarstellung wäre wünschenswert.

- In § 12 III BKAG-E wird auf § 12 II 1 Nr. 2 BKAG-E verwiesen, jedoch die Weiterverarbeitung von einer dringenden Gefahr bzw. Gefahrenlage nach § 49 BKAG-E abhängig gemacht. Dies beschränkt die Weiterverwendung auf Zwecke

der Gefahrenabwehr (§ 5 BKAG-E), schließt aber eine Nutzung in *Strafverfahren* (§ 4 BKAG-E) aus (zutreffend *Bäcker*, Stellungnahme, S. 13). Diese Verwendungsbeschränkung erscheint dysfunktional, ist möglicherweise ein Redaktionsfehler und sollte korrigiert werden. Da eine Verwendung in Strafverfahren ohnehin nur formalisiert nach Maßgabe der StPO erfolgen kann, erscheint es hier ausreichend, für Zwecke der Strafverfolgung einen einfachen (tatsachengestützten) Verdacht (§ 152 Abs. 2 StPO) ausreichen zu lassen.

- Die §§ 18, 19 BKAG-E normieren *keine zeitliche Grenze der Speicherung* (kritisch *Bäcker*, Stellungnahme, S. 14). Eine solche besteht zwar nicht absolut, ergibt sich aber aus dem Grundsatz der Verhältnismäßigkeit. Werden Daten zur Aufgabenerfüllung nicht mehr benötigt, sind diese zu löschen; im Übrigen wächst mit Zeitablauf der Rechtfertigungsdruck. Insoweit ist auch die Rechtsprechung des EGMR zu beachten, der eine undifferenzierte, unbefristete und voraussetzungslose Speicherung von personenbezogenen Daten fallbezogen für unvereinbar mit Art. 8 EMRK erachtet hat (EGMR, Entsch. v. 4.12.2008, Marper u.a. vs. UK, No. 30562/04 u.a., Rn. 121 ff.). Diese Voraussetzungen lassen sich freilich durch eine verhältnismäßige Rechtsanwendung wahren. Insoweit ist daran zu erinnern, dass der EGMR keine Feststellung über die Konventionsrechtswidrigkeit einer gesetzlichen Regelung getroffen hat (der Gerichtshof enthält sich generell solcher Aussagen), sondern nur eine Verletzung des Art. 8 EMRK aufgrund Umstände des Einzelfalles (vgl. Rn. 125; in den Folgerungen mE zu weitgehend daher *Bäcker*, Stellungnahme, S. 15).

## 2. Kooperationsrecht

Das Kooperationsrecht folgt mit den §§ 25-27 BKAG-E einer sachgerechten, verfassungskonformen und bewährten Gliederung, die die Kooperationsintensität und den Grad des wechselseitigen rechtsstaatlichen Grundvertrauens berücksichtigt: Übermittlung an (1) inländische Sicherheitsbehörden, (2) inländische andere Behörden, (3) Behörden anderer EU-Mitgliedstaaten und (4) Einrichtungen im internationalen Raum jenseits der EU.

Eine effektive und rechtlich abgesicherte zwischenstaatliche Behördenkooperation ist gerade in den Aufgabenfeldern des BKA unerlässlich und im Übrigen implizit durch die Kompetenzbestimmungen des Art. 73 I Nr. 9a, 10 Halbs. 2 GG sanktioniert. Dass auch ein Datenaustausch innerhalb der EU – in Bezug auf einzelne Mitgliedstaaten und unberechenbare politische Entwicklungen – trotz der gemeinsamen Bindung an gemeineuropäische Rechtsstaatsstandards nicht grenzenlos zulässig ist, namentlich möglichen Grundrechtsverletzungen im Zielstaat der Datenweitergabe ggf. anlassbedingt Rechnung zu tragen ist, bleibt selbstverständliche Grundlage des § 27 BKAG-E und ist im Rahmen der Ermessensausübung (vgl. den in Bezug genommenen § 25 Abs. 1 BKAG-E: „kann“) zu berücksichtigen.

## 3. Elektronische Aufenthaltsüberwachung

Die Regelung des § 56 BKAG-E zur elektronischen Aufenthaltsüberwachung ermächtigt zwar zu schwerwiegenden Grundrechtseingriffen, die mit der physischen Elektronisierung des Einzelnen („elektronische Fußfessel“) einhergehen und den mit der intensiven Überwachung weitreichende Einblicke in das persönliche Leben der Betroffenen ermöglichen. Ungeachtet dessen erweist sich die Regelung durch die enge tatbestandliche Bindung an schwerstwiegende Gefahrenlagen (Terrorismus nach § 5 I 2 BKAG-E) sowie durch die formalen und materialen Schranken in § 56 I-VIII BKAG-E als verhältnismäßig. Es sol-

len nämlich terroristische Handlungen verhindert werden, die in absehbarer Zeit drohen. Und die Überwachung ist auf drei Monate zu befristen (§ 56 VIII BKAG-E).

Der geläufige Einwand, dass die elektronische Überwachung ungeeignet sei, Terroranschläge zu verhindern, und damit den Anforderungen an die Verhältnismäßigkeit nicht genüge, lässt sich nicht aufrechterhalten. Unter Zugrundelegung der Einschätzungsprärogative des Gesetzgebers gibt es genügend mögliche Anwendungsfelder, in denen eine entsprechende Maßnahme Erfolg verspricht. Gewiss hindert ein elektronisches Gerät nach § 56 I BKAG-E einen fest zum Anschlag entschlossenen Selbstmordattentäter nicht daran, einen bereits geplanten und vorbereiteten Angriff auch auszuführen. Eine „elektronische Fußfessel" und die daran anknüpfende Überwachung hindern ihn aber möglicherweise daran, noch nicht abgeschlossene Anschlagsvorbereitungen (z. B. konspirative Treffen, Material- oder Waffenbeschaffung, Kontaktaufnahme mit Mittelspersonen) fortzusetzen. Gerade bei arbeitsteiligen Aktivitäten innerhalb einer Vereinigung nach §§ 129a, 129b StGB würde das Aufdeckungsrisiko erheblich steigen. Und wer das Gerät nach § 56 I BKAG-E mutwillig entfernt, um sich wieder „Beinfreiheit" zu verschaffen, wird ggf. die notwendigen tatsächlichen Anhaltspunkte für weitergehende Maßnahmen der Gefahrenabwehr liefern.

Bei der Bewertung der Bewertung der Verhältnismäßigkeit ist ferner zu berücksichtigen, dass bei einer konkreten Gefahr von Straftaten im Rahmen des § 5 I 2 BKAG-E auch weitergehende Freiheitseingriffe verhältnismäßig sein können. Namentlich ein – bislang im geltenden Recht nur unter den engen Voraussetzungen des § 20p BKAG (künftig: § 57 BKAG-E) möglicher – Gewahrsam kann abhängig von dem Wahrscheinlichkeitsgrad der Gefahr, der zeitlichen Nähe des möglichen Schadenseintritts und der Wertigkeit der bedrohten Rechtsgüter bei den hier in Rede stehenden Gefahren auch über Zeiträume, wie sie § 56 VIII BKAG-E vorsieht, ohne zuvor begangene Straftat verhältnismäßig sein. Auch wenn die rechtsstaatlichen Grenzen einer präventiven und tatunabhängigen Freiheitsentziehung bislang nicht geklärt sind, liegt es jedenfalls auf der Hand, dass § 56 BKAG-E auch der Versuch ist, einen längerfristigen Gewahrsam für „Gefährder" zu vermeiden und durch einen weniger schwer wiegenden Eingriff zu ersetzen. Es würde dem Verhältnismäßigkeitsgebot zuwider laufen, wenn man terroristischen „Gefährdern" ausschließlich durch Freiheitsentziehung (Gewahrsam) begegnen dürfte, weil sich nur so Anschläge weitgehend sicher verhindern lassen, aber mildere Mittel aufgrund der damit verbundenen Unsicherheiten noch nicht einmal (experimentell) erprobt werden dürften.

Dass das geltende Bundesrecht eine entsprechende Regelung – jenseits des funktional begrenzten § 68b I StGB – bei vergleichbaren Gefährdungen ohne internationalterroristischen Bezug nicht kennt, führt weder zur Unverhältnismäßigkeit noch zu einem Gleichheitsverstoß (Art. 3 I GG). Vielmehr ist die Begrenzung auf den Kontext des internationalen Terrorismus eine Folge der kompetenzrechtlichen Schranken, die sich aus Art. 73 I Nr. 9a GG ergeben. Für die unmittelbare Abwehr rein nationaler Terrorgefahren kann das BKA nämlich nicht verfassungskonform zuständig gemacht werden.

(Prof. Dr. Klaus F. Gärditz)

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

**Prof. Dr. Kyrill-Alexander Schwarz**
Institut für Staats- und Verwaltungsrecht,
Rechtphilosophie



Prof. Dr. Kyrill-A. Schwarz, Domerschulstraße 16, 97070 Würzburg

97070 Würzburg
Domerschulstraße 16
Telefon: (0931) 31-8 82335
E-Mail: Kyrill-alexander.schwarz@uni-wuerzburg.de

Würzburg, den 15.3.2017

**Sachverständige Stellungnahme zu dem**

**Gesetzentwurf der Fraktionen der CDU/CSU und der SPD für ein Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes (BT-Drs. 18/11163)**

## I. Ausgangssituation

Nachdem das Bundesverfassungsgericht mit seiner Entscheidung vom 16. April 2016 – unter grundsätzlicher Bestätigung der legitimen Aufgabe der Bekämpfung des internationalen Terrorismus – das BKA-Gesetz gleichwohl in Teilen für verfassungswidrig erklärt hatte und dem Gesetzgeber zahlreiche – nach Ansicht der abweichenden Meinung der Richter *Eichberger* und *Schluckebier* zu weitgehende – Vorgaben für die Neukonzeption des BKA-Gesetzes gemacht hat, nimmt der jetzt vorliegende Gesetzentwurf der Fraktionen von CDU/CSU und SPD die Vorgaben des Gerichts auf und setzt diese in verfassungskonformer Weise um.

In Ansehung der Tatsache, dass der Gesetzgeber sich mit der Aufgabe konfrontiert sah, eine Vielzahl von Vorgaben umzusetzen und der dies zum Anlass genommen hat, das BKA-Gesetz insgesamt zu novellieren, will sich die nachfolgende Stellungnahme auf einen – auch in der Öffentlichkeit besonders diskutierten – Aspekt konzentrieren, nämlich die in § 56 BKAG-E geregelte elektronische Aufenthaltsüberwachung – auch bezeichnet als „elektronische Fußfessel“. Wie nachfolgend aufgezeigt wird, ist dieses Mittel in hohem Maße problematisch, begegnet aber in Ansehung der zentralen Staatsaufgabe „Sicherheit“ keinen verfassungsrechtlichen Bedenken.

## II. Die Staatsaufgabe Sicherheit

### 1. Verfassungsrechtliche Vorgaben

Wie spätestens – allerdings sind auch zuvor eine Vielzahl von beabsichtigten Terroranschlägen entweder aufgrund der Aufmerksamkeit der Sicherheitsbehörden oder des Dilletantismus der Täter verhindert worden – der Terroranschlag in Berlin im Dezember 2016 gezeigt hat, dürfte es kaum mehr nur um gefühlte Bedrohungslagen gehen; es existiert vielmehr eine nicht mehr nur theoretische Bedrohung bisher ungeahnten Ausmaßes, die den Staat in der Wahrnehmung seiner Schutzpflichten zwingt, im Interesse einer effektiven Terrorabwehr Grundrechte zu beschränken, um so die ihm anvertrauten Bürger zu schützen.

Zwar erkennt die durch das Grundgesetz konstituierte wertgebundene Ordnung den Schutz von Freiheit und Menschenwürde als obersten Zweck allen Rechts an

> - vgl. dazu nur aus der Rechtsprechung des Bundesverfassungsgerichts *BVerfGE* 12, 45 (51); 28, 175 (189); 33, 1 (10 f.); 37, 57 (65) -

und beschränkt daher den Zweck des Staates auf die Wahrung des Gemeinwohls;

> - *BVerfGE* 42, 312 (332) -

gleichwohl setzt die Verfassung die Existenz des Staates und seiner Handlungsfähigkeit voraus. Dies bedeutet, dass der Staat auch und gerade unter den Vorzeichen terroristischer Bedrohungen eine Balance von Freiheit und Sicherheit herstellen muss,

> - Zum prekären Verhältnis von Freiheit und Sicherheit siehe ausführlich *Schwarz*, Die Dogmatik der Grundrechte – Schutz und Abwehr im freiheitssichernden Staat, in: Blaschke/Förster/Lumpp/ Schmidt (Hrsg.), Sicherheit statt Freiheit?, Berlin 2005, S. 29 ff. -

die maßgeblich auch durch die Aussage geprägt wird, dass das in den Grenzen der Rechtsordnung verbleibende Opfer den vorrangigen Schutz des Staates verdient.

> - Ausführlich und m.w.N. *Hillgruber*, in: JZ 2007, 209 (211 ff.) -

In der Sache geht es darum, dass das Grundrecht auf Freiheit die Gewährleistung von Sicherheit durch den Staat bedingt. Das damit umschriebene Problem lässt sich auch mit dem plakativen Stichwort der Freiheitsgewährleistung durch Freiheitsbeschränkung benennen.

> - *BVerfGE* 49, 23 (56 f.): *„Es wäre eine Sinnverkehrung des Grundgesetzes, wollte man dem Staat verbieten, terroristischen Bestrebungen, die erklärtermaßen die Zerstörung der freiheitlichen demokratischen Grundordnung zum Ziel haben und die planmäßige Vernichtung von Menschenleben als Mittel zur Verwirklichung dieses Vorhabens einsetzen, mit den erforderlichen rechtsstaatlichen Mitteln wirksam entgegenzutreten. Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölke-*

*rung sind Verfassungswerte, die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet*." -

Dabei darf nicht geleugnet werden, dass der mit der tatsächlichen Eskalation der Bedrohungslage

- insoweit ist es auch verfehlt, die Veränderung der Realität auszublenden, wie dies beispielsweise im Schrifttum geschieht, wenn von partiell „eingebildeten Bedrohungen" ausgegangen wird, so beispielsweise früher *Waechter*, DVBl. 1999, S. 809 ff. -

gestiegene Informationsbedarf der Sicherheitsbehörden dazu führt, dass sich Eingriffsbefugnisse immer weiter in das Vorfeld von Gefahren ausdehnen, dass also der herkömmliche Gefahrenbegriff nur bedingt tauglich ist, den Herausforderungen des 21. Jahrhunderts gerecht zu werden. Gefahrenabwehr wird vor diesem Hintergrund zur Gefahrenvorsorge, wobei zu konstatieren ist, dass sich die Befugnisse zur Gefahrenvorsorge überaus dynamisch entwickeln. Dies bringt für das Verfassungsrecht die Frage mit sich, wie diese Dynamik sich in das System des Schutzes grundrechtlicher Freiheit einfügen lässt, da jedenfalls nach allgemeiner Ansicht gerade in diesem Bereich – anders als bei der klassischen Gefahrenabwehr oder bei der Verfolgung bereits begangener Straftaten – klassische rechtsstaatliche Begrenzungsansätze nur bedingt zur Zielverwirklichung tauglich erscheinen.

- ausführlich zu entsprechenden Veränderungen im Schrifttum: *Schoch*, Der Staat 43 (2004), S. 347 (362 f.) -

Es sei in Erinnerung gerufen: Die Erweiterung strafprozessualer oder gefahrenabwehrrechtlicher – Befugnisse ist kein Selbstzweck im Sinne von bloßem Aktionismus, sondern Reaktion (in den 70er Jahren auf die Terrorismusgefahr seitens der RAF, später auf das Phänomen der Organisierten Kriminalität und seit dem 11. September 2001 auf einen global agierenden, aber lokal organisierten Terrorismus). Dabei ist der Rechtsstaat gefordert, wenn er, um neuen Herausforderungen gerecht zu werden, das überkommene rechtliche Instrumentarium behutsam fortentwickelt.

Dementsprechend sei auch vor Diffamierungstendenzen gewarnt, die staatliche Institutionen wider besseres Wissen bezichtigen, Bürgerrechte ohne Not auf dem Altar der Sicherheit opfern zu wollen. Das Grundgesetz misst auch und gerade dem Schutz der freiheitlichen demokratischen Grundordnung eine zentrale Bedeutung zu. Dies belegt auch die Rechtsprechung des Bundesverfassungsgerichts, wenn es der zu gewährleistenden Sicherheit der Bevölkerung den gleichen Rang zubilligt wie anderen hochwertigen Verfassungsgütern.

- *BVerfGE* 49, 24 (46 f.); 115, 320 (346, 357); 120, 274 (319); 133, 277 (333); zuletzt auch *BVerfG*, Urt. v. 16.4.2016 – 1 BvR 966/09 u.a., Rn. 96 -

Dies gilt umso mehr angesichts einer veränderten Bedrohungslage und einer veränderten Bedrohungsqualität; der Staat ist zur Risikovorsorge und Risikominimierung verpflichtet.

- zum verfassungsrechtlichen „…*Grundsatz der bestmöglichen Gefahrenabwehr und Risikovorsorge…"* vgl. nur *BVerfGE* 49, 89 (139) -

Insoweit ist der Schutz der Bevölkerung im Vorfeld vor der Begehung schwerster Straftaten ein wesentlicher Auftrag eines rechtsstaatlichen Gemeinwesens. Wer dem Staat präventive Mittel – und dies erfasst auch Vorfeldmaßnahmen – aus der „*grundrechtsgebundenen*" Hand nehmen will, läuft Gefahr, den Staat und die Gemeinschaft der rechtstreuen Bürger wehrlos gegenüber Bedrohungen zu machen, die die Werte einer freiheitlich verfassten Gemeinschaft negieren.

Gerade wegen der zunehmenden Nutzung elektronischer und digitaler Informationsmittel in nahezu allen Lebensbereichen wäre der Schutz der freiheitlichen demokratischen Grundordnung sowie des Bestandes und der Sicherheit des Bundes und der Länder erheblichen Gefährdungen ausgesetzt, wenn nicht auch den Sicherheitsbehörden die Möglichkeit eingeräumt wird, ihre informationstechnische Handlungsfähigkeit den aktuellen Rahmenbedingungen anzupassen.

- *BVerfGE* 115, 320 (360): „*Die Verfassung hindert den Gesetzgeber nicht grundsätzlich daran, die traditionellen rechtsstaatlichen Bindungen (…) auf der Grundlage einer seiner Prärogative unterliegenden Feststellung neuartiger oder veränderter Gefährdungs- und Bedrohungssituationen fortzuentwickeln. Die Balance zwischen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch von ihm nicht grundlegend verschoben werden.*" -

Von einer solchen grundlegenden Verschiebung kann jedoch mit Blick auf die neu eingeführten Befugnisse des BKA keine Rede sein. Moderne Kommunikationstechniken werden bei der Begehung und Vorbereitung unterschiedlichster Straftaten zunehmend eingesetzt und tragen so zur Effektivierung krimineller Handlungen bei. Das Schritthalten der Strafverfolgungsbehörden kann daher nicht lediglich als sinnvolle Abrundung des Arsenals kriminalistischer Ermittlungsmethoden bzw. Aufklärungsmittel im Vorfeld konkreter Straftaten begriffen werden, welche die weiterhin wirkungsvollen herkömmlichen Ermittlungsmaßnahmen ergänzt. Es ist vielmehr vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr einschließlich der anschließenden digitalen Verarbeitung und Speicherung als notwendiges Instrument zur Herstellung einer gewissen „technischen Parität" zu sehen.

- zum vorstehenden siehe nur *BVerfGE* 115, 166 (193); siehe zuletzt auch *BVerfG*, Urt. v. 16.4.2016 – 1 BvR 966/09 u.a., Rn. 96 -

Es wäre in der Tat eine bemerkenswerte Verdrehung eines grundgesetzlichen Freiheitsverständnisses, „…*wollte man dem Staat verbieten, terroristische(n) Bestrebungen (…) mit den erforderlichen rechtsstaatlichen Mitteln wirksam entgegenzutreten.*"

- *BVerfGE* 49, 24 (56) -

Mit Blick auf die zentrale Aufgabe des BKA und die ihm zur Verfügung stehenden Eingriffsbefugnisse bedeutet dies auch, dass die grundrechtlichen Kautelen jedenfalls auch im Lichte der Bedeutung des BKA für den Bestand der freiheitlichen demokratischen Grundordnung ausgelegt werden müssen. Es dürfte nämlich kaum „*…der Sinn der Verfassung sein, zwar den verfassungsmäßigen obersten Organen im Staat eine Aufgabe zu stellen und für diesen Zweck ein besonderes Amt vorzusehen, aber den verfassungsmäßigen Organen und dem Amt die Mittel vorzuhalten, die zur Erfüllung ihres Verfassungsauftrages nötig sind*."

- *BVerfGE* 30, 1 (19 f.) -

Insoweit kommt insgesamt der Gewährleistung von Sicherheit eine verfassungsrechtliche Wertigkeit zu, die sich auch und gerade bei der Prüfung der Verhältnismäßigkeit der hier in Rede stehenden Grundrechtseingriffe entfalten muss.

- *BVerfGE* 115, 320 (357); 120, 274 (319); 133, 277 (333), *BVerfG*, Urt. v. 16.4.2016 – 1 BvR 966/09 u.a., Rn. 96 -

## 2. Rechtsstaatliche Kautelen

Datenschutzrelevante Grundrechtsgarantien bedürfen nach der Rechtsprechung des Bundesverfassungsgerichts organisations- und verfahrensrechtlicher Sicherungen; dies verwirklichen zum einen Auskunftsansprüche.

- *BVerfGE* 120, 351 (359 ff.); in Sonderheit zu behördlichen Benachrichtigungspflichten bei heimlichen Datenerhebungen vgl. nur *BVerfGE* 100, 313 (361, 364); 109, 279 (363 f.); 118, 168 (208 ff.) -

Der Gesetzentwurf sieht ein abgestuftes System von Benachrichtigungen der Betroffenen bei Zugriffen auf ihre Daten vor und genügt damit den verfassungsgerichtlichen Vorgaben in vollem Umfang.

Nach der Rechtsprechung des Bundesverfassungsgerichts kann sich im Einzelfall aus der Rechtsschutzgarantie des Art. 19 Abs. 4 GG ein Anspruch auf Benachrichtigung über die Erhebung personenbezogener Daten ergeben, wenn diese Form der Kenntnisgewähr Voraussetzung für die Inanspruchnahme gerichtlichen Rechtsschutzes ist,

- *BVerfGE* 100, 313 (364); 109, 279 (364); 120, 351 (362); 125, 260 (335) -

da ohne nachträgliche Kenntnis die Betroffenen weder die Unrechtmäßigkeit der Datenverwendung noch etwaige Rechte auf Löschung, Berichtigung oder ähnliches geltend machen könnten.

Der Gesetzgeber hat sich – frei von verfassungsrechtlichen Bedenken – für ein Konzept entschieden, wonach Daten jedenfalls unter bestimmten Voraussetzungen auch „ohne Wissen des Be-

troffenen“ erhoben werden dürfen. Dies hat auch seinen guten Grund. Denn Ermittlungen sind regelmäßig von einer beachtlichen Dynamik gekennzeichnet und beschleunigt zu führen. Aufwände, die verfahrenssichernden und rechtsschützenden Zwecken nicht zwingend *zeitnah* geschuldet sind, sollen *zunächst* in Grenzen gehalten werden. Der Gesetzgeber hat dementsprechend eine differenzierte Regelung über die Benachrichtigung getroffen, die eine vorherige Benachrichtigung nicht vorschreibt. Zudem hat er mit der Gestattung, zunächst auch ohne Wissen des Betroffenen Verkehrsdaten zu erheben, erkennbar eine Typisierung vorgenommen, die darauf zurückgeht, dass zumeist der Untersuchungszweck, das Nichtbekanntsein des Aufenthaltsortes des Betroffenen oder die notwendige Beschleunigung der Sachaufklärung einer Vorab-Benachrichtigung entgegenstehen. Das ist ersichtlich nicht unangemessen, dem Betroffenen zumutbar und infolgedessen dem Gesetzgeber von Verfassungs wegen unbenommen.

Es sei im Übrigen der Hinweis gestattet, dass sogar eine fehlende Benachrichtigungspflicht in Ansehung der geringen Eingriffsintensität von Verfassungs wegen unproblematisch sein dürfte, weil jedenfalls eine Rechtsschutzmöglichkeit gegenüber den abschließenden behördlichen Entscheidungen besteht.

- *BVerfG*, NJW 2012, 1419 (1430, Rdnr. 186) -

Im Übrigen ist der Rechtsordnung auch keine generelle Informationsverpflichtung durch Benachrichtigungen zu entnehmen, wie sich in Sonderheit den Bestimmungen der Strafprozessordnung entnehmen lässt. So ist im Fall der Verfahrenseinstellung nach § 170 Abs. 2 StPO eine Benachrichtigung des Beschuldigten nicht in jedem Fall der Einstellung, sondern nur unter den dort genannten Voraussetzungen vorgesehen. Auch die Benachrichtigungspflichten in § 100 StPO gehen von einem abgestuften System der Benachrichtigungspflichten aus, für die insbesondere die Eingriffsintensität der Maßnahme (Verpflichtung zur Benachrichtigung „erheblich mitbetroffener Personen“) entscheidend sind.

- *BVerfG*, NJW 2012, 833 (838, Rdnr. 227 f.) -

Insgesamt ist daher der Gesetzgeber nicht in jedem Fall verpflichtet, Regelungen über eine Benachrichtigungspflicht zu treffen. Dass er sie getroffen hat, ist schon verfassungsrechtlich nicht erforderlich, mag rechtspolitisch aber eine gewisse Befriedungsfunktion zu entfalten. Im Übrigen sei aber auch der Hinweis gestattet, dass Benachrichtigungspflichten zur Kompensation der Heimlichkeit oder Nichterkennbarkeit eines informatorischen Eingriffs nur sehr bedingt tauglich sind, etwaige Defizite zu kompensieren, da die ex-post-Information nicht die Möglichkeit zur effektiven Abwendung der Grundrechtsgefährdung bzw. des Grundrechtseingriffs eröffnet.

Eine weitere Möglichkeit zur Kompensation – hier unterstellter – bestehender Rechtsschutzdefizite stellt der Richtervorbehalt dar. Dabei handelt es sich um eine traditionelle prozedurale Vorkehrung gegenüber Datenerhebungen, die kompensieren soll, dass die überwachte Person – mangels

Kenntnis des Grundrechtseingriffs – selbst über keinen primären, präventiven Abwehrrechtsschutz verfügt.

- *BVerfGE* 103, 142 (152); 107, 299 (325); 109, 279 (359); 120, 274 (322) -

Wenngleich ein Richtervorbehalt ausdrücklich nur für Maßnahmen bei Art. 13 GG vorgesehen ist, so geht da Bundesverfassungsgericht gleichwohl in ständiger Rechtsprechung von einem abgestuften Konzept grundrechtsübergreifend wirkender Richtervorbehalte aus. So hatte das Gericht beispielsweise in der GPS-Entscheidung

- *BVerfGE* 112, 304 (318) -

einen Richtervorbehalt eingefordert, obwohl die betroffenen Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 GG einen solchen Vorbehalt nicht vorsehen. Dieser Ansatz wurde bei Eingriffen in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ausgebaut und ein grundsätzlicher Vorbehalt einer richterlichen Entscheidung postuliert.

- *BVerfGE* 120, 274 (331*)* -

Auch in dieser Hinsicht begegnet der Gesetzentwurf keinen durchgreifenden Bedenken, verwirklicht er vielmehr die vom Bundesverfassungsgericht geforderten Grundrechtssicherungen.

## III. Die elektronische Aufenthaltsüberwachung (EAÜ)

Von zentraler Bedeutung für die wirksame Erfüllung der Staatsaufgabe Sicherheit ist die in § 56 BKAG-E erstmals eingeführte Möglichkeit der elektronischen Aufenthaltsüberwachung (EAÜ). Voraussetzung für diese Maßnahme ist, dass entweder bestimmte Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine bestimmte Straftat begehen wird, oder deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass eine bestimmte Straftat begangen wird.

Der Gesetzgeber nimmt sich hiermit der Problematik sog. „Gefährder“ an, die gerade noch nicht den Bereich der Strafbarkeit eines Verhaltens (auch im Vorbereitungs- oder Versuchsstadium) erreicht haben, die aber gleichwohl eine nicht unerhebliche Gefahr aufgrund ihres „kriminellen Potentials“ darstellen.

Mit dieser Maßnahme versucht der Gesetzgeber dem Gedanken Rechnung zu tragen, dass letzten Endes auch das Recht ein Seismograph für Veränderungen der politischen Wirklichkeit ist. So ist das Strafrecht regelmäßig – wie die Entwicklung seit den 70er Jahren zeigt – der jeweiligen terroristischen Bedrohungslage angepasst worden und hat sich damit zu einem Sicherheitsrecht entwi-

ckelt. Vergleichbares gilt auf Bundesebene für die Strafprozessordnung und auf Landesebene für die Polizeigesetze der Länder.

Mit der jetzt – im Bereich des StGB bereits in § 68b geregelten – elektronischen Aufenthaltsüberwachung geht es primär um die Sicherung der Gesellschaft vor potentiell gefährlichen Personen, die aber in der Regel bisher nicht strafrechtlich oder gefahrenabwehrrechtlich in Erscheinung getreten sind.

Man mag dem Gesetzgeber hier vorhalten, er stelle eine bestimmte Gruppe von der Unschuldsvermutung frei und verstieße damit gegen geltendes Recht. Dem ist aber – wie sogleich nachzuweisen ist – nicht so. Denn die Anordnung einer präventiven Fußfessel begegnet keinen verfassungsrechtlichen Bedenken.

So hat auch das Bundesverfassungsgericht in der Entscheidung zum BKAG betont, dass der Gesetzgeber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt sei, die dem „tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren“ entsprechen. Vielmehr könne er die Grenzen auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziere. So könne eine hinreichend konkrete Gefahr auch dann bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lasse, gleichwohl aber bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinwiesen. So könne der Gesetzgeber beispielsweise in Bezug auf terroristische Straftaten auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie „in überschaubarer Zeit“ Straftaten begehen wird. Letzten Endes geht es darum, eine sachgerechte Abwägung zwischen der notwendigen Eintrittswahrscheinlichkeit in Abhängigkeit von der Schwere des drohenden Schadens vorzunehmen.

- dazu *Kubiciel*, ZRP 2017, 57 (59)-

Im Übrigen ist zu berücksichtigen, dass zur Abwendung erheblicher Gefahren für Bund und Länder auch Maßnahmen wie beispielsweise eine Präventivhaft möglich wären, um so eine Abkehr von der „grundrechtsschonenden Sicherheitspolitik“ der letzten 15 Jahre herbeizuführen. Der Gesetzgeber ist daran nicht gehindert; vielmehr erweist sich die elektronische Aufenthaltsüberwachung als das deutlich mildere Mittel im Vergleich zu der Möglichkeit der Präventivhaft.

Insgesamt erfordert daher die aktuelle Terrorgefahr die Normierung einer präventiven elektronischen Aufenthaltsüberwachung, da nur auf diese Weise den Gefahren vorgebeugt werden kann, die sich aus dem Potential von Gefährdern ergibt, selbst dann wenn sich noch keine konkreten Straftaten einschließlich strafbarer Vortaten gesichert nachweisen lassen. Insgesamt wird damit aber auch deutlich gemacht, dass Maßnahmen des BKA nicht etwa aufgrund bloßer Vermutungen

getroffen werden können. Mit der präventiv wirkenden Fußfessel wird ein Instrument geschaffen, das bei einer entsprechenden Gefahrenlage im Einzelfall die umfassende Überwachung deutlich erleichtern kann, da sie auch geeignet ist, die im Einzelfall erforderliche Rund-um-die-Uhr-Überwachung zu verringern; zudem stellt sie eine Mindermaßnahme zu einem verfassungsrechtlich gleichermaßen zulässigen Präventivgewahrsam dar.

gez. Kyrill-A. Schwarz

DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)749

Stellungnahme

**Nr. 2/17**
Januar 2017

# Stellungnahme des Deutschen Richterbundes zum Gesetzentwurf zur Stärkung des Datenschutzes und der Zentralstellenfunktion im Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten

## A. Tenor der Stellungnahme

Der Deutsche Richterbund begrüßt die schnelle Vorlage eines Gesetzentwurfs, mit dem das Urteil des Bundesverfassungsgerichts vom 20. April 2016 umgesetzt werden soll. Der Entwurf weist allerdings Änderungsbedarf etwa bei den Benachrichtigungsfristen und Speicherfristen auf.

Positiv ist, dass ein weitgehender Gleichlauf der Zuständigkeiten des Bundeskriminalamts (BKA) und des Generalbundesanwalts beim Bundesgerichtshof geschaffen werden soll. Der Deutsche Richterbund bedauert allerdings, dass dieser Gleichlauf nur unvollständig ist, was dem Ziel der Harmonisierung zuwiderläuft. Insbesondere soll dem BKA nicht die originäre Zuständigkeit bei der Wahrnehmung von polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung bei Straftaten nach dem Völkerstrafgesetzbuch zugewiesen werden.

**Deutscher Richterbund**
Haus des Rechts
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

**Verfasserin der Stellungnahme:**
Dr. Heike Neuhaus, Bundesanwältin beim BGH, Mitglied des Präsidiums

## B. Bewertung im Einzelnen

Im Hinblick auf die Kürze der für die Abgabe einer Stellungnahme zur Verfügung stehenden Zeit und die Komplexität des Vorhabens ist es dem Deutschen Richterbund nicht möglich, umfassend zu dem Gesetzentwurf Stellung zu nehmen. Er beschränkt seine Anmerkungen deshalb auf Regelungen, die einen unmittelbaren Bezug zur Tätigkeit von Staatsanwaltschaften und ordentlichen Gerichten aufweisen und behält sich vor, im Laufe des Gesetzgebungsverfahrens zu weiteren Vorschriften Stellung zu nehmen.

Der Deutsche Richterbund begrüßt die schnelle Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichts vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, durch das die Vorschriften des Bundeskriminalamtgesetzes (BKAG) über Befugnisse im Rahmen der Abwehr von Gefahren des internationalen Terrorismus teilweise für verfassungswidrig erklärt wurden. Die Umsetzung erscheint allerdings nur zum Teil gelungen.

### Erweiterung der originären Zuständigkeit des BKA für polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung, § 4 BKAG-E

Der Referentenentwurf sieht eine Ergänzung des in der geltenden Fassung von § 4 Absatz 1 Satz 1 BKAG festgeschriebenen enumerativen Katalogs originärer Zuständigkeiten des BKA bei der Wahrnehmung polizeilicher Aufgaben auf dem Gebiet der Strafverfolgung vor.

Die Vorschrift des § 4 Absatz 1 Satz 1 BKAG soll um eine Nummer 6 ergänzt werden, die dem BKA künftig die Wahrnehmung der polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung originär auch in folgenden Fällen zuweist:

a) Straftaten nach §§ 80, 81, 83 Absatz 1, 87, 88 und 94 bis 100a des Strafgesetzbuches;
b) Straftaten nach §§ 211, 212, 234, 234a, 239, 239a, 239b des Strafgesetzbuches, wenn anzunehmen ist, dass die Tat durch Angehörige des Geheimdienstes einer fremden Macht oder im Auftrag einer fremden Macht oder den Geheimdienst einer fremden Macht begangen worden ist.

Zur Begründung dieser Zuständigkeitserweiterung führt der Referentenentwurf aus, dass ein weitgehender Gleichlauf der Zuständigkeiten des BKA und des Generalbundesanwalts beim Bundesgerichtshof geschaffen werden soll.

Der Deutsche Richterbund begrüßt einen solchen Gleichlauf der nach § 142a Absatz 1 in Verbindung mit § 120 GVG zu bestimmenden Zuständigkeiten des Generalbundesanwalts beim Bundesgerichtshof und derjenigen des BKA. Allerdings findet sich lediglich eine Teilmenge der in die originäre oder evokative Zuständigkeit des Generalbundesanwalts beim Bundesgerichtshof fallenden Straftatbestände in § 4 Absatz 1 Satz 1 Nr. 6 Buchstaben a) und b) BKAG-E wieder. Andererseits geht durch die Aufnahme von § 234 und § 239 des Strafgesetzbuches § 4 Absatz 1 Satz 1 Nr. 6 Buchstabe b) BKAG-E über die Zuständigkeit des Generalbundesanwalts hinaus.

Diese selektive Zuständigkeitserweiterung führt zu einer Vielzahl unterschiedlicher Konstellationen der Zuständigkeitsverteilung, die dem Ziel der Harmonisierung zuwiderläuft. Ausschlaggebende Kriterien für die Verteilung der polizeilichen Zuständigkeiten bei der Wahrnehmung von Aufgaben auf dem Gebiet der Strafverfolgung im Bereich des Staatsschutzstrafrechts sollten ein ausschließlicher oder zumindest vorrangiger internationaler oder Bundesbezug sein. Solche Bezüge rechtfertigen die originäre Zuständigkeit des BKA innerhalb des bundesstaatlichen Kompetenzgefüges mit Blick auf die beim BKA vorherrschende Fachexpertise und Vernetzung sowie die damit einhergehende Effektivität der Strafverfolgung.

Der Deutsche Richterbund bedauert es besonders, dass dem BKA nicht – in Anlehnung an die Zuständigkeit des Generalbundesanwalts beim Bundesgerichtshof gemäß §§ 120 Absatz 1 Nummer 8, 142 a GVG – die originäre Zuständigkeit bei der Wahrnehmung von polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung bei Straftaten nach dem Völkerstrafgesetzbuch zugewiesen werden soll. Die für eine originäre Zuständigkeit des BKA sprechenden Argumente, nämlich das Vorliegen nationaler und internationaler Bezüge, gelten bei der Verfolgung von Straftaten nach dem Völkerstrafgesetzbuch in besonderer Weise. Hinzu kommt die Notwendigkeit einer engen Zusammenarbeit mit ausländischen und internationalen Ermittlungsbehörden. Die Verfolgung von Straftaten nach dem Völkerstrafgesetzbuch ist von hoher außenpolitischer Bedeutung. Die zunehmende Anzahl von Ermittlungsverfahren wegen Kriegsverbrechen, Verbrechen gegen die Menschlichkeit und auch Völkermord im Hinblick auf die bewaffneten Konflikte in Syrien und im Irak gegen Beschuldigte, die sich in Deutschland aufhalten, zeigt, dass der Verfolgung dieser Straftaten auch eine wachsende Bedeutung für

die nationale Sicherheit zukommt. Infolgedessen ist es aus Sicht des Deutschen Richterbundes unverständlich, dass der Bereich des BKA, der sich mit der Verfolgung von Straftaten nach dem Völkerstrafgesetzbuch befasst, keine originäre Zuständigkeit bei der Wahrnehmung polizeilicher Aufgaben auf dem Gebiet der Strafverfolgung – verbunden mit einer entsprechenden personellen Aufstockung – erhalten soll.

**Zeugenschutz**

Wie nach geltendem Recht obliegt dem BKA der Zeugenschutz gemäß § 7 BKAG-E nicht in allen Fällen, in denen das BKA die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrnimmt. Das Auseinanderfallen der polizeilichen Zuständigkeit bei der Ermittlung und beim Zeugenschutz ist aus Sicht des Deutschen Richterbundes wenig effektiv. Die Zuständigkeit des BKA beim Zeugenschutz sollte der Zuständigkeit bei der Wahrnehmung der polizeilichen Aufgaben im Bereich der Strafverfolgung entsprechen.

**Benachrichtigungspflichten**

§ 67 BKAG-E regelt die Pflichten des BKA zur Benachrichtigung Betroffener im Anschluss an bestimmte Maßnahmen. Gemäß Absatz 2 Satz 2 erfolgt die Benachrichtigung durch die Strafverfolgungsbehörde nach den Vorschriften der Strafprozessordnung, wenn wegen des zugrunde liegenden Sachverhalts ein Ermittlungsverfahren geführt wird. Grundsätzlich erscheint es sachgerecht, die Entscheidung über die Benachrichtigung und ihren Zeitpunkt der Strafverfolgungsbehörde zu überlassen, damit laufende Ermittlungen nicht gefährdet werden. Die Anwendung des Strafverfahrensrechts eröffnet in diesem Fall insbesondere die Möglichkeit, gemäß § 101 Absatz 5 StPO die Benachrichtigung der Betroffenen über Maßnahmen nach dem BKAG-E zurückzustellen, bis diese ohne Gefährdung des Untersuchungszwecks erfolgen kann. Die Durchführung der Benachrichtigung sollte allerdings aus folgenden Gründen vom BKA vorgenommen werden.

Zum einen fallen der nach dem BKAG-E zulässige Maßnahmenkatalog und der nach der Strafprozessordnung zulässige Maßnahmenkatalog auseinander. Zum anderen ist der Inhalt der Benachrichtigungen nach dem BKAG-E und der Strafprozessordnung nicht identisch. Ersteres ist von Belang, weil unklar bleibt, ob die Staatsanwaltschaft auch über Maßnahmen benachrichtigen muss, die nach der Strafprozessordnung gar nicht zulässig wären.
Letzteres ist von Belang, weil der Referentenentwurf in § 67 BKAG-E umfangreiche und detaillierte Regelungen zum Inhalt der Benachrichtigung

enthält, die die Strafprozessordnung nicht vorschreibt. Hingegen müssen die Strafverfolgungsbehörden gemäß § 101 Absatz 4 Satz 2 StPO in Benachrichtigungen gegenüber den Betroffenen von verdeckten Maßnahmen im Sinne von § 101 Absatz 4 Satz 1 StPO auf die Möglichkeit hinweisen, nachträglichen Rechtsschutz gemäß § 101 Absatz 7 StPO zu erlangen. § 101 Absatz 4 Satz 2 StPO kann in den Fällen des § 67 BKAG-E aber nicht sinnvoll angewendet werden, weil der betreffende strafprozessuale Rechtsbehelf gegenüber den gefahrenabwehrrechtlichen Maßnahmen des BKA nicht besteht.

Hinzu kommt der Aufwand, den eine Benachrichtigungspflicht durch die Staatsanwaltschaften mit sich brächte. Das BKA wäre verpflichtet, der Staatsanwaltschaft alle für die Benachrichtigung erforderlichen Angaben zu übermitteln, die Staatsanwaltschaft müsste Rechtsfragen klären, die polizeipräventiver Natur sind.

### Speicherfrist

Die in § 70 BKAG-E vorgesehene Verlängerung der Speicherfristen ist zu begrüßen. Problematisch erscheint allerdings die vorgesehene Regelung zum Fristbeginn. Nach § 32 Absatz 5 BKAG beginnen die Fristen derzeit mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Fristen geführt hat. Nach § 70 Absatz 3 BKAG-E sollen in Zukunft die Fristen für alle zu einer Person gespeicherten Daten einheitlich mit dem Tag beginnen, an dem die letzte Eintragung erfolgt ist. Dass Daten, die zu einer Person gespeichert sind und einen einheitlichen Sachverhalt betreffen, einheitlich gelöscht werden, erscheint sinnvoll, weil nur so ein vollständiges Bild über die Gefahrenlage existiert. Die Löschung aller eingetragenen Daten zu versagen, weil eine Eintragung hinzu kommt, die keinerlei Bezug zu den vorherigen Eintragungen hat, erscheint allerdings nicht unproblematisch. Datenschutzrechtlich sehr bedenklich ist, dass es für den Beginn der Frist nicht mehr auf das Ereignis ankommen soll, das zur Eintragung geführt hat, sondern auf die Eintragung selbst. Denn dadurch hat es das BKA in der Hand, den Beginn der Frist hinauszuzögern, ohne dass es zu neuen Ereignissen gekommen ist, die ein solches Hinauszögern der Frist gebieten.

**Das anordnende Gericht als „unabhängige Stelle“ gemäß § 42 Absatz 7 und § 45 Absatz 7 BKAG-E**

Der Gesetzentwurf bestimmt den Richter, der eine Maßnahme im Bereich des § 4a BKAG, § 5 BKAG-E anordnet (nach § 82 BKAG-E das Amtsgericht Wiesbaden) zur „unabhängigen Stelle“, die nach den Vorgaben des BVerfG zunächst alle Daten auf Kernbereichsbezug zu sichten hat, bevor sie vom BKA verwertet werden dürfen.

Das BVerfG hat in seiner Entscheidung vom 20. April 2016 ausgeführt, dass die geltenden Vorschriften des BKAG den Schutz des Kernbereichs privater Lebensgestaltung nicht hinreichend gewährleisteten. So müssten bei einer Wohnraumüberwachung zunächst alle Daten – außer bei Gefahr im Verzug – von einer unabhängigen Stelle daraufhin gesichtet werden, ob sie höchstprivate Informationen enthalten, bevor sie vom BKA verwertet werden dürfen. Auch für den Zugriff auf informationstechnische Systeme fehle es an einer hinreichenden Regelung zum Schutz des Kernbereichs privater Lebensgestaltung.

Diese Vorgaben setzt der Entwurf um, indem er in § 42 Absatz 7 BKAG-E bestimmt, dass alle aus einer Wohnraumüberwachung gewonnenen Erkenntnisse unverzüglich dem anordnenden Gericht vorzulegen sind. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Eine Ausnahme ist nach § 42 Absatz 8 BKAG-E bei Gefahr im Verzug vorgesehen. Bei einem verdeckten Eingriff in informationstechnische Systeme sieht das geltende Recht bereits eine Vorabkontrolle vor. Nach § 20k Absatz 7 BKAG werden erhobene Daten unter Sachleitung des anordnenden Gerichts unverzüglich vom Datenschutzbeauftragten des BKA und zwei weiteren Bediensteten des BKA, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchgesehen. Obwohl geregelt ist, dass der Datenschutzbeauftragte bei Ausübung dieser Tätigkeit weisungsfrei ist, hat das BVerfG entschieden, dass die mit der Sichtung betraute Stelle nicht hinreichend unabhängig sei. Erforderlich sei, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird. Auch hier sieht der Gesetzentwurf das anordnende Gericht nach § 45 Absatz 7 BKAG-E als „unabhängige Stelle“ vor. Gemäß § 45 Absatz 7 Satz 3 BKAG-E sind die Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, dem anordnenden Gericht unverzüglich vorzulegen, das dann nach Satz 4 unverzüglich über die Verwertbarkeit oder Löschung entscheidet. In Absatz 8 gibt es wiederum eine Ausnahmeregelung bei Gefahr im Verzug.

Es ist eine unter rechtsstaatlichen Gesichtspunkten sicherlich gute Lösung, die Vorabprüfung durch einen Richter oder eine Richterin vorzusehen. Der Deutsche Richterbund gibt aber zu bedenken, dass die Menge der anfallenden und zu prüfenden Daten immens sein kann. Anders als eine Behörde, wie etwa die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, kann der Richter die Prüfung nicht ohne weiteres auf mehrere Schultern verteilen. Der Richter trägt allein die Verantwortung. Daran ändert auch nichts die in § 82 Absatz 4 BKAG-E vorgesehene technische Unterstützung oder fachliche Beratung durch das BKA.
Das heißt, dass er auch die zeitliche Kapazität dafür haben muss, alle Aufzeichnungen, die durch eine Wohnraumüberwachung erlangt wurden, oder alle Daten, die aus einem Eingriff in ein informationstechnisches System stammen, zu sichten und zu überprüfen, und dies so zügig, dass eine zeitnahe Verwertung der Daten durch das BKA sichergestellt werden kann. Wenn dem anordnenden Richter die Aufgabe der Vorabprüfung übertragen werden soll, muss deshalb dafür Sorge getragen werden, dass das zuständige Gericht über ausreichende personelle Kapazitäten verfügt, um die Wahrnehmung dieser zusätzlichen zeitintensiven Aufgabe leisten zu können.

**Abwehr von Gefahren des internationalen Terrorismus**

Die Regelung des § 4a BKAG wird weitgehend unverändert in § 5 BKAG-E übernommen. Die Vorschrift ist aber bereits nach geltendem Recht in Verbindung mit § 20v Absatz 2 BKAG problematisch, sodass auch hierzu Stellung genommen werden soll.

§ 4a des geltenden Rechts und § 5 des Entwurfs übertragen dem BKA polizeipräventive Maßnahmen im Bereich der Abwehr von Gefahren des internationalen Terrorismus. Zur Wahrnehmung dieser Aufgabe werden dem BKA Befugnisse übertragen, die sehr weitgehend in Grundrechte eingreifen – wie die Wohnraumüberwachung in § 42 BKAG-E und der Eingriff in informationstechnische Systeme in § 45 BKAG-E. Der Maßnahmenkatalog, der dem BKA zur Gefahrenabwehr zur Verfügung steht, geht über den Maßnahmenkatalog der Strafprozessordnung hinaus. Aber während im Rahmen von Ermittlungen der Bundesanwaltschaft, die für die Aufklärung und Verfolgung der in § 5 BKAG-E genannten Straftaten grundsätzlich zuständig ist, der Ermittlungsrichter des Bundesgerichtshofs über grundrechtseingriffsintensive Maßnahmen entscheidet, wird die Anordnungsbefugnis im Rahmen des § 4a BKAG bzw. des § 5 BKAG-E dem Amtsgericht gemäß § 20v Absatz 2 BKAG bzw. § 82 Absatz 2 BKAG-E zugewiesen.

Dies ist ein kaum begründbarer Wertungswiderspruch, zumal die aus den präventiven Maßnahmen gewonnenen Erkenntnisse anschließend in das Strafverfahren überführt werden müssen. Problematisch ist darüber hinaus, dass die Bundesanwaltschaft, die die Fälle des § 4a des geltenden Rechts und des § 5 des zukünftigen Rechts in einem späteren Stadium übernimmt, wenn die präventive in die repressive Phase übergeht, mit zahlreichen Beschlüssen des Amtsgerichts umgehen muss, in deren Erlass sie zuvor nicht eingebunden war. Aus Sicht des Deutschen Richterbundes sollte im Rahmen der Neufassung des BKAG für diesen Bereich ein Konzept entwickelt werden, das widerspruchsfrei ist und den in vielen Fällen zu erwartenden Übergang von der Gefahrenabwehr zur Strafverfolgung erleichtert.

*Der Deutsche Richterbund ist mit mehr als 16.000 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.*

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)781

BPtK
BundesPsychotherapeutenKammer

# Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (BT-Drs. 18/11163)

## Stellungnahme der Bundespsychotherapeutenkammer vom 23.02.2017

BPtK
Klosterstraße 64
10179 Berlin
Tel.: 030 278785-0
Fax: 030 278785-44
info@bptk.de
www.bptk.de

# Inhaltsverzeichnis

# I. Zusammenfassung

Die Bundespsychotherapeutenkammer (BPtK) kritisiert, dass mit dem Gesetzentwurf zur Neustrukturierung des Bundeskriminalamtgesetzes (BKAG) weiterhin der Schutz einiger Berufsgeheimnisträger, die gesetzlich zur Verschwiegenheit verpflichtet sind, erheblich eingeschränkt bleibt.

Das Bundesverfassungsgericht hat am 20. April 2016 entschieden, dass die Befugnisse des Bundeskriminalamts (BKA) zur Abwehr des internationalen Terrorismus teilweise verfassungswidrig sind, und einen präziseren Schutz von Berufsgeheimnisträgern gefordert (Az.: 1 BvR 966/09 und Az.: 1 BvR 1140/09).

Maßnahmen zur Abwehr von Gefahren des internationalen Terrorismus waren nach dem BKAG nur nicht zulässig, wenn sie sich gegen Geistliche, Strafverteidiger und Abgeordnete richten. Durch das Gesetz zur Neustrukturierung des BKAG werden nunmehr auch Rechtsanwälte und Kammerrechtsbeistände in den absoluten Schutz aufgenommen. Für alle anderen Berufsgeheimnisträger, z. B. für Psychotherapeuten und Ärzte, fehlt ein solch absoluter Schutz.

Das Bundesverfassungsgericht hat in seinem Urteil betont, dass Gespräche, in denen es Einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, in die höchstpersönliche Privatsphäre fallen und damit der Staat keinen Zugriff darauf hat. Dazu gehören vertrauliche Gespräche mit einem Strafverteidiger, aber auch und gerade Gespräche mit einem Psychotherapeuten.

Der Gesetzentwurf zur Neustrukturierung des BKAG garantiert weiterhin keinen ausreichenden Schutz des Kernbereichs der persönlichen Lebensgestaltung und der Psychotherapeuten als Berufsgeheimnisträger.

Grundlage einer erfolgversprechenden Psychotherapie ist ein uneingeschränktes Vertrauensverhältnis zwischen Patient und Psychotherapeut. Nur unter dieser Voraussetzung kann das Therapieziel, wozu auch Gewaltprävention zählen kann, erreicht werden.

Insbesondere auch Personen, die eine Gewalttat erwägen, werden darüber im Rahmen einer psychotherapeutischen Behandlung überhaupt nur unter dieser Voraussetzung berichten. Die besondere Schutzbedürftigkeit von Gesprächen zwischen Psychotherapeuten und ihren Patienten bringt die dringende Notwendigkeit mit sich, allen Patienten die Sicherheit zu geben, dass eine psychotherapeutische Behandlung, aber auch schon die Kontaktaufnahme keine negativen Konsequenzen nach sich ziehen kann. Dieses Vertrauen wird durch die Regelungen im BKAG-E untergraben. Insbesondere Patienten, bei denen ein im Extremfall wahnhaftes Misstrauen Ausdruck ihrer Erkrankung ist, haben in der Regel große Schwierigkeiten, Vertrauen zu einem Psychotherapeuten aufzubauen und zu halten. Alle Patienten benötigen die Möglichkeit, sich jederzeit und insbesondere in Krisensituationen an einen Psychotherapeuten wenden zu können und auf die uneingeschränkte Gewährleistung der absoluten Vertraulichkeit ihrer Gespräche vertrauen zu können. Bereits das Gefühl einer Überwachung kann eine unter Umständen überlebensnotwendige Kontaktaufnahme verhindern.

Geheimnisse, die in der Psychotherapie offenbart werden, sind regelmäßig dem Kernbereich der privaten Lebensführung zuzuordnen, sodass sie einem besonders hohen Schutz unterliegen müssten. Dennoch werden in § 62 Absatz 1 Seite 7 BKAG-E Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten nicht ausdrücklich genannt. Anders als Gespräche mit Seelsorgern unterliegen die Gespräche mit Psychotherapeuten nicht dem absoluten Schutz.

## II. Einbeziehung von Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten in den absoluten Schutz – § 62 Absatz 1 BKAG-E

Die BPtK begrüßt ausdrücklich die Einbeziehung von Rechtsanwälten in den absoluten Schutzbereich der Vorschrift. Die BPtK hält jedoch die Einbeziehung von Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten in den Schutzbereich für mindestens so dringlich. Psychotherapeutische Gespräche berühren stets den Kernbereich privater Lebensführung. Intime Einblicke in die Persönlichkeit des Patienten sind konstitutiv für eine gelingende Psychotherapie.

Besonders problematisch ist dabei der Umstand, dass nicht nur das tatsächlich überwachte psychotherapeutische Gespräch beeinträchtigt wird. Die Therapie wird bereits durch die Möglichkeit beeinträchtigt, dass ein Gespräch nicht vertraulich bleibt und eine Kenntnisnahme Dritter vom Inhalt eines Gesprächs nicht von vornherein ausgeschlossen ist. Es ist von einer Vielzahl von Fällen auszugehen, in denen sich ein Patient aufgrund seiner psychischen Erkrankung bei der abstrakt bestehenden Möglichkeit der Überwachung entscheidet, eine dringend erforderliche Therapie nicht in Anspruch zu nehmen. Davon ist besonders bei bestimmten Diagnosen und Symptomen auszugehen, wie sie sich regelhaft bei psychotischen und paranoiden Störungen finden – diese Patienten würden damit krankheitsbedingt von der notwendigen Behandlung in nicht vertretbarer Weise abgehalten werden. Zum Schutz aller Patienten muss eine Überwachung eines psychotherapeutischen Gesprächs, aber auch der Kontaktaufnahme mit einem Psychotherapeuten absolut ausgeschlossen sein.

Geheimnisse, die in der Psychotherapie offenbart werden, sind regelmäßig dem Kernbereich der privaten Lebensführung zuzuordnen, sodass sie einem besonders hohen Schutz unterliegen müssen. Die BPtK hält daher die ausdrückliche Nennung der Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten in § 62 Absatz 1 Satz 7 BKAG-E für erforderlich. Eine Begrenzung des Anwendungsbereiches der Überwachungsmaßnahmen nach Abschnitt 5 des BKAG – Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus – durch eine Einbeziehung von Psychotherapeuten in den absoluten Schutzbereich würde diese Problematik beseitigen. Die Psychotherapeut-Patient-Beziehung wäre staatlichem Eingriff entzogen.

Die einzelfallbezogene Verhältnismäßigkeitsprüfung bietet nicht die Gewähr, dass dem Patienten der absolute Schutz seines psychotherapeutischen Gesprächs mit dem Psychotherapeuten deutlich ist.

Anzumerken bleibt noch, dass die Einbeziehung von allen in § 53 Absatz 1 Nummer 3 StPO genannten Berufsgeheimnisträgern in den absoluten Schutz von § 62 BKAG aus unserer Sicht sinnvoll erscheint. Von den dort genannten Berufsgruppen ist der Schutz von Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten sowie von psychotherapeutisch tätigen Ärzten aus Sicht der BPtK jedoch am dringlichsten geboten. Denn – anders als bei den anderen genannten Berufsgruppen

– berühren psychotherapeutische Gespräche unabhängig von ihrem Inhalt stets den absolut zu schützenden Kernbereich privater Lebensführung.

Um den Schutz aller Patientinnen und Patienten von Psychotherapeuten sicherzustellen, sollte in Artikel 1 des Entwurfs folgende Änderung ergänzt werden:

**Änderungsvorschlag zu Artikel 1**

§ 62

Schutz zeugnisverweigerungsberechtigter Personen

(1) Maßnahmen nach diesem Abschnitt, die sich gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. § 41 Absatz 3 bleibt unberührt. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 bis 6 nur, soweit es sich um Rechtsanwälte**,** ~~**oder**~~ Kammerrechtsbeistände**, Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten oder Apotheker** handelt.

(...)

## III. Auskunftsverweigerungsrecht für Psychotherapeuten – § 41 BKAG-E

Das in § 41 BKAG-E normierte Auskunftsverweigerungsrecht sollte für alle Berufsgeheimnisträger und dabei insbesondere für Psychotherapeuten gelten.

§ 53 Absatz 1 Seite 1 StPO regelt für alle Berufsgeheimnisträger, wie z. B. Geistliche, Verteidiger, Rechtsanwälte, Abgeordnete, Ärzte und Psychotherapeuten, das Zeugnisverweigerungsrecht. Anders als bei einer Psychotherapie müssen im Rahmen ihrer Tätigkeit nicht allen in dieser Vorschrift ausdrücklich genannten Berufsgruppen zwingend Informationen aus dem Kernbereich der privaten Lebensführung offenbart werden. Angesichts der Intimität der in der Psychotherapie regelmäßig offenbarten Geheimnisse und der Bedeutung des Vertrauensschutzes und damit der Schweigepflicht für die Psychotherapie und deren Erfolg ist die Stellung der Psychotherapeuten als Berufsgeheimnisträger im Gesetz zur Neustrukturierung des BKAG entsprechend des § 53 StPO zu festigen.

Psychotherapeuten müssen wie in § 53 Absatz 1 Seite 1 StPO den gleichen privilegierten Schutz wie Geistliche erhalten. Beide Berufsgruppen bieten in seelischen Krisen und Notlagen Hilfe durch Beratung oder psychotherapeutische Behandlung. Es ist kein Grund ersichtlich, der Geistlichen ein absolutes Auskunftsverweigerungsrecht einräumt, aber dies nicht für Psychotherapeuten vorsieht.

Um den notwendigen Schutz der zeugnisverweigerungsberechtigten Berufsgeheimnisträger sicherzustellen, sollte in Artikel 1 § 41 Absatz 3 folgende Änderung vorgenommen werden:

**Änderungsvorschlag zu Artikel 1**

§ 41
Befragung und Auskunftspflicht

(…)

(3) Unter den in den §§ 52 bis 55 der Strafprozessordnung bezeichneten Voraussetzungen ist die betroffene Person zur Verweigerung der Auskunft berechtigt. Dies gilt nicht, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person erforderlich ist. Eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder 4 der Strafprozessordnung genannte Person

ist auch in den Fällen des Satzes 2 zur Verweigerung der Auskunft berechtigt. Die betroffene Person ist über ihr Recht zur Verweigerung der Auskunft zu belehren. Auskünfte, die nach Satz 2 erlangt wurden, dürfen nur für den dort bezeichneten Zweck verwendet werden. Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 bis 5 nur, soweit es sich um Rechtsanwälte**, ~~und~~** Kammerrechtsbeistände **sowie um Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten und Apotheker** handelt.

## IV. Prognoseentscheidung – Psychotherapeutische Praxis als geschützter Raum – § 45 Absatz 7 BKAG-E

Vor der Durchführung von Maßnahmen nach § 45 BKAG-E (Besondere Mittel der Datenerhebung) soll eine Prognoseentscheidung getroffen werden, damit allein Äußerungen, die den Kernbereich der persönlichen Lebensgestaltung betreffen, nicht erfasst werden. In der Gesetzesbegründung zu § 45 Absatz 7 BKAG ist nicht darauf verwiesen, dass bei einem psychotherapeutischen Gespräch stets der Kernbereich der privaten Lebensgestaltung betroffen ist. Eine solche Klarstellung ist vorzunehmen. Zudem ist ein Hinweis aufzunehmen, dass anders als bei sonstigen Geschäftsräumen der Umstand, dass ein Gespräch zwischen Patient und Psychotherapeut in einer psychotherapeutischen Praxis geführt wird, gerade für das Betreffen des Kernbereichs der persönlichen Lebensgestaltung spricht und daher die Maßnahme zu unterlassen ist. Die psychotherapeutische Praxis ist ein nicht-öffentlicher Raum, der der vertraulichen Beziehung zwischen Patient und Psychotherapeut dient, in dem frei gesprochen werden soll und der Patient sich geschützt fühlt.

Die BPtK schlägt daher folgende Änderung in der Gesetzesbegründung zu Artikel 1 § 45 BKAG-E vor:

**Änderungsvorschlag zur Gesetzesbegründung Artikel 1**

**Zu § 45 (Besondere Mittel der Datenerhebung)**

**(...)**

**Zu Absatz 7**

(...)

Nach Satz 1 ist daher vor der Durchführung der Maßnahme, also auf der Erhebungsebene, eine Prognose dahingehend zu treffen, dass mit der Maßnahme allein Äußerungen, die den Kernbereich der persönlichen Lebensgestaltung betreffen, nicht erfasst werden. Diese Prognose muss sich auf tatsächliche Anhaltspunkte stützen; vollständige Gewissheit ist demnach nicht erforderlich. Anhaltspunkte, anhand welcher Kriterien eine solche Prognose zu erstellen sein kann, können sich aus der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander ergeben. Schützenswert ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens. Zu diesen Personen können insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, sowie Strafverteidiger, Ärzte, **Psychotherapeuten,** Geistliche und enge persönliche Freunde zählen. Dabei ist zu beachten, dass entsprechend § 100c Absatz 4 Satz 2 StPO Gespräche in Betriebs- und Geschäftsräumen in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen sind**, es sei denn, es handelt sich um Räume, die ausdrücklich einem besonderen Vertrauensverhältnis dienen, wie etwa eine psychotherapeutische Praxis**. (...)

**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)791

DGKJP - Deutsche Gesellschaft für Kinder- und Jugendpsychiatrie,
Psychosomatik und Psychotherapie e.V.
Geschäftsstelle • Reinhardtstraße 27 B • 10117 Berlin

dgkjp

Deutsche Gesellschaft für Kinder- und Jugendpsychiatrie, Psychosomatik und Psychotherapie e.V.

# Stellungnahme der Deutschen Gesellschaft für Kinder- und Jugendpsychiatrie, Psychosomatik und Psychotherapie

## zum Gesetzentwurf der Bundesregierung

## Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (BKA-G)

### Stellungnahme zu den Eckpunkten:

Das Bundeskabinett hat in seiner Sitzung vom 01.02.2017 den oben genannten Gesetzentwurf beschlossen. Der Gesetzentwurf dient der Umsetzung des Bundesverfassungsgerichtsurteils vom 20.04.2016 und der Richtlinie EU 2016/680 vom 27.04.2016.

Die DGKJP hält die vorgesehenen Änderungen zum Schutz zeugnisverweigerungsberechtigter Personen nur teilweise für gelungen. Selbstverständlich begrüßen wir z.B., dass der Gesetzentwurf den Schutz der Rechtsanwälte weiter ausbaut. Leider wird der Schutz von Angehörigen der Heilberufe nur unzureichend gewährleistet. Als wissenschaftliche Fachgesellschaft, welche die Fachärzte für Kinder- und Jugendpsychiatrie und Psychotherapie vertritt, sind wir gerade mit Blick auf die Inanspruchnahme von Hilfe durch gefährdete Jugendliche mit einem möglichen Gefährderpotential alarmiert. Wir möchten darauf hinweisen, dass gerade die vertrauensvolle Behandlungsbeziehung, die natürlich auch Telefonkontakte etc. mit einschließt, eine Grundvoraussetzung ist, gefährliche Entwicklungen früh zu erkennen und ggf. zusammen mit einem Jugendlichen und seiner Familie und wenn dies nicht hinreichend möglich ist, auch bei direkt drohender Gefahr, gegen dessen Willen, Maßnahmen zu ergreifen. Wie bereits von einigen anderen Verbänden moniert, sollten auch aus Sicht unserer Fachgesellschaft, insbesondere (kinder- und jugend-) psychiatrisch und psychotherapeutisch tätige Ärzte und andere psychotherapeutisch tätige Personen erweiterten Schutz genießen.

**Stellungnahme zum Regelungstext:**

Im Einzelnen wird in der gebotenen Kürze zum geplanten § 62 BKA-Gesetzentwurf, der den bisherigen § 20 u BKA-Gesetz ersetzen soll, wie folgt Stellung genommen:

§ 62 BKA-Gesetzentwurf soll – wie schon bisher § 20 u BKA-Gesetz - nicht alle Personen, die nach § 53 StPO ein Zeugnisverweigerungsrecht besitzen, erfassen. In § 62 Abs.1 werden künftig (wohl als Reaktion auf das Urteil des BVerfG vom 20.04.2016) jedenfalls Rechtsanwälte erfasst werden. Dies halten wir für richtig, aber für nicht ausreichend.
Gerade für psychotherapeutisch tätige Ärzte und Angehörige anderer psychotherapeutisch tätiger Berufsgruppen ist absolute Vertraulichkeit von höchster Bedeutung. Der Aufbau einer auf Vertrauen basierenden Beziehung ist Ausgangspunkt der therapeutischen Tätigkeit. Ohne den Aufbau von entsprechendem Vertrauen ist eine Behandlung nicht möglich. Es besteht jedenfalls die Gefahr, dass der/ die Patient(in) sich nicht öffnen wird, wenn er/ sie sich der Gefahr ausgesetzt sieht, dass die übermittelten Informationen nicht geschützt sind. Besonders sensibel ist das Ganze selbstverständlich bei der Behandlung von Kindern und Jugendlichen, was z.B. Angaben über deren Eltern oder die Kernfamilie betrifft.

Daher fordern wir im Interesse der uns als Patienten anvertrauten Kinder und Jugendlichen, § 62 BKA-Gesetzentwurf um die Gruppe der psychotherapeutisch tätigen Ärzte und andere psychotherapeutisch tätige Personen zu erweitern.

Gerade für Kinder und Jugendliche wäre überdies die Überwachung von email-, SMS-, Skype oder telefonischer Kommunikation mit dem Arzt oder Psychotherapeuten fatal. V.a. Kinder und Jugendliche mit Migrations- oder Fluchthintergrund nutzen diese Medien viel und alle Jugendlichen nutzen sie zunehmend auch zur Kommunikation mit ihren Therapeuten. Die real mögliche Überwachung ist dazu angetan, irreale paranoide Befürchtungen zu stimulieren und kann von den therapeutisch Tätigen künftig nicht mehr entkräftet werden.

Wir halten es nicht für ausreichend, dass diese Berufsgruppen nur nach § 62 Abs.2 BKA-Gesetzentwurf geschützt werden. Die unter § 53 Abs.1 Nr. 3 StPO genannten Berufsgruppen (also z.B. auch Ärzte und Psychotherapeuten) sind nämlich nur insofern geschützt als nach dem neuen § 62 Abs.2 BKA-Gesetz weiterhin eine Verhältnismäßigkeitsprüfung im Einzelfall durchgeführt werden muss.
Insbesondere erschließt sich uns auch nicht, wo der Unterschied zwischen dem Vertrauensverhältnis zwischen einem Rechtsanwalt/Verteidiger und seinem Mandanten einerseits und dem Vertrauensverhältnis zwischen Patient und Arzt/ Psychologischem Psychotherapeut/ Kinder- und Jugendlichenpsychotherapeut gesehen wird.

Wir verstehen durchaus, dass Zweck des BKA- Gesetzes auch bzw. sogar vor allem eine möglichst gute Gefahrenabwehr sein soll. Es darf aber nicht verkannt werden, dass eine gelungene psychiatrische und/ oder psychotherapeutische Behandlung durchaus auch zur Gefahrenabwehr beitragen kann. Wie bereits beschrieben, kann dies aber nur im unbedingt geschützten Raum erfolgen.

Das BVerfG weist in der Urteilsbegründung selbst auf die Vertraulichkeit psychotherapeutischer Gespräche hin, die sich insofern von Gesprächen mit Geistlichen nicht unterscheiden. Weiter weist das BVerfG darauf hin, dass solche Gespräche in vielen Fällen sowieso zum Kernbereich privater Lebensgestaltung gehören. Das macht es nach unserer Auffassung unbedingt erforderlich, den hier bereits angelegten Schutz auch im Gesetz zu normieren. Für atypische Fälle ließe sich beispielsweise auch eine Ausnahmeregelung in das Gesetz integrieren.

**Fazit:**

Die Regelung in § 62 BKA-Gesetzentwurf berücksichtigt psychotherapeutisch tätige Ärzte wie die von uns vertretenen Fachärzte für Kinder- und Jugendpsychiatrie und –psychotherapie, Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten in kinder- und jugendpsychiatrischen Einrichtungen nicht ausreichend. Wir halten eine Erweiterung der Vorschrift für erforderlich.

Analog sollte § 41 um ein Auskunftsverweigerungsrecht von psychotherapeutisch tätigen Ärzten erweitert werden. In der Gesetzesbegründung zu § 45 BKA-Gesetz sollte klargestellt werden, dass auch Gespräche mit nicht-ärztlichen Psychotherapeuten zur nichtöffentlichen Kommunikation mit Personen des höchstpersönlichen Vertrauens gehören.

Nicht zuletzt sei darauf hingewiesen, dass das Gesetz auch enorme Auswirkungen auf Patienten haben wird, die nicht die Zielpersonen von Überwachungsmaßnahmen („verdeckter Eingriff in elektronische Systeme“) sind.
Es ist unseres Erachtens nicht hinreichend geprüft worden, inwieweit dieses Gesetzesvorhaben mit dem vor nicht allzu langer Zeit verabschiedeten Patientenrechtegesetz kollidiert, das sich auch auf Kinder und Jugendliche z.B. in kinder- und jugendpsychiatrischer und psychotherapeutischer Behandlung bezieht.

Der Vorstand der DGKJP im März 2017

**Richter Sandy PA4**

**Von:** Schaper, Karin (DAV) <schaper@anwaltverein.de>
**Gesendet:** Freitag, 7. April 2017 12:29
**Betreff:** DAV-SN 33-2017 zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes
**Anlagen:** DAV-SN_33-17.pdf

Sehr geehrte Damen und Herren,

in der Anlage übersende ich Ihnen die Stellungnahme Nr. 33/2017 des Deutschen Anwaltvereins durch seinen Ausschuss Gefahrenabwehrrecht zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes.

Der Gesetzesentwurf begegnet zum Teil schweren Bedenken. Hinsichtlich der vorgesehenen Einrichtung eines zentralen polizeilichen Informationssystems beim BKA sind die Grenzen der polizeilichen Datennutzung zu unbestimmt. Die Vorschriften zur Datenübermittlung im In- und Ausland genügen den Anforderungen der verfassungsrechtlichen Rechtsprechung nicht und sind insgesamt zu undurchsichtig.

An vielen Stellen lässt der Gesetzesentwurf Normenklarheit vermissen und beschränkt sich darauf, die vom Bundesverfassungsgericht postulierten Anforderungen schlicht im Wortlaut in den Gesetzestext zu übernehmen. Der DAV fordert den Gesetzgeber auf, transparente Regelungen darüber zu schaffen, wo und durch wen Informationen gespeichert, verwendet oder weitergegeben werden.

Das in § 55 geregelte Aufenthalts- und Kontaktverbot verlagert den Bereich der Gefahrenabwehr noch weiter vor und ist angesichts der Intensität des mit ihm verbundenen Grundrechtseingriffes unverhältnismäßig. Die elektronische Fußfessel ist zur Gefahrenabwehr bereits ungeeignet. Des Weiteren regelt der Gesetzesentwurf den Richtervorbehalt nur lückenhaft, etwa beim Einsatz von verdeckten Ermittlern und V-Leuten. Ausdrücklich begrüßt wird, dass der Gesetzesentwurf nunmehr wie in § 160a StPO ein einheitliches Schutzniveau für alle anwaltlichen Berufsgeheimnisträger schafft.

Einzelheiten entnehmen Sie bitte der ausführlich begründeten Stellungnahme.

Mit freundlichen Grüßen

Max Gröning
Referent in der Geschäftsführung

**Deutscher Anwaltverein**
Rechtsanwalt Max Gröning
Referent in der Geschäftsführung
Littenstraße 11, 10179 Berlin
Tel. +49 30 72 61 52 -106
groening@anwaltverein.de

Sekretariat: Karin Schaper
Tel. +49 30 72 61 52 -171
Fax +49 30 72 61 52 -195

DeutscherAnwaltVerein

# Stellungnahme

## des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht

## zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

**Stellungnahme Nr.: 33/2017** **Berlin, im April 2017**

### Mitglieder des Ausschusses

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende und Berichterstatterin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwältin Dr. Annika Dießner, Berlin (Berichterstatterin)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln (Berichterstatter)
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln (Berichterstatter)
- Rechtsanwalt Dr. Stefan König, Berlin (Berichterstatter)
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main (Berichterstatterin)
- Rechtsanwältin Kerstin Oetjen, Freiburg (Berichterstatterin)
- Rechtsanwältin Lea Voigt, Bremen (Berichterstatterin)

### Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

**Deutscher Anwaltverein**
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

**Büro Brüssel**
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

## Verteiler

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag - Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Deutscher Richterbund
Bundesverband der Freien Berufe
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) der Universität Trier

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung
Berliner Zeitung
Juris Newsletter
JurPC

**Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 66.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.**

---

## 1. Teil: Einleitung

Mit dem Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (im Folgenden BKAG-E) will die Bundesregierung das Urteil des BVerfG vom 20. April 2016[1] und die Richtlinie (EU) 2016/680 vom 27. April 2016 umgesetzt wissen.

Dimension und Reichweite des Gesetzesentwurfes spiegeln sich nicht nur im Erfüllungsaufwand der Verwaltung – z.B. beziffert der Entwurf die Verwirklichungskosten des BKA mit EUR 254 Mio. und dessen wiederkehrende Personal- und Sachkosten mit jährlich EUR 29,4 Mio. – wieder, sondern auch in der Komplexität des Regelwerkes, die dem Betroffenen keine Chance lässt, sicher beurteilen zu können, ob und welche Informationen von wem dauerhaft gespeichert, verwendet oder weitergegeben werden. Hinzu kommt, dass der BKAG-E die vom BVerfG postulierten Anforderungen an die Ausgestaltung von Anordnungsbefugnissen nicht normenklar regelt, sondern sich darauf beschränkt, diese schlicht als Gesetzeswortlaut zu übernehmen. Der Reihe nach:

Der BKAG-E regelt unter anderem:

- eine neue Struktur der IT-Architektur des BKA,
- Datenübermittlungsvorschriften,
- Anordnungsbefugnisse, die weit über den Maßnahmenkatalog der StPO hinausgehen,
- ein Aufenthalts- und Kontaktverbot,
- die elektronische Aufenthaltsüberwachung,
- Richtervorbehalte.

[1] NJW 2016, 1781.

Der Entwurf begegnet tiefgreifenden rechtlichen Bedenken:

## A. Datenschutzkontrolle/IT-Struktur

Mit Urteil vom 20. April 2016 hat das BVerfG Vorschriften des BKAG teilweise für verfassungswidrig erklärt. Diese Entscheidung nimmt die Bundesregierung zum Anlass, den polizeilichen Datenschutz völlig neu auszurichten. Das BKA soll einen „einheitlichen polizeilichen Informationsverbund“ unterhalten[2], in den sämtliche von Bundes- und Landespolizeien erhobenen und vorgehaltenen Daten ohne nähere Zweckbestimmung eingespeist werden sollen. Entgegen der insoweit immer noch geltenden Vorgaben des Volkzählungsurteils vom 15. Dezember 1983[3] wird damit aber keine Begrenzung, sondern eine Entgrenzung des Handlungsrahmens der Sicherheitsbehörden bewirkt[4]. Denn nach der Neugestaltung des polizeilichen Datenschutzes ist der Erstellung von „Persönlichkeitsprofilen“ fortan „Tür und Tor“ geöffnet.

## B. Übermittlungsvorschriften

Dass der Entwurf weit über die Vorgaben des Urteils des BVerfG vom 20. April 2016 hinausgeht, zeigen auch und insbesondere die Regelungen zur Datenweitergabe. Unter Verstoß gegen das vom BVerfG entwickelten Prinzips der hypothetischen Datenneuerhebung soll eine solche Erhebung bereits dann zulässig sein, wenn „vergleichbar bedeutsame Rechtsgüter“ dies erforderten. Auf die Maßgabe, dass eine Zweckänderung nur dann gerechtfertigt ist, wenn bei vergleichbar bedeutsam einzustufendem Rechtsgüterschutz eine Neuerhebung auch mit „vergleichbar schwerwiegenden Mitteln“ zulässig wäre, soll es nicht mehr ankommen. Noch schwerer wiegt, dass das BKA ohne „Ersuchen“ eines Mitgliedsstaates „spontan“ auf eigene Initiative Daten an Mitgliedsstaaten übermitteln darf. Damit ist der Weg einer zentralen europäischen Datenbank vorgezeichnet, bei der sämtliche in den Mitgliedsstaaten gesammelten Daten gespeichert und diese von unzähligen Behörden ohne justizielle

[2] Vgl. § 2 Abs. 3 BKAG-E.
[3] *BVerfG* NJW 1984, 419.
[4] Vgl. zum geltenden Recht Roggan/*Kutscha* Handbuch zum Recht der Inneren Sicherheit 2. Auflage S. 39.

Kontrolle eingesehen und verwertet werden könnten. Bedenken bestehen auch bezüglich der Übermittlung im internationalen Bereich. Der BKAG-E stellt nicht sicher, dass die vom BVerfG geforderte „Vergewisserung“, Daten nur an solche Länder weiterzugeben, die ein angemessenes (rechtsstaatliches) Schutzniveau garantieren, auch tatsächlich erfolgt. **Der Gesetzgeber ist aufgefordert, transparente Regelungen darüber zu schaffen, wo und durch wen Informationen gespeichert, verwendet oder weitergegeben werden. Der BKAG-E ist hiervon weit entfernt, er ist schon für Juristen kaum verständlich, Nichtjuristen haben keine Möglichkeit, die Tragweite der Regelung zu durchschauen, für sie stellen sich Datenerhebung und -weiterleitung als „Black Box“ dar.**

## C. Befugnisse

Gerade für Anordnungsbefugnisse mit einem gravierenden Eingriffsgewicht fehlt es an hinreichend bestimmten Kriterien, die das BVerfG geregelt wissen will. Die höchstrichterliche Forderung nach Normenklarheit versucht der BKAG-E dadurch nachzukommen, dass er die vom BVerfG geforderten Kriterien (nur) im Wortlaut übernimmt – diese aber nicht regulatorisch ausfüllt. § 45 BKAG-E (= Besondere Mittel der Datenerhebung) zeigt dies eindrucksvoll. Während das BVerfG zum Beispiel für den Einsatz von Verdeckten Ermittlern eine auf eine Gefahr bezogene Prognose verlangt, die sich nicht nur auf allgemeine Erfahrungssätze stützt, sondern zum Beispiel auf ein individuelles Verhalten einer Person, das die konkrete Wahrscheinlichkeit begründet, sie werde in überschaubarer Zukunft terroristische Straftaten begehen, beschränkt sich § 45 Abs. 1 S. 1 Nr. 3 BKAG-E darauf, Urteilsgründe 1:1 im Wortlaut zu übernehmen. Das aber ist keine Umsetzung der Vorgaben des BVerfG, das ist nur „Copy+Paste“ – mit der Folge, dass es an Normenklarheit fehlt. Zudem fällt § 49 BKAG-E (= Onlinedurchsuchung) hinter § 20 k BKAG zurück. Entgegen der Vorgaben des BVerfG soll die Onlinedurchsuchung nach § 49 Abs. 1 S. 2 Nr. 1 BKAG-E zulässig sein, wenn bestimmte Tatsachen die Annahme rechtfertigten, dass innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt. Mit Urteil vom 20. April 2016 hat das BVerfG jedoch klargestellt, dass nur in informationstechnische Systeme von solchen Personen eingegriffen werden darf, die erkennbar an der in Rede stehenden Rechtsgutverletzung beteiligt und die hinreichend individualisierbar sind. Die Regelung

über die Vorratsdatenspeicherung (§ 52 BKAG-E = Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten) bedient sich der gleichen Technik und übernimmt Urteilsgründe ihrem Wortlaut nach. Hier kommt hinzu, dass die Norm mit den Vorgaben des Europäischen Gerichtshofes mit Urteil vom 21. Dezember 2016 (Az: C-203/15, C-698/15) unvereinbar ist, da sie keine Beschränkung auf das „absolut Notwendige“ vorsieht.

## D. Aufenthalts- und Kontaktverbot

Das in § 55 BKAG-E geregelte Aufenthalts- und Kontaktverbot richtet sich an Personen, die weder Verdächtige im Sinne der StPO noch Verursacher einer Gefahr (Störer) sind. Es soll zum Beispiel ausreichen, dass das individuelle Verhalten der betroffenen Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine Straftat nach § 5 Abs. 1 S. 2 begehen wird[5]. Mit diesem neuen Begriff des „Gefährders“ wird der Bereich der Gefahrenabwehr noch weiter vorverlagert, als er dies ohnehin schon ist. Der damit verbundene Grundrechtseingriff ist unverhältnismäßig.

## E. Elektronische Aufenthaltsüberwachung

Die in § 56 BKAG-E geregelte elektronische Aufenthaltsüberwachung ist als Mittel der Gefahrenabwehr ungeeignet. Die Evaluation der im Bereich der Führungsaufsicht in § 68 b Abs. 1 S. 1 Nr. 12 StGB geregelten elektronischen Fußfessel hat ergeben, dass diese ungeeignet ist, die Betroffenen von Straftaten abzuhalten. Gleiches gilt für die Gefahrenwehr. Kein Terrorist wird sich aufgrund einer elektronischen Fußfessel davon abhalten lassen, Straftaten zu begehen.

## F. Richtervorbehalt

Der Richtervorbehalt ist zum Teil nur lückenhaft geregelt. So ist zum Beispiel nach der Entscheidung des BVerfG vom 20. April 2016 jeder Einsatz von Verdeckten Ermittlern richterlich zu genehmigen – und nicht nur solche Einsätze, in denen der verdeckte

[5] Vgl. § 55 Abs. 1 Nr. 2 BKAG-E.

Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist. Hier muss nachgebessert werden. Gleiches gilt für den Einsatz von Vertrauenspersonen.

## 2. Teil: Regelungen im Einzelnen

### A. Datenschutzkontrolle / IT-Struktur

**I.**

Der Gesetzesentwurf sieht weitreichende Veränderungen im Bereich der polizeilichen Datenverarbeitung vor. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts zum BKA-Gesetz vom 20. April 2016 sowie die Vorgaben aus der EU-Richtlinie umzusetzen, sondern geht weit darüber hinaus. Dies hat gravierende Konsequenzen für den Datenschutz. Das BKA soll zur Erfüllung seiner Funktion als informationelle Zentralstelle mit einem neu zu konstruierenden „einheitlichen Verbundsystem“[6] ausgestattet werden. Im Gegensatz zu dem bisherigen „polizeilichen Informationssystem“[7] sollen die Daten von Landes- und Bundespolizeien zentral im BKA vorgehalten werden[8]. Das bisher geltende Prinzip einzelner logischer Dateien, durch das vorhandene Daten gewissermaßen in unterschiedlichen Schubladen lagen, soll aufgegeben werden. Dadurch werden die Daten global durchsuch-, auswert- und analysierbar.

Begründet wird diese Umstrukturierung mit der Entscheidung des Bundesverfassungsgerichts zum BKAG vom 20. April 2016 (1 BvR 966/09 u. a.). Dort werde der bisherigen „vertikalen“ IT-Architektur eine Absage erteilt[9], weshalb dringender und grundlegender Neuregelungsbedarf bestehe. Das Urteil gebe dem Gesetzgeber auf, die Grundsätze der *Zweckbindung* und der *hypothetischen Datenneuerhebung* zu verwirklichen. Dies sei mit einer Unterteilung in logische Dateien nicht möglich, da „[i]nnerhalb einer Datei, auf die der jeweilige Bearbeiter aufgrund seiner Zugehörigkeit zu einer Organisationseinheit des

[6] Vgl. §§ 2 Abs. 3, 29 Abs. 1 BKAG-E.
[7] Vgl. § 2 Abs. 3 BKAG.
[8] Vgl. S. 91 d. Regierungsentwurfs.
[9] Vgl. S. 89 des Regierungsentwurfs.

Bundeskriminalamtes Zugriff hat“, dieser „(rollenabhängig) auf alle Daten zugreifen“ könne[10].

In der avisierten zentralen Datenhaltung sollen alle Daten hinsichtlich ihres Ursprungs und des Erhebungszwecks gekennzeichnet sein[11], womit eine Prüfung der ebenfalls geregelten Voraussetzungen für eine Zweckänderung[12] ermöglicht werden soll. Dies sei nach der Entscheidung des BVerfG erforderliche, aber auch *hinreichende* Bedingung, um den Persönlichkeitsrechten der Betroffenen gerecht zu werden. Weiterer, die Datenverarbeitung einschränkender Maßgaben bedürfe es nicht[13].

**II.**

Sowohl die vorgeschlagene Neustrukturierung des polizeilichen Datenverbundes selbst als auch die in dem Entwurf angeführte Begründung begegnet grundlegenden Bedenken.

1.

Auch wenn man die Entscheidung des Bundesverfassungsgerichts so liest wie die Verfasser des Gesetzesentwurfs, ergibt sich aus ihr nicht zwingend das Erfordernis der Schaffung eines globalen polizeilichen Datenbestandes. Eine Kennzeichnung der einzelnen Daten (bzgl. Quelle, Erhebungszweck etc.) wäre auch im Rahmen der Speicherung in logischen Dateien möglich.

2.

Zudem sind beide datenschutzrechtlichen Prinzipien (Zweckbindung, hypothetische Neuerhebung) seit dem Volkszählungsurteil des BVerfG etabliert und wurden seitdem vom BVerfG vielfach wiederholt und konkretisiert. So hat das BVerfG etwa in seiner Entscheidung zur Fernmeldeüberwachung durch den Bundesnachrichtendienst ausgeführt[14]:

[10] Vgl. S. 89 f. d. Regierungsentwurfs.
[11] Vgl. § 14 Abs. 1 BKAG-E.
[12] Vgl. § 12 BKAG-E.
[13] Vgl. S. 90 des Regierungsentwurfs.
[14] *BVerfG*, 1 BvR 2226/94 u. a., *NJW* 2000, 55, 57.

*„Zwar schließt der Grundsatz der Zweckbindung Zweckänderungen nicht rundweg aus. Sie bedürfen jedoch ihrerseits einer gesetzlichen Grundlage, die formell und materiell mit dem Grundgesetz vereinbar ist. Dazu gehört, dass die Zweckänderungen durch Allgemeinbelange gerechtfertigt sind, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden, und hinreichend normenklar geregelt sein. Ferner dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht miteinander unvereinbar sein (vgl. BVerfGE 65, 1 [51, 62] = NJW 1984, 419).*

*Die Zweckbindung lässt sich nur gewährleisten, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungswegen geboten.“*

Es erstaunt deshalb, dass nun plötzlich so ein enormer Handlungsdruck gesehen wird. Betrachtet man zusätzlich die kurze Zeitspanne zwischen der Urteilsverkündung in Karlsruhe und der Veröffentlichung des ersten Referentenentwurfs und dort insbesondere der enormen, für den Bund bereits konkret bezifferten Beschaffungskosten für die neue EDV, liegt die Vermutung nahe, dass die Entscheidung des Bundesverfassungsgerichts nicht Auslöser, sondern Katalysator des gesetzgeberischen Vorhabens ist bzw. sein soll.

3.
Es mag viele gute Gründe geben, das polizeiliche EDV-System grundlegend zu reformieren und den heutigen technischen Möglichkeiten anzupassen. Indem aber – wenig überzeugend – vorgegeben wird, die Neuregelung sei in erster Linie ein Gebot des Datenschutzes, wird eine offene, kritische und besonnene Diskussion erschwert. Diese ist aber angesichts der grundrechtlichen Dimension polizeilicher Datenverarbeitung dringend erforderlich.

4.
Bei genauerer Betrachtung erscheinen die wenigen in dem Entwurf vorgesehenen Grenzen der polizeilichen Datennutzung, durch die der reklamierte Grundrechtsschutz sichergestellt werden soll, zu unbestimmt. Es bleibt etwa offen, worin der Unterschied zwischen § 12 Abs. 1 Nr. 1 BKAG-E (es ist keine Zweckänderung, wenn die Datenverarbeitung der Erfüllung derselben Aufgabe oder zum Schutz derselben Rechtsgüter oder zur Verfolgung oder zur Verhütung derselben Straftaten) und der bisherigen Nutzung aller Daten innerhalb z.B. einer staatsschutzspezifischen Datei besteht. Daten, die bisher in einer solchen Datei lägen, sind auch nach dem neuen Modell für den polizeilichen Anwender nutzbar (da dies – im Bereich Staatsschutz – dem Schutz derselben Rechtsgüter dient). Letztlich scheint daher der wesentliche Unterschied zwischen der bisherigen Rechtslage und der beabsichtigten Neuregelung die zentrale Datenhaltung zu sein.

5.
Konkrete Aussagen darüber, wie die niedrigen Schranken des § 12 Abs. 1 und 2 BKAG-E in dem neuen Informationspool konkret umgesetzt werden sollen, treffen weder der Gesetzesentwurf noch die Begründung. Es steht zu befürchten, dass ein Gesamtdatenbestand geschaffen wird, der zunächst global durchsuch- und auswertbar ist und bei dem eine Auslese der Ergebnisse anhand des Kriteriums der Erlaubnis zur Nutzung der Daten erst zu einem späteren Zeitpunkt „händisch“ stattfindet. Das würde – den theoretischen Beschränkungen zum Trotz – praktisch eine unbegrenzte Nutzbarkeit der Daten zumindest als „Spurenansatz“ nach sich ziehen.

6.
Die Fülle der Daten, die in einem einheitlichen polizeilichen Datenbestand anfallen werden, und die vielen Möglichkeiten, diese mithilfe von Such- und Analysealgorithmen auszuwerten, wirft die Frage auf, wie dem verfassungsgerichtlich anerkannten Verbot der Erstellung von Persönlichkeitsprofilen Rechnung getragen werden kann. Darin dürfte eine der größten Herausforderungen im Zusammenhang mit der Modernisierung der

polizeilichen Datenbanken liegen. Der Gesetzesentwurf versäumt es, dies in den Blick zu nehmen.

7.

Auch der neue Entwurf sieht vor, dass Daten von „Beschuldigten“ selbst dann weiter gespeichert werden dürfen, wenn das Strafverfahren ohne Verurteilung abgeschlossen wurde. Nur wenn der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren endgültig eingestellt wurde und die Gründe der Entscheidung ergeben, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat[15], ist die Weiterverarbeitung der Daten unzulässig. Die Polizei erhält so die Deutungshoheit über den sog. Restverdacht. Dies führt gerade bei Bagatellvorwürfen, bei denen die Verfahren durch die Staatsanwaltschaften ohne ausführliche Begründung eingestellt werden, dazu, dass die Betroffenen gegenüber der Polizei langfristig als „Beschuldigte“ gelten und sich das polizeiliche Register füllt, ohne dass der Person je eine Straftat nachgewiesen wurde. Die geplante Änderung des BKAG wäre eine gute Gelegenheit, hier nachzubessern.

## B. Übermittlungsvorschriften

Die Reichweite des BKAG-E kommt auch in den Regelungen über die Datenweitergabe zum Ausdruck.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat insoweit zutreffend mit Schreiben vom 22. Februar 2017[16] und mit Stellungnahme vom 10. März 2017[17] u.a. an den Vorsitzenden des Innenausschusses des Deutschen Bundestages datenschutzrechtlichen Verbesserungsbedarf angemeldet. Der DAV schließt sich diesen Vorschlägen an.

[15] Vgl. § 18 Abs. 5.
[16] Schreiben vom 22.02.2017 an den Vorsitzenden des Innenausschusses des Deutschen Bundestages et al.
[17] *Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 10..03.2017 zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes.*

## I. Prinzip der „hypothetischen Datenneuerhebung“

Das BVerfG hat mit Urteil vom 20. April 2016 entschieden, dass sich die Anforderungen an die Nutzung und **Übermittlung** staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung richten und sich die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung am Grundsatz der „*hypothetischen Datenneuerhebung*“ zu orientieren haben. Auch die Übermittlung von Daten an öffentliche Stellen im Ausland unterliege diesen verfassungsrechtlichen Grundsätzen der Zweckänderung und Zweckbindung.

Zur hypothetischen Datenneuerhebung hat das BVerfG u.a. Folgendes ausgeführt:[18] *Während früher im Rahmen der Verhältnismäßigkeit (nur) darauf abgestellt wurde, ob die geänderte Nutzung mit der ursprünglichen Zwecksetzung unvereinbar war, wurde dies inzwischen durch das Prinzip der **hypothetischen Datenneuerhebung** konkretisiert und ersetzt. Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den **geänderten Zweck** mit **vergleichbar schwerwiegenden Mitteln** erhoben werden dürften.*

### 1. Die innerstaatliche Übermittlung nach dem Regierungsentwurf

Die Übermittlung von Daten im innerstaatlichen Bereich ist bisher in § 10 BKAG normiert. Der Regierungsentwurf sieht jetzt dafür § 25 BKAG-E vor. Die Neu-Regelung wurde **durch einen Bezug auf § 12 Abs. 2 - 4 BKAG-E** modifiziert. § 12 BKAG-E regelt in allgemeiner Form und damit für **jede Datenverarbeitung** nach dem BKAG-E anwendbar[19] die „*Zweckbindung [nach dem] Grundsatz der hypothetischen Datenneuerhebung*“.

Der Regierungsentwurf interpretiert in seiner Begründung zu § 12 Abs. 2 - 4 BKAG-E das Prinzip der „hypothetischen Datenneuerhebung wie folgt:[20]

[18] Urteil vom 20.04.2016, Rn. 287 ff.
[19] Vgl. Regierungsentwurf, S. 110.
[20] Vgl. S. 111.

*„Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten* ***dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts*** *dient, die* ***verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln*** *rechtfertigen könnten."*

## 2. Die Bedeutung der Regelungen des BKAG über die innerstaatliche Datenübermittlung

Der Regelung der innerstaatlichen Übermittlung im BKAG kommt eine überragende Bedeutung zu. Denn die Befugnis zur Übermittlung von Dateiinformationen aus dem BKA-Datenbestand an **innerstaatliche** Strafverfolgungsbehörden entscheidet gleichzeitig über die Weitergabe an die Strafverfolgungsbehörden **in den Mitgliedsstaaten**.[21] Nach dem Rahmenbeschluss 2006/960/JI[22] des Rates der EU vom 18. Dezember 2006 „*über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union*" ist den Strafverfolgungsbehörden[23] eines anderen Mitgliedstaates unter den gleichen Bedingungen Zugang zu vorhandenen Informationen zu gewähren wie innerstaatlichen Behörden(„Diskriminierungsverbot").

Dies bedeutet, dass entsprechend dieses „Verfügbarkeitsprinzips" jedes europäisches Mitgliedslands, das z.B. den Zugang zu einer deutschen Datenbank wünscht, so behandelt wird, als handele es sich um eine deutsche anfordernde Strafverfolgungsbehörde. Es ist dann allein zu prüfen, ob es einer deutschen Polizeibehörde erlaubt wäre, unter den gegebenen Umständen die angeforderten Daten aus einem innerstaatlichen Dateisystem abzurufen. Ist dies zu bejahen, ist auch die Polizeibehörde aus dem Mitgliedsstaat dazu berechtigt. Umgekehrt erhalten auch deutsche Strafverfolgungsbehörden Zugang zu Dateien in den Mitgliedsstaaten in demselben Umfang, wie dies den dortigen Behörden untereinander gestattet ist. Wegen dieses Prinzips darf eine Übermittlung von

[21] So auch der Regierungsentwurf, S. 125.
[22] ABl. L 386 v. 29.12.2006, S. 89, L 75 v. 15.3.2007
[23] Hierunter fallen neben den Staatsanwaltschaften auch alle Polizei-, Zoll- und sonstige Behörden, die für die Verhütung von Straftaten zuständig sind, vgl. BT-Drucks. 17/596, S. 15.

Daten auch nicht von der Entscheidung einer Justizbehörde abhängig gemacht werden, wenn dies für den innerstaatlichen Datenverkehr nicht ebenfalls vorgesehen ist[24].

Deshalb sind an die Regelung zur Übermittlung an die innerstaatlichen Stellen hohe Anforderungen im Hinblick an Normenklarheit und Rechtsstaatlichkeit zu stellen. Nicht gerechtfertigte Eingriffsbefugnisse in die Grundrechte auf Privatheit und informationelle Selbstbestimmung von Bürgern im innerstaatlichen Rechtskreis transportieren sich damit nämlich mittels des allgemeinen „Verfügbarkeitsprinzips“ automatisch in den europäischen Raum und damit in alle Mitgliedsstaaten.

### 3. Bewertung

Die Interpretation, die der Regierungsentwurf dem Prinzip der hypothetischen Datenneuerhebung zugrunde gelegt hat, entspricht nicht der verfassungsrechtlichen Rechtsprechung und stellt damit weder für das Inland noch im Hinblick auf die Mitgliedsstaaten der Europäischen Union eine tragfähige Grundlage der Datenübermittlung dar.

Der Regierungsentwurf hält es ersichtlich für ausreichend, bei Anlegung des „Vergleichbarkeitsmaßstabs“ allein auf eine Vergleichbarkeit des Rechtsgüterschutzes („vergleichbar bedeutsame **Rechtsgüter**“, § 12 Abs. 2 Ziff. 1b BKAG-E[25]) abzustellen. Unberücksichtigt bleibt damit aber die darüber hinausgehende Maßgabe des BVerfG, dass die Zweckänderung nur dann gerechtfertigt ist, wenn bei vergleichbar bedeutsam einzustufendem Rechtsgüterschutz eine Neuerhebung auch mit „**vergleichbar schwerwiegenden Mitteln**“[26] zulässig wäre. Diese Vergleichbarkeit auch in Bezug auf die Mittelverwendung (z.B. Telefon- oder Raumüberwachung) findet in § 12 Abs. 2 bis 4 BKAG-E keine Erwähnung. Damit verkennt der Regierungsentwurf, dass ein mit der ursprünglichen Datenerhebung vergleichbar gewichtiger Rechtsgüterschutz

[24] Vgl. Art. 3 Abs. 3 S. 2 RbDatA.
[25] So auch Regierungsentwurf, S. 111.
[26] BVerfG, Rn. 287.

nicht automatisch bedeutet, dass eine Neuerhebung auch mit (in demselben Maß) vergleichbar schwerwiegenden Mitteln zulässig wäre.

## II. Übermittlung von Daten an Mitgliedstaaten der Europäischen Union

### 1. Regelung im Regierungsentwurf

Die „Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union“ ist in § 14 a BKAG geregelt. Der Entwurf sieht dafür jetzt § 26 BKAG-E „Datenübermittlung an Mitgliedstaaten der Europäischen Union“ vor.
Der Regierungsentwurf hebt den „Gleichbehandlungsgrundsatz“ bei der Datenübermittlung im Inland mit den Mitgliedsstaaten hervor (= „Verfügbarkeitsprinzip“ nach dem Rahmenbeschluss, s. oben Ziffer I. 2.).[27]
Die Differenzierung zwischen der Übermittlung aufgrund eines Ersuchens und „**Spontanübermittlungen**“ wird aufgehoben. In § 14a BKAG ist die Übermittlung (noch) an ein „Ersuchen“ eines Mitgliedsstaates geknüpft, das zudem die in § 14 a Abs. 2 BKAG genannten besonderen Voraussetzungen (z.B. ersuchende Behörde, Sachverhaltsbenennung, Zweckbenennung, Zusammenhang zwischen Zweck und Person etc.). erfüllen muss. Die Zulässigkeit von „Spontanübermittlungen“ bedeutet nunmehr, dass das BKA auf eigene Initiative mit „öffentlichen und nichtöffentlichen Stellen in den Mitgliedsländern“ in Kontakt treten kann. Nach § 26 Abs. 1 Nr. 2 BKAG-E kann auch an „zwischen- und überstaatliche Stellen der Europäischen Union“ übermittelt werden, die mit der Verhütung und Verfolgung von Straftaten befasst sind, z.B. also auch an das ohnehin schon gigantische Datensammelsystem von **Europol**.[28]

### 2. Bewertung

a) Um mit Letzterem zu beginnen: **Europol**[29] stellt für Europa die wichtigste europäische Datensammelstelle dar. Sie war – als heutige Agentur der

[27] Regierungsentwurf, S. 126.
[28] Regierungsentwurf, S. 126.
[29] S. hierzu die website: https://www.europol.europa.eu/.

Europäischen Union[30] – ursprünglich als reine Koordinationsstelle für den Informationsaustausch für die nationalen Polizeibehörden in Europa ausgestaltet. Durch Verbindungsbeamte von Europol (sog. ELOS[31]) wurde die Anbindung an die nationalen Strafverfolgungsbehörden sichergestellt. Eine eigene Datenerhebungskompetenz hatte Europol nicht. Im Zuge der Einrichtung des neuen **Zentrums für Terrorismusabwehr** am 1. Januar 2016 änderte sich dies. Die Mitgliedstaaten sind seitdem angehalten, alle ihnen zur Verfügung stehenden Daten bei Europol „einzuspeisen". Gänzlich zur „Superbehörde"[32] hat sich Europol durch die Neufassung der **Europol-Verordnung** entwickelt, die am 1. Mai 2017 in Kraft tritt und die Mitgliedsstaaten zur Informationsweitergabe ausdrücklich *verpflichtet*.[33] Vorgesehen ist jetzt der Austausch von Daten auch mit privaten Unternehmen u.a. in Drittstaaten. Dies betrifft z.B. Internetkonzerne wie Facebook, Google oder Twitter, mit denen die Agentur schon zuvor zusammenarbeitete. Eine bei Europol bestehende Meldestelle durchsucht das Internet nach „gewaltverherrlichenden Inhalten" und beantragt bei Dienstleistern deren Entfernung. Zukünftig sollen die Unternehmen Personendaten der betreffenden Nutzer übergeben, damit Europol gegen diese ermitteln kann.[34] Eine neue „Meldestelle für Internetinhalte" arbeitet mit Unternehmen wie Google, YouTube, Facebook und Twitter zusammen und soll helfen, Postings oder Videos mit strafbaren Inhalten aus dem Internet zu entfernen. Anfangs hatte es geheißen, die „Meldestelle" widme sich allein den „islamistisch-terroristischen" Aktivitäten. Nun sollen auch Inhalte beobachtet und entfernt werden im Zusammenhang mit Schleuserkriminalität und „hybriden Bedrohungen".[35] Auch die europäische Datenbank Eurodac[36] speist ihre Daten bei Europol ein. An Eurodac übermitteln die EU-Mitgliedsstaaten von Asylbewerbern und illegal Einreisenden u.a.

[30] Wie z.B. OLAF, CEPOL und Eurojust.
[31] EUROPOL-Liaison Officers
[32] https://www.jungewelt.de/2016/05-12/001.php.
[33] https://www.janalbrecht.eu/presse/pressemitteilungen/europol.html; s. hierzu auch: Monroy, https://netzpolitik.org/2016/mehr-parlamentarische-kontrolle-fuer-europol-geht-das-ueberhaupt/.
[34] Hierzu auch Albrecht: https://www.janalbrecht.eu/presse/pressemitteilungen/europol.html; Hunko, Soz Nr. 12/2015 vom 1. Dezember 2015).
[35] BT-Drucks. 18/8845 v. 21.6.2016.
[36] VERORDNUNG (EU) Nr. 603/2013 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Juni 2013

Fingerabdruck, Herkunftsmitgliedsstaat, Geschlecht, Ort- und Zeitpunkt der Antragstellung bzw. Zeitpunkt des Aufgreifens, Zeitpunkt der Abnahme der Fingerabdrücke, Zeitpunkt der Datenübermittlung.

Durch die Möglichkeit, auch „Spontanübermittlungen“ zuzulassen – neben den Übermittlungen aufgrund eines konkreten *Ersuchens* – ist ein weiterer Schritt getan in Richtung auf eine zentrale europäische Datenbank, bei der alle gespeicherten Informationen, die – aus welchem (niederschwelligen) Anlass auch immer – in den Mitgliedsstaaten gesammelt und übermittelt wurden, von tausenden Behörden in ganz Europa durchforstet werden können. Eine solche Entwicklung würde grundlegende Datenschutz-Prinzipien, wie vor allem das der Zweckbindung und der Verhältnismäßigkeit, ohne Vorhandensein einer justiziellen Kontrolle, außer Kraft setzen.

b) In diesem Zusammenhang kommt umso mehr dem folgenden Hinweis in der Begründung des Regierungsentwurfs[37] zu den „*zu übermittelnden Stellen*“ Bedeutung zu. Es heißt dort:

*„Der Regelfall von Übermittlungen nach Satz 1 Nummer 1 stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat gemäß Artikel 2 Buchstabe a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.3.2007, S. 26) benannt wurden.“*

Wer alles nach dem Rahmenbeschluss als „*Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle*

[37] Regierungsentwurf S. 126.

*eines Mitgliedstaates der Europäischen Union“* gilt, ist nicht hinreichend ersichtlich. Im o.a. Rahmenbeschluss ist zwar bestimmt:
*„Jeder Mitgliedstaat erklärt bis zum 18. Dezember 2007 in einer beim Generalsekretariat des Rates zu hinterlegenden Erklärung, welche Behörden unter den Begriff „zuständige Strafverfolgungsbehörde“ fallen.“*

Da diese Liste aber nicht veröffentlicht werden muss, ist unklar, welche Stellen dies sein können.

Das ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – hat in seiner Stellungnahme vom 13.9.2011 zum Begriff dieser „Strafverfolgungsbehörde eines Mitgliedstaates“ im Rahmen des „Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union“ (BT-Drs. 17/5096) folgendes ausgeführt:

„*Der Begriff der Strafverfolgungsbehörde eines Mitgliedstaats, an die auf Ersuchen Daten übermittelt werden müssen oder dürfen, ist im vorliegenden Gesetzentwurf nicht hinreichend bestimmt. Da es sich nicht um inländische Strafverfolgungsbehörden handelt, kann der im deutschen Recht gebräuchliche Begriff der Strafverfolgungsbehörde nicht angewandt werden. Dass nicht nur Strafverfolgungsbehörden nach deutschem Rechtsverständnis unter die Regelung fallen, wird in § 92 Abs. 5 IRG-E deutlich, der den Anwendungsbereich der Übermittlungspflichten allein von der Bestimmung der Mitgliedstaaten abhängig macht. Die zuständigen Behörden müssen nach Art. 2 Buchstabe a des* ***Rahmenbeschlusses 2006/960/JI*** *von den Mitgliedstaaten gegenüber dem Generalsekretariat des Rates angegeben werden. Der Geltungsbereich des vorliegenden Gesetzentwurfs erschließt sich somit weder aus dem Gesetz, noch aus dem Rahmenbeschluss, sondern erst durch Hinzuziehung der gegenüber dem Generalsekretariat des Rates abgegebenen Erklärungen, die im Übrigen jederzeit geändert werden können. Eine Veröffentlichung dieser Erklärungen ist nicht vorgeschrieben. Eine solche wäre jedoch erforderlich, damit das*

*Gesetz nicht nur für die Normadressaten, sondern insbesondere für die betroffenen Bürgerinnen und Bürger hinreichend transparent und bestimmt wird.*[38]

Dem ist nichts hinzuzufügen.

c) Durch § 26 Abs. 1 Satz 1 BKAG-E wird eine sehr weitgehende Übermittlungsbefugnis geschaffen. Der Adressatenkreis „*öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union“* erfasst auch sämtliche Nachrichten- und Geheimdienste in den EU-Staaten. Die Nachrichten- und Geheimdienste in den 28 EU-Mitgliedstaaten sind extrem unterschiedlich organisiert und verfügen entsprechend über z.T. sehr unterschiedliche Aufgabenbereiche und Befugnisse.[39] Da in einzelnen EU-Mitgliedsstaaten Geheimdienste z.T. mit Exekutivbefugnissen ausgestattet sind[40] und auch Aufgaben wahrnehmen, die dem Bereich der Gefahrenabwehr bei weiter Auslegung zugeordnet werden können, entsteht durch die beabsichtigte Regelung in §§ 25, 26 BKAG-E eine sehr weitgehende Übermittlungsbefugnis an Nachrichten- und Geheimdienste. Dies ist insbesondere im Hinblick auf diejenigen Geheimdienste in den Mitgliedsstaaten der EU, die mit Exekutivbefugnissen ausgestattet sind, bedenklich. Denn diese dürfen *de jure* schon regelmäßig weit im Vorfeld einer polizeirechtlichen Gefahr tätig werden. Wenn sie zudem mit Exekutivbefugnissen ausgestattet sind und somit Zwangsmaßnahmen vornehmen dürfen, führt dies zu einer erheblichen Vorverlagerung der Eingriffsmöglichkeit. Mit unserem rechtstaatlichen Verständnis ist dies nicht in Einklang zu bringen. Das Problem stellt sich in der Bundesrepublik Deutschland deswegen nicht, weil deutsche Nachrichtendienste aufgrund des insoweit strengen Trennungsgebots über keine Exekutivbefugnisse verfügen und solche auch nicht im Wege der Amtshilfe erlangen können.

---

[38] ULD - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/sicherheit-justiz/20130911-Schwedische-Initiative.pdf.

[39] Vgl. dazu etwa European Agency for Fundamental Rights (FRAU), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Mapping Member States's legal frameworks, Wien 2015, S. 14.

[40] Ebd.

Bei weiter Auslegung der §§ 25, 26 BKAG-E soll es dem BKA indes gestattet sein, etwa dem rumänischen Inlandsgeheimdienst SRI, der wegen seiner Praktiken bei der Unterstützung von Strafverfolgungsmaßnahmen bereits mehrfach kritisiert worden ist, dem Grunde nach Daten im selben Umfang zu übermitteln wie an eine inländische Stelle. Ein weiteres Beispiel ist Ungarn, wo eine spezielle Einheit der Polizei im Bereich der Terrorismusbekämpfung existiert, die mit geheimdienstlichen Befugnissen ausgestattet ist und nicht-strafrechtliche Untersuchungen unter Nutzung von Geheimdienstinformationen vornehmen darf. Hier verschwimmen die Grenzen zwischen Polizeibehörde und Geheimdienst. Dies ist rechtstaatlich bedenklich. Die in § 28 BKAG-E geregelten Übermittlungsverbote bieten hier keinen ausreichenden Schutz.

Übermittlungen an Nachrichtendienste im Ausland sollten nicht nur *de facto*, sondern auch *de jure* den dafür vorgesehenen Stellen in Deutschland vorbehalten bleiben: Dies sind die Nachrichtendienste des Bundes, insbesondere der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz.

## III. Übermittlung im internationalen Bereich

### 1. Regelung nach dem Regierungsentwurf

Die „Befugnisse bei der Zusammenarbeit im internationalen Bereich“ sind in § 14 BKAG geregelt. § 14 Abs. 1 (ohne S. 1 Nr. 2) BKAG ist nach der Entscheidung des BVerfG vom 20. April 2016 **unvereinbar** mit Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1, 10 Abs. 1, 13 Abs. 1 und 3 auch i.V.m. Art. 1 Abs. 1 und Art. 19 Abs. 4 GG.[41] Der Regierungsentwurf sieht in § 27 BKAG-E die „Datenübermittlung im internationalen Bereich“ vor. In § 28 BKAG-E sind die „Übermittlungsverbote und Verweigerungsgründe“ geregelt.

[41] jedoch weiterhin anwendbar bis zu einer Neuregelung, längstens bis 30.06.2018.

Das BVerfG hat diese Unvereinbarkeit damit begründet, dass es der Regelung in § 14 Abs. 1 S. 1 Nr. 1 BKAG an Maßgaben fehle, die sicherstellten, dass Daten aus eingriffsintensiven Überwachungsmaßnahmen nur für die Zwecke übermittelt werden dürfen, die dem Kriterium der hypothetischen Datenerneuerung entsprechen.[42] Des Weiteren bedürfe es bei einer Übermittlung von Daten in das Ausland[43] der **Vergewisserung**[44] darüber, dass sowohl die Zweckbindung der Datenübermittlung sowie ein angemessenes Datenschutzniveaus und die Menschenrechtsstandards im Empfängerland eingehalten werden.[45] Das Bundesverfassungsgericht hat mit deutlichen Worten dargelegt, dass und weshalb die „Vergewisserung" über einen **hinreichend rechtsstaatlichen Umgang** mit den Daten im Empfängerland erforderlich ist.[46] Danach hat sich die Vergewisserung über das geforderte Schutzniveau auf

„*gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können*".[47]

## 2. Bewertung

a) Die Sicherstellung der Einhaltung des Prinzips der hypothetischen Datenneuerhebung bei den Übermittlungen im internationalen Bereich löst der Regierungsentwurf unter Hinweis auf die Generalklausel des § 12 Abs. 2 bis 4 BKAG-E.[48] Dazu, dass dieses Prinzip in § 12 Abs. 2 bis 4 BKAG-E nicht entsprechend der verfassungsrechtlichen Vorgaben normiert ist, siehe die obigen Ausführungen (Ziff. I. 3.).

[42] BVerfG, Rn. 343.
[43] Damit ist das nicht-europäische Ausland gemeint.
[44] BVerfG, Rn. 339.
[45] BVerfG, Ls. 3 und Rn. 333 ff.
[46] BVerfG, Ls. 3 und Rn. 333 ff.
[47] BVerfG, Rn. 339
[48] Regierungsentwurf, S. 127.

b) Die beabsichtigten Regelungen im Regierungsentwurf werden auch nicht im Hinblick auf die Vorgaben für die „Vergewisserung“ über die Einhaltung eines angemessenen Schutzniveaus im Ausland den Maßgaben des Bundesverfassungsgerichts gerecht.

Die vom BVerfG geforderte „Vergewisserung“ setzt denknotwendig die Erkenntnisgewinnung **vor** der Übermittlung an Stellen im Ausland voraus. Wie diese verantwortliche Überprüfung (z.B. durch den Datenschutzbeauftragten) erfolgen kann, ist den beabsichtigten Regelungen nicht zu entnehmen. Es gibt zwar in § 28 Abs. 3 BKAG-E den Hinweis darauf, dass „*aktuelle Erkenntnisse der Bundesregierung*“[49] über u.a. Menschenrechtsverstöße im Empfängerland zu berücksichtigen sind. In welcher Weise diese „Berücksichtigung“ stattzufinden hat, ist allerdings unklar. Die Prüfung ist offensichtlich im eigenen Hause des BKA vorzunehmen, da die Verantwortung für die Übermittlung in den Händen des BKA liegt[50]. Dabei können Interessenskonflikte nicht ausgeschlossen werden. Im Entwurf finden sich im Weiteren nur Regelungen, die sich auf eine erkennbar erst **im Nachhinein** durchzuführende Kontrolle durch den Datenschutzbeauftragten des BKA im 2-Jahres-Turnus beziehen[51]. Soweit § 90 BKAG-E gerichtliche Zuständigkeiten regelt, sind dabei Auslandsübermittlungen von Dateninformationen nicht aufgeführt.

Auch insoweit besteht deshalb Nachbesserungsbedarf.

Dies gilt einmal mehr auch vor dem Hintergrund, dass bei weiter Lesart § 27 BKAG-E (wie auch § 26 BKAG-E) auch eine Übermittlung von Daten an ausländische Geheimdienste in aller Welt gestattet. Denn auch insoweit existieren Geheimdienste in anderen Staaten, die (teilweise) Aufgaben der Gefahrenabwehr und Strafverfolgung wahrnehmen. Auch hier sollte – wie bei § 26 BKAG-E – schon *de jure* eine Übermittlungsbefugnis allein den dafür in

[49] Auch im Hinblick auf das Vorliegen eines „Angemessenheitsbeschlusses“ der Europäischen Kommission nach Art. 36 der Datenschutzrichtlinie 2016/680.
[50] Vgl. § 27 Abs. 7 BKAG-E.
[51] Vgl. §§ 69 ff. BKAG-E.

unserer Sicherheitsarchitektur vorgesehenen Stellen vorbehalten bleiben: den Nachrichtendiensten des Bundes.

## C. Anordnungsbefugnisse

Die Ausgestaltung zahlreicher Befugnisnormen macht die Schwächen des Gesetzesentwurfes deutlich: Es fehlt an Normenklarheit. Der Gesetzgeber setzt die Vorgaben des Bundesverfassungsgerichts nicht um. Vielmehr übernimmt er lediglich den Wortlaut einzelner Urteilsgründe und lässt diese 1:1 in das Gesetz einfließen. Die damit verbundenen Probleme sind vorprogrammiert: Gerade für die Befugnisse mit einem gravierenden Eingriffsgewicht fehlt es an hinreichend bestimmten Kriterien, die vor einer unverhältnismäßigen Weite der Norm schützen. Exemplarisch wird dies nachfolgend an drei Regelungen dargestellt:

### I. Besondere Mittel der Datenerhebung, § 45 BKAG-E

§ 45 BKAG-E soll § 20g BKAG ablösen. Die Vorschrift erlaubt Überwachungsmaßnahmen, die „an der Wohnungstür enden“ – wie längerfristige Observation, die Anfertigung von Bildaufnahmen oder -aufzeichnungen, das Abhören oder Aufzeichnen des außerhalb von Wohnungen nichtöffentlich gesprochenen Wortes, den Einsatz von Vertrauenspersonen und verdeckten Ermittlern. Nach § 20g Abs. 1 Nr. 2 BKAG kann das Bundeskriminalamt diese Überwachungsmaßnahmen hinsichtlich solcher Personen einsetzen, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 S. 2 BKAG begehen werden und die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Straftaten gemäß § 4a Abs. 1 S. 2 BKAG sind solche, die in § 129a Abs. 1, Abs. 2 StGB bezeichnet und dazu bestimmt sind,

„*die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder*

*ihrer Auswirkung einen Staat oder eine internationale Organisation erheblich schädigen können*“.

Mit Urteil vom 20. April 2016 hat das Bundesverfassungsgericht § 20g Abs. 1 Nr. 2 BKAG für verfassungswidrig erklärt und dies wie folgt begründet:

„*(…) Allerdings bedarf es aber auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (…). In Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht (…). Die diesbezüglichen Anforderungen sind* ***normenklar*** *zu regeln.*
*(…) Dem genügt § 20 Abs. 1 Nr. 2 BKAG nicht. Zwar knüpft die Vorschrift an eine mögliche Begehung terroristischer Straftaten an. Die diesbezüglichen Prognoseanforderungen sind hierbei jedoch nicht hinreichend gehaltvoll ausgestaltet. Die Vorschrift schließt nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderungen, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Damit gibt sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand und eröffnet Maßnahmen, die unverhältnismäßig weit sein können*“[52].

§ 45 Abs. 1 S. 1 Nr. 2 und Nr. 3 BKAG-E berücksichtigen die Vorgaben des Bundesverfassungsgerichts wie folgt:

> „*Das Bundeskriminalamt kann personenbezogene Daten mit den besonderen Mitteln nach Absatz 2 erheben über*

[52] *BVerfG* U. v. 20.04.2016, 1 BvR 966/09, juris Rn. 164, 165.

*1. (…),*
*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. (…),*

*wenn die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre*“.

Straftaten nach § 5 Abs. 1 S. 2 BKAG-E sind wiederum die, die in § 129a Abs. 1, Abs. 2 StGB bezeichnet sind – wie zum Beispiel Mord, Totschlag, Völkermord, Geiselnahme, Computersabotage, Zerstörung von Bauwerken, Brandstiftung, gefährlicher Eingriff in den Bahn-, Schiffs- und Luftverkehr, schwere Gefährdung durch Freisetzen von Giften oder Straftaten nach dem Kriegswaffenkontrollgesetz.

Unklar bleibt aber, was mit den folgenden Begriffsbestimmungen gemeint sein soll:

- übersehbarer Zeitraum,
- zumindest ihrer Art nach konkretisierte Weise

und

- individuelles Verhalten.

Gesetzliche Definitionen fehlen. Dies aber steht im diametralen Widerspruch zu der Vorgabe des Bundesverfassungsgerichts, Prognoseanforderungen hinreichend gehaltvoll auszugestalten. Eine solche Ausgestaltung kann nicht dadurch ersetzt werden, dass nur höchstrichterliche Vorgaben im Wortlaut übernommen, aber nicht umgesetzt werden. Dass das Bundesverfassungsgericht dem Gesetzgeber einen

Rahmen vorgegeben hat, entbindet ihn nicht von seiner Aufgabe, diese durch klare und verständliche Regelungen auszufüllen.

## II. Verdeckter Eingriff in informationstechnische Systeme, § 49 BKAG-E

Der Gesetzgeber hat die Vorgaben des BVerfG in der Entscheidung vom 20. April 2016 in § 49 BKAG-E hinsichtlich des Kernbereichsschutzes umgesetzt, deren Missachtung in § 20k Abs. 7 S. 3, 4 und 8 BKAG a.F. noch zu dessen Verfassungswidrigkeit geführt hatten. § 49 Abs. 7 S. 3, 4 BKAG-E sieht nunmehr eine gerichtliche Kontrolle kernbereichsrelevanter Daten vor. Damit ist nun zwar sichergestellt, dass die Sichtung der erlangten Daten durch eine „unabhängige Stelle“ erfolgt, praktisch dürfte dies jedoch aufgrund der regelmäßig anfallenden Datenmenge kaum umsetzbar sein. So verfügen moderne informationstechnische Systeme über enorme Speicherkapazitäten von zum Teil mehreren Terabyte. Die Überprüfung aller nach Abs. 1 erhobenen Daten dürfte daher die Grenzen der Belastbarkeit der möglichen „Stelle“ und erst recht mit Blick auf die erforderliche Kontrolle der zuständigen Gerichte regelmäßig sprengen.

In § 49 Abs. 7 S. 8 BKAG-E wurden die vom BVerfG gestellten Anforderungen an die Aufbewahrungsfrist der Löschungsprotokolle umgesetzt. Neu eingefügt wurden ferner die Absätze 5 und 8. Absatz 5 enthält nun die vom BVerfG vorgegebenen Anforderungen an den zu stellenden Antrag, während Absatz 8 als neue Vorschrift die Handlungsmöglichkeiten des BKA bei Gefahr in Verzug regelt.

Allerdings hat die mit dem Ziel einer Klarstellung erfolgte Umsetzung der Kritik des Ersten Senats bzgl. Abs. 1 S. 2 die Konsequenz, dass Nr. 2 weiterhin einer verfassungskonformen Auslegung bedarf und Nr. 1 nunmehr sogar als verfassungswidrig einzustufen ist:

Zwar übernimmt § 49 Abs. 1 S. 2 BKAG-E nahezu wortlautgetreu die Ausführungen des BVerfG in der Entscheidung vom 20. April 2016. Ein wesentliches vom Ersten Senat gefordertes Tatbestandsmerkmal ignoriert der Gesetzesentwurf dagegen völlig: Der Erste Senat hatte noch vorgegeben, dass § 20k Abs. 1 S. 2 BKAG a.F. dahingehend auszulegen sei, dass zum einen *„Maßnahmen nur erlaubt sind, wenn*

*die Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen",* und zum anderen ***„wenn erkennbar ist, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann"***[53].

§ 49 Abs. 1 S. 2 BKAG lässt diese zweite Eingriffsvoraussetzung vermissen.

Das BVerfG differenzierte insoweit nicht zwischen der Nr. 1 und der Nr. 2, so dass die Voraussetzung der Individualisierbarkeit der betroffenen Person jeweils gilt. Der Entwurf verzichtet dagegen auf eine entsprechende ausdrückliche Begrenzung der Maßnahme auf einen bestimmten Personenkreis. Lediglich Nr. 2 eröffnet durch den Wortlaut „*individuelles Verhalten einer Person*" überhaupt eine verfassungskonforme Auslegung, kann die vom BVerfG aufgezeigten Unsicherheiten in der Rechtsanwendung aber gerade nicht beseitigen. Ausgeschlossen ist eine verfassungskonforme Auslegung indes hinsichtlich Nr. 1, in der eine personelle Begrenzung der Maßnahme gar keinen Anklang findet. Ohne diese, vom BVerfG vorausgesetzte Begrenzung ist § 49 Abs. 1 S. 2 BKAG-E somit verfassungswidrig. § 49 BKAG-E fällt mithin hinter die – wenn auch aus anderen Gründen – für verfassungswidrig erklärte Norm des § 20k BKAG a.F. zurück.

Darüber hinaus ist – insbesondere mit Hinblick auf das Gebot der Normenklarheit – fraglich, was unter einem „individuellen Verhalten" im Sinne von Nr. 2 zu verstehen ist. Im Entwurf finden sich hierzu keine erläuternden Ausführungen. Das BVerfG hat dazu lediglich beispielhaft angeführt, dass dies etwa denkbar sei, *„wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist"*[54]. Dadurch ist bereits jetzt absehbar, dass die Konkretisierung des Tatbestandsmerkmals letztlich auf die Gerichte übertragen wird, obwohl der Gesetzgeber hier hätte Klarheit schaffen können bzw. müssen.

[53] BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 – 1 BvR 1140/09, Rn. 213.
[54] BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 – 1 BvR 1140/09, Rn. 112.

## III. Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten, § 52 BKAG-E

Die Regelung des § 52 BKAG-E soll nach dem Willen der Verfasser des Entwurfs künftig den bisherigen § 20m BKAG ersetzen, der die Befugnis des Bundeskriminalamts zum Abruf von Telekommunikationsverkehrsdaten und Nutzungsdaten betrifft, die gemäß § 96 Abs. 1 TKG bei den Diensteanbietern für einen bestimmten Zeitraum auf Vorrat gespeichert sind. Der Erste Senat des Bundesverfassungsgerichts hatte § 20m Abs. 1, 3 BKAG mit Urteil vom 20. April 2016 für unvereinbar mit Art. 10 GG erklärt und angeordnet, dass die Norm bis spätestens 30. Juni 2018 neu gefasst werden müsse.[55]

**1.**

Die beabsichtigte Neuregelung der Thematik in § 52 BKAG-E ist bei näherer Betrachtung in weiten Teilen nicht mit den Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09) vereinbar.

Die Entwurfsverfasser befolgen die Vorgaben des Bundesverfassungsgerichts[56] zwar insoweit, als nun im Antrag auf Erlass einer Genehmigung zum Abruf von Telekommunikationsverkehrs- und Nutzungsdaten der Sachverhalt und eine Begründung angegeben werden müssen (§ 52 Abs. 3 i.V.m. § 51 Abs. 4 Nr. 5 und 6 BKAG-E). Dies ist zu begrüßen, weil es dem Sinn und Zweck des Richtervorbehalts Rechnung trägt, dem Gericht vor Erlass der Maßnahme eine Prüfung zu ermöglichen, die diesen Namen verdient.

Allerdings ist die Umsetzung der weiteren Maßgaben des Bundesverfassungsgerichts zu kritisieren:

Dies gilt insbesondere für die Ergänzung des § 52 Abs. 1 Nr. 2 BKAG und für die Einfügung des § 52 Abs. 1 Nr. 3 BKAG. Zwar sollen hiermit nach den Vorstellungen der Entwurfsverfasser die Vorgaben des

[55] BVerfG Urteil vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09), Rn. 247, 251, 357.
[56] BVerfG Urteil vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09), Rn. 118.

Bundesverfassungsgerichts an die zu treffende Prognoseentscheidung bei einer konkreten Gefahr für eine terroristische Straftat umgesetzt werden.[57] Tatsächlich schreiben sie die Vorgaben der Karlsruher Richter jedoch lediglich ab.

Die bloße Übernahme der Formulierung des Bundesverfassungsgerichts in den Regelungstext verfehlt im Ergebnis dessen Aufforderung an den Gesetzgeber,[58] dem Gebot der Normenklarheit Rechnung zu tragen. Sinn und Zweck dieses Gebots ist es einerseits, den von der Regelung Betroffenen die Eingriffsvoraussetzungen vor Augen zu führen, so dass diese ihr Verhalten danach ausrichten können.[59] Es geht aber andererseits auch darum, dem Richter, der über den Antrag auf Abruf der Daten bei den Diensteanbietern zu entscheiden hat, zu verdeutlichen, wie konkret die Gefahrenlage, die einen Eingriff in Art. 10 GG rechtfertigt, beschaffen sein muss. In diesem Zusammenhang sind die Maßgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung aus dem Jahr 2010 zu beachten: Das Gericht hatte seinerzeit geurteilt, aus den Regelungen zum Abruf der gespeicherten Daten müsse sich die Intensität der Gefährdung der geschützten Rechtsgüter ergeben, um die Eingriffsschwelle für den Staat klar zu definieren.[60]

Diesen Anforderungen trägt die beabsichtigte Ergänzung der bestehenden Eingriffsbefugnisse nicht in der gebotenen Weise Rechnung. Insbesondere was unter dem Begriff des *„übersehbaren Zeitraums“* im Sinne des § 52 Abs. 1 Nr. 2 und Nr. 3 BKAG-E zu verstehen ist, ist weder für den von dem Abruf der Daten betroffenen Bürger noch für den Richter, dem der Antrag auf diesen Abruf übermittelt wird, „übersehbar“. Hätte das Bundesverfassungsgericht eine derart unkonkrete Regelung für ausreichend erachtet, so hätte das Gericht es dabei belassen können, § 20m Abs. 1 Nr. 2 BKAG verfassungskonform eng auszulegen. Das hat es allerdings bewusst nicht getan.

Auch soweit es speziell die Neufassung des § 52 Abs. 1 Nr. 2 BKAG-E – *„auf eine zumindest ihrer Art nach konkretisierte Weise“* – betrifft, wird der Entwurf der

[57] RegE, S. 144 f.
[58] BVerfG, Urt. v. 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09), Rn. 164.
[59] BVerfG, Beschluss vom 22. Juni 1977 – 1 BvR 799/76 –, BVerfGE 45, 400-421 - Rn. 81 m.w.N.
[60] BVerfG, Urt. v. 02. März 2010 – 1 BvR 256/08 -, Rn. 230.

Zielvorgabe des Gerichts, die Voraussetzungen für den Eingriff „normenklar“ zu regeln, nicht gerecht. Letztlich hat das Bundesverfassungsgericht betont, dass es darum geht, die Gefahr – die für sich genommen nicht konkret sein muss – aus konkreten Tatsachen[61] abzuleiten und nicht nur aus Erfahrungssätzen.[62] Die beabsichtigte Neuregelung, die auch insoweit das Bundesverfassungsgericht schlicht wörtlich übernimmt, ist eher geeignet, Fragen aufzuwerfen als in der praktischen Anwendung der Norm für Klarheit zu sorgen.

Was die vom Bundesverfassungsgericht geforderte[63] verfassungskonforme Auslegung der Nummern 3 und 4 des § 20m Abs. 1 BKAG im Lichte des § 20b Abs. 2 Nr. 2 BKAG anbelangt, so fragt sich schließlich, warum der Gesetzgeber bei der Formulierung des § 52 BKAG-E nicht zum Zwecke der Klarstellung den ausdrücklichen Verweis auf § 39 Abs. 2 BKAG-E[64] aufgenommen hat.

**2.**

Die beabsichtigte Neuregelung ist auch nicht mit den Vorgaben des Europäischen Gerichtshofs in dessen Urteil vom 21. Dezember 2016 (Az. C-203/15, C-698/15)[65] vereinbar.

In dieser Entscheidung legten die Luxemburger Richter Art. 15[66] der sogenannten E-Privacy-Richtlinie (2002/58/EG) im Lichte der Grundrechtecharta – Art. 7, 8, 11, 52 Abs. 1 GRC – aus und betonten den Ausnahmecharakter der Norm, die eng auszulegen und abschließend sei. Zulässige Eingriffe in die bei der Vorratsdatenspeicherung tangierten Grundrechte der Art. 7, 8 und 11 GRC

[61] Im Gegensatz zu dem neugefassten § 52 Abs. 1 Nr. 3 BKA-G, der auf das „individuelle Verhalten“ deiner Person als Ausgangspunkt für eine Gefahrenprognose abstellt.
[62] BVerfG Urteil vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09), Rn. 164.
[63] BVerfG, Urt. v. 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09), Rn. 251, 233, 166 f.
[64] Die Norm entspricht § 20b Abs. 2 BKAG.
[65] Hierzu instruktiv jüngst *Roßnagel*, NJW 2017, 696, 697.
[66] „(I) Die Mitglieder können Rechtsvorschriften erlassen, die die Rechte und Pflichten nach Artikel 5, (...) beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Informationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedsstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz ausgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. (...)“

müssten daher auf das absolut Notwendige (sowohl sachlich als auch zeitlich) beschränkt sein.

Die Beschränkung auf das „absolut Notwendige“ in diesem Sinne erfordere präzise, klare nationale Regelungen zu den Voraussetzungen derartiger Maßnahmen und zum Schutz vor Missbrauch der gespeicherten Daten. Erforderlich seien objektive Kriterien, die einen (zumindest mittelbaren) Zusammenhang zwischen den zu speichernden Daten und dem mit der Speicherung verfolgten Ziel herstellten und in der Praxis eine begrenzende Wirkung entfalteten. Dementsprechend stehe Art. 15 Abs. 1 der E-Privacy-Richtlinie im Lichte der Art. 7, 8 und 11, 52 Abs. 1 GRC einer nationalen Regelung entgegen, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierter Nutzer hinsichtlich aller elektronischer Kommunikationsmittel vorsieht.[67]

Im Lichte dieser Maßgaben des EuGH ist zu der beabsichtigten Neufassung der Befugnis zum Abruf von Telekommunikationsverkehrsdaten und Nutzungsdaten folgendes zu sagen:

Die amtliche Überschrift von § 52 BKAG-E in dem Regierungsentwurf (*„Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten“*[68]) ist, wie bereits bei der aktuellen Regelung des § 20m BKAG, ungenau und missverständlich: Tatsächlich erheben die Dienstebetreiber die Verkehrsdaten gemäß § 96 TKG; die beabsichtigte Regelung betrifft vielmehr den Abruf der dergestalt bereits erhobenen Daten durch das BKA.[69]

Die Vereinbarkeit von § 52 BKAG-E mit den Vorgaben des EuGH setzt daher logisch vorrangig voraus, dass die Dienstebetreiber auf der „1. Stufe“ der Vorratsdatenspeicherung die Daten rechtmäßiger Weise erheben. Daran bestehen

[67] Das Gericht urteilt damit anders als der Generalanwalt, der die EuGH-Entscheidung „Digital Rights Ireland“ vom 08. April 2014 (Az.: C-293/12) dahingehend interpretiert hatte, dass die Nichtigkeit der Vorratsdatenspeicherungsrichtlinie maßgebend aus den fehlenden Garantien zum Zugriff auf die gespeicherten Daten gefolgert worden sei.
[68] RegE, S. 56.
[69] Vgl. dazu bereits BVerfG, Urt. v. 02. März 2010 – 1 BvR 256/08 -, Rn. 190 ff.

im Hinblick auf die genannten Ausführungen des EuGH Zweifel. Die Vorschrift des § 96 Abs. 1 TKG[70] – auf den § 52 BKAG-E Bezug nimmt und der die Speicherung der Verkehrsdaten durch die Diensteanbieter regelt – sieht keine Beschränkung auf das „absolut Notwendige“ vor,[71] weder in geografischer noch in personaler Hinsicht. Vor allem ist kritikwürdig, dass die Vorschrift für die Datenerhebung durch die Anbieter keine Differenzierung dahingehend vorsieht, ob es sich bei der Kommunikation um eine solche mit einem Berufsgeheimnisträger handelt.[72]

Vielmehr verfolgt die Regelung das Prinzip des „Catch-all“, d.h. die Diensteanbieter speichern zunächst nahezu[73] sämtliche Telekommunikation. Erst auf der 2. Stufe – beim Abruf der auf diese Weise gespeicherten Daten – soll danach differenziert werden, was staatliche Stellen abrufen dürfen. Ob § 52 BKAG-E die Anforderungen, die der EuGH für diese 2. Stufe entwickelt hat, erfüllt, kann dahinstehen, weil bereits § 96 TKG mit den europarechtlichen Vorgaben – konkret: mit Art. 7, 8, 11 GRC – nicht vereinbar ist.

---

[70] „1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:
1.
die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2.
den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3.
den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4.
die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5.
sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.
Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.
(2) Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.“

[71] So auch *Roßnagel,* NJW 2017, 696, 698.

[72] Dazu bereits auch die Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten, Mai 2015, S. 5, 12 ff.

[73] Ausnahme: § 116b Abs. 6 i.V.m. § 99 TKG: Nicht gespeichert werden Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen, soweit die Bundesnetzagentur die angerufenen Anschlüsse in eine Liste aufgenommen hat.

## D. Aufenthalts- und Kontaktverbot, § 55 BKAG-E

### I. Inhalt des § 55 BKAG-E

§ 55 BKAG-E sieht neben einer neuen Regelung von Kontaktverboten eine Ermächtigung für Aufenthaltsverbote vor. Regelungen zu Aufenthaltsverboten an bestimmten Örtlichkeiten für Personen, von denen die Begehung einer Straftat erwartet werden kann, sind mit deutlich geringeren Eingriffsvoraussetzungen bereits heute nach den Polizeigesetzen der Länder möglich. Hauptanwendungsfall ist die Verhütung von Straftaten im Zusammenhang mit Fußballspielen. In diesen Fällen ist die abzuwehrende Gefahr, gewalttätige Auseinandersetzungen im Zusammenhang mit Fußballspielen, bereits konkret absehbar.

Neu an der jetzt in § 55 BKAG-E vorgesehenen Regelung ist die Ermächtigung der Polizeibehörden den Betroffenen den Aufenthalt in einem bestimmten Bereich vorzuschreiben. Derartige Regelungen sehen die Polizeigesetze der Länder bislang nicht vor - sieht man von den Regelungen zum polizeilichen Gewahrsam ab, die nur unter strengen Voraussetzungen zulässig sind. Da der „Bereich“ des vorgeschriebenen Aufenthalts räumlich nicht näher begrenzt ist, könnte dies theoretisch bis zum Hausarrest gehen. Die Gesetzesbegründung führt „ein oder mehrere Stadtbezirke“ einer Großstadt als möglichen Bereich einer Aufenthaltsbeschränkung an. Ausländerrechtlich gibt es entsprechende Befugnisse nach § 62 Abs. 3 Nr. 1a AufenthG.

Neben der Möglichkeit, eine Pflicht zum Aufenthalt an einem bestimmten Ort vorschreiben zu können, und den Regelungen zu den Kontaktverboten liegt die Besonderheit der mit § 55 BKAG-E vorgesehenen Eingriffen darin, dass diese Maßnahmen § 55 BKAG-E auch gegen Personen gerichtet werden können, die nicht Störer sind. Die Regelung enthält erstmals bundesrechtliche Regelungen für Eingriffe gegenüber „Gefährdern“.

Eine – informelle – Definition des „Gefährders“ gab es in der Arbeitsgemeinschaft der Landeskriminalämter und des Bundeskriminalamtes „AG Kripo“. Danach sollte ein

„Gefährder“ eine Person sein, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche im Sinne von § 100 a StPO, begehen wird[74].

## II. Verfassungsrechtliche Bewertung

### 1. Erheblicher Grundrechtseingriff

§ 55 BKAG-E ermächtigt insbesondere mit der Begründung einer Befugnis, den Aufenthaltsort einer Person vorzuschreiben zu erheblichen Eingriffen in Art. 2 Abs. 2 Satz 2 GG. Nach Art. 2 Abs. 2 Satz 2 GG ist die Freiheit der Person unverletzlich. Damit bringt das Grundgesetz zum Ausdruck, dass Art. 2 Abs. 2 Satz 2 GG ein besonders hohes Rechtsgut schützt, das nur aus besonders gewichtigem Grund angetastet werden darf. Jede Einschränkung dieser Freiheit ist stets der strengen Prüfung am Grundsatz der Verhältnismäßigkeit zu unterziehen. Für präventive Eingriffe in die Freiheit der Person gilt dies nach der Rechtsprechung des Bundesverfassungsgerichts in besonderem Maße, da diese Einschränkungen der Freiheit nicht dem Schuldausgleich dienen. Sie sind deshalb nur zulässig, wenn der Schutz hochwertiger Rechtsgüter dies unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfordert[75].

Die Beschränkung des Aufenthalts auf einen bestimmten Bereich ist deshalb ein Grundrechtseingriff von erheblichem Gewicht. Die in der Gesetzesbegründung angeführte Möglichkeit, Ausnahmen von dem Verbot, einen bestimmten Bereich zu verlassen, um bestimmte Angelegenheiten zu erledigen, stellt einen erheblichen Rahmen privater Lebensgestaltung unter polizeilichen Genehmigungsvorbehalt.

[74] Schriftliche Antworten der Bundesregierung auf die Frage des MdB Wolfgang Neskovic vom 20. November 2006, BT-Drucksache 16/3570 v. 24.11.2006.
[75] BVerfG, Urteil vom 04. Mai 2011 – 2 BvR 2333/08 –, Rn. 98, juris.

## III. Tatbestandliche Voraussetzungen des § 55 BKAG-E

Eingriffe nach § 55 BKAG-E setzen keine „Gefahr“ voraus. Aus der Gegenüberstellung der tatbestandlichen Voraussetzungen der Abwehr einer Gefahr und der Verhütung von Straftaten ist ersichtlich, dass mit der „Verhütung von Straftaten“ bereits Umstände Eingriffsmaßnahmen rechtfertigen können, die nicht die Gefahrenschwelle erreichen. Angesprochen ist damit die vorbeugenden Bekämpfung von Straftaten, bei denen ein weit größerer Grad an Ungewissheit der Verwirklichung einer Gefahr in Kauf genommen wird, als dies etwa bei einem Gefahrenverdacht der Fall wäre. Bei der „Verhütung von Straftaten“ geht es um einen „ungleich geringeren Wahrscheinlichkeitsgrad einer künftigen Straftatbegehung als bei einer Gefahrenprognose“[76].

Nach der Rechtsprechung des Bundesverfassungsgerichts ist der Gesetzgeber von Verfassungswegen bei der Normierung von Eingriffsbefugnissen nicht auf die Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren beschränkt[77].

Vielmehr kann er die Grenzen auch weiter ziehen, insbesondere mit dem Ziel schon der Verhütung terroristischer Straftaten, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. Allerdings müssen die Eingriffsgrundlagen auch dann verlangen, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus, um den Zugriff zu rechtfertigen. Es müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen[78]. Da gerade terroristische Straftaten, oft lange geplant und von bisher nicht auffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können nach der Rechtsprechung des BVerfG Eingriffe auch dann erlaubt sein, wenn zwar noch

[76] Vgl. Rachor in: Lisken/Denninger, Handbuch des Polizeirechts, S. 345.

[77] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 116.
[78] Vgl. BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>.

nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, aber das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird[79]. Diese Rechtsprechung des Bundesverfassungsgerichts bezieht sich aber auf Eingriffe, die der Informationsgewinnung dienen.

In diesem Sinne knüpft § 55 BKAG-E an den Straftatenkatalog des § 129 a Abs. 1 und Abs. 2 StGB an, der seinerseits an die Definition des internationalen Terrorismus im EU-Rahmenbeschluss vom 13. Juni 2002 angelehnt ist[80].

§ 55 BKAG-E unterscheidet insoweit zwei Alternativen: entweder müssen bestimmte Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird, oder das individuelle Verhalten der betroffenen Person begründet die konkrete Wahrscheinlichkeit, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird.

Die 2. Alternative ist jedoch zu unbestimmt, da auf eine Konkretisierung der Straftat verzichtet wird.

## IV. Bewertung

### 1. Verhältnismäßigkeit

Der durch Art. 2 Abs. 1 GG gewährleistete Freiheitsanspruch des Betroffenen ist das Sicherungsbedürfnis der Allgemeinheit entgegenzuhalten; beide Gesichtspunkte sind im Einzelfall abzuwägen[81]. Das Freiheitsgrundrecht der Betroffenen ist sowohl auf der Ebene des Verfahrensrechts als auch materiellrechtlich abzusichern[82].

[79] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 112.
[80] ABl. EU Nr. L 164 S. 3.
[81] Vgl. BVerfGE 109, 133 <157>; 128, 326 <373>.
[82] BVerfGE 70, 297 <311>; 109, 133 <159>.

Anders als es in der Gesetzesbegründung heißt, knüpft das Gesetz nicht an die Anforderungen des BVerfG im Urteil zum BKA Gesetz an.

Das BVerfG hat in dieser Entscheidung ausgeführt, „Maßnahmen mit hoher Eingriffsintensität“ seinen „im Bereich der Gefahrenabwehr“ zum Schutz von Rechtsgütern „grundsätzlich nur verhältnismäßig, 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.“[83]. Ferner könnten „Überwachungsmaßnahmen“ auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird[84].

Die vorgesehene Regelung, einer Person den Aufenthalt in einem bestimmten Bereich vorzuschreiben, stellt ohne Zweifel eine Maßnahme von hoher Eingriffsintensität dar, sodass eine Gefährdung von Rechtgütern hinreichend konkret absehbar sein muss. Die Einschreitschwelle des § 55 BKAG-E knüpft damit an weit im Vorfeld einer Gefahr liegende Umstände an, bei denen per definitionem nur relativ diffuse Anhaltspunkte für mögliche künftige Gefahren bestehen können. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, sich aber auch konkretisieren und in eine Gefahr münden. In einer solchen Situation mögen Überwachungsmaßnahmen möglich sein.

Eingriffe der Informationsverschaffung sind jedoch weit weniger intensive also solche, mit dem einer Person der Aufenthalt in einem bestimmten Bereich vorgeschrieben wird. Diese Beschränkung der persönlichen Freiheit durch eine Beschränkung des Aufenthalts geht über eine Überwachungsmaßnahme weit hinaus. Denn bei einer Überwachungsmaßnahme bleibt die Bewegungsfreiheit einer Person grds. unberührt.

[83] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 109.
[84] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 112.

Für einen solchen Eingriff in die persönliche Freiheit ist eine Konkretisierung der Gefahrenlage in jedem Falle erforderlich. Ohne eine solche Konkretisierung der Gefahrenlage bleibt auch unklar, wie der Bereich umschrieben werden soll, an dem sich die Person nicht aufhalten darf, bzw. in dem sie sich aufhalten muss. Jede Beschränkung des Aufenthaltsbereichs einer Person ist rechtfertigungsbedürftig. Wie soll aber eine Beschränkung des Aufenthaltsbereichs aus Gründen der Gefahrenabwehr eingegrenzt werden, wenn die abzuwehrende Gefahr, deren Entstehung allenfalls befürchtet wird, nicht hinreichend konkret ist?

Es stellt sich auch die Frage der Geeignetheit von Aufenthaltsge- oder verboten zur Abwehr möglicher terroristischer Gewalttaten. Wird dem „Gefährder“ nämlich auferlegt, einen oder zwei bestimmte Stadtbezirke nicht zu verlassen, wird er möglicherweise davon abgehalten, in einem dritten oder vierten Bezirk Anschläge zu verüben. Er ist aber nicht gehindert, in dem Bereich, in dem er sich frei bewegen darf, sich Ziele wie Schulen, Kindergärten, Einkaufs-Zentren oder andere öffentlich frequentierte Orte auszusuchen, die es in allen Stadtbezirken gibt. Bei dem Personenkreis, der als terroristischer „Gefährder“ in Betracht kommt, ist, wie die Erfahrung mit Anschlägen in den letzten Jahren zeigt, eine Vorhersehbarkeit der Angriffsziele nicht gegeben. Daher sind Aufenthaltsge- und verbote, wenn sie nicht wie ein haftähnlicher Hausarrest ausgestaltet werden (was dann andere verfassungsrechtliche Fragen aufwerfen würde), auch unter dem Gesichtspunkt fehlender Geeignetheit unverhältnismäßig.

Hinzu kommt Folgendes: Ermächtigungen zur vorbeugenden Bekämpfung von Straftaten enthalten allenfalls Ermächtigungen zur Datenerhebung[85] und beschränken sich in erster Linie auf die Informationsgewinnung im Hinblick auf die Feststellung einer das polizeiliche Handeln rechtfertigenden Gefahr und haben eine ungleich geringere Eingriffsintensität. Gleiches gilt für die in den Polizeigesetzen der Länder vorgesehenen Aufenthaltsverbote an bestimmten Orten. Nicht erkennbar ist auch, weshalb Überwachungsmaßnahmen, die mit einer geringeren Eingriffsintensität verbunden sind, in diesem weiten Vorfeld einer

[85] Vgl. § 20 Abs. 3 Nr. 1 PolG Baden-Württemberg.

Gefahr nicht ausreichen können. Allein die Entlastung polizeilicher Tätigkeit kann den erheblichen Grundrechtseingriff nicht rechtfertigen.

Aus diesem Grund ist die Regelung des § 55 BKAG-E insoweit abzulehnen, als danach einer Person der Aufenthalt in einem bestimmten Bereich vorgeschrieben werden kann, ohne dass sie durch ihr Verhalten Anlass zu der Annahme gegeben hat, konkrete Straftaten zu begehen.

**2. Rechtsschutz**

Bei Eingriffen in die persönliche Freiheit kommt dem Rechtsschutz durch ein effektives Verfahren besondere Bedeutung zu. Für Freiheitsentziehungen wird dies durch Art. 104 GG konkretisiert.

Die Rechtswegzuweisung an das Amtsgericht am Sitz des BKA ist nicht gerechtfertigt. Es handelt sich um eine öffentlich-rechtliche Maßnahme der Gefahrenabwehr. Stehen polizeiliche Maßnahmen unter Richtervorbehalt, dann wird die Zuweisung dieser Verfahren an die Amtsgerichte damit gerechtfertigt, dass – etwa bei der Ingewahrsamnahme – das Amtsgericht das ortsnähere Gericht ist und eine Anhörung des Betroffenen und damit effektiver Rechtsschutz besser gewährleistet werden kann, als durch das Verwaltungsgericht. Diese Erwägungen können eine Zuweisung der gerichtlichen Entscheidung an das Amtsgericht am Sitz des BKA nicht rechtfertigen.

Sachgerecht wäre deshalb eine Zuständigkeit des Amtsgerichts am Aufenthaltsort des Betroffenen. Dies entspricht der Zuständigkeit bei anderen präventiv polizeilichen Rechtswegzuweisungen. Auf diese Weise ist es insbesondere möglich Rechtsschutzgesuche, etwa im Hinblick auf die Erlaubnis zum Verlassen des zugewiesenen Aufenthaltsbereichs, ortsnah zu bescheiden.

Weshalb am Sitz des BKA jedoch das Amtsgericht und nicht das Verwaltungsgericht zuständig sein sollte ist nicht erkennbar. Die „Ortsnähe“ kann diese Rechtswegzuweisung sicher nicht rechtfertigen. Auch bei

ausländerrechtlichen Auflagen hinsichtlich des Aufenthalts ist die Zuständigkeit der Verwaltungsgerichte gegeben.

Nicht nachvollziehbar ist auch, weshalb eine richterliche Entscheidung nicht unverzüglich eingeholt werden muss, und polizeiliche Aufenthaltsbeschränkungen für die Dauer von 3 Tagen auch ohne richterliche Anordnung zulässig sein können.

## E. Elektronische Aufenthaltsüberwachung, § 56 BKAG-E

### 1. Inhalt

§ 56 Abs. 1 Satz 1 BKAG-E ermächtigt das BKA, eine Person dazu zu verpflichten, eine „elektronische Fußfessel“ zur Überwachung des Aufenthaltsorts in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen. Tatbestandliche Voraussetzung dieser Verpflichtung ist es allein, dass diese Person als „Gefährder“ im Sinne von § 55 Abs. 1 BKAG-E anzusehen ist.

Im Unterschied zur Regelung des § 55 BKAG-E ermächtigt § 56 BKAG-E allein zu Überwachungsmaßnahmen. Damit können in einem erheblichen Umfang Informationen über diese Person, ihre sozialen Kontakte und Beziehungen gewonnen werden. Darin liegt ein erheblicher Eingriff in das durch Art. 1, Art. 2 Abs. 1 GG geschützte Persönlichkeitsrecht. Daten können auch innerhalb der Wohnung erhoben werden, eine Einschränkung der Datenerhebung ist daran geknüpft, dass es „technisch möglich“ ist allein den Aufenthalt der Person in der Wohnung zu registrieren. Die Speicherung der Daten wird zwar nach § 56 Abs. 2 Satz 4 darauf begrenzt, dass sie „spätestens zwei Monate nach ihrer Erhebung zu löschen“ sind. Die Löschung der Daten steht jedoch unter dem Vorbehalt, dass sie nicht mehr für die Zwecke, zu denen sie erhoben wurden, verwendet werden. Angesichts der Weite der mit der „Verhütung von Straftaten“ denkbaren weiten Zwecke, dürfte diese Beschränkung, die nur Selbstverständliches zum Ausdruck bringt, kaum praktische Relevanz erhalten. § 56 Abs. 4 ermächtigt zu umfangreichen Datenübermittlungen an Polizei- und Strafverfolgungsbehörden.

Die elektronische Fußfessel ist nur auf Anordnung eines Gerichts zulässig. Nähere Einzelheiten zur Bestimmung der Zuständigkeit des Gerichts enthält das Gesetz nicht.

**2. Bewertung**

Die elektronische Aufenthaltsüberwachung kann als Weisung im Rahmen der Führungsaufsicht auferlegt werden[86]. Voraussetzung ist eine Verurteilung zu einer Freiheitsstrafe von mindestens drei Jahren. Sie ist also von deutlich strengeren Voraussetzungen abhängig, als nach § 56 BKAG-E. In diesem Rahmen wurde die „elektronische Fußfessel“ 2015 durch Prof. Kinzig, Tübingen evaluiert. Sie wird zurzeit bei 70 permanent überwachten ehemaligen Straftätern oder Maßregelinsassen eingesetzt, 45 dieser Fälle entfallen allein auf das Bundesland Bayern. Sie ist für die Betroffenen mit einem erheblichen Aufwand verbunden, „da sie sich während des Ladevorgangs (mindestens zwei Stunden pro Tag, bei manchem Probanden zweimal täglich) nicht von der Steckdose entfernen können“. „Bewährungshelferinnen und Bewährungshelfer gaben zu bedenken, dass eine EAÜ die Betroffenen stigmatisiere“, etwa bei der Wohnungssuche oder bei einer Erwerbstätigkeit.

Im Hinblick auf die Eignung der elektronischen Fußfessel kommt die Studie in dem hier interessierenden Zusammenhang zu einem eindeutigen Ergebnis: „Insgesamt sind sich alle Akteure einig, dass eine Aufenthaltsüberwachung die Begehung neuer Straftaten letztlich nicht verhindern kann“[87]. Dies dürfte erst recht beim Einsatz gegen (vermeintliche) Straftäter aus dem Bereich des Terrorismus gelten. Die Maßnahme ist daher zwar einerseits mit erheblichen Eingriffen in das Persönlichkeitsrecht verbunden, erweist sich aber nach allen Erfahrungen als ungeeignet.

[86] Vgl. § 68b Abs. 1 S. 1 Nr. 12 StGB.
[87] Bräuchle/Kinzig: Die elektronische Aufenthaltsüberwachung im Rahmen der Führungsaufsicht Kurzbericht über die wesentlichen Befunde einer bundesweiten Studie mit rechtspolitischen Schlussfolgerungen Tübingen 2015, S. 12.

## F. Richtervorbehalt

Der Richtervorbehalt ist zum Teil nur unvollständig geregelt. So sieht etwa § 45 Abs. 3 Nr. 5 BKAG-E (nur) vor, dass Einsätze von Vertrauenspersonen und von Verdeckten Ermittlern nur dann durch das Gericht angeordnet werden müssen, wenn sich die Einsätze gegen eine bestimmte Person richten oder bei denen die Vertrauensperson oder der Verdeckte Ermittler eine Wohnung betritt, die nicht allgemein zugänglich ist. Hingegen hat das Bundesverfassungsgericht mit Urteil vom 20. April 2016 klargestellt, dass bis zu einer Neuregelung bzw. bis zum 30. Juni 2018 sämtliche Einsätze von Vertrauenspersonen und Verdeckten Ermittlern „*nur durch ein Gericht angeordnet werden dürfen*“[88]. Dies aber lässt den Schluss zu, dass nach Auffassung des BVerfG jeder Einsatz von Vertrauenspersonen und Verdeckten Ermittlern den verfassungsrechtlichen Anforderungen nur genügt, soweit dieser auf eine richterliche Entscheidung zurückgeht.

## G. Schutz zeugnisverweigerungsberechtigter Personen

Ausdrücklich zu begrüßen ist, dass der Gesetzesentwurf nunmehr wie in § 160a StPO ein einheitliches Schutzniveau für alle anwaltlichen Berufsgeheimnisträger schafft. Dass die Unterscheidung zwischen Strafverteidigern und anderen Rechtsanwälten bei der Ausgestaltung des Vertrauensschutzes verfassungsrechtlich nicht tragfähig ist, hatte das Bundesverfassungsgericht ausdrücklich festgestellt[89]. Folgerichtig schützt § 62 Abs. 1 BKAG-E nunmehr gleichermaßen das Vertrauensverhältnis zu Strafverteidigern wie auch zu anderen Rechtsanwälten durch ein absolutes Erhebungs- und Verwertungsverbot. Dies entspricht einer langjährigen Forderung des DAV[90]. Der Gesetzgeber bleibt aufgefordert, die verfassungswidrige Unterscheidung zwischen Rechtsanwälten und Strafverteidigern in § 3b G 10 sowie bei § 23a Abs. 5 ZFdG aufzuheben und alle Rechtsanwälte in den absoluten Schutz vor Ermittlungsmaßnahmen einzubeziehen.

---

[88] BVerfG U. v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09 Tenor Ziffer 4.
[89] BVerfG aaO; Rn. 257.
[90] DAV-SN 16/10 zur Einbeziehung weiterer Berufsgeheimnisträger in den absoluten Schutz des § 160a StPO; DAV-SN 25/15 zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein
Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten; DAV SN 47/15 zur Reform der Nachrichtendienste.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)793

18. Wahlperiode

Deutscher Bundestag
Parlamentarischer Beirat
f. nachhaltige Entwicklung

Ausschussdrucksache
18(23)99-35



# Gutachtliche Stellungnahme/Prüfbitte

## Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

Bundestags-Drucksache 18/11326
Bundesrats-Drucksache 109/17

Im Rahmen seines Auftrags zur Überprüfung von Gesetzentwürfen und Verordnungen der Bundesregierung auf Vereinbarkeit mit der nationalen Nachhaltigkeitsstrategie hat sich der Parlamentarische Beirat für nachhaltige Entwicklung gemäß Einsetzungsantrag (BT-Drs. 18/559) in seiner 59. Sitzung am 8. März 2017 mit dem Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (BT-Drs. 18/11326) befasst.

Folgende Aussagen zur Nachhaltigkeit wurden in der Begründung des Gesetzentwurfes getroffen:

„Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie. Die Wirkungen des Gesetzentwurfs zielen auf eine nachhaltige Entwicklung, weil er das Bundeskriminalamt mit rechtssicheren Befugnissen zum Schutz der Bürgerinnen und Bürger ausstattet und gleichzeitig den Datenschutz nach Maßgabe des Urteils des Bundesverfassungsgerichts stärkt.“

**Formale Bewertung durch den Parlamentarischen Beirat für nachhaltige Entwicklung:**

Eine Nachhaltigkeitsrelevanz des Gesetzentwurfes ist gegeben. Der Bezug zur nationalen Nachhaltigkeitsstrategie ergibt sich hinsichtlich und folgenden Indikators:

Indikator 16.1 n. F. (Kriminalität),

Eine Nachhaltigkeitsprüfung ist durchgeführt worden, allerdings ohne konkreten Bezug auf die Indikatoren bzw. Managementregeln der Nachhaltigkeitsstrategie.

**Prüfbitte:**

Der Parlamentarische Beirat für nachhaltige Entwicklung bittet deshalb den federführenden Innenausschuss, bei der Bundesregierung nachzufragen, warum der Bezug zur nationalen Nachhaltigkeitsstrategie nicht hinreichend deutlich hergestellt wurde und welche konkreten Auswirkungen auf die Ziele der nationalen Nachhaltigkeitsstrategie zu erwarten sind sowie die Ergebnisse in Kurzform in den Bericht des Ausschusses aufzunehmen.

Berlin, 8. März 2017

Dr. Lars Castellucci, MdB
Berichterstatter

Dr. Valerie Wilms, MdB
Berichterstatterin