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 *„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“* und *„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.“* Für die Länderdaten fehlt anders als bisher jede Vorgabe.“ [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.

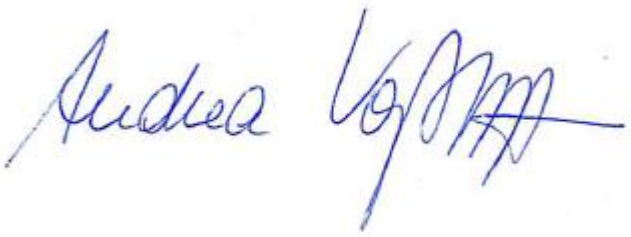
6. Datenschutzkontrolle

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