Stellungnahme
zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) vom 30. Januar 2018
Bayerischer Landtag Drucksache 17/20425

im Auftrag der Fraktion der SPD im Bayerischen Landtag

von RiLG Dr. Markus Löffelmann, München

A. Inhaltsverzeichnis

B. Gutachterliche Stellungnahme

I. Vorbemerkung

1

Das Recht der Sicherheitsbehörden auf Bundes- und Länderebene ist, namentlich determiniert durch die Entwicklung der verfassungsgerichtlichen Rechtsprechung, terroristische Anschläge und Bedrohungslagen sowie Erkenntnisse aus Untersuchungsausschüssen in einem Erneuerungsprozess begriffen. Für die letzten Jahre zu nennen sind für den Bereich des Polizeirechts die Novellierung des BPolG[1] und des BKAG im Jahr 2017[2] sowie die Änderung des BayPAG mit dem Gesetz vom 24.07.2017[3]. In den Ländern Hessen[4] und Baden-Württemberg[5] befinden sich aktuelle Änderungsgesetze im Gesetzgebungsverfahren. Im Bereich des Rechts der Nachrichtendienste wurden auf Bundesebene substanziell geändert das BVerfSchG in den Jahren 2015 bis 2017[6] und das BNDG im Jahr 2016.[7] Auf Länderebene sind in Bereich des Rechts der Nachrichtendienste zu erwähnen die Novellierungen der Verfassungsschutzgesetze von Nordrhein-Westfalen 2013[8], Thüringen 2015[9], Bayern 2016[10] und Niedersachsen 2016[11], sowie die Entwürfe in Baden-Württemberg[12] und Hessen[13]. Im Bereich der Strafverfolgung wurde im Jahr 2015 (erneut) die sog. „Vorratsdatenspeicherung" geregelt[14] und zuletzt mit dem Gesetz vom 17.08.2017 die sog. „Online-Durchsuchung" eingeführt.[15] Übergreifend ist bei allen Änderungen eine klare Tendenz zur Ausweitung eingriffsintensiver sicherheitsbehördlicher Befugnisse festzustellen.

2

Im Kontext dieser Entwicklung ist auch der gegenständliche Gesetzentwurf zu sehen, der sich in einigen Punkten an Reformbemühungen auf Bundesebene und in anderen Ländern anlehnt, ganz überwiegend aber eine eigene Agenda verfolgt und darin eine Vorbildrolle für ganz Deutschland erblickt.[16] Namentlich soll der Entwurf neben der Umsetzung der Vorgaben der Europäischen Datenschutzricht-

[1] BGBl. I 2017, 1066.
[2] BGBl. I 2017, 1354.
[3] GVBl. 2017, 388.
[4] Vgl. Art. 3 unter Hessischer Landtag Drucksachen 19/5412 und 19/5782.
[5] Vgl. Landtag von Baden-Württemberg Drucksache 16/2741.
[6] BGBl. I 2015, 1938; 2016, 1818; 2017, 1634 und 2017, 2097.
[7] BGBl. I 2016, 3346.
[8] GV. NRW 2013, 367.
[9] ThürGVBl. 2014, 529.
[10] GVBl. 2016, 145.
[11] GVBl. NI 2016, 194.
[12] Vgl. Landtag von Baden-Württemberg Drucksache 16/2740.
[13] Vgl. Hessischer Landtag Drucksache 19/5412.
[14] BGBl. I 2015, 2218.
[15] BGBl. I 2017, 3202.

linie (EU) 2016/680 und der vom BVerfG in seinem Urteil zum BKAG konsolidierten und neu entwickelten Maßstäbe dem Zweck dienen, dass *„die mit dem Gesetz zur effektiveren Überwachung gefährlicher Personen (LT-Drs. 17/16299) erfolgte Novellierung zeitnah fortgeführt* (wird), *was die dem Stand der Technik entsprechende Ergänzung und noch effektivere Ausgestaltung wichtiger weiterer polizeilicher Instrumentarien betrifft, um auf die aktuelle Gefährdung durch vielfältige Formen des Terrorismus, Extremismus, aber auch durch anderweit motivierte gewichtige Bedrohungslagen bis hin zu Cyberangriffen reagieren zu können"* (S. 64[17]). Nähere Ausführungen zu Art und Gewicht der Gefahrenlagen, deren Verhinderung und Bekämpfung das Gesetz dienen soll, sowie zu etwaigen in der bisherigen Polizeipraxis aufgetretenen Defiziten enthält der Gesetzentwurf nicht.

II. Einzelne Kritikpunkte

1. Zu Art. 11 Abs. 3 PAG-E (drohende Gefahr):

a) Bestimmtheitsdefizite:

3

Mit dem Gesetz vom 24.07.2017 führte der bayerische Gesetzgeber in Art. 11 Abs. 3 PAG die neue Kategorie der „drohenden Gefahr" ein und erweiterte damit eine Anzahl polizeilicher Befugnisse, die auf diese Gefahrkategorie Bezug nehmen. Bereits im damaligen Gesetzgebungsverfahren war diese Weiterung starker Kritik ausgesetzt.[18] Es wurde eingewendet, durch die Anknüpfung polizeilicher Befugnisse an eine lediglich „drohende Gefahr" werde der Aufgabenbereich der Polizei weit in das Gefahrenvorfeld ausgedehnt und damit gezielt eine weitere „Vernachrichtendienstlichung" der Polizei[19] betrieben. Die konkrete Gefahr als bislang klare Eingriffsschwelle und deutliches Abgrenzungskriterium zu den Vorfeldbefugnissen der Nachrichtendienste werde aufgegeben.[20] Zudem sei der Begriff der „drohenden Gefahr", der lediglich Formulierungen des BVerfG paraphrasiere, selbst sehr vage, seine einfachgesetzliche Ausgestaltung in Art. 11 Abs. 3 S. 1 PAG weise zahlreiche unbestimm-

---

[16] Vgl. Pressemitteilung Nr. 33/2018 vom 07.02.2018 des Bayerischen Staatsministeriums des Innern, für Bau und Verkehr.

[17] Die Zitierung der Entwurfsbegründung folgt der Fassung des Gesetzentwurfs vom 28.11.2017 (Verbändeanhörung).

[18] Namentlich durch die Sachverständigen *Stockinger*, *Wächtler* und den *Verf.*; vgl. ferner *Brodmerkel*, BayRVR v. 09.03.2017 (Net-Dok. BayRVR2017030901) und *Heidebach*, BayRVR v. 13.03.2017 (Net-Dok. BayRVR2017031301) sowie ausf. *Löffelmann*, BayVBl. Heft 5/2018 (erscheint am 1. März 2018); gegen das Gesetz sind mittlerweile mehrere Popularklagen beim BayVerfGH anhängig, bzw. in Vorbereitung.

[19] Vgl. zu diesem Begriff *Dietrich*, in: Dietrich/Eiffler, Teil III § 3 Rn. 8 m.w.N.; *Paeffgen*, StV 2002, 336; *Paeffgen*, GA 2003, 647.

[20] Nach BVerfGE 133, 277, 327 seien der Polizei „Befugnisse gegenüber Einzelnen grundsätzlich nur aus konkretem Anlass verliehen", Voraussetzung ihres Handelns sei „in der Regel, dass Anhaltspunkte für einen Tatverdacht oder eine Gefahr" vorlägen; vgl. auch näher und für eine Beibehaltung des Gefahrbegriffs als „klare Grenzlinie zwischen dem Bereich der - oberhalb der Gefahrenschwelle angesiedelten - Gefahrenabwehr und ihrem - unterhalb der Gefahrenschwelle angesiedelten - informationellen Vorfeld" *Möstl*, S. 180 f.

te Kriterien auf, die durch die Polizei selbst ausgefüllt werden müssten. Im Einzelnen handelt es sich dabei (in der Reihenfolge ihrer Erwähnung im Gesetztext) um folgende Merkmale:

- „bedeutendes Rechtsgut“[21],
- „das individuelle Verhalten einer Person“[22],
- „konkrete Wahrscheinlichkeit“[23],
- „Vorbereitungshandlungen“[24],
- „seiner Art nach konkretisiertes Geschehen“[25],
- „in absehbarer Zeit“[26],
- „Angriffe von erheblicher Intensität oder Auswirkung“[27],
- „erhebliche Eigentumspositionen“[28],
- „Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt“[29].

Auch aus dem Begriff der „drohenden Gefahr“ selbst lässt sich kein Anhalt für eine Konkretisierung entnehmen. Der Gesetzgeber hat den Begriff der Rechtsprechung des BVerfG entlehnt[30], ohne zu berücksichtigen, dass „drohend“ dort nicht in einem die Qualität des Subjekts näher kennzeichnenden attributiven Sinn (wie im Falle von „abstrakt“, „konkret“, „dringend“, „gegenwärtig“) Verwendung findet, sondern als Prädikat.[31] Zusätzlich stiftet Verwirrung, dass der Begriff der „drohenden Gefahr“

[21] Soweit ersichtlich, wird der Begriff vom BVerfG überhaupt nur in BVerfGE 81, 310, 334 verwendet, ohne dort aber näher ausgefüllt zu werden. In BVerfGE 141, 220, 335 f. verweist das BVerfG im Zusammenhang mit der Übermittlung von Daten mit dem Begriff „Gefahr für ein bedeutsames Rechtsgut“ lediglich auf eine Auslegung des Begriffs der „erheblichen Gefahr“ im allgemeinen Sicherheitsrecht. Aus sich heraus vermittelt der Begriff keinerlei Einschränkung, denn „unbedeutende“ im Gegensatz zu „bedeutenden“ Rechtsgütern gibt es nicht. Ferner ergibt sich aus dem thematischen Zuschnitt des Katalogs keine substanzielle Begrenzung, denn zu den die genannten Rechtsgüter potenziell verletzenden Handlungen zählen z.B. auch einfache, sogar fahrlässige, Körperverletzungen, Sachbeschädigungen oder sexuell motivierte Belästigungen.

[22] Die Formulierung ist tautologisch; vgl. auch die Kritik an der mangelhaften Bestimmtheit der Formulierung in der Stellungnahme Nr. 33/2017 des Deutschen Anwaltvereins von April 2017 zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes, S. 27.

[23] Im gewöhnlichen wie auch juristischen Sprachgebrauch werden Wahrscheinlichkeiten üblicherweise nicht als „konkret“ charakterisiert, sondern im Rahmen einer ordinalen Skala zum Beispiel als niedrig, mittel oder hoch eingeordnet (vgl. etwa *Denninger*, in: Lisken/Denninger, Teil D Rn. 46, 52; *Pieroth*/*Schlink*/*Kniesel*, § 4 Rn. 6 f.; *Fischer*, § 63 Rn. 15 m. w. N.).

[24] Der normativ aufgeladene Begriff impliziert unausgesprochen eine im Gefahrenvorfeld noch gar nicht vorhandene Kenntnis dessen, was vorbereitet wird, wobei der Gesetztext im Unklaren lässt, worauf sich die Vorbereitung beziehen muss.

[25] Nach welchen Maßstäben die Klassifizierung des Geschehens als „seiner Art nach konkretisiert“ vorzunehmen sei (etwa nach Herkunft oder Gesinnung, Geschlecht, Alter oder Körpergröße der handelnden oder betroffenen Personen, Örtlichkeit, Deliktscharakter des Handelns, Art und Maß der polizeilichen Reaktion, etc. pp.), bleibt völlig im Unklaren.

[26] Soweit ersichtlich wird dieser Begriff im Sicherheitsrecht sonst nicht verwendet. Das BKAG benutzt seit der Novelle 2017 die etwas konkretere Formulierung „innerhalb eines übersehbaren Zeitraums“, vgl. §§ 20y, 20z BKAG.

[27] Im Bereich des Strafverfahrensrechts wird mit dem Begriff „erheblich“ ein mittleres Niveau von Rechtsgutbeeinträchtigungen umschrieben (vgl. BVerfGE 103, 21, 33 f.; 107, 299, 321 f.; 110, 33, 65). Wann einem Angriff eine mittlere „Intensität“ oder „Auswirkung“ zukommt, ist völlig unklar, zumal ein substanziell unterschiedlicher Bedeutungsgehalt der beiden alternativ verknüpften Begriffe nicht erkennbar ist.

[28] Auch dieser Begriff hat - soweit ersichtlich - im geltenden Verfassungsrecht und Sicherheitsrecht kein Vorbild.

[29] Öffentliche Straßen und Wege, Zäune, Mauern, Gebäude, Bäume, Schilder, Skulpturen, „Stolpersteine“, Leitpfosten, Blumenkübel, Rasenflächen, etc. pp.

[30] Vgl. BVerfGE 100, 313, 316; 115, 118, 145; 120, 274, 326; 125, 260, 330 f.; 141, 220, 272 f., 305.

[31] Gefahren sind drohende Rechtsgutsverletzungen. In Zusammenhänge wie den vom BVerfG beschriebenen gestellt, führt die Rede von der „drohenden Gefahr“ deshalb zu unsinnigen Doppelungen (etwa „eine im Einzelfall drohende drohende Gefahr“). Bereits unter sprachlichen Aspekten wäre daher eine andere Begriffsbildung vorzugswürdig (vgl. etwa *Thiel*,

bereits in der bisherigen polizeirechtlichen Literatur sowohl als Synonym für eine konkrete[32] als auch für eine gegenwärtige Gefahr[33] gebraucht wird. In einem technischen Sinne, der auf das Gefahrenvorfeld verweist, findet der Begriff hingegen in § 1 Abs. 1 Nr. 1 G 10, also im Bereich nachrichtendienstlicher Regelungsmaterie, Verwendung. Im dortigen Zusammenhang wird deutlich, dass drohende Gefahren gerade keine Gefahren sind, sondern eine Bedrohungslage kennzeichnen, für deren Bestehen tatsächliche Anhaltspunkte vorliegen müssen, d. h. es darf sich nicht um eine lediglich gefühlte oder vermutete Bedrohung handeln.[34] Hinzu kommt, dass sich aus dem Gesetztext nicht deutlich erschließt, in welchem systematischen Zusammenhang die einzelnen Befugnisvoraussetzungen zueinander stehen. So verlangt zwar Art. 11 Abs. 3 Satz 1 BayPAG, dass die beabsichtigten Maßnahmen auf die Verhinderung der „Entstehung einer Gefahr für ein bedeutendes Rechtsgut" zielen, lässt aber für die Feststellung einer „drohenden Gefahr" eine durch „das individuelle Verhalten einer Person" (Nr. 1) oder „Vorbereitungshandlungen" bzw. andere „bestimmte Tatsachen" (Nr. 2) konkretisierte Erwartung von „Angriffen von erheblicher Intensität oder Auswirkung" - die sich also nicht gegen „bedeutende Rechtsgüter" richten müssen - ausreichen. Nicht die Bezugnahme auf den Katalog bedeutender Rechtsgüter[35], der nur hinsichtlich der subjektiven Zielsetzung der Maßnahme eine Rolle spielt („um ... zu"), sondern die Qualität der zu erwartenden Angriffe stellt damit das eigentliche objektive (wenig) begrenzende Merkmal dar, wobei offen bleibt, wogegen sich die Angriffe richten müssen und ob gegebenenfalls auch die Erwartung eines singulären Angriffs ausreicht. Hinzu kommt, dass das BVerfG die situationsbezogene („ein seiner Art nach konkretisiertes Geschehen") und die personenbezogene Komponente („dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Maßnahme gezielt gegen sie eingesetzt und koordiniert werden kann") als kumulative Erfordernisse eines Tätigwerdens im Gefahrenvorfeld ansieht[36], Art. 11 Abs. 3 PAG hingegen als alternative Voraussetzungen. In konkretisierender Umsetzung der generalisierenden Formulierung des BVerfG, die viel Spielraum für gesetzgeberische Entscheidungen lässt, wäre es denkbar, beispielhaft Indizien zu benennen[37], aus denen auf die Wahrscheinlichkeit eines Gefahreintritts geschlossen werden kann.[38] Ein Beispiel für eine verfassungsrechtlich nicht beanstandete[39] Ausgestaltung von Vor-

---

S. 303, der mit Blick auf die missverständlichen Ausführungen in BVerfGE 120, 274, 329 die Begrifflichkeiten „konkrete Gefahrerwartung" oder „konkrete Gefahrenbesorgnis" vorschlägt; *Möstl*, DVBl. 2007, 581, 587 f. und *Möstl*, DVBl. 2010, 808, 810 f.: „konkreter personenbezogener Gefahrverdacht"; *Streiß*, S. 111: „präsumtive Gefahr").

[32] Vgl. etwa *Schmidbauer/Steiner*, Bayerisches Polizeiaufgabengesetz und Polizeiorganisationsgesetz, 4. Aufl. 2014, Art. 11 PAG Rn. 54; darauf weist auch die Gesetzbegründung (Bayerischer Landtag, Drs. 17/16299 S. 10) hin.

[33] Vgl. *Pewestorf*/Söllner/Tölle, § 1 ASOG Rn. 26 m. w. N.

[34] Vgl. näher zur Auslegung des Begriffs der drohenden Gefahr in § 1 Abs. 1 Nr. 1 G 10 *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 4 Rn. 33; *Huber*, in: Schenke/Graulich/Ruthig, § 1 Art. 10-Gesetz Rn. 28.

[35] So aber Bayerischer Landtag, Drs. 17/17058.

[36] Darauf weist zutreffend hin *Darnstädt*, DVBl 2017, 88, 90.

[37] Z. B. bestimmte bereits verübte Straftaten, die erfahrungsgemäß indizielle Wirkung besitzen; die Rückkehr aus bestimmten, als Rückzugs- oder Ausbildungsorte für Terroristen bekannten Regionen nach Deutschland; Erkenntnisse der Nachrichtendienste über den Kontakt zu Mitgliedern terroristischer Vereinigungen oder über die Inanspruchnahme bestimmter Informationsquellen; Erkenntnisse der Ausländerbehörden aus Befragungen im Zusammenhang mit Asylverfahren.

[38] So auch *Kubiciel*, ZRP 2017, 57, 59.

[39] BVerfGK 10, 283.

feldbefugnissen stellt § 23a Abs. 1 ZfdG dar, der die Überwachung der Telekommunikation darauf beschränkt, dass Tatsachen die Annahme der Vorbereitung bestimmter Straftaten nach dem Kriegswaffenkontrollgesetz rechtfertigen (Abs. 1), wobei der Begriff der Vorbereitung wiederum in Abs. 2 beispielhaft konkretisiert wird.

4

Der im PAG verwendete Begriff der drohenden Gefahr stellt damit eine schwer auf die Lebenswirklichkeit zu übertragende Konstruktion dar, welche Präzision und Normenklarheit lediglich suggeriert. Das gerade im Gefahrenvorfeld besonders hohe Prognoserisiko kann anhand der im Gesetz genannten Kriterien nicht adäquat eingeschränkt werden. Dabei ist zu berücksichtigen, dass das BVerfG für Ermächtigungsgrundlagen im Gefahrenvorfeld ein gegenüber dem originären Bereich der Gefahrenabwehr höheres Maß an Bestimmtheit fordert, um eine vergleichbare Kontrolle zu ermöglichen:

> *„Bei der Vorsorge für die Verfolgung künftiger Straftaten oder bei ihrer Verhütung kann nicht an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind. Maßnahmen der Gefahrenabwehr, die in die Freiheitsrechte der Bürger eingreifen, setzen eine konkrete Gefahrenlage voraus. Die Strafverfolgung knüpft an den Verdacht einer schon verwirklichten Straftat an. Solche Bezüge fehlen, soweit die Aufgabe darin besteht, im Vorfeld der Gefahrenabwehr und Strafverfolgung Vorsorge im Hinblick auf in der Zukunft eventuell zu erwartende Straftaten zu treffen. Deshalb müssen hier die Bestimmtheitsanforderungen spezifisch an dieser Vorfeldsituation ausgerichtet werden.*
>
> *Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich die Konturen eines Straftatbestandes noch nicht abzeichnen, besteht das Risiko, dass der Eingriff an ein nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten noch schwer fassbares und unterschiedlich deutbares Geschehen anknüpft. Sachverhaltsfeststellung und Prognose sind mit vorgreiflichen Einschätzungen über das weitere Geschehen, ebenso wie über die erst noch bevorstehende strafrechtliche Relevanz der festgestellten Tatsachen verknüpft (vgl. BVerfGE 110, 33 <59>). Da der Eingriff sich auf mögliche zukünftige Aktivitäten bezieht, kann er sich häufig nur auf Tatsachen stützen, bei denen noch offen ist, ob sie sich zu einer Rechtsgutverletzung weiterentwickeln (vgl. BVerfGE 110, 33 <59>). Die Situation der Vorfeldermittlung ist insofern durch eine hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt. Die Indizien oder einzelne beobachtete Tätigkeiten können in harmlosen, strafrechtlich unerheblichen Zusammenhängen verbleiben; sie können aber auch der Beginn eines Vorgangs sein, der zur Straftat führt.*
>
> *Sieht der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist. Die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist (vgl. BVerfGE 110, 33 <56>).“*[40]

[40] BVerfGE 113, 348, 377 f.

Diesen erhöhten Anforderungen genügt der Begriff der drohenden Gefahr nicht. Namentlich reicht Art. 11 Abs. 3 PAG unter Bestimmtheitsgesichtspunkten nicht an die im BKAG verwendeten, auf das Gefahrenvorfeld verweisenden Kriterien heran, wo ein Zuschnitt der Gefahr auf die in § 4a Abs. 1 S. 2 BKAG i. V. m. § 129a Abs. 1 und 2 StGB genannten terroristischen Straftaten gefordert wird. Weil durch die Begrenzung der die Anordnungsvoraussetzungen konkretisierenden Straftaten zugleich eine Einhegung des zulässigen Zwecks der Maßnahmen erfolgt und der Straftatenkatalog zudem auf den Schutz höchstrangiger Rechtsgüter verweist, begegnen die dortigen Regelungen unter Bestimmtheitsaspekten geringeren Bedenken, wenngleich eine noch aussagekräftigere Fassung wünschenswert wäre. Die entsprechenden Regelungen des BKAG machen auch deutlich, dass polizeiliche Vorfeldbefugnisse strengen Ausnahmecharakter haben, indem sie auf den Schutz höchstrangiger Rechtsgüter bezogen sein müssen und nur dann in Betracht kommen, wenn einer Bedrohungslage mit den herkömmlichen Mitteln des Polizeirechts nicht mehr begegnet werden kann.[41] Eine solche Differenzierung kann dem PAG-E nicht entnommen werden. Bei alledem ist nicht zu bestreiten, dass eine Ausweitung einzelner polizeilicher Befugnisse ins Gefahrenvorfeld notwendig sein kann, um veränderten Herausforderungen für die Gefahrenabwehr, insbesondere die Abwehr terroristischer Bedrohungen, gerecht zu werden.[42] Das bedeutet aber zum einen keine Legitimierung einer *generellen* Ausdehnung des polizeilichen Handelns auf das Gefahrenvorfeld und zum anderen keinen Verzicht auf eine hinreichend präzise Fassung der Voraussetzungen solchen Handelns. Die Übernahme des verfassungsrechtlichen Präzisierungsgebots in den Gesetztext ersetzt nicht die Benennung von Kriterien, anhand derer die Präzisierung durch die Rechtsanwendung im Einzelfall zu erfolgen hat.

b) Kumulierung erweiterter Handlungsbefugnisse:

5

Bereits im Verfahren zu dem Gesetz vom 24.07.2017 wurde zudem darauf hingewiesen, dass die Vorverlagerung des polizeilichen Aufgabenbereichs im Zusammenhang mit der zusätzlichen inhaltlichen Ausweitung polizeilicher Handlungsbefugnisse zu würdigen ist. Dass durch die damaligen Änderungen die Bayerische Polizei früher und zugleich in größerem Umfang tätig werden dürfe, leite einen Paradigmenwandel hin zu einer „omnipotenten“ Polizei ein.[43]

Der gegenständliche Gesetzentwurf bestätigt diese Befürchtung. Mit der - euphemistisch als „Neuordnung“ bezeichneten - beabsichtigten Novellierung wird die Eingriffsschwelle der drohenden Gefahr

[41] Vgl. ausf. *Kral*, S. 195 ff., der ein differenziertes rechtsgutbezogenes Schutzmodell entwickelt.

[42] Vgl. zum Übergang von einem repressiven zu einem präventiven Terrorismusbekämpfungsrecht *Darnstädt*, GSZ 2017, 16; zu veränderten Herausforderungen des Polizeirechts in der Gegenwart *Albers*, S. 97 ff.; *Schoch*, Der Staat 2004, 347; *Möstl*, DVBl 2007, 581 und DVBl 2010, 808; *Streiß*, S. 91 ff.; *Kral*, S. 21 ff.; *Park*, S. 149 ff.; *Kugelmann*, Die Verwaltung (47) 2014, 25; Überblick zur Problematik und zu aktuellen Ansätzen der Entwicklung einer neuen Polizeirechtsdogmatik *Baldus*, Die Verwaltung (47) 2014, 1.

[43] Vgl. *Löffelmann*, Stellungnahme zum Entwurf eines Gesetzes zur effektiveren Überwachung gefährlicher Personen, unter III.

auf zahlreiche weitere informationelle und aktionelle Befugnisse ausgedehnt. Im Einzelnen handelt es sich um folgende Maßnahmen, die in Zukunft bei Vorliegen einer (lediglich) drohenden Gefahr ergriffen werden können:

- Art. 13 Abs. 1 Nr. 1 lit. b) PAG (Identitätsfeststellung)
- Art. 14 Abs. 1 S. 1 Nr. 4 PAG-E (Erkennungsdienstliche Maßnahmen)
- Art. 15 Abs. 3 Nr. 1 PAG-E (zwangsweise Durchsetzung der Vorladung)
- Art. 16 Abs. 1 S. 1 Nr. 2 PAG (Platzverweisung)
- Art. 16 Abs. 2 S. 1 Nr. 1 PAG-E (Kontaktverbot)
- Art. 16 Abs. 2 S. 1 Nr. 2 lit. a) PAG-E (Aufenthaltsverbot)
- Art. 16 Abs. 2 S. 1 Nr. 2 lit. b) PAG-E (Aufenthaltsgebot)
- Art. 16 Abs. 2 S. 2 PAG-E (Meldeanordnung)
- Art. 21 Abs. 1 Nr. 3 PAG (Durchsuchung von Personen)
- Art. 22 Abs. 1 Nr. 1 i. V. m. Art. 21 Abs. 1 Nr. 3 PAG (Durchsuchung von mitgeführten Sachen)
- Art. 22 Abs. 2 i. V. m. Abs. 1 Nr. 1, Art. 21 Abs. 1 Nr. 3 Pag-E (Durchsuchung räumlich getrennter Speichermedien bei Mitsichführen von Zugangsgeräten)
- Art. 25 Abs. 1 Nr. 1 lit. b) PAG-E (Sicherstellung von Sachen)
- Art. 25 Abs. 2 i. V. m. Abs. 1 PAG-E (Sicherstellung von Vermögensrechten)
- Art. 25 Abs. 3 i. V. m. Abs. 1 PAG-E (Sicherstellung von Daten)
- Art. 30 Abs. 2 S. 1 Nr. 2 lit. b) PAG-E (Verarbeitung besonderer Kategorien personenbezogener Daten)
- Art. 33 Abs. 2 PAG-E (offene Bild- und Tonaufnahmen)
- Art. 33 Abs. 5 S. 1 i. V. m. Abs. 2 PAG-E (Verwendung automatischer Mustererkennungssysteme)
- Art. 33 Abs. 5 S. 2 i. V. m. S. 1, Abs. 2 PAG-E (Verwendung automatischer Personenerkennungssysteme)
- Art. 35 Abs. 1 S. 1 Nr. 1 PAG-E (Postsicherstellung)
- Art. 36 Abs. 2 PAG-E (Verwendung besonderer Mittel der Datenerhebung)
- Art. 37 i. V. m. Art. 36 Abs. 2 PAG-E (Einsatz Verdeckter Ermittler)
- Art. 38 i. V. m. Art. 36 Abs. 2 PAG-E (Einsatz von Vertrauensleuten)

- Art. 39 Abs. 1 S. 1 i. V. m. Art 13 Abs. 1 S. 1 lit. b) PAG-E (Einsatz automatisierter Kennzeichenerkennungssysteme)
- Art. 39 Abs. 3 S. 3 i. V. m. Abs. 1 S. 2 Nr. 2 lit. a), Art. 13 Abs. 1 S. 1 lit. b) PAG-E (Erstellung von Bewegungsbildern durch Einsatz automatisierter Kennzeichenerkennungssysteme)
- Art. 40 Abs. 1 Nr. 2 PAG-E (Ausschreibung zur polizeilichen Beobachtung)
- Art. 42 Abs. 1 S. 1 Nr. 1 PAG-E (Telekommunikationsüberwachung)
- Art. 42 Abs. 1 S. 2 i. V. m. S. 1 Nr. 1 PAG-E (Überwachung räumlich getrennter Kommunikationssysteme)
- Art. 42 Abs. 2 i. V. m. Abs. 1 S. 1 Nr. 1 PAG-E (Quellen-Telekommunikationsüberwachung)
- Art. 42 Abs. 3 i. V. m. Abs. 1 S. 1 PAG-E (Einsatz des IMSI-/IMEI-Catchers)
- Art. 42 Abs. 4 PAG-E (Telekommunikationsüberwachung zu Schutzzwecken)
- Art. 42 Abs. 5 S. 1 i. V. m. Abs. 1 S. 1 Nr. 1 PAG-E (Unterbrechung, Verhinderung und Entziehung von Kommunikationsverbindungen)
- Art. 42 Abs. 5 S. 3 i. V. m. S. 2, Abs. 1 S. 1 Nr. 1 PAG-E (Unterbrechung des Zugangs zu Rundfunk, Fernsehen und vergleichbaren Medien)
- Art. 43 Abs. 2 S. 1 i. V. m. Art. 42 Abs. 1 S. 1 Nr. 1 PAG-E (Auskunftsersuchen betreffend Telekommunikationsverkehrsdaten)
- Art. 43 Abs. 2 S. 2 i. V. m. Art. 42 Abs. 1 S. 1 Nr. 1 PAG-E (Auskunftsersuchen betreffend Vorratsdaten)
- Art. 43 Abs. 4 i. V. m. Art. 42 Abs. 1 S. 1 Nr. 1 PAG-E (Auskunftsersuchen betreffend Telemedien-Nutzungsdaten)
- Art. 43 Abs. 5 S. 1 PAG-E (Auskunftsersuchen betreffend Telekommunikationsbestandsdaten)
- Art. 45 Abs. 1 S. 1 Nr. 1 PAG-E (Online-Durchsuchung)
- Art. 47 Abs. 1 Nr. 1, 2, 4, 5 i. V. m. Art. 33 Abs. 2, Art. 36 Abs. 1, 2, Art. 42 Abs. 1 bis 5, Art. 45 Abs. 1 S. 1 Nr. 1 PAG-E (Drohneneinsatz)
- Art. 60 Abs. 3 Nr. 1 PAG-E (Übermittlungsersuchen an nachrichtendienstliche Stellen)

Damit sind nach dem Entwurf mit Ausnahme der Wohnraumüberwachung (Art. 41 PAG-E) und der Rasterfahndung (Art. 44 PAG-E) sämtliche polizeilichen Befugnisse unter bestimmten Voraussetzungen schon ab der Schwelle einer drohenden Gefahr verfügbar. Die durch diese Maßnahmen erlangten personenbezogenen Daten dürfen zu anderen Zwecken der Gefahrenabwehr verwendet (Art. 48 Abs. 1 PAG-E) und an andere für Gefahrenabwehr, Strafverfolgung und nachrichtendienstliche Aufklärung zuständige inländische Stellen (Art. 48 Abs. 2 und 3, Art. 56 PAG-E) sowie ausländische und suprana-

tionale öffentliche (Art. 57, 58 PAG-E) und nichtöffentliche Stellen (Art. 59 PAG-E) übermittelt werden. Der Umstand, dass die Daten auf der Grundlage einer lediglich drohenden Gefahr erhoben wurden, spielt dabei keine Rolle.

6

Die mit dem Entwurf verfolgte Ausweitung polizeilicher Befugnisse - sowohl hinsichtlich bestehender Maßnahmen durch die Absenkung von Anordnungsvoraussetzungen, als auch durch Schaffung neuer Eingriffsbefugnisse - erscheint mit Blick auf die Problematik der Kumulierung von Überwachungsmaßnahmen[44] und das Verbot einer Total- oder Rundumüberwachung[45] schon als solche in hohem Maße verfassungsrechtlich bedenklich. Durch die Verlagerung fast aller Befugnisse in das Gefahrenvorfeld wird diese Problematik nochmals ganz erheblich verschärft. Dies wird auch deutlich, wenn man die - verfassungsrechtlich nicht zu beanstandenden - informationellen Befugnisse des BKA im Gefahrenvorfeld mit den beabsichtigten Befugnissen der Bayerischen Polizei vergleicht. Während jene des BKA auf die Bekämpfung terroristischer Straftaten zielen, enthalten die der bayerischen Polizei keine entsprechend enge Begrenzung. Während das BKA lediglich über wenige ausgewählte Befugnisse im Bereich des Gefahrenvorfelds verfügt[46], steht der bayerischen Polizei im Gefahrenvorfeld beinahe das vollständige polizeiliche Handlungsspektrum offen.

2. Zu Art. 14 Abs. 3 PAG-E (DNA-Analyse):

7

Die in Art. 14 Abs. 3 PAG-E neu geschaffene Möglichkeit der Feststellung des DNA-Identifizierungsmusters als Mittel der erkennungsdienstlichen Behandlung begegnet verfassungsrechtlichen Bedenken.

Die Feststellung, Speicherung und (künftige) Verwendung des DNA-Identifizierungsmusters greifen in das durch Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG verbürgte Grundrecht auf informationelle Selbstbestimmung ein. Dieses Recht gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[47] Diese Verbürgung darf nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen

[44] Vgl. BVerfGE 112, 304, 319 f.; 141, 220, 280, 317.
[45] Vgl. BVerfGE 65, 1, 43; 112, 304, 319; 109, 279, 323.
[46] Vgl. § 45 Abs. 1 Nr. 2 und 3, § 49 Abs. 1 Satz 2, § 51 Abs. 1 Nr. 2 und 3, § 52 Abs. 1 Nr. 2 und 3, § 55 Abs. 1 und § 56 Abs. 1 BKAG (in der ab 25.05.2018 gültigen Fassung).
[47] Vgl. BVerfGE 65, 1, 41 f.

als es zum Schutz öffentlicher Interessen unerlässlich ist.[48] Diesen Maßstab hat das BVerfG für die Feststellung des DNA-Identifizierungsmusters zur Vorsorge für die Verfolgung künftiger Straftaten (vgl. § 81g StPO) dahin konkretisiert, erforderlich sei eine Prognoseentscheidung, der eine zureichende Sachaufklärung zugrunde liegt[49], sowie in der betroffenen Person bestehende konkrete Anhaltspunkte dafür, es werde zu künftigen Strafverfahren wegen Straftaten von erheblicher Bedeutung gegen sie kommen.[50] Da es sich bei der Maßnahme nach § 81g StPO (trotz der kompetenzrechtlichen Zuordnung zur Strafverfolgung[51]) der Sache nach auch um eine solche mit präventiver Wirkung handelt[52], können diese Maßstäbe jedenfalls im Ansatz auf das Recht der Gefahrenabwehr übertragen werden.

8

Art. 14 Abs. 3 PAG-E genügt diesen Ansprüchen nicht. Die Vorschrift setzt keinerlei in der Person des Betroffenen liegende Umstände voraus, aufgrund derer die Feststellung des DNA-Identifizierungsmusters zur Abwehr einer Gefahr unerlässlich sei. Eine Zuordnung dergestalt, dass die Gefahr überhaupt von der betroffenen Person ausgehe, fehlt. Die Subsidiarität gegenüber anderen erkennungsdienstlichen Maßnahmen bleibt hinter dem Unerlässlichkeitserfordernis zurück. Außerdem deckt sich der Begriff der „Gefahr für ein bedeutendes Rechtsgut“ hinsichtlich der Einschreitschwelle nicht mit derjenigen, die in § 81g Abs. 1 StPO durch die dort genannten Straftaten konkretisiert wird. Während es sich dort um eine im konkreten Fall erhebliche Rechtsgutverletzung handeln muss, reicht in Art. 14 Abs. 3 PAG-E auch eine geringfügige Gefahr für ein bedeutendes Rechtsgut (z. B. eine leichte oder auch fahrlässige Körperverletzung). Es besteht damit die Gefahr, dass die erhöhten, verfassungsrechtlich gebotenen Voraussetzungen des § 81g Abs. 1 StPO durch die Anordnung nach Art. 14 Abs. 3 PAG-E unterlaufen werden. Demgegenüber erlauben § 21a ASOG und andere entsprechende landesrechtliche Vorschriften die molekulargenetische Untersuchung nur in wesentlich geringerem Umfang, nämlich bei Verstorbenen und hilflosen Personen, weil dies erforderlich ist, um deren Identität außerhalb strafrechtlicher Verfahren klären zu können.[53] Anders als § 21a Abs. 2 S. 2 ASOG enthält Art. 14 Abs. 3 PAG-E auch keine Vorschrift zur Löschung der erlangten personenbezogenen Daten, was in Anbetracht der Sensibilität der Daten schon für sich verfassungsrechtlich bedenklich ist.

[48] Siehe BVerfGE 65, 1, 44; 67, 100, 143.
[49] Vgl. dazu BVerfGE 70, 297, 309.
[50] Vgl. *Krehl*, in: Jahn/Krehl/Löffelmann/Güntge, Rn. 762 ff. m. w. N.
[51] Vgl. BVerfGE 103, 21.
[52] Vgl. *Schmidbauer*/Steiner, PAG, Art. 11 Rn. 193, der betont, das vorliegende Ergebnis einer molekulargenetischen Untersuchung entfalte „größte spezial- und generalpräventive Wirkung“.
[53] Vgl. Pewestorf/*Söllner*/Tölle, ASOG, § 21a vor Rn. 1; Tegtmeyer/*Vahle*, PolG NRW, § 14a Rn. 1.

3. Zu Art. 15 Abs. 3 PAG-E (Vorführung):

9

Die zwangsweise Durchsetzung der Vorladung gem. Art. 15 Abs. 3 PAG-E erlaubt einen Eingriff in das Freiheitsgrundrecht des Art. 2 Abs. 2 S. 2 GG. Generell besitzt das Freiheitsgrundrecht unter den grundrechtlich verbürgten Rechten einen besonderen Rang[54], weshalb es als „unverletzlich" gekennzeichnet ist und Art. 104 GG für seine Beschränkung qualifizierte Anforderungen statuiert. Eingriffe in das Freiheitsgrundrecht - zumal zu Zwecken, die nicht dem Schuldausgleich dienen - sind nur „aus besonders gewichtigen Gründen" unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig.[55]

10

Diesem Maßstab genügt Art. 15 Abs. 3 PAG-E nicht, soweit er die zwangsweise Durchsetzung des Erscheinens einer Person bei der Polizei erlaubt, um Angaben entgegenzunehmen, die für die Abwehr einer lediglich „drohenden Gefahr" erforderlich sind. Aufgrund der weiten Verlagerung der Anknüpfungspunkte in das Gefahrenvorfeld kann die Maßnahme Personen betreffen, die selbst zu konkreten Gefahrenlagen in keinerlei persönlicher Beziehung stehen. Danach könnte z. B. das zwangsweise Erscheinen beliebiger Personen aus dem Umfeld einer Person, deren „individuelles Verhalten (…) die konkrete Wahrscheinlichkeit begründet (…), wonach in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung zu erwarten sind" (Art. 11 Abs. 3 S. 1 Nr. 1 PAG), durchgesetzt werden. Damit wäre für die Zielperson, von der eine „drohende Gefahr" ausgeht, zugleich eine erhebliche, u. U. rufschädigende Belastung verbunden. Letztlich wäre die Maßnahme geeignet, aufgrund nur vager Verdachtsmomente als Mittel der Einschüchterung und Gängelung missbraucht zu werden. In den anderen Bundesländern ist die zwangsweise Durchsetzung des Erscheinens nur zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder zur Durchführung erkennungsdienstlicher Maßnahmen zulässig.[56] Als weniger eingriffsintensives Mittel wäre es außerdem jederzeit möglich, dass die Polizei die Auskunftsperson selbst aufsucht, wenn sie nicht bei der Polizei erscheinen möchte.

Richtigerweise sollte die Vorführung - wie in den Ländern Brandenburg, Hessen, Nordrhein-Westfalen und Sachsen-Anhalt - nur durch den Richter angeordnet werden können.

[54] BVerfGE 104, 220, 234.
[55] BVerfGE 90, 145, 172; 58, 208, 224; 70, 297, 307; 128, 326, 372 f.; BVerfG NVwZ 2016, 1079.
[56] Vgl. Pewestorf/*Söllner*/Tölle, ASOG, § 20 Rn. 22; Tegtmeyer/*Vahle*, PolG NRW, § 10 Rn. 10.

4. Zu Art. 16 Abs. 2 S. 2 PAG-E (Meldeanordnung):

11

Soweit deutsche Staatsbürger betroffen sind, wird durch die Meldeanordnung - ebenso wie durch das Aufenthaltsverbot nach Art. 16 Abs. 2 Nr. 2 lit. a) und das Aufenthaltsgebot nach Art. 16 Abs. 2 Nr. 2 lit. b) PAG-E - in das Grundrecht auf Freizügigkeit gem. Art. 11 GG eingegriffen, das einen qualifizierten Schrankenvorbehalt vorsieht. Nach dem dortigen Kriminalvorbehalt (Art. 11 Abs. 2 Alt. 5 GG) sind Eingriffe nur zulässig, „um strafbaren Handlungen vorzubeugen". Erforderlich ist insoweit, dass im konkreten Fall mit hinreichender Wahrscheinlichkeit die Begehung von Straftaten zu erwarten ist.[57] Diese Voraussetzung wird durch das Merkmal der Geeignetheit „zur Abwehr einer Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut" - die nicht einmal die Schwelle der nach Nr. 2 erforderlichen (allerdings ebenfalls unzureichenden[58]) drohenden „Begehung von Straftaten" erreicht - zweifellos nicht erfüllt. Handelt es sich sogar um eine lediglich „drohende Gefahr", sind Straftaten gerade nicht mit hinreichender Wahrscheinlichkeit zu erwarten. Obwohl es sich um ein praktisch bewährtes und effektives Instrument der Gefahrenabwehr handeln mag, dessen Kodifizierung grundsätzlich zu begrüßen ist, entspricht seine Ausgestaltung nicht den verfassungsrechtlichen Anforderungen.

Im Übrigen wird hinsichtlich der weiterhin bestehenden erheblichen Bedenken gegen aufgrund der Regelung ermöglichte Eingriffe in das Freiheitsgrundrecht auf die Stellungnahme des *Verf.* zu dem Gesetz zur effektiveren Überwachung gefährlicher Personen Bezug genommen.[59]

5. Zu Art. 18 Abs. 1 S. 2 bis 5 PAG-E (Verzicht auf persönliche Anhörung):

12

Die praxisgerechte Änderung ist zu begrüßen. Entgegen der Auffassung des Bayerischen Landesbeauftragten für den Datenschutz[60] dürfte hier keine kompetenzrechtliche Problematik vorliegen. Der bayerische Gesetzgeber übt mit der von § 422 Abs. 1 FamFG abweichenden Regelung des Art. 18 Abs. 1 S. 3 PAG-E keine Kompetenz im Bereich der konkurrierenden Gesetzgebung betreffend das gerichtliche Verfahren (Art. 74 Abs. 1 Nr. 1 GG) aus, sondern seine originäre Kompetenz für das Poli-

---

[57] *Jarass*/Pieroth, Art. 11 Rn. 17 m. w. N.; vgl. auch *Schmidbauer*/Steiner, PAG, Art. 11 Rn. 217 m. d. V. auf OVG Berlin, B. v. 18.07.2001, 1SN61.01, demzufolge die "erforderliche konkrete Gefahr (…) regelmäßig in der Wahrscheinlichkeitsprognose, dass der Betroffene sich an einem bestimmten Ort innerhalb eines bestimmten Zeitraumes an Ausschreitungen oder der Begehung von Straftaten beteiligen will" liege. Entscheidend sei dabei "die Prognose über die Gewaltbereitschaft des Betroffenen."

[58] Die Schranke des Art. 11 GG wird durch die Formulierung „wenn die Begehung von Straftaten droht" nur dann gewahrt, wenn dieses Drohen die Qualität einer konkreten Gefahr erreicht, vgl. hierzu im Zusammenhang mit Aufenthaltsgeboten *Löffelmann*, BayVBl. Heft 5/2018 unter 2. b) bb).

[59] Vgl. *Löffelmann* (Fn. 43), unter II. 2.

[60] Vgl. Der Bayerische Landesbeauftragte für den Datenschutz, Stellungnahme vom 21.12.2017 zu den Entwurf eines Gesetzes zur Neuordnung des Bayerischen Polizeirechts, Verbändeanhörung, abrufbar unter: https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf, S. 9.

zeirecht, in dessen Rahmen er eine verfahrensrechtliche Regelung trifft. Dabei steht es ihm frei, eine solche Regelung selbst zu formulieren oder auf andere Verfahrensvorschriften - auch des Bundesrechts - zu verweisen.

6. Art. 22 Abs. 1 Nr. 6 PAG-E (Durchsuchung von Sachen an einer Kontrollstelle):

13

Die Erstreckung der Durchsuchungsbefugnis auf sämtliche bewegliche Sachen, die sich an einer Kontrollstelle befinden, erscheint sachgerecht und schließt eine Regelungslücke.[61] Angesichts der relativ hohen Schwelle des Art. 13 Abs. 1 Nr. 4 PAG i. V. m. § 100a StPO bestehen unter Verhältnismäßigkeitsgesichtspunkten keine Bedenken.

7. Art. 22 Abs. 2 PAG-E (Erstreckung der Durchsuchung auf räumlich getrennte Speichermedien):

14

Der Entwurf bildet die Regelung des Art. 22 Abs. 2 PAG-E derjenigen des § 110c Abs. 3 StPO nach (S. 72), berücksichtigt dabei aber nicht, dass die letztgenannte Norm nur zur Durchsicht eines elektronischen Speichermediums sowie damit verbundener räumlich getrennter weiterer Medien berechtigt, um festzustellen, ob sich darauf relevante Daten befinden und der betreffende Datenträger also zu beschlagnahmen ist. Sowohl bei der Durchsuchung nach §§ 102, 103 StPO als auch bei derjenigen nach Art. 22 PAG handelt es sich um offene Maßnahmen, die mit einem körperlichen Eindringen in geschützte Bereiche verbunden sind.[62] Die Analogie einer Durchsuchung von Datenträgern ist daher schief; man würde auch die Auswertung analoger Datenträger nicht als Durchsuchung bezeichnen. Hinzu kommt, dass § 110 Abs. 3 StPO die Durchsicht lediglich erlaubt, wenn andernfalls der Verlust der Daten zu besorgen ist. Eine entsprechende, der Schutzwürdigkeit der Daten Rechnung tragende Einschränkung enthält Art. 22 Abs. 2 PAG-E nicht.

15

Perspektivisch bedürften sowohl die Durchsuchungs- und Beschlagnahmeregelung der StPO als auch der Polizeigesetze einer Neuregelung, die den Besonderheiten digitaler Datenherrschaft und den hierzu entwickelten verfassungsrechtlichen Maßstäben Rechnung trägt. So hat das BVerfG anerkannt, dass die Beschlagnahme und Auswertung von Datenträgern grundsätzlich nach den strafprozessualen Vorschriften über die Beschlagnahme (§§ 94, 98 StPO) erfolgen könne, einer etwaigen besonderen

[61] Vgl. *Schmidbauer*/Steiner, PAG, Art. 22 Rn. 26.
[62] Vgl. auch VollzBek zu Art. 22, Ziff. 22.1: „Sache im Sinn dieser Vorschrift ist jeder körperliche Gegenstand (…)."

Schutzbedürftigkeit der Daten - etwa wenn es sich um solche aus Telekommunikationsvorgängen handelt - sei jedoch im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen.[63] Darüber hinaus - was bislang in Rechtsprechung und Schrifttum kaum ausdrücklich thematisiert wurde[64] - kann durch den Zugriff auf elektronische Speichermedien das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme berührt werden. Dieses, vom BVerfG im Zusammenhang mit der „Online-Durchsuchung" entwickelte Grundrecht *„bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten."*[65] Eine Einschränkung im Hinblick auf die Art und Weise des Zugriffs nimmt das BVerfG bei der Schutzbereichsbestimmung nicht vor. Das Auslesen der Festplatten von Personalcomputern, der Speichereinheiten von Mobiltelefonen oder von anderen externen Datenträgern erlaubt grundsätzlich einen umfassenden Zugriff auf die dort gespeicherten Daten und damit, *„einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten."*[66] Ein schutzwürdiges Interesse der betroffenen Person daran, dass die gespeicherten Daten vertraulich bleiben, ist hier zweifellos gegeben. Soweit durch das Auslesen Zugriffsbeschränkungen überwunden (z. B. Passwörter „gehackt") werden müssen, ist dadurch auch die Integrität des Systems betroffen.[67] Andererseits ist zu berücksichtigen, dass die besondere Eingriffsintensität der Online-Durchsuchung gerade aus ihrer Heimlichkeit, Dynamik und großen Streubreite herrührt, weshalb das BVerfG die „offene Durchsuchung" grundsätzlich als milderes Mittel ansieht.[68] Dieser Unterschied spricht dafür, dass - obwohl das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme bei der Auswertung von Datenträgern betroffen sein dürfte - die erhöhten Anordnungsvoraussetzungen, die das BVerfG für Online-Durchsuchungen aufgestellt hat, auf diese Konstellation nicht übertragbar sind.[69]

16

Gleichwohl ist vor diesem Hintergrund eine differenzierte Regelung für den Zugriff auf elektronische Speichermedien samt grundrechtssichernder Verfahrensregeln erforderlich, die der besonderen Schutzwürdigkeit entsprechender Daten und ihrer Bedeutung für die Entfaltung der Persönlichkeit,

[63] BVerfGE 115, 166, 183 ff.; BVerfGE 120, 274, 307 f.; anders noch BVerfGK 5, 74, 82 ff. (Beschlagnahme und Auswertung von Mobiltelefonen nur unter den Voraussetzungen der Telekommunikationsverkehrsdatenabfrage); dazu ablehnend *Günther*, NStZ 2005, 485; *Hauschild*, NStZ 2005, 339 (Anm.); zur Kritik der kriminalistischen Praxis *Thiede*, Kriminalistik 2005, 346; *König*, Kriminalistik 2005, 520.
[64] Vgl. *Herrmann*/*Soiné*, NJW 2011, 2922, 2923.
[65] BVerfGE 120, 274, 313.
[66] BVerfGE 120, 274, 314.
[67] Vgl. BVerfGE 120, 274, 314.
[68] BVerfGE 120, 274, 321 f.
[69] Vgl. näher zum Zugriff auf dezentral gespeicherte Daten im Bereich des Rechts der Nachrichtendienste *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 5 Rn. 48 ff. m. w. N.

einschließlich einer etwaigen Gefährdung des Kernbereichs privater Lebensgestaltung und von Berufsgeheimnissen angemessen Rechnung trägt. Art. 22 Abs. 2 PAG-E genügt nicht diesem Anspruch.

8. Zu Art. 23 PAG-E (Betreten und Durchsuchen von Wohnungen):

17

Soweit der Entwurf die Erweiterung des Art. 23 Abs. 1 Nr. 3 PAG-E auf (lediglich) dringende Gefahren damit begründet, eine Beschränkung auf gegenwärtige Gefahren sei verfassungsrechtlich nicht geboten (S. 74), ist darauf hinzuweisen, dass Art. 13 Abs. 7 Alt. 3 GG für das Betretungsrecht den Zweck der Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung anhand mehrerer Regelbeispiele der Art und Schwere nach konkretisiert (Behebung der Raumnot, Bekämpfung von Seuchengefahr, Schutz gefährdeter Jugendlicher). Damit kann verfassungsrechtlich nicht jegliche dringende Gefahr eine Wohnungsbetretung legitimieren. Ob alle in Art. 11 Abs. 3 S. 2 PAG genannten Rechtsgüter mit dieser Schwelle vergleichbar sind, erscheint fraglich. Namentlich dürfte nicht jede dringende Gefahr für die Rechtsgüter Gesundheit, sexuelle Selbstbestimmung, erhebliche Eigentumspositionen und Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt, ein Eindringen in das „letzte Refugium“[70] der Privatwohnung legitimieren können.

Im Hinblick auf die unveränderte Beibehaltung von Art. 23 Abs. 1 Nr. 2 und 3 PAG wird der vom Bayerischen Landesbeauftragten für den Datenschutz geäußerten Kritik beigetreten.[71]

9. Zu Art. 24 Abs. 2 S. 2 PAG-E (Zuziehung von Durchsuchungszeugen):

18

Die Formulierung sollte - schon aus Praktikabilitätsgründen in Fällen von Gemengelagen - an § 105 Abs. 2 StPO angepasst werden.

10. Zu Art. 25 PAG-E (Sicherstellung):

19

Die Eingriffsschwelle wird hier von einer gegenwärtigen Gefahr auf eine nur konkrete oder auch lediglich „drohende“ Gefahr für ein bedeutendes Rechtsgut deutlich abgesenkt. Auf die allgemeine Kritik an den Begriffen „drohende Gefahr“ und „bedeutendes Rechtsgut“ wird Bezug genommen (Rn. 3

[70] BVerfGE 109, 279, 314.
[71] Vgl. (Fn. 60), S. 12 f.

f.). Da eine Konnexität dergestalt, dass die Gefahr von der Sache selbst ausgehen muss, nicht erforderlich ist, sondern die Gefahr auch aus dem Zustand des Besitzers oder der von ihm (vermeintlich) verfolgten Absichten hergeleitet werden kann[72], stellt die Änderung keine nur marginale Weiterung dar. Infolge der Änderung können bei einer Person, deren Verhalten die Erwartung einer „drohenden Gefahr" begründet, sämtliche Gegenstände sichergestellt werden, deren Verwendung zur Herbeiführung einer Gefahr geeignet ist, darunter zahlreiche Gegenstände des täglichen Gebrauchs wie Werkzeuge, Kraftfahrzeuge, aber auch datenverarbeitende Systeme und Kommunikationseinrichtungen, die erfahrungsgemäß für die Vorbereitung einer Gefahr Verwendung finden können. Durch die Entkoppelung von dem Erfordernis einer gegenwärtigen Gefahr verändern sich der Charakter und die Anwendungsbreite der Maßnahme grundlegend. Ein Eingriff in Art. 14 GG ist danach nicht nur, wie bisher, in Einzelfällen zur unmittelbaren Abwendung einer tatsächlich bevorstehenden Gefahr durch die Sicherstellung des Gegenstands, von dem die Gefahr ausgeht oder der sie erhöht, zulässig, sondern aufgrund vager Verdachtsmomente zur präventiven Entziehung von Gegenständen, von denen potenziell eine Gefahr ausgehen könnte. Damit überschreitet die Norm die Schwelle von der Gefahrenabwehr zur Gefahrvorsorge. Für die große Weite und Tiefe der durch die Norm ermöglichten Grundrechtseingriffe stellen sich die Anordnungsvoraussetzungen als deutlich zu undifferenziert und unpräzise dar (vgl. demgegenüber die Vorschriften zur strafprozessualen Einziehung in §§ 111b ff. StPO).

20

Diese Kritik gilt erst recht für die Erweiterung der Sicherstellung auf Vermögensrechte nach Art. 25 Abs. 2 PAG-E. Nach dieser Vorschrift können z. B. bei einer Person, deren Verhalten die Erwartung einer „drohenden Gefahr" begründet, sämtliche Konten gepfändet werden. Es liegt auf der Hand, dass derart schwer wiegende und u. U. existenzvernichtende Eingriffe in Eigentumsrechte nicht auf der Grundlage einer Prognoseentscheidung im Gefahrenvorfeld anhand unbestimmter Kriterien erfolgen darf.

21

Soweit Art. 25 Abs. 3 PAG-E die Sicherstellung auf Daten erweitert, wird auf die Ausführungen unter Rn. 14 ff. Bezug genommen. Erforderlich wäre hier aufgrund der etwaigen besonderen Schutzbedürftigkeit der sicherzustellenden Daten eine differenzierte Regelung einschließlich grundrechtssichernder Verfahrensvorschriften (Richtervorbehalt, technische Sicherungen). So ist kein durchgreifender Grund ersichtlich, warum auf kernbereichs- und berufsgeheimnisschützende Vorkehrungen schon auf der Erhebungsebene verzichtet werden sollte. Anhand von Dateibezeichnungen oder Metadaten ist hier eine Auswahl grundsätzlich möglich. Art. 25 Abs. 3 PAG-E verfolgt demgegenüber das - freilich für die Polizeibehörden bequemere - Modell einer zunächst globalen Datensicherstellung mit erst auf der

[72] Vgl. VollzBek zu Art. 25, Ziff. 25.3; *Schmidbauer*/Steiner, PAG, Art. 25 Rn. 11 ff.

Verwendungsebene greifenden Schutzvorkehrungen (Art. 25 Abs. 3 S. 2 i. V. m. Art. 49 Abs. 5 PAG-E).

11. Zu Art. 29 PAG-E (Wahrnehmung grenzpolizeilicher Aufgaben):

22

Die durch den Entwurf vorgesehenen Änderungen erweitern die grenzpolizeilichen Befugnisse der Bayerischen Landespolizei. [73] Soweit die Begründung ausführt, in Abs. 1 werde „die Diktion mit dem neuen Abs. 3 harmonisiert“ (S. 79), ist darauf hinzuweisen, dass der einfachgesetzlichen Ausprägung des Verhältnismäßigkeitsgrundsatzes in Abs. 1 der bisherigen Fassung durchaus eine Funktion zukommt, indem der Polizei für die Bewertung der Notwendigkeit kein Beurteilungsspielraum oder Ermessen zukommt. Vielmehr handelt es sich bei dem Gesichtspunkt der Erforderlichkeit um einen unbestimmten Rechtsbegriff, der gerichtlich voll überprüfbar ist.[74] Gerade dann, wenn dieselben grenzpolizeilichen Aufgaben auch durch eine Bundesbehörde wahrgenommen werden oder wenn es zu Konflikten zwischen Bundes- und Landespolizei im Rahmen des Grenzschutzes kommt[75], kann es an der Erforderlichkeit i. S. d. Art. 29 Abs. 1 PAG fehlen. Die Änderung dürfte also auf eine Stärkung der Befugnisse der Bayerischen Polizei gegenüber denen der Bundespolizei zielen. Die Klarstellung in dem neuen Abs. 3 begegnet mit Blick auf die Ermächtigung in § 2 Abs. 4 BPolG i. V. m. Art. 71 GG (als Ausnahme zur ausschließlichen Gesetzgebungskompetenz des Bundes für den Grenzschutz nach Art. 73 Abs. 1 Nr. 5 GG) und den Grundsatz der exekutiven Eigenverantwortung der Länder (Art. 83 GG) keinen Bedenken.[76] Für die Rechtsanwendung hilfreich wäre aber ein klarstellender Hinweis (zumindest in der Gesetzbegründung), um welche bundesrechtlichen Befugnisse es sich im Einzelnen handelt.

12. Zu III. Abschnitt PAG-E (Datenverarbeitung):

23

Der neu gefasste III. Abschnitt des PAG-E dient der Umsetzung der Vorgaben der Richtlinie (EU) 2016/680. Dass insoweit eine Ausweitung des Datenschutzes im PAG erfolgt, ist zu begrüßen. In ge-

[73] Derzeit beschränkt sich die grenzsichernde Zuständigkeit der Bayerischen Landespolizei nach der Befugnisübertragung gem. § 2 Abs. 1 und 3 BPolG i. V. m. § 1 Abs. 1 des Verwaltungsabkommens zwischen dem Bundesministerium des Innern und der Bayerischen Staatsregierung über die Wahrnehmung von Aufgaben des grenzpolizeilichen Einzeldienstes in Bayern vom 17.04.2008 (GVBl. S. 149) auf die Sicherung der auf dem Bayerischen Staatsgebiet liegenden Flughäfen mit Ausnahme des Flughafens München (MUC).

[74] *Schmidbauer*/Steiner, PAG, Art. 29 Rn. 2; *Grünewald*, in: Beck-OK BayPAG, Art. 29 Rn. 4.

[75] Vgl. die Kooperationsgebote nach § 4 und die Kontrollbefugnisse von Bundesbeamten nach § 5 des Verwaltungsabkommens (Fn. 73).

[76] Vgl. *Graulich*, in: Schenke/Ruthig/Graulich, BPolG, § 2 Rn. 5, 36.

setzestechnischer und systematischer Hinsicht gerät der III. Abschnitt allerdings reichlich unübersichtlich. Nach der Fassung des Entwurfs soll der III. Abschnitt künftig vier Unterabschnitte enthalten, nämlich erstens betreffend „Datenerhebung“ (Art. 31 und 32 PAG-E), zweitens betreffend „besondere Befugnisse und Maßnahmen der Datenerhebung“ (Art. 33 bis 52 PAG-E), drittens betreffend „Datenspeicherung, -übermittlung und sonstige Datenverarbeitung“ (Art. 53 bis 65 PAG-E) und viertens betreffend die „Anwendung des Bayerischen Datenschutzgesetzes“ (Art. 66 PAG-E). Diesen vier Unterabschnitten ist ein Art. 30 PAG-E mit „Allgemeinen Grundsätzen“ vorangestellt. Art. 30 PAG-E enthält - anders als Art. 4 RiLi - allerdings nicht sämtliche allgemeinen Grundsätze, die „vor die Klammer gezogen“ werden könnten, sondern stellt nur die Anwendbarkeit der nachfolgenden Regelungen für jegliche Form der Datenspeicherung klar (Abs. 1) und bezieht sich weiter auf Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten (Abs. 2, Art. 10 RiLi), die Unterscheidung zwischen faktenbasierten und auf persönlichen Einschätzungen beruhenden personenbezogenen Daten (Abs. 3, Art. 7 Abs. 1 RiLi) sowie verschiedene Kategorien betroffener Personen (Abs. 4, Art. 6 RiLi). Weitere allgemeine Grundsätze sind z. B. die der Verhältnismäßigkeit, der Zweckbindung, der Datensparsamkeit, der Datenlöschung nach Zweckerfüllung, der Kennzeichnung qualifiziert erhobener Daten, der Datenrichtigkeit und der Transparenz.[77] Auch Vorschriften betreffend den besonderen Schutz grundrechtssensibler Bereiche könnten hier verortet werden, sowie die Verweisungsnorm des Art. 66 PAG-E, der als einzige Vorschrift einen eigenen Unterabschnitt bildet. Andererseits finden sich unter dem 2. Unterabschnitt über „Besondere Befugnisse und Maßnahmen der Datenerhebung“ auch Vorschriften, die nicht die Erhebung, sondern daran anschließende Formen der Datenverarbeitung betreffen (etwa Art. 48 PAG-E) sowie Normen, die den Rechtsschutz Betroffener (Art. 50 PAG-E) und andere externe Kontrollmechanismen regeln (Art. 51, 52 PAG-E). Umgekehrt enthält der II. Abschnitt über „Befugnisse der Polizei“ auch Regelungen, die mit der Erhebung personenbezogener Daten einhergehen (etwa Art. 12 bis 14 und 21 bis 23 PAG-E). Insgesamt sollte im Wege der Novellierung viel konsequenter zwischen Regelungen betreffend die Datenerhebung und betreffend die weitere Verwendung bereits erhobener Daten differenziert werden. Rechtsschutz- und Kontrollmechanismen sollten in einem eigenen Abschnitt gebündelt werden. Zentrale allgemeine Grundsätze, etwa betreffend den Schutz grundrechtssensibler Bereiche, sollten in einem eigenen Abschnitt vorangestellt werden.

[77] Vgl. Art. 5 der Europäischen Datenschutzgrundverordnung; *Wolff*, in: Wolff/Brink, Syst. A Rn. 2 ff.

13. Zu Art. 30 PAG-E (Allgemeine Grundsätze):

24

In Umsetzung von Art. 10 RiLi erlaubt Art. 30 Abs. 2 PAG-E die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter besonderen Voraussetzungen, nämlich in S. 1 Nr. 1 ihrer subsidiären Erforderlichkeit, in Nr. 2 der Beschränkung des Verwendungszwecks auf die Abwehr von Gefahren oder drohenden Gefahren für ein bedeutendes Rechtsgut [wobei unklar ist, ob sich lit. a) allgemein auf Gefahren oder nur auf solche für ein bedeutendes Rechtsgut bezieht], in Nr. 3 einer ausdrücklichen schriftlichen Zustimmung des Betroffenen, in Nr. 4, sofern der Betroffene die Daten bereits offensichtlich öffentlich gemacht hat, und in Nr. 5 für Zwecke der Eigensicherung. Die einzelnen Erlaubnistatbestände überschneiden sich dabei, insbesondere dürfte Nr. 1 aufgrund seiner weiten Formulierung i. d. R. auch die Fälle der Nr. 2 umfassen. Nr. 3 und 4 beruhen auf allgemeinen datenschutzrechtlichen Gedanken, die im Katalog der „Allgemeinen Grundsätze" systematisch besser aufgehoben wären. Generell erscheint die differenzierende Regelung in Abs. 1 S. 1 wenig praxisgerecht. Sie führt dazu, dass, sofern besondere Kategorien personenbezogener Daten betroffen sind, auf einer weiteren Stufe zusätzlich zu den jeweiligen maßnahmespezifischen Datenverarbeitungsbefugnissen der Katalog des Abs. 1 S. 1 geprüft werden muss. Die jeweiligen Zulässigkeitsvoraussetzungen auf beiden Stufen können dabei voneinander abweichen. Praktisch wird es zudem häufig nicht möglich sein, besondere Kategorien personenbezogener Daten getrennt von den übrigen personenbezogenen Daten zu würdigen, etwa wenn im Rahmen eines überwachten Gesprächs auch politische Meinungen, religiöse oder weltanschaulicher Überzeugungen erfasst werden. Vor diesem Hintergrund besteht die Gefahr, dass der Schutz besonderer Kategorien personenbezogener Daten im Anwendungsfall nur pro forma erfolgt. Praxisgerechter als das abgestufte Schutzkonzept der RiLi erschiene eine Regelung, die - in Anlehnung an das vom BVerfG zum Kernbereichsschutz entwickelte „Zwei-Stufen-Modell"[78] - einen maßnahmespezifischen Schutzmechanismus auf der Erhebungsebene und einen allgemeinen Schutzmechanismus auf der Verwendungsebene vorsähe. Auf der Erhebungsebne würde durch erhöhte Anordnungsvoraussetzungen bei solchen Maßnahmen, die die gezielte Erfassung personenbezogener Daten einer besonderen Kategorie bezwecken (z. B. DNA-Analyse) oder bei denen jedenfalls insofern eine Verletzungsgeneigtheit[79] besteht, der besonderen Schutzbedürftigkeit solcher Daten i. S. d. von Art. 10 RiLi geforderten „unbedingten Erforderlichkeit" Rechnung getragen. Auf der Verwendungsebene müssten besondere Kennzeichnungspflichten und Weiterverarbeitungsbeschränkungen sowie Rechtsschutzmechanismen für Betroffene vorgesehen sein. Ergänzend würde auf beiden Ebenen ein ebenfalls zweistufiges System zum besonderen Schutz grundrechtssensibler Bereiche zum Tragen kommen. Ein derartiges, in der deutschen Verfassungsdogmatik besser verankertes, Regelungsmodell stünde im

[78] BVerfGE 109, 279, 318, 320, 323, 328 ff.; 120, 274, 337 ff.; 129, 208, 245 f.; 141, 220, 278 f., 295.

Einklang mit der RiLi, denn „geeignete Garantien für die (…) Rechte und Freiheiten der betroffenen Person“ können auch auf der Verwendungsebene geschaffen werden. Im Übrigen erfordert die RiLi neben der Voraussetzung, dass die Verarbeitung „unbedingt erforderlich“ (also streng subsidiär gegenüber Maßnahmen, bei denen keine Daten einer besonderen Kategorie erhoben werden) sein müsse nur, dass die Datenverarbeitung „in durch Rechtsvorschriften geregelten Fällen erlaubt ist“ (vgl. Erwägungsgrund 37). Die RiLi fordert also einen strengen Gesetzesvorbehalt, dem polizeiliche Befugnisse, welche in Grundrechte eingreifen, ohnehin von Verfassung wegen genügen müssen.[80] Die bloße Soll-Vorschrift des Abs. 2 S. 2 genügt auf der Verwendungsebene dem Erfordernis „geeigneter Garantien“ allerdings nicht; hier müsste eine verbindliche und präzisere Regelung vorgesehen werden. Um welche Daten es sich bei solchen handelt, die einer „besonderen Kategorie“ i. S. v. Art. 10 RiLi zugehören, sollte außerdem aus Gründen der Praktikabilität unmittelbar im PAG (deklaratorisch) festgelegt werden.

14. Zu Art. 31 PAG-E (Grundsätze der Datenerhebung):

25

In Umsetzung der Vorgaben von Art. 12 und 13 RiLi werden in Art. 31 Abs. 3 S. 2 und 3 PAG-E allgemeine Informationspflichten der Polizei eingeführt. Nach der Entwurfsbegründung könnten die relevanten Informationen über den Internetauftritt der Polizei zur Verfügung gestellt werden (S. 84). Entsprechend lässt sich Abs. 3 S. 2 so verstehen, dass nicht Informationen zu einem konkreten, eine bestimmte Person betreffenden, Datenerhebungsvorgang gemeint sind, sondern lediglich generelle Angaben. Ob dieser allgemeine Zuschnitt der Informationspflichten den Vorgaben der RiLi gerecht wird, ist fraglich. Laut Erwägungsgrund 38 der RiLi sollte eine automatisierte Datenverarbeitung *„mit geeigneten Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person (...).“* Nach Erwägungsgrund 39 sollen, *„damit die betroffene Person ihre Rechte wahrnehmen kann, (...) alle Informationen für sie leicht zugänglich - auch auf der Website des Verantwortlichen - (...) sein.“* Art. 12 Abs. 1 S. 2 RiLi spricht von der *„Übermittlung“* der relevanten Informationen *„in einer beliebigen geeigneten Form, wozu auch die elektronische Übermittlung zählt“*. Generell zielt die RiLi auf eine signifikante Anhebung des Rechtsschutzes betroffener Personen. Dies setzt zunächst voraus, dass die betroffene Person von dem Vorgang der Datenerhebung überhaupt Kenntnis erhält. Art. 12 und 13 RiLi dürften vor diesem Hintergrund so zu verstehen sein, dass in jedem Fall eine spezifische Unterrichtung der betroffenen Person darüber, dass ihre personenbezogenen Daten erhoben

[79] BVerfGE 141, 220, 277, 279; ausf. zu eine Kernbereichsgefährdung indizierenden Gesichtspunkten *Löffelmann*, in: Dietrich/Eiffler, Teil III § 3 Rn. 6 ff.

[80] Vgl. ähnlich zu dem Art. 10 der RiLi korrespondierenden Art. 9 der Datenschutzgrundverordnung und allg. krit. zum abgestuften europäischen Schutzkonzept *Kampert*, in: Sydow, Artikel 9 Rn. 2 f., 65 f., 83 ff.

wurden, erforderlich ist.[81] Entsprechend spricht Erwägungsgrund 42 von der *„Existenz des Verarbeitungsvorgangs“*, über die informiert werden müsse. Allerdings ist darauf hinzuweisen, dass die RiLi in diesem Punkt uneindeutig ist, denn im selben Erwägungsgrund wird ausdrücklich festgestellt, die Bereitstellung der Informationen könne *„auf der Website der zuständigen Behörde erfolgen.“* Dazu, auf welche Weise die betroffene Person auf der Webseite der zuständigen Behörde über die Existenz eines diese Person betreffenden Verarbeitungsvorgangs in Kenntnis gesetzt werden kann (etwa durch Bereitstellung eines Passworts), verhält sich die RiLi nicht. Art. 31 Abs. 3 S. 2 PAG-E sieht jedenfalls eine *spezifische* Unterrichtung der betroffenen Person nicht vor und bleibt daher hinter dem Anliegen der RiLi zurück. Dass ergänzend zu einer spezifischen Unterrichtung allgemeine Informationen über die Rechte der betroffenen Person auf der Webseite der Polizei zur Verfügung gestellt werden, wäre freilich zu begrüßen.

26

Soweit Art. 31 Abs. 4 S. 1 Nr. 2 PAG-E die Zulässigkeit verdeckter Datenerhebungen darauf ausdehnt, dass dies überwiegenden Belangen Dritter diene, erschließt sich - auch aus der Entwurfsbegründung - nicht, welche Belange damit gemeint sind. Verfassungsdogmatisch erscheint es außerhalb des Bereichs der Drittwirkung von Grundrechten prekär, grundrechtlich geschützte Interessen der von hoheitlichen Maßnahmen betroffenen Personen gegen „Belange“ dritter Personen abzuwägen, zumal hier eine einfache Eignung der Maßnahme, solchen Belangen zu „dienen“, ausreichen soll. Die Formulierung „oder Dritter“ sollte daher gestrichen und anstelle der Formulierung „dient“ der bisherige Wortlaut beibehalten werden.

27

Nicht den Vorgaben der Richtlinie (vgl. Art. 13 Abs. 3 RiLi) dürfte ferner Art. 31 Abs. 4 S. 4 PAG-E entsprechen, der ein dauerhaftes Absehen von der Benachrichtigung der betroffenen Person erlaubt, *„wenn es sich nur um einen kurzfristigen Eingriff handelt, an den sich keine Folgemaßnahmen anschließen.“* Ein derartiger Ausnahmetatbestand ist in der RiLi nicht vorgesehen. Auch kurzzeitige Grundrechtseingriffe können außerdem mit erheblichen Beeinträchtigungen einhergehen. Der in der Entwurfsbegründung ergänzend herangezogene Gedanke einer etwaigen Vertiefung des Eingriffs durch die Benachrichtigung ist hiervon zu unterscheiden und als Rechtfertigung eines Absehens von der Benachrichtigung anerkannt.[82] Unter einem praktischen Blickwinkel ist die Regelung freilich gut nachvollziehbar.

---

[81] Ähnlich zum entsprechenden Art. 12 der Datenschutzgrundverordnung *Greve*, in: Sydow, Artikel 12 Rn. 17: „Die an den Betroffenen zu richtenden Informationen müssen individuell und gezielt erfolgen (…). Erst wenn die Informationen gezielt und für ihn deutlich erkennbar an den Betroffenen adressiert sind, wird den Anforderungen des Transparenzgebots entsprochen.“ Dass die Information auch über das Internet, z. B. mittels Pop-Up-Fenster zur Verfügung gestellt werden könnten (Rn. 18), macht nur dann Sinn, wenn der Betroffene von sich aus Dienste über das Internet in Anspruch nimmt. Für die aufgrund polizeilicher Datenerhebungen erforderlichen Informationspflichten trifft das nicht zu.

[82] Vgl. BVerfGE 109, 279, 365.

28

Übergreifend ist festzustellen, dass Art. 31 PAG-E entgegen der Intention der Verfasser (vgl. S. 84 o.) kaum an Übersichtlichkeit gewinnt. Nach der Entwurfssystematik würden die allgemeinen Informationspflichten des Abs. 3 S. 2 und 3 nur für offene, nicht aber für verdeckte Maßnahmen gelten, wofür kein Grund erkennbar ist. Andererseits würde der Ausnahmetatbestand des Abs. 4 S. 2 - entgegen der bisherigen Rechtslage - für offene Maßnahmen keine Wirkung entfalten. Vor dem Hintergrund der RiLi, die eine umfassende Stärkung der Betroffenenrechte fordert, ist diese Differenzierung schwer nachzuvollziehen.

15. Zu Art. 32 PAG-E (Datenerhebung):

29

Die Erweiterung der Analyse von DNA-Spurenmaterial in Art. 32 Abs. 1 S. 2 und 3 PAG-E ist zu begrüßen. Für eine entsprechende Ausweitung hatten sich anlässlich der Innenministerkonferenz im Juni 2017 bereits die Innenminister von Bund und Ländern ausgesprochen. Der Bundesminister der Justiz hatte sich im Rahmen der Justizministerkonferenz im Juni 2017 dieser Auffassung angeschlossen.[83] Bedenken hinsichtlich einer Nutzung kodierender Bereiche der DNA greifen insoweit nicht durch. Auch in § 81e StPO hat der Gesetzgeber eine Unterscheidung von zulässigen und nicht zulässigen Untersuchungen anhand der Begriffe „kodierender" und „nicht kodierender" Merkmale nicht vorgenommen.[84] Die Gesetzbegründung zu § 81e StPO führt in diesem Zusammenhang aus: *„Eine Unterscheidung von zulässigen und nichtzulässigen Untersuchungen anhand der Begriffe ‚kodierender' und ‚nicht-kodierender' Merkmale berücksichtigt ohnehin nicht ausreichend die neueren wissenschaftlichen Erkenntnisse. Auch nicht-kodierende Abschnitte des menschlichen Genoms sind nämlich Persönlichkeitsmerkmale. (...) Im Übrigen ist die DNA-Analyse nur Teilaspekt eines umfassenden Spurengutachtens. Herkunft, Entstehungsweise und Zusammensetzung des Spurenmaterials müssen oft im Wege einer ‚Genprodukt-Analyse' (ABO-Blutgruppen und zahlreiche weitere ‚genetisch' determinierte Blutmerkmalsysteme) untersucht werden, die zunehmend durch ‚Gen-Analysen' ersetzt werden. In unterschiedlichem Maße enthalten also bereits die derzeitigen Spurengutachten Informationen über kodierende und nicht-kodierende Anteile."*[85] § 81e StPO gestattet damit grundsätzlich auch die Analyse kodierender Bereiche der DNA, soweit hierdurch keine Feststellungen über schutzbedürftige Persönlichkeitsmerkmale getroffen werden und also der absolut geschützte Kernbereich der Persönlichkeit nicht betroffen ist.[86] Die Vorschrift ermöglicht es auf diese Weise, wissenschaftlichen Fortent-

[83] Vgl. becklink 2007036: „Justizministerkonferenz: Maas für Nutzung erweiterter DNA-Analyse im Strafverfahren".
[84] *Krause*, in: Löwe-Rosenberg, § 81e Rn. 25 m. w. N.; für eine Beschränkung der Untersuchungen im nicht-kodierenden Bereich allerdings der Entwurf der Fraktion der SPD unter BT-Drs. 13/3116, S. 6.
[85] BT-Drs. 13/667, S. 6.
[86] Vgl. auch BVerfGE 103, 21, 32.

wicklungen bei den Analysemethoden - in den von § 81e Abs.1 Satz 3 StPO gesetzten Grenzen - Rechnung zu tragen. Diese Überlegungen lassen sich auch auf die Verwendung zu Zwecken der Gefahrenabwehr übertragen. Soweit der Bayerische Landesbeauftragte für den Datenschutz in seiner insoweit ablehnenden Stellungnahme die Geeignetheit der Untersuchung in Frage stellt[87], ist darauf hinzuweisen, dass unter den prognostischen Erfordernissen der Gefahrenabwehr Wahrscheinlichkeiten zwischen 75 und 98 %[88] als praktisch äußerst relevant angesehen werden können. Insoweit sind andere Maßstäbe als für die Verurteilungswahrscheinlichkeit im strafprozessualen Bereich anzulegen.

16. Zu Art. 33 PAG-E (Offene Bild- und Tonaufnahmen):

a) Zu Abs. 1 Nr. 2 (Bildaufnahmen wegen Größe oder Unübersichtlichkeit der Örtlichkeit):

30

Dass bei Veranstaltungen oder Ansammlungen, die an unübersichtlichen oder ausgedehnten Örtlichkeiten stattfinden, ein praktisches Bedürfnis für eine ressourcenschonende Gewährleistung der öffentlichen Sicherheit und Ordnung besteht, ist im Ansatz nachvollziehbar. Indem Art. 33 Abs. 1 Nr. 2 PAG-E den Einsatz offener Bild- und Tonaufnahmen lediglich an ein nicht näher spezifiziertes Kriterium der Erforderlichkeit bindet, verletzt die Norm das verfassungsrechtliche Erfordernis einer präzisen bereichsspezifischen Ermächtigungsgrundlage für diesen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung Betroffener.[89] Bereits in einer Kammerentscheidung aus dem Jahre 2007 hatte das BVerfG die auf Art. 16 Abs. 1 und Art. 17 Abs. 1 BayDSG gestützte Videoüberwachung eines öffentlichen Platzes als verfassungswidrig angesehen. Das Gericht führte aus, die Videoüberwachung sei ein *„intensiver Eingriff. Sie beeinträchtigt alle, die den betroffenen Raum betreten. Sie dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Das Gewicht dieser Maßnahme wird dadurch erhöht, dass infolge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden kann. Von den Personen, die die Begegnungsstätte betreten, dürfte nur eine Minderheit gegen die Benutzungssatzung oder andere rechtliche Vorgaben, die sich aus der allgemeinen Rechtsordnung für die Benutzung der Begegnungsstätte ergeben, verstoßen. Die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials erfassen daher - wie bei solchen Maßnahmen stets - überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird.“*[90] Eine allgemeine Regelung, die die Datenerhebung lediglich durch das Gebot der Erforderlichkeit begrenze und bei der aufgaben- oder bereichsspezifische Voraus-

[87] (Fn. 60), S. 22 f.
[88] Vgl. BR-Drs. 117/17, S. 5.
[89] Vgl. BVerfGE 65, 1, 44 ff.; 100, 313, 359 f.; 110, 33, 52; 113, 348, 375.
[90] BVerfG NVwZ 2007, 688, 691.

setzungen der Datenerhebung fehlten, genüge nicht dem Bestimmtheitsgebot. *„Das in Art.16 Abs.1 BayDSG enthaltene Gebot der Erforderlichkeit kann die behördliche Praxis nicht hinreichend anleiten oder Kontrollmaßstäbe bereitstellen, wenn es nicht auf ein näher beschriebenes Normziel ausgerichtet wird. Die Norm bietet daher keine hinreichenden Maßstäbe für die Beurteilung der Rechtmäßigkeit einer Videoüberwachung. Auch kann der Einzelne auf dieser Grundlage nicht vorhersehen, bei welcher Gelegenheit, zu welchem Zweck und auf welche Weise Informationen über ihn erhoben werden dürfen.“*[91]

31

An diesen Maßstäben ist auch Art. 33 Abs. 1 Nr. 2 PAG-E zu messen. Zwar findet hier eine gewisse bereichsspezifische und ermessensleitende Konkretisierung dergestalt statt, dass die Maßnahme „wegen der Größe oder Unübersichtlichkeit der Örtlichkeit“ erforderlich sein muss. Die Vorschrift lässt aber völlig offen, wozu die Maßnahme erforderlich sein muss, welcher Zweck also mit ihr verfolgt wird. Auch spezifiziert die Vorschrift nicht, ob die betroffenen Personen für die Maßnahme einen Anlass geben müssen und wie dieser beschaffen sein muss. Damit wird die Entscheidung über ihren Einsatz einseitig in das Ermessen der Polizei gestellt und erlaubt die Vorschrift letzten Endes die anlasslose Überwachung jeglicher Menschenansammlungen (etwa: Konzertveranstaltungen, Bürgerfeste, Sportveranstaltungen, public viewing-Veranstaltungen) und Örtlichkeiten (etwa: belebte öffentliche Plätze und Straßen, Einkaufszentren, Bahnhöfe, Pausenhöfe, Schwimmbäder), die nicht ohne weiteres ohne Einsatz von Videotechnik überblickt werden können. Schon die Vielzahl der möglichen Einsatzszenarien zeigt, dass der Einzelne anhand der gesetzlichen Norm nicht vorhersehen kann, bei welcher Gelegenheit, zu welchem Zweck und auf welche Weise Informationen über ihn erhoben werden dürfen. Die Ermächtigung des Art. 33 Abs. 1 Nr. 2 PAG-E dürfte damit verfassungswidrig sein.

b) Zu Abs. 4 (Aufnahmegeräte zum Personenschutz):

32

Die Einführung einer Rechtsgrundlage in Art. 33 Abs. 4 PAG-E für den Einsatz von sog. Bodycams und ähnlichen Aufzeichnungsgeräten zum Personenschutz insbesondere eingesetzter Polizeibeamter ist ausdrücklich zu begrüßen. Mit dem - dringend regelungsbedürftigen - Einsatz solcher Geräte zu privaten Zwecken[92] ist die Maßnahme unter Verhältnismäßigkeitsgesichtspunkten nicht zu vergleichen. Von einer abschreckenden und das Verhalten betroffener Personen lenkenden Wirkung von Videoaufzeichnungen geht auch das BVerfG grundsätzlich aus[93], weshalb an der Eignung der Maßnahme, das Ziel des Personenschutzes zu fördern - trotz erwägenswerter Einwände des Bayerischen Lan-

[91] A. a. O.
[92] Vgl. *Löffelmann*, JR 2016, 661.
[93] Vgl. BVerfG NVwZ 2007, 688, 690 m. d. H. auf *Geiger*, Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung, 1994, S. 52 ff.

desbeauftragten für den Datenschutz[94] - keine durchgreifenden Zweifel bestehen. Auch die technikoffene Ausgestaltung der Vorschrift ist sachgerecht. Verfassungsrechtlich problematisch erscheint hingegen die Regelung in Abs. 4 S. 2 zum Einsatz solcher Geräte in Wohnungen. Den erläuternden Hinweisen in der Entwurfsbegründung (S. 88 f.), die diesen Einsatzzweck auf die Schranke des Art. 13 Abs. 7 GG stützen, kann nicht gefolgt werden. Art. 13 Abs. 7 GG betrifft als Auffangtatbestand lediglich Eingriffe in das Wohnungsgrundrecht, die nicht eine Durchsuchung darstellen oder durch den Einsatz technischer Mittel erfolgen.[95] Einschlägig wäre hier die Schranke des Art. 13 Abs. 5 GG, allerdings müsste in diesem Fall der Einsatz streng auf den Schutz der in der Wohnung tätigen Polizeibeamten beschränkt sein, da der Einsatz technischer Mittel sich ausdrücklich nicht auf den Schutz dritter Personen bezieht. Am einfachsten ließe sich die Verfassungskonformität der Regelung daher durch Streichung der Formulierung „oder eines Dritten“ in S. 2 herstellen. Die mit Blick auf die Schranke des Art. 13 Abs. 4 GG wichtige Einschränkung „sofern damit nicht die Überwachung der Wohnung verbunden ist“, wäre dann entbehrlich, ohne dass es einer Festlegung bedürfte, ob durch den Einsatz von Bodycams in Wohnungen eine (ungezielte) technische Überwachung der Wohnung zu sehen sei.[96]

c) Zu Abs. 5 (Verwendung automatischer Erkennungs- und Auswertungssysteme):

33

Durch den Einsatz automatischer Erkennungs- und Auswertungssysteme bei Maßnahmen nach den Abs. 1 bis 3, zu dem Abs. 5 ermächtigt, erhöht sich beträchtlich die jeweilige Leistungsfähigkeit der Maßnahme zur Erfassung relevanter personenbezogener Daten, an die sich weitere Verwendungsmöglichkeiten anschließen können, und damit ihre Eingriffsintensität. In diesem Sinne hat das BVerfG festgestellt, eine *„Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte. Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz.“*[97] In seiner Entscheidung zur automatisierten Kfz-Kennzeichenerfassung hat das BVerfG ausgeführt, die *„besondere Schlagkraft und Eingriffsintensität eines derartigen Observationsmittels entsteht sowohl aus der Vervielfachung der Zahl der möglichen Erfassungsvorgänge (vgl. BVerfGE 107, 299 [328]; 115, 320 [357]) gegenüber den bisherigen technischen und personellen Möglichkeiten der Polizei als auch aus den durch die*

[94] (Fn. 60), S. 25.
[95] *Jarass*/Pieroth, Art. 13 Rn. 34.
[96] So der Bayerische Landesbeauftragte für den Datenschutz, (Fn. 60), S. 26; ggf. ließe sich eine (weitgehende) Beschränkung des Einsatzes auf den Personenschutz auch durch geeignete technische Vorkehrungen erreichen, etwa durch die Verwendung von nur für Nahaufnahmen geeignete Geräte.
[97] BVerfGE 65, 1, 42; 113, 29, 45 f.; 115, 320, 342; 120, 278, 398.

Automatisierung und Vernetzung ermöglichten verbesserten Bedingungen für eine effektive und zudem heimliche Datenerfassung und -verarbeitung.“[98]

34

Dieser Befund trifft auch auf den Einsatz automatischer Erkennungs- und Auswertungssysteme für Video- und Bildaufzeichnungen zu. Die konkreten Anforderungen an die Bestimmtheit und Klarheit der Ermächtigung richten sich nach der Art und Schwere des Eingriffs.[99] Hier handelt es sich um eine Maßnahme, die über eine große Streubreite verfügt und von der entsprechend Einschüchterungseffekte und ein Gefühl des Überwachtwerdens ausgehen können[100], zumal den betroffenen Personen nicht erkennbar ist, ob die Aufzeichnungen automatisiert ausgewertet werden. Teilweise knüpft die Maßnahme sogar an Voraussetzungen an, die vollkommen unabhängig von einer etwaigen Verantwortlichkeit der betroffenen Personen für eine Gefahr (Abs. 1 Nr. 2, Abs. 2 und 3) oder davon sind, ob überhaupt eine Gefahr für ein Rechtsgut gegeben ist (Abs. 1 Nr. 2). An die erfolgreiche Datenanalyse können sich zudem weitere Maßnahmen von großer Tragweite anschließen, bis hin zur strafrechtlichen Verfolgung. Dabei sind die betroffenen Personen einem rein automatischen Vorgang ausgesetzt, auf den sie keinerlei Einfluss haben.[101] Vor diesem Hintergrund ist der Einsatz automatischer Erkennungs- und Auswertungssysteme als schwer wiegender Eingriff in das Recht auf informationelle Selbstbestimmung betroffener Personen zu qualifizieren. Eine Ermächtigung hierfür bedarf einer präzisen bereichsspezifischen Grundlage, die sicherstellt, dass sich Anlass und Umfang der Maßnahme sowie die Verwendung daraus gewonnener Daten in den vom Gesetzgeber festgelegten Grenzen der Verhältnismäßigkeit halten. Diese Funktion erfüllt Abs. 5 nicht. S. 1 macht den Einsatz solcher Systeme ausschließlich davon abhängig, dass dies „die jeweilige Gefahrenlage auf Grund entsprechender Erkenntnisse erfordert.“ Ermessensleitende Kriterien dafür, unter welchen Umständen dies der Fall sei, fehlen vollständig. Damit legt die Norm die Entscheidung über die relevanten Maßstäbe und damit den Einsatz der Systeme ganz in die Hand der Polizeibehörden. Auch eine Beschränkung der Maßnahme auf die Bekämpfung von Bedrohungen durch Terrorismus und gewaltbereiten Extremismus, worauf die Begründung hinweist (S. 89), enthält die Norm nicht. Die Ermächtigung nach Abs. 5 S. 1 dürfte daher als verfassungswidrig zu qualifizieren sein. Mit Blick auf das gezielte Tracking individueller Personen nach Abs. 5 S. 2 ist die Norm zwar präziser gefasst, da dieser Einsatz nur zur Abwehr einer Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut zulässig ist. In Konstellationen nach Abs. 1 Nr. 2 schließt dies eine Anwendung aus, in den anderen Konstellationen nach Abs. 1 Nr. 1, Abs. 2

[98] BVerfGE 120, 278, 407.
[99] BVerfGE 110, 33, 55.
[100] Zu diesen Topoi vgl. BVerfGE 65, 1, 42; 107, 299, 328; 113, 29, 46; 115, 320, 354 f.; 120, 378, 402; 125, 260, 319, 332; ähnlich EuGH, Urteil vom 8.4.2014, C293/12 und C594/12, Rn. 37 zur „Vorratsdatenspeicherung“.
[101] Art. 11 Abs. 1 der Richtlinie (EU) 2016/680 verlangt daher, „dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung - einschließlich Profiling -, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, verboten ist, es sei denn, sie ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten,

und 3 schränkt es sie ein. Vor dem Hintergrund, dass die Eingriffsintensität hier nochmals höher anzusetzen ist, erscheint die Maßnahme aber jedenfalls, soweit sie auch bei lediglich drohenden Gefahren eingesetzt werden kann, verfassungsrechtlich als nicht unbedenklich.

17. Zu Art. 34 PAG-E (Elektronische Aufenthaltsüberwachung):

35

Auf die im Gesetzgebungsverfahren zur Einführung der Elektronischen Aufenthaltsüberwachung durch das Gesetz vom 24.07.2017 geäußerte Kritik wird Bezug genommen.[102] Die Novellierung der Vorschrift sollte Anlass bieten, die rechtstatsächliche Wirksamkeit und Praxistauglichkeit der Maßnahme anhand der bislang gewonnenen Erfahrungswerte zu überprüfen.

Eine Weiterung enthält die Norm in der Fassung des Entwurfs nur dahin, dass nach Abs. 1 Hs. 2 des Art. 48 PAG-E, der Art. 34a Abs. 5 und 6 PAG ersetzt, für die weitere Verwendung der erhobenen Daten für Zwecke der Gefahrenabwehr nunmehr „auch ein Ansatz für weitere Sachverhaltsaufklärungen“ ausreichend ist. Da es sich bei den durch eine elektronische Aufenthaltsüberwachung erhobenen personenbezogenen Daten um solche von hoher Persönlichkeitsrelevanz handelt, die u. a. auch die Erstellung eines lückenlosen Bewegungsprofils über einen längeren Zeitraum erlauben, erscheint diese Schwelle unter Verhältnismäßigkeitsgesichtspunkten als zu niedrig. Ein bloßer „Ansatz für weitere Sachverhaltsaufklärungen“ auch in anderen Zusammenhängen kann sich aus diesen Daten z. B. dergestalt ergeben, dass sie Auskunft über Örtlichkeiten geben, an denen sich die überwachte Person aufgehalten hat, und an denen weitere Aufklärungsmaßnahmen ansetzen können. Damit können die erlangten sensiblen Daten praktisch unbegrenzt weiter verarbeitet werden.

18. Zu Art. 35 PAG-E (Postsicherstellung):

a) Zu Abs. 1 S. 1 Nr. 1 (Anordnung bei drohender Gefahr):

36

Die neu geschaffene Ermächtigung zur Postsicherstellung ist zu beanstanden, soweit sie als Anlass eine drohende Gefahr für ein in Art. 11 Abs. 3 S. 2 Nr. 1, 2 oder 5 genanntes bedeutendes Rechtsgut ausreichen lässt. Angesichts dessen, dass die Maßnahme in schwer wiegender Weise in das Postgeheimnis des Art. 10 Abs. 1 GG eingreift, sind die an das Bestehen einer drohenden Gefahr geknüpften Anordnungsvoraussetzungen zu vage. Auf die Ausführungen unter Rn. 3 f. wird Bezug genommen.

---

dem der Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen erlaubt.“

[102] Vgl. *Löffelmann* (Fn. 43) unter II. 3.; *ders*., BayVBl. Heft 5/2018 unter 2. c).

Der Zuschnitt des § 50 BKAG, auf den sich die Entwurfsbegründung bezieht, ist schon im Ansatz wegen des engeren Aufgabenbereichs des BKA deutlich enger.

b) Zu Abs. 1 S. 1 Nr. 2 (Anordnung gegen Nachrichtenmittler):

37

Die Bedenken des Bayerischen Landesbeauftragten für den Datenschutz zu Art. 35 Abs. 1 Nr. 2 PAG-E betreffend die Einbeziehung von Nachrichtenmittlern in die Überwachung[103] werden hingegen nicht geteilt. Die entsprechenden Ausführungen des BVerfG im BKAG-Urteil, auf die sich der Landesbeauftragte bezieht, sind einerseits im Zusammenhang mit den dort überprüften – noch eingriffsintensiveren – heimlichen technischen Überwachungsmaßnahmen zu sehen. Auf die Postbeschlagnahme, die eine wesentlich geringere Streubreite aufweist, können diese Maßstäbe nicht ohne weiteres übertragen werden, da das BVerfG der Eingriffstiefe maßgebliche Bedeutung für die Art der Überwachungsmaßnahmen gegenüber Dritten zumisst.[104] Entsprechend erlaubt § 99 S. 2 StPO - bislang verfassungsrechtlich unbeanstandet - die Beschlagnahme von Postsendungen bei dritten Personen, wenn *„aus vorliegenden Tatsachen zu schließen ist, dass sie von dem Beschuldigten herrühren oder für ihn bestimmt sind."* Nicht beanstandet hat das BVerfG[105] zudem sogar im Bereich der strafprozessualen Telekommunikationsüberwachung die Anordnung gegen Personen, *„von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt"* (§ 100a Abs. 3 StPO). Im BKAG-Urteil ist das BVerfG vor diesem Hintergrund so zu verstehen, dass die erforderliche *„spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat"* gerade aus der Eigenschaft, Nachrichtenmittler für die verantwortliche Person zu sein, herrühren kann. Demgegenüber *„reicht es nicht schon, dass sie mit der Zielperson überhaupt in irgendeinem Austausch stehen. Vielmehr bedarf es zusätzlicher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird (vgl. BVerfGE 107, 299 <322 f.>; 113, 348 <380 f.>)."* Nachrichtenmittler zu sein, ist mehr, als „in irgendeinem Austausch" zu stehen; die dieser Wertung zugrunde liegenden Tatsachen stellen „zusätzliche Anhaltspunkte" für die Geeignetheit der Maßnahme dar. Die Formulierung „und sie daher mutmaßlich in Zusammenhang mit der Gefahrenlage steht" in Art. 35 Abs. 1 S. 1 Nr. 2 PAG-E ist daher entbehrlich und missverständlich und sollte gestrichen werden.

[103] (Fn. 60), S. 31 f.
[104] BVerfGE 141, 220, 274 f.
[105] BVerfGE 129, 208, 242 f.

c) Zu Abs. 3 (gerichtliche Anordnung):

38

Um dem Gewicht und der Bedeutung des Grundrechtseingriffs angemessen Rechnung zu tragen, sollte neben den qualifizierten Begründungspflicht für die gerichtliche Anordnung in Art. 35 Abs. 3 PAG-E - wie auch in § 50 Abs. 2 und 3 BKAG[106] - ein qualifiziertes Antragserfordernis vorgesehen werden.

d) Zu Abs. 4 S. 2 (Übertragung der Befugnis zum Öffnen):

39

Soweit in Art. 35 Abs. 4 S. 2 PAG-E die Befugnis zur Öffnung der Sendungen auf die Polizei übertragen werden kann, erscheint auch dies zu weit. Die Übertragung ist – anders als in § 100 Abs. 3 S. 2 StPO, wo dies nur in Betracht kommt, wenn der Erfolg der Ermittlungen von einem sofortigen Eingreifen der Staatsanwaltschaft abhängt und damit zu rechnen ist, dass sich aus der beschlagnahmten Post Anhaltspunkte für Art, Umfang oder Ort weiterer Ermittlungen ergeben[107] – an keinerlei substanzielle Voraussetzungen gebunden. Die Formulierung „soweit dies in zeitlicher Hinsicht erforderlich ist“, ermöglicht eine Übertragung z. B. bereits bei jeder aus der zusätzlichen Belastung des Gerichts resultierenden Verzögerung der Überprüfung. Hinzu kommt, dass, anders als von der Staatsanwaltschaft, bei der es sich um ein Organ der Rechtspflege handelt, die Wahrnehmung einer präventiv grundrechtsschützenden Funktion von der Polizei nicht ohne weiteres erwartet werden kann. Entsprechend ist die Übertragungsbefugnis nach § 50 Abs. 5 S. 2 BKAG deutlich enger gestaltet (Zuständigkeit des Präsidenten des BKA oder seiner Vertretung) und auch nur bei Gefahr im Verzug möglich.

Im Übrigen ist die Schaffung der Ermächtigung, die eine Regelungslücke zur Telekommunikationsüberwachung schließt[108], zu begrüßen.

19. Zu Art. 36 PAG-E (Besondere Mittel der Datenerhebung):

a) Zur Überschrift und Systematik:

40

Die Überschrift der Norm, die bislang diverse Mittel der Datenerhebung versammelt (langfristige Observation, verdeckte Bildaufnahmen, verdeckter Einsatz von Peilsendern und ähnlichen Geräten, „kleiner Lauschangriff“, Einsatz von V-Leuten, automatische Kennzeichenüberwachung), ist nach der

[106] Vgl. BT-Drs. 18/11163, S. 119.
[107] BT-Drs. 7/551, S. 65.
[108] Vgl. BT-Drs. 18/11163, S. 119, wo zu § 50 BKAG darauf hingewiesen wird, die Regelung sei „notwendig, da terroristische Tätergruppen verstärkt auf konventionelle Postsendungen in bestimmten Bereichen Ihrer Kommunikation zugreifen. Auch für die Verbringung von logistischen Gütern erlangt der Postweg zunehmende Bedeutung gegenüber den bisher prak-

beabsichtigten „Auslagerung“ der in Abs. 1 Nr. 3 und Abs. 2 geregelten Maßnahmen wenig aussagekräftig. Es sollte daher erwogen werden, im Zuge der Novellierung entsprechend der sonstigen Systematik des Entwurfs den verbleibenden Maßnahmen jeweils eigene Normen zuzuweisen, auch um ihre selbständige Bedeutung und unterschiedliche Eingriffsintensität deutlich zu machen.

b) Zu Abs. 1 Nr. 2 lit. a) (Einsatz automatisierter Erkennungs- und Auswertungssysteme):

41

Auf die erheblich erhöhte Eingriffsintensität von Bildaufnahmen und Videoaufzeichnungen, wenn deren Einsatz mit automatisierten Erkennungs- und Auswertungssystemen verbunden ist, wurde bereits hingewiesen (oben Rn. 33 f.). Die Ermächtigungsnorm trägt dem nicht durch erhöhte Anordnungsvoraussetzungen Rechnung und begegnet daher, insbesondere, soweit sie bei nur drohenden Gefahren zulässig ist, unter Verhältnismäßigkeitsgesichtspunkten verfassungsrechtlichen Bedenken. Anders als für die längerfristige Observation und die akustische Überwachung des gesprochenen Worts außerhalb von Wohnraum (vgl. Abs. 4 S. 1) wird hier auch keine verfahrensrechtliche Absicherung in Form eines Richtervorbehalts geschaffen, sondern lediglich ein Behördenleitervorbehalt mit weiterer Delegationsmöglichkeit (Abs. 5 S. 1 Nr. 1 i. V. m. Abs. 4 S. 2 und 3).

c) Zu Abs. 1 Nr. 2 lit. b) (längerfristiger Einsatz von technischen Observationsmitteln):

42

Ähnliches gilt für die Befugnis unter Abs. 1 Nr. 2 lit. b), soweit diese auch eine Ermächtigung zum Erstellen von Bewegungsbildern enthält. Das BVerfG hat insoweit in seinem Urteil zum BKAG ausgeführt, nicht zu beanstanden sei, *„dass für die Anfertigung von Bildaufnahmen sowie für nur kurzfristige Observationen - auch mittels Bildaufzeichnungen oder technischer Mittel wie Peilsender - ein Richtervorbehalt nicht vorgesehen ist. Bleiben die Überwachungsmaßnahmen in dieser Weise begrenzt, haben sie kein so großes Eingriffsgewicht, dass deren Anordnung durch einen Richter verfassungsrechtlich geboten ist (...). Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich aber unverzichtbar, wenn Observationen im Sinne des § 20g Abs. 2 Nr. 1 BKAG längerfristig - zumal unter Anfertigung von Bildaufzeichnungen oder unter Nutzung besonderer technischer Mittel wie Peilsender - durchgeführt werden, wenn nichtöffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden. Diese Maßnahmen dringen unter Umständen so tief in die Privatsphäre ein, dass deren Anordnung einer unabhängigen Instanz, etwa einem Gericht, vorbehalten bleiben muss.“*[109] Danach ist für den längerfristigen Einsatz von technischen Observationsmitteln und erst recht dann, wenn

tizierten persönlichen Übergaben.“ Das gilt auch für bestimmte Bereiche nicht-terroristischer Kriminalität, etwa den Handel mit Betäubungsmitteln.

[109] BVerfGE 141, 220, 294.

damit die Erstellung von Bewegungsbildern verbunden ist, eine richterliche Anordnung erforderlich, zumal die Einsatzmöglichkeiten nach PAG-E ungleich weiter sind als nach dem BKAG.

d) Zu Abs. 1 Nr. 2 lit. c) („kleiner Lauschangriff"):

43

In seiner Eingriffsintensität ist das heimliche Mithören und Aufzeichnen des gesprochenen Worts außerhalb von Wohnraum grundsätzlich dem Gewicht einer Telekommunikationsüberwachung vergleichbar (vgl. auch § 100f StPO).[110] Andererseits ist zu berücksichtigen, dass das Recht am gesprochenen Wort einen stärkeren persönlichkeitsrelevanten Gehalt hat, der in unterschiedlichen Überwachungssituationen stark variieren kann. Bei Art. 10 GG steht hingegen unabhängig von der Gesprächssituation und den Gesprächsinhalten der Schutz der technisch bedingten Einbuße an Privatheit im Vordergrund des Normzwecks.[111] Vor dem Hintergrund des im Einzelfall durch die Überwachung außerhalb von Wohnraum vermittelten beachtlichen Grundrechtseingriffs erscheint das Fehlen qualifizierter Anordnungsvoraussetzungen auch hier, insbesondere soweit die Maßnahme schon bei nur drohender Gefahr, also im Gefahrenvorfeld, angeordnet werden kann, verfassungsrechtlich bedenklich. Zu begrüßen ist allerdings, dass in Art. 36 Abs. 4 S. 1 PAG-E nunmehr die notwendige Anordnung durch einen Richter vorgesehen ist.

e) Zu Abs. 2 Nr. 2 (Maßnahmen gegen Kontakt- und Begleitpersonen):

44

Anders als bei Art. 35 Abs. 1 S. 1 Nr. 2 PAG-E (vgl. oben Rn. 37) genügt die Erstreckung besonderer Maßnahmen der Datenerhebung auf „mutmaßlich in Zusammenhang mit der Gefahrenlage stehende Kontakt- und Begleitpersonen" nicht den verfassungsrechtlichen Anforderungen an die heimliche Überwachung dritter Personen. Bestimmte Tatsachen, die auf eine „spezifische individuelle Nähe der Betroffenen zu der aufzuklärenden Gefahr" deuten, sind hier nicht vorausgesetzt. Auch die bereits konkretisierte Annahme eines Kontakts in Gestalt der Eigenschaft, Nachrichtenmittler zu sein, spielt hier keine Rolle. Gesetzliche Voraussetzung ist allein die auf die Erkenntnis, dass es sich um eine Kontakt- oder Begleitperson handelt, gestützte Vermutung, die Person stehe in einem Zusammenhang mit der Gefahrenlage. Anders als in § 16a Abs. 1 S. 3 und 4 PolG NRW enthält der PAG-E auch keine konkretisierenden Kriterien zur Bestimmung von Kontakt- und Begleitpersonen. Damit können beliebige Personen, mit denen die Zielperson in Kontakt tritt, überwacht werden. In seinem Urteil zum

[110] So BT-Drs. 12/989, S. 39; vgl. auch die Anlehnung der einschlägigen Regelung in § 100f StPO an die Vorschriften zur Telekommunikationsüberwachung.

[111] Vgl. BVerfGE 106, 28, 36; 107, 299, 313; BVerfGK 9, 62; BVerfG NJW 2007, 2752; 2007, 3343, 3344. Vor diesem Hintergrund erscheint fraglich, ob Art. 10 GG generell als lex specialis gegenüber dem Recht auf informationelle Selbstbe-

BKAG hat das BVerfG deutlich festgestellt: *„Eine Überwachung von Personen, die - allein gestützt auf die Tatsache eines Kontaktes zu einer Zielperson - erst versucht herauszufinden, ob sich hierüber weitere Ermittlungsansätze erschließen, ist verfassungsrechtlich unzulässig.“*[112] Hier handelt es sich auch nicht durchgehend um Überwachungsmaßnahmen, die eine geringere als die dort maßgebliche Eingriffstiefe aufweisen, so dass geringere Anforderungen an die Überwachung dritter Personen gestellt werden könnten.[113] Namentlich trifft dies nicht auf die akustische Überwachung des gesprochenen Worts außerhalb von Wohnraum und auf die Erstellung von Bewegungsbildern zu.[114]

f) Zu Abs. 2 Nr. 3 (Maßnahmen gegen nicht verantwortliche Personen):

45

Auch die Anforderungen an den Einsatz besonderer Mittel der Datenerhebung gegen nicht verantwortliche Personen werden gegenüber dem geltenden Recht beträchtlich abgesenkt, indem auf die Einschränkung, dass *„dies erforderlich ist zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder für Sachen, deren Erhaltung im öffentlichen Interesse geboten erscheint“* verzichtet wird. Die besonderen Mittel der Datenerhebung stellen damit im Hinblick auf nicht verantwortliche Personen eine Standardbefugnis dar, die nicht mehr als verhältnismäßig angesehen werden kann. Soweit die Entwurfsbegründung (S. 95) unter Verweis auf das Urteil des BVerfG zum BKAG davon ausgeht, die Überwachung von Nichtstörern unter den Voraussetzungen des Art. 10 PAG sei verfassungsrechtlich nicht zu beanstanden, verwundert dies. Das BVerfG würdigt die Möglichkeit der Inanspruchnahme nicht verantwortlicher Personen unzweideutig und differenzierend im Kontext der Aufgabe des BKA zur Terrorabwehr und kommt zu dem Schluss: *„Erforderlich ist das Vorliegen einer gegenwärtigen Gefahr für die in § 20g Abs. 1 Satz 1 BKAG genannten Rechtsgüter, für deren Abwehr die Maßnahme unmittelbar zielführend sein muss. Unter diesen Maßgaben ist eine Inanspruchnahme des Nichtstörers nicht unverhältnismäßig.“*[115] Weder entspricht der Katalog der Rechtsgüter des § 20g Abs. 1 BKAG dem des Art. 36 Abs. 2 PAG-E, noch stehen die dortigen Maßnahmen - entgegen der Entwurfsbegründung, die von „ultima ratio“ spricht (S. 95) - unter einem strengen Subsidiaritätsvorbehalt („auf andere Weise aussichtslos“).

---

stimmung angesehen werden kann, da es der verschiedenen Persönlichkeitsrelevanz von Gesprächsinhalten nicht ausreichend Rechnung trägt.

[112] BVerfGE 141, 220, 274 f.

[113] Vgl. a. a. O. a. E.: „Dies hindert hinsichtlich solcher Kontaktpersonen allerdings von Verfassungs wegen nicht Ermittlungsmaßnahmen geringerer Eingriffstiefe mit dem Ziel, gegebenenfalls die Eingriffsschwelle für intensivere Überwachungsmaßnahmen zu erreichen.“

[114] BVerfGE 141, 220, 287.

g) Zu Abs. 3 S. 2 (Erstellung von Bewegungsbildern in Wohnungen):

46

Unzureichend ist auch der in Abs. 3 S. 2 neu in Bezug genommene Schutzmechanismus des Art. 34 Abs. 2 S. 2 und 3 PAG-E bei der Erstellung von Bewegungsbildern, soweit Daten aus Wohnungen betroffen sind. Auf die entsprechende Kritik im Verfahren zu dem Gesetz vom 24.07.2017 wird Bezug genommen.[116]

20. Zu Art. 37 und 38 PAG-E (Einsatz Verdeckter Ermittler und von Vertrauenspersonen):

47

Die ausdrückliche und separate Regelung des Einsatzes Verdeckter Ermittler und von Vertrauenspersonen in Art. 37 und 38 PAG-E ist zu begrüßen. Sie folgt einer breiteren Tendenz in der Sicherheitsgesetzgebung auf Bundes- und Landesebene, dieses, für die Aufklärung konspirativer Strukturen wichtige Mittel normenklar zu regeln und dabei insbesondere die Handlungsspielräume klar zu begrenzen sowie unzuverlässige Personen von einer Verwendung als V-Person auszuschließen.[117] Die Eingriffsschwelle in Art. 37 Abs. 1 PAG-E und Art. 38 Abs. 1 PAG-E ist nur insoweit zu beanstanden, als der Einsatz auch bei lediglich drohender Gefahr zulässig ist. Auf die Ausführungen unter Rn. 3 f. und Rn. 41 - 43 wird Bezug genommen. Entsprechend gilt auch hier die Kritik am zulässigen Kreis der Zielpersonen (vgl. oben Rn. 44 f.). Daran anschließend stellt sich freilich die Frage, ob der Einsatz von Verdeckten Ermittlern und Vertrauenspersonen ein geeignetes und erforderliches Instrument auch im Bereich der Gefahrenabwehr darstellt. Dieses Mittel findet seinen primären Anwendungsbereich in der präventiven Ausleuchtung staatsgefährdender und krimineller konspirativer Strukturen, also im Bereich der nachrichtendienstlichen Aufklärung und der Organisationsdelikte, dort namentlich zur Gewinnung weiterer Ermittlungsansätze.[118] Die Beweisrelevanz der durch den Einsatz von Verdeckten Ermittlern und Vertrauenspersonen für die Verfolgung von Straftaten gewonnenen Erkenntnisse ist demgegenüber erfahrungsgemäß sehr gering, gerade auch aufgrund der begrenzten gerichtlichen Durchsetzbarkeit der Offenlegung der Einsatzmodalitäten und des dadurch stark verminderten Beweiswerts der erlangten Erkenntnisse. Ähnlich dürfte für den Bereich der Gefahrenabwehr zutreffen, dass die Geheimhaltung der Identität von Verdeckten Ermittlern und Vertrauenspersonen nur in eng begrenzten Ausnahmefällen riskiert wird, um eine Gefahr abzuwehren. Vor diesem Hintergrund wäre

---

[115] BVerfGE 141, 220, 289.
[116] Vgl. *Löffelmann* (Fn. 43) unter II. 3. a).
[117] Vgl. §§ 9a und 9b BVerfSchG, eingeführt durch das Änderungsgesetz vom 17.11.2015, BGBl. I, 1938; Art. 18, 19 BayVSG, eingeführt durch das Änderungsgesetz vom 12.07.2016, GVBl. 2016, 145; §§ 13, 14 Entwurf eines Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen, Hessischer Landtag Drucksache 19/5412.
[118] Ausf. zu Bedeutung und Notwendigkeit des Einsatzes geheimer Mitarbeiter im Bereich der Nachrichtendienste *Dietrich*, in: Dietrich/Eiffler, Teil VI § 2, insbes. Rn. 50 ff.

grundsätzlich zu erwägen, ob der Einsatz von Verdeckten Ermittlern und Vertrauenspersonen nicht konsequent auf den Einsatz zu Zwecken der nachrichtendienstlichen Aufklärung und der Verfolgung von Organisationsdelikten konzentriert werden sollte, auch um Kompetenzüberschneidungen nach Möglichkeit zu vermeiden. Um einen verbleibenden Bereich identifizieren zu können, in welchem der Einsatz geheimer Mitarbeiter zum Zweck der Gefahrenabwehr Sinn macht, wären rechtstatsächliche Erkenntnisse über die dort gesammelten Erfahrungen notwendig.[119]

48

Grundsätzlich sachgerecht und mit Blick auf die zunehmende Bedeutung von Aufklärungsmaßnahmen im Internet zu begrüßen ist die Erstreckung der Befugnisse nach Art. 37 Abs. 4 S. 1 und 3 PAG-E auf Internetermittler (Abs. 4 S. 4 Nr. 1).[120] Allerdings trägt sie nicht den insoweit in Betracht kommenden unterschiedlichen Eingriffsintensitäten verschiedener Arten von Internetrecherche Rechnung.[121] So bedarf zwar das Recherchieren in öffentlich zugänglichen Bereichen im Internet - auch wenn diese eine Registrierung als Nutzer erfordern[122] - nach allgemein konsentierter Auffassung keiner besonderen Ermächtigung[123], wohl aber, wenn die so gewonnenen Daten durch ihre systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhalten[124], wenn durch Sichtung allgemein zugänglicher Inhalte und unter Hinzuziehung weiterer Daten ein umfassendes Persönlichkeitsprofil des Betroffenen erstellt wird[125], wenn in zugangsgeschützte Kommunikationsbereiche im Internet ohne Einwilligung eines der Kommunikationsteilnehmer eingedrungen wird[126] sowie wenn ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausgenutzt wird, um persönliche Daten zu erheben, die die staatlichen Stellen ansonsten nicht erhalten würden [127]. Vor diesem Hintergrund ist zu befürchten, dass Art. 37 Abs. 4 S. 4 PAG-E in der Praxis als Ermächtigungsgrundlage für jedwede Art von Datenerhebung im Internet herangezogen wird.

49

Erwägenswert wäre es zudem, im Gesetztext klarzustellen, dass Verdeckte Ermittler keine Straftaten begehen dürfen und ggf. ihr Einsatz unverzüglich zu beenden ist. In § 9a Abs. 2 BVerfSchG und Art.

---

[119] Über den tatsächlichen Umfang und die Bedeutung des Einsatzes von Verdeckten Ermittlern und V-Personen im Bereich der Gefahrenabwehr liegen keine Erkenntnisse vor, vgl. die wenig aussagekräftige Antwort der Bayerischen Staatsregierung auf die schriftliche Anfrage des Abgeordneten *Schindler* unter Bayerischer Landtag Drucksache 17/18079.

[120] So bereits in Art. 18 Abs. 4 BayVSG, dazu *Löffelmann*, BayVBl. 2017, 253, 261.

[121] Dazu ausf. *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 5 Rn. 53 ff., auch zu weiteren landesrechtlichen Sonderregelungen.

[122] Meyer-Goßner/*Schmitt*, § 100a Rn. 7; *Kudlich*, GA 2011, 193, 198 f.

[123] Vgl. BVerfGE 120, 274, 340 ff., 344 ff.; *Zöller*, GA 2000, 563, 567, 569; *Böckenförde*, S. 196 f.; Meyer-Goßner/*Schmitt*, § 100a Rn. 7; *Kudlich*, StV 2012, 560, 566; *Bär*, ZIS 2011, 58; *Schulz*/*Hoffmann*, CR 2010, 131 , 136; *Soiné*, NStZ 2014, 248; ausf. *Biemann*, S. 65 ff.

[124] BVerfGE 120, 351, 361 f.; vgl. auch BVerfGE 115, 320 zur präventiv-polizeilichen Rasterfahndung; BVerwG NVwZ 2011, 161, 163; enger *Singelnstein*, NStZ 2012, 593, 600: Eingriff bereits bei gezielter Recherche zu einer bestimmten Person.

[125] BVerfGE 120, 274, 344 f.

[126] BVerfGE 120, 274, 341; vgl. auch *Zöller*, GA 2000, 563, 573; *Böckenförde*, S. 255; *Sankol*, JuS 2006, 698, 699; *Singelnstein*, NStZ 2012, 593, 600.

[127] BVerfGE 120, 274, 344 f.; dazu *Soiné*, NStZ 2014, 248, 249.

18 Abs. 2 BayVSG findet sich hierfür ein Regelungsvorbild. Der in diese Richtung zielenden Kritik des Bayerischen Landesbeauftragten für den Datenschutz wird beigetreten.[128]

Im Übrigen sind Art. 37 und 38 PAG-E - auch mit Blick auf die erweiterte Höchstdauer der Anordnung von sechs Monaten[129] - nicht zu beanstanden. Im Hinblick auf die Bedenken des Bayerischen Landesbeauftragten für den Datenschutz an der Ausgestaltung des Zuverlässigkeitsüberprüfungsverfahrens[130] erscheint fraglich, ob Vertrauenspersonen tatsächlich in einem Subordinationsverhältnis stehen, da sie - anders als Verdeckte Ermittler - nicht weisungsgebunden sind und keinem Dienstrecht unterstehen. Da die einfachgesetzliche Regelung des Einsatzes von Verdeckten Mitarbeitern und V-Leuten auf Bundesebene in dem dortigen Gesetzgebungsverfahren eingehend erörtert wurde[131], wird hier auf eine weitere vertiefte Auseinandersetzung der Problematik verzichtet.

21. Zu Art. 39 PAG-E (Automatisierte Kennzeichenerfassungsysteme):

50

Die beabsichtigte Regelung der automatisierten Kennzeichenerfassung in einer eigenständigen Norm ist unter systematischen Gesichtspunkten zu begrüßen. Soweit die Maßnahme durch Bezugnahme auf Art. 13 Abs. 1 Nr. 1 lit. b) PAG-E nunmehr auch bei lediglich drohenden Gefahren zulässig ist und soweit sie die Erstellung von Bewegungsbildern erlaubt, ist dies allerdings zu beanstanden.

In seiner Entscheidung zur automatisierten Erfassung von Kfz-Kennzeichen hat das BVerfG herausgearbeitet, dass dieser Maßnahme, soweit sie nicht ausschließlich auf die Identifizierung eines (z. B. gestohlenen) Fahrzeugs gerichtet ist, sondern genutzt werde, um die gewonnen Informationen für weitere Zwecke zu nutzen, etwa um Aufschluss über das Verhalten des Fahrers zu erhalten, eine beträchtliche Grundrechtsrelevanz zukomme. So ließen sich durch die Kennzeichenerfassung Informationen über das Bewegungsverhalten des Betroffenen sowie Zeitpunkte und Dauer seiner Aufenthalte an bestimmten Örtlichkeiten gewinnen, die Rückschlüsse auf sein Verhalten und seine Gewohnheiten zulassen. Bei einem längeren Einsatz könne die Kennzeichenerfassung als ein Mittel der Observation eingesetzt werden. Die *„besondere Schlagkraft und Eingriffsintensität eines derartigen Observationsmittels“* entstehe *„sowohl aus der Vervielfachung der Zahl möglicher Erfassungsvorgänge gegenüber den bisherigen technischen und personellen Möglichkeiten der Polizei als auch aus den durch die Automatisierung und Vernetzung ermöglichten verbesserten Bedingungen für eine effektive und zudem*

[128] (Fn. 60), S. 36.
[129] Zum Vergleich: § 110b StPO sieht eine Höchstfrist gar nicht vor; a. A. der Bayerische Landesbeauftragte für den Datenschutz, (Fn. 60), S. 35.
[130] (Fn. 60), S. 38.
[131] Vgl. insbes. die Stellungnahmen der Sachverständigen unter Deutscher Bundestag, Innenausschuss, Ausschussdrucksachen 18(4)328A (*Bäcker*), 18(4)328B (*Körting*), 18(4)328C (*Maaßen*), 18(4)328 D (*Roth*), 18(4)328E (*Wolff*), 18(4)328F

heimliche Datenerfassung und -verarbeitung.“[132] Vor diesem Hintergrund moniert das BVerfG u. a., dass die damals in Rede stehende Regelung des HessSOG die Maßnahme nicht auf die Abwehr einer konkreten Gefahr beschränke.[133]

51

Indem die Regelung des Art. 39 Abs. 1 PAG-E ausdrücklich an Art. 13 Abs. 1 PAG-E anknüpft, also an Maßnahmen der Identitätsfeststellung, zielt sie auf das Erlangen von Informationen, die über die Identifizierung des Fahrzeugs hinausgehen und unmittelbar den Fahrer betreffen. Erfasst werden neben dem Kennzeichen Ort, Datum, Uhrzeit und Fahrtrichtung. Sind Personen zur polizeilichen Beobachtung, gezielten Kontrolle oder verdeckten Registrierung ausgeschrieben [Abs. 1 S. 2 Nr. 2 lit. a)], dürfen die einzelnen Daten auch zu einem Bewegungsbild verbunden werden (Abs. 3 S. 3). Die Ausschreibung zur polizeilichen Beobachtung oder gezielten Kontrolle unterliegt dabei nach Art. 40 PAG-E selbst keinen sonderlich hohen Anforderungen und ist insbesondere nach dem dortigen Abs. 1 Nr. 2 auch bei lediglich drohender Gefahr für bedeutende Rechtsgüter und nach der dortigen Nr. 3 sogar im Falle von Kontaktpersonen zulässig. Damit ermöglicht Art. 39 PAG-E im Gefahrenvorfeld die Erstellung von Bewegungsbildern mutmaßlicher Kontaktpersonen vermeintlicher „Gefährder“. Ihrer gesetzlichen Ausgestaltung nach eignet ihr daher eine sehr große Streubreite, von der maßgebliche Einschüchterungseffekte ausgehen können, und auch eine große Eingriffstiefe. Daran gemessen erscheinen die Anordnungsvoraussetzungen deutlich zu niedrig und jedenfalls im Falle lediglich drohender Gefahren nicht mehr verfassungsmäßig. Die - an Ausführungen des BVerfG anschließende[134] - Eingrenzung durch das „Vorliegen entsprechender Lageerkenntnisse“ (S. 1) begrenzt die Weite der Norm nicht hinreichend, denn dieser Formulierung fehlt jede Konkretisierung dahin, worauf sich solche Erkenntnisse beziehen müssen: Auch die Erkenntnis, dass sich eine mutmaßliche Kontaktperson eines vermeintlichen „Gefährders“ gegenwärtig auf deutschem Staatsgebiet aufhält, stellt in diesem allgemeinen Sinn eine „Lageerkenntnis“ dar. Soweit die Vorschrift die Erstellung von Bewegungsbildern erlaubt, ist aufgrund der Schwere des Grundrechtseingriffs außerdem eine verfahrensrechtliche Absicherung in Gestalt eines Richtervorbehalts und von Höchstfristen angezeigt (vgl. bereits oben Rn. 42).

(*Scharmer*) und 18(4)328G (*Aden*), sowie das Wortprotokoll der 48. Sitzung des Innenausschusses am 08.06.2015, Protokoll-Nr. 18/48 und die Bundestags-Plenarprotokolle 18/101, S. 9686D ff. und 18/116, S. 11283B ff.

[132] BVerfGE 120, 378, 406 f.

[133] BVerfGE 120, 378, 430.

[134] BVerfGE 120, 378, 431: „Die automatisierte Kennzeichenerfassung ist auch nicht auf Situationen begrenzt worden, in denen Umstände der konkreten Örtlichkeit – zum Beispiel das Fahren auf Straßen in Bereichen nahe der Bundesgrenze – oder **dokumentierte Lageerkenntnisse über Kriminalitätsschwerpunkte** einen Anknüpfungspunkt geben, der auf gesteigerte Risiken der Rechtsgutgefährdung oder -verletzung und zugleich auf eine hinreichende Wahrscheinlichkeit hinweist, dass diesen Risiken mit Hilfe der automatisierten Kennzeichenerfassung begegnet werden kann.“ (Hervorh. d. d. Verf.)

22. Zu Art. 40 PAG-E (Ausschreibung zur polizeilichen Beobachtung):

52

Die bestehende Regelung in Art. 36 Abs. 1 PAG lässt die Ausschreibung zur polizeilichen Beobachtung nur zu, wenn von der betroffenen Person künftig Straftaten von erheblicher Bedeutung zu erwarten sind und die Beobachtung zur vorbeugenden Abwehr dieser Straftaten erforderlich ist. Bei Straftaten von erheblicher Bedeutung handelt es sich um solche, die mindestens dem Bereich der mittleren Kriminalität zuzurechnen und geeignet sind, das Sicherheitsempfinden der Bevölkerung in erheblicher Weise zu beeinträchtigen.[135]

53

Art. 40 Abs. 1 PAG-E senkt die Anforderungen an eine Ausschreibung beträchtlich ab. Die Prognose einer künftigen Begehung von Straftaten ist danach nicht mehr erforderlich, es reicht vielmehr unter Nr. 1 die Prognose, dass von der betroffenen Person künftig eine - nicht zwingend strafbare - Gefahr für bedeutende Rechtsgüter ausgeht. Hierunter fallen z. B. auch selbstschädigende Handlungen oder fahrlässige Sachbeschädigungen, die erhebliche Eigentumspositionen oder Sachen betreffen, deren Erhalt im besonderen öffentlichen Interesse liegt (vgl. Art. 11 Abs. 3 S. 2 Nr. 4 und 5 PAG). Unter Nr. 2 kann eine Ausschreibung zudem erfolgen, wenn die betroffene Person für eine drohende Gefahr für bedeutende Rechtsgüter verantwortlich ist. Inwiefern sich Nr. 1 und 2 unterscheiden, ist schwer zu sagen, denn die im Gefahrenvorfeld angesiedelte Feststellung einer drohenden Gefahr setzt ihrerseits die Prognose einer künftigen Rechtsgutverletzung voraus (vgl. Art. 11 Abs. 3 S. 1 PAG). Nr. 3 erlaubt die Ausschreibung schließlich auch betreffend Kontaktpersonen von Zielpersonen i. S. d. Nr. 1 und 2, die mutmaßlich im Zusammenhang mit der Gefahrenlage stehen. Damit kann auf Grundlage einer bloßen Vermutung und einer im Gefahrenvorfeld erstellten und daher mit einem hohen Prognoserisiko behafteten Gefahrenprognose eine Ausschreibung zur polizeilichen Beobachtung erfolgen.

54

Da an diese Maßnahme - was namentlich im Fall der Ausschreibung zur gezielten Kontrolle intendiert ist - weitere konkrete und eingriffsintensive polizeiliche Maßnahmen anknüpfen können, wie etwa die Erstellung eines Bewegungsbilds mittels automatisierter Kennzeichenerfassung [Art. 39 Abs. 1 S. 2 Nr. 2 lit. a) PAG-E], andere Observationsmaßnahmen oder Durchsuchungsmaßnahmen, vermittelt sie schwere Eingriffe in Grundrechte. Entsprechend wäre es notwendig, die Maßnahme nach Anlass, Zweck und Dauer eng zu begrenzen, was in keiner der Alternativen von Abs. 1 ausreichend geschieht.

[135] Vgl. *BVerfGE* 103, 21, 33 f.; 107, 299, 321 f.; 110, 33, 65; BVerfG, NJW 2001, 2320, 2321; *BVerfG*, StV 2003, 1; vgl. auch *Rieß*, GA 2004, 623 m. w. N. sowie BT-Drucks. 13/10791, S. 5.

55

Die Ermächtigung zur Ausschreibung von Kontaktpersonen ist zudem nicht vereinbar mit den Vorgaben des BVerfG zur Überwachung dritter Personen (vgl. bereits oben Rn. 44)[136], da die Eigenschaft, „Kontaktperson" zu sein (anders, als die Eigenschaft, Nachrichten für die Zielperson zu überbringen oder entgegenzunehmen), zu unspezifisch ist, um eine ausreichende Begrenzung des Kreises betroffener Personen zu gewährleisten.[137] Soweit die Entwurfsbegründung (S. 103) in diesem Zusammenhang auf Ausführungen des BVerfG im Zusammenhang mit § 20b Abs. 2 Nr. 2 BKAG abstellt, ist darauf hinzuweisen, dass in der genannten Vorschrift der Begriff der „Kontakt- und Begleitperson" weitaus spezifischer gefasst ist und deshalb die darauf gründende Ermächtigung vom BVerfG als „verfassungsrechtlich tragfähig" angesehen wird.[138]

56

Abs. 2 S. 1 dehnt die polizeilichen Befugnisse noch weiter aus, indem er die Übermittlung von Erkenntnissen über mutmaßlich im Zusammenhang mit der Gefahrenlage stehende Begleitpersonen und Fahrzeugführer an die ausschreibende Polizeidienststelle erlaubt. Aufgrund reiner Mutmaßungen können damit personenbezogene Daten von Begleitpersonen mutmaßlich mit der Gefahrenlage im Zusammenhang stehender Kontaktpersonen vermeintlicher „Gefährder" übermittelt werden. Es ist unschwer zu sehen, dass eine derartige Kumulierung von Mutmaßungen und Prognosen über mehrere Ebenen keine geeignete Grundlage für die Rechtfertigung eines Eingriffs in Grundrechte darstellt.

Angesichts der Eingriffstiefe der Maßnahme wäre - wie auch in § 163e Abs. 4 S. 1 StPO - eine gerichtliche Anordnung zudem zwingend erforderlich.

23. Zu Art. 41 PAG-E (Einsatz technischer Mittel in Wohnungen):

a) Zur rechtstatsächlichen Relevanz:

57

Die rechtstatsächliche Relevanz des verdeckten Einsatzes technischer Mittel zur Wohnraumüberwachung im Bereich der Gefahrenabwehr ist marginal. In den gemäß Art. 13 Abs. 6 GG jährlich dem Bundestag zu erstattenden Berichten haben entsprechende durch das BKA durchgeführte Maßnahmen Einzelfallcharakter.[139] Dasselbe gilt für entsprechende Maßnahmen der Bayerischen Polizei nach Art. 34 PAG, wo im Nachgang zur Entscheidung des BVerfG zur akustischen Wohnraumüberwachung im Jahr 2004 eine deutlich abnehmende Tendenz zu erkennen ist. In den vergangenen 10 Jahren wurde in

[136] BVerfGE 141, 220, 274.
[137] Vgl. i. d. S. auch BVerfGE 113, 348, 380.
[138] BVerfGE 141, 220, 291 f.
[139] Vgl. bisher BT-Drs. 18/9660 (2015); 18/5900 (2014); 18/2495 (2013); 17/14835 (2012); 17/10601 (2011); 17/7008 (2010); 17/3038 (2009); 16/14116 (2008); 16/10300 (2007); 16/6336 (2006); 16/3068 (2005); 15/5971 (2004); 15/3699 (2003); 15/1504 (2002); 14/9860 (2001); 14/6778 (2000); 14/3998 (1999); 14/2452 (1998).

Bayern überhaupt nur eine einzige solche Maßnahme im Bereich der Gefahrenabwehr durchgeführt.[140] Vor diesem Hintergrund stellt sich nachdrücklich die Frage, ob auf dieses ressourcenaufwändige und in hohem Maße eingriffsintensive Instrument nicht verzichtet werden sollte, da ein substanzieller Anwendungsbedarf bislang offenbar nicht bestanden hat. Das dürfte nicht zuletzt damit zusammenhängen, dass die Schranke des Art. 13 Abs. 4 GG eine dringende Gefahr voraussetzt, die technische Überwachung von Wohnraum aber einen gewissen zeitlichen Vorlauf erfordert, der bei dringenden Gefahren naturgemäß nicht zur Verfügung steht. Schon von den verfassungsrechtlichen Vorgaben her ist daher nur ein äußerst begrenzter und eher theoretischer Anwendungsbereich der Wohnraumüberwachung zum Zwecke der Gefahrenabwehr eröffnet.

b) Zu Abs. 1 S. 1 (Anordnungsvoraussetzungen):

58

Durch die beabsichtigte Änderung soll der bisherige Anlassgefahrenkatalog (Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person) durch einen Verweis auf Art. 11 Abs. 3 S. 2 Nr. 1, 2 und 5 PAG ersetzt und die Anordnungsschwelle damit abgesenkt werden. Ob die neu hinzugenommenen Rechtsgüter Gesundheit und Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt, ohne weitere Konkretisierung diesen schweren Eingriff in Art. 13 GG legitimieren können, erscheint zweifelhaft. Gefährdungen der Gesundheit (z. B. durch den Konsum von Betäubungsmitteln) und von Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt (z. B. Kunstwerke), stellen nicht ohne weiteres Gefahren für die öffentliche Sicherheit i. S. d. Art. 13 Abs. 4 GG dar.[141] Ein rechtstatsächliches Bedürfnis für die Ausweitung ist außerdem nicht erkennbar.

c) Zu. Abs. 1 S. 2 (Schutz des Kernbereichs und von Berufsgeheimnisträgern):

59

Abgesehen davon, dass die verschachtelte Regelung kaum verständlich ist, genügt sie nicht den verfassungsrechtlichen Anforderungen an den Kernbereichsschutz bei der Wohnraumüberwachung. Dabei ist zu berücksichtigen, dass es sich bei der Wohnraumüberwachung nach der Rechtsprechung des BVerfG um eine im Hinblick auf den Kernbereich privater Lebensgestaltung typischerweise verletzungsgeneigte Maßnahme handelt. Das BVerfG fordert daher schon bei der nur akustischen Überwachung von Wohnraum (erst recht müsste dies also für die darüber hinausreichende optische Überwa-

[140] Vgl. Bayerischer Landtag, Drs. 14/12498, S. 7 (3 Maßnahmen); 14/9754, S. 1 (keine Maßnahmen); 15/3945, S. 7 (4 Maßnahmen); 15/1443, S. 8 (4 Maßnahmen); 15/10675, S. 1 (keine Maßnahmen); 15/6226, S. 4 (2 Maßnahmen); 16/17319, S. 1 (keine Maßnahme); 16/12870, S. 1 (keine Maßnahme); 16/8368, S. 1 (keine Maßnahme); 16/4833, S. 6 (1 Maßnahme); 16/1388, S. 1 (keine Maßnahme); 17/18179, S. 1 (keine Maßnahme); 17/12096, S. 1 (keine Maßnahme); 17/7152, S. 1 (keine Maßnahme); 17/2180, S. 1 (keine Maßnahme).

chung gelten) ein strenges präventiv wirkendes Schutzkonzept in Gestalt einer negativen Kernbereichsprognose.[142] Dem wird Abs. 2 S. 2 nicht gerecht, der nur unter den in Nr. 1 genannten Voraussetzungen eine - wiederum mit Ausnahmen versehene - Einschränkung vorsieht. Die dortige Regelung stellt das vom BVerfG geforderte Schutzkonzept, demzufolge präventive Anstrengungen unternommen werden müssen, damit ein Eingriff in den Kernbereich von vornherein unterbleibt, auf den Kopf. Nach Abs. 2 S. 2 wären z. B. kernbereichsschützende Maßnahmen in Geschäftsräumen generell entbehrlich, wohingegen diese nach Maßgabe des BVerfG nur eine Vermutung begründen, dass es zu kernbereichsrelevanten Gesprächen in der Regel nicht kommt.[143] Auch sofern sich die betroffene Person in einer Wohnung mit anderen als den unter Nr. 1 genannten Personen aufhält, würde der Schutzmechanismus des Abs. 2 S. 2 nicht greifen. Liegen die Voraussetzungen nach Nr. 1 vor, handelt es sich also um eine prima facie kernbereichsrelevante Überwachungssituation, soll für die Zulässigkeit ausreichen, dass (überhaupt) Gespräche geführt werden, die einen unmittelbaren Bezug zu den in S. 1 genannten Gefahren haben. Hier wird das weniger strenge und faktisch wirkungslose - gleichwohl dort vom BVerfG wegen der Wirksamkeit von Schutzvorkehrungen auf der Verwertungsebene akzeptierte[144] - Schutzmodell aus dem Bereich der Telekommunikationsüberwachung auf die Wohnraumüberwachung übertragen. Tatsächliche Anhaltspunkte dafür, dass überhaupt solche Gespräche geführt werden, sind aber bereits Voraussetzung, um die Maßnahme als geeignet zu qualifizieren. Dieses Defizit im Bereich des präventiven Rechtsschutzes wird auch nicht durch die Regelung des Art. 49 PAG-E kompensiert, die den bereits laufenden Überwachungsvorgang betrifft. Auch um im Falle einer Gemengelage einen Gleichlauf mit den entsprechenden - verfassungsmäßigen[145] - strafprozessualen Regelungen zu gewährleisten, ist eine Anlehnung des Kernbereichsschutzes an § 100c Abs. 4 StPO dringen anzuraten.

60

Soweit Abs. 2 S. 2 darüber hinaus auf §§ 53, 53a StPO Bezug nimmt, ist in diesem Zusammenhang ferner darauf hinzuweisen, dass dadurch in unkritischer Weise Kautelen, die auf den Bereich des Strafverfahrensrechts zugeschnitten sind und dort entwickelt wurden, auf das Recht der Gefahrenabwehr übertragen werden.[146] Soweit der Schutz von Berufsgeheimnisträgern an das strafprozessuale Zeugnisverweigerungsrecht der Mitglieder bestimmter Berufsgruppen (§ 53 StPO) anknüpft, gibt es hierfür im Recht der Gefahrenabwehr mangels Zeugnispflicht schon keinen Anwendungsbereich.

---

[141] Vgl. auch die prägnante und zutreffende Kritik des Bayerischen Landesbeauftragten für den Datenschutz, (Fn. 60), S. 41 f.
[142] Ausf. zur Dogmatik des Kernbereichsschutzes *Löffelmann*, in Dietrich/Eiffler, Teil VI § 3 Rn. 6 ff.; zur negativen Kernbereichsprognose *ders*., NJW 2005, 2033 und ZIS 2006, 87, 89 ff.
[143] BVerfGE 109, 279, 320 f.; vgl. auch BT-Drs. 15/5486, S. 17.
[144] BVerfGE 113, 348, 390; 129, 208, 245 ff.; BVerfG NJW 2016, 3508, 3511; zur Frage der Übertragbarkeit der in der Entscheidung zur Wohnraumüberwachung entwickelten Maßstäbe auf die Telekommunikationsüberwachung auch *Löffelmann*, ZStW 118 (2006), 358.
[145] BVerfGK 11, 164 = NJW 2007, 2753 m. zust. Anm. *Geis*, CR 2007, 501 und *Sankol*, MMR 2007, 574.
[146] Vgl. zu dieser generellen Kritik bereits mit Blick auf das Recht der Nachrichtendienste *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 4 Rn. 58, § 5 Rn. 39; *ders*., BayVBl 2017, 253, 255.

Sinnvoll könnte hier ein Anknüpfen an Zeugnisverweigerungsrechte nur für die Übermittlung erhobener Daten an Strafverfolgungsbehörden sein. Generell ist außerdem anerkannt, dass der Schutz von Berufsgeheimnisträgern schon im Strafverfahrensrecht einer schlüssigen dogmatischen Grundlage entbehrt und reformbedürftig ist.[147] An die Stelle der dort für die Güterabwägung u. a. maßgeblichen, das Strafverfahren tragenden Prinzipien der umfassenden Erforschung der materiellen Wahrheit[148] und der Funktionsfähigkeit der Strafrechtspflege[149] müsste im Polizeirecht das öffentliche Interesse an der Abwehr qualifizierter Gefahrenlagen treten. Dies macht ein dortiges eigenständiges Schutzkonzept erforderlich, bei dem etwa auch an den Gedanken des § 203 StGB angeknüpft werden könnte, dessen hoheitliche Durchbrechung selbst eine - dem Zweck der Gefahrenabwehr entgegengesetzte - Gefährdung der öffentlichen Sicherheit und Ordnung begründen würde. Ein polizeirechtsspezifisches Schutzkonzept für Berufsgeheimnisträger müsste folglich auf einer Abwägung der ihrem Schutz zugrundeliegenden öffentlichen Interessen mit denen der Gefahrenabwehr aufbauen.[150]

d) Zu Abs. 1 S. 3 (Art der technischen Überwachung):

61

Ausdrücklich zu begrüßen ist die einschränkende Klarstellung der zulässigen Arten der technischen Überwachung in Abs. 1 S. 3. Unter Bestimmtheitsgesichtspunkten ist Art. 34 PAG bislang dahin zu beanstanden, dass der Eingriff in Art. 13 GG durch jedwede technische Mittel erfolgen darf, ohne dass diese näher konkretisiert werden. Denkbar ist danach z. B. ein Abgreifen von Daten der Haustechnik (Heizungsverbrauch, Wasserzähler, Licht- und Rollladensteuerung, Alarmmelder, Fernsehempfang etc.) mittels durch die Polizei angebrachter technischer Einrichtungen, wodurch sich ein relativ detailliertes Bild der Lebensgewohnheiten der Bewohner gewinnen ließe. Darüber hinaus eröffnet das „Internet der Dinge“ faktisch ganz neue, in diese Richtung zielende Aufklärungsansätze durch die hoheitliche Befugnis zum Eindringen in die Integrität informationstechnischer Systeme. Diese neuartigen Überwachungstechniken schließt S. 3 nun aus, indem der Anwendungsbereich auf eine (nur) akustische und/oder optische Überwachung beschränkt wird. S. 4 trägt außerdem den Erwägungen des BVerfG in seiner Entscheidung zum BKAG zur erhöhten Eingriffsintensität der Wohnraumüberwachung bei kumuliert akustischer und optischer Überwachung Rechnung.[151]

---

[147] Vgl. grundlegend zu dieser Kritik mit einem alternativen differenzierenden Regelungsvorschlag *Löffelmann*, Schutz von Berufsgeheimnisträgern, in: *ders.*, Rechtspolitik 2013, S. 66 ff.; kritisch zur geltenden Rechtslage auch *Baum*/*Schantz*, ZRP 2008, 137, 139; prägnant *Gärditz*/*Stuckenberg*, in: Wolter/Schenke, S. 132: die grundrechtliche Fundierung des Schutzes sei „allenfalls fragmentarisch und konzeptionslos verwirklicht“.

[148] Näher *Löffelmann*, S. 99 ff.

[149] BVerfGE 33, 367, 383; 51, 324, 345; 77, 65, 75 f.; BVerfG NJW 1996, 771.

[150] Vgl. zu einem entsprechenden Regelungsvorschlag für den Bereich des Verfassungsschutzrechts der Änderungsantrag der Fraktion der SPD zum Gesetzgebungsverfahren zur Novellierung des BayVSG, Bayerischer Landtag, Drs. 17/11610 S. 2, 20 ff.

e) Zu Abs. 4 S. 3 (Betretungsrecht):

62

Dass das Betretungsrecht zur Vorbereitung einer Wohnraumüberwachung (erneut) ausdrücklich geregelt wird, ist aus Gründen der Normklarheit zu begrüßen. Als Annexkompetenz wurde es bislang ganz überwiegend als von der Ermächtigungsnorm umfasst angesehen.[152]

f) Zu Abs. 5 (unabhängige Stelle):

63

In Abs. 5 werden die Vorgaben des BVerfG im BKAG-Urteil zur notwendigen Kontrolle der Datenverwendung durch eine „unabhängige Stelle" sachgerecht umgesetzt.

24. Zu Art. 42 PAG-E (Eingriffe in den Telekommunikationsbereich):

a) Zu Abs. 1 S. 1 Nr. 1 (Anordnungsvoraussetzungen):

64

Die Voraussetzungen für die Anordnung einer Telekommunikationsüberwachung werden durch die beabsichtigte Änderung - entgegen der Entwurfsbegründung (S. 108) - beträchtlich abgesenkt. Bisher kam diese Maßnahme nur in Betracht *„zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht"*. Sowohl den Grad der Gefahr als auch die Auswahl der zu schützenden Rechtsgüter betreffend enthält S. 1 Nr. 1 Weiterungen. So soll die Telekommunikationsüberwachung künftig bereits ab der Schwelle einer konkreten Gefahr (Alt. 1) und sogar einer nur drohenden Gefahr (Alt. 2) zulässig sein. Hinsichtlich der zu schützenden Rechtsgüter wird auf den Katalog des Art. 11 Abs. 3 S. 2 Nr. 1, 2 und 5 PAG Bezug genommen. Die dort genannten Rechtsgüter Gesundheit und Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt sind in ihrem Gewicht nicht mit den bislang in Abs. 1 S. 1 Nr. 1 genannten Rechtsgütern Bestand oder die Sicherheit des Bundes oder eines Landes sowie Leib, Leben oder Freiheit einer Person vergleichbar. Auf die Ausführungen zu Rn. 58 wird Bezug genommen. Soweit Sachen betroffen sind, bindet die bisherige Regelung die Maßnahme an die qualifizierte Kategorie einer gemeinen Gefahr. Künftig soll die Telekommunikationsüberwachung hingegen bereits bei drohender Gefahr für Sachen zulässig sein, soweit deren Erhalt im besonderen öffentlichen Interesse liegt. Dieser Einschränkung kommt jedoch keine substanziell begrenzende Funktion zu, da sie in hohem Maße unbestimmt ist.

---

[151] Vgl. auch BVerfGE 141, 220, 297.

[152] Vgl. BT-Drs. 13/8651, S. 13; *Schwabenbauer*, in: BeckOK BayPAG, Art. 34 Rn. 49; Meyer-Goßner/*Schmitt*, § 100c Rn. 7; *Hauck*, in: Löwe-Rosenberg, § 100c Rn. 8 f., 97; BGHSt 46, 266, 273 f.

65

Unter Verhältnismäßigkeitsgesichtspunkten sind diese Weiterungen nicht akzeptabel. Bei der Überwachung der Telekommunikation handelt es sich um einen intensiven, schwer wiegenden Eingriff in Art. 10 GG.[153] Indem das Fernmeldegeheimnis die einzelnen Kommunikationsvorgänge grundsätzlich dem staatlichen Zugriff entzieht, will es zugleich die Bedingungen einer freien Telekommunikation aufrechterhalten.[154] Außerdem gewährleistet Art. 10 GG die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen, besitzt also einen starken Menschenwürdegehalt.[155] In seinen das Polizeirecht betreffenden Entscheidungen zur Telekommunikationsüberwachung nach dem AWG[156] und dem NdsSOG[157] forderte das BVerfG vor diesem Hintergrund, Anlass, Zweck und Grenzen eines präventiven Eingriffs in Art. 10 GG müssten in der Ermächtigung bereichsspezifisch, normenklar und so präzise festgelegt werden, *„dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist.“*[158] Im Gegensatz zum Bereich der Strafverfolgung, in welchem die Ermächtigung an *„einen in der Vergangenheit liegenden, zumindest teilweise abgeschlossenen Sachverhalt“* anknüpfe, trete für das Abhören im Vorfeld einer strafbaren Handlung als Anknüpfungskriterium *„ein zunächst meist nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten noch schwer fassbares Geschehen“*. Die führe *„zu dem erheblichen Risiko, dass die Überwachungsmaßnahme an ein Verhalten anknüpft, das sich im Nachhinein als strafrechtlich irrelevant erweist.“*[159] Dem müsse die Ermächtigungsnorm in geeigneter Weise entgegenwirken. Die Bestimmtheitsanforderungen müssten *„spezifisch an dieser Vorfeldsituation ausgerichtet werden.“*[160] Bei der erforderlichen Verhältnismäßigkeitsabwägung spielt ferner der vom BVerfG in ständiger Rechtsprechung betonte komplementäre Charakter von prognostischen Elementen und dem Gewicht zu erwartender Rechtsgutverletzungen eine Rolle: *„Je gewichtiger das durch die geplante Tat betroffene Rechtsgut ist und je weiter gehend es beeinträchtigt würde, desto geringer darf die Wahrscheinlichkeit sein, mit der auf eine geplante Straftat geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die dem Verdacht zu Grunde liegen.“*[161]

Diesen verfassungsrechtlichen Maßstäben wird Art. 42 PAG-E nicht gerecht, soweit er die Telekommunikationsüberwachung schon bei drohenden Gefahren erlaubt. Der Begriff der drohenden Gefahr ist zu unbestimmt, um zu gewährleisten, dass betroffene Personen grundsätzlich erkennen könnten, bei

[153] BVerfGE 110, 33, 53, 57; 113, 348, 365.
[154] BVerfGE 100, 313, 359, 381.
[155] BVerfGE 110, 33, 53; 113, 348, 391; 115, 166, 182; nicht aber BVerfGK 9, 62.
[156] BVerfGE 110, 33.
[157] BVerfGE 113, 348.
[158] BVerfGE 113, 348, 375 f.; BVerfGE 110, 33, 53.
[159] BVerfGE 110, 33, 57 ff.; ähnlich BVerfGE 113, 348, 377.
[160] BVerfGE 113, 348, 377.
[161] BVerfGE 110, 33, 60 m. d. H. auf BVerfGE 100, 313, 392.

welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist (vgl. näher Rn. 3 f.). Die im Gefahrenvorfeld bestehende Schwierigkeit der Abgrenzung eines harmlosen Verhaltens von dem, das in eine Gefahr mündet, wird in der Ermächtigung nicht durch einschränkend wirkende Tatbestandsmerkmale bewältigt. Auf eine - durch die Bezugnahme auf bestimmte Tatbestandsvoraussetzungen vermittelte - Konkretisierung des Anlasses der Überwachung anhand von ausgewählten Straftatbeständen wird in Art. 42 PAG-E ganz verzichtet. Das Bemühen, ein gefahrenabwehrspezifisches, am Rechtsgüterschutz orientiertes alternatives Regelungsmodell umzusetzen, verdient zwar grundsätzlich Zustimmung[162]; ein solches Modell müsste aber einen vergleichbaren Bestimmtheitsgrad aufweisen, was hier nicht der Fall ist. Letztlich obliegt die Bestimmung der Voraussetzungen und Grenzen des Eingriffs allein den ausführenden Behörden, die sich ihre Maßstäbe dafür, in welchen Grenzen in das Fernmeldegeheimnis eingegriffen werden darf, selbst zurechtlegen und insoweit tatbestandsergänzend tätig werden.

66

Hinzu kommt, dass es sich bei den in Abs. 1 S. 1 genannten Rechtsgütern des Art. 11 Abs. 3 S. 2 Nr. 1, 2 und 5 PAG nicht durchgehend um solche von so hohem Gewicht handelt, dass die Anforderungen an die Bestimmtheit abgesenkt werden könnten, zumal die Ermächtigungsnorm und auch Art. 11 Abs. 3 PAG keinerlei Aussage über den Grad ihrer zu erwartenden Verletzung treffen. Der bloße Umstand, dass ein hochrangiges Rechtsgut verletzt wird, bedeutet nicht, dass diese Verletzung ein Ausmaß erreicht, das geeignet ist, einen schweren Grundrechtseingriff zu rechtfertigen. Vor diesem Hintergrund ist die Ermächtigung in Art. 42 PAG-E - entgegen der Entwurfsbegründung (S. 108[163]) - ganz anders zu bewerten, als die vom BVerfG im BKAG-Urteil ausnahmsweise für zulässig erachteten informationellen Maßnahmen im Gefahrenvorfeld. Bei den dort in Rede stehenden terroristischen Taten handelt es sich per definitionem um schwerste Verletzungen höchstrangiger Rechtsgüter. Unter Verhältnismäßigkeitsgesichtspunkten begegnet daher auch die Absenkung der Eingriffsschwelle des Art. 42 Abs. 1 PAG-E soweit nunmehr konkrete Gefahren für die in Art. 11 Abs. 3 S. 2 Nr. 1, 2 und 5 PAG genannten Rechtsgüter ausreichend sind, verfassungsrechtlichen Bedenken.

b) Zu Abs. 1 S. 2 (Erstreckung auf räumlich getrennte Kommunikationssysteme):

67

Der Sinn der Änderung erschließt sich nicht. Nach der Entwurfsbegründung (S. 109) werde dadurch *„klargestellt bzw. berücksichtigt, dass die laufende Kommunikation auch unter Verwendung von Systemen, die von dem von Betroffenen physisch benutzen Kommunikationssystem entfernt sind (etwa*

[162] Vgl. dazu BVerfGE 125, 260, 329 f.

[163] Soweit die Begründung zur Rechtfertigung auf Rn. 232 des BKAG-Urteils verweist, ist darauf hinzuweisen, dass das BVerfG dort ausdrücklich - und im gerade entgegengesetzten Sinn - erklärt, die Erstreckung der Telekommunikations-

entsprechende Server bei IP-basierter Telekommunikation) erfolgt, auf die sich im Rahmen der Möglichkeiten dann im Einzelfall ebenfalls eine TKÜ-Maßnahme nach Satz 1 erstrecken darf." Die Durchführung der Maßnahme erfolgt in der Regel durch Ausleitung der Kommunikation bei den Telekommunikationsdiensteanbietern und ihrer Zurverfügungstellung an die Polizei über eine Schnittstelle. An welche Konstellationen die Entwurfsverfasser denken, in denen (durch die Polizei selbst?) auf räumlich getrennte Kommunikationssysteme zugegriffen werden soll, ist nicht durchschaubar. Um etwaigen, vom Gesetzgeber nicht gesehenen oder gewollten Einsatzmöglichkeiten der Maßnahme vorzubeugen, sollte die Änderung gestrichen werden.

c) Zu Abs. 4 (Überwachung zum Schutz der betroffenen Person):

68

Die Erstreckung der Maßnahme auf das Gefahrenvorfeld erscheint hier unbedenklich, da die Überwachung, welche eine schnelle wirkungsvolle Rettung hilfloser, verirrter oder vermisster Personen bezweckt[164], ausschließlich deren Schutz dient. Allerdings passt das dogmatische Konzept der drohenden Gefahr i. S. d. Art. 11 Abs. 3 PAG schlecht zu dem gegebenen Regelungszweck, da es schief ist, von dem Verhalten einer schutzbedürftigen Person als einem „Angriff von erheblicher Intensität und Auswirkung" zu sprechen. Der hier gegebene Regelungskontext veranschaulicht, dass die vom BVerfG für die Abwehr terroristischer Bedrohungen im Gefahrenvorfeld entwickelten Kriterien nicht verallgemeinert werden können.

69

Sehr problematisch erscheint hingegen die - laut Entwurfsbegründung lediglich „redaktionelle" (S. 110) - Änderung in Nr. 1. Hierdurch wird die Maßnahme dergestalt ausgeweitet, dass nicht nur die Erhebung personenbezogener Daten der schutzbedürftigen Person mittels Telekommunikationsüberwachung (also in der Regel die Überwachung der Telekommunikation *dieser* Person), sondern ohne jede Eingrenzung jedwede Telekommunikationsüberwachung zum Zweck des Schutzes dieser Person zulässig ist. Das ist unter Bestimmtheits- und Verhältnismäßigkeitsgesichtspunkten dezidiert abzulehnen.

überwachung auf Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie terroristische Straftaten vorbereiten, sei mit der Verfassung nicht zu vereinbaren.

d) Zu Abs. 5 (Unterbrechung von Kommunikationsverbindungen):

70

Nach der Entwurfsfassung erlaubt S. 1 nicht mehr lediglich die Unterbrechung oder Verhinderung von Kommunikationsverbindungen des Störers[165], sondern jeglicher Personen, wenn dies zur Abwehr einer Gefahr für ein Rechtsgut i. S. d. Art. 11 Abs. 3 S. 2 Nr. 1, 2 oder 5 PAG erforderlich ist. Es handelt sich daher - entgegen der Entwurfsbegründung (S. 110) - nicht um eine lediglich klarstellende Änderung.

Gegen die (sehr eingriffsintensive) Weiterung in S. 3 bestehen wegen der hohen Eingriffsschwelle (gegenwärtige Gefahr für Leib, Leben, Freiheit; strenge Subsidiarität) keine Bedenken.

Systematisch erwägenswert wäre schließlich eine Kodifizierung der Maßnahmen nach Abs. 5 in einer eigenständigen Norm samt Verfahrensregelungen (vgl. Art. 44 Abs. 2 PAG-E), da es sich hinsichtlich ihrer Zielrichtung um besondere, nicht der Überwachung dienende, Eingriffe handelt.

e) Zu Abs. 7 (Einbeziehung der unabhängigen Stelle):

71

Unter datenschutzrechtlichen Gesichtspunkten ist die Einbeziehung der unabhängigen Stelle in die Prüfung der erhobenen Daten im Falle einer automatischen Aufzeichnung grundsätzlich zu begrüßen. Da - anders als bei der Wohnraumüberwachung - im Falle der Telekommunikationsüberwachung die automatische Aufzeichnung aber die Regel ist, stellt sich die Frage, wie die unabhängige Stelle die bislang von der Polizei geleistete hoch personalaufwändige Sichtung und Auswertung der Aufzeichnungen leisten kann. Das BVerfG verlangt in seiner Entscheidung zum BKAG bei Telekommunikationsüberwachungen, da es sich nicht um sog. verletzungsgeneigte Maßnahmen handelt, gerade nicht die zwingende Befassung einer unabhängigen Stelle mit sämtlichem Datenmaterial.[166] Dies lässt Raum für eine vorgängige Sichtung durch die Polizeibehörden, die aus Praktikabilitätsgründen vorzugswürdig erscheint.

25. Zu Art. 43 PAG-E (Mitwirkungspflichten der Diensteanbieter):

a) Zu Abs. 1 (Mitwirkungspflichten):

72

Systematisch gehören die Mitwirkungspflichten nach Abs. 1 zur inhaltsbezogenen Telekommunikationsüberwachung und wären daher besser in Art. 42 PAG-E verortet. Art. 43 PAG-E könnte aussage-

[164] Vgl. *Schmidbauer*/Steiner, PAG, Art. 34a Rn. 97.
[165] Vgl. *Schmidbauer*/Steiner, PAG, Art. 34a Rn. 103.

kräftiger mit der Überschrift „Auskunftspflichten der Diensteanbieter“ versehen werden. Im Übrigen ist die Zusammenführung der diversen Auskunftsersuchen über Telekommunikationsverkehrsdaten, Telemedien-Nutzungsdaten und Bestandsdaten in einer Vorschrift zu begrüßen.

b) Zu Abs. 2 S. 1 (Auskunft über Telekommunikationsverkehrsdaten):

73

Durch die Verweisung auf Art. 42 Abs. 1 S. 1 PAG-E ist das Auskunftsersuchen nach dem Änderungsentwurf auch im Falle einer nur drohenden Gefahr für ein in Art. 11 Abs. 3 S. 2 Nr. 1, 2 oder 5 PAG genanntes Rechtsgut zulässig. Auf die unter Rn. 3 f. und Rn. 64 bis 66 dargestellte Kritik wird Bezug genommen. Da der Beauskunftung von Verkehrsdaten allerdings ein geringeres Gewicht als der inhaltsbezogenen Telekommunikationsüberwachung zukommt[167], wirken sich die Bestimmtheits- und Verhältnismäßigkeitsdefizite hier weniger schwer aus, weshalb die Weiterung verfassungsrechtlich noch akzeptabel sein dürfte.

74

Zutreffend ist andererseits die Feststellung des Bayerischen Landesbeauftragten für den Datenschutz[168], Art. 43 PAG-E enthalte (anders als seit geraumer Zeit § 100g StPO) keine Regelung der sog. Funkzellenabfrage. Mangels erforderlicher Rechtsgrundlage ist diese Maßnahme mithin auch nach dem PAG-E unzulässig. Dasselbe gilt für das sog. stealth ping-Verfahren („stille SMS“). Da es sich dabei um eine praktisch sehr wichtige Methode zur Standortbestimmung handelt, könnte über die Schaffung einer entsprechenden Rechtsgrundlage nachgedacht werden.[169]

c) Zu Abs. 2 S. 2 und Abs. 4 (Auskunft über Vorratsdaten und Nutzungsdaten):

75

Vor dem Hintergrund, dass die Neuregelung des § 113b TKG nach der jüngsten Rechtsprechung des EuGH als europarechtswidrig anzusehen ist[170] und einzelne Fachgerichte mittlerweile betroffene Telekommunikationsdiensteanbieter von einer Umsetzung der Speicherpflicht entbunden haben[171], sollte auf die Regelung (vorläufig) verzichtet werden, bis die „Vorratsdatenspeicherung“ einer europarechts-

---

[166] BVerfGE 141, 220, 279, 313.
[167] BVerfGE 107, 299, 318 ff.
[168] (Fn. 60), S. 43 ff. Zu der im Bericht zitierten Gesetzbegründung unter BR-Drs. 249/15, S. 32 f. ist freilich zu bemerken, dass das BVerfG bereits in seiner Entscheidung zu § 12 FAG (BVerfGE 107, 299, 328) festgestellt hat, die automatische Aussonderung einer Vielzahl von Verkehrsdaten, ohne dass sich daran weitere Eingriffe anschließen, entbehre bereits der Eingriffsqualität. Diese Rechtsprechung hat das BVerfG nachfolgend in einer Vielzahl anderer Entscheidungen aufrechterhalten (BVerfGE 115, 320, 343; 120, 378, 399; BVerfGK 9, 62; 15, 71; noch weiter geht BVerwG NJW 2015, 906, 908, wo - zutreffend - auch bei einem manuellen Aussondern eines „unechten“ Treffers die Eingriffsqualität verneint wird). Verfassungsrechtlich wäre eine „Nachjustierung“ der Vorschrift des § 100g Abs. 3 StPO daher nicht geboten.
[169] Dazu näher *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 5 Rn. 76, 78 f. m. w. N.
[170] EuGH NJW 2017, 717 (Tele2Sverige).
[171] OVG Münster GSZ 2017, 33 m. Anm. *Löffelmann*.

konformen Neuregelung zugeführt wurde. Für die erweiterte Abfragebefugnis betreffend Telemedien-Nutzungsdaten (Abs. 4) gilt das entsprechend.

d) Zu Abs. 5 S. 1 (Bestandsdatenabfrage):

76

Gegen die Erweiterung der Bestandsdatenabfrage auf drohende Gefahren bestehen – ungeachtet der auch hier angezeigten dogmatischen Kritik an diesem Konzept – wegen der geringen mit der Erhebung von Bestandsdaten verbundenen Eingriffstiefe, unter Verhältnismäßigkeitsaspekten keine Einwände.

e) Zu Abs. 8 (Richtervorbehalt):

77

Die Regelung ist verfassungsrechtlich nicht zu beanstanden. Erwägenswert wäre freilich unter Praktikabilitätsgesichtspunkten eine durchgängige Vereinheitlichung des Richtervorbehalts für *alle* Auskunftsersuchen, da so verschiedene Anordnungen mit unterschiedlicher Zielrichtung besser miteinander verbunden werden könnten.

26. Zu Art. 44 PAG-E (Besondere Verfahrensregeln für Maßnahmen nach Art. 42 und 43):

78

In Abs. 5 S. 3 sieht der Entwurf eine Kompetenz zur nicht offenen Durchsuchung von Sachen sowie zum verdeckten Betreten und Durchsuchen der Wohnung des Betroffenen vor, soweit dies zur Durchführung einer Telekommunikationsüberwachung nach Art. 42 PAG-E erforderlich ist. Diese, früher bereits in Art. 34e PAG a. F. enthaltene und wieder gestrichene Ermächtigung erscheint verfassungsrechtlich hoch problematisch. Wegen der Betroffenheit verschiedener Grundrechte (einerseits Art. 10 GG, andererseits Art. 13, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1, u. U. Art. 14 GG) dürfte - anders als beim Betretungsrecht zur Vorbereitung einer Wohnraumüberwachung (vgl. Rn. 62) - eine Ermächtigung im Wege der Annexkompetenz nicht in Betracht kommen, weshalb eine gesetzliche Regelung zu begrüßen ist. Für die Befugnis zur nicht offenen Durchsuchung von Sachen stellt die gesetzliche Regelung in Abs. 5 S. 3 i. V. m. Art. 42 PAG-E eine ausreichende Ermächtigungsgrundlage dar, da insoweit der Grundsatz der Verhältnismäßigkeit die einzige zu beachtende Schranke darstellt. Anderes gilt für das Recht zum heimlichen Betreten und Durchsuchen der Wohnung des Betroffenen. Art. 13 GG sieht hierfür keine verfassungsrechtliche Schranke vor, denn Art. 13 Abs. 2 GG bezieht sich ausschließlich auf offene Maßnahmen der Durchsuchung und Art. 13 Abs. 3, 4 und 5 GG auf den Einsatz technischer Mittel zur Überwachung der Wohnung. Art. 13 Abs. 7 GG stellt zwar einen Auffangtatbe-

stand dar, setzt aber voraus, dass der Eingriff in das Wohnungsrecht „zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung“ erfolgt. Diese Voraussetzung deckt sich nicht mit denen des Abs. 5 S. 3 i. V. m. Art. 42 Abs. 1 PAG-E. Soweit das Recht, Wohnungen zu betreten und zu durchsuchen betroffen ist, dürfte Art. 44 Abs. 5 S. 3 PAG-E daher verfassungswidrig sein.

27. Zu Art. 45 PAG-E (Online-Durchsuchung):

a) Zu Abs. 1 S. 1 Nr. 1 (Anordnungsvoraussetzungen):

79

Nach Abs. 1 S. 1 Nr. 1 soll die Online-Durchsuchung künftig auch zulässig sein zur Abwehr drohender Gefahren für die in Art. 11 Abs. 3 S. 2 Nr. 1 und 2 PAG bezeichneten Rechtsgüter (Bestand oder Sicherheit des Bundes oder eines Landes; Leben, Gesundheit, Freiheit). Damit werden die Anordnungsvoraussetzungen sowohl hinsichtlich des erforderlichen Gefahrgrads (bislang: dringende Gefahr) als auch der geschützten Rechtsgüter (bislang: Bestand oder Sicherheit des Bundes oder eines Landes; Leib, Leben, Freiheit einer Person) abgesenkt. Darüber hinaus stellt auch die Zulässigkeit bei konkreter Gefahr eine Absenkung dar, wie sich aus Abs. 1 S. 6, wo der Begriff der dringenden Gefahr im Sinne einer erhöhten Schwelle verwendet wird, erschließt.

80

Vor dem Hintergrund, dass es sich bei der Online-Durchsuchung um den schwersten informationstechnischen Eingriff handelt, den das Sicherheitsrecht erlaubt, und sich bereits die bisherige Regelung an der Grenze des verfassungsrechtlich Zulässigen bewegte, erscheint die Weiterung nicht verfassungskonform. Hinsichtlich des Kriteriums der Rechtsgüter ist nach den Vorgaben des BVerfG die Online-Durchsuchung nur zulässig zum Schutz von „überragend wichtigen Rechtsgütern“, zu denen grundsätzlich Leib, Leben und Freiheit der Person zählen, außerdem solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, wie z. B. die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.[172] Es muss sich allgemein für den Einzelnen oder die Gemeinschaft um eine existenzielle Bedrohungslage handeln.[173] Darüber geht Art. 45 Abs. 1 S. 1 Nr. 1 PAG-E jedenfalls insoweit hinaus, als er die Gesundheit der Person einbezieht. Darüber hinaus bedürfen auch die anderen genannten Rechtsgüter der verfassungskonformen Auslegung dahin, dass nicht jedwede Gefährdung, sondern nur solche, die ein existenzielles Ausmaß erreichen, eine Online-Durchsuchung legitimieren können. Das sollte auch im Gesetztext zum Ausdruck kommen. Hinsichtlich des erforderlichen

[172] BVerfGE 120, 274, 328.
[173] BVerfGE 120, 274, 328.

Gefahrengrads verlangt das BVerfG (nur[174]) das Vorliegen einer „konkreten Gefahr“[175] und versteht darunter *„eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird.“*[176] Sofern es sich um eine Gefahr für ein überragend wichtiges Rechtsgut handelt, sei es hingegen nicht erforderlich, dass sich mit hinreichender Wahrscheinlichkeit feststellen lässt, die Gefahr werde schon in näherer Zukunft eintreten. In diesem Fall müssen die Tatsachen den Schluss auf ein *„wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen“*, sowie darauf, *„dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. (…) Ausreichend ist insoweit auch, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten eines Betroffenen eine konkrete Wahrscheinlichkeit begründet, dass er solche Straftaten in überschaubarer Zukunft begehen wird.“*[177] Diese Formulierung hat der Bayerische Gesetzgeber in weiten Teilen in seine Legaldefinition der drohenden Gefahr in Art. 11 Abs. 3 PAG übernommen und folgert daraus, dass die Online-Durchsuchung generell schon bei Vorliegen einer drohenden Gefahr zulässig sei (Entwurfsbegründung S. 115). Dabei wird einerseits übersehen, dass die Ausführungen des BVerfG im Kontext der Terrorismusbekämpfung stehen, wo erfahrungsgemäß von einem hohen Grad an Konspiration ausgegangen werden muss, der eine Vorverlagerung des polizeilichen Tätigwerdens ins Gefahrenvorfeld zusätzlich legitimiert. Und andererseits bleibt unberücksichtigt, dass die entsprechenden Ausführungen des BVerfG einen Regelungsauftrag an den Gesetzgeber enthalten, die genannten Begrenzungen in bereichsspezifischer und normenklarer Weise in so konkrete Anordnungsvoraussetzungen umzugestalten, dass eine verlässliche Rechtsanwendung gewährleistet ist. Diese erforderliche Bestimmtheit weist Art. 11 Abs. 3 PAG aber nicht auf (näher oben Rn. 3 f.), was wegen der hier gegebenen hohen Eingriffsintensität verstärkt zum Tragen kommt.

81

Bei alldem ist durchaus anzuerkennen, dass die Online-Durchsuchung gerade im Gefahrenvorfeld - namentlich also für die Nachrichtendienste von Bund und Ländern - ein effizientes, effektives und zielgerichtetes Mittel darstellen kann, um Bedrohungslagen, die von einem hohen Maß an Konspiration geprägt sind, frühzeitig zu erkennen. Nach den Vorgaben des BVerfG in der Entscheidung zum BKAG setzt dies aber entsprechend hochrangige zu schützende Rechtsgüter voraus sowie eine präzise und normenklare Begrenzung des Anlasses der Maßnahme. Beiden Kriterien genügt das Regelungsmodell im PAG-E, wie dargestellt, nicht.

[174] Vgl. BVerfGE 141, 220, 296.
[175] BVerfGE 141, 220, 304 f.
[176] BVerfGE 120, 274, 328 f.; 141, 220, 305.
[177] A. a. O.

b) Zu Abs. 1 S. 1 Nr. 2 (weitere Zielpersonen):

82

Die Streichung der Nachrichtenmittler aus Nr. 2 ist nicht nur nach Maßgabe der Entscheidung des BVerfG zum BKAG geboten[178], sondern auch sachgerecht, da deren Einbeziehung in den Anwendungsbereich nur im Rahmen der Überwachung laufender Kommunikation (also bei der Quellen-Telekommunikationsüberwachung) Sinn macht. Der Halbsatz „und die Personen daher mutmaßlich in Zusammenhang mit der Gefahrenlage stehen" dürfte entbehrlich sein. Die auf bestimmten Tatsachen gründende Annahme, dass die verantwortliche Person informationstechnische Systeme der Zielperson nutzt stellt eine ausreichend spezifische individuelle Nähe der Zielperson zu der abzuwehrenden Gefahr i. S. d. Rechtsprechung des BVerfG dar.[179]

c) Zu Abs. 1 S. 2 (Erstreckung auf räumlich getrennte Systeme):

83

Die Regelung zur Erstreckung der Online-Durchsuchung auf verbundene aber räumlich getrennte Systeme (z. B. Cloud-Speicher) ist verfassungsmäßig[180], sachgerecht und zu begrüßen. Sie setzt aber voraus, dass die Eingriffsermächtigung im Ausgang ausreichend eng gefasst ist. Die zur Erstreckung der offenen „Durchsuchung" von Speichermedien auf räumlich getrennte Systeme angebrachten Einwände (vgl. oben Rn. 14 ff.) greifen hier nicht, da der Umstand, dass ein schwer wiegender Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gegeben ist, bereits bei der Gestaltung der Anordnungsvoraussetzungen zu berücksichtigen ist.

d) Zu Abs. 1 S. 6 (Löschung und Manipulation von Daten):

84

Erheblichen verfassungsrechtlichen Bedenken begegnet hingegen die Befugnis zum Löschen und Verändern von Daten des infiltrierten Systems bei einer dringenden Gefahr für ein in S. 1 bezeichnetes Rechtsgut. Die Maßnahme erhält durch diese Befugnis zur Datenvernichtung und Datenmanipulation nochmals ein beträchtlich erhöhtes Gewicht. Da das BVerfG die Online-Durchsuchung überhaupt nur unter der Voraussetzung als verfassungsgemäß angesehen hat, dass mittels technischer Vorkehrungen sichergestellt wird, die Verletzung der Integrität des betroffenen Systems werde so gering wie möglich gehalten[181], stellt eine - nicht nur unvermeidbare, durch die Durchsuchung technisch bedingte, sondern

[178] BVerfGE 141, 220, 273 f.
[179] BVerfGE 141, 220, 274 f.
[180] BVerfGE 141, 220, 303.
[181] BVerfGE 120, 274, 331 ff.; 141, 220, 305 f.

gezielt beabsichtigte - Integritätsverletzung eine gänzlich andere Eingriffsqualität dar. Schon im geltenden Recht ist zweifelhaft, ob die Befugnis zu Datenlöschungen in Art. 34d Abs. 1 S. 3 PAG unter der Voraussetzung, dass eine gegenwärtige Gefahr für Leib oder Leben nicht anders abgewehrt werden kann, den verfassungsrechtlichen Anforderungen genügt. Die neue Befugnis in Abs. 1 S. 6 geht darüber noch hinaus, indem sie einerseits nicht nur Datenlöschungen, sondern (erneut[182]) auch Datenmanipulationen erlaubt und andererseits die Eingriffsschwelle von einer gegenwärtigen auf eine dringende Gefahr herabstuft. Andererseits sind durchaus Konstellationen denkbar, in denen eine derartige Manipulation die einzige wirksame Art darstellt, eine Gefahr zu beseitigen, weshalb die vorgeschlagene Weiterung insoweit nicht von vornherein abgelehnt werden sollte. Eine solche Maßnahme darf aber nur unter engsten Voraussetzungen und im absoluten Ausnahmefall zulässig sein. Denkbar wären in einem derartigen Fall auch zusätzliche prozessuale Absicherungen, z. B. die Anordnung nicht „nur" durch einen Richter, sondern durch ein Kollegialorgan (vgl. etwa Art. 13 Abs. 3 S. 3 GG).

e) Zu Abs. 3 S. 5 (Durchsuchungs- und Betretungsrecht):

85

Im Hinblick auf die unter Abs. 3 S. 5 neu beabsichtigte Befugnis, zur Durchführung der Online-Durchsuchung Sachen der betroffenen Person zu durchsuchen sowie ihre Wohnung zu betreten und zu durchsuchen, stellt sich dieselbe Problematik wie bei der Telekommunikationsüberwachung (oben Rn. 78).[183] Eine Annexkompetenz zum Betreten der Wohnung ist nach geltendem Recht abzulehnen.[184] Würde die Online-Durchsuchung verfassungskonform ausgestaltet und streng auf die Abwehr dringender Gefahren für höchstrangige Rechtsgüter beschränkt, könnte eine Befugnis zum Eingriff in das Wohnungsgrundrecht allerdings auf Art. 13 Abs. 7 GG gestützt werden.

f) Zu Abs. 3 S. 6 (Verlängerungsanordnung):

86

Ein durchgreifender sachlicher Grund für die Erweiterung der Verlängerungsmöglichkeit von einem auf drei Monate ist nicht erkennbar. Aufgrund der hohen Eingriffsintensität sollte eine Überprüfung in möglichst kurzen Abständen erfolgen.

[182] Vgl. Art. 34d Abs. 1 S. 2 PAG a. F., der mit Gesetz vom 27.07.2009 aufgehoben wurde.
[183] Vgl. auch *Löffelmann*, in: Dietrich/Eiffler, Teil VI § 5 Rn. 41 zur Regelung im BayVSG, wo ein Betretungsrecht derzeit nicht geregelt ist. Die ursprünglich in Art. 6g S. 1 BayVSG a. F. als vorbereitende Maßnahme vorgesehene Betretens- und Durchsuchungsbefugnis für Wohnungen, in denen sich informationstechnische Systeme befinden, wurde mit Wirkung vom 1.9.2009 wieder aufgehoben.
[184] So zutr. *Petri*, in: BeckOK BayPAG, Art. 34d Rn. 34 f. m. w. N.

28. Zu Art. 46 PAG-E (Rasterfahndung):

87

Durch die Bezugnahme auf Art. 11 Abs. 3 S. 2 Nr. 1, 2 und 5 PAG in Abs. 1 S. 1 wird der Anwendungsbereich der Maßnahme leicht ausgeweitet. In seiner Entscheidung zur Rasterfahndung nach dem PolG NW 1990 hat das BVerfG festgestellt, diese Maßnahme dürfe für Zwecke der Gefahrenabwehr nur eingesetzt werden, wenn eine *„konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist.“*[185] Dieses Gewicht erreichen die Rechtsgüter Gesundheit (Nr. 2) und Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt (Nr. 5), wie bereits ausgeführt (s. oben Rn. 58, 66), nicht. Allerdings ist in diesem Zusammenhang zu berücksichtigen, dass die Entscheidung zur präventiv-polizeilichen Rasterfahndung - die im Übrigen viel Kritik erfahren hat[186] - bei einer Gesamtbetrachtung der Rechtsprechung des BVerfG im Bereich des Sicherheitsrechts etwas aus dem Rahmen fällt.[187] So dürfte aus heutiger Perspektive die Rasterfahndung als ein weniger eingriffsintensives Instrument als die Online-Durchsuchung anzusehen sein, was dafür spricht, dass die Anordnungsvoraussetzungen niedriger ausfallen können. In diesem Sinne sieht die - bislang verfassungsrechtlich nicht beanstandete - Rasterfahndung nach § 98a StPO relativ moderate Anordnungsvoraussetzungen vor, nämlich den Verdacht einer durch einen Straftatenkatalog näher qualifizierten Straftat von erheblicher Bedeutung.[188] Diese Schwelle liegt deutlich unter derjenigen für die strafprozessuale Telekommunikationsüberwachung und erst recht derjenigen für die Wohnraumüberwachung und Online-Durchsuchung.

88

Auch ist aus heutiger Sicht schwer nachvollziehbar, dass das BVerfG die Rasterfahndung im Gefahrenvorfeld grundsätzlich - wenngleich nicht kategorisch, wie die Entwurfsverfasser annehmen (S. 120) - ausgeschlossen hat.[189] Gerade im Gefahrenvorfeld[190] - aufgrund des Trennungsgebots freilich vorzugsweise im Tätigkeitsbereich der Nachrichtendienste - stellt das Zusammenführen von bereits erhobenen personenbezogenen Daten ein wirksames Mittel der Aufklärung dar, das zugleich eine vergleichsweise geringere Eingriffstiefe als die Datenerhebung aufweist. Die - praktisch wichtige und sinnvolle - Tendenz zur Errichtung spezifischer „Gefährderdateien“ (vgl. etwa die Antiterrordatei nach

---

[185] BVerfGE 115, 320 - amtlicher Leitsatz. S. 60 f.

[186] Vgl. u. a. *Kirchberg*, CR 2007, 10; *Brenneisen/Bock*, DuD 2006, 685; *Schewe*, NVwZ 2007, 174.

[187] Vgl. auch die zutreffende Kritik im Sondervotum der Richterin Haas, die u. a. darauf hinweist, bei der Rasterfahndung handele es sich um ein „umständliches Verfahren“, welches im Zeitrahmen der konkreten Gefahr „mit überwiegender Wahrscheinlichkeit nicht zum Abschluss zu bringen“ sei (BVerfGE 115, 371, 377 f.). Das Erfordernis eines Nähebezugs der Betroffenen zur Bedrohung sei „im Ansatz verfehlt“, werde doch „typischerweise die Rasterfahndung gerade dann eingesetzt, wenn die möglichen Täter noch unbekannt sind.“

[188] Zu diesem Begriff die Nachweise unter Fn. 135.

[189] BVerfGE 115, 320, 360 ff.

[190] Vgl. BVerfGE 115, 320, 355: „Die Rasterfahndung ist ‚Verdachts-‘ oder ‚Verdächtigengewinnungseingriff‘ (…) insbesondere dann, wenn sie (…) zur Aufdeckung von so genannten terroristischen Schläfern führen soll.“

ATDG, die Rechtsextremistendatei nach REDG oder auch Dateianordnungen nach dem reformierten BNDG) folgt dieser Logik. Da nur durch ein Zusammenführen von personenbezogenen Daten aus verschiedenen Quellen im Gefahrenvorfeld eine aussagekräftige Identifizierung gefährlicher Personen gelingen kann (und damit zugleich eine größtmögliche Schonung unbeteiligter Personen), sollte in der Schaffung entsprechender Rechtsgrundlagen ein Schwerpunkt der legislatorischen Tätigkeit liegen. In diesem Zusammenhang müsste dann auch die Frage gestellt werden, in welchem Umfang den Polizeibehörden Kompetenzen im Bereich des Gefahrenvorfelds zustehen sollen. Gemessen am eigenen Anspruch, die Polizei insoweit mit möglichst umfassenden Befugnissen auszustatten, greift der Entwurf vor diesem Hintergrund in Art. 46 PAG-E zu kurz. Die Entscheidung des BVerfG zur Rasterfahndung eröffnet dabei durchaus einen Weg zu deren Nutzung im Gefahrenvorfeld, wenn nämlich *„das rechtsstaatliche Defizit, das mit dem für die Rasterfahndung typischen Verzicht auf eine Nähebeziehung zwischen dem gefährdeten Rechtsgut und den von dem Grundrechtseingriff Betroffenen verbunden ist, (…) auf andere Weise kompensiert werden“* kann, *„um die Uferlosigkeit der Ermächtigung auszuschließen.“*[191] Dabei müsste hinsichtlich der Eingriffsschwelle konsequent zwischen der Verarbeitung von Daten, die aus hoheitlich geführten Dateien stammen und solchen aus privaten Dateien differenziert werden.

Die Einführung einer Eilkompetenz in Abs. 3 S. 1 ist nicht zu beanstanden.

29. Zu Art. 47 PAG-E (Einsatz von unbemannten Luftfahrtsystemen):

89

Die Vorschrift ist nicht in allen Aspekten nachvollziehbar.

Drohnen sind ohne Zweifel geeignete technische Mittel zur Anfertigung von Bildaufnahmen aus der Luft. Dass offene Bildaufnahmen nach Art. 33 PAG-E auch durch Drohnen angefertigt werden sollen (Nr. 1 Alt. 1), leuchtet also ein. In diesem Fall kommt der Maßnahme - worauf auch die Entwurfsbegründung generell hinweist (S. 121) - eine zusätzliche nicht unerhebliche Eingriffsqualität zu, weshalb es erforderlich wäre, die Anordnungsvoraussetzungen insoweit enger zu fassen. Systematisch ließe sich das am besten im Zusammenhang mit der Befugnisnorm für das Erstellen von Bildaufnahmen machen, also in Art. 33 und Art. 36 PAG-E.

Weniger schlüssig erscheint der Einsatz von Drohnen hingegen bereits im Falle offener Tonaufnahmen (Nr. 1 Alt. 2). Erfahrungsgemäß setzt die Erstellung brauchbarer Tonaufnahmen eine größere Nähe zur Geräuschquelle voraus. Der Vorteil von Bildaufnahmen aus der Vogelperspektive bei un-

[191] BVerfGE 115, 320, 362 f.

übersichtlichen Situationen, etwa großen Menschenansammlungen, kommt bei Tonaufnahmen überhaupt nicht zum Tragen.

Noch fragwürdiger erscheint der Einsatz von Drohnen zum Zweck des heimlichen Abhörens des gesprochenen Worts außerhalb von Wohnungen [Nr. 2 i. V. m. Art. 36 Abs. 1 Nr. 2 lit. c) PAG-E]. Dass Zielpersonen, deren Gespräche abgehört werden sollen, sich unbeeindruckt von einer über ihren Köpfen kreisenden Drohne über für die Gefahrenabwehr relevante Themen unterhalten, ist eher unwahrscheinlich.

Soweit die Verwendung von Drohnen außerdem im Zusammenhang mit dem Einsatz technischer Mittel in Wohnungen (Nr. 3), mit Maßnahmen der Telekommunikationsüberwachung (Nr. 4) und solchen der Online-Durchsuchung (Nr. 5) zulässig sein soll, erschließt sich schon nicht, auf welche Weise ein derartiger Einsatz überhaupt denkbar ist. Der Entwurf enthält zu den technischen Möglichkeiten und Grenzen des Drohneneinsatzes keinerlei Hinweise.

Vor diesem Hintergrund muss prima facie davon ausgegangen werden, dass es sich mit Ausnahme des Erstellens von Bildaufzeichnungen um ungeeignete und damit unverhältnismäßige Maßnahmen handelt. Darüber hinaus wird mit Blick auf die Eingriffsintensität der beträchtliche Einschüchterungseffekt zu bedenken gegeben, der mit dem Einsatz von Drohnen verbunden ist. Dieser ist zugleich im Kontext der erheblichen Ausweitung der polizeilichen Kompetenzen im Gefahrenvorfeld zu sehen. Dass in Zukunft im Falle vager Anhaltspunkte für etwaige künftige Gefahren aufgrund zahlreicher Eingriffsbefugnisse - also mit einer sehr hohen Streubreite - Drohnen eingesetzt werden können, stellt ein Besorgnis erregendes Szenario dar.

30. Zu Art. 48 PAG-E (Weiterverarbeitung von Daten):

a) Zur Systematik:

90

Die Bündelung der Befugnisse zur Weiterverarbeitung von Daten aus qualifizierten Erhebungsmaßnahmen und die Unterteilung nach den verschiedenen Weiterverarbeitungszwecken (Abs. 1: zur eigenen Gefahrenabwehr; Abs. 2: zur Gefahrenabwehr durch andere Behörden; Abs. 3: zur Strafverfolgung) ist wegen der dadurch erreichten größeren Übersichtlichkeit zu begrüßen. Die Vorgaben des BVerfG aus der Entscheidung zum BKAG werden sachgerecht umgesetzt. Allgemein ist unter systematischen Gesichtspunkten jedoch anzumerken, dass die Gedanken der Zweckbindung und der hypothetischen Datenneuerhebung allgemeiner Natur sind und deshalb als allgemeine Grundsätze „vor die Klammer“ gezogen werden könnten (vgl. bereits oben Rn. 23 f.). Maßnahmespezifische Abweichungen könnten dann bei den jeweiligen Maßnahmen geregelt werden. So könnte eine noch größere Anwendungsfreundlichkeit hergestellt werden.

91

Allgemein festzuhalten ist, dass sich die durchgängige Ausweitung der Datenerhebungsbefugnisse auf der Ebene der Weiterverarbeitung fortsetzt, indem die diversen Weiterverarbeitungsbefugnisse des Art. 48 PAG-E abstrakt an die Zwecke und Rechtsgüter der Erhebungsbefugnisnormen anknüpfen. Die Grundsätze der Zweckbindung und der hypothetischen Datenneuerhebung können sich auf diese Weise auch grundrechtsbelastend auswirken, wenn nämlich die Erhebung unter höheren Voraussetzungen (etwa aufgrund einer konkreten Gefahr) erfolgte als die Weiterverarbeitung (etwa aufgrund einer drohenden Gefahr) zulässig ist. Außerdem erfordert die Weiterverarbeitung auch dann keine höheren Voraussetzungen, wenn solche im Erhebungsfall unter Verhältnismäßigkeitsgesichtspunkten geboten wären. Generell gilt: Je niedriger die Schwelle in der Erhebungsbefugnis ausgestaltet ist, umso mehr potenzieren sich die Möglichkeiten der Weiterverarbeitung und umso unwahrscheinlicher ist es, dass erhobene Daten einmal endgültig gelöscht werden.

Vor diesem Hintergrund sollte perspektivisch darüber nachgedacht werden, ob an einem - so vom BVerfG wohl nicht verstandenen[192] - Automatismus der hypothetischen Datenneuerhebung festgehalten werden kann oder nicht vielmehr mit besonders weit reichenden und ins Gefahrenvorfeld verlagerten Erhebungsbefugnissen eher restriktive Verarbeitungsregelungen kombiniert werden müssten - und umgekehrt.

b) Zu Abs. 1 (Weiterverarbeitung zu eigenen Zwecken):

92

Die Auffassung des Bayerischen Landesbeauftragten für den Datenschutz, die Möglichkeit der Weiterverarbeitung sei auf das jeweilige Polizeipräsidium zu begrenzen, kann nicht geteilt werden. Diese Einschränkung lässt sich den Vorgaben des BVerfG nicht entnehmen. Sie stünde auch quer zu der praktischen Notwendigkeit und Tatsächlichkeit einer übergreifenden Zusammenarbeit zwischen verschiedenen Polizeibehörden. Jedenfalls im Bereich der Strafverfolgung ist es gang und gäbe, dass Ermittlungen an spezialisierte oder mit Parallelverfahren befasste Polizeibehörden - auch präsidiumsübergreifend - oder das LKA abgegeben werden.

c) Zu Abs. 2 (Weiterverarbeitung für andere Zwecke der Gefahrenabwehr):

93

In Abs. 2 sollte klargestellt werden, dass mit „anderen für die Gefahrenabwehr zuständigen Behörden“ auch die Nachrichtendienste des Bundes und der Länder gemeint sind.

[192] BVerfGE 141, 220, 327 f., 329.

d) Zu Abs. 3 (Weiterverarbeitung für Zwecke der Strafverfolgung):

94

Die Straffung in Abs. 3 ist zu begrüßen, die Norm in der Fassung der Drucksache sprachlich aber immer noch ungenau. Verständlicher wäre hier die Formulierung:

> *„Die Polizei darf personenbezogene Daten, die durch in Abs. 1 genannte Maßnahmen erhoben wurden, für Zwecke der Strafverfolgung weiterverarbeiten und an andere Strafverfolgungsbehörden übermitteln, wenn die Daten insoweit einen konkreten Ermittlungsansatz erkennen lassen,*
>
> *1. im Falle ihrer Erhebung mittels elektronischer Aufenthaltsüberwachung nach Art. 34 Abs. 1*
>
> *a) wenn die Voraussetzungen des § 68b Abs. 1 Satz 3 StGB vorliegen, zur (…),*
>
> *b) zur Verfolgung von Straftaten der in § 66 Abs. 3 Satz 1 StGB genannten Art,*
>
> *2. im Falle ihrer Erhebung durch eine der in Abs. 1 Nr. 2 bis 7 genannten Maßnahmen zur Verfolgung von Straftaten, zu deren Aufklärung eine solche Maßnahme nach den entsprechenden strafprozessualen Befugnissen angeordnet werden dürfte.“*

e) Zu Abs. 4 (Sonderregelungen für Wohnraumüberwachung und Online-Durchsuchung):

95

Der Regelungsgehalt des Abs. 4 ließe sich eleganter abbilden, indem die Maßnahmen der Online-Durchsuchung und der Wohnraumüberwachung auch in den Katalog des Abs. 1 aufgenommen und die jeweiligen verfassungsrechtlich gebotenen Einschränkungen der Verwendbarkeit in Abs. 2 bzw. Abs. 3 als Ausnahmen angefügt würden.

31. Zu Art. 49 PAG-E (Schutz von Berufsgeheimnisträgern und des Kernbereichs):

a) Zu Abs. 1, 2 und 5 (Schutz von Berufsgeheimnisträgern):

96

Die Bündelung der Vorschriften zum Schutz grundrechtssensibler Bereiche ist ebenfalls im Grundsatz zu begrüßen. Soweit der Schutz von Berufsgeheimnisträgern betroffen ist, entbehrt der Entwurf allerdings eines schlüssigen bereichsspezifischen Konzepts. Die Anlehnung des Schutzes an die Zeugnisverweigerungsrechte der §§ 53, 53a StPO übernimmt die dortigen dogmatischen Schwächen und lässt eine eigene gesetzgeberische Abwägung der im Bereich der Gefahrenabwehr relevanten Belange vermissen. Außerdem stellt sich die Frage, warum der Schutz bestimmter Vertrauensverhältnisse nur auf die in Abs. 1 S. 1 bezeichneten besonderen Maßnahmen der Datenerhebung beschränkt sein soll. In ein geschütztes Vertrauensverhältnis kann durch jede - auch (teilweise erst recht) durch eine offene -

Datenerhebung eingegriffen werden. Andererseits genießen die schutzwürdigen Interessen der Berufsgeheimnisträger (und der Öffentlichkeit an deren Tätigkeiten) keinen absoluten Vorrang vor Belangen der Gefahrenabwehr.[193] Warum also z. B. zur Abwehr gegenwärtiger Gefahren für hochrangige Rechtsgüter von vornherein nicht in solche Vertrauensverhältnisse soll eingegriffen werden können, erscheint unausgewogen und widersprüchlich. Wenn zur Abwehr etwa einer gegenwärtigen Lebensgefahr so massive aktionelle Eingriffe wie ein finaler Rettungsschuss zulässig sind, sollte ein informationeller Eingriff in ein besonderem grundrechtlichen Schutz unterstehendes Vertrauensverhältnis auch möglich sein. Richtigerweise müsste zudem zwischen dem unterschiedlichen verfassungsrechtlichen Gewicht des Schutzes der verschiedenen Vertrauensverhältnisse differenziert werden. So ist z. B. der Schutz von Seelsorgern (Beichtgeheimnis, Kernbereich[194]), Suchtberatern (Persönlichkeitsrecht, evtl. Selbstbelastungsfreiheit[195]) oder Abgeordneten (institutioneller Schutz des Mandats[196]) nicht an denselben verfassungsrechtlichen Grundsätzen zu messen. All dies macht ein eigenständiges ausgewogenes polizeirechtliches Schutzkonzept erforderlich. Auf die weiteren Ausführungen unter Rn. 60 wird ergänzend Bezug genommen.

b) Zu Abs. 3 und 5 (Kernbereichsschutz):

97

Soweit in Abs. 3 S. 1 der Kernbereichsschutz ausgeschlossen wird, sofern Anhaltspunkte dafür bestehen, „dass diese Daten dazu dienen sollen, ein Erhebungsverbot herbeizuführen“, wird dadurch der vom BVerfG gemeinte Missbrauchsgedanke nur unzureichend erfasst. Gemeint ist, dass eine Kernbereichsrelevanz lediglich vorgetäuscht wird, es sich also nur prima vista aber nicht tatsächlich um Kernbereichsdaten handelt[197] (z. B. Gespräche über geplante Straftaten werden im Beichtstuhl geführt). Sind die Daten hingegen zweifellos als Kernbereichsdaten zu qualifizieren, und werden sie (auch) erzeugt oder verwendet, um ein Erhebungsverbot herbeizuführen (z. B. Gespräche über geplante Straftaten werden bewusst bei der Vornahme intimer sexueller Handlungen geführt), muss konsequenter Weise der Kernbereichsschutz greifen. Das ist aus Sicht der Gefahrenabwehr zwar unbefriedigend, verfassungsrechtlich aber nicht zu umgehen.

98

Erfreulich ist, dass der Kernbereichsschutz auf der Erhebungsebene für alle unter Abs. 3 S. 1 genannten Maßnahmen gleich ausgestaltet ist. Das erleichtert die praktische Anwendbarkeit. Andererseits stellt sich die Frage, warum der Schutz nicht auch auf andere, auch offene, Maßnahmen erstreckt wird.

[193] Vgl. nur BVerfGE 33, 367, 379; 107, 299, 332; 108, 251, 269; 129, 208, 258 ff.; BVerfGE 141, 220, 281, 318 f.; BVerfG NJW 2005, 1917; 2011, 1859, 1860.
[194] BVerfGE 109, 279, 322 f.; daran anschließend BVerfGE 141, 220, 276.
[195] BVerfGE 109, 279, 322; 110, 226, 253.
[196] BVerfGE 108, 251, 269; 109, 279, 358.
[197] BGHSt 54, 69, 99.

So sind Eingriffe in den Kernbereich ohne weiteres denkbar beim offenen Betreten und Durchsuchen von Wohnungen, beim offenen Durchsuchen von Sachen, namentlich von elektronischen Datenträgern, und beim Auswerten von Dokumenten.[198] Den Kernbereichsschutz lediglich auf einige eingriffsintensive heimliche Maßnahmen zu erstrecken, verkennt den hinter ihm stehenden allgemeinen Gedanken. Auch insoweit verfügt der Entwurf demnach über kein schlüssiges Konzept.

99

Zu begrüßen ist die Sonderregelung für Online-Durchsuchungen in Abs. 3 S. 5 und 6, die die praktische Durchführbarkeit der Maßnahme gewährleistet. Um nicht im Einzelfall schwierige Wahrscheinlichkeitserwägungen anstellen zu müssen (zumal der erforderliche Grad der Wahrscheinlichkeit gesetzlich nicht näher bestimmt wird), könnte erwogen werden, die Zulässigkeit der Datenerhebung durch die Formulierung *„darf auf das informationstechnische System auch dann zugegriffen werden, wenn dabei solche Daten voraussichtlich nur in untergeordnetem Umfang miterfasst werden."* Eine wörtliche Übernahme der entsprechenden Formulierung des BVerfG ist auch hier nicht notwendig.[199]

32. Zu Art. 50 bis 52 PAG-E (Benachrichtigung, Kontrolle, Berichtspflichten):

100

Die Bündelung der Benachrichtigungspflichten bei verdeckten Maßnahmen in Art. 50 PAG-E ist wegen der dadurch erhöhten Übersichtlichkeit und Anwendungsfreundlichkeit zu begrüßen. Die Rechtsprechung des BVerfG zu den Benachrichtigungspflichten wird vorbildlich umgesetzt. Praktisch wichtig und vollkommen sachgerecht ist zudem die Möglichkeit eines Absehens von der Benachrichtigung nach Abs. 1 S. 5, sofern die zu benachrichtigende Person von der Maßnahme nur unerheblich betroffen wurde. Da in diesem Fall in der Regel zugleich eine Konstellation dergestalt vorliegen wird, dass durch erforderliche Maßnahmen zur Identifizierung der betroffenen Person der Eingriff weiter vertieft würde, ist diese Ausnahmeregelung verfassungsrechtlich nicht zu beanstanden.[200] Diesen Gedanken stellt S. 6 nochmals klar. Auch Abs. 3 und 4 enthalten begrüßenswerte Klarstellungen zum maßgeblichen Zeitpunkt der Benachrichtigung bzw. Fristbeginn für eine Zurückstellungsentscheidung.

Auch in Art. 51 PAG-E werden die Vorgaben des BVerfG zu Protokollierungs- und Prüfpflichten übersichtlich und sachgerecht umgesetzt. Dem Einwand des Bayerischen Landesbeauftragten für den Datenschutz, es erschließe sich nicht, wie durch eine Protokollierung eine Gefährdung der jeweiligen

[198] Vgl. den Tagebuchfall BVerfG 80, 367 in dem mit 4 : 4 Stimmen ein Eingriff in den Kernbereich abgelehnt wurde. Abgesehen davon, dass noch intimere Aufzeichnungen denkbar sind, spricht viel dafür, dass der Fall heute anders entschieden würde; vgl. auch BVerfG, Beschluss vom 17.11.2007, 2 BvR 518/07, juris; VerfGH Berlin, 21.4.2009, 170/08, 170 A/08, Z. 10 ff., juris.
[199] BVerfGE 141, 220, 307.
[200] Vgl. BVerfGE 109, 279, 365.

Maßnahme herbeigeführt werden könne, die entsprechende Formulierung in Art. 51 Abs. 1 S. 1 PAG-E sei daher zu streichen[201], ist allerdings zuzustimmen.

101

Die Unterrichtungs- und Berichtspflichten nach Art. 52 PAG-E gehen, was den Umfang der Maßnahmen betrifft, über die zu berichten ist, teilweise sogar über den Rahmen des verfassungsrechtlich Gebotenen hinaus.[202] Die auf diese Weise in der Breite hergestellte größere Transparenz ist ausdrücklich zu begrüßen. Berechtigt ist allerdings auch der Einwand des Bayerischen Landesbeauftragten für den Datenschutz, der eine vorrangige Einbindung des Parlamentarischen Kontrollgremiums moniert und zurecht auf die funktionalen und organisatorischen Unterschiede zwischen Verfassungsschutz und Polizei hinweist.[203] Letztlich muss in dieser Regelung auf der Kontrollebene ein weiterer deutlicher Beleg für eine gewollte „Vernachrichtendienstlichung" der Polizei (vgl. Rn. 3) erblickt werden.

33. Zu Art. 53 bis 65 PAG-E (Datenspeicherung, -übermittlung und sonstige Datenverarbeitung):

a) Zur Systematik:

102

Unter systematischen Gesichtspunkten ist anzumerken, dass die Verstreuung der dem Datenschutz dienenden Regelungen in allgemeine Grundsätze (Art. 30 PAG-E), Vorschriften, die besondere Befugnisse und Maßnahmen der Datenerhebung betreffen (Art. 48 bis 51 PAG-E) und solche, die für jede Form der Datenverarbeitung nach dem PAG gelten (Art. 53 bis 65 PAG-E), das Erfassen des maßgeblichen Regelungsgehalts schwierig gestaltet, zumal die Trennung nicht konsequent durchgehalten wird (vgl. Art. 59 Abs. 3 PAG-E). Diese Regelungstechnik führt zwangsläufig zu Doppelungen (vgl. etwa Art. 48 Abs. 1 und Art. 53 Abs. 2 PAG-E) und Auslegungsunsicherheiten. Eine Bündelung dieser Vorschriften in einem Abschnitt („Weiterverarbeitung von Daten") wäre hilfreich.

---

[201] (Fn. 60), S. 53.

[202] „Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können", erhebt das BVerfG zwar die Forderung, „hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen" (BVerfGE 141, 220, 285). Das Urteil bezieht sich aber nicht auf alle der in Art. 52 Abs. 1 S. 1 PAG-E genannten Maßnahmen. Zuvor hatte das BVerfG entsprechende Berichtspflichten lediglich bei der akustischen Wohnraumüberwachung (BVerfGE 109, 279, 373) aufgrund von Art. 13 Abs. 6 GG für von Verfassung wegen erforderlich gehalten.

[203] (Fn. 60), S. 55 f.

b) Zu Art. 53 Abs. 2 S. 2 PAG-E (zweckändernde polizeiliche Nutzung):

103

Die Vorschrift ist sprachlich etwas ungenau, indem sich nicht deutlich erschließt, ob nur die Übermittlung zu einem anderen polizeilichen Zweck zulässig sei oder auch die Speicherung und Veränderung zu einem anderen polizeilichen Zweck (wie wohl beabsichtigt, vgl. Entwurfsbegründung S. 134). Klarer wäre die Formulierung *„Die Verarbeitung einschließlich einer erneuten Speicherung, Veränderung und Übermittlung zu einem anderen polizeilichen Zweck ist zulässig (…).“*

c) Zu Art. 53 Abs. 3 PAG-E (Ausnahme vom Verwendungsverbot):

104

Die Regelung, die die Weiterverarbeitung von Daten, welche ohne Vorliegen der Erhebungsvoraussetzungen erlangt wurden, ausnahmsweise zur Abwehr einer gegenwärtigen Gefahr für ein in Art. 11 Abs. 3 S. 2 Nr. 1 und 2 genanntes Rechtsgut oder für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, erlaubt, ist in ihrem Grundgedanken ausdrücklich zu begrüßen. Unzutreffend ist freilich, dass hier ein Verwendungsverbot normiert werde (S. 134), vielmehr handelt es sich um eine Ausnahmeregelung zu einem ungeschriebenen Verwendungsverbot.

Zu überlegen ist aber, ob die Regelung nicht zu kurz greift, denn aus der Rechtswidrigkeit einer Datenerhebung folgt nicht automatisch die Unzulässigkeit der Datenverwendung. Im Bereich der strafprozessualen Verwertungsverbote (die die Verwendung von Daten zu Beweiszwecken betreffen und damit eine besondere Art von Verwendungsverboten darstellen), betonen die höchstrichterliche Rechtsprechung und das BVerfG seit langem, dass es einen derartigen Automatismus nicht gebe. Vielmehr sei im Einzelfall das Strafverfolgungsinteresse mit dem Interesse an der Nichtverwendung der Daten abzuwägen.[204] Warum dies im Zusammenhang mit der Verwendung zu Zwecken der Gefahrenabwehr anders zu beurteilen sei, ist nicht zu erkennen, zumal das öffentliche Interesse an der Abwehr von Gefahren in der Regel höher einzustufen ist als dasjenige an einer „bloßen“ Strafverfolgung. Hinzu kommt, dass die Gründe für eine Nichtbeachtung der Erhebungsvoraussetzungen vielfältig sein können. Sie können von einer willkürlichen Missachtung bis zu einer unabsichtlichen Fehleinschätzung reichen. Die Abwehr der Gefahr kann außerdem im Interesse der von der rechtswidrigen Datenerhebung betroffenen Person liegen. Das Verbot der Datenverwendung als Mittel zur Disziplinierung der Polizeibehörden zu sehen (sog. Disziplinierungstheorie[205]) mutet im Bereich der Gefahrenabwehr noch verfehlter an als im Bereich der Strafverfolgung. Denn die Abwehr einer Gefahr liegt nicht im Interesse einzelner, mit der Datenerhebung betrauter Polizeibeamter, sondern der gefährdeten Personen und

[204] Vgl. BVerfGK 4, 283, 285; 17, 390, 399; BVerfG NJW 2007, 499, 503 f.; 2008, 3053; 2014, 532, 534; BVerfGE 130, 1, 31; BVerfG, ZD 2015, 423.
[205] Näher hierzu *Löffelmann*, S. 71 f.

der Allgemeinheit, die im Falle eines Datenverwendungsverbots und einer deshalb sich verwirklichenden Gefahr auch den Schaden zu tragen haben. Bewusste Rechtsverstöße können schließlich auch auf andere Weise sanktioniert werden.[206] Auch im Falle unzulässig gespeicherter Daten ist im Übrigen nicht eine zwingende Löschung vorgesehen (vgl. Art. 62 Abs. 2 und 3 PAG-E). Datenschutzrechtlichen Belangen kann auch durch eine teilweise Sperrung der Daten Rechnung getragen werden.

Vor diesem Hintergrund weist die Regelung in Abs. 3 zwar in die richtige Richtung. Die schwierige Frage, inwieweit ein schematisches Festhalten am Grundsatz der Datenneuerhebung verfassungsrechtlich geboten ist oder weitere Ausnahmen erlaubt, müsste jedoch dringend näher beleuchtet werden.

d) Zu Art. 53 Abs. 4 PAG-E (Grunddaten):

105

Die Klarstellung in Art. 53 Abs. 4 PAG-E, welche Grunddaten von der Polizei stets verarbeitet werden dürfen, ist aus Gründen der Praktikabilität ausdrücklich zu begrüßen.

e) Zu Art. 54 Abs. 2 S. 1 und 2 PAG-E (Verarbeitung strafrechtlicher Daten):

106

Die Beibehaltung der Regelung zur Weiterverarbeitung im Rahmen strafrechtlicher Ermittlungen gewonnener Daten und ihrer Löschung bei Wegfall des Tatverdachts harmoniert nicht mit dem im Übrigen im Entwurf verfolgten Konzept der Weiterverarbeitung. Die Vorschrift führt dazu, dass bereits rechtmäßig erhobene Daten, die zur Gefahrenabwehr benötigt werden, gelöscht werden müssen und also nicht mehr verwendet werden können, (nur) weil der strafrechtlich relevante Verdacht weggefallen ist. Da dies für jedwede Art der Verwendung zu Zwecken der Gefahrenabwehr gilt, liegt die Regelung evident quer zu der des Art. 53 Abs. 3 PAG-E, die eine Verwendung sogar im Falle einer rechtswidrigen Datenerhebung zulässt. Außerdem ist zu berücksichtigen, dass die Annahme eines strafrechtlichen Tatverdachts in der Regel von sehr spezifischen Tatbestandsvoraussetzungen abhängt, was für die Annahme einer Gefahr im polizeirechtlichen Sinne nicht gilt. Richtigerweise müsste auch hier - also für den umgekehrten Fall der Verwendung zu anderen Zwecken erhobener Daten für solche der Gefahrenabwehr - (mindestens, vgl. Rn. 104) - der Grundsatz der hypothetischen Datenneuerhebung zur Anwendung gelangen (vgl. spiegelbildlich für das Strafverfahren § 161 Abs. 2 S. 1 StPO), zumal die bisherige Löschungsregelung hinsichtlich der Entscheidung, wann ein Tatverdacht entfallen ist, mit einer Vielzahl von Unwägbarkeiten befrachtet[207] und daher wenig praxistauglich ist.

[206] Vgl. als prominentes Beispiel den Fall Gäfgen, (EGMR, NJW 2007, 2461; 2010, 3145), wo die rechtswidrig handelnden Polizeibeamten strafrechtlich verurteilt wurden.
[207] Vgl. *Schmidbauer*/Steiner, PAG, Art. 38 Rn. 31 ff.

f) Zu Art. 54 Abs. 4 S. 3 und 4 PAG-E (Verarbeitung zu wissenschaftlichen Zwecken):

107
Die neue Befugnis zur Datenverarbeitung zu wissenschaftlichen Zwecken ist ausdrücklich zu begrüßen. Eine bessere rechtstatsächliche Erschließung der Polizeiarbeit ist für die künftige Entwicklung der Gesetzgebung dringend erforderlich.

g) Zu Art. 55 Abs. 3 S. 5 PAG-E (Verarbeitungsverbot nach Übermittlung):

108
Das Verbot für die empfangende Stelle, Daten weiterzuverarbeiten, die aufgrund einer rechtswidrigen Übermittlung erlangt wurden, müsste konsequenter Weise in den die Tätigkeit dieser Stellen betreffenden Gesetzen geregelt werden. Soweit es sich dabei z. B. um Bundesbehörden handelt, fehlt dem Bayerischen Gesetzgeber schon die Kompetenz, entsprechend verbindliche Regelungen für andere Stellen zu erlassen. In den dortigen bereichsspezifischen Vorschriften wäre dann ggf. zu regeln, ob dort eine Weiterverarbeitung nach dem Grundsatz der hypothetischen Datenneuerhebung zulässig sei.

h) Zu Art. 56 Abs. 1 Nr. 4 PAG-E (Übermittlung an Nachrichtendienste):

109
Die beabsichtigte Klarstellung der Übermittlungsbefugnis an die Nachrichtendienste von Bund und Ländern ist zu begrüßen.[208]

i) Zu Art. 57 und 59 PAG-E (Übermittlung an ausländische Stellen):

110
Die detaillierte Ausgestaltung der Übermittlungsbefugnisse an ausländische Stellen ist zu begrüßen.

Allerdings ist zu erwägen, ob einer Datenübermittlung an ausländische Stellen nicht grundsätzlich eine Benachrichtigung der betroffenen Person - also die Gewährung rechtlichen Gehörs - vorauszugehen hat. Mit der Übermittlung personenbezogener Daten ins Ausland begibt sich der deutsche Staat weitgehend der Verfügungsgewalt über diese Daten. Missbräuchliche Verwendungen kann er nicht mehr - allenfalls auf völkerrechtlichem Wege - verhindern. Für die betroffene Person kann die Datenverwendung im Ausland mit weitaus gravierenderen Nachteilen verbunden sein, als im Inland, so z. B. bei der Verwendung zu Zwecken der Strafverfolgung, wenn die ausländische Rechtsordnung als Sanktionsmöglichkeit die Todesstrafe vorsieht. Dabei ist insbesondere zu berücksichtigen, dass der deutsche Staat von Verfassung wegen nicht „die Hand zu Menschenrechtsverletzungen durch einen ausländi-

[208] BVerfGE 141, 220, 329 f.

schen Staat reichen“ darf.[209] Da Art. 57 und 58 PAG-E Ausnahmetatbestände vorsehen, die an schutzwürdige Interessen der betroffenen Person (Art. 58 Abs. 1 S. 2 Nr. 2 PAG-E) und seine Grundrechte (Art. 58 Abs. 4 S. 1 Nr. 3 PAG-E) anknüpfen, sollte für diese auch die Möglichkeit ihrer tatsächlichen Geltendmachung bestehen. Sofern aus Gründen der Gefahrenabwehr eine nichtoffene Datenübermittlung erforderlich ist, könnte dem mit einem Ausschlusstatbestand und einer Pflicht zur nachträglichen Benachrichtigung Rechnung getragen werden.

Im Übrigen wird der vom Bayerischen Landesbeauftragten für den Datenschutz in diesem Zusammenhang angebrachten Kritik beigetreten.[210]

j) Zu Art. 60 Abs. 1 S. 1, Abs. 2 S. 3 PAG-E (Datenübermittlung an die Polizei):

111

Befugnisse und Pflichten anderer öffentlicher Stellen zur Datenübermittlung an die Polizei sind in den deren Tätigkeit regelnden bereichsspezifischen Gesetzen vorzusehen.

k) Zu Art. 60 Abs. 3 PAG-E (Übermittlungsersuchen an inländische Nachrichtendienste):

112

Die Klarstellung ist grundsätzlich zu begrüßen. Allerdings ist darauf hinzuweisen, dass infolge der weiten Vorverlagerung der polizeilichen Tätigkeit in das Gefahrenvorfeld nunmehr zur Abwehr lediglich drohender Gefahren (Nr. 1) von den Nachrichtendiensten Daten erlangt werden können. Damit kommt es bei der Polizei zu einer Kumulierung von das Gefahrenvorfeld betreffenden Daten, was den Befund einer weitgehenden „Vernachrichtendienstlichung“ der Polizei (vgl. oben Rn. 3) verstärkt. Dies steht nicht im Einklang mit dem vom BVerfG im Urteil zur Antiterrordatei entwickelten informationellen Trennungsgebot, demzufolge die Datenübermittlung von Nachrichtendiensten an Polizeibehörden nur ausnahmsweise erfolgen darf und einer präzisen, normenklaren bereichsspezifischen Ermächtigung bedarf.[211] Davon kann bei der Generalklausel des Abs. 3 keine Rede sein. Darüber hinaus weist der Bayerische Landesbeauftragte für den Datenschutz zutreffend auf die Divergenz der gegenständlichen Regelung und der des Art. 25 Abs. 2 S. 1 Nr. 1 BayVSG hin.[212] Für die die anderen nachrichtendienstlichen Behörden auf Bundes- und Landesebene betreffenden Übermittlungsbefugnisse (soweit solche im jeweiligen Landesrecht bereits existieren) gilt dies entsprechend.

[209] BVerfGE 140, 317, 347 m. w. N.; BVerfGE 141, 220, 342.
[210] (Fn. 60), S. 63 - 67.
[211] BVerfGE 133, 277, 329 f.
[212] (Fn. 60), S. 67.

l) Zu Art. 61 PAG-E (Datenabgleich innerhalb der Polizei):

113
Es sollte erwogen werden, die Vorschrift des Art. 61 PAG-E allgemeiner zu fassen, etwa nach dem Vorbild des § 25a HSOG-E.[213] Dabei ist zu berücksichtigen, dass polizeiliche Tätigkeit, sei es im Bereich der Verfolgung von Straftaten oder durch informationelles Handeln im Bereich der Gefahrenabwehr seit jeher als zentrales Element ein Zusammenführen von aus unterschiedlichen Quellen stammenden und an verschiedenen Orten innerhalb des polizeilichen Bereichs abgelegten Daten beinhaltet. Dieser Kernkompetenz könnte für die (selbstverständliche) Nutzung informationsverarbeitender Systeme mit einer allgemeinen Befugnis zum Datenabgleich innerhalb der Polizei die erforderliche gesetzliche Grundlage gegeben werden. Um eine gemeinsame Datei verschiedener Behörden handelte es sich dabei nicht, so dass der Gedanke des informationellen Trennungsgebots nicht zum Tragen käme.

m) Zu Art. 62 Abs. 2 Nr. 1, Abs. 3 Nr. 4 PAG-E (Löschung unzulässig erhobener oder verarbeiteter Daten):

114
Die Erweiterung der Ausnahmen entsprechend der Regelung in Art. 53 Abs. 3 und 4 PAG-E ist konsequent und ausdrücklich zu begrüßen. Die zu der in Bezug genommenen Vorschrift dargestellten Überlegungen gelten aber auch hier. Auf die Ausführungen unter Rn. 104 wird insoweit Bezug genommen.

n) Zu Art. 64 PAG-E (Dateianordnung und Folgenabschätzung):

115
Da es sich um ein automatisiertes Verfahren (vgl. § 46 Abs. 1 Nr. 1 BDSG) handelt, treten an die Stelle verfahrensrechtlicher Schritte, die sonst die Einhaltung der Übermittlungsvoraussetzungen im Einzelfall gewährleisten, rechtliche und technische Vorgaben für die Einrichtung und Nutzung des eingesetzten informationstechnischen Systems. Zu diesen Vorgaben zählen auch zu beachtende technische Standards, um die Art. 64 Abs. 1 S. 1 PAG-E zu erweitern wäre, insbesondere zum Schutz des Dateienverbunds gegen unberechtigte Zugriffe.

[213] § 25a HSOG-E lautet: „Automatisierte Anwendung zur Datenanalyse (1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind. (2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden. (3) Die Einrichtung und wesentli-

Erwägenswert wäre zudem, die Regelung des Art. 64 Abs. 2 PAG-E, die nicht nur spezifisch das Polizeirecht betrifft, in das BayDSG aufzunehmen.

34. Zu Art. 78 bis 86 PAG-E (unmittelbarer Zwang):

116

In den Bestimmungen zur Anwendung unmittelbaren Zwangs sieht der Gesetzentwurf eine Ausweitung zulässiger Hilfsmittel auf Drohnen (Art. 78 Abs. 3 PAG-E) und zulässiger Waffen auf Explosivmittel (Art. 78 Abs. 5 PAG-E) vor. Soweit Drohnen betroffen sind, sieht der Entwurf in der Änderung lediglich eine Klarstellung (S. 161). Gleichwohl kommt dem Einsatz dieses Hilfsmittels aufgrund seiner mittlerweile unproblematischen Verfügbarkeit im Zusammenhang mit der Anwendung unmittelbaren Zwangs eine ganz neue Bedeutung und Dimension zu. Anders als beim Einsatz von Drohnen nach Art. 47 PAG-E als Hilfsmittel für eine (bloße) Aufklärungsmaßnahme, ist ihre ausdrückliche Definition als „Hilfsmittel der körperlichen Gewalt" in Art. 78 Abs. 3 PAG-E auf die Ausübung unmittelbaren Zwangs gerichtet. Das verdeutlicht auch ihre Nennung im unmittelbaren Zusammenhang mit Wasserwerfern, Reiz- und Betäubungsstoffen oder Sprengmitteln. Soweit die Entwurfsbegründung (S. 161) darauf abstellt, dass Luftfahrzeuge auch bisher schon Hilfsmittel der körperlichen Gewalt sein konnten, erscheint das zweifelhaft.[214] Denn mit Luftfahrzeugen kann nicht, ähnlich wie etwa mit Dienstfahrzeugen, unmittelbar auf Menschen oder Sachen eingewirkt werden oder können Sperren errichtet werden. Mit der Erweiterung der Beispiele für Hilfsmittel auf Drohnen ist daher eine beträchtliche Weiterung verbunden, in deren Folge z. B. (mit Reizstoffen, Gummigeschossen oder auch scharfer Munition) bewaffnete Drohnen unmittelbar gegen Menschen eingesetzt werden könnten. Eine derartige Befugnis ist rechtlich und ethisch höchst problematisch[215] und darf keinesfalls en passant eingeführt werden.

117

Soweit eine Erweiterung der zulässigen Waffen auf Explosivmittel und eine Erweiterung von deren Einsatzmöglichkeiten (Art. 86 Abs. 1 S. 2 PAG-E) beabsichtigt ist und dies pauschal mit „neuen Bekämpfungsszenarien bei der Terrorismusabwehr" begründet wird (S. 161), sollte bedacht werden, dass der Einsatz solcher Mittel stets eine massive Gefährdung einer Vielzahl unbeteiligter Personen bedingt (vgl. daher die hohen Strafdrohungen unter §§ 308, 310 StGB). Generell begründen das Mitsichführen

---

che Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten."

[214] *Schmidbauer*/Steiner, PAG, Art. 61 Rn. 4 ff. und *Buggisch*, in: BeckOK BayPAG, Art. 61 Rn. 11 ff. nennen Luftfahrzeuge nicht als Hilfsmittel körperlicher Gewalt.

[215] Vgl. *Boothby*, HuV-I 2/2011, 81, 89 f.; zum (quasi-)polizeilichen Einsatz von Aufklärungsdrohnen *Hertwig*/*Kuvvet*, HuV-I 2/2011, 120 und *Mahraun*, HuV-I 2/2011, 128; zum Einsatz bewaffneter Drohnen im Spannungsfeld von Verfassungsrecht und humanitärem Völkerrecht ferner *Löffelmann*, JR 2013, 496; *ders.*, Kritische Justiz 2013, 372.

und der Einsatz von Waffen durch Polizeibeamte im öffentlichen Raum stets eine abstrakte Gefahr für hochrangige Rechtsgüter wie Leib und Leben. Der entsetzliche Vorfall von Juni 2017 am S-Bahnhof in Unterföhring, wo ein geistig verwirrter Mann einem Polizisten die Dienstwaffe entwinden konnte und anschließend durch Schüsse mehrere Personen verletzte, darunter eine Polizistin, die seitdem im Wachkoma liegt, verdeutlicht diese Gefahr.[216] Versuche von Störern, Dienstwaffen der am Tatort agierenden Polizisten an sich zu bringen, ereignen sich in jüngerer Zeit immer wieder.[217] Vor diesem Hintergrund könnte - entgegen der Intention des Gesetzentwurfs, die Möglichkeiten des polizeilichen Einsatzes von Waffen und Explosivmitteln auszuweiten - eher ein Umdenken dergestalt angezeigt sein, die Verfügbarkeit und den Einsatz von solchen Mitteln, die eine Gefahr für das Rechtsgut Leben begründen können (insbesondere Schusswaffen mit scharfer Munition), einzuschränken.

118

Soweit in Art. 83 Abs. 2 S. 2 PAG-E die Formulierung „Lebensgefahr oder der gegenwärtigen Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit“ durch die Wörter „Gefahr für Leib oder Leben“ ersetzt werden soll, handelt es sich dabei entgegen der Entwurfsbegründung (S. 162) um eine Weiterung, da die Qualifikation „schwerwiegende Verletzung“ entfällt. Die Kommentarliteratur weist in diesem Zusammenhang darauf hin, die Regelung sei *„schon deswegen notwendig, da es oft allein von der Konstitution des Opfers abhängt, ob die Quälereien eines Geiselnehmers ‚bloß‘ mit einer schweren Verletzung enden oder tödlich sind.“* Der Gesetzgeber habe daher - trotz verfassungsrechtlicher Bedenken - den finalen Rettungsschuss bereits bei der Gefahr der schwerwiegenden Verletzung der körperlichen Unversehrtheit freigegeben.[218] Eine Gefahr für den Leib, die bereits dann gegeben ist, wenn eine Verletzung der körperlichen oder geistigen Unversehrtheit oder der Gesundheit droht[219], erreicht diese Schwelle nicht, weshalb die verfassungsrechtlichen Bedenken hier erst recht greifen.

---

[216] Vgl. http://www.abendzeitung-muenchen.de/inhalt.wie-konnte-er-die-waffe-entreissen-schiesserei-in-unterfoehring-polizei-gibt-neue-details-zu-taeter-bekannt.d72bb8c8-7560-4ee3-aa9b-8d7ee4294d92.html (14.06.2017).

[217] Vgl. http://www.abendzeitung-muenchen.de/inhalt.26-jaehriger-rastet-voellig-aus-ertappter-ladendieb-will-polizist-dienstwaffe-entreissen.9c59af7e-5857-4536-ad09-42cedee8a298.html (11.01.2018); http://www.abendzeitung-muenchen.de/inhalt.er-wehrte-sich-gegen-festnahme-harlaching-mann-versucht-polizist-pistole-zu-entreissen.62160208-1070-46b7-bf3f-239e10263e80.html (23.01.2018).

[218] *Schmidbauer*/Steiner, PAG, Art. 66 Rn. 8 und 14, wo unter Hinweis auf die staatliche Schutzpflicht allerdings ein noch weitergehender Einsatz des finalen Rettungsschusses gefordert wird.

[219] *Schmidbauer*/Steiner, PAG, Art. 17 Rn. 18; ob dabei jeder Gesundheitsschaden genüge (so a. a. O. Art. 23 Rn. 22) oder jedenfalls erhebliche körperliche Beeinträchtigungen (so a. a. O. Art. 34 Rn. 47) oder nicht nur leichte Körperverletzungen (so a. a. O. Art. 11 Rn. 50, Art. 34a Rn. 21) erforderlich sind, wird je nach Kontext unterschiedlich beantwortet, jedenfalls aber liegt die Schwelle unter derjenigen der schwerwiegenden Verletzung der körperlichen Unversehrtheit.

35. Zu Art. 92 PAG-E (gerichtliche Entscheidungen):

119

Die Bündelung und Vereinheitlichung der Regelungen über die gerichtliche Zuständigkeit und das gerichtliche Verfahren in einer eigenen Vorschrift ist nachdrücklich zu begrüßen. Das in der Entwurfsbegründung (S. 167 f.) hervorgehobene Erfordernis, dass die Polizeibehörden Anträge auf gerichtliche Entscheidung stets qualifiziert zu begründen haben, sollte gesetzlich verankert werden, da es sich um ein verfassungsrechtliches Gebot handelt.[220] Soweit der Bayerische Landesbeauftragte für den Datenschutz außerdem die Ausnahmeregelung in Abs. 3 S. 2 moniert[221], ist dem zuzustimmen. Dabei ist namentlich zu berücksichtigen, dass an die Rechtmäßigkeit der Datenerhebung auch die Zulässigkeit der Weiterverarbeitung der erhobenen Daten anschließt (vgl. Art. 53 Abs. 4 PAG-E). Die präventiv grundrechtsschützende Funktion des Richtervorbehalts entfaltet demnach nicht nur bei der Datenerhebung, sondern auch bei der Weiterverarbeitung Wirkung. Ein Absehen von der gerichtlichen Bestätigung wäre demnach nur in Fällen erfolgloser Erhebungsmaßnahmen denkbar. Aber auch in diesen Fällen ist zu berücksichtigen, dass das BVerfG in mittlerweile gefestigter Rechtsprechung[222] von einem Fortbestehen des Rechtsschutzbedürfnisses bei erledigten Maßnahmen ausgeht, wenn hierdurch in Grundrechte eingegriffen wurde oder die Gefahr einer Wiederholung besteht.

36. Zu Art. 93 S. 2 und Art. 94 PAG-E (Kostentragungspflicht und Opferschutzmaßnahmen):

120

Die neue Regelung in Art. 93 S. 2 PAG-E, der zufolge polizeirechtlich verantwortlichen Personen auch im Falle einer Gemengelage die Kosten für den Polizeieinsatz auferlegt werden können, ist nachdrücklich zu begrüßen. Dasselbe gilt für die neue Opferschutzregelung in Art. 94 PAG-E, wobei in diesem Zusammenhang auf einen generellen Reformbedarf im Bereich der Opferschutzmaßnahmen wie auch der Opferentschädigung hinzuweisen ist. Hier werden viele wichtige Leistungen bislang von privaten Trägern erbracht.

37. Zur „Gesamtbilanz“:

121

Unter Verhältnismäßigkeitsgesichtspunkten ist es erforderlich, einzelne Eingriffsbefugnisse nicht nur isoliert zu betrachten, sondern auch in ihrem wechselseitigen Zusammenwirken. So hat das BVerfG

[220] BVerfGE 141, 220, 275.
[221] (Fn. 60), S. 75 f.

bereits in seiner Entscheidung zum Einsatz technischer Observationsmittel nach StPO auf die Problematik der „Kumulierung" von Ermittlungsmaßnahmen hingewiesen und gefordert, beim Einsatz moderner, insbesondere dem Betroffenen verborgener, Ermittlungsmethoden müssten die Strafverfolgungsbehörden mit Rücksicht auf das dem „additiven" Grundrechtseingriff innewohnende Gefährdungspotential besondere Anforderungen an das Verfahren beachten. Es sei sicherzustellen, dass die für eine Maßnahme verantwortliche Stelle (dort die Staatsanwaltschaft) als primär verantwortliche Entscheidungsträgerin über alle Eingriffe informiert ist, die den Grundrechtsträger im Zeitpunkt der Antragstellung und im Zeitpunkt einer zeitlich versetzten Ausführung der Maßnahme jeweils treffen, da andernfalls eine verantwortliche Prüfung und Feststellung übermäßiger Belastung nicht möglich wäre. Für den Fall, dass neben den Strafverfolgungsinstanzen auch Verfassungsschutzbehörden und Nachrichtendienste ermittelnde Maßnahmen anordnen und vollziehen, fordert das BVerfG eine entsprechende behördenübergreifende Informationspflicht zum Zwecke einer grundrechtssichernde Abstimmung der Ermittlungstätigkeit. Darüber hinaus werde der Gesetzgeber *„zu beobachten haben, ob die bestehenden verfahrensrechtlichen Vorkehrungen auch angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern."*[223] In seiner Entscheidung zur „Vorratsdatenspeicherung" weist das BVerfG darauf hin, die Speicherung der Telekommunikationsverkehrsdaten dürfe *„nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. (...) Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (...)."* In einer Vielzahl weiterer Entscheidungen hat das BVerfG außerdem auf das Verbot einer „Total- oder Rundumüberwachung" betroffener Personen hingewiesen[224] und die von Überwachungsmaßnahmen ausgehenden „Einschüchterungseffekte" für die Allgemeinheit betont.[225]

---

[222] BVerfGE 96, 27; 96, 44; daran anschließend BVerfG NJW 1998, 2131; 1999, 273 u. ö.
[223] BVerfGE 112, 304, 319 f.
[224] BVerfGE 65, 1, 43; 112, 304, 319; 109, 279, 323; 112, 304, 319; 130, 1, 24; 141, 220, 280.
[225] BVerfGE 65, 1, 42; 107, 299, 328; 113, 29, 46; 115, 320, 354 f.; 120, 378, 402; 125, 260, 319, 332.

122
Mit dieser Problematik der „Gesamtbilanz“ setzt sich der Gesetzentwurf nicht auseinander. Besondere verfahrensrechtliche Absicherungen, die gewährleisten, dass alle gegen eine betroffene Person ergriffenen Maßnahmen bei der Entscheidung über eine Anordnung - sei es eine polizeiliche oder gerichtliche - dem Entscheidungsträger bekannt sind, fehlen. Der Umstand, dass die durch den Entwurf beabsichtigte generelle Vorverlagerung der polizeilichen Befugnisse ins Gefahrenvorfeld zu weiten Überschneidungen mit dem Tätigkeitsbereich der Nachrichtendienste führt und es also zu Mehrfachmaßnahmen verschiedener Behörden gegen dieselbe Person kommen kann, wird nicht berücksichtigt. Bei einer Gesamtbetrachtung weist der Gesetzentwurf, insbesondere wenn er im Kontext weiterer Ausdehnungen der sicherheitsbehördlichen Befugnisse auf Bundes- und Landesebene betrachtet wird, eine starke Tendenz zu einer totalen Erfassung der Freiheitswahrnehmung der Bürgerinnen und Bürger auf.

III. Zusammenfassende Bewertung

123
Bei einer Gesamtbetrachtung fällt die Bewertung des gegenständlichen Gesetzentwurfs ambivalent aus. Die Vorgaben der Richtlinie (EU) 2016/680 werden überwiegend (vgl. aber Rn. 24, 25, 27) sachgerecht, wenngleich nicht in sonderlich anwendungsfreundlicher Weise umgesetzt. An begrüßenswerten Änderungen sind außerdem zu nennen

- der Verzicht auf die **persönliche Anhörung** nach Art. 18 Abs. 1 S. 2 bis 5 PAG-E (Rn. 12);
- die **Erstreckung der Durchsuchungsbefugnis** auf sämtliche bewegliche Sachen, die sich an einer Kontrollstelle befinden nach Art. 22 Abs. 1 Nr. 6 PAG-E (Rn. 13);
- die **Erweiterung der Analyse von DNA-Spurenmaterial** in Art. 32 Abs. 1 S. 2 und 3 PAG-E (Rn. 29);
- die Regelung des Einsatzes sog. **Bodycams** zum Zweck des Personenschutzes nach Art. 33 Abs. 4 PAG-E, soweit nicht ihre Verwendung innerhalb von Wohnräumen zum Schutz dritter Personen betroffen ist (Rn. 32);
- die Schaffung einer Befugnis zur **Postbeschlagnahme** nach Art. 35 PAG-E, soweit nicht Fälle lediglich drohender Gefahr betroffen sind (Rn. 36 - 39);
- die ausdrückliche Regelung des Einsatzes von **Verdeckten Ermittlern und Vertrauensleuten** nach Art. 37 und 38 PAG-E, mit der Einschränkung, dass die Erforderlichkeit dieser Instrumente im Bereich der Gefahrenabwehr zu hinterfragen ist (Rn. 47);
- die Klarstellung der **zulässigen technischen Mittel** bei der Wohnraumüberwachung gem. Art. 41 Abs. 1 S. 3 PAG-E (Rn. 61);

- die ausdrückliche Regelung des **Betretungsrechts** bei der Wohnraumüberwachung gem. Art. 41 Abs. 4 S. 3 PAG-E (Rn. 62);
- die Umsetzung der Vorgaben des BVerfG zur Überprüfung sensibler Daten durch eine „**unabhängige Stelle**“ nach Art. 41 Abs. 5, Art. 42 Abs. 7 und Art. 45 Abs. 4 PAG-E (Rn. 63, 71);
- die Erstreckung der Online-Durchsuchung auf **räumlich getrennte Systeme** nach Art. 45 Abs. 1 S. 2 PAG-E, soweit die Maßnahme nicht selbst unter Verhältnismäßigkeitsgesichtspunkten Bedenken begegnet (Rn. 83);
- die Ausdehnung des **Kernbereichsschutzes** auf alle in Art. 49 Abs. 3 S. 1 PAG-E genannten Maßnahmen und Schaffung einer Sonderregelung für die Online-Durchsuchung (Rn. 98 f.);
- die Neufassung der **Benachrichtigungs- und Berichtspflichten** in Art. 50 bis 52 PAG-E (Rn. 100 f.);
- die gesetzliche Regelung der **Übermittlungsbefugnisse** an Nachrichtendienste und ausländische Stellen nach Art. 56 Abs. 1 Nr. 4 und Art. 57, 59 PAG-E, mit der Einschränkung, dass bei einer Übermittlung ins Ausland die betroffene Person benachrichtigt werden sollte (Rn. 109 f.);
- die Bündelung und Vereinheitlichung der Regelungen über die **gerichtliche Zuständigkeit** und das gerichtliche Verfahren in Art. 92 PAG-E (Rn. 119);
- die neu geschaffene Möglichkeit der **Auferlegung von Kosten** bei Gemengelagen nach Art. 93 S. 2 PAG-E (Rn. 120);
- die neu geschaffenen Regelungen zu **Opferschutzmaßnahmen** in Art. 94 PAG-E (Rn. 120).

124

In einigen Punkten erkennt der Gesetzentwurf außerdem in begrüßenswerter Weise Änderungsbedarf, ohne diesen aber durchgängig sachgerecht umzusetzen. Dies betrifft

- die Erstreckung der Durchsuchung auf **räumlich getrennte Speichermedien** bzw. Kommunikationseinrichtungen nach Art. 22 Abs. 2, Art. 25 Abs. 3 und Art. 42 Abs. 1 S. 2 PAG-E (Rn. 14 ff., 21, 67);
- die Umsetzung der durch die Richtlinie (EU) 2016/680 und des Grundsatzes der hypothetischen Datenneuerhebung veranlassten **Ausweitung des Datenschutzes** im PAG in systematischer Hinsicht (Rn. 23 - 28, 90, 102, 106, 108, 111);
- die Regelung **besonderer Mittel der Datenerhebung** in Art. 36 PAG-E (Rn. 40 - 46);
- die Regelung der Befugnisse von **Internetermittlern** in Art. 37 Abs. 4 S. 1 und 3 PAG-E (Rn. 48);

- die Regelung des besonderen Schutzes von **Berufsgeheimnisträgern** in Art. 41 Abs. 2 S. 2 und Art. 49 Abs. 2 und des **Kernbereichsschutzes** in Art. 49 Abs. 3 PAG-E (Rn. 60, 96, 98);
- die **Weiterverarbeitung**, insbesondere Zusammenführung bereits erhobener personenbezogener Daten (Rn. 87 f., 90 f., 104, 106, 113, 114).

Die Notwendigkeit der Regelung der sog. Funkzellenabfrage und des stealth ping-Verfahrens („stille SMS“) wird nicht gesehen (Rn. 74).

125

Andererseits ist zu monieren, dass der Entwurf insgesamt eine Ausgewogenheit von Eingriffen in Freiheitsrechte und den davon zu erwartenden Gewinnen für die innere Sicherheit vermissen lässt. Die Grenzen des verfassungsrechtlich Zulässigen werden fast durchgehend ausgereizt und vielfach überschritten. Aussagen des BVerfG, die eine behutsame Öffnung der Verfassung für sicherheitspolitische Belange enthalten, werden in Art einer „feindlichen Übernahme“ aus dem Zusammenhang genommen und verallgemeinert, um Befugniserweiterungen den Anschein verfassungsrechtlicher Legitimität zu verleihen. Dies trifft insbesondere auf die starke Ausweitung der polizeilichen Befugnisse im Gefahrenvorfeld zu, obwohl die entsprechenden Äußerungen des BVerfG sich ausschließlich auf informationelle Maßnahmen zum Zweck der Terrorismusbekämpfung beziehen. Als verfassungsrechtlich in hohem Maße bedenkliche bzw. nicht mehr verfassungsgemäße Änderungen sind zu nennen

- die in Art. 14 Abs. 3 PAG-E neu geschaffene Möglichkeit der Feststellung des **DNA-Identifizierungsmusters** als Mittel der erkennungsdienstlichen Behandlung (Rn. 7 f.);
- die in Art. 15 Abs. 3 PAG-E neu geschaffene Möglichkeit der zwangsweisen **Durchsetzung des Erscheinens** einer Person bei der Polizei, um Angaben entgegenzunehmen, die für die Abwehr einer „drohenden Gefahr“ erforderlich sind (Rn. 9 f.);
- die neu geschaffene **Meldeanordnung** nach Art. 16 Abs. 2 S. 2 PAG-E (Rn. 11);
- die Absenkung der Eingriffsschwelle für die **Sicherstellung**, insbesondere auch auf **Vermögensrechte**, nach Art. 25 PAG-E (Rn. 19 ff.);
- die Zulässigkeit von **Bildaufnahmen wegen Größe oder Unübersichtlichkeit** der Örtlichkeit nach Art. 33 Abs. 1 Nr. 2 PAG-E (Rn. 30 f.);
- die Ermöglichung der Verwendung **automatischer Erkennungs- und Auswertungssysteme** unter den in Art. 33 Abs. 5 PAG-E genannten Voraussetzungen (Rn. 33 f.);
- die Erweiterung der Verwendungsmöglichkeit aus einer **elektronischen Aufenthaltsüberwachung** gewonnener Daten nach Art. 34 i. V. m. Art. 48 Abs. 1 Hs. 2 und Art. 36 Abs. 1 Nr. 2 lit. a) PAG-E (Rn. 35, 41);
- die Schaffung einer Befugnis zur **Postbeschlagnahme** in Fällen drohender Gefahr nach Art. 35 Abs. 1 S. 1 Nr. 1 PAG-E (Rn. 36);

- der Verzicht auf einen Richtervorbehalt in Fällen **längerfristiger Observationen** nach Art. 36 Abs. 1 Nr. 2 lit. b) PAG-E (Rn. 42);
- die Zulässigkeit der heimlichen **Überwachung des gesprochenen Worts** außerhalb von Wohnraum ohne besondere Anordnungsvoraussetzungen nach Art. 36 Abs. 1 Nr. 2 lit. c) PAG-E (Rn. 43);
- die Erstreckung besonderer Mittel der Datenerhebung auf „**Kontakt- und Begleitpersonen**" nach Art. 36 Abs. 2 Nr. 2 PAG-E (Rn. 44);
- der Verzicht auf erhöhte Anordnungsvoraussetzungen für den Einsatz besonderer Mittel der Datenerhebung **gegen nicht verantwortliche Personen** nach Art. 36 Abs. 2 Nr. 3 PAG-E (Rn. 45);
- die Zulässigkeit des Einsatzes **automatisierter Kennzeichenerfassungssysteme** jedenfalls in Fällen lediglich drohender Gefahr nach Art. 39 i. V. m. Art. 13 Abs. 1 Nr. 1 lit. b) PAG-E (Rn. 50 f.);
- die Absenkung der Voraussetzungen für eine **Ausschreibung zur polizeilichen Beobachtung** nach Art. 40 PAG-E (Rn. 52 - 56);
- die Absenkung der Voraussetzungen für eine **Wohnraumüberwachung** und die dortige Ausgestaltung des Kernbereichsschutzes nach Art. 41 PAG-E (Rn. 58 f.);
- die Ermöglichung der **Telekommunikationsüberwachung** jedenfalls in Fällen lediglich drohender Gefahr nach Art. 42 Abs. 1 S. 1 Nr. 1 PAG-E (Rn. 64 - 66);
- die Schaffung einer **Betretungs- und Durchsuchungsbefugnis** für Wohnungen zum Zweck der Durchführung einer Telekommunikationsüberwachung und einer Online-Durchsuchung nach Art. 44 Abs. 5 S. 3 und Art. 45 Abs. 3 S. 5 PAG-E (Rn. 78, 85);
- die Ermöglichung der **Online-Durchsuchung** jedenfalls in Fällen lediglich drohender Gefahr nach Art. 45 Abs. 1 S. 1 Nr. 1 PAG-E (Rn. 79 - 81);
- die Absenkung der Voraussetzungen für die **Datenlöschung** und Ermöglichung der **Datenmanipulation** im Rahmen der Online-Durchsuchung nach Art. 45 Abs. 1 S. 6 PAG-E (Rn. 84);
- die Schaffung einer Befugnis zum Einsatz von **Drohnen** nach Art. 47 PAG-E, soweit deren Zweck nicht im Erstellen von Bild- und Videoaufnahmen liegt (Rn. 89);
- die Neuregelung von **Ermittlungsersuchen an inländische Nachrichtendienste** nach Art. 60 Abs. 3 PAG-E im Lichte der Ausweitung der polizeilichen Befugnisse ins Gefahrenvorfeld (Rn. 112);

– die Ermöglichung des Einsatzes von (auch bewaffneten) **Drohnen** zur Anwendung unmittelbaren Zwangs nach Art. 78 Abs. 3 PAG-E (Rn. 116).

Eine **Gesamtbilanz** der beträchtlich erweiterten Befugnisse der Bayerischen Polizei fällt in hohem Maße verfassungsrechtlich bedenklich aus (Rn. 121 f.).

126

Darüber hinaus ist der Gesetzentwurf im Kontext der generellen Ausweitung sicherheitsbehördlicher Befugnisse zu sehen. Die gegenständlichen Weiterungen werden flankiert von weiteren eingriffsintensiven Änderungen im Bereich der Nachrichtendienste und der Strafverfolgung (vgl. Rn. 1). Der unterschiedliche Aufgabenzuschnitt der Behörden in den jeweiligen Bereichen wird dabei zugunsten einer möglichst weiten Ausdehnung der jeweiligen Befugnisse ausgeblendet. Je höher die „Gesamtbilanz" der hoheitlichen Eingriffsbefugnisse ausfällt, desto kritischer ist aber bei jeder Verschärfung des Sicherheitsrechts zu fragen, ob bei einer Gesamtbetrachtung noch die Grenze des Zumutbaren gewahrt ist. Diese Grenze kann freilich nicht absolut definiert werden, sondern nur relativ zu den aktuellen sicherheitspolitischen Erfordernissen. Diesbezüglich bleibt der Gesetzentwurf - wie schon das Gesetz vom 24.07.2017 - im Ungefähren, indem die erheblichen Befugniserweiterungen pauschal mit dem Hinweis auf eine gesteigerte Bedrohungslage gerechtfertigt werden, ohne diesen Befund rechtstatsächlich zu untermauern. Dass der Entwurf einen vermeintlichen Bedarf polizeilicher Befugniserweiterungen unterlegt, obwohl Bayern nach offiziellen Bewertungen seit vielen Jahren das sicherste Bundesland sei und über die effektivsten polizeilichen Befugnisse verfüge[226], stellt einen grundlegenden Selbstwiderspruch dar. Unverzichtbar ist als Grundlage derartig weit reichender Ausdehnungen und Umstrukturierungen des Polizeirechts, wie der Entwurf sie beabsichtigt, eine substanzielle rechtstatsächliche Kenntnis von Defiziten und Bedarfen der polizeilichen Praxis angesichts einer nachweislich veränderten Sicherheitslage. In den Worten von *Friedrich Schoch* in einer ausgewogenen Analyse aus der Zeit des beginnenden „Abschieds vom Polizeirecht des liberalen Rechtsstaats": *„Ohne eine dem Sachanliegen gerecht werdende Realanalyse verfehlt die rechtliche Problembewältigung ihr Ziel, das doch in der Herstellung praktischer Konkordanz liegen muss. Deshalb müssen wir uns Klarheit darüber verschaffen, dass es unter den gegebenen Umständen auf der einen Seite nicht (mehr) um die vollständige staatliche Garantie von Sicherheit gehen kann, sondern nur noch um die (möglichst weit gehende) Reduktion von Unsicherheit. Auf der anderen Seite ist nicht zu leugnen, dass z. B. die Terrorismusbekämpfung selbstverständlich ein Stück ‚Überwachungsstaat' erfordert. Und als Garant relativer Sicherheit ist der Staat notwendigerweise auf erfolgreiche Prävention angewiesen. Dies wiederum setzt, will man nicht naiv sein, staatliche Informationsvorsorge, d. h. ‚Vorfeldaktivitäten' der Po-*

[226] Vgl. Pressemitteilung Nr. 33/2018 des Bayerischen Staatsministers *Joachim Herrmann* vom 07.02.2018: „Bayern hat schon jetzt das effektivste Polizeirecht in ganz Deutschland. Mit unserem Gesetzespaket bauen wir diese bundesweite Spitzenposition jetzt noch weiter aus."; vgl. auch die laut PKS seit Jahren konstant hohe Aufklärungsquote in Bayern,

lizei voraus."[227] Dieser Befund trifft heute nicht minder zu. Eine entsprechende Realanalyse und ein Bemühen um praktische Konkordanz, also Ausgewogenheit, lässt der Entwurf nicht erkennen.

127

Schließlich ist in diesem Zusammenhang zu bemängeln, dass der Gesetzentwurf einer Ordnungsidee, wie in Zukunft Veränderungen der Sicherheitslage Rechnung getragen werden kann, ohne die Freiheit der Bürgerinnen und Bürger über Gebühr zu gefährden, entbehrt. Dem Entwurf lässt sich kein perspektivischer Ansatz entnehmen, sein Konzept erschöpft sich in einer weitgehendsten Ausdehnung polizeilicher Befugnisse auf Kosten der Freiheitsrechte. Eine moderne Sicherheitspolitik sollte sich demgegenüber an der Idee orientieren, ihre Ressourcen auf die Verhütung und Bekämpfung schwer wiegender Bedrohungen, Gefahrenlagen und Formen der Kriminalität zu konzentrieren, statt einem Paradigma größtmöglicher Sicherheit bei größtmöglicher Überwachung und Steuerung der Bevölkerung zu folgen. Dies beinhaltet einerseits das Gebot einer möglichst effizienten Koordination und Kooperation der diversen Sicherheitsbehörden im Sinne einer arbeitsteiligen Vorgehensweise. Durch einen bereichsspezifischen Zuschnitt der jeweiligen Befugnisse würde zugleich dem Trennungsgebot in seinen verschiedenen Dimensionen Rechnung getragen.[228] Andererseits impliziert die Idee einer effektiven und zugleich grundrechtsschonenden Ausgestaltung des Sicherheitsrechts, dass Eingriffe möglichst zielgerichtet erfolgen müssen. Darin liegt, bezogen auf informationelle Maßnahmen, zugleich - entsprechend dem Grundsatz der Datensparsamkeit - die effektivste Form des Schutzes informationeller Selbstbestimmung. Der möglichst zielgerichtete Einsatz hoheitlicher Befugnisse setzt neben einem funktionierenden Datenaustausch der Sicherheitsbehörden untereinander sowie leistungsfähigen Analysemöglichkeiten auch die Gewinnung von interdisziplinärem und empirisch fundiertem Grundlagenwissen über Chancen und Risiken moderner Formen der Datenverarbeitung für das Sicherheitsrecht voraus.[229] Derlei Perspektiven lässt der Gesetzentwurf vermissen. Stattdessen folgt er einer nicht mehr zeitgemäßen Philosophie möglichst flächendeckender Überwachung und quantitativer Optimierung der Datenerhebung. Dass dieses Paradigma an rechtliche und tatsächliche Grenzen stößt und deshalb ein Beschreiten neuer Wege erforderlich ist, belegt nachdrücklich die verfahrene Lage im Bereich der sog. „Vorratsdatenspeicherung".[230]

---

https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2016/InteraktiveKarten/01StraftatenInsgesamt/01_StraftatenInsgesamt_node.html.

[227] *Schoch*, Der Staat 2004, 347, 365 f.

[228] Zur Notwendigkeit eines „ganzheitlichen Konzepts" als Folge des Trennungsgebots und der aktuellen sicherheitspolitischen Herausforderungen ausf. *Streiß*, insbes. S. 137 ff., 231 ff., 235 ff.; zum komplementären Charakter von Trennung, Koordination und Kooperation *Dietrich*, in Dietrich/Eiffler, Teil III § 3 Rn. 35 ff.

[229] Vgl. *Gärditz*, Sicherheitsrecht als Perspektive, GSZ 2017, 1, 3.

[230] Vgl. dazu *Löffelmann*, GSZ 2017, 38 ff.

IV. Handlungsempfehlungen

128

Abschließend wird empfohlen,

1. im Dialog mit Polizei und anderen Sicherheitsbehörden und, falls möglich, unter wissenschaftlicher Begleitung, deren tatsächliche Bedarfe zu eruieren;
2. im Dialog mit Rechtswissenschaft und Praxis und unter Berücksichtigung der sicherheitspolitischen Zielsetzungen im Bund und den Ländern Konzepte für ein modernes und ausgewogenes Sicherheitsrecht zu entwickeln, das der Digitalisierung der Lebenswirklichkeit und den damit einhergehenden sozialen, kulturellen und technischen Veränderungen im Umgang mit personenbezogenen Daten gerecht wird;
3. im Falle des Inkrafttretens des Gesetzes die Möglichkeit einer Rechtssatzverfassungsbeschwerde zum BVerfG zu prüfen, wobei der Umstand, dass zahlreiche Weiterungen im Bereich von Überwachungsmaßnahmen mit hoher Streubreite zu erwarten sind, insoweit eine Beschwerdebefugnis begründen dürfte.

C. Literatur (Kommentare und Monografien):

Albers, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2001.

Beck-Online Kommentar, Polizei- und Sicherheitsrecht Bayern, Hrsg. Möstl/Schwabenbauer, 7. Edition, Stand: 1.1.2018 (zit. BeckOK BayPAG).

Biemann, „Streifenfahrten" im Internet. Die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum, 2013.

Böckenförde, Die Ermittlung im Netz, 2003.

Dietrich/*Eiffler* (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017.

Fischer, Strafgesetzbuch, 65. Aufl. 2019.

Jarass/*Pieroth*, Grundgesetz für die Bundesrepublik Deutschland: GG, Kommentar, 13. Aufl. 2014.

Jahn/*Krehl*/*Löffelmann*/*Güntge*, Die Verfassungsbeschwerde in Strafsachen, 2. Aufl. 2017.

Kral, Die polizeilichen Vorfeldbefugnisse als Herausforderung für Dogmatik und Gesetzgebung des Polizeirechts. Begriff, Tatbestandsmerkmale und Rechtsfolgen, 2012.

Lisken/*Denninger*, Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 5. Aufl. 2012.

Löffelmann, Die normativen Grenzen der Wahrheitserforschung im Strafverfahren. Ideen zu einer Kritik der Funktionsfähigkeit der Strafrechtspflege, 2008.

Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, Erb u.a. (Hrsg.), 26. Aufl. 2006 ff. und 27. Aufl. 2017.

Meyer-Goßner/*Schmitt*, Strafprozessordnung mit GVG und Nebengesetzen, 60. Aufl. 2017.

Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung. Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, 2002.

Park, Wandel des klassischen Polizeirechts zum neuen Sicherheitsrecht. Eine Untersuchung am Beispiel der Entscheidung über sogenannte Online-Durchsuchungen, 2013.

Pewestorf/*Söllner*/*Tölle*, Polizei- und Ordnungsrecht, 2. Aufl. 2017.

Pieroth/*Schlink*/*Kniesel*, Polizei- und Ordnungsrecht, 9. Aufl. 2016.

Schenke/*Graulich*/*Ruthig*, Sicherheitsrecht des Bundes, 1. Aufl. 2014.

Schmidbauer/*Steiner*, Bayerisches Polizeiaufgabengesetz und Polizeiorganisationsgesetz, 4. Aufl. 2014.

Streiß, Das Trennungsgebot zwischen Polizei und Nachrichtendiensten im Lichte aktueller Herausforderungen des Sicherheitsrechts, 2011.

Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2017.

Tegtmeyer/*Vahle*, Polizeigesetz Nordrhein-Westfalen, 11. Aufl. 2014.

Thiel, Die „Entgrenzung" der Gefahrenabwehr. Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, 2011.

Wolff/*Brink*, Datenschutzrecht in Bund und Ländern, 2013.

Wolter/*Schenke* (Hrsg.), Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen, 2002.

München, den 14. Februar 2018

Dr. Markus Löffelmann

Zur Person des Verfassers:

Dr. Markus Löffelmann ist Richter am Landgericht München I. Zuvor arbeitete er unter anderem als Staatsanwalt, Referent im Bundesministerium der Justiz und wissenschaftlicher Mitarbeiter am Bundesverfassungsgericht. Von 2008 bis 2010 leitete er das deutsche Unterstützungsvorhaben für den Aufbau des Afrikanischen Gerichtshofs für Menschenrechte und Rechte der Völker in Arusha, Tansania. Der Verfasser hat zahlreiche Publikationen, namentlich auf den Gebieten des Verfassungsrechts, Strafverfahrensrechts und Rechts der Nachrichtendienste vorgelegt, u. a. als Mitherausgeber und Mitautor des Anwaltkommentars StPO (Deutscher Anwaltverlag), des Praxishandbuchs „Die Verfassungsbeschwerde in Strafsachen" (C. F. Müller) und des „Handbuch des Rechts der Nachrichtendienste" (R. Boorberg). Er ist im Nebenamt als Lehrbeauftragter an der Hochschule des Bundes für öffentliche Verwaltung, Fachbereich Nachrichtendienste, tätig.