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.