Gutachtliche Anmerkungen
zu den Gesetzentwürfen der Bayerischen Staatsregierung

vom 20.02.2018 zur Änderung des Bayerischen Verfassungsschutzgesetzes
(LT-Drs. 17/20763
und
vom 30.01.2018 für ein Gesetz zur Neuordnung des bayerischen Polizeirechts
(PAG-Neuordnungsgesetz (LT-Drs. 17/20425)

auf Benennung der Landtagsfraktion B.90/DIE GRÜNEN

von

RiBVerwG a.D. Prof. Dr. Kurt Graulich

Berlin, d. 14. März 2018

Vorbemerkung

Anlass der vorgelegten Stellungnahme ist die Anhörung der Ausschüsse für Kommunale Fragen, Innere Sicherheit und Sport sowie für Verfassung, Recht und Parlamentsfragen zu den Gesetzentwürfen der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts (Drs. 17/20425) und zur Änderung des Bayerischen Verfassungs-schutzgesetzes (Drs. 17/20763) am Mittwoch, den 21. März 2018 im Bayerischen Landtag. Aus Gründen der Nützlichkeit folgt die Stellungnahme dem Fragenkatalog des Bayerischen Landtags für die Ausschusssitzung.

A. PAG

1. Ist der Gesetzentwurf geeignet, die aus der Richtlinie (EU) 2016/680 erwachsenden Umsetzungserfordernisse abzubilden, insbesondere in den nachfolgend genannten Teilbereichen?

a) Wurden die Pflichten des Verantwortlichen wie beispielsweise die Hinweis- und Belehrungspflichten ausreichend umgesetzt?
Der Gesetzesentwurf steht bei der Beachtung und Umsetzung von Unionsrecht in der Gefahr der Über- oder Untererfüllung. In ihrem Bereich gilt die DS-GVO - unveränderbar und unverbesserbar - direkt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden sollen (Art. 2 Abs. 1 DSGVO). Die DS-GVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafverfolgung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 2 Abs. 2 lit. d)). Systematisch ist dies als eine Abgrenzung zum Geltungsbereich der RL 2016/680/EU zu verstehen, die wiederum den Rahmenbeschluss 2008/977/JI im Bereich von Gefahrenabwehr und Strafverfolgung ablöst. Die Richtlinie umfasst sowohl präventiv als auch repressiv erforderliche Verarbeitungsvorgänge zu den genannten Zwecken. So dass in Deutschland insbesondere die StPO und die Polizeigesetze betroffen sind. Polizeiliche Tätigkeiten ohne Bezug zu Straftaten – z.B. im Rahmen von Vermisstenanzeigen – unterfallen weiterhin der DSGVO (Kühling/Raab in Kühling/Buchner, DS-GVO Art. 2 Rn. 29).

b) Wurden die Rechte der betroffenen Person wie zum Beispiel das Recht auf Berichtigung Datenlöschung und Auskunft ausreichend umgesetzt?
An dieser systematischen Vorgabe gemessen fallen zwei Punkte im PAG-E auf, die nicht als befriedigend gelöst erscheinen. Zum einen der Umgang mit dem

Schutz privater Rechte in § 2 PAG-E und zum anderen die beibehaltene Verwendung des Instituts der datenschutzrechtlichen Errichtungsanordnung.

Der Schutz privater Rechte durch die Gefahren abwehrende Polizei fällt nicht unter die Bereichsausnahme von Art. 2 Abs. 2 lit. d) DS-GVO. Die DS-GVO gilt dort unmittelbar. Die durch den PAG-E vorgesehen Umstellung „In Abs. 2 werden die Wörter „Der Schutz privater Rechte obliegt der Polizei“ durch die Wörter „Im Rahmen ihrer Aufgabe nach Abs. 1 obliegt der Polizei der Schutz privater Rechte“ ersetzt.“ ändert daran nichts. Sie verunklart den Normwirkungszusammenhang nur.

c) Wie bewerten Sie die Tatsache, dass neben der neu eingeführten Datenschutzfolgenabschätzung in Art. 64 Gesetzentwurf PAG-Neuordnungsgesetz (nachfolgend: PAG-E) das Instrument der Errichtungsanordnung beibehalten und soweit dies rechtspraktisch möglich war, mit der Folgenabschätzung verbunden wurde?
Das Zusammenspiel von DS-GVO und RL 2016/680/EU hat dazu geführt, dass bislang fachgesetzliche Regelungen über datenschutzrechtliche Errichtungsanordnungen obsolet geworden sind. Der Bund hat daraus die Konsequenz gezogen und § 34 BKAG a.F. gestrichen (BT-Drs. 18/11163 S. 131). Das funktionale Äquivalent findet sich in dem „Verzeichnis von Verarbeitungstätigkeiten“ nach § 70 BDSG. Danach ist der Verantwortliche zur Führung eines Verzeichnisses aller Kategorien von Verarbeitungstätigkeiten verpflichtet, die in seine Zuständigkeit fallen. Das Verzeichnis nach § 70 BDSG ist nicht identisch mit der Errichtungsanordnung für Dateien, die das Fachrecht für Sicherheitsdateien vielfach kennt (Gräber/Nolden/Paal, in Paal/Pauly, 2. Aufl., BDSG § 70 Rn. 2 unter Hinw. auf BT-Drs. 18/11325 S. 118). Das PAG ist auch nicht gehindert, an dem Institut weiterhin festzuhalten, weil ihm weder die DS-GVO noch die RL entgegensteht. Es verunklart aber das Verhältnis zu dem unverzichtbaren „Verzeichnis von Verarbeitungstätigkeiten“ nach § 70 BDSG, das wiederum keine deutsche Kreation enthält, sondern Art. 24 JI-RL umsetzt.

2. Wie beurteilen Sie gemessen an den Maßgaben des BVerfG, besonders in seinem Urteil vom 20.04.2016 zum BKAG, dass Befugnisse, die tief in die Privatsphäre hineinreichen und zudem noch verdeckt erfolgen, insbesondere
• auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein müssen,
• Gefährdungen der gewichtigen Rechtsgüter hinreichend konkret absehbar sein müssen,
• die Befugnisse sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte erstrecken dürfen,
• besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und von Berufsgeheimnisträgern normiert werden müssen,

• die Befugnisse bestimmten Transparenzanforderungen unterliegen müssen,
• durch Regelungen zur Erlangung individuellen Rechtsschutzes und aufsichtlicher Kontrolle flankiert sein müssen,
• mit Löschungspflichten im Hinblick auf die erhobenen Daten ergänzt sein müssen,
die Ausgestaltung der Befugnisse im III. Abschnitt 2. Unterabschnitt PAG-E nach Art. 33 bis 47 PAG-E und erläutern Sie im Hinblick auf die Maßgaben des BVerfG im BKAG-Urteil vom 20.04.2016 bitte Folgendes:

Die Fragestellung des Ausschusses gibt in einer vorangestellten Aufzählung die wesentlichen Maßgaben des Urteils des BVerfG vom 20. April 2016 zum BKAG zutreffend wieder. Die Linearität der Liste darf allerdings nicht darüber hinwegtäuschen, dass die Maßgaben als Prüfungsmaßstäbe für Normen unterschiedlich ansetzen. Daran ändert auch nichts ihr – im Urteil - einheitlicher Ausgangspunkt im Verhältnismäßigkeitsgrundsatz.

a) Wie ist die Neugestaltung von einzelnen Befugnisnormen in folgender Hinsicht zu bewerten:
aa) Wurden die geforderten Richtervorbehalte ausreichend umgesetzt?
Es wurden zahlreiche Richtervorbehalte eingeführt. Im Falle des Kernbereichsschutzes besteht die Gefahr, dass die Zentrale Datenprüfstelle die richterliche Überprüfung aufweicht.

bb) Wie bewerten Sie die Neuausrichtung der polizeilichen Befugnisnormen hin zu einer konsequent rechtsgüterschutzorientierten Ausgestaltung bei gleichzeitiger Abschaffung der bislang enthaltenen Straftatenkataloge?

Der Richtervorbehalt bei beabsichtigten Eingriffen unter hochinvasiven Umständen oder in hochwertige Individualrechte berücksichtigt die einander ergänzenden Grundsätze der Gewaltenteilung und der Verhältnismäßigkeit. Er salviert aber nicht den gesetzlich ermöglichten Eingriff selbst. Insbesondere setzt der – meistens beim Amtsgericht liegende - Richtervorbehalt vor dem Normgebrauch an, ersetzt also nicht die anschließende Rechtmäßigkeitskontrolle – meistens durch die Verwaltungsgerichtsbarkeit.

Die rechtsgüterschutzorientierte Ausgestaltung der Befugnisnormen anstelle der bislang praktizierten Straftatenkataloge ist jedenfalls einen Versuch wert. Die Straftatenkataloge hatten ein großes Maß an Genauigkeit für sich, sind mit dem Ansatz der Anführung schützenswerten Rechtsgütern aber inhaltlich verbunden, indem die Straftatenkataloge hintergründig ebenfalls am Rechtsgüterschutz orientiert sind. Allerdings haben sie die Polizeigesetze in zunehmendem Maße unleserlich gemacht. Nun bleibt abzuwarten, ob die verminderte Genauigkeit noch innerhalb der verfassungsrechtlich

erforderlichen Bestimmtheit zu liegen kommt. Dies ist nicht offenkundig und wird – wie im Verwaltungsrecht häufig – die Rechtspraxis zeigen müssen.

b) Sehen Sie im Hinblick darauf, dass bei einigen polizeilichen Befugnissen – z.B. bei der neu geschaffenen Befugnis der Postsicherstellung (Art. 35 PAG-E), aber auch bei den bereits bisher im PAG bestehenden Befugnissen „Eingriffe in den Telekommunikationsbereich" (Art. 42 PAG-E) und „Verdeckter Zugriff auf informationstechnische Systeme (vgl. Art. 45 PAG-E) - der mit dem Gesetz zur effektiveren Überwachung gefährlicher Personen zum 01.08.2018 in das PAG aufgenommene Gefahrenbegriff der drohenden Gefahr eingeführt wird, eine Herabsetzung der polizeilichen Eingriffsschwelle und wie bewerten Sie dies verfassungsrechtlich?
Die „drohende Gefahr" verlegt die Gefahrenprognose i.U. zur „konkreten Gefahr" weiter nach vorne. Dies kann der Sache nach angemessen sein und ist unter Beachtung bestimmter Voraussetzungen verfassungsrechtlich zulässig. Nach der Rspr. des BVerfG ist der Gesetzgeber von Verfassungs wegen nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen für bestimmte Bereiche mit dem Ziel schon der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert. Allerdings müssen die Eingriffsgrundlagen auch dann eine hinreichend konkretisierte Gefahr in dem Sinne verlangen, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen (vgl. BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>). Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 112).

c) Wie ist die Ausgestaltung der hypothetischen Datenneuerhebung zu bewerten? (Art. 48 PAG-E)

Das Bundesverfassungsgericht hat in seinem Urteil zum BKAG festgestellt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung und sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigung für die Datenerhebung richten. Die Datenerhebung selbst bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren Die Ermächtigung zu einer Zweckänderung ist dabei am Verhältnismäßigkeitsgrundsatz zu messen. Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken benutzt werden (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 286). Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit schwerwiegenden Mitteln erhoben werden dürften.

Der Regelungsentwurf in Art. 48 PAG-E unternimmt die Positivierung des Grundsatzes der hypothetischen Datenneuerhebung, geht dabei aber nicht sehr übersichtlich vor. Dies liegt – vom Gesetzgeber nicht zu vertreten – an der komplizierten Materie. Zu vertreten hat der Entwurf aber die Undeutlichkeit durch inzidente Verweisungen. Es werden zu häufig Voraussetzungen für polizeiliche Befugnisse nicht genannt, sondern in Verweisungsirrgärten versteckt. Dies darf nicht zum Problem des Rechtspflichtigen werden. Daher ist es als Verstoß gegen den rechtsstaatlichen Grundsatz Normklarheit dem Gesetzgeber anzulasten.

Unter diesen Voraussetzungen ist zumindest die Regelung in Art. 48 Abs. 4 PAG-E nicht überzeugend. Dort geht es in Satz 1 um die Verarbeitung von Daten, die (Nr. 1) durch den Einsatz technischer Mittel in Wohnungen und (Nr. 2) durch den verdeckten Zugriff auf informationstechnische Systeme erhoben wurden. Deren Weiterverwendung ist nach dem vorgenannten Urteil eng begrenzt. Hier ist jede weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 283). Die Neufassung

das BKAG berücksichtigt diese Begrenzungsanforderung in § 12 Abs. 3 BKAG, während sie in Art. 48 Abs. 4 PAG-E fehlt.

d) Wie bewerten Sie die Ausgestaltung der polizeilichen Befugnisse in Art. 33 bis 47 PAG-E im Hinblick auf die rechtsstaatlichen Gebote der Normenklarheit und Bestimmtheit?

Postbeschlagnahme nach Art. 35 PAG-E
Bislang war der Satz richtig: Die allgemeinen Polizeigesetze legitimieren nicht zu Eingriffen in das Brief- und Postgeheimnis. Die Verhältnisse haben sich aber geändert. Denn seit der Novellierung des BKAG im Jahr 2017 gehört zu den – verdeckten - polizeilichen Befugnissen auch die **Postbeschlagnahme**. Sie ist – trotz der traditionell wirkenden Art der Maßnahme - eingeführt worden, weil terroristische Tätergruppen verstärkt auf das Mittel konventioneller Postsendungen in bestimmten Bereichen ihrer Kommunikation zurückgreifen (vgl. Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 759 ff.). An die Regelung in § 50 BKAG lehnt sich Art. 35 PAG-E eng an. Auch für die Verbringung von logistischen Gütern erlangt der Postweg nach Einschätzung der Bundesregierung zunehmende Bedeutung gegenüber den bisher praktizierten persönlichen Übergaben (BT-Drs. 18/11163, 119 BT-Drs. 18/11163, 119). Die Polizei kann in diesen Fällen nach der nunmehr geschaffenen Befugnis ohne Wissen der betroffenen Person zu präventiven Zwecken **Postsendungen und Telegramme beschlagnahmen**, die sich im Gewahrsam von Personen oder Unternehmen befinden, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder daran mitwirken und die an eine Person gerichtet sind, welche bestimmte Störervoraussetzungen erfüllt (vgl. zB § 50 Abs. 1 BKAG). Inhaltlich lehnt sich die Regelung in § 50 BKAG wiederum an die §§ 99 und 100 StPO an (BR-Drs. 109/17, 139).

Eingriffe in die Inhalte der Telekommunikation
Quellen-TKÜ (Art. 42 PAG-E)
Ein besonders schwerer Eingriff in die Inhalte der Telekommunikation wird durch die sog. Quellen-TKÜ ermöglicht, die bereits mit dem Gesetz vom 24. Juli 2017 (GVBl. S. 388) durch Einfügung von Art. 34a Abs. 1a PAG unternommen wurde; die Regelung soll nunmehr zu Art 42 Abs. 2 werden. Bei der Quellen-Telekommunikationsüberwachung wird ein fremdes informationstechnisches System infiltriert, um mit einer eigens für diesen Zweck entwickelten Überwachungssoftware die Kommunikation zwischen den Beteiligten überwachen und aufzeichnen zu können (BT-Drs. 18/12785 S. 51). Die nunmehr beabsichtigte Änderung von Art. 42 Abs. 1 PAG-E versucht einem rechtlich-technologischen Dilemma zu entkommen, das weder im BKAG noch in der StPO vollständig gelöst ist. An Art. 10 Abs. 1 GG ist nicht nur die traditionelle Telekommunikationsüberwachung zu messen, (z.B. nach § 51 Abs. 1 BKAG), sondern auch solche Regelungen, welche die präventive Quellen-

Telekommunikationsüberwachung erlauben (z.B. Art. 42 Abs. 2 PAG-E, § 51 Abs. 2 BKAG), sofern durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird (Graulich in Arndt/Fetzer/Scherer/Graulich, TKG § 88 Rn. 52). Zwar setzt diese technisch einen Zugriff auf das entsprechende informationstechnische System voraus, jedoch erlaubt die polizeiliche Befugnis (z.B. § 51 Abs. 2 BKAG) ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Die Vorschrift hat damit lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und - ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems - eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Von daher ist sie nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern an Art. 10 Abs. 1 GG zu messen (BVerfGE 141, 220 (Rn. 228)). Es ist in der öffentlichen Diskussion angezweifelt worden, ob sich bei der Quellen-TKÜ der Eingriff auf die laufende Telekommunikation beschränken lässt. Das BVerfG hat diesen Umstand abgewogen und im Ergebnis verfassungsrechtlich nicht für erheblich gehalten. Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Befugnisnorm, nicht aber ihre Gültigkeit. Insoweit hat es das BVerfG nicht als Aufgabe des anhängigen Verfahrens angesehen, hierüber eine Klärung herbeizuführen. Das geprüfte Gesetz (§ 20l BKAG a.F.) ließ jedenfalls keinen Zweifel, dass eine Quellen-TKÜ nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt war (heute § 51 BKAG). Andernfalls wäre ein Vorgehen nicht auf der Grundlage der Befugnis zur Teklekommunikationsüberwachung des § 20l BKAG a.F. in Betracht gekommen, sondern nur auf derjenigen zur Online-Durchsuchung in § 20 k Abs. 1 BKAG a.F. (heute § 49 BKAG).

Sollten diese Anforderungen – aus tatsächlichen Gründen - nicht erfüllbar sein, liefe die Vorschrift folglich bis zum Zeitpunkt der technischen Realisierbarkeit leer. Eine Ermächtigung zur Telekommunikationsüberwachung deckt für sich genommen nämlich keine Quellen-Telekommunikationsüberwachung, bei der ein komplexes Endgerät infiltriert wird, um die überwachte Kommunikation mitzuschneiden (so zutr. Bäcker, Kriminalpräventionsrecht, S. 259). Auch dies macht eine entsprechende Befugnis jedoch nicht widersprüchlich und verfassungswidrig, weil damit nicht ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können. Dabei schließt der für die Quellen-TKÜ erforderliche Zugriff auf das informationstechnische System eine Erfüllung derartiger Voraussetzungen auch nicht etwa schon begrifflich aus mit der Folge, dass die Vorschrift selbstwidersprüchlich wäre. Denn maßgeblich ist nicht, ob durch eine technisch

aufwendige Änderung des Überwachungsprogramms selbst - sei es durch die Behörde, sei es durch Dritte - dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden kann, sondern ob das Programm so ausgestaltet ist, dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern des BKA inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 771 unter Hinw. auf BVerfGE 141, 220 (Rn. 234).

Eingriffe in die technischen Umstände der Telekommunikation
Verkehrsdaten (Art. 43 PAG-E)
Die Begrifflichkeit bei den Regelungen über Verkehrsdaten ist nicht einheitlich. In Art. 43 Abs. 1 PAG wird auf § 96 Abs. 1 TKG Bezug genommen. In Art. 43 Abs. 3 PAG-E – seither Art. 34b Abs. 3 PAG - wird dafür eine eigene landesrechtliche Definition angeführt. Dieses Problem hat im Verhältnis von nationalen und unionalen Vorschriften Tradition, weil sich der Begriff Verkehrsdaten erst gegenüber dem der – dasselbe meinenden – Verbindungsdaten durchsetzen musste (Graulich in Arnd/Fetzer/Scherer/Graulich, 2. Aufl, TKG § 113 Rn. 9). Es wäre besser, auf eine landesgesetzliche Umschreibung des Begriffes zu verzichten und sich ausschließlich auf die Definition in § 96 Abs. 1 TKG abzustützen, die ohnehin gegenüber den TK-Dienstleistern die vorrangige ist.

Online-Durchsuchung (Art. 45 PAG-E)
Bei der Regelung der sog. Online-Überwachung folgt der Entwurf möglichst eng der Vorgabe des BVerfG und verwendet den Begriff der „drohenden Gefahr“ anstelle der „konkreten Gefahr. Der Zugriff auf informationstechnische Systeme - und auch die Wohnraumüberwachung - dürfen sich unmittelbar nur gegen diejenigen als Zielpersonen richten, die für die drohende oder dringende Gefahr verantwortlich sind. Verfassungsrechtlich nicht zu beanstanden ist allerdings, wenn die gegen die Verantwortlichen angeordneten Maßnahmen, soweit unvermeidbar, auch Dritte miterfassen (BVerfGE 141, 220). Ganz überwiegend wird von den Polizeigesetzen gesehen, dass bei heimlichen Ermittlungsmaßnahmen oft auch „Dritte unvermeidbar betroffen werden“ (zB Art. 33 Abs. 4 BayPAG; § 34 Abs. 1 S. 2 NdsSOG; § 39 Abs. 7 S. 1 SächsPolG). Für diesen Fall wird die Datenerhebung ebenfalls erlaubt. Dritte sind Personen, die erkennbar in keiner Beziehung zum anlassgebenden Sachverhalt stehen und gegen die Maßnahme deshalb nicht gerichtet ist. Es kann sich dabei um Nachbarn handeln, die sich bei der Zielperson gelegentlich etwas borgen, um Passanten, Inhaber von Ladengeschäften, welche die Zielperson frequentiert, Kinder der Zielperson und deren Freunde sowie deren Eltern. Informationen über diese Personen sind für die vorbeugende Straftatenbekämpfung regelmäßig nicht erforderlich. Deshalb ist die Datenerhebung insoweit nur

zulässig, wenn andernfalls der Zweck des Einsatzes gefährdet oder gar vereitelt würde. Sind von einer Maßnahme ausschließlich Dritte betroffen, sind die Daten zu löschen oder die Datenträger zu vernichten (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 698).

e) Wurden die Maßgaben des BVerfG zum Kernbereichs- und Berufsgeheimnisträgerschutz ausreichend umgesetzt?
Mit Einschränkungen, ja.

f) Ist die Aufhebung der Unterscheidung innerhalb der Berufsgeheimnisträger in Art. 49 PAG-E zwingend erforderlich oder kann der Entscheidung des Bundesverfassungsgerichts und der Datenschutzgrundverordnung auch dadurch Folge geleistet werden, dass eine Ausgestaltung des Art. 49 PAG-E entsprechend § 160a StPO bzw. § 62 BKAG-neu erfolgt?
Beides geht.

g) Halten Sie eine besondere Rechtsgrundlage für die Maßnahme der Funkzellenabfrage für erforderlich (Art. 44 PAG-E)?

Die Funkzellenabfrage greift in das Fernmeldegeheimnis ein und bedarf daher einer Rechtsgrundlage und steht unter Richtervorbehalt. Dies ist im präventiven Bereich des BKAG ebenso anerkannt wie im repressiven der StPO. Dies ergibt sich aus dem technisch-inhaltlichen Vorgang dieser Maßnahme. Eingeschaltete Mobiltelefone melden sich automatisch in der jeweils nächsten der über das gesamte Bundesgebiet verteilten Funkzellen an, um erreichbar zu sein. Bei den Funkzellen werden durch die Provider die Daten aller Mobilfunkgeräte, die während eines bestimmten Zeitpunkts in einer bestimmten Region geführt wurden, erfasst und gespeichert, so dass diese Daten später beispielsweise durch eine Strafverfolgungsbehörde ausgewertet werden können (Graulich in Arndt/Fetzer/Scherer/Graulich, TKG § 88 Rn. 60). Bei diesen handelt es sich nicht um Standortdatenerhebungen; vielmehr werden bei einer solchen Abfrage alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren (BT-Drs. 18/5088, 32).

Grundlage des Ermittlungsinstruments im repressiven Bereich des Strafverfahrens sind § 100 g Abs. 2 S. 2, § 100 h StPO. Als Form der Verkehrsdatenabfrage handelt es sich um eine Überwachung der Telekommunikation im engeren Sinn. Es werden notwendigerweise die Verkehrsdaten all der Personen, die sich zum fraglichen Zeitpunkt bei der überprüften Funkzelle eingeloggt haben, erfasst (Graulich in Arndt/Fetzer/Scherer/Graulich, TKG § 88 Rn. 60). Nach der Legaldefinition in §

100 g Abs. 3 S. 1 StPO ist eine Funkzellenabfrage die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten. Die Funkzellenabfrage erlaubt in nicht individualisierter (Bäcker, Kriminalprävention, S. 303) Form den Zugriff auf Verkehrsdaten bei einer räumlich und zeitlich hinreichend bestimmten Bezeichnung der Kommunikation. Sie besteht in der Abfrage und Analyse der Daten der über einen bestimmten Zeitraum in einer Funkzelle angemeldeten Mobilfunkendgeräte. Durch Funkzellenabfragen werden regelmäßig unvermeidbar Verkehrsdaten Dritter, namentlich solcher Personen erhoben, die – ohne Beschuldigte oder Nachrichtenmittler zu sein – in der abgefragten Funkzelle mit ihrem Mobiltelefon kommuniziert haben. Verkehrsdaten Unbeteiligter dürfen nicht über das zur Strafverfolgung unerlässliche Maß hinaus erhoben werden. Zu diesem Zweck wird die Funkzellenabfrage legal definiert und die strenge Subsidiaritätsklausel des § 100 a Abs. 1 Nr. 3 StPO übernommen. Außerdem muss die Funkzellenabfrage wie bisher die zu erfassende Telekommunikation räumlich und zeitlich eng begrenzt und hinreichend bestimmt bezeichnen. Damit wird die Erstellung von Bewegungsprofilen unbescholtener Bürgerinnen und Bürger wirksam verhindert (BT-Drs. 18/5088, 24).

Die Funkzellenauswertung ist eine richterlich angeordnete Maßnahme (§ 101 a Abs. 1 iVm § 100 g, § 100 a Abs. 3 und § 100 b Abs. 1 bis 4 StPO), die Auskunft über gespeicherte Verkehrsdaten in einer Mobilfunkzelle der Mobilnetzbetreiber gibt. Diese Verkehrsdaten umfassen die Aufzeichnung der Netzbetreiber, welche Mobilfunkendgeräte in der Zelle im ermittlungsrelevanten Zeitraum eingebucht waren. Von den Netzbetreibern werden dabei nur aktiv gewordene (z.B. durch Telefonate, SMS) Endgeräte erfasst. Bei Funkzellenabfragen nach § 100 g Abs. 3 genügt gem. § 101 a Abs. 1 S. 3 StPO abweichend von § 100 b Abs. 2 S. 2 Nr. 2 StPO eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation. Ein gesetzlich besonders geregelter Fall der Standortermittlung besteht bei Notrufverbindungen (§ 108 TKG). Nach § 108 Abs. 1 S. 3 Nr. 2 TKG haben die TK-Dienstleister sicherzustellen, dass der Notrufabfragestelle auch die Daten übermittelt werden, die zur Ermittlung des Standortes erforderlich sind, von dem der Notruf ausgeht (Vgl. auch zu den europarechtlichen Anforderungen Graulich in Arndt/Fetzer/Scherer/Graulich, TKG § 108 Rn. 13 ff.). Eine Befugnis für Funkzellenabfragen durch das BKAG befindet sich in § 52 Abs. 3 S. 2 BKAG und steht unter Richtervorbehalt (§ 52 Abs. 3 S. 1 iVm § 51 Abs. 3 S. 1 BKAG) (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 698 ff.). Dem passt das PAG sich an.

h) Sind die vom BVerfG statuierten Unterrichtungspflichten ausreichend abgebildet?

Prima facie ja.

i) Wie bewerten Sie allgemein die Einrichtung einer „Zentralen Datenprüfstelle“ als unabhängige Stelle zur Vermeidung von Kernbereichsverletzungen (Art. 41 Abs. 5, 42 Abs. 7, Art. 45 Abs. 4 und Art. 53 Abs. 3 PAG-E; Art. 13 f. POG-E)?
Es ist zu befürchten, dass die Konstruktion einer Zentralen Datenprüfstelle die gebotene unverzügliche Einschaltung eines Gerichts bei der Gefahr von Kernbereichsverletzungen unangemessen verzögert. Das neue BKAG geht daher einen anderen Weg: Das Bundesverfassungsgericht macht in seinem Urteil vom 20. April 2016 detaillierte Vorgaben für den Schutz des Kernbereichs der privaten Lebensgestaltung und weitet den Richtervorbehalt aus. Insbesondere aus der Verpflichtung, sämtliche Erkenntnisse aus Onlinedurchsuchungen und Wohnraumüberwachungen dem anordnenden Gericht vorzulegen, muss sichergestellt werden, dass Daten unverzüglich dem anordnenden Gericht vorgelegt werden, damit dieses unverzüglich über die Verwertbarkeit oder Löschung der Daten entscheiden kann (BT-Drs. 18/11163 S. 88).

aa) Ist es nach den Vorgaben des BVerfG möglich, die geforderte Sichtung der Daten einer solchen Stelle zu übertragen, die nicht bei der Judikative angesiedelt ist?
Die Frage lässt sich im Lichte der Rechtsprechung des BVerfG mit einem „es kommt darauf an“ beantworten. Der Kernbereichsschutz ist nach dem Bundesverfassungsgericht auf zwei Ebenen Rechnung zu gewährleisten. Zum einen sind auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zum anderen sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 126). In diesem Rahmen kann der Gesetzgeber den Schutz des Kernbereichs privater Lebensgestaltung in Abhängigkeit von der Art der Befugnis und deren Nähe zum absolut geschützten Bereich privater Lebensgestaltung für die verschiedenen Überwachungsmaßnahmen verschieden ausgestalten (vgl. BVerfGE 120, 274 <337>; 129, 208 <245>). Er hat hierbei jedoch auf beiden Ebenen Vorkehrungen zu treffen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 127).

bb) Wie bewerten Sie die konkrete Ausgestaltung der Unabhängigkeit?
Die Unabhängigkeit der „Zentralen Datenprüfstelle“ ist schwach ausgeprägt. Sie betrifft im Wesentlichen nur den Leiter der Einrichtung. Soweit die weiteren Bediensteten an Entscheidungen beteiligt sind, fehlt ihnen die Unabhängigkeit weitestgehend.

cc) Wie bewerten Sie die vorgesehene Möglichkeit, polizeilichen Sachverstand hinzuziehen zu können (vgl. Art. 13 Abs. 4 POG-E)?
Daten aus dem Kernbereich sind höchst diskret. Die Bewertung eines Datums als dem Kernbereich zugehörig folgt keinen polizeifachlichen, sondern allgemein-menschlichen Kriterien. Es erscheint demgegenüber als sachwidrig, wenn die Zentrale Datenprüfstelle nach Art. 13 Abs. 4 Satz 1 PAG-E „sich zur Aufgabenerfüllung der Unterstützung von Polizeidienststellen bedienen". Hinzu kommt, dass die Diskretionsverletzung durch die Beteiligung weiterer Stellen und Personen größer wird.

3. Zur Ergänzung polizeilicher Befugnisnormen:

a) Wie bewerten Sie die DNA-Analyse als (neue) erkennungsdienstliche Maßnahme nach Art 14 Abs. 3 PAG-E?
Nach Art. 14 Abs. 3 Satz 1 PAG-E kann die Polizei dem Betroffenen zudem Körperzellen entnehmen und diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen, wenn dies zur Abwehr einer Gefahr für ein bedeutendes Rechtsgut erforderlich ist und andere erkennungsdienstliche Maßnahmen nicht hinreichend sind; bei der Untersuchung darf eine andere Feststellung als die genannte nicht getroffen werden. Diese gesetzlichen Voraussetzungen treffen für sich genommen auf keine Bedenken. Ihre Crux liegt eher in der Anwendungspraxis. Dafür liefert die Rechtsprechung des BVerfG Beispiele, und zwar insbesondere zu den parallelen Regelungen im Strafverfahrensrecht, bei der Anwendung der Ermächtigungen durch die Instanzgerichte.

Die Feststellung, Speicherung und (künftige) Verwendung eines DNA-Identifizierungsmusters greift in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgte Grundrecht auf informationelle Selbstbestimmung ein (vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 14. Dezember 2000 - 2 BvR 1741/99 u.a. -, BVerfGE 103, 21 <32 f.>). 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 (BVerfGE 65, 1 <41 ff.>; 78, 77 <84>). Diese Verbürgung darf nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen, als es zum Schutz des öffentlichen Interesses unerlässlich ist (BVerfG, Stattgebender Kammerbeschluss vom 29. September 2013 – 2 BvR 939/13 –, Rn. 13, juris).

Die Gerichte sind bei der Auslegung und Anwendung des § 81g StPO gehalten, die Bedeutung und Tragweite dieses Grundrechts angemessen zu berücksichtigen (BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20.

Dezember 2001 - 2 BvR 429/01 u.a. -, juris, Rn. 17; Beschluss der 1. Kammer des Zweiten Senats vom 18. September 2007 - 2 BvR 2577/06 -, juris, Rn. 17; Beschluss der 2. Kammer des Zweiten Senats vom 1. September 2008 - 2 BvR 939/08 -, juris, Rn. 12; Beschluss der 2. Kammer des Zweiten Senats vom 22. Mai 2009 - 2 BvR 287/09 u.a. -, juris, Rn. 22; Beschluss der 3. Kammer des Zweiten Senats vom 2. Juli 2013 - 2 BvR 2392/12 -, juris, Rn. 11).

b) Wie bewerten Sie die Befugnis der Meldeanordnung nach Art. 16 Abs. 2 Satz 1 Nr. 2 PAG-E?

Die Schaffung einer spezialgesetzlichen Befugnis für die Meldeanordnung ist zu begrüßen. Nach der Rspr. des BVerwG ist sie zwar nicht erforderlich, weil sie auf die Generalermächtigung gestützt werden könnte: Die Anwendung der Generalermächtigung als Grundlage für die umstrittene Meldeauflage war auch nicht deswegen ausgeschlossen, weil es der vorrangigen Schaffung einer speziellen Befugnisnorm bedurft hätte (BVerwG, Urteil vom 25. Juli 2007 – 6 C 39/06 –, BVerwGE 129, 142-155, Rn. 31). Die angestrebte Regelung schafft aber ein höheres Maß an Rechtsklarheit.

c) Stellt die vorgesehene Regelung zur Sicherstellung von unbaren Vermögensrechten (Art. 25 Abs. 2 PAG-E) eine angemessene Reaktion auf die Rechtsprechung des BayVGH dar?

Der BayVGH hat Art. 25 PAG a.F. dahin verstanden, dass die Regelung nicht zur Sicherstellung einer schuldrechtlichen Forderung ermächtigt, auch wenn die Forderung durch Einzahlung von zunächst strafprozessual beschlagnahmten Bargeld auf ein Konto entstanden ist und sich damit gegen eine Rspr. des OVG Lüneburg, U.v. 21.11.2013 – 11 LA 135/13 – gestellt, die aus der Vergleichsnorm in § 26 Nds. SOG die gegenteilige rechtliche Möglichkeit abgeleitet hatte (Bayerischer Verwaltungsgerichtshof, Urteil vom 23. Februar 2016 – 10 BV 14.2353 –, juris). Der RegE zu Art. 25 Abs. 2 PAG überwindet den Einwand des BayVGH, ohne neue Rechtsprobleme aufzuwerfen. Denn die präventive Sicherstellung von Vermögenswerten ist nicht gleichgewichtig der zu Recht umstrittenen präventiven Gewinnabschöpfung (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 660 unter Hinweis auf VGH Hessen Beschl. v. 13.8.2015 – 8 B 1061/15 – Rn. 30: „Über die Zulässigkeit einer staatlichen Vereinnahmung der sichergestellten Gelder (sog. präventive Gewinnabschöpfung) ist hier nicht zu entscheiden“).

d) Halten Sie Art. 22 Abs. 1 Satz 1 PAG-E für eine verfassungsmäßige Rechtsgrundlage für die Durchsuchung vom Durchsuchungsobjekt räumlich getrennter Speichermedien?

Betrifft die Durchsuchung ein elektronisches Speichermedium, können nach § 22 Abs. 2 Satz 1 PAG-E auch vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, soweit von diesem aus auf sie zugegriffen werden kann. Diese Regelung interpretiert den Eingriffssachverhalt

verniedlichend, indem sie ihn zum Nebenprodukt der Beschlagnahme eines Speichermediums stilisiert. Dem kann nicht gefolgt werden. Es geht um den Zugriff auf Daten, die in einer sog. Cloud gespeichert sind unter Zuhilfenahme eines beschlagnahmten elektronischen Speichermediums. Der Zugriff auf die Cloud ist aber nicht Nebenprodukt der Beschlagnahme des Speichermediums, sondern ein eigenständiger Eingriff unter verfassungsrechtlich schwerer wiegenden Voraussetzungen. Zwischen den Datenberechtigten und seine Daten ist nämlich noch technisch und rechtliche das Verhältnis mit dem Dienstleister der Cloud geschaltet.

Zunächst erstreckt sich der Schutz aus Art. 10 Abs. 1 GG nicht allgemein auf alle Informationen, die das Telekommunikationsverhalten oder insgesamt die Beziehungen zwischen den Telekommunikationsdiensteanbietern und ihren Kunden betreffen. Insbesondere schützt das Telekommunikationsgeheimnis nicht die Vertraulichkeit der jeweiligen Umstände der Bereitstellung von Telekommunikationsdienstleistungen wie etwa die Zuordnung der von den Diensteanbietern vergebenen Telekommunikationsnummern zu bestimmten Anschlussinhabern (BVerfGE 130, 151 Rn. 113). Nicht von Art. 10 Abs. 1 GG erfasst ist ferner, wenn ausschließlich technische Geräte Daten austauschen, um ihre Betriebsbereitschaft sicherzustellen ohne Bezug zu einem menschlich veranlassten Kommunikationsvorgang (BVerfG NJW 2007, 351, 353 f.). Nicht abschließend geklärt ist, inwiefern der zwischen diesen Polen anzusiedelnde Bereich der Datenübertragung, etwa beim Online-Banking oder Cloud Computing, dem Telekommunikationsbegriff unterfällt. Zwar handelt es sich hierbei nicht um Kommunikation im klassischen Sinne. Jedoch werden mit einer berechtigten Vertraulichkeitserwartung individuell veranlasst Informationen ausgetauscht. Angesichts des entwicklungsoffenen Charakters von Art. 10 Abs. 1 GG, für dessen Schutz es nicht auf die Inhalte der Kommunikation ankommt, sollten daher auch diese Formen möglichst weitgehend dem Fernmeldegeheimnis unterstellt werden, auch wenn sie nur durch eine Person veranlasst werden (Graulich in Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl., § 88 Rn. 6 unter Hinw. auf Singelnstein, in NStZ 2012, 593, 594).

Der Begriff Cloud Computing bezeichnet nicht eine bestimmte Art von Diensten, sondern die Form ihrer Bereitstellung: Verschiedenste IT-Dienste und –Anwendungen werden dezentral über das Internet – „aus der Wolke“ – verfügbar gemacht. Gemeinsam ist den Angeboten, dass dem Kunden bestimmte IT-Ressourcen – Anwendungssoftware, Systemsoftware und/oder Hardwarekapazitäten – über das Internet zur Verfügung gestellt werden. Von herkömmlichen Outsourcing- oder Application Service Provider (ASP-)Modellen unterscheidet sich Cloud Computing dabei durch den Verzicht auf eine feste Zuordnung bestimmter physikalischer Infrastrukturen zu einem konkreten Kunden (Grünwald/Döpkens, MMR 2011, 287). Das

Fernmeldegeheimnis nach § 88 TKG gilt auch für nach § 6 Abs. 1 TKG meldepflichtige Cloud Computing-Angebote. Der Begriff des Diensteanbieters ist in § 3 Nr. 6 TKG legal definiert und umfasst jeden, der ganz oder teilweise geschäftsmäßig TK-Dienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Es gilt in diesem Zusammenhang aber auch für solche Anbieter, die zwar nicht selber einen TK-Dienst i.S.d. § 3 Nr. 27 TKG erbringen, die aber auf Grund der technischen Konfiguration ihres Dienstes die Möglichkeit haben, auf TK-Inhalte bzw. Verbindungsdaten zuzugreifen (Graulich in Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl., § 88 Rn. 6.).

Handelt es sich bei dem Zugriff auf die Cloud aber um einen selbständigen Eingriff in den Schutzbereich von Art. 10 Abs. 1 GG, steht dieser unter gesondertem Richtervorbehalt. Dieser müsste in die Vorschrift aufgenommen werden.

Halten Sie in Art. 22 Abs. 2 PAG-E Vorkehrungen zum Schutz von Daten, die dem Kernbereich privater Lebensgestaltung unterfallen oder über deren Inhalt nach §§ 53, 53a StPO das Zeugnis verweigert werden könnte, für erforderlich?
Ja. Beim Zugriff auf gespeicherte Daten unbekannten Inhaltes ist nie auszuschließen, dass diese dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Daher greift die Erwägung im BKAG-Urteil des BVerfG auch insoweit: Allerdings ist auch hier vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen; können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt (vgl. BVerfGE 120, 274 <338>). Können demgegenüber kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist ein Zugriff auf das informationstechnische System jedoch auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden. Der Gesetzgeber hat insofern dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür kommt dabei einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch das Bundeskriminalamt herausfiltert (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 220).

e) Ist Art. 25 Abs. 3 PAG-E eine verfassungsgemäße Rechtsgrundlage für diese Befugnis oder halten Sie ist einen Richtervorbehalt für erforderlich?
Ein Richtervorbehalt ist erforderlich (s.o.).

f) Wie bewerten Sie die konkrete Ausgestaltung der Regelung zur molekulargenetischen Untersuchung aufgefundenen Spurenmaterials unbekannter Herkunft (Art. 32 Abs. 1 Satz 2 und 3 PAG-E) im Hinblick auf den Rechtseingriff?

Diese Regelung ist nicht nachvollziehbar. Sie ermächtigt zum Zweck der Gefahrenabwehr zur molekulargenetischen Untersuchung von Spurenmaterial unbekannter Herkunft. Das befugte Vorgehen setzt – s. „unbekannte Herkunft" – also an einer Stelle an, wo noch nicht einmal ein Gefahrenverdacht besteht - denn dieser müsste sich immerhin auf einen Gefährder beziehen - und begibt sich in rechtlich höchst schwieriges Gelände –und muss sich evtl. am Ende –, sofern tatsächlich ein Gefahrenverursacher ausgemacht wird, den bekannten Fragen zum Schutz personenbezogener Daten stellen. Die Gesetzesbegründung lässt alle Warnlampen des Diskriminierungsverbotes aufleuchten: „…..darf sich die Feststellung neben dem DNA-Identifizierungsmuster auch auf das Geschlecht, die Augen-, Haar- und Hautfarbe sowie das biologische Alter und die biogeographische Herkunft eines Spurenverursachers beziehen" (LT-Drs. 17/20425 S.50). Es wird dringend davon abgeraten, diesen abschüssigen Weg weiterzugehen. Die bereits bundesgesetzlich geregelte Befugnis zur molekulargenetischen Untersuchung zwecks Ausschluss von sog. Trugspuren (vgl. § 24 BKAG) dient immerhin der Auffindung eines realen Gefahrverursachers.

g) Wie bewerten Sie die Regelungen der Bildaufnahmen und Übersichtsaufzeichnungen nach Art. 33 Abs. 1 Nr. 2 PAG-E?

Es handelt sich um die Befugnis zu offenen Bildaufnahmen oder Übersichtsaufnahmen oder Übersichtsaufzeichnungen. Kompetenzrechtliche bestehen dagegen keine Einwände. Die Offenheit von Bildaufzeichnungen ist hergestellt, wenn der von vom Aufzeichnungsgerät im öffentlichen Raum erfasste Überwachungsbereich für den Betroffenen erkennbar ist (Schenke PolR, S. 111, Fn. 497 unter Hinweis auf VG Hannover NVwZ-RR 2011, 943). Entsprechende Befugnisse finden sich in den meisten Polizeigesetzen von Bund und Ländern (§§ 26, 27 BPolG; § 21 BWPolG; Art. 32 BayPAG; §§ 24, 24 a ASOG Bln; § 31 BbgPolG; § 29 BremPolG; § 8 HbgPolDVG; § 14 HSOG; § 32 MVSOG; § 32 NdsSOG; §§ 15, 15 a, 15 b NRWPolG; § 27 RhPfPOG; § 27 SaarlPolG; § 16 LSASOG; § 184 SchlHLVwG; § 33 ThürPAG). Insbesondere große Städte machen auch von der Möglichkeit der offenen Videoüberwachung aus Gründen der präventiven Sicherheit und Kostenersparnis („Der stattdessen erwägenswerte größere Personaleinsatz der Polizei trifft auf Finanzierungsgrenzen." BVerwGE 141, 329 (Rn. 46)) Gebrauch. Dagegen erhobene kompetenzrechtliche Einwände, insbesondere auf die konkurrierende Gesetzgebungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 1 GG gestützte, überzeugen nicht. Die Gefahrenabwehr gehört in die ausschließliche Gesetzgebungskompetenz der Länder, und dazu wiederum gehört auch die

Gefahrenvorsorge. Von dort ist in der Polizeiarbeit der Übergang zur Strafverfolgungsvorsorge fließend. Aber auch dies verstärkt den kompetentiellen Einwand nicht, weil der Bund von seiner Möglichkeit, entsprechende Regelungen zur Strafverfolgungsvorsorge (Graulich NVwZ 2014, 685) zu erlassen, bislang keinen Gebraucht gemacht hat (Schenke PolR Rn. 185 ff.; BVerwGE 141, 329 (Rn. 35)). Der Landesgesetzgeber ist im Übrigen nicht gehindert, Befugnisse zum Zwecke der Gefahrenvorsorge zu treffen, selbst wenn der Bundesgesetzgeber parallel dazu Regelungen zur Strafverfolgungsvorsorge getroffen hat (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 811).

Größeres Gewicht als die kompetentiellen Einwände haben materiellrechtliche, die auf eine Gefährdung des informationellen Selbstbestimmungsrechts abheben. Das Beobachten öffentlicher Veranstaltungen und Ansammlungen durch Polizeibeamte mit bloßem Auge, mit einem Fernglas oder mittels Bild- und Tonaufnahmen ohne Aufzeichnung ist kein Eingriff. Die bloße Videoüberwachung verletzt nicht das allgemeine Persönlichkeitsrecht aus Art. 1 Abs. 1, 2 Abs. 1. GG; die Videoüberwachung ist - im Gegensatz zu einer Videoaufzeichnung - kein Eingriff in Freiheitsrechte (VG Halle (Saale), Beschl. v. 17.1.2000 – 3 B 121/99 HAL). Bei Übersichtsaufnahmen ist zu unterscheiden. In einem einstweiligen Anordnungsverfahren zum Bayerischen Versammlungsgesetz hat das BVerfG im Jahr 2009 die Ansicht vertreten, nach dem damaligen Stand der Technik stelle eine Übersichtsbildaufzeichnung für die Aufgezeichneten immer einen Grundrechtseingriff dar, der aufgrund der Möglichkeit der Datennutzung für Folgeeingriffe an Gewicht gewinnt; (BVerfGE 122, 342 (Rn.129)) Übersichtsaufzeichnung, die nicht gespeichert würden, blieben hingegen unter bestimmten Voraussetzungen zur Leitung des Polizeieinsatzes zulässig. (BVerfGE 122, 342 (Rn.135)). Das gleiche gilt für sog. Übersichtsaufnahmen, die eine Identifizierung von Personen nicht zulassen. Von einem Eingriff ist erst auszugehen, wenn Aufzeichnungen gefertigt werden, deren Auswertung eine Identifizierung von Personen zulässt. (BT-Drs. 12/7562, 55 ff.). Die Videoüberwachung greift jedenfalls insoweit in das Recht betroffener Personen auf informationelle Selbstbestimmung ein, als sie mittels Bildaufzeichnung erfolgt. Dies wäre nur anders zu beurteilen, wenn die aufgezeichneten Bilder unmittelbar nach der Aufzeichnung wieder gelöscht würden (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 812).

Die vorgesehen Regelung in Art. 33 Abs. 1 Nr. 2 PAG-E löst das Problem nicht. Wer eine Bildaufzeichnung anfertigt, welche die „gezielte Feststellung der Identität einer auf der Übersichtsaufzeichnung abgebildeten Person“ zulässt, kann jede darauf abgebildete Person in dieser Weise behandeln. Das ist weder mit Art. 8 GG – soweit die „Ansammlung“ die rechtlichen Voraussetzungen

einer „Versammlung“ erfüllt – noch in verhältnismäßiger Weise mit Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG vereinbar.

h) Stellt Art. 33 Abs. 4 PAG-E eine ausreichende Rechtsgrundlage für den Einsatz von Bodycams dar? Ergibt sich aus den am 28.02.2018 vorgestellten Ergebnissen der AG Bodycam Änderungsbedarf für die vorgesehene Regelung?

Die Ergebnisse der AG Bodycam sind hier nicht bekannt. Allgemein lässt sich aber folgendes anmerken: Bild- und Tonaufzeichnungen stellen einen Grundrechtseingriff dar. Die polizeirechtlichen Schutzgüter einschließlich der Strafverfolgungsvorsorge sind aber grundsätzlich geeignet, um entsprechende Eingriffe legitimieren zu können. Die verfassungs-rechtliche Beurteilung konzentriert sich daher auf das Bestimmtheitsgebot und vor allem auch die Verhältnismäßigkeitsprüfung. Das Bestimmtheitsgebot verlangt, dass auch die mit der Datenerhebung verbundenen Zwecke im Gesetz benannt werden. Dies ist bei Art. 33 Abs. 4 PAG-E der Fall: „zum Schutz von Polizeibeamten oder eines Dritten vor Gefahren für ein bedeutendes Rechtsgut“. Es ist unzulässig, personenbezogene Informationen auf Vorrat zu unbestimmten Zwecken zu sammeln (BVerfGE 118, 168, 187 = NJW 2007, 2464). Das ist aber kein Problem von Art. 33 Abs. 4 PAG-E, sondern allenfalls des anschließenden Umgangs mit dem Bildmaterial. Im Rahmen der Verhältnismäßigkeit sind Eignung, Erforderlichkeit und Angemessenheit zu prüfen. Zweifel an der Geeignetheit der Datenerhebung zum Selbst- und Drittschutz konnten empirisch ausgeräumt werden. Im Ergebnis konzentriert sich die verfassungsrechtliche Bewertung also auf die Angemessenheit im engeren Sinne. Diese erfordere über die tatbestandlichen Anforderungen hinaus insbesondere die verfahrensmäßigen Absicherungen (vgl. exemplarisch Zöller, S. 55 ff.; Kipker/Gärtner, NJW 2015, 296, 297. Krit, zur Forderung nach Aufbewahrung der Daten bei einer „Treuhandstelle“ Zöller, S. 60 f. m.w.Nachw.). Es ist grundsätzlich auch verfassungsrechtlich zulässig, dass von den Datenerhebungen gegenüber Störern bzw. Gefährdern Dritte (z.B. Passanten) unvermeidbar betroffen sind (vgl. Ruthig, Der Einsatz mobiler Videotechnik im Polizeirecht, in GSZ 2018, 12, 15).

i) Stellen die vorgesehenen Regelungen zur Erhebung und Auswertung von Bild- und Videomaterial (Art. 33 Abs. 5 und 6 Abs. 1 und 2 PAG-E) eine ausreichende Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch Muster- und Gesichtserkennung dar?

Nach Art. 33 Abs. 5 PAG-E dürfen bei Maßnahmen nach den Abs. 1 bis 3 Systeme zur automatischen Erkennung und Auswertung von Mustern, bezogen auf Gegenstände und das Verhalten von Personen, einschließlich der automatischen Systemsteuerung zu diesen Zwecken verwendet werden, soweit dies die jeweilige Gefahrenlage auf Grund entsprechender Erkenntnisse erfordert. Diese Regelung ist kein bayerisches Spezifikum. Das Polizeirecht kann

für bestimmte Zwecke innerhalb eines Aufgabenbereichs zum Einsatz von automatischen Bildaufnahme- und Bildaufzeichnungsgeräten befugen (z.B. § 27 BPolG). Diese Geräte sind an einem festen Standort installiert und ihr Bildwinkel ist zumeist — fest oder variabel — vorgegeben, kann aber mitunter auch ferngesteuert verändert werden. Ihre Besonderheit besteht vor allem darin, dass Bildaufnahmen nicht erst im Falle einer konkreten Gefahr und dann zielgerichtet nur von Störern gefertigt werden. Die Geräte werden vielmehr — zumeist im Dauerbetrieb — an bestimmten, abstrakt gefährdeten Gebäuden oder Anlagen, etwa im Rahmen des Objektschutzes, eingesetzt, um frühzeitig etwaige konkrete Gefahren erkennen zu können. Sie ergänzen oder ersetzen die Polizeistreife und tragen somit zur Erhöhung des Sicherheitsstandards im Rahmen bestimmter polizeilicher Aufgaben wesentlich bei (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 814).

Die selbsttätigen Bildaufnahme- und Bildaufzeichnungsgeräte erfassen — je nach Standort — auf Grund ihrer besonderen Betriebsweise nicht nur Störer oder potentielle Störer, sondern jede Person, die sich im Bereich der gefährdeten Anlagen oder Objekte bzw. an der Grenze befindet. Als datenschutzrechtliches Korrektiv ist daher eine Verpflichtung zur unverzüglichen Löschung von Bildaufnahmen mit personenbezogenen Daten vorzusehen, wenn sie nicht mehr zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden. Dies geschieht gewöhnlich dadurch, daß ein mitlaufendes Aufnahmeband nach kurzer Zeit automatisch gelöscht wird, sofern nicht wegen einer eingetretenen Störung die Aufzeichnung festgehalten wird (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 816). Art. 33 Abs. 8 PAG-E enthält eine Löschungsregelung

Nach Art. 33 Abs. 6 PAG-E weist die Polizei bei Maßnahmen nach den Abs. 1 bis 4 in geeigneter Weise auf die Bild- und Tonaufnahmen und -aufzeichnungen hin, soweit diese nicht offenkundig sind oder Gefahr im Verzug besteht. Dies entspricht auch der Regelung im BPolG. Die Aufzeichnung erfolgt offen, so dass eine verdeckte Aufnahme aufgrund der Befugnis ausgeschlossen ist (§ 27 a Abs. 1 1. Hs. BPolG). Für die betroffenen Bürgerinnen und Bürger muss erkennbar sein, dass aufgezeichnet wird (BR-Drs. 790/16, 7 ff.). Auf Maßnahmen nach § 27 a Abs. 1 BPolG ist in geeigneter Form hinzuweisen; bei Gefahr im Verzug kann der Hinweis unterbleiben (§ 27 a Abs. 2 BPolG). Die Bild- und Tonaufzeichnungsgeräte dürfen im Bereitschaftsbetrieb in ihrem Zwischenspeicher kurzzeitig Daten erfassen (Graulich in Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. Kapitel E Rn. 818).

j) Sind bezüglich der Durchführung verdeckter polizeilicher Maßnahmen Annexkompetenzen anzuerkennen, wenn die Maßnahme ohne

Überwindung besonderer (Zutritts-)Sicherungen etwa an Türen andernfalls nicht durchführbar wäre, oder bedürfte es hierzu einer ausdrücklichen Rechtsgrundlage?
Die Frage ist unverständlich.

k) Halten Sie die Regelung des Art. 86 Abs. 1 Satz 2 PAG-E, wonach besondere Sprengmittel, wie z.B. Handgranaten, gegen Personen in bestimmten Sachlagen zulässig ist, für verhältnismäßig und - gemessen an den rechtsstaatlichen Geboten der Normenklarheit und Bestimmtheit - auch für bestimmt genug?
Nein. Auch die bundesgesetzliche Regelung in § 14 UZwG trifft auf größte Bedenken. Ebenso wie Art. 69 Abs. 1 PAG-E durch den Verweis auf die Regelung über den Schusswaffengebrauch regelt § 14 UZwG den Einsatz von Explosivmitteln nicht eigenständig, sondern ordnet lediglich eine entsprechende Anwendung der Vorschriften über den Einsatz von Schusswaffen an. Diese Regelungstechnik ist nicht überzeugend. Insofern bestimmt UZwVwV-BMI VIII Abs. 2, dass eine Anwendung von Explosivmitteln gegen Personen nur zulässig ist, wenn die Anwendung von Schusswaffen ohne Erfolg war oder keinen Erfolg verspricht. Es erscheint unter Verhältnismäßigkeitsgesichtspunkten bedenklich, den Einsatz von Explosivmitteln pauschal an die gleichen Voraussetzungen zu knüpfen wie den Einsatz von Schusswaffen. Denn die durch den Einsatz von Explosivmitteln für den Betroffenen und Unbeteiligte entstehende Gefahrenlage ist jedenfalls schon deswegen eine andere, weil Explosivmittel nicht im gleichen Maße zielgerichtet eingesetzt werden können wie Schusswaffen. Ob durch diese Bestimmung Rechtssicherheit produziert werden kann, ist zu bezweifeln. Jedenfalls wäre auch hierdurch die Möglichkeit, Explosivmittel sogar gegen Menschenmengen einsetzen zu können (§ 14 i.V.m. 10 Abs. 2 und 12 Abs. 2 S. 2), nicht ausdrücklich aus-geschlossen, was größten Bedenken begegnet. Der Gefahrenabwehrauftrag der Polizei dürfte in solchen Fällen regelmäßig überschritten sein (Ruthig in Schenke/Graulich/Ruthig, UZwG § 14). Der Bezugsvorfall „Berliner Weihnachtsmarkt 2016“ kann weder als Referenz für den Einsatz von Maschinenwaffen noch denjenigen von Explosivmitteln herangezogen werden, weil der – hypothetisch – bekannte terroristische Einsatz eines LKW naheliegender Weise mit anderen Mitteln abzuwehren gewesen wäre.

l) Wird durch die neue Kostenpflicht des Art. 93 PAG-E die bislang unzureichende Kostenerhebungsmöglichkeit bei doppelfunktionalen Maßnahmen einer praktikablen Lösung zugeführt?
Der Regelung ist Erfolg zu wünschen.

m)Wie bewerten sie die in Art. 94 PAG-E vorgesehene Möglichkeit, präventivpolizeiliche Opferschutzmaßnahmen treffen zu können?

Bei Legendierungen lässt sich ohne Zweifel auch an Opfer von Gefährdungen denken. Allerdings muss in Betracht gezogen werden, dass eine getarnte Persönlichkeit auch anderen staatlichen Zugriffen entzogen ist.

4. Zur Ergänzung des BayDSG:
Stellt die im allgemeinen Datenschutzrecht vorgesehene Regelung zur Erhebung und Verarbeitung von DNA-Material (Art. 29 Abs. 5 bis 6 BayDSG-E) eine ausreichende Rechtsgrundlage zur Errichtung einer DNA-Referenzdatenbank zum Ausschluss von Trugspuren dar?

B. BayVSG

1. Inwieweit sind die Vorgaben des BKAG-Urteils auf den Bereich des Verfassungsschutzes übertragbar?
Bei den im o.g. Urteil judizierten Befugnissen handelte es sich weitgehend um Dateneingriffe. Deren Ausführung unterscheidet nicht nach staatlichen Behörden. Sie sind gleich wirksam, ungeachtet ihrer Ausführung durch eine Bundes- oder Landesbehörde, durch eine Polizei oder einen Nachrichtendienst. Insofern sind die in dem Urteil aufgestellten Grundsätze auch auf das Nachrichtendienstrecht übertragbar (Graulich in KriPoZ 2017, 43, 52).

Hierbei sollen besonders folgende Aspekte berücksichtigt werden:

a) Welche Bedeutung kommt dabei der Aussage des ATDG-Urteils zu, die Rechtsordnung unterscheide zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung hin ausgerichtet und durch detaillierte Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten, die auf die Beobachtung und Aufklärung im Vorfeld beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können (BVerfGE 133, 277 Rn. 122)?
Die in Bezug genommene Stelle des Urteils befasst sich mit der Zusammenlegung von polizeilichem und nachrichtendienstlichem Datenmaterial und dessen unterschiedlicher Valenz. In diesem Zusammenhang tauch die Erwägung auf, die Rechtsordnung unterscheide zwischen einer grundsätzlich offen arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung hin ausgerichtet und durch detaillierte Rechtsgrundlagen angeleitet ist, und den grundsätzlich verdeckt arbeitenden Nachrichtendiensten, die auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können (BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 122). Damit ist kein Argument aufgestellt gegen die Vergleichbarkeit datenrechtlicher Eingriffsbefugnisse mit der Konsequenz ihrer gemeinsamen Bindung an die

Verhältnismäßigkeitsanforderungen aus dem Urteil zum BKAG. In den dort geprüften Fällen ging es im Übrigen – wie bei den Nachrichtendiensten – um heimliche Maßnahmen. Das legt die Verwendung des gleichen rechtlichen Prüfungsmaßstabes umso mehr nahe.

b) Welche verfassungsrechtliche Bedeutung kommt dabei dem Umstand zu, dass dem Verfassungsschutz als Nachrichtendienst keine exekutiv-polizeilichen Befugnisse zustehen (Art. 5 Abs. 2 BayVSG)?
Die verfassungsrechtlichen Anforderungen an die Regelung des tatsächlichen Eingriffsanlasses sind im Fall des heimlichen Zugriffs auf ein informationstechnisches System für alle Eingriffsermächtigungen mit präventiver Zielsetzung zu beachten. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die Gleiche ist, besteht hinsichtlich seiner Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 254). Die Bedeutung liegt vor allem darin, dass dann „exekutiv-polizeiliche Befugnisse“ im Falle der Nachrichtendienstgesetze auch nicht verfassungsrechtlich zu überprüfen sind. Das BVerfG hat in seinem Urteil zum BKAG – umgekehrt – keinen härteren Prüfungsmaßstab angelegt, weil die heimlichen Maßnahmen von einer Polizeibehörde anzuwenden waren.

c) Wie wirkt sich die durch das Trennungsgebot in Deutschland bewirkte Aufgliederung des Gefahrenabwehrprozesses in Gefahrenerforschung (Nachrichtendienste) und Gefahrenintervention (Polizeibehörden) auf den Grundrechtsschutz des Betroffenen im Vergleich zu einem monistischen Modell aus, wie es z.B. in Gestalt des Österreichischen Bundesamts für Verfassungsschutz und Terrorismusbekämpfung verwirklicht ist?
Die österreichische Rechtslage kann hier nicht kompetent beurteilt werden. Das Trennungsgebot von Polizei und Nachrichtendiensten in Deutschland Dieses Gebot besagt, dass Geheimdienste keine polizeilichen Zwangsbefugnisse besitzen dürfen, also etwa keine Vernehmungen, Durchsuchungen, Beschlagnahmen durchführen oder anderen Zwang ausüben dürfen. Sie dürfen mithin nicht zur gezielten Erlangung von Zufallsfunden für nicht-nachrichtendienstliche Zwecke eingesetzt werden (BVerfG, Nichtannahmebeschluss vom 09. November 2010 – 2 BvR 2101/09 –, Rn. 59, juris unter Hinw. auf Roggan/Bergemann,NJW 2007, S. 876). Demnach hat der Betroffene im Fall von Grundrechtseingriffen es mit jeweils getrennten Beklagten zu tun.

d) Welche Bedeutung haben die Anforderungen des BKAG-Urteils an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle für den Verfassungsschutz? Insbesondere:

aa) Wie wirkt es sich aus, dass Art. 10 Abs. 2 Satz 2 und Art. 45d GG den individuellen Rechtsschutz des Betroffenen gegenüber nachrichtendienstlichen Maßnahmen durch parlamentarisch bestellte Organe oder Hilfsorgane ersetzt?

Das PKGr ist nach § 1 Abs. 1 PKGrG ein parlamentarisches Kontrollorgan über die Bundesregierung hinsichtlich der Tätigkeit des Bundesamtes für Verfassungsschutz, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes. Es dient nicht der Durchsetzung individueller Rechte.

Nach § 1 Abs. 2 G 10 in Verbindung mit §§ 14, 15 G 10 obliegt die Kontrolle der nach dem G 10 angeordneten Beschränkungsmaßnahmen dem Parlamentarischen Kontrollgremium und der G 10-Kommission. Dabei erfolgt die Kontrolle der im Einzelfall angeordneten und zu vollziehenden Beschränkungsmaßnahmen durch die G 10-Kommission (BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, BVerfGE 143, 1-21, Rn. 40). Mit der G 10-Kommission hat der Gesetzgeber ein Kontrollorgan eigener Art außerhalb der rechtsprechenden Gewalt geschaffen, das an die Stelle des Rechtswegs tritt (vgl BVerfGE 30, 1 <23>) und als Ersatz für den fehlenden gerichtlichen Rechtsschutz dient (BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, BVerfGE 143, 1-21, Rn. 41). Ihre Kontrollfunktion erstreckt sich in erster Linie auf die angeordneten, aber noch nicht vollzogenen Beschränkungsmaßnahmen, die sie zu genehmigen oder abzulehnen hat (§ 15 Abs. 6 G 10). Sie hat weiter die Zustimmung zu erteilen, wenn einem Betroffenen die Beschränkungsmaßnahme nach ihrer Einstellung nicht mitgeteilt werden soll (§ 15 Abs. 7 G 10 in Verbindung mit § 12 G 10). Der Gesetzgeber hat damit im Lichte der Rechtsprechung des Bundesverfassungsgerichts ein Organ geschaffen, das an die Stelle des Rechtswegs tritt (vgl. BVerfGE 30, 1 <23>), aber kein Gericht ist (vgl. BVerfGE 67, 157 <170 f.>; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 13. Juli 1993 - 1 BvR 1016/93 -, juris, Rn. 3), das innerhalb des Funktionsbereichs der Exekutive agiert, aber nicht in diese inkorporiert ist (vgl. BVerfGE 30, 1 <28>), das Rechtskontrolle ausübt, aber auch Opportunitätserwägungen treffen kann (vgl. BVerfGE 30, 1 <23 f.>). Es handelt sich um ein Kontrollorgan eigener Art außerhalb der rechtsprechenden Gewalt, das als Ersatz für den fehlenden gerichtlichen Rechtsschutz dient (BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, BVerfGE 143, 1-21, Rn. 41).

bb) Welche Bedeutung kommt dem Umstand zu, dass die EU-Polizei-Justiz-Richtlinie, deren Gleichlauf mit dem deutschen Verfassungsrecht das BKAG-Urteil betont (Rn. 134, 138), für Nachrichtendienste nicht gilt?

Auf Tätigkeiten, die nicht in den Anwendungsbereich von Unionsrecht fallen, finden keine unionalen Regeln Anwendung. Dies hat zuletzt Art. 2 Abs. 2 lit. a) DS-GVO ausgedrückt. Dadurch werden Nachrichtendienste nicht von Unionsrecht erfasst. Demgegenüber werden strafverfolgende und gefahrenabwehrende Einrichtungen von der RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 erfasst. Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist (ErwGr 12).

e) Inwieweit lässt sich der Grundsatz der hypothetischen Datenneuerhebung auf Übermittlungsvorgänge des Verfassungsschutzes übertragen?
Der Grundsatz der hypothetischen Datenneuerhebung ist keine Erfindung des BKAG-Urteils, sondern eine Zusammenfassung verschiedener Judikate zur Bedeutung der Zweckbindung bei der Übermittlung oder Neuverwendung personenbezogener Daten. Er ist demnach auch zu berücksichtigen, soweit es an einer ausdrücklichen gesetzlichen Regelung fehlt.

Insbesondere:
aa) Inwieweit verringert sich das Eingriffsgewicht der Datenübermittlung gegenüber der ursprünglichen Datenerhebung dadurch, dass Informationen aus dem Kernbereich der privaten Lebensführung bereits vor der Übermittlung herausgefiltert werden (Art. 8a BayVSG-E)?
Zum Kernbereich gehörende Daten dürfen weder erhoben noch weiterverarbeitet werden. Dies gilt von Verfassungs wegen. Die Berücksichtigung dieses Grundsatzes verschafft der eingreifenden Behörde keinen „Rabatt“ in Gestalt einer zu unterstellenden Verringerung des Eingriffsgewichts.

bb) Inwieweit verändert sich das Eingriffsgewicht der Datenübermittlung gegenüber der ursprünglichen Datenerhebung dadurch, dass der Verfassungsschutz grundsätzlich keine Rohdaten übermittelt, sondern verdichtete und aufbereitete Auswertungsergebnisse?

Solange die übermittelten Daten – beispielsweise wegen ihrer Technizität oder Allgemeinheit - nicht den Charakter von personenbezogenen Daten haben, sind die einschlägigen Begrenzungen nicht wirksam. Die Begrenzung greift erst wieder, wenn im Anschluss an die Übermittlung eines solchen „Auswertungsergebnisses“ eine gezielte Frage beantwortet wird, die personenbezogene Daten enthält. Dies hat das BVerfG in seiner ATGD-Entscheidung genauso bewertet: Das Eingriffsgewicht der Antiterrordatei ist allerdings dadurch gemindert, dass sie als Verbunddatei ausgestaltet ist, die in ihrem Kern auf die Informationsanbahnung beschränkt ist und eine Nutzung der Daten zur operativen Aufgabenwahrnehmung nur in dringenden Ausnahmefällen vorsieht (BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 124).

cc) In welchem Verhältnis steht der Grundsatz der hypothetischen Datenneuerhebung des BKAG-Urteils zum informationellen Trennungsprinzip des ATDG-Urteils (BVerfGE 133, 277 Rn. 123)?
Beide Grundsätze ergänzen einander, denn sie sind beide Ausdruck des Verhältnismäßigkeitsprinzips. Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein informationelles Trennungsprinzip. Danach dürfen Daten zwischen den Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen der Datentrennung sind nur ausnahmsweise zulässig. Soweit sie zur operativen Aufgabenwahrnehmung erfolgen, begründen sie einen besonders schweren Eingriff. Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt. Dies muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein; auch die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei nicht unterlaufen werden (BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 123).

2. Steht die Aufhebung der Beschränkungen in Art. 15 Abs. 2 Satz 2 BayVSG in Einklang mit der Rechtsprechung des BVerfG?
Ja.