Prof. Dr. Matthias Bäcker, LL.M.
Ludwig-Frank-Straße 52
68199 Mannheim

Mannheim, den 21. Juli 2017

Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Verfassungsbeschwerde

1. des Herrn M…
2. des Herrn Dr. M…
3. des Herrn S…

g e g e n

Art. 8 Abs. 1 Satz 1,

Art. 9,

Art. 10 Abs. 1,

Art. 11 Abs. 2 Satz 3, Abs. 3 Nr. 1 und Nr. 2,

Art. 12 Abs. 1,

Art. 13,

Art. 15 Abs. 2 und Abs. 3,

Art. 16 Abs. 1,

Art. 17 Abs. 2 Satz 1,

Art. 18 Abs. 1,

Art. 19 Abs. 1,

Art. 23 Abs. 1 Satz 1 und Satz 3,

Art. 25 Abs. 1, Abs. 2 Satz 1 Nr. 2 und Nr. 3, Abs. 2 Satz 2, Abs. 3 Nr. 2 und Nr. 3

des Bayerischen Verfassungsschutzgesetzes (BayVSG) vom 12. Juli 2016 (BayGVBl S. 145, BayRS 12-1-I).

Namens und in beigefügter Vollmacht **(Anlage 1)** der Beschwerdeführer erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen von Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1, Art. 19 Abs. 4, Art. 31 und Art. 70 GG.

Gliederung

A. Sachverhalt

Die Verfassungsbeschwerde richtet sich gegen Ermächtigungen zu verschiedenen Überwachungsmaßnahmen sowie gegen damit zusammenhängende Verfahrensregelungen und Datenübermittlungsermächtigungen im Bayerischen Verfassungsschutzgesetz (im Folgenden: BayVSG).

I. Die angegriffenen Regelungen

Das BayVSG wurde im Jahr 2016 vollständig neu erlassen und dabei inhaltlich erheblich umgestaltet. Nach der Gesetzesbegründung soll das neue Gesetz der Bedrohungslage durch den internationalen Terrorismus Rechnung tragen, die Zusammenarbeit zwischen Verfassungsschutz und Polizei verbessern, das Landesverfassungsschutzrecht an die Änderungen des Bundesverfassungsschutzgesetzes anpassen und die aus der jüngeren Rechtsprechung des angerufenen Gerichts folgenden verfassungsrechtlichen Anforderungen umsetzen,

LT-Drs. 17/10014, S. 13 ff.

Gegenstand der Verfassungsbeschwerde sind die meisten Überwachungsermächtigungen des BayVSG einschließlich zugehöriger Verfahrensregelungen, die Regelung über den datenschutzrechtlichen Auskunftsanspruch des Betroffenen sowie mehrere Ermächtigungen zur Übermittlung von Informationen durch das Bayerische Landesamt für Verfassungsschutz (im Folgenden: Landesamt) an andere Stellen.

Im Einzelnen richtet sich die Verfassungsbeschwerde gegen die Ermächtigungen zum Einsatz nachrichtendienstlicher Mittel (Art. 8 BayVSG), zu Wohnraumüberwachungen (Art. 9 BayVSG), zu „Online-Durchsuchungen“ (Art. 10 BayVSG), zur Ortung von Mobilfunkendgeräten (Art. 12 BayVSG), zu „Quellen-Telekommunikationsüberwachungen“ (Art. 13 BayVSG), zu Auskunftsersuchen betreffend Transaktionsdaten aus den Bereichen Post, Telemedien und Telekommunikation (Art. 15 Abs. 2 und Abs. 3 BayVSG) sowie Luftfahrt und Kreditwesen (Art. 16 BayVSG), zum Einsatz Verdeckter Mitarbeiter (Art. 18 BayVSG) und zum Einsatz von Vertrauensleuten (Art. 19 BayVSG). Gegenstand der Verfassungsbeschwerde sind die materiellen Eingriffsschwellen dieser Regelungen sowie zugehörige Verfahrensregelungen zum Schutz besonders sensibler Äußerungen und zur Gewährleistung von Transparenz und effektivem Rechtsschutz. Hinsichtlich von „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ sind auch die technisch-sozialen Modalitäten der Infiltration informationstechnischer Systeme zur Durchführung von Überwachungen von der Verfassungsbeschwerde umfasst.

Darüber hinaus richtet sich die Verfassungsbeschwerde gegen Beschränkungen des Auskunftsanspruchs des von Datenverarbeitungen des Landesamts Betroffenen (Art. 23 BayVSG) und gegen verschiedene Ermächtigungen des Landesamts zu Datenübermittlungen an öffentliche und nicht-öffentliche Stellen im In- und Ausland (Art. 25 BayVSG sowie § 4 Abs. 4 G 10, auf den das Gesetz teilweise verweist).

II. Die Beschwerdeführer

…

B. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig. Insbesondere sind die Beschwerdeführer beschwerdebefugt (unten I) und sind der Grundsatz der Subsidiarität der Verfassungsbeschwerde (unten II) sowie die Beschwerdefrist gewahrt (unten III).

I. Beschwerdebefugnis

Die Beschwerdeführer sind beschwerdebefugt.

1. Verfassungsrechtliche Rügen

Die Beschwerdeführer rügen folgende Grundrechtsverletzungen:

Die angegriffenen Datenerhebungserhebungsermächtigungen in Art. 8 bis Art. 19 BayVSG und die mit diesen Regelungen zusammenhängenden Verfahrensregelungen zum Schutz besonders vertraulicher Äußerungen, zur Vorabkontrolle eingriffsintensiver Überwachungsmaßnahmen und zur Benachrichtigung der Betroffenen verletzen die Grundrechte der Beschwerdeführer aus Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1 und Art. 19 Abs. 4 GG. Darüber hinaus steht Art. 13 BayVSG nicht mit der Ordnung der Gesetzgebungskompetenzen in Einklang und verstößt deshalb gegen Art. 70 GG. Art. 15 Abs. 3 BayVSG verletzt Bundesrecht und ist daher gemäß Art. 31 GG nichtig.

Der in Art. 23 BayVSG enthaltene Auskunftsanspruch unterliegt zu weitreichenden Beschränkungen. Die Norm verletzt insoweit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1 und Art. 19 Abs. 4 GG.

Die in Art. 25 BayVSG sowie in Art. 13 Abs. 2 und Art. 17 Abs. 2 Satz 1 BayVSG (jeweils i.V.m. § 4 Abs. 4 G 10) enthaltenen Ermächtigungen zu Datenübermittlungen reichen zu weit und verletzen deshalb Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG.

2. Eigene, gegenwärtige und unmittelbare Beschwer

Die Beschwerdeführer sind durch die angegriffenen Regelungen selbst, gegenwärtig und unmittelbar betroffen.

a) Eigene Beschwer

…

b) Gegenwärtige Beschwer

Die Beschwerdeführer sind durch die angegriffenen Regelungen gegenwärtig betroffen. Dies gilt auch insoweit, als sich die Verfassungsbeschwerde gegen Art. 15 Abs. 3 BayVSG richtet, der dem Landesamt für Verfassungsschutz erlaubt, auf die nach §§ 113a ff. TKG bevorrateten Telekommunikations-Verkehrsdaten zuzugreifen. Gemäß § 150 Abs. 13 TKG haben die Telekommunikationsunternehmen die gesetzliche Bevorratungspflicht seit dem 1. Juli 2017 zu erfüllen. Seit diesem Zeitpunkt stehen die Vorratsdaten für sicherheitsbehördliche Zugriffe zur Verfügung.

Allerdings hat das Oberverwaltungsgericht Nordrhein-Westfalen kürzlich in einem Eilverfahren dem Antrag eines Telekommunikationsunternehmens auf vorübergehende Aussetzung der Bevorratungspflicht stattgegeben, da §§ 113a ff. TKG europarechtswidrig seien,

> OVG Nordrhein-Westfalen, Beschluss vom 22. Juni 2017 – 13 B 238/17.

Daraufhin hat die Bundesnetzagentur, die für den Vollzug der Datenschutzregelungen des Telekommunikationsrechts primär zuständig ist, erklärt, sie werde bis zum rechtskräftigen Abschluss des zugehörigen Hauptsacheverfahrens die gesetzliche Bevorratungspflicht generell nicht mit Zwangsmitteln durchsetzen und Verstöße gegen sie nicht sanktionieren,

> https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html (letzter Abruf am 21. Juli 2017).

Daraufhin haben zahlreiche Telekommunikationsunternehmen erklärt, bis auf weiteres keine Verkehrsdaten nach §§ 113a ff. TKG zu bevorraten. Es ist daher davon auszugehen, dass Art. 15 Abs. 3 BayVSG derzeit faktisch in beträchtlichem Ausmaß leerläuft.

Allerdings ist es nach der Mitteilung der Bundesnetzagentur den Telekommunikationsunternehmen nicht verboten, Verkehrsdaten gemäß §§ 113a ff. TKG zu bevorraten. Es ist zumindest gut möglich, dass einzelne Unternehmen ihrer (vermeintlichen) gesetzlichen Pflicht zur Datenspeicherung nachkommen. Dementsprechend erscheint zumindest möglich, dass die Ermächtigung des Art. 15 Abs. 3 BayVSG in näherer Zukunft faktische Belastungswirkungen für die Beschwerdeführer zeitigen wird. Dabei kommt es nicht allein darauf an, ob

die von den Beschwerdeführern genutzten Anbieter von Telekommunikationsdiensten die Bevorratungspflicht umsetzen – was sich gegebenenfalls überprüfen ließe –, da die Beschwerdeführer auch aufgrund eines gegen einen ihrer Kommunikationspartner gerichteten Verkehrsdatenabrufs von Art. 15 Abs. 3 BayVSG betroffen sein können.

c) Unmittelbare Beschwer

Schließlich werden die Beschwerdeführer durch die angegriffenen Regelungen unmittelbar betroffen. Zwar bedürfen die Ermächtigungen zu Überwachungsmaßnahmen und Datenübermittlungen der behördlichen Umsetzung. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu,

> BVerfGE 133, 277 (311); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 82.

Die in den angegriffenen Regelungen geregelten Überwachungsmaßnahmen und Datenübermittlungen werden zumindest in der Regel verdeckt durchgeführt. Die im BayVSG vorgesehenen Pflichten des Landesamts zur Benachrichtigung der Betroffenen fangen dies nur teilweise auf, weil sie nicht alle Überwachungsmaßnahmen erfassen, möglicherweise erst spät greifen und weitreichende Ausnahmen kennen. Von der Übermittlung personenbezogener Daten erhalten die Betroffenen sogar in aller Regel keine Kenntnis. Der in Art. 23 BayVSG enthaltene Auskunftsanspruch enthält gleichfalls weitreichende Ausnahmetatbestände, so dass Personen, die von Überwachungsmaßnahmen und Datenübermittlungen betroffen sind, auch mit seiner Hilfe nicht durchweg einen effektiven Rechtsschutz erlangen können.

II. Subsidiarität der Verfassungsbeschwerde

Ein Rechtsweg unmittelbar gegen die angegriffenen Regelungen ist nicht eröffnet und muss daher auch nicht gemäß § 90 Abs. 2 Satz 1 BVerfGG erschöpft werden.

Darüber hinaus steht der Grundsatz der Subsidiarität der Verfassungsbeschwerde der Zulässigkeit der vorliegenden Verfassungsbeschwerde nicht entgegen. Es ist den Beschwerdeführern nicht möglich oder zumindest nicht zumutbar, gegen den Vollzug der angegriffenen Normen durch das Landesamt

vorzugehen und sich so einen indirekten Rechtsschutz gegen diese Normen zu verschaffen.

Soweit die angegriffenen Regelungen Ermächtigungen zu Überwachungsmaßnahmen und zu Datenübermittlungen oder dazugehörige Verfahrensregelungen enthalten, ist insoweit auf die Ausführungen zur unmittelbaren Beschwer zu verweisen.

Daneben können die Beschwerdeführer unter dem Gesichtspunkt der Subsidiarität der Verfassungsbeschwerde nicht darauf verwiesen werden, ihren Auskunftsanspruch aus Art. 23 BayVSG gegen das Landesamt geltend zu machen und gegebenenfalls in einem verwaltungsgerichtlichen Verfahren um die Auskunftserteilung ihre verfassungsrechtlichen Argumente gegen die angegriffenen Ausschlusstatbestände des Art. 23 BayVSG vorzubringen. Ein solches Vorgehen ist den Beschwerdeführern nicht zumutbar, weil ein wirksamer fachgerichtlicher Rechtsschutz gegen eine Auskunftsverweigerung im Einzelfall nicht durchweg gewährleistet ist.

Grund hierfür ist, dass das Landesamt gemäß Art. 23 Abs. 3 Satz 1 BayVSG nicht verpflichtet ist, eine Auskunftsverweigerung zu begründen. Fehlt eine Begründung, so kann der Auskunftspetent vor Gericht nicht umfassend darlegen, weshalb die vom Landesamt für die Auskunftsverweigerung herangezogenen Gründe unzureichend sind. Auch Bedenken gegen einen der gesetzlichen Ausschlusstatbestände kann der Petent dann allenfalls pauschal ins Blaue hinein und nicht in Bezug auf den konkreten Einzelfall und den in diesem Fall maßgeblichen Ausschlusstatbestand vorbringen. Die Gründe für die Auskunftsverweigerung können gerichtlich (zunächst) nur in einem In-Camera-Verfahren gemäß § 99 Abs. 2 VwGO überprüft werden. Vom Prozessstoff dieses Verfahrens erhält der Auskunftspetent jedoch wiederum keine umfassende Kenntnis, so dass er sich auch in diesem Rahmen nicht detailliert zu der Auskunftsverweigerung und den für sie herangezogenen Gründen äußern kann.

Dementsprechend hat das angerufene Gericht in seinem Urteil zur Antiterrordatei auf eine Rechtssatzverfassungsbeschwerde gegen die diese Datei errichtenden Normen auch die Auskunftsregelung in § 10 Abs. 2 ATDG-a.F. überprüft,

vgl. BVerfGE 133, 277 (367 ff.).

Dabei versprach eine fachgerichtliche Überprüfung der Auskunftsverweigerung auf der Grundlage von § 10 Abs. 2 ATDG-a.F. noch eher einen wirksamen Rechtsschutz, als er in den Fällen des Art. 23 BayVSG gegeben ist. Denn

§ 10 Abs. 2 ATDG-a.F. verwies auch auf § 19 Abs. 5 BDSG, der zumindest grundsätzlich vorsieht, dass die Auskunftsverweigerung zu begründen ist.

III. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die angegriffenen Regelungen sind gemäß Art. 30 Abs. 1 BayVSG am 1. August 2016 in Kraft getreten.

C. Begründetheit

Die Verfassungsbeschwerde ist begründet. Die angegriffenen Überwachungsermächtigungen verletzen teilweise die Kompetenzordnung oder verstoßen gegen Bundesrecht (unten I). Die gesetzlichen Eingriffsschwellen dieser Ermächtigungen sind durchweg zu weit oder zu unbestimmt gefasst (unten II). Zudem verfehlen die zugehörigen Verfahrensregelungen in weitem Umfang die verfassungsrechtlichen Anforderungen (unten III). Die Ermächtigungen zu „Online-Durchsuchungen“ und zu „Quellen-Telekommunikationsüberwachungen“ begründen überdies nicht mehr hinnehmbare Risiken für die Integrität informationstechnischer Systeme in der Bundesrepublik und verletzen so objektiv-rechtliche Grundrechtsgehalte (unten IV). Das BayVSG enthält daneben keine verfassungsrechtlich hinreichenden transparenzschaffenden Vorgaben (unten V). Schließlich stehen auch die Ermächtigungen des Landesamts für Verfassungsschutz zu Datenübermittlungen an andere öffentliche und nichtöffentliche Stellen nicht mit den verfassungsrechtlichen Anforderungen in Einklang (unten VI).

I. Verstöße gegen die Kompetenzordnung bzw. gegen Bundesrecht

Die Überwachungsermächtigungen des BayVSG bilden die Grundlage für Grundrechtseingriffe und müssen daher über die materiell-grundrechtlichen Anforderungen hinaus vollumfänglich mit der Verfassung übereinstimmen,

stRspr seit BVerfGE 6, 32 (41).

Dies ist jedoch nicht bei allen der angegriffenen Regelungen der Fall. Die Ermächtigung zu „Quellen-Telekommunikationsüberwachungen“ in Art. 13 BayVSG steht nicht mit der Ordnung der Gesetzgebungskompetenzen in Einklang und verletzt daher Art. 70 GG (unten 1). Die Ermächtigung zum Zugriff auf bevorratete Telekommunikations-Verkehrsdaten verstößt gegen einfaches Bundesrecht und ist daher gemäß Art. 31 GG nichtig (unten 2).

1. „Quellen-Telekommunikationsüberwachung“, Art. 13 BayVSG

Art. 13 BayVSG verletzt die Kompetenzordnung, indem diese Regelung lediglich ergänzend zu § 3 G 10 hinzutreten soll. Die damit in Bezug genommene bundesrechtliche Eingriffsermächtigung des § 3 G 10 wurde jedoch ihrerseits unter Verstoß gegen Art. 70 GG kompetenzwidrig erlassen, soweit sie, wie sich aus § 1 Abs. 1 Nr. 1 G 10 ergibt, Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden zum Gegenstand hat. Die darauf bezugnehmende Ergänzungsregelung in Art. 13 BayVSG nimmt an diesem Kompetenzverstoß teil.

Sollte das angerufene Gericht hingegen § 3 G 10 insoweit für kompetenzgemäß halten, so ist Art. 13 BayVSG gleichwohl als kompetenzwidrig anzusehen. Denn in diesem Fall ist neben der bundesrechtlichen Überwachungsermächtigung für eine landesrechtliche Ergänzungsregelung kein Raum. Falls § 3 G 10 hinsichtlich der Landesverfassungsschutzbehörden kompetenzgemäß ist, sind zudem neben Art. 13 BayVSG auch die meisten weiteren Überwachungsermächtigungen des BayVSG kompetenzwidrig. Dies wird im Folgenden hilfsweise ausgeführt.

Art. 13 BayVSG ist nur dann als kompetenzgemäß anzusehen, wenn *erstens* § 3 G 10 kompetenzwidrig ist und *zweitens* Art. 13 BayVSG entgegen der Gesetzesbegründung nicht als bloße Ergänzungsregelung zu § 3 G 10, sondern als eigenständige Überwachungsermächtigung anzusehen ist.

Da es für die kompetenzrechtliche Beurteilung von Art. 13 BayVSG in jedem Fall darauf ankommt, ob § 3 G 10 kompetenzgemäß erlassen wurde, soweit diese Norm Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden regelt, ist diese Frage im vorliegenden Verfahren zwingend als Vorfrage zu klären.

a) Kompetenzwidrigkeit von Art. 13 BayVSG wegen Kompetenzwidrigkeit von § 3 G 10

Es liegt nahe, Art. 13 BayVSG nicht als originäre Überwachungsermächtigung zu verstehen, sondern als eine unselbstständige Ergänzungsregelung, welche lediglich eine bestimmte technische Vorgehensweise bei einer Telekommunikationsüberwachung nach § 3 G 10 ermöglicht. Hierfür spricht zum einen die Gesetzesbegründung,

> LT-Drs. 17/11609, S. 22.

Zum anderen sind §§ 3 ff. G 10 darauf angelegt, die Voraussetzungen und weitgehend auch das Verfahren für Telekommunikationsüberwachungen durch *alle* Nachrichtendienste – also einschließlich der Landesverfassungsschutzbehörden – bundesweit verbindlich und abschließend zu regeln. Dies ergibt sich aus § 1 Abs. 1 Nr. 1 G 10. Es ist nicht ersichtlich, dass sich der bayerische Gesetzgeber durch Erlass von Art. 13 BayVSG hierüber hinwegsetzen wollte.

Jedoch verletzt § 3 G 10 die Kompetenzordnung jedenfalls insoweit, als er eine Vollregelung für Telekommunikationsüberwachungen für Landesverfassungsschutzbehörden enthält. An diesem Kompetenzverstoß nimmt Art. 13 BayVSG teil.

aa) Keine Gesetzgebungskompetenz des Bundes für Überwachungsermächtigungen der Landesverfassungsschutzbehörden

§ 3 G 10 verletzt die Kompetenzordnung zumindest insoweit, als er eine Ermächtigung für Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden enthält. Für eine solche Ermächtigung fehlt dem Bund die Gesetzgebungskompetenz,

> näher zum Folgenden und dort auch zu der hier nicht verfahrensgegenständlichen Frage, ob der Bund eine originäre Ermächtigung für Telekommunikationsüberwachungen durch das Bundesamt für Verfassungsschutz schaffen durfte, Bäcker, DÖV 2011, S. 840 ff.; ders., DÖV 2012, S. 560 ff.

Allerdings hat das angerufene Gericht in seinem ersten G 10-Urteil aus dem Jahr 1970 die Vorgängerregelung des heutigen § 3 G 10, den damaligen Art. 1 § 2 G 10, kompetenzrechtlich gebilligt. Als maßgeblichen Kompetenztitel für die Überwachungsermächtigung hat das Gericht Art. 74 (heute: Abs. 1) Nr. 1 GG angeführt, nach dem der Bund das gerichtliche Verfahren regeln darf. Dazu heißt es in dem Urteil:

> „Art. 1 § 2 G 10 dient der Abwehr verfassungsfeindlicher Bestrebungen im Vorfeld strafprozessualer Ermittlungen. Die zulässigen Beschränkungsmaßnahmen sind begrenzt auf die Fälle, in denen tatsächliche Anhaltspunkte für den Verdacht bestehen, daß bestimmte strafbare Handlungen geplant, begangen werden oder begangen worden sind. Die Beschränkungsmaßnahmen nach Art. 1 § 2 G 10 dienen also (wenigstens mittelbar) der Verhinderung, Aufklärung und Verfolgung von Straftaten.“
>
> BVerfGE 30, 1 (29).

Diese Begründung ist jedoch jedenfalls bei dem heutigen Stand der Verfassungsauslegung unhaltbar. Träfe die darin vertretene Interpretation von Art. 74 Abs. 1 Nr. 1 GG zu, so könnte der Bund neben dem Verfassungsschutzrecht auch das allgemeine Polizeirecht, das anerkanntermaßen in die alleinige Gesetzgebungskompetenz der Länder fällt, weitgehend an sich ziehen. Denn das allgemeine Polizeirecht hat maßgeblich die Verhinderung von Straftaten zum Gegenstand.

Demgegenüber ist zu den von dem angerufenen Gericht seinerzeit herausgearbeiteten Zwecken des Gesetzes Folgendes einzuwenden: Die *Aufklärung*

von Straftaten ist kompetenzrechtlich unergiebig, da für die Verteilung der Gesetzgebungskompetenzen das Ziel einer Aufklärungsmaßnahme maßgeblich ist. Die *Verfolgung* von Straftaten unterfällt in der Tat Art. 74 Abs. 1 Nr. 1 GG, ist aber nicht das Ziel von Überwachungsmaßnahmen der Verfassungsschutzbehörden,

> näher zu den Aufgaben der Nachrichtendienste in Abgrenzung zu Polizei- und Strafverfolgungsbehörden BVerfGE 133, 277 (325 ff.).

Die *Verhinderung* von Straftaten ist unmittelbar nicht Gegenstand der Aufgabe der Verfassungsschutzbehörden, die sich auf Beobachtung und Bewertung beschränkt. Selbst wenn sie aber als mittelbares Ziel von Überwachungen nach § 3 G 10 anzusehen sein sollte, lässt sich die Verhinderung von Straftaten jedoch nicht unter Art. 74 Abs. 1 Nr. 1 GG subsumieren. Eine allgemeine Gesetzgebungskompetenz des Bundes für präventiv ausgerichtete Überwachungsmaßnahmen besteht vielmehr gerade nicht. Nur bereichsspezifisch lässt sich eine Gesetzgebungskompetenz des Bundes begründen, wenn bestimmte Überwachungsmaßnahmen notwendig mit einem Sachbereich zusammenhängen, für den eine Bundeskompetenz besteht,

> BVerfGE 113, 348 (369), unter Verweis auf BVerfGE 109, 190 (215); ähnlich BVerfGE 110, 33 (48).

Als Kompetenztitel für Überwachungsermächtigungen im Verfassungsschutzrecht kommt daher allein Art. 73 Abs. 1 Nr. 10 lit. b und c GG in Betracht. Danach ist der Bund ausschließlich dafür zuständig, die Zusammenarbeit des Bundes und der Länder zum Verfassungsschutz und zum Schutz gegen gewaltbereite inländische Bestrebungen, die auswärtige Belange der Bundesrepublik gefährden, zu regeln. Der Begriff der Zusammenarbeit verdeutlicht, dass es hierbei um ein Kooperationsrecht für Bundes- und Landesbehörden mit parallelen Aufgaben und in den Grenzen ihrer je eigenen Befugnisse geht,

> vgl. BVerfGE 133, 277 (317 f.).

Im Übrigen sind die Länder zum Erlass von Gesetzen zur Abwehr von Bestrebungen gegen die freiheitliche demokratische Grundordnung befugt, soweit sich diese im jeweiligen Land auswirken und damit dort Gefahren hervorrufen können,

> BVerfGE 113, 63 (79).

In extensiver Interpretation mag zu der Gesetzgebungskompetenz des Bundes für die Zusammenarbeit des Bundes und der Länder im Verfassungsschutz noch gehören, dass der Bund den Ländern Mindeststandards für die

Aufgaben und möglicherweise auch für bestimmte Befugnisse der Landesverfassungsschutzbehörden auferlegt, um eine hinreichend effektive Kooperation zu gewährleisten,

> hierfür etwa BVerwG, Beschluss vom 9. Januar 1995 - 1 B 231.94 u.a. -, DÖV 1995, S. 692 (693); Uhle, in: Maunz/Dürig, GG, Bearbeitungsstand 2010, Art. 73 Rn. 232.

Dabei kann es sich jedoch allenfalls um rahmenartige Vorgaben handeln. Innerhalb dieses Rahmens muss den Ländern freistehen, zu welchen Maßnahmen sie ihre Verfassungsschutzbehörden unter welchen Voraussetzungen ermächtigen,

> vgl. zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (346).

Der Bund kann dementsprechend nicht selbst Eingriffsermächtigungen für die Landesverfassungsschutzbehörden schaffen, zumal wenn diese Ermächtigungen nicht unmittelbar der Zusammenarbeit von Bund und Ländern dienen. Gerade eine solche eigenständige Eingriffsermächtigung enthält jedoch § 3 G 10, soweit die Norm auch für die Landesverfassungsschutzbehörden gilt. Diese Regelung lässt sich daher auf Art. 73 Abs. 1 Nr. 10 GG auch bei extensivster Auslegung nicht mehr stützen.

bb) Auswirkung auf die landesrechtliche Ergänzungsregelung des Art. 13 BayVSG

An dem Kompetenzverstoß von § 3 G 10 nimmt Art. 13 BayVSG teil. Zwar ist der bayerische Landesgesetzgeber gemäß Art. 70 GG befugt, Ermächtigungen zu Telekommunikationsüberwachungen durch das Landesamt für Verfassungsschutz zu schaffen. Die kompetenzwidrigen Regelungen in §§ 3 ff. G 10 stehen dem nicht entgegen.

Jedoch enthält Art. 13 BayVSG gerade keine eigenständige Überwachungsermächtigung, sondern lediglich eine unselbstständige Regelung bestimmter technischer Vorbereitungsmaßnahmen. Diese Regelung hat ohne den in Bezug genommenen § 3 G 10 keinen Anwendungsbereich und läuft ins Leere. Dies führt nicht lediglich dazu, dass Art. 13 BayVSG gegenstandslos wird. Wird Art. 13 BayVSG vielmehr als eine unselbstständige Regelung bestimmter technischer Vorbereitungsmaßnahmen für Telekommunikationsüberwachungen nach § 3 G 10 verstanden, so erzeugt diese Regelung den Rechtsschein der Verfassungskonformität und Wirksamkeit der kompetenzwidrigen bundesrechtlichen Norm. Der bayerische Gesetzgeber ist jedoch nicht dazu befugt,

einen solchen Rechtsschein zu setzen. Denn die Kompetenzordnung steht nicht zur Disposition der Länder. Landesgesetzliche Regelungen können daher dem Bund keine Gesetzgebungsbefugnisse einräumen, die er nach dem Grundgesetz nicht hat,

> BVerfGE 1, 14 (35); Uhle, in: Maunz/Dürig, GG, Bearbeitungsstand 2008, Art. 70 Rn. 154, m.w.N.

Rechtsstaatlich ist es daher geboten, den von Art. 13 BayVSG erzeugten Rechtsschein zu beseitigen, indem die Verfassungswidrigkeit der Norm als bloßer Ergänzungsregelung festgestellt wird. Anschließend mag der bayerische Landesgesetzgeber eine kompetenzgemäße originäre Überwachungsermächtigung schaffen.

b) Hilfsweise: Kompetenzwidrigkeit von Art. 13 BayVSG, falls das G 10 kompetenzgemäß ergangen ist

Wird entgegen der oben begründeten Auffassung davon ausgegangen, dass der Bund die Gesetzgebungskompetenz für Überwachungsermächtigungen der Landesverfassungsschutzbehörden hat, so ist Art. 13 BayVSG selbst kompetenzwidrig. Denn in diesem Fall ist für eine landesrechtliche Regelung zu Telekommunikationsüberwachungen durch das Landesamt auch dann kein Raum, wenn Art. 13 BayVSG lediglich als unselbstständige Ergänzungsregelung zu § 3 G 10 begriffen wird.

Die Gesetzgebungskompetenz des Bundes für § 3 G 10 lässt sich, soweit es um Überwachungsmaßnahmen durch Landesverfassungsschutzbehörden geht, allenfalls auf Art. 73 Abs. 1 Nr. 10 GG stützen. Der von dem angerufenen Gericht 1970 beschrittene Weg über Art. 74 Abs. 1 Nr. 1 GG ist jedenfalls heute nicht mehr gangbar, will man nicht fundamental und ohne überzeugenden Grund mit der jüngeren Rechtsprechung zu diesem Kompetenztitel brechen.

Art. 73 Abs. 1 Nr. 10 GG begründet eine ausschließliche Gesetzgebungskompetenz des Bundes. In ihrem Anwendungsbereich sind die Länder gemäß Art. 71 GG zur Gesetzgebung nur dann berufen, wenn und soweit der Bund sie hierzu ausdrücklich gesetzlich ermächtigt hat. Eine solche Ermächtigung der Länder findet sich weder im G 10, das in § 16 G 10 lediglich für die parlamentarische Kontrolle von Überwachungen auf das Landesrecht verweist, noch in einem anderen Bundesgesetz.

c) Hilfsweise: Kompetenzwidrigkeit weiterer Überwachungsermächtigungen des BayVSG, falls das G 10 kompetenzgemäß ergangen ist

Sollte das angerufene Gericht entgegen der oben begründeten Auffassung eine extrem weite Interpretation von Art. 73 Abs. 1 Nr. 10 GG befürworten, der zufolge der Bund befugt ist, abschließende Ermächtigungen für Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden zu schaffen, so hätte dies Auswirkungen weit über Art. 13 BayVSG hinaus. Denn der Kompetenztitel des Art. 73 Abs. 1 Nr. 10 GG differenziert nicht zwischen unterschiedlichen Überwachungsmaßnahmen. Eine kompetenzrechtliche Sonderstellung der Telekommunikationsüberwachung lässt sich auch sonst nicht begründen. Daher wäre in dieser Auslegung von Art. 73 Abs. 1 Nr. 10 GG der Bund umfassend dazu berufen, die Überwachungsbefugnisse der Landesverfassungsschutzbehörden zu regeln. Da es sich um eine ausschließliche Gesetzgebungsbefugnis handelt, wären die Länder dann grundsätzlich überhaupt nicht für solche Überwachungsermächtigungen zuständig.

Damit wären die Überwachungsermächtigungen der Art. 8 ff. BayVSG fast alle als kompetenzwidrig anzusehen. Die einzigen Ausnahmen bildeten Art. 15 Abs. 2 Satz 1 Nr. 2 und Nr. 3 BayVSG, da sich insofern eine Öffnungsregelung für landesrechtliche Ermächtigungen in § 8b Abs. 10 BVerfSchG findet. Im Übrigen fehlte es für landesrechtliche Überwachungsermächtigungen an der gemäß Art. 71 GG erforderlichen ausdrücklichen bundesgesetzlichen Ermächtigung. Der Umstand, dass der Bund die Gesetzgebungstätigkeit der Länder im Verfassungsschutzrecht seit langem widerstandslos hinnimmt, kann die erforderliche ausdrückliche Regelung nicht ersetzen. Auch der Bund kann sich über die im Grundgesetz vorgesehenen Formen nicht hinwegsetzen.

Die Kompetenzwidrigkeit aller Überwachungsermächtigungen in Art. 8 ff. BayVSG mit Ausnahme von Art. 15 Abs. 2 Satz 1 Nr. 2 und Nr. 3 BayVSG wird hiermit hilfsweise für den Fall, dass das angerufene Gericht § 3 G 10 als kompetenzgemäße Ermächtigungsgrundlage für die Landesverfassungsschutzbehörden ansieht, ausdrücklich gerügt.

d) Höchst hilfsweise: Interpretation von Art. 13 BayVSG als eigenständige Überwachungsermächtigung

Nur unter zwei Bedingungen kann Art. 13 BayVSG als kompetenzgemäß angesehen werden:

Erstens muss Art. 13 BayVSG entgegen der naheliegenden und auch von der Gesetzesbegründung vertretenen Interpretation als eigenständige Überwachungsermächtigung ausgelegt werden. In dieser Auslegung ist Art. 13

BayVSG keine bloße Ergänzungsregelung zu der Ermächtigung in § 3 G 10, die deren Kompetenzwidrigkeit teilt. Vielmehr hat nach dieser Auslegung der bayerische Gesetzgeber selbst Voraussetzungen, Ziel und Verfahren der „Quellen-Telekommunikationsüberwachung“ umfassend geregelt. Die Verweise auf das G 10 in Art. 13 BayVSG sind dann nicht als bloße deklaratorische Bezugnahmen auf ohnehin anwendbare Vorschriften anzusehen, sondern als dynamische Verweisungen, die der bayerische Gesetzgeber zur Konkretisierung von Eingriffsschwelle und Verfahren aus eigener Regelungshoheit gesetzt hat.

Zweitens muss hierzu mit der oben begründeten Auffassung angenommen werden, dass der Bund keine Gesetzgebungskompetenz für Überwachungsermächtigungen der Landesverfassungsschutzbehörden hat und § 3 G 10 daher kompetenzwidrig ist, soweit er eine solche Ermächtigung enthält. Denn wenn sich § 3 G 10 auf Art. 73 Abs. 1 Nr. 10 GG stützen lässt, ist Art. 13 BayVSG aufgrund von Art. 71 GG kompetenzrechtlich nicht haltbar, ohne dass es darauf ankäme, ob es sich um eine bloße Ergänzungsregelung oder eine eigenständige Überwachungsermächtigung handelt.

In dieser – fachrechtlich fernliegenden – Auslegung ist Art. 13 BayVSG kompetenzgemäß, allerdings materiell verfassungswidrig, wie noch auszuführen sein wird,

siehe unten II. 5.

Da Art. 13 BayVSG die Kompetenzordnung nur wahrt, wenn § 3 G 10 als kompetenzwidrig angesehen wird, ist die Kompetenzmäßigkeit von § 3 G 10 im vorliegenden Verfahren als Vorfrage für die kompetenzrechtliche Beurteilung von Art. 13 BayVSG in jedem Fall klärungsbedürftig. Zudem muss die Reichweite der Gesetzgebungsbefugnis des Bundes aus Art. 73 Abs. 1 Nr. 10 lit. b und c GG auch deshalb geklärt werden, weil von ihr die Kompetenzmäßigkeit fast aller anderen Überwachungsermächtigungen des BayVSG abhängt.

2. Erhebung bevorrateter Telekommunikations-Verkehrsdaten, Art. 15 Abs. 3 BayVSG

Die Datenerhebungsermächtigung in Art. 15 Abs. 3 BayVSG ist zwar kompetenzgemäß ergangen, verletzt jedoch bundesrechtliche Vorgaben und ist daher gemäß Art. 31 GG nichtig. Der Widerspruch zwischen einer landesrechtlichen Norm und dem Bundesrecht kann mit einer Verfassungsbeschwerde gel-

tend gemacht werden, wenn die landesrechtliche Norm einen Grundrechtseingriff bewirkt. In diesem Fall hat das Bundesverfassungsgericht die Vereinbarkeit der Norm mit Bundesrecht zu untersuchen,

vgl. etwa BVerfGE 26, 116 (135 ff.); 121, 317 (348 f.).

Art. 31 GG setzt eine Kollision zwischen Bundes- und Landesrecht voraus. Eine Bundes- und eine Landesrechtsnorm müssen dazu auf denselben Sachverhalt anwendbar sein und zu unterschiedlichen Rechtsfolgen führen können,

BVerfGE 36, 342 (363); 96, 345 (364); 121, 317 (348).

Eine solche Kollision liegt hier vor, da Art. 15 Abs. 3 BayVSG, der den Abruf von gemäß §§ 113a ff. TKG bevorrateten Telekommunikations-Verkehrsdaten durch den Verfassungsschutz regelt, im Widerspruch zu § 113c Abs. 1 Nr. 2 TKG steht, der die Übermittlung dieser Daten durch die bevorratungspflichtigen Telekommunikationsdiensteanbieter zum Gegenstand hat.

Die Kompetenzen zur Regelung von Bevorratung, Übermittlung und Abruf von Telekommunikations-Verkehrsdaten sind nach der Rechtsprechung des angerufenen Gerichts zwischen Bund und Ländern aufgeteilt. Gemäß Art. 73 Abs. 1 Nr. 7 GG steht dem Bund die Gesetzgebungsbefugnis zu, eine Bevorratung von Verkehrsdaten durch die Anbieter von Telekommunikationsdiensten anzuordnen. Diese Befugnis umfasst Regelungen zum Bevorratungszweck. Der Bund kann (und muss) daher insbesondere normenklare und hinreichend begrenzte Übermittlungserlaubnisse für die bevorratungspflichtigen Diensteanbieter schaffen. Die behördlichen Ermächtigungen zum Abruf der bevorrateten Daten kann der Bund hingegen nur insoweit regeln, als ihm aus einem anderen Kompetenztitel die Regelungsbefugnis für das Fachrecht der abrufenden Behörden zusteht,

BVerfGE 125, 260 (314 ff.).

Untrennbarer Bestandteil des Datenabrufs ist die Auskunftspflicht des angefragten Diensteanbieters. Für die behördliche Erhebung von Telekommunikations-Verkehrsdaten bedarf es daher einer Rechtsgrundlage im behördlichen Fachrecht, die neben der Datenerhebung selbst auch die korrespondierende Auskunftspflicht des Diensteanbieters regelt,

vgl. zum Abruf von Telekommunikations-Bestandsdaten BVerfGE 130, 151 (201 f.).

Für das Verhältnis von § 113c Abs. 1 Nr. 2 TKG und Art. 15 Abs. 3 BayVSG folgt hieraus, dass § 113c Abs. 1 Nr. 2 TKG die Vorratsdaten gegenüber den

bevorratungspflichtigen Diensteanbietern für bestimmte Übermittlungen öffnet. Hierbei handelt es sich allerdings um eine bloße Erlaubnisnorm, die das grundsätzliche datenschutzrechtliche Verarbeitungsverbot des § 4 Abs. 1 BDSG aufhebt. Hingegen enthält Art. 15 Abs. 3 BayVSG neben der Ermächtigung des Verfassungsschutzes, Vorratsdaten zu erheben, auch eine korrespondierende Mitwirkungspflicht der Diensteanbieter. Dem Wortlaut der Norm, nach dem der Verfassungsschutz „Auskünfte“ zu Vorratsdaten „einholen“ darf, lässt sich diese Pflicht zwar noch nicht eindeutig entnehmen. Sie entspricht jedoch dem Regelungszweck, da ansonsten den Diensteanbietern grundsätzlich freistünde, ob sie einem Auskunftsersuchen des Verfassungsschutzes nachkommen wollen. Für diese Auslegung von Art. 15 Abs. 3 BayVSG spricht zudem in systematischer Hinsicht, dass die Unternehmen, an die sich Auskunftsersuchen nach Art. 14 ff. BayVSG richten können, in Art. 17 Abs. 1 Satz 1 BayVSG als „Verpflichtete“ bezeichnet werden.

§ 113c Abs. 1 Nr. 2 TKG und Art. 15 Abs. 3 BayVSG stehen zueinander in einem nur durch die Nichtigkeit der landesrechtlichen Regelung auflösbaren Widerspruch, da Art. 15 Abs. 3 BayVSG die Diensteanbieter zu einer Mitwirkung verpflichtet, zu der sie gemäß § 113c Abs. 1 Nr. 2 TKG datenschutzrechtlich nicht berechtigt sind. Denn § 113c Abs. 1 Nr. 2 TKG erlaubt eine Übermittlung bevorrateter Verkehrsdaten zu präventiven Zwecken nur, wenn Empfängerin der Übermittlung eine „Gefahrenabwehrbehörde der Länder“ ist. Das Landesamt kann jedoch nicht als solche Gefahrenabwehrbehörde eingeordnet werden. Dies ergibt sich aus einer systematischen, historischen und teleologischen Auslegung von § 113c Abs. 1 Nr. 2 TKG.

Systematisch ist vor allem der Vergleich von § 113c Abs. 1 und § 113 Abs. 3 TKG bedeutsam. § 113 Abs. 3 TKG regelt, an welche Behörden Telekommunikations-Bestandsdaten im manuellen Verfahren beauskunftet werden dürfen. Die Norm unterscheidet zwischen den für die Gefahrenabwehr zuständigen Behörden, die in Nr. 2 genannt werden, und den in Nr. 3 aufgeführten Verfassungsschutzbehörden. Dem lässt sich entnehmen, dass der Bundesgesetzgeber im TKG die Verfassungsschutzbehörden gerade nicht als Gefahrenabwehrbehörden ansieht. Ansonsten wäre ihre gesonderte Erwähnung in § 113 Abs. 3 Nr. 3 TKG überflüssig gewesen. Daneben enthält auch etwa § 14 Abs. 2 TMG jeweils eigenständige Erlaubnisse zur Datenübermittlung einerseits an die Polizeibehörden der Länder zur Gefahrenabwehr, andererseits an die Verfassungsschutzbehörden des Bundes und der Länder zur Erfüllung ihrer gesetzlichen Aufgaben.

Historisch lässt die Gesetzesbegründung zu § 113c Abs. 3 Nr. 2 TKG nicht erkennen, dass der Bundesgesetzgeber Verfassungsschutzbehörden als Gefahrenabwehrbehörden angesehen haben könnte. Als taugliche Empfänger von Vorratsdaten werden dort lediglich Landespolizeibehörden ausdrücklich genannt,

BT-Drs. 18/5088, S. 40.

Teleologisch liegt es fern, Verfassungsschutzbehörden als Gefahrenabwehrbehörden anzusehen. Die Aufgabe dieser Behörden besteht gerade nicht darin, drohende Schadensereignisse im Einzelfall zu verhindern und so konkrete Gefahren abzuwehren. Sie verfügen dazu auch nicht über geeignete Befugnisse, da ihnen imperative Eingriffsmaßnahmen versagt sind. Die Aufgabe der Verfassungsschutzbehörden besteht vielmehr gemäß § 3 Abs. 1 BVerfSchG darin, Informationen über verfassungsfeindliche Bestrebungen und Tätigkeiten im Vorfeld konkreter Gefahren zu sammeln und zu analysieren, um diese Informationen zu bewerten und diese Bewertungen politischen Entscheidungsträgern sowie der Öffentlichkeit als „Frühwarnsystem der Demokratie“,

so BVerwG, Urteil vom 26. Juni 2013 – 6 C 4/12 –, NVwZ 2014, S. 233 (235),

zur Verfügung zu stellen. Prägnant hat das angerufene Gericht dementsprechend allgemein zur Aufgabe der Nachrichtendienste formuliert: „Ziel ist nicht die operative Gefahrenabwehr, sondern die politische Information“,

BVerfGE 133, 277 (326).

Der Beobachtungsauftrag der Verfassungsschutzbehörden endet zwar nicht, wenn verfassungsfeindliche Bestrebungen und Tätigkeiten in konkrete Gefahren umschlagen. Er verwandelt sich jedoch auch dann nicht in einen Auftrag zur Gefahrenabwehr, sondern bleibt unmodifiziert bestehen. Entgegen der Gesetzesbegründung kann darum daraus, dass das Landesamt für Verfassungsschutz auch in konkreten Gefahrlagen noch zur Aufklärung befugt ist, nicht darauf geschlossen werden, dass das Landesamt eine Gefahrenabwehrbehörde ist,

so aber LT-Drs. 17/10014, S. 36.

Zur Gefahrenabwehr kann das Landesamt in einer solchen Lage allein dadurch beitragen, dass es relevante Informationen an andere Behörden übermittelt, insbesondere an die Polizei, je nach Einzelfall auch an weitere Stellen wie etwa Gewerbeaufsichts- oder Ausländerbehörden. Auch der Umstand, dass das Landesamt dementsprechend über Datenübermittlungsbefugnisse

verfügt, die unter anderem an konkrete Gefahren anknüpfen, macht das Landesamt entgegen der Gesetzesbegründung nicht zu einer Gefahrenabwehrbehörde. In den geregelten Datenübermittlungen liegen vielmehr in datenschutzrechtlicher Terminologie Zweckänderungen, da der Zweck der Datenverarbeitung von der verfassungsschutzbehördlichen Beobachtung in die sicherheitsbehördliche Gefahrenabwehr überführt wird. Im Übrigen verfügen praktisch alle Behörden über ähnliche Datenübermittlungsbefugnisse, ohne dass sie deshalb durchweg als Gefahrenabwehrbehörden anzusehen wären.

Irrelevant ist schließlich, ob sich das bayerische Landesamt für Verfassungsschutz selbst als Gefahrenabwehrbehörde begreift und vom bayerischen Gesetzgeber als solche gesehen wird. Der bundesrechtliche Begriff der Gefahrenabwehrbehörde in § 113c Abs. 1 Nr. 2 TKG steht nicht zur Disposition der Länder. Dies gilt zumal für die Verfassungsschutzbehörden, deren Aufgaben und teils auch Befugnisse weitreichend bundesrechtlich durch das auf Grundlage der ausschließlichen Bundeskompetenz des Art. 73 Abs. 1 Nr. 10 lit. b und c GG ergangene BVerfSchG vorgeformt sind.

II. Materielle Mängel der gesetzlichen Eingriffsschwellen

Auf der Grundlage der in der Rechtsprechung des angerufenen Gerichts entwickelten grundrechtlichen Maßstäbe für präventiv ausgerichtete Eingriffstatbestände im Sicherheitsrecht (unten 1) weisen fast alle Überwachungsermächtigungen des BayVSG auch materielle Mängel auf (unten 2 bis 7).

1. Verfassungsrechtliche Maßstäbe

Die verfassungsrechtlichen Maßstäbe, denen die Tatbestände von Überwachungsermächtigungen im Verfassungsschutzrecht genügen müssen, lassen sich aus der Rechtsprechung des angerufenen Gerichts zum Sicherheitsrecht ableiten und wie folgt zusammenfassen:

Ausgangspunkt für die Ableitung dieser Maßstäbe ist der Verhältnismäßigkeitsgrundsatz und insbesondere das Gebot der Verhältnismäßigkeit im engeren Sinne. Danach sind an die gesetzlichen Eingriffsschwellen desto höhere Anforderungen zu stellen, je schwerer der geregelte Überwachungseingriff wiegt. Dies kann dazu führen, dass eine bestimmte Überwachungsmaßnahme nicht zur Durchsetzung bestimmter Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange,

BVerfGE 120, 274 (322).

Im Einzelnen knüpfen die verfassungsrechtlichen Anforderungen an die gesetzliche Eingriffsschwelle an zwei Parameter an: Erstens muss das Gesetz einen hinreichend gewichtigen Anlass für die jeweilige Überwachungsmaßnahme in normenklarer Weise regeln. Zweitens muss das Gesetz gewährleisten, dass die Zielperson der Überwachungsmaßnahme – falls es sich, wie durchweg im vorliegenden Verfahren, um eine gezielt gegen bestimmte Personen gerichtete Maßnahme handelt – in einem hinreichenden Näheverhältnis zu dem Anlass der Maßnahme steht.

Für die Konkretisierung der verfassungsrechtlichen Maßstäbe ist insbesondere bedeutsam, ob und inwieweit auf die Rechtsprechung des angerufenen Gerichts zu präventivpolizeilichen Überwachungsmaßnahmen zurückgegriffen werden kann, um Ermächtigungen im Verfassungsschutzrecht zu beurteilen.

Im Ausgangspunkt hat das angerufene Gericht wiederholt anerkannt, dass die unterschiedlichen Aufgaben und Befugnisse von Polizeibehörden und Nachrichtendiensten es grundsätzlich rechtfertigen, an Überwachungsermächtigungen im Nachrichtendienstrecht weniger strenge Anforderungen zu stellen als an entsprechende Ermächtigungen im Polizeirecht,

> vgl. BVerfGE 100, 313 (383); 120, 274 (330); 130, 151 (206); 133, 277 (325 ff.); kritisch mit der Forderung nach einer partiellen „Deprivilegierung der Geheimdienste“ Wegener, VVDStRL 75 (2016), S. 293 (312 ff.).

Allerdings ist zugleich seit geraumer Zeit in der Rechtsprechung anerkannt, dass sich die verfassungsrechtlichen Anforderungen an die gesetzlichen Eingriffsschwellen auch im Nachrichtendienstrecht mit zunehmender Eingriffsintensität der jeweiligen Überwachungsmaßnahme verschärfen,

> vgl. beispielhaft zu Eingriffen in das Fernmeldegeheimnis BVerfGE 120, 274 (342 f.).

Bereits mehrfach hat zudem das angerufene Gericht deutlich gemacht, dass die Anforderungen an Überwachungsermächtigungen des Nachrichtendienstrechts bei besonders eingriffsintensiven Maßnahmen mit den Anforderungen an polizeirechtliche Ermächtigungen konvergieren. Für solche Maßnahmen hat das angerufene Gericht ausdrücklich ausgeführt, dass die verfassungsrechtliche Mindesteingriffsschwelle auch nicht deshalb abzusenken ist, weil

die Nachrichtendienste aufgrund ihres spezifischen Auftrags zur Vorfeldaufklärung nicht dazu berufen sind, konkrete Gefahren mit imperativen Mitteln abzuwehren,

> vgl. zur „Online-Durchsuchung“ BVerfGE 120, 274 (329 ff.); zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (331 f.). Für die Wohnraumüberwachung ergibt sich diese Konvergenz bereits aus Art. 13 Abs. 4 GG, der alle präventiv ausgerichteten Überwachungen an denselben Maßstab bindet und nicht zwischen unterschiedlichen Behörden differenziert.

Auf der Grundlage des Urteils zum BKA-Gesetz, das die verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsermächtigungen präzisiert und konsolidiert hat, lassen sich die Maßstäbe auch für Ermächtigungen im Nachrichtendienstrecht weiter schärfen.

In diesem Urteil hat das angerufene Gericht eingriffsintensive Überwachungsmaßnahmen an das Erfordernis einer konkreten Gefahr als einheitliche Mindesteingriffsschwelle gebunden. Zugleich hat das Gericht den verfassungsrechtlichen Begriff der konkreten Gefahr von dem polizeirechtlichen Gefahrbegriff entkoppelt und im Verhältnis zu diesem erweitert.

Eine konkrete Gefahr im verfassungsrechtlichen Sinne liegt danach nicht nur dann vor, wenn situationsbezogen ein Schaden mit hinreichender Wahrscheinlichkeit droht, wie es der polizeirechtliche Gefahrbegriff verlangt. Daneben könne eine „hinreichend konkretisierte Gefahr“ auch 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.“ Diese Tatsachen müssten „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.“ (Zumindest) in Bezug auf terroristische Straftaten hat das angerufene Gericht es darüber hinaus für ausreichend gehalten, „wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die

konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird.“

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 112.

Insbesondere die zweite Formulierung zielt erkennbar auf eine Ergänzung der *situationsbezogenen* Schadensprognose des hergebrachten polizeirechtlichen Gefahrbegriffs um eine *personenbezogene* Gefährlichkeitsprognose, die allerdings auf hinreichend aussagekräftigen Tatsachen beruhen muss,

> vgl. für einen Ansatz zur rechtsdogmatischen Erfassung und Rationalisierung personenbezogener Prognoseurteile Bäcker, Kriminalpräventionsrecht, 2015, S. 205 ff.

Offenbleiben mag hier, ob diese Erweiterung des verfassungsrechtlichen Gefahrbegriffs durchweg eine tragfähige Grundlage für eine rechtsstaatliche Konsolidierung des polizeilichen Vorfeldrechts darstellt,

> so zumindest tendenziell mit unterschiedlichen Vorschlägen im Einzelnen Darnstädt, DVBl 2017, S. 88 ff.; Albrecht/Poscher, Evaluationsgutachten zu §§ 4a, 20j, 20k BKAG, BT-Drs. 18/13031, S. 56 ff.,

oder ob es sich – so der Eindruck des Unterzeichners – um eine konzeptionell problematische Verwischung unterschiedlicher Tatbestandskategorien und hinsichtlich höchst eingriffsintensiver Überwachungsmaßnahmen wie Wohnraumüberwachung und „Online-Durchsuchung“ um eine bedenkliche Aufweichung rechtsstaatlicher Grundsätze handelt.

Jedenfalls ist der erweiterte verfassungsrechtliche Gefahrbegriff jedoch für das Nachrichtendienstrecht höchst anschlussfähig:

Einerseits ermöglicht der erweiterte verfassungsrechtliche Gefahrbegriff Überwachungsmaßnahmen bereits im Vorfeld akuter Krisenlagen, das in besonderem Maße die Domäne der nachrichtendienstlichen Aufklärung darstellt. Insbesondere ein personenbezogener Prognosetatbestand kommt dem spezifischen Aufklärungsauftrag des Verfassungsschutzes entgegen, indem er Überwachungsmaßnahmen gegen „Gefährder“ bereits im Vorfeld klar konturierter schadensträchtiger Situationen ermöglicht.

Andererseits schirmt der erweiterte verfassungsrechtliche Gefahrbegriff das Risiko ab, dass gerade die Nachrichtendienste Überwachungsmaßnahmen von hoher Eingriffsintensität im Wesentlichen auf allgemeine Erfahrungssätze stützen könnten, deren Gebrauch rechtlich nicht näher angeleitet wird und die

möglicherweise nur sehr grobe Prognosen zulassen. Denn der erweiterte verfassungsrechtliche Gefahrbegriff ermöglicht Überwachungsmaßnahmen gerade nur gegenüber Personen, die aufgrund ihres Vorverhaltens belastbar als „gefährlich“ gekennzeichnet werden können.

Die von dem angerufenen Gericht umrissene personenbezogene Gefährlichkeitsprognose eignet sich daher besonders dazu, personengerichtete Überwachungsmaßnahmen der Nachrichtendienste im benötigten Umfang zu ermöglichen und sie zugleich hinreichend trennscharf zu begrenzen.

Damit ist nach der partiellen Neukonzeption der verfassungsrechtlichen Anforderungen an das Polizeirecht im Urteil zum BKA-Gesetz nunmehr auch eine Anpassung der verfassungsrechtlichen Anforderungen an das Nachrichtendienstrecht angezeigt. Aufklärungsmaßnahmen der Nachrichtendienste lassen sich – soweit für das vorliegende Verfahren relevant – auf dieser Grundlage grob in zwei Kategorien einteilen, für die fundamental unterschiedliche verfassungsrechtliche Maßstäbe gelten:

Erstens dürfen Aufklärungsmaßnahmen ohne Eingriffscharakter oder mit nur geringer Eingriffsintensität den Nachrichtendiensten von Verfassungs wegen ohne konkretisierten Verdacht zur Verdachtsgewinnung eingeräumt werden.

Zweitens sind hingegen personengerichtete Überwachungsmaßnahmen hoher Eingriffsintensität auch im Nachrichtendienstrecht an eine situationsbezogene Schadens- oder eine personenbezogene Gefährlichkeitsprognose zu binden, wie sie das angerufene Gericht für das Polizeirecht entwickelt hat. Eine Absenkung der verfassungsrechtlichen Mindesteingriffsschwelle ist für solche Überwachungsmaßnahmen nach der Erweiterung des verfassungsrechtlichen Gefahrbegriffs nicht (mehr) angezeigt,

> vgl. andeutungsweise bereits BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 320: danach bedürfen „ungeachtet ihres im Wesentlichen auf das Vorfeld von Gefahren beschränkten Handlungsauftrags“ auch Datenerhebungen von Verfassungsschutzbehörden grundsätzlich einer „konkretisierten Gefahrenlage“.

Zur Einstufung der Aufklärungsmaßnahmen kommt es bei personengerichteten Maßnahmen ohne besondere Streubreite vor allem darauf an, ob sie in besondere Rückzugsbereiche der Privatheit eindringen, auf einem Bruch schutzwürdigen personengebundenen Vertrauens beruhen, Wahrnehmungsschranken insbesondere durch technische Mittel oder ein planvoll verdecktes

Vorgehen überwinden oder – insbesondere durch den Einsatz informationstechnischer Mittel – Eigenschaften, Verhalten oder Sozialkontakte der betroffenen Person in besonderem Maße für die Überwachungsbehörde verfügbar machen.

Daneben sind auch die von dem angerufenen Gericht in seinem Urteil zum BKA-Gesetz entwickelten Anforderungen an die Bestimmung der zulässigen Zielpersonen einer personengerichteten Überwachungsmaßnahme ohne weiteres auf das Nachrichtendienstrecht zu übertragen: Personengerichtete Maßnahmen von hoher, aber nicht höchster Eingriffsintensität dürfen danach auch gegen Unverdächtige als Zielpersonen gerichtet werden, wenn diese in einer spezifischen individuellen Nähe zum Aufklärungsziel stehen, die von der gesetzlichen Eingriffsermächtigung normenklar zu beschreiben ist. Wohnraumüberwachungen und „Online-Durchsuchungen“ als Überwachungsmaßnahmen höchster Eingriffsintensität dürfen hingegen nur gegen Verdächtige als Zielpersonen gerichtet werden,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 114 ff.

2. Einsatz nachrichtendienstlicher Mittel, Art. 8 Abs. 1 BayVSG

Unzureichende Anforderungen errichtet nach diesen Maßstäben zunächst die Ermächtigung zum Einsatz nachrichtendienstlicher Mittel in Art. 8 Abs. 1 Satz 1 BayVSG.

Diese Norm ermöglicht pauschal den Einsatz nachrichtendienstlicher Mittel, soweit keine der Sonderregelungen der Art. 9 ff. BayVSG greift. Um welche Mittel genau es sich dabei handelt, klärt Art. 8 BayVSG nicht abschließend, sondern überlässt die Spezifikation einer Dienstvorschrift. Allerdings zählt Art. 8 Abs. 1 Satz 1 BayVSG bestimmte nachrichtendienstliche Mittel beispielhaft auf. Unter anderem nennt die Regelung Observationen sowie Bild- und Tonaufzeichnungen. Hierbei kann es sich – je nach Dauer und technischen Modalitäten – um sehr eingriffsintensive Überwachungsmaßnahmen handeln,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 151.

Jedoch reicht die gesetzliche Eingriffsschwelle nicht aus, um derartige Überwachungsmaßnahmen zu rechtfertigen.

Die tatbestandlichen Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel nach Art. 8 Abs. 1 Satz 1 BayVSG ergeben sich aus Art. 5 Abs. 1 Satz 1 und 2 BayVSG,

vgl. die Gesetzesbegründung, LT-Drs. 17/10014, S. 26.

Erforderlich und ausreichend ist danach, dass tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen oder Tätigkeiten im Sinne von Art. 3 BayVSG bestehen und dass die Aufklärung dieser Anhaltspunkte mit nachrichtendienstlichen Mitteln für die in Art. 5 Abs. 1 Satz 1 BayVSG genannten Zwecke erforderlich ist.

Dabei handelt es sich um eine sehr niedrige Eingriffsschwelle, die bereits in hochgradig unklaren und ambivalenten Sachlagen überschritten sein kann. Auch wenn berücksichtigt wird, dass das Landesamt Bedrohungen gerade im Vorfeld konkreter Gefahren für bestimmte Rechtsgüter aufklären soll und dass es nicht über operative Befehls- und Zwangsbefugnisse verfügt, reicht ein solcher Eingriffstatbestand nicht aus, um schwerer wiegende Informationseingriffe zu rechtfertigen. Dieses Defizit lässt sich auch nicht durch einen Verweis auf den in Art. 6 BayVSG normierten Verhältnismäßigkeitsgrundsatz beheben. Denn im Nachrichtendienstrecht ist es – wie generell bei Informationseingriffen durch Sicherheitsbehörden – Sache des Gesetzgebers, durch normenklare tatbestandliche Begrenzungen zu gewährleisten, dass der Verhältnismäßigkeitsgrundsatz gewahrt wird,

vgl. etwa BVerfGE 120, 274 (315 f.); 125, 260 (328).

Hinzu kommt, dass Art. 5 und Art. 8 BayVSG nicht regeln, gegen wen sich der Einsatz nachrichtendienstlicher Mittel richten darf. Art. 8 Abs. 1 Satz 3 BayVSG bestimmt lediglich, dass diese Mittel auch eingesetzt werden dürfen, wenn Dritte unvermeidbar betroffen werden. Über die möglichen Zielpersonen von Überwachungen ist damit nichts ausgesagt. Die gesetzliche Ermächtigung erlaubt damit auch gezielte Überwachungen von Personen, von denen keine verfassungsfeindlichen Bestrebungen oder Tätigkeiten ausgehen und die derartigen Bestrebungen und Tätigkeiten auch nicht besonders nahestehen, wenn aus diesen Überwachungen nur überhaupt relevante Erkenntnisse zu erwarten sind. Bereits lose Kontakte mit potenziellen Exponenten verfassungsfeindlicher Bestrebungen könnten hierfür ausreichen. Dies genügt nicht

den Anforderungen an die Eingrenzung des Betroffenenkreises für eingriffsintensive Überwachungsmaßnahmen,

> vgl. demgegenüber zu einer verfassungsrechtlich tragfähigen Betroffenenregelung BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 166 ff.

Auf Art. 8 Abs. 1 Satz 1 BayVSG können daher nur Informationseingriffe von geringem Gewicht gestützt werden. Hingegen enthält die Norm keine tragfähige Ermächtigung zu den in ihr ausdrücklich genannten eingriffsintensiven Überwachungsmaßnahmen. Insoweit ist Art. 8 Abs. 1 Satz 1 BayVSG verfassungswidrig.

3. Wohnraumüberwachungen und „Online-Durchsuchungen“, Art. 9 und Art. 10 Abs. 1 BayVSG

Ebenfalls verfassungsrechtlich nicht tragfähig sind die Tatbestände der Ermächtigungen zu Wohnraumüberwachungen und „Online-Durchsuchungen“. Auch diese Normen enthalten keine verfassungsrechtlich hinreichende Eingriffsschwelle und grenzen den Kreis der möglichen Zielpersonen nicht hinreichend ein.

Wohnraumüberwachungen und „Online-Durchsuchungen“ mit präventiver Zielrichtung können aufgrund ihrer besonders hohen Eingriffsintensität nur zur Abwehr einer konkreten Gefahr (im verfassungsrechtlichen Sinne) für ein besonders bedeutsames Rechtsgut gerechtfertigt werden. Diese verfassungsrechtliche Mindesteingriffsschwelle gilt uneingeschränkt auch für Eingriffsermächtigungen des Nachrichtendienstrechts. Dies ergibt sich für Wohnraumüberwachungen unmittelbar aus Art. 13 Abs. 4 GG, der keine Differenzierung der Eingriffsschwelle für unterschiedliche Behörden vorsieht. Auch für „Online-Durchsuchungen“ hat das angerufene Gericht bereits ausgeführt, dass die verfassungsrechtliche Mindesteingriffsschwelle für alle präventiv tätigen Behörden identisch ist,

> BVerfGE 120, 274 (329 ff.).

Zudem dürfen sich Wohnraumüberwachungen und „Online-Durchsuchungen“ nur gegen denjenigen als Zielperson richten, der für die Gefahr verantwortlich sind. Eine gezielte Überwachung Nichtverantwortlicher ist auch dann unzuläs-

sig, wenn der Betroffene mit dem Verantwortlichen – etwa als Kommunikationsmittler oder als Kontakt- und Begleitperson – in einer näheren Beziehung steht,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 115.

Art. 9 und Art. 10 BayVSG verfehlen diese Anforderungen. Zwar verlangen sie als Anlass der Überwachung tatsächliche Anhaltspunkte für eine dringende Gefahr für bestimmte hochwertige Rechtsgüter. Jedoch begrenzen sie das Ziel der Überwachung nicht darauf, diese Gefahr abzuwehren. Zudem ermöglichen sie gezielte Überwachungen gegen Unverdächtige.

Art. 9 und Art. 10 BayVSG regeln selbst nicht, welchem Ziel die Überwachung dienen soll. Eine Zielvorgabe lässt sich nur mittelbar aus Art. 11 Abs. 3 BayVSG ableiten. Diese Vorschrift begrenzt die Verwendung der Daten, die mit einer Wohnraumüberwachung oder „Online-Durchsuchung“ erhoben wurden, auf die Abwehr „von“ Gefahren im Sinne von Art. 9 Satz 1 BayVSG (Nr. 1), die Verhinderung und Verhütung „von“ Straftaten im Sinne von § 100c Abs. 2 StPO (Nr. 2) oder die Verfolgung von Straftaten, wenn die Voraussetzungen der Strafprozessordnung für die Datenerhebung bei der Erhebung vorgelegen haben und bei der Übermittlung noch vorliegen (Nr. 3). Auch wenn Art. 11 Abs. 3 Nr. 3 BayVSG als Zweckänderungsermächtigung angesehen und darum als Zielvorgabe nicht berücksichtigt wird, ermöglichen Art. 11 Abs. 3 Nr. 1 und 2 BayVSG Überwachungen pauschal mit dem Ziel, schwere Gefahren abzuwehren oder schweren Straftaten vorzubeugen. Ein Bezug des Überwachungsziels zu der konkreten Gefahr, die den Überwachungsanlass bildet, wird nicht gefordert. Der Verfassungsschutz könnte danach eine konkret eingetretene Gefahr als Ausgangspunkt nutzen, um ein weiterreichendes strategisches Überwachungsziel zu verfolgen und bei Gelegenheit dieser Gefahr den Betroffenen der Überwachung und sein Umfeld weitwinklig auszuleuchten. Dies ist auch keine nur theoretische Möglichkeit, sondern im Aufklärungsauftrag des Verfassungsschutzes angelegt, Informationen im Vorfeld von Gefahren und über einzelne Gefahrlagen hinaus zu sammeln und zu bündeln. Auf diese Weise wird jedoch die verfassungsrechtliche Mindesteingriffsschwelle der konkreten Gefahr maßgeblich entwertet, die im Rahmen von Überwachungsermächtigungen gerade erst im Zusammenwirken mit dem Ziel der Gefahrenabwehr ihre Begrenzungswirkung entfaltet,

> näher Bäcker, Kriminalpräventionsrecht, 2015, S. 94 ff., 109 ff.

Die verfassungsrechtliche Mindesteingriffsschwelle der konkreten Gefahr für ein besonders bedeutsames Rechtsgut wird daher verfehlt, wenn eine Überwachung lediglich als Anlass eine solche Gefahr voraussetzt, das Überwachungsziel aber nicht auf die Abwehr der Gefahr beschränkt. Für Wohnraumüberwachungen ergibt sich dies auch bereits aus dem Wortlaut von Art. 13 Abs. 4 GG. Da Art. 9 und Art. 10 BayVSG das Ziel der Gefahrenabwehr nicht enthalten, sind sie insoweit verfassungswidrig.

Darüber hinaus verfehlen die gesetzlichen Ermächtigungstatbestände für Wohnraumüberwachungen und „Online-Durchsuchungen“ die verfassungsrechtlichen Anforderungen auch deshalb, weil sie solche Überwachungen nicht auf den für eine Gefahr Verantwortlichen als Zielperson beschränken. Stattdessen ermöglicht der für beide Maßnahmen geltende Art. 9 Satz 2 BayVSG i.V.m. § 3 Abs. 2 Satz 2 G 10 Überwachungen, die sich gezielt gegen bloße Nachrichtenmittler und Anschlussinhaber und damit gegen Nichtverantwortliche richten,

> vgl. zur Verfassungswidrigkeit von Wohnraumüberwachungen gegen Kontakt- und Begleitpersonen BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 191 ff.

4. Ortung von Mobilfunkendgeräten, Art. 12 Abs. 1 BayVSG

Die Ermächtigung zur Ortung von Mobilfunkendgeräten in Art. 12 Abs. 1 BayVSG ist zu unbestimmt und darum unverhältnismäßig weit gefasst.

Die von dieser Regelung ermöglichte Ortungsmaßnahme kann eine hohe Eingriffsintensität erreichen. Dies ist insbesondere anzunehmen, wenn die Maßnahme über einen längeren Zeitraum hinweg andauert. In einem solchen Fall ermöglicht sie, ein umfassendes Bewegungsprofil des Betroffenen zu erstellen, mit dessen Hilfe auch das zukünftige Bewegungsverhalten prognostiziert werden kann. Zudem können die Ortungsdaten mit weiteren – auch öffentlich zugänglichen – Daten verknüpft werden, um weitreichende Aussagen über die Lebensgestaltung des Betroffenen zu ermöglichen,

> vgl. zur Eingriffsintensität der funktional vergleichbaren Observation mittels GPS BVerfGE 112, 304 (316 f.); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 103. Ein instruktives Auswertungsbeispiel für die Verknüpfung von Mobilfunk-Standortdaten mit weiteren, teils öffentlich zugänglichen Kommunikationsdaten findet sich unter http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten (letzter Abruf am 21. Juli 2017).

Der potenziell hohen Eingriffsintensität der geregelten Maßnahme muss der Gesetzgeber durch eine hinreichend restriktive Eingriffsschwelle Rechnung tragen. Art. 12 Abs. 1 BayVSG leistet dies nicht. Grund hierfür ist in erster Linie, dass die Regelung zu unbestimmt ist.

Auf den ersten Blick scheint zwar das Erfordernis einer „schwerwiegenden Gefahr“ für bestimmte Schutzgüter klar gefasst zu sein. Insbesondere scheint zur Konkretisierung dieses Erfordernisses ein Rekurs auf den polizeirechtlichen Gefahrbegriff nahezuliegen, der auch gewichtige Eingriffsmaßnahmen anleiten kann. Jedoch zeigt sich bei näherer Betrachtung, dass der polizeirechtliche Gefahrbegriff hier nicht weiterführt. Stattdessen müsste ein spezifisch nachrichtendienstlicher Gefahrbegriff gebildet werden, den das Gesetz jedoch nicht ansatzweise konkretisiert und dessen Konturen äußerst unscharf bleiben.

Der polizeirechtliche Gefahrbegriff kann zur Konkretisierung von Art. 12 Abs. 1 BayVSG nicht herangezogen werden, weil er in engem Zusammenhang mit den polizeilichen Schutzgütern der öffentlichen Sicherheit und Ordnung steht und durch sie seine Konturen gewinnt. Art. 12 Abs. 1 BayVSG nimmt diese Schutzgüter – aufgrund der unterschiedlichen Aufgaben von Polizei und Verfassungsschutz konsequent – nicht in Bezug. Die Norm nennt jedoch auch ansonsten keine Schutzgüter, die sinnvoller Gegenstand einer Schadensprognose im Sinne des polizeirechtlichen Gefahrbegriffs sein könnten.

Nicht erhellend ist insoweit der Verweis von Art. 12 Abs. 1 BayVSG auf „die von Art. 3 [BayVSG] umfassten Schutzgüter“. Art. 3 BayVSG definiert keine Schutzgüter, sondern formuliert Aufklärungsaufträge des Landesamts für Verfassungsschutz. Allenfalls partiell und mittelbar lassen sich aus dieser Norm Güter ableiten, welche das Landesamt schützen soll. So mag man Art. 3 Satz 1 BayVSG i.V.m. § 3 Abs. 1 Nr. 1 BVerfSchG als Schutzgüter die freiheitlich demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes und die Amtsführung der Verfassungsorgane von Bund und Ländern entnehmen können. Schutzgut von Art. 3 Satz 1 BayVSG i.V.m. § 3 Abs. 1 Nr. 3 BVerfSchG wären dementsprechend die auswärtigen Belange der Bundesrepublik. Allerdings stößt diese Extraktion von Schutzgütern im Rahmen von Art. 3 Satz 1 BayVSG i.V.m. § 3 Abs. 1 Nr. 2 und Nr. 4 BVerfSchG an ihre Grenzen. Hinzu kommt, dass die so gewonnenen Schutzgüter des Verfassungsschutzes fast durchweg sehr unscharf gefasst sind. Je nachdem, wie sie verstanden werden, lässt sich eine polizeirechtliche Gefahr für eines dieser Schutzgüter so gut wie nie oder fast immer annehmen.

So können selbst hochgradig gewalttätige Gruppierungen die freiheitlich demokratische Grundordnung als konstitutives Element der tatsächlichen Verfassungsordnung der Bundesrepublik und des Freistaats Bayern ebenso wenig ernsthaft bedrohen wie den Bestand oder die – generelle – Sicherheit des Bundes oder eines Landes. Andererseits lässt sich insbesondere die Sicherheit des Bundes oder eines Landes auch als Kollektivgut interpretieren, das schon deutlich unterhalb der Schwelle zum illegalen Verhalten beeinträchtigt wird. So ließe sich die Sicherheit im Sinne eines freiheitlichen gesellschaftlichen Klimas auf das Sicherheitsgefühl der Bevölkerung beziehen. Die Sicherheit in diesem Sinne könnte schon leiden, wenn es einer verfassungsfeindlichen Gruppierung durch gesetzeskonformes Verhalten gelingt, das gesellschaftliche Leben in einem Bundesland oder möglicherweise auch nur lokal begrenzt mitzuprägen, soweit diese Gruppierung aufgrund ihrer Ziele von beachtlichen Teilen der Bevölkerung mit nachvollziehbaren Gründen als Bedrohung angesehen wird,

> vgl. zu einem – verfehlten – Versuch, das Sicherheitsgefühl der Bevölkerung sogar als polizeiliches Schutzgut einzustufen, Meyer, in: Arndt u.a. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 111 ff.

Die so verstandene Sicherheit des Bundes oder eines Landes reichte noch deutlich weiter als die polizeilichen Schutzgüter der öffentlichen Sicherheit und Ordnung.

Angesichts dieser Interpretationsprobleme liegt nahe, den Gefahrbegriff im Verfassungsschutzrecht eigenständig zu verstehen und vom polizeirechtlichen Gefahrbegriff abzukoppeln. So geht, soweit ersichtlich, auch die Praxis vor. Allerdings weist der spezifisch nachrichtendienstliche Gefahrbegriff praktisch keine Konturen auf und geht letztlich kaum über das Erfordernis tatsächlicher Anhaltspunkte hinaus, das gemäß Art. 5 Abs. 1 Satz 2 BayVSG für alle Maßnahmen des Verfassungsschutzes zu beachten ist,

> vgl. beispielhaft den Konkretisierungsversuch bei VG Berlin, Urteil vom 7. September 2016 – 1 K 12.15 –, juris, Rn. 26 ff.

Das weitere Merkmal einer „schwerwiegenden“ Gefahr, das gemeinhin auf das Schädigungspotenzial der betreffenden Bestrebung bezogen wird, kann diese Unschärfe nicht beseitigen, da die relevanten Schutzgüter unklar bleiben. Nur mit Blick auf bestimmte Schutzgüter lässt sich das Schädigungspotenzial aber überhaupt bestimmen.

Schließlich führt die Unschärfe des nachrichtendienstlichen Gefahrbegriffs dazu, dass auch die zugehörigen Betroffenenregelungen – wie Art. 12 Abs. 2 BayVSG i.V.m. § 3 Abs. 2 G 10 – unklar werden. Wenn sich nicht klar angeben lässt, wann eine nachrichtendienstliche Gefahr besteht, kann auch nicht bestimmt werden, wer verdächtig ist, für diese Gefahr verantwortlich zu sein oder sonst zu ihr beigetragen zu haben.

Dem Befund, dass der nachrichtendienstliche Gefahrbegriff des Art. 12 Abs. 1 BayVSG zu unbestimmt ist, kann nicht das Urteil des angerufenen Gerichts zum nordrhein-westfälischen Verfassungsschutzgesetz entgegengehalten werden. In diesem Urteil hat das Gericht zwar einen gleichartigen Eingriffstatbestand für eine vergleichbar eingriffsintensive Überwachungsmaßnahme verfassungsrechtlich gebilligt,

vgl. zum Abruf von Kontoinhalten BVerfGE 120, 274 (348 f.).

Die dafür seinerzeit gegebene Begründung überzeugt jedoch nicht und bedarf im Lichte der jüngeren Rechtsprechung des angerufenen Gerichts einer Neubewertung. Das angerufene Gericht hat sich mit den in Bezug genommenen Schutzgütern des Verfassungsschutzes in der damaligen Entscheidung nicht auseinandergesetzt und daher auch die Unschärfe des nachrichtendienstlichen Gefahrbegriffs nicht reflektiert. Demgegenüber steht mit der im neueren Urteil zum BKA-Gesetz vorgenommenen Ausdehnung des Gefahrbegriffs von einer rein situations- zu einer auch personenbezogenen Schadensprognose nunmehr ein trennschärferer verfassungsrechtlicher Kontroll- und fachrechtlicher Regulierungsansatz zur Verfügung. Eines darüberhinausgehenden spezifisch nachrichtendienstlichen Gefahrbegriffs, dessen Gehalt sich nicht klar bestimmen lässt, bedarf es daneben nicht.

5. „Quellen-Telekommunikationsüberwachung“, Art. 13 Abs. 1 BayVSG

Falls die Regelung zu „Quellen-Telekommunikationsüberwachungen“ in Art. 13 Abs. 1 BayVSG nicht lediglich als (kompetenzwidrige) Ergänzungsregelung zu § 3 G 10 interpretiert wird,

siehe oben I. 1. a),

ist sie als eigenständige Überwachungsermächtigung an den für solche Ermächtigungen geltenden verfassungsrechtlichen Anforderungen zu messen. Diese Anforderungen verfehlt sie. Zum einen verletzt sie das Gebot der Normenklarheit sowie das Demokratieprinzip, da sie Anlass und Ziel der Überwachung nicht selbst, sondern durch eine dynamische Verweisung auf die bundesrechtliche Vorschrift des § 3 Abs. 1 G 10 regelt. Zum anderen genügt der

in Bezug genommene § 3 Abs. 1 G 10 seinerseits nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu Telekommunikationsüberwachungen.

a) Unzulässige dynamische Verweisung auf § 3 Abs. 1 G 10

Nach Art. 13 Abs. 1 BayVSG sind die Voraussetzungen einer „Quellen-Telekommunikationsüberwachung“ § 3 Abs. 1 G 10 zu entnehmen. Wird Art. 13 Abs. 1 BayVSG als eigenständige Überwachungsermächtigung und nicht lediglich als unselbstständige Ergänzungsvorschrift zu dieser Norm angesehen, so ist die Bezugnahme auf § 3 Abs. 1 G 10 als dynamische Verweisung einzuordnen. Aus der Gesetzesbegründung geht der Wille des Gesetzgebers deutlich hervor, die „Quellen-Telekommunikationsüberwachung“ unter denselben Voraussetzungen und im selben Verfahren wie eine herkömmliche Beschränkung im Einzelfall nach dem G 10 zuzulassen,

vgl. LT-Drs. 17/11609, S. 22.

Dieses Ziel lässt sich nur im Wege einer dynamischen Verweisung auf das G 10 erreichen, da ansonsten im Zuge der – durchaus häufigen – Änderungen des G 10 Eingriffstatbestand und Verfahrensvorgaben der landesrechtlichen und der bundesrechtlichen Überwachungsermächtigungen im Laufe der Zeit immer weiter voneinander abweichen würden. Demgegenüber lassen sich weder dem Wortlaut noch der Begründung des Gesetzes Anhaltspunkte dafür entnehmen, dass Art. 13 Abs. 1 BayVSG als bloß statische Verweisung auf das G 10 zu interpretieren sein könnte.

Soweit Art. 13 Abs. 1 BayVSG Anlass und Ziel der „Quellen-Telekommunikationsüberwachung“ durch eine dynamische Verweisung auf § 3 Abs. 1 G 10 bestimmt, verfehlt die Norm die Anforderungen des rechtsstaatlichen Gebots der Normenklarheit und des Demokratieprinzips.

Dynamische Verweisungen insbesondere zwischen Regelungen unterschiedlicher Gesetzgeber sind nach der Rechtsprechung des angerufenen Gerichts zwar nicht generell ausgeschlossen. Sie sind aber nur in dem Rahmen zulässig, den die Prinzipien der Rechtsstaatlichkeit, der Demokratie und der Bundesstaatlichkeit ziehen. Grundrechtliche Gesetzesvorbehalte können diesen Rahmen zusätzlich einengen,

BVerfGE 47, 285 (312); 67, 348 (363); ferner zu Verweisen aus Gesetzen auf außerstaatliche Regelungswerke BVerfGE 64, 208 (214); 78, 32 (36).

Aus den Grundrechten, ferner auch aus dem Demokratieprinzip ergeben sich besonders hohe Anforderungen an die gesetzliche Regulierung verdeckter Überwachungsmaßnahmen der Sicherheitsbehörden. Insbesondere die gesetzlichen Eingriffsschwellen sind in der Eingriffsermächtigung hinreichend bestimmt anzugeben, um die Kontrollierbarkeit und Vorhersehbarkeit des behördlichen Handelns zu gewährleisten,

> vgl. etwa BVerfGE 110, 33 (53 ff.); 113, 348 (375 ff.); 120, 378 (407 ff.).

Darüber hinaus hat die Gestaltung der gesetzlichen Eingriffsschwellen bei verdeckten Überwachungsmaßnahmen eine wesentliche demokratische Funktion. Da Art und Ausmaß solcher Überwachungen im Einzelfall auch im Nachhinein nicht flächendeckend bekanntwerden, muss die öffentliche Auseinandersetzung über die Befugnisse der Sicherheitsbehörden zwangsläufig zu erheblichen Teilen anhand der abstrakt-generellen Eingriffsermächtigungen geführt werden. Dies setzt eine hinreichend gehaltvolle Fassung der Eingriffsvoraussetzungen voraus.

Den spezifischen Funktionen des formellen Gesetzes für sicherheitsbehördliche Überwachungsermächtigungen entspricht eine grundrechtliche und demokratische Regelungsverantwortung des Gesetzgebers. Er muss die Voraussetzungen einer Überwachung selbst möglichst trennscharf beschreiben, um so Überwachungen im Einzelfall voraussehbar und kontrollierbar zu machen und eine generelle Diskussion über die jeweilige Überwachungsmaßnahme zu ermöglichen. Durch die dynamische Verweisung auf das G 10 hat sich der bayerische Gesetzgeber dieser Regelungsverantwortung partiell entzogen. Die Gestaltung des gesetzlichen Eingriffstatbestands ist aufgrund dieser Verweisung zukünftig nicht mehr Sache des Landesgesetzgebers, sondern er gibt sie aus der Hand. Für denkbare Erweiterungen der Ermächtigung und die damit verbundenen grundrechtlichen Probleme muss er dann nicht mehr einstehen. Auch eine spezifisch auf das Bayerische Landesamt für Verfassungsschutz bezogene demokratische Diskussion wird anlässlich solcher Änderungen nicht mehr zu führen sein. In einem so sensiblen Regelungsfeld wie dem sicherheitsbehördlichen Eingriffsrecht ist eine derartige Delegation grundrechtlicher Regelungsverantwortung nicht hinnehmbar.

b) Defizite der Eingriffstatbestände in § 3 Abs. 1 G 10

Darüber hinaus genügen die in § 3 Abs. 1 G 10 enthaltenen Eingriffstatbestände ihrerseits nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu eingriffsintensiven Überwachungsmaßnahmen.

§ 3 Abs. 1 G 10 enthält zwei alternative Eingriffstatbestände: Nach § 3 Abs. 1 Satz 1 G 10 darf die Telekommunikation überwacht werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat aus einem Straftatkatalog plant, begeht oder begangen hat. Nach § 3 Abs. 1 Satz 2 G 10 ist eine Überwachung zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, die auf Straftaten gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes ausgerichtet ist.

Gemäß § 3 Abs. 1 Satz 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 muss die Überwachung zudem dazu dienen, Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes, eines Landes oder der in Deutschland stationierten NATO-Truppen abzuwehren. Dieses weitere Erfordernis begrenzt allerdings den Ermächtigungstatbestand kaum. Insbesondere kann § 1 Abs. 1 Nr. 1 G 10 angesichts der Aufgabe der Nachrichtendienste, Bedrohungslagen im Vorfeld akuter Krisen aufzuklären, nicht so verstanden werden, dass bereits eine konkrete Gefahr im polizeirechtlichen Sinne vorliegen müsste,

> so die allgemeine Auffassung, etwa Roggan, G 10, 2012, § 1 Rn. 4; B. Huber, in: W.-R. Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 1 G 10 Rn. 28.

Die Ermächtigungen in § 3 Abs. 1 G 10 sind sehr weit gefasst und ermöglichen Telekommunikationsüberwachungen bereits in diffusen Bedrohungslagen mit teils nur geringem Schadenspotenzial. Sie verfehlen daher zumindest in weitem Umfang die auch für die Nachrichtendienste zu beachtende verfassungsrechtliche Mindesteingriffsschwelle einer (verfassungsrechtlichen) konkreten Gefahr für ein besonders bedeutsames Rechtsgut.

Bei § 3 Abs. 1 Satz 1 G 10 beruht dies auf drei Defiziten, die einander zudem noch wechselseitig verstärken:

Erstens knüpft dieser Eingriffstatbestand nicht nur an die gegenwärtige Begehung einer Straftat an, die zumindest in der Regel auf eine Rechtsgutsgefahr schließen lässt, sondern ermöglicht Übermittlungen bereits im Planungsstadium. Der Umstand allein, dass jemand eine Straftat plant, begründet jedoch noch nicht zwangsläufig eine Gefahr für die Rechtsgüter, die durch diese Straftat verletzt würden. Die Planungen können sich noch in einem so frühen Sta-

dium befinden und vor der Tatbegehung noch so erhebliche Hürden zu überwinden sein, dass eine konkrete Straftat nicht einmal grob konturiert absehbar oder ihre Begehung sehr unwahrscheinlich sein kann,

vgl. BVerfGE 110, 33 (58 ff.).

§ 3 Abs. 1 Satz 1 G 10 enthält keine präzisierenden Tatbestandsmerkmale, um das potenziell fast uferlose Planungsstadium einzugrenzen,

kritisch auch B. Huber, in: W.-R. Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 3 G 10 Rn. 13.

Zweitens ermöglicht § 3 Abs. 1 Satz 1 G 10 Telekommunikationsüberwachungen auch, um dem Verdacht der Planung oder Begehung minderschwerer Straftaten nachzugehen, die keine besonders bedeutsamen Rechtsgüter schädigen. Zu nennen sind mindestens das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10), die Zuwiderhandlung gegen ein Vereinsverbot (§ 20 Abs. 1 Nr. 1 bis 4 VereinsG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10) und die Zugehörigkeit zu einer geheim gehaltenen Vereinigung von Ausländern (§ 95 Abs. 1 Nr. 8 AufenthG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 7 G 10).

Drittens finden sich in dem Straftatkatalog des § 3 Abs. 1 Satz 1 G 10 neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor.

Beispielhaft sei auf § 129a StGB (Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 6 lit. a G 10) verwiesen, der bereits die Gründung oder Beteiligung an einer terroristischen Vereinigung bei Strafe verbietet, also eine Tathandlung weit im Vorfeld konkreter Schädigungshandlungen beschreibt. Eine sehr weitreichende Vorverlagerung der Strafbarkeit sieht auch etwa § 89a StGB vor (Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 2 G 10). Diese Norm stellt die Vorbereitung eines terroristischen Anschlags bereits in einem sehr frühen Stadium unter Strafe, wenn noch kaum absehbar ist, ob der Täter sein Vorhaben letztlich in die Tat umsetzen können wird. Die Rechtsprechung begrenzt die sehr weit gefasste Norm vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt,

vgl. BGH, Urteil vom 8. Mai 2014 – 3 StR 243/13 –, juris, Rn. 45; BGH, Urteil vom 27. Oktober 2015 – 3 StR 218/15 –, juris, Rn. 10.

Diese Begrenzung wirkt sich jedoch im präventiven behördlichen Handlungsfeld, dem § 3 Abs. 1 Satz 1 G 10 angehört, allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen

kaum erschließen. Eine präventiv ausgerichtete Überwachung muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsachen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 3 Abs. 1 Satz 1 G 10 geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen.

Ungeachtet der Einstufung der von § 3 Abs. 1 Satz 1 G 10 in Bezug genommenen Vorfeldtatbestände als Erscheinungsformen der Schwerkriminalität, die sich im gesetzlichen Strafrahmen zeigt, sind diese Straftatbestände daher nicht geeignet, den Anlass präventiv ausgerichteter Eingriffsmaßnahmen trennscharf zu beschreiben,

> vgl. zu einer eingehenden Kritik der Verknüpfung präventivpolizeilicher Ermächtigungen mit strafrechtlichen Vorfeldtatbeständen Bäcker, Kriminalpräventionsrecht, 2015, S. 349 ff.

Die Defizite des gesetzlichen Übermittlungsanlasses verschärfen sich, wenn sie miteinander verbunden werden. § 3 Abs. 1 Satz 1 G 10 ermöglicht eine Überwachung auch, wenn der Verdacht besteht, dass jemand eine Vorfeldstraftat plant. Materiell-strafrechtliche und prozedural-nachrichtendienstrechtliche Vorverlagerung verstärken dann einander, so dass sich der Übermittlungstatbestand nahezu vollständig auflöst und Überwachungen weitgehend nach Belieben ermöglicht.

Dies lässt sich an einem Beispiel illustrieren: Nach § 89a Abs. 1, Abs. 2 Nr. 3 StGB macht sich unter anderem strafbar, wer sich Stoffe beschafft, um daraus Mittel für einen terroristischen Anschlag herzustellen. Erfasst sind insbesondere auch vielfältig nutzbare Stoffe, deren deliktischer Bezug sich erst aus den Vorstellungen des Handelnden ergibt. Den Straftatbestand erfüllt beispielsweise der Kauf von Unkrautvernichtungsmittel mit dem Ziel, daraus Sprengstoff herzustellen. In der Folge kann das Landesamt gemäß § 3 Abs. 1 Satz 1 Nr. 2 G 10 die Telekommunikation einer Person bereits überwachen, wenn der Verdacht besteht, dass diese Person plant, mit entsprechendem Vorbereitungsvorsatz Unkrautvernichtungsmittel zu kaufen. Auf welcher Grundlage ein solcher Verdacht fußen könnte, bleibt offen. Fast zwangsläufig wird es sich hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die per-

sönlichen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 113.

Auch § 3 Abs. 1 Satz 2 G 10 ermöglicht eine Telekommunikationsüberwachung bereits weit im Vorfeld konkreter Gefahren. Der Verdacht der Mitgliedschaft in einer Vereinigung kann bereits bestehen, wenn die genauen Ziele und das Gefährdungspotenzial der Vereinigung noch weitgehend unbekannt sind. Bedeutsam ist hierbei auch, dass die Regelung bereits einen strafrechtlich relevanten Zweck der Vereinigung ausreichen lässt. Anhaltspunkte für bereits begangene Straftaten sind danach nicht erforderlich. Schließlich schränkt der in § 3 Abs. 1 Satz 2 G 10 enthaltene Eingriffstatbestand den Kreis der Straftaten nicht ein, auf welche die Zwecke oder die Tätigkeit der mutmaßlichen Vereinigung gerichtet sein müssen. Eine Überwachung könnte daher auch an den Verdacht der Mitgliedschaft in einer Vereinigung anknüpfen, von der lediglich minder schwere Straftaten wie Beleidigungen oder einfache Sachbeschädigungen erwartet werden, wenn diesen Straftaten eine verfassungsfeindliche Motivation zugrunde liegt. Eine Gefahr für besonders bedeutsame Rechtsgüter geht von einer solchen Vereinigung nicht aus.

6. Erhebung von Transaktionsdaten, Art. 15 Abs. 2 Satz 1 und Abs. 4 und Art. 16 BayVSG

Die Ermächtigungen in Art. 15 Abs. 2 Satz 1 und Abs. 4 sowie Art. 16 BayVSG zur Erhebung bestimmter Transaktionsdaten bei Unternehmen sind wiederum zu unbestimmt gefasst.

Diese Normen erlauben die Erhebung solcher Transaktionsdaten, wenn tatsächliche Anhaltspunkte für „eine schwerwiegende Gefahr für die von Art. 3 [BayVSG] umfassten Schutzgüter“ bestehen. Art. 15 Abs. 2 Satz 2 BayVSG qualifiziert den Überwachungsanlass bei Datenerhebungen in den Bereichen Post, Telekommunikation und Telemedien dadurch, dass die Ermächtigung für Bestrebungen nach § 3 Abs. 1 Nr. 1 BVerfSchG nur anwendbar ist, wenn diese eine besondere Gewaltaffinität aufweisen. Auch diese Qualifikation ändert jedoch nichts daran, dass der Begriff der schwerwiegenden Gefahr nicht unter Rekurs auf den hergebrachten polizeirechtlichen Gefahrbegriff konkretisiert werden kann und als spezifisch nachrichtendienstlicher Begriff keine klaren

Konturen aufweist. Er kann daher die von Art. 15 Abs. 2 Satz 1 und Art. 16 BayVSG vorgesehenen eingriffsintensiven Maßnahmen nicht rechtfertigen,

> siehe oben II. 4.

7. Einsatz von Verdeckten Mitarbeitern und Vertrauenspersonen, Art. 18 Abs. 1 und Art. 19 Abs. 1 BayVSG

Schließlich genügen auch die Tatbestände der Ermächtigungen zum Einsatz von Verdeckten Mitarbeitern und Vertrauenspersonen nicht den verfassungsrechtlichen Anforderungen.

Art. 18 und Art. 19 BayVSG regeln selbst nicht, unter welchen Voraussetzungen das Landesamt solche Personen einsetzen darf, um Informationen zu gewinnen. Maßgeblich ist hierfür vielmehr die allgemeine Regelung in Art. 5 Abs. 1 Sätze 1 und 2 BayVSG,

> so zum Einsatz von Vertrauensleuten auch die Gesetzesbegründung, LT-Drs. 17/10014, S. 41.

Diese Regelung enthält einen sehr weit gefassten Eingriffsanlass, der unbedenklich ist als Grundlage für den Einsatz von nachrichtendienstlichen Mitteln von geringerer Eingriffsintensität, mit denen der Verfassungsschutz in noch weitgehend diffusen Lagen Anhaltspunkte gewinnen soll, auf deren Grundlage gezieltere Maßnahmen eingesetzt werden sollen. Gewichtigere Grundrechtseingriffe kann er hingegen nicht legitimieren,

> siehe oben unter II. 2.

Der Einsatz eines Verdeckten Mitarbeiters oder einer Vertrauensperson kann jedoch nicht als Mittel geringerer Eingriffsintensität angesehen werden.

Selbst in einer Frühphase der Ausforschung, in der eher ungezielt erste Erkenntnisse über eine Bestrebung beschafft werden sollen, können solche Personen zur Informationsgewinnung in erheblichem Ausmaß schutzwürdiges Vertrauen enttäuschen und so einen Grundrechtseingriff gehobener Intensität bewirken,

> vgl. zum Vertrauensbruch als Kriterium für das Vorliegen eines Grundrechtseingriffs BVerfGE 120, 274 (345). Konsequenterweise ist das Ausmaß enttäuschten Vertrauens auch als Kriterium für die Bestimmung der Eingriffsintensität heranzuziehen, in diese Richtung auch BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 160.

Ein derartiger Vertrauensbruch kann für die Betroffenen auch erhebliche psychische Folgen haben, die gleichfalls in die Bestimmung der Eingriffsintensität einzubeziehen sind. Zur Illustration sei auf die Berichte über die Einschleusung verdeckter Ermittler der Polizei in linke Kreise in Hamburg und Heidelberg verwiesen,

> vgl. zu dem Hamburger Fall http://www.zeit.de/politik/2015-08/rote-flora-polizei-maria-block; zu dem Heidelberger Fall http://www.zeit.de/campus/2016/03/spitzel-uni-heidelberg-linke-szene (letzte Abrufe am 21. Juli 2017).

Der Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten muss daher selbst dann, wenn er sich noch nicht gezielt gegen bestimmte Personen richtet, zumindest an eine hinsichtlich des Ziels der Aufklärung qualifizierte Eingriffsschwelle gebunden werden muss. Beispielhaft kann auf § 9a Abs. 1 Satz 2 BVerfSchG verwiesen werden, der einen solchen Einsatz auf die Aufklärung verfassungsfeindlicher Bestrebungen von erheblicher Bedeutung begrenzt.

Zudem steigt die Eingriffsintensität erheblich, wenn ein Verdeckter Mitarbeiter oder eine Vertrauensperson gezielt an einzelne Angehörige einer Bestrebung herangeführt wird, um deren Rolle und Vernetzungen innerhalb der Bestrebung aufzuklären. Ein derartiger personengerichteter Einsatz kann sich auf einen erheblichen Teil der Lebensgestaltung der Betroffenen erstrecken und sensible Informationen zum Gegenstand haben. Auch insoweit mögen die Fälle aus Hamburg und Heidelberg als Illustration dienen,

> für ein hohes Eingriffsgewicht auch BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 160. Nach Auffassung von Bergemann, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. H 85, handelt es sich bei dem Einsatz einer Vertrauensperson in dieser Phase um „[m]öglicherweise … (nach der akustischen Wohnraumüberwachung) das eingriffsintensivste Mittel überhaupt“.

Für den personengerichteten Einsatz eines Verdeckten Mitarbeiters oder einer Vertrauensperson bedarf es daher eines qualifizierten gesetzlichen Eingriffstatbestands. Dieser Eingriffstatbestand muss einen hinreichend gewichtigen Eingriffsanlass vorgeben und die möglichen Zielpersonen präzise und restriktiv beschreiben. Art. 18 und Art. 19 BayVSG leisten dies nicht ansatzweise.

III. Verfahrensrechtliche Defizite der Überwachungsermächtigungen

Neben den materiellen Eingriffsschwellen stehen auch die flankierenden verfahrensrechtlichen Schutzvorkehrungen der Überwachungsermächtigungen des BayVSG in weitem Umfang nicht mit den verfassungsrechtlichen Anforderungen in Einklang. Das Gesetz enthält keine zureichenden Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung (unten 1) und von beruflichen Vertrauensverhältnissen (unten 2). Zudem sieht es nicht durchweg eine Vorabkontrolle von Überwachungsmaßnahmen durch eine unabhängige Stelle vor, wo dies verfassungsrechtlich geboten wäre (unten 3).

1. Unzureichender Schutz des Kernbereichs privater Lebensgestaltung

Staatliche Überwachungen müssen den durch Art. 1 Abs. 1 GG absolut geschützten Kernbereich privater Lebensgestaltung wahren. Das materiell-rechtliche Verbot einer Kernbereichsverletzung muss in Ermächtigungen zu Überwachungsmaßnahmen, die eine gesteigerte Kernbereichssensibilität aufweisen, durch prozedurale Schutzregelungen flankiert werden,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 123 ff.

Das BayVSG genügt den Anforderungen an den prozeduralen Kernbereichsschutz nicht. Teils fehlen die gebotenen kernbereichsschützenden Regelungen vollständig. Teils verfehlen die im Gesetz enthaltenen Schutzregelungen die verfassungsrechtlichen Vorgaben.

a) Fehlen kernbereichsschützender Regelungen

Keine Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung finden sich in Art. 8 BayVSG. Solcher Regelungen bedarf es aber, da diese Norm das Landesamt unter anderem zu längerfristigen Bild- und Tonaufzeichnungen ermächtigt. Hierbei handelt es sich um Überwachungsmaßnahmen, die typischerweise ein gesteigertes Risiko einer Kernbereichsverletzung begründen und daher durch besondere Schutzregelungen abgeschirmt werden müssen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 175 ff.

Zwar sieht Art. 8 Abs. 2 Satz 1 BayVSG vor, dass die zu erlassende Dienstvorschrift zum Einsatz nachrichtendienstlicher Mittel auch den Schutz des Kernbereichs gewährleistet. Das angerufene Gericht hat jedoch in seiner bis-

herigen Rechtsprechung zum Kernbereichsschutz stets ausdrücklich den Gesetzgeber dazu verpflichtet gesehen, die gebotenen Schutzregelungen zu erlassen,

> BVerfGE 109, 279 (318); 113, 348 (392); 120, 274 (335); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 123.

Es handelt sich mithin bei dem prozeduralen Kernbereichsschutz um eine wesentliche Frage, die im formellen Gesetz zu klären ist. Dieser Schutz kann bei kernbereichssensiblen Maßnahmen nicht untergesetzlichen Regelungswerken überlassen werden. Erst recht kann ihn eine Dienstvorschrift als bloßes Innenrecht der Verwaltung nicht hinreichend zuverlässig gewährleisten.

b) Inhaltlich defizitäre Schutzregelungen

Soweit das Gesetz Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung enthält, genügen diese nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen.

Für den Kernbereichsschutz bei „Quellen-Telekommunikationsüberwachungen“ verweist Art. 13 Abs. 2 BayVSG auf § 3a G 10. Diese Regelung ist insoweit defizitär, als § 3a Satz 12 G 10 vorsieht, Dokumentationen von Kernbereichsverletzungen spätestens am Ende des Kalenderjahres zu löschen, das dem Jahr der Dokumentation folgt, da auf diese Weise nicht gewährleistet ist, dass die Dokumentationen tatsächlich für gerichtliche und aufsichtsbehördliche Kontrollverfahren zur Verfügung stehen,

> vgl. zu dem weitgehend gleichlautenden § 20l Abs. 6 BKAG BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 246.

Für den Kernbereichsschutz bei Wohnraumüberwachungen und „Online-Durchsuchungen“ verweist Art. 9 Satz 2 BayVSG gleichfalls auf § 3a G 10. Die hinter diesem Verweis stehende konzeptionelle Entscheidung, den Kernbereichsschutz für alle kernbereichssensiblen Überwachungsmaßnahmen gleich zu gestalten, ist im Ansatz verfehlt. Denn zum einen sind die unterschiedlichen Maßnahmen unterschiedlich sensibel. Zum anderen verfügt der Gesetzgeber je nach Maßnahme über unterschiedliche Möglichkeiten, den Kernbereichsschutz zu gewährleisten,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 127.

Der verfehlte Regelungsansatz hat zur Folge, dass die gesetzlichen Schutzregelungen die verfassungsrechtlichen Anforderungen, die im Rahmen von Wohnraumüberwachungen und „Online-Durchsuchungen“ an den Kernbereichsschutz zu stellen sind, in erheblichem Ausmaß verfehlen.

Wird § 3a G 10 auf Wohnraumüberwachungen übertragen, so verfehlt die Norm den verfassungsrechtlich gebotenen Kernbereichsschutz bereits auf der ersten Stufe der Datenerhebung. Zum einen trägt die Norm der verfassungsrechtlichen Vermutung nicht Rechnung, dass Gespräche in Wohnräumen dem Kernbereich zuzuordnen sind und daher nicht überwacht werden dürfen. Zum anderen ermöglicht sie eine automatische Daueraufzeichnung, die im Rahmen von Wohnraumüberwachungen nicht zugelassen werden darf,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 198.

Darüber hinaus ist § 3a G 10 als kernbereichsschützende Regelung für Wohnraumüberwachungen auch auf der zweiten Stufe der Datenauswertung insoweit mangelhaft, als eine Sichtung der erhobenen Daten durch eine unabhängige Stelle nicht generell, sondern nur in Zweifelsfällen vorgesehen ist,

> vgl. zum Gebot einer Sichtung aller erhobenen Daten BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 200.

Hinsichtlich von „Online-Durchsuchungen“ verfehlt der durch § 3a G 10 gewährleistete Kernbereichsschutz gleichfalls auf beiden Stufen die verfassungsrechtlichen Anforderungen.

Auf der ersten Stufe der Datenerhebung ist insoweit zu bemängeln, dass das Gesetz nicht vorsieht, eine Erhebung von kernbereichsrelevanten Daten nach Möglichkeit durch informationstechnische Mittel zu vermeiden,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 219.

Auf der zweiten Stufe der Datenauswertung fehlt es wiederum an dem verfassungsrechtlich erforderlichen generellen Gebot, die erhobenen Daten durch eine unabhängige Stelle sichten zu lassen,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 220.

Schließlich genügt die kurze Frist des § 3a Satz 12 G 10 zur Löschung von Verletzungsdokumentationen auch im Rahmen von Wohnraumüberwachungen und „Online-Durchsuchungen“ nicht den verfassungsrechtlichen Anforderungen.

2. Unzureichender Schutz von Berufsgeheimnissen

Im Zusammenhang mit Ermächtigungen zu eingriffsintensiven Überwachungsmaßnahmen muss der Gesetzgeber dem Schutz von Berufsgeheimnissen durch besondere Schutzregelungen Rechnung tragen, wenngleich er hierbei über einen beträchtlichen Gestaltungsspielraum verfügt,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 131 ff.

Derartige Schutzregelungen fehlen im BayVSG für die meisten Überwachungsmaßnahmen völlig. Dies ist verfassungsrechtlich nicht hinnehmbar.

Lediglich Art. 9 Satz 2 und Art. 13 Abs. 2 BayVSG verweisen zum Schutz zeugnisverweigerungsberechtigter Personen auf § 3b G 10. Diese Regelung ist jedoch insoweit verfassungsrechtlich unzulänglich, als sie unterschiedliche Schutzniveaus für Strafverteidiger und sonstige Rechtsanwälte vorsieht. Diese Differenzierung steht zumindest in präventiv ausgerichteten Regelungswerken mit dem Gleichheitssatz nicht in Einklang,

> vgl. zu dem weitgehend gleichlautenden § 20u BKAG BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 257.

3. Fehlende Vorabkontrolle durch eine unabhängige Stelle

Verdeckte eingriffsintensive Überwachungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstpersönliche Informationen erfassen, bedürfen grundsätzlich einer vorherigen Kontrolle durch eine unabhängige Stelle. Es ist Sache des Gesetzgebers, eine solche Kontrolle verbindlich vorzugeben. Zudem muss er strenge Anforderungen an den Inhalt und die Begründung der Entscheidung dieser Stelle errichten,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 117 f.

Bei präventivpolizeilichen Überwachungsermächtigungen ist die Vorabkontrolle grundsätzlich Gerichten zu übertragen. Demgegenüber begegnet es im Nachrichtendienstrecht keinen generellen Bedenken, stattdessen andere Stellen wie etwa die G 10-Kommissionen des Bundestags und der Landtage mit

der Kontrolle zu befassen. Voraussetzung dafür ist allerdings, dass diese Stellen in gleicher Weise wie ein Gericht eine unabhängige Prüfung gewährleisten. Zudem gibt es zumindest bei personengerichteten Überwachungsmaßnahmen wie den hier verfahrensgegenständlichen keinen Grund, die inhaltlichen Anforderungen an die Anordnung einer Überwachungsmaßnahme abzusenken. Hinnehmbar erscheint es allerdings, das Kontrollverfahren nach dem Muster von § 10 und § 15 G 10 so auszugestalten, dass die Verfassungsschutzbehörde selbst oder die zuständige oberste Landesbehörde die Überwachungsanordnung erlässt und dabei das Begründungserfordernis zu erfüllen hat, die Anordnung jedoch grundsätzlich vor ihrem Vollzug durch eine unabhängige Stelle zu kontrollieren ist.

Das BayVSG sieht nicht für alle Überwachungsmaßnahmen eine Vorabkontrolle durch eine unabhängige Stelle vor, bei denen dies verfassungsrechtlich geboten ist. Ein Kontrollverfahren fehlt bei längerfristigen Bild- und Tonaufzeichnungen (Art. 8 BayVSG), bei der Ortung von Mobilfunkendgeräten (Art. 12 BayVSG) sowie bei eingriffsintensiveren Formen des Einsatzes von Verdeckten Mitarbeitern und Vertrauenspersonen (Art. 18 und Art. 19 BayVSG).

Soweit das BayVSG eine Vorabkontrolle durch eine unabhängige Stelle vorsieht, sind die inhaltlichen Vorgaben für die Überwachungsanordnung teils zu unspezifisch gefasst. Grund hierfür ist, dass das Gesetz wegen des Inhalts der Anordnung durchweg auf das G 10 verweist (vgl. Art. 11 Abs. 2 Satz 3, Art. 12 Abs. 2, Art. 13 Abs. 2, Art. 17 Abs. 2 Satz 1 BayVSG, jeweils mit Verweis auf § 10 Abs. 2 G 10). Dies führt insbesondere bei Wohnraumüberwachungen, „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ zu Defiziten: Wohnraumüberwachungen müssen auf bestimmte Räumlichkeiten beschränkt werden, bei „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ muss das Zielsystem der Überwachung möglichst präzise beschrieben werden. Beides sieht das Gesetz nicht vor.

IV. Übermäßige Folgerisiken für die Integrität informationstechnischer Systeme

Die Regelungen zu „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ stehen mit der objektiv-rechtlichen Dimension des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (IT-Grundrecht) aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nicht in Einklang, da sie keine begrenzenden Vorgaben dafür enthalten, in welcher Weise die Zielsysteme solcher Überwachungen infiltriert werden dürfen.

Neben seiner Funktion als subjektives Abwehrrecht hat das IT-Grundrecht auch objektiv-rechtliche Gehalte. Deren besondere Bedeutung gerade für dieses Grundrecht schlägt sich bereits in seiner Bezeichnung durch das angerufene Gericht und dort im Begriff der Gewährleistung nieder. Relevant ist hier insbesondere die Integritätskomponente. Die öffentliche Gewalt ist verpflichtet, dazu beizutragen, dass die IT-Infrastruktur in der Bundesrepublik ein möglichst hohes Sicherheitsniveau aufweist,

> näher zu den objektiv-rechtlichen Ausprägungen des IT-Grundrechts und zu weiteren, insbesondere objektiv-rechtlichen Gewährleistungsaufträgen im Bereich der elektronischen Kommunikation Hoffmann-Riem, JZ 2009, S. 165 ff.; ders., AöR 134 (2009), S. 513 ff.; ders., JZ 2014, S. 53 ff.

Die Infiltration informationstechnischer Systeme zu Überwachungszwecken kann neben dem individuellen Eingriff in Grundrechte der Zielperson und dritter Betroffener auch die objektiv-rechtliche Dimension des IT-Grundrechts empfindlich treffen. Dies kann dann der Fall sein, wenn zum Zweck der Infiltration Software-Sicherheitslücken ausgenutzt werden (sogenannte Exploits). Insbesondere stellt es eine schwerwiegende Bedrohung der IT-Sicherheit in der Bundesrepublik dar, wenn eine Sicherheitsbehörde eine solche Sicherheitslücke geheim hält, um sie in der Zukunft für Überwachungen nutzen zu können. In einem solchen Fall können nicht nur Dritte die Sicherheitslücke weiterhin nutzen, um informationstechnische Systeme zu ihren eigenen – kriminellen – Zwecken zu infiltrieren. Darüber hinaus wird vielmehr die Sicherheitsbehörde selbst zum lohnenden Angriffsziel Krimineller, die sich Informationen über die dort bekannten Sicherheitslücken beschaffen könnten. Die Schäden, die hieraus resultieren könnten und zu deren Entstehung der Staat durch die Sammlung und Geheimhaltung der Sicherheitslücken aktiv beigetragen hätte, könnten enorm sein. Sie könnten – etwa wenn mit Hilfe einer Sicherheitslücke informationstechnische Systeme von Infrastruktureinrichtungen oder Krankenhäusern geschädigt würden – bis zum Tod von Menschen reichen.

Hierbei handelt es sich nicht um ein weitgehend hypothetisches Szenario, das als Restrisiko der sicherheitsbehördlichen Aufklärung außer Acht gelassen werden könnte. Die oben skizzierten Schadensereignisse liegen vielmehr ausgesprochen nahe und sind teilweise bereits eingetreten. So hat erst im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. Dieses Schadprogramm nutzte eine Sicherheitslücke des Betriebssystems Windows 7 aus, welche die kriminellen Angreifer nach verbreiteter Ein-

schätzung bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte,

> vgl. etwa http://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung; http://faktenfinder.tagesschau.de/wanna-cry-cyberangriff-101.html (letzte Abrufe am 21. Juli 2017).

Es liegt fern, dass das Bayerische Landesamt für Verfassungsschutz oder andere deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Software-Sicherheitslücken bedeutend besser schützen können als die NSA. Mit vergleichbaren Vorfällen infolge einer Sammlung solcher Sicherheitslücken bei diesen Behörden wäre zu rechnen.

Die Überwachungsbedürfnisse, welche die Ermächtigungen zu „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ auf der Ebene des individuellen Grundrechtseingriffs rechtfertigen mögen, können die erhebliche allgemeine Gefährdung der IT-Sicherheit in der Bundesrepublik nicht legitimieren, die von einer Sammlung von Sicherheitslücken bei den deutschen Sicherheitsbehörden ausgehen. Auch zur Aufklärung gefährlicher verfassungsfeindlicher Bestrebungen darf der Staat nicht auf Mittel zurückgreifen, die mit beträchtlicher Wahrscheinlichkeit bei unbeteiligten Dritten zu empfindlichen Schäden führen werden. Die bislang in der Rechtsprechung des angerufenen Gerichts entwickelten subjektiv-abwehrrechtlichen Anforderungen an diese Überwachungsmaßnahmen,

> BVerfGE 120, 274 (318 ff.); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 208 ff.,

sind daher aus objektiv-rechtlicher Perspektive ergänzungsbedürftig. Zur Durchführung einer „Online-Durchsuchung“ oder einer „Quellen-Telekommunikationsüberwachung“ dürfen nur solche Infiltrationsmethoden genutzt werden, welche kein besonderes allgemeines Risiko für die IT-Sicherheit in der Bundesrepublik begründen. Verfassungsrechtlich zulässig ist es danach etwa, heimlich in eine Wohnung einzudringen, um ein dort befindliches Zielsystem manuell zu manipulieren, oder Zugriffspasswörter durch eine Messung der elektromagnetischen Abstrahlungen des Zielsystems zu ermitteln. Auch die punktuelle Ausnutzung einer bereits bekannten, auf dem konkreten Zielsystem aber noch nicht geschlossenen Software-Sicherheitslücke erscheint noch hinnehmbar. Aufgrund der objektiv-rechtlichen Gehalte des IT-Grundrechts nicht mehr tragbar ist hingegen die gezielte Beschaffung von Informationen über

Sicherheitslücken, die planmäßig geheim gehalten werden, um möglichst lange ausgenutzt zu werden. Wegen der besonderen Bedeutung dieses Verbots für die objektiv-rechtliche Dimension des IT-Grundrechts muss eine gesetzliche Ermächtigung zu „Online-Durchsuchungen“ oder „Quellen-Telekommunikationsüberwachungen“ die Bevorratung von Software-Sicherheitslücken ausdrücklich untersagen. Hieran fehlt es in Art. 10 und Art. 13 BayVSG.

V. Unzureichende transparenzschaffende Vorgaben

Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen müssen durch transparenzschaffende Regelungen flankiert werden, um dem Betroffenen eine Orientierung über ihn betreffende Eingriffsmaßnahmen sowie einen effektiven Rechtsschutz zu ermöglichen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 134 f.

Das BayVSG enthält in zweierlei Hinsicht keine verfassungsrechtlich hinreichenden transparenzschaffenden Vorgaben: Erstens ist eine Benachrichtigung des Betroffenen im Anschluss an eingriffsintensive verdeckte Überwachungsmaßnahmen nicht im gebotenen Ausmaß gewährleistet (unten 1). Zweitens ist der Auskunftsanspruch des Betroffenen über ihn betreffende Datenverarbeitungen zu restriktiv ausgestaltet (unten 2).

1. Benachrichtigung des Betroffenen

Der Gesetzgeber muss nach der Rechtsprechung des angerufenen Gerichts Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen durch Benachrichtigungspflichten flankieren. Das Gesetz kann Ausnahmen von der Benachrichtigungspflicht vorsehen, um bedeutsame Allgemeininteressen oder Rechtsgüter Dritter zu schützen. Solche Ausnahmen sind jedoch auf das unbedingt Erforderliche zu beschränken und müssen dem Gebot der Normenklarheit und Bestimmtheit genügen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 136.

Das BayVSG verfehlt die verfassungsrechtlichen Anforderungen an die nachträgliche Benachrichtigung des Betroffenen für annähernd alle Überwachungsermächtigungen.

Einige Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen sehen eine Benachrichtigung überhaupt nicht vor und sind schon deshalb mangelhaft. Im Einzelnen gilt dies für die Ermächtigungen zum Einsatz

auch eingriffsintensiver nachrichtendienstlicher Mittel wie längerfristiger Bild- und Tonaufzeichnungen (Art. 8 BayVSG), zur (ggfs. wiederum längerfristigen) Ortung von Mobilfunkendgeräten (Art. 12 BayVSG), zum Abruf von Telekommunikations-Bestandsdaten, soweit hierfür auf nach §§ 113a ff. TKG bevorratete Internet-Verkehrsdaten zurückgegriffen wird (Art. 15 Abs. 1 BayVSG i.V.m. § 113 Abs. 1 Satz 3, § 113c Abs. 1 Nr. 3 TKG),

vgl. insoweit BVerfGE 125, 260 (344),

sowie zum Einsatz von Verdeckten Mitarbeitern (Art. 18 BayVSG) und Vertrauensleuten (Art. 19 BayVSG).

Soweit das BayVSG eine Benachrichtigung des Betroffenen überhaupt vorsieht, verweist das Gesetz durchweg auf die Benachrichtigungsregelung des § 12 Abs. 1 G 10 (vgl. Art. 11 Abs. 2 Satz 3, Art. 13 Abs. 2, Art. 17 Abs. 2 Satz 1 BayVSG). Diese Regelung enthält jedoch viel zu weit gefasste Ausschlusstatbestände und verfehlt daher die verfassungsrechtlichen Anforderungen.

Bereits sehr weit geht der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 1 G 10, nach dem die Benachrichtigung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann. Zwar ist die Sicherung des Überwachungszwecks grundsätzlich ein verfassungsrechtlich tragfähiger Grund, die Benachrichtigung zurückzustellen,

BVerfGE 129, 208 (254); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 136.

Indem jedoch § 12 Abs. 1 Satz 2 Alt. 1 G 10 die Benachrichtigung generell sperrt, solange eine Gefährdung des Überwachungszwecks lediglich *nicht auszuschließen* ist, lässt die Norm ihrem Wortlaut nach bereits entfernte Risiken ausreichen, damit der Ausnahmetatbestand greift. Angesichts des weit gefassten Aufklärungsauftrags der Verfassungsschutzbehörden wird sich kaum je mit Sicherheit ausschließen lassen, dass eine Benachrichtigung solche Risiken birgt. § 12 Abs. 1 Satz 2 Alt. 1 G 10 beschränkt die Benachrichtigungspflicht daher unverhältnismäßig weit. Zumindest bedarf die Norm einer verfassungskonformen Auslegung, nach der die Benachrichtigung nur ausgeschlossen ist, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks sprechen,

vgl. die einschränkende Auslegung des (deutlich restriktiver gefassten) Ausnahmetatbestands in § 20w Abs. 2 Satz 1 Hs. 2 BKAG durch BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –

, Rn. 261; ferner zu der Vorgängerregelung des heutigen § 12 G 10 BVerfGE 100, 313 (397 f.).

Unverhältnismäßig und auch keiner verfassungskonformen Auslegung zugänglich ist § 12 Abs. 1 Satz 2 Alt. 2 G 10, der die Benachrichtigung ausschließt, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

Sowohl der Begriff des Bundes- oder Landeswohls als auch der Begriff der übergreifenden Nachteile sind weitgehend unbestimmt und grenzen den Grund für eine Zurückstellung der Benachrichtigung praktisch nicht ein. Letztlich lässt sich unter das Wohl des Bundes oder eines Landes – anders als unter den etwa in § 20w Abs. 2 Satz 1 BKAG genannten Bestand des Staates – der gesamte Aufgabenkreis des Landesamts für Verfassungsschutz oder auch jeder anderen Behörde subsumieren,

vgl. zur Interpretation dieses Begriffs im Rahmen von § 96 StPO Ritzert, in: BeckOK StPO, § 96 Rn. 4: „Der Begriff des Nachteils für das Staatswohl wird weit gefasst und ist bereits gegeben, wenn die Erfüllung öffentlicher Aufgaben ernstlich gefährdet oder erheblich erschwert würde.“

Zudem müssen die befürchteten Nachteile nach dem Wortlaut von § 12 Abs. 1 Satz 2 Alt. 2 G 10 in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird.

Für die Zurückstellung und – auf der Grundlage von § 12 Abs. 1 Satz 5 G 10 – den endgültigen Ausschluss der Benachrichtigung reichen damit annähernd beliebige behördliche Opportunitätserwägungen aus, solange diese aufgrund einer normativ nicht angeleiteten Abwägung wichtiger erscheinen als die Benachrichtigung.

Für die Verfassungsmäßigkeit von § 12 Abs. 1 Satz 2 Alt. 2 G 10 lässt sich nicht anführen, dass dieser Ausschlusstatbestand weitgehend wörtlich dem Urteil des angerufenen Gerichts zur strategischen Telekommunikationsüberwachung nach dem G 10 vom 14. Juli 1999 entnommen ist,

vgl. BVerfGE 100, 313 (398).

Das Bundesverfassungsgericht ist keine Rechtsetzungsinstanz, sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Es kann sinnvoll oder sogar angezeigt sein, im Rahmen verfassungsgerichtlicher Ent-

scheidungen allgemeine, nicht notwendigerweise unmittelbar subsumtionsfähige Formulierungen zu wählen, um so gesetzgeberische Regelungsspielräume offenzuhalten. Hingegen besteht die Aufgabe des Gesetzgebers darin, diese Regelungsspielräume durch einfaches Recht auszufüllen und so die Verfassung zu konkretisieren. Er kann sich dieser Aufgabe zumindest nicht in jedem Fall dadurch entziehen, dass er Formulierungen aus der Rechtsprechung des Bundesverfassungsgerichts schlicht abschreibt.

Insbesondere wäre es sowohl möglich als auch geboten gewesen, den Ausnahmetatbestand zum Schutz des Staatswohls näher zu spezifizieren und auf hinreichend gewichtige Ausnahmegründe zu beschränken. Hierbei hätten auch spezifisch nachrichtendienstliche Belange wie etwa der Quellenschutz oder die Erhaltung von Austauschbeziehungen mit ausländischen Diensten benannt werden können, soweit diese eine Ausnahme von der Benachrichtigungspflicht rechtfertigen können,

> vgl. mit Blick auf die strategische Telekommunikationsüberwachung die beispielhafte Aufzählung bei BVerfGE 100, 313 (398).

2. Auskunftsanspruch des Betroffenen

Die Regelung über den Auskunftsanspruch des Betroffenen in Art. 23 BayVSG genügt ebenfalls nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen, da das Gesetz den Auskunftsanspruch an zu hohe Anforderungen knüpft und zu weitgehend beschränkt.

Der Auskunftsanspruch des Betroffenen über ihn betreffende Datenverarbeitungen ist das grundlegende Datenschutzrecht,

> statt aller Worms, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 19 BDSG Rn. 1.

Das angerufene Gericht hat insbesondere die zentrale Bedeutung dieses Anspruchs für den Grundrechtsschutz betont, wenn eine staatliche Stelle – wie das Landesamt für Verfassungsschutz – zu Informationseingriffen befugt ist, deren Vornahme oder Umfang der Betroffene nicht sicher abschätzen kann, da er in den Informationsverarbeitungsprozess nicht oder nicht stets einbezogen wird, und wenn zudem keine (durchgängige) Pflicht dieser Stelle zur aktiven Benachrichtigung des Betroffenen von Eingriffsmaßnahmen besteht,

> BVerfGE 120, 351 (364).

Gerade in solchen Fallkonstellationen bestehen hohe Anforderungen an Einschränkungen des Auskunftsanspruchs. Eine Einschränkung muss gegenläu-

figen Interessen von höherem Gewicht dienen. Die gesetzlichen Ausschlusstatbestände müssen sicherstellen, dass die betroffenen Interessen einander umfassend und auch mit Blick auf den Einzelfall zugeordnet werden,

> BVerfGE 120, 351 (365); 133, 277 (367 f.); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 137.

Der in Art. 23 BayVSG geregelte Auskunftsanspruch ist nach diesen Maßstäben in dreierlei Hinsicht defizitär, indem er eine Auskunftsversagung ohne Rücksicht auf die Umstände des Einzelfalls vorsieht:

a) Darlegung eines besonderen Auskunftsinteresses

Erstens hat der Betroffene gemäß Art. 23 Abs. 1 Satz 1 BayVSG einen gebundenen Auskunftsanspruch nur, wenn er „ein besonderes Interesse an einer Auskunft darlegt“. Damit wird dem Betroffenen eine Darlegungslast auferlegt, die mit der Transparenzvorstellung nicht vereinbar ist, welche dem Recht auf informationelle Selbstbestimmung zugrunde liegt. Der Auskunftsanspruch soll dem Betroffenen gerade ermöglichen, sich darüber zu orientieren, wer was über ihn weiß und welche Folgen dieses Wissen für ihn haben kann. Die vom Gesetz errichtete Darlegungslast führt hingegen dazu, dass der Betroffene bereits – zumindest ansatzweise – über eine solche Orientierung verfügen muss, da er sonst kein „besonderes“ Auskunftsinteresse begründen kann. Schlimmstenfalls kann der Betroffene seinen Auskunftsanspruch nur geltend machen, wenn er das Landesamt selbst auf gegen ihn bestehende Verdachtsmomente hinweist, die sein Auskunftsinteresse begründen,

> drastische, in der Sache aber zutreffende Kritik hieran bei Kauß/Werkentin, KJ 1991, S. 492 (496): „Verpflichtung zur Selbstdenunziation“.

Ein grundrechtlich anerkanntes Auskunftsinteresse ergibt sich vielmehr bereits daraus, dass der Auskunftspetent möglicherweise Betroffener von Eingriffen in sein Recht auf informationelle Selbstbestimmung oder in andere Bestandteile des grundrechtlichen Informationsschutzes ist. Ein weitergehendes besonderes Interesse kann nur gefordert werden, wenn sich das Auskunftsinteresse des Betroffenen gegen kollidierende staatliche Geheimhaltungsbelange durchsetzen muss. Eine solche Kollisionslage, die mit einer Abwägung zu bewältigen wäre, setzt Art. 23 Abs. 1 Satz 1 BayVSG jedoch nicht voraus. Das verfassungsrechtliche Defizit dieser Norm wird auch nicht dadurch ausgeglichen, dass der Betroffene, wenn er kein besonderes Auskunftsinteresse darlegt, immerhin aus Art. 23 Abs. 1 Satz 2 BayVSG einen Anspruch auf ermes-

sensfehlerfreie Entscheidung über sein Auskunftsbegehren hat. Für ein behördliches Auskunftsermessen ist verfassungsrechtlich jedenfalls dann kein Raum, wenn der Auskunftsanspruch sich auf Datenverarbeitungsprozesse bezieht, die der Betroffene typischerweise nicht vollständig abschätzen kann,

vgl. BVerfGE 120, 351 (364).

b) Keine Auskunft über Herkunft und Empfänger personenbezogener Daten

Zweitens erstreckt sich die Auskunft gemäß Art. 23 Abs. 1 Satz 3 Nr. 1 BayVSG von vornherein nicht auf die Herkunft personenbezogener Daten und die Empfänger von Übermittlungen. Gerade diese Angaben können aber für den Betroffenen besonders wichtig sein, um seine informationelle Stellung einzuschätzen. Dies gilt insbesondere für Auskunftsbegehren gegen Verfassungsschutzbehörden. Diese Behörden müssen seit 2015 miteinander einen umfassenden bundesweiten Informationsverbund unterhalten,

näher Bergemann, NVwZ 2015, S. 1705 f.

Zudem sind sie mit zahlreichen anderen Sicherheitsbehörden eng vernetzt, unter anderem auch in ständigen Kooperationen wie in den sogenannten gemeinsamen Zentren,

vgl. zu dem Zentrenmodell und den damit verbundenen verfassungsrechtlichen Problemen den Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, S. 165 ff.

Damit der Auskunftsanspruch des Betroffenen gegenüber einer Verfassungsschutzbehörde seine grundrechtlich gewährleistete Orientierungswirkung entfalten kann, muss er deshalb grundsätzlich Auskünfte über Informationsflüsse zu der und von der Behörde umfassen. Geheimhaltungsinteressen können einer hierauf bezogenen Auskunft im Einzelfall entgegenstehen und sind dann im Rahmen einer einzelfallbezogenen Abwägung abzuarbeiten, wie sie die Ausschlussgründe in Art. 23 Abs. 2 VSG vorsehen,

vgl. ausdrücklich mit Blick auf Datenbestände von Sicherheitsbehörden BVerfGE 120, 351 (375 f.).

Ein genereller Vorrang des Geheimhaltungsinteresses hinsichtlich der in Art. 23 Abs. 1 Satz 3 Nr. 1 BayVSG genannten Informationen, der einen einzelfallunabhängigen Anspruchsausschluss rechtfertigen könnte, besteht hingegen nicht.

c) Begrenzung auf Daten in strukturierten Dateien

Drittens erstreckt sich der Auskunftsanspruch gemäß Art. 23 Abs. 1 Satz 3 Nr. 2 BayVSG nicht auf Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, der Betroffene macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse.

Der prinzipielle Anspruchsanschluss für Daten außerhalb strukturierter Dateien reicht zu weit, weil unter heutigen informationstechnischen Bedingungen insbesondere auch unstrukturierte elektronische Datenbestände (wie elektronische Akten) mit einer Volltextsuche umfassend erschlossen werden können. Jedenfalls soweit das Landesamt seine Datenbestände selbst elektronisch in solcher Weise erschließen darf, muss auch der Auskunftsanspruch ohne Weiteres bestehen. Ansonsten würde der Betroffene den Risiken, welche die heutigen Möglichkeiten der Informationsverarbeitung für seine Persönlichkeitsrechte mit sich bringen, in weitem Ausmaß ausgesetzt, ohne dies wenigstens durch eine Nutzung dieser Möglichkeiten zugunsten des Persönlichkeitsschutzes zu kompensieren.

Im Zusammenhang mit elektronisch geführten und informationstechnisch erschließbaren Datenbeständen kann dem Betroffenen auch nicht zugemutet werden, über seine Identität hinaus zusätzliche Angaben zu machen. Denn so wird er zur Preisgabe von Informationen gezwungen, die gegebenenfalls wiederum gegen ihn verwendet werden könnten. Ein sachlicher Grund hierfür besteht nicht, wenn die ihn betreffenden Informationen auch ohne zusätzliche Angaben gefunden werden können.

Schließlich geht es im Zusammenhang mit solchen Datenbeständen nicht an, den Auskunftsanspruch von einer Abwägung zwischen dem Informationsinteresse des Betroffenen und dem mit der Auskunftserteilung verbundenen Aufwand abhängig zu machen. Es ist vielmehr Sache des Landesamts, seine Datenverarbeitungsprozesse im Sinne eines *Privacy by Design* von vornherein auf den Schutz des Persönlichkeitsrechts einzurichten und zu gewährleisten, dass die Auskunft mit vertretbarem Aufwand erteilt werden kann.

VI. Übermäßige Befugnisse zu Datenübermittlungen

Das BayVSG ermöglicht dem Landesamt in zu weitem Umfang, die personenbezogenen Daten, die es im Rahmen seiner Aufklärungstätigkeit erhoben hat, an andere Stellen zu übermitteln. Verfassungswidrig sind zum einen die meis-

ten der in Art. 25 BayVSG enthaltenen Übermittlungsermächtigungen (unten 1), zum anderen teilweise auch die Übermittlungsermächtigungen in § 4 Abs. 4 G 10, auf die einige Normen des BayVSG verweisen (unten 2).

1. Übermittlungsermächtigungen in Art. 25 BayVSG

Die Ermächtigungen zu Informationsübermittlungen in Art. 25 BayVSG verfehlen in weitem Umfang die verfassungsrechtlichen Anforderungen. Dies gilt für Übermittlungen an inländische Behörden ebenso wie für Übermittlungen an ausländische, zwischen- oder überstaatliche Einrichtungen sowie an nicht-öffentliche Stellen.

a) Übermittlungen an inländische Behörden

Die vorgesehenen Ermächtigungen des Landesamts, personenbezogene Informationen an inländische Behörden zu übermitteln, gehen teilweise zu weit und stehen mit den Grundrechten der Betroffenen nicht in Einklang.

aa) Verfassungsrechtliche Anforderungen

Das angerufene Gericht hat in seinem Urteil zum Antiterrordateigesetz aus dem Recht auf informationelle Selbstbestimmung hohe Anforderungen an Datenübermittlungen von Nachrichtendiensten an Behörden mit operativen Eingriffsbefugnissen errichtet. Zu beurteilen waren seinerzeit insbesondere Datenübermittlungen an Polizei- und Strafverfolgungsbehörden. Für das Verhältnis der Nachrichtendienste zu diesen Behörden hat das Bundesverfassungsgericht ein informationelles Trennungsprinzip errichtet.

Der Grund hierfür liegt in den unterschiedlichen Aufgaben dieser Behörden, denen unterschiedliche Verteilungen von Datenerhebungs- und Zwangsbefugnissen zugrunde liegen. Bei einer Datenübermittlung von einem Nachrichtendienst an eine Polizei- oder Strafverfolgungsbehörde wirken die weitreichenden Datenerhebungsbefugnisse der Nachrichtendienste mit den weitreichenden operativen Zwangsbefugnissen der Polizei- und Strafverfolgungsbehörden zusammen. Hierin liegt ein besonders schwerer Grundrechtseingriff.

Dieser Eingriff genügt nur dann dem Verhältnismäßigkeitsgrundsatz, wenn er einem herausragenden öffentlichen Interesse dient. Dies muss durch eine hinreichend konkrete und qualifizierte Eingriffsschwelle gesichert sein,

BVerfGE 133, 277 (329).

In seinem Urteil zum BKA-Gesetz hat das angerufene Gericht dieses Erfordernis allgemeingültig für die Zweckänderung, die in einer Datenübermittlung liegt, durch das Kriterium der hypothetischen Datenneuerhebung konkretisiert:

Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Zudem muss sich aus den Daten im Zeitpunkt der Übermittlung ein konkreter Ermittlungsansatz ergeben,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 288 ff.

Es ist Aufgabe des Gesetzgebers der Übermittlungsermächtigung, eine Eingriffsschwelle festzulegen, die den verfassungsrechtlichen Anforderungen genügt. Denn dieser Gesetzgeber trägt eine grundrechtliche Regelungsverantwortung für den Umgang mit den Daten, die er zur Erhebung und dann zur Übermittlung freigibt,

> vgl. BVerfGE 125, 260 (346); 130, 151 (201); ferner BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 305.

Die Übermittlungsermächtigungen in Art. 25 BayVSG werden den verfassungsrechtlichen Anforderungen, die sich aus der jüngeren Rechtsprechung des angerufenen Gerichts ergeben, nicht durchweg gerecht, da sie in erheblichen Teilen zu weit gefasst sind.

bb) Sonderregelung für Übermittlungen an besondere Vollzugsbehörden, Art. 25 Abs. 2 Satz 1 BayVSG

Art. 25 BayVSG unterscheidet hinsichtlich der Übermittlungsschwelle zwischen Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, und sonstigen (insbesondere aus öffentlichen Quellen gewonnenen) Daten des Landesamts. Dies ist eine tragfähige Differenzierung,

> näher zu der unterschiedlichen Eingriffsintensität in beiden Übermittlungskonstellationen Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 249 ff.

Für die sensibleren Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, enthält das Gesetz unterschiedliche Übermittlungstatbestände je nachdem, ob die Daten an die in Art. 25 Abs. 2 Satz 1 BayVSG genannten besonderen Vollzugsbehörden oder an andere Behörden übermittelt werden sollen. Die in Art. 25 Abs. 2 Satz 1 Nr. 1 BayVSG enthaltene Übermittlungsermächtigung ist in materieller Hinsicht verfassungsrechtlich unbedenklich. Zu weit und daher verfassungswidrig sind hingegen die Ermächtigungen in Art. 25 Abs. 2 Satz 1 Nr. 2 und Nr. 3 BayVSG Bedenken.

Zu weit gefasst sind sämtliche Übermittlungstatbestände des Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG. Soweit diese Regelung eine Informationsübermittlung zur Verfolgung von Straftaten von erheblicher Bedeutung vorsieht, ist sie deshalb unzureichend, weil der Begriff der Straftat von erheblicher Bedeutung nicht konkretisiert und begrenzt wird. Nach gängiger Auffassung im strafprozessrechtlichen Schrifttum können als Straftaten von erheblicher Bedeutung bereits Delikte aus dem Bereich der mittleren Kriminalität anzusehen sein,

> vgl. etwa zu § 98a StPO Ritzert, in: BeckOK-StPO, § 98a Rn. 1: schon Vergehen mit einer Strafrahmenobergrenze über zwei Jahren.

Da auf der Grundlage von Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG auch Informationen übermittelt werden können, die mit eingriffsintensiven nachrichtendienstlichen Mitteln wie etwa längerfristigen Bild- und Tonaufzeichnungen außerhalb von Wohnungen oder dem personengerichteten Einsatz eines Verdeckten Mitarbeiters gewonnen wurden, reicht diese Eingriffsschwelle nicht durchweg aus, um die Übermittlung zu rechtfertigen,

> vgl. zu dem insoweit gleichlautenden § 19 BVerfSchG Bergemann, NVwZ 2015, S. 1705 (1707 f.).

Vielmehr müssen die Straftaten, zu deren Verfolgung die Übermittlung ermöglicht werden soll, so schwer wiegen, dass die übermittelten Informationen auch auf der Grundlage einer strafprozessualen Ermächtigung erlangt werden könnten. Unerheblich ist insoweit, ob die Informationen strafprozessual als Beweismittel oder lediglich als Spurenansatz verwendet werden sollen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 315.

Soweit Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG eine Informationsübermittlung auch zur Verhinderung oder zur sonstigen Verhütung von Straftaten von erheblicher Bedeutung ermöglicht, vertiefen sich die verfassungsrechtlichen Bedenken noch. Hierfür gibt es zwei Gründe:

Erstens droht der strafprozessuale Begriff der Straftat von erheblicher Bedeutung diesen präventiv ausgerichteten Übermittlungstatbestand zu entgrenzen. Wenn durch eine Straftat Schäden für besonders bedeutsame Rechtsgüter konkret drohen, ist bereits der verfassungsrechtlich unbedenkliche Übermittlungstatbestand des Art. 25 Abs. 1 Satz 1 Nr. 1 BayVSG verwirklicht. Einer weiteren Übermittlungsermächtigung, die spezifisch auf die Kriminalpräven-

tion zugeschnitten ist, bedarf es insoweit nicht. Allerdings finden sich im materiellen Strafrecht zahlreiche Deliktstatbestände, die Handlungen im Vorfeld strafbarer Rechtsgutsverletzungen bei Strafe verbieten. Insbesondere das Terrorismusstrafrecht zeichnet sich durch eine nahezu flächendeckende Vorfeldkriminalisierung aus. Viele dieser Straftaten sind schon wegen hoher Strafandrohungen ohne weiteres als Straftaten von erheblicher Bedeutung anzusehen. Der Verdacht auf eine solche Straftat kann im strafrechtlichen Ermittlungsverfahren eingriffsintensive Überwachungsmaßnahmen rechtfertigen,

> vgl. beispielhaft § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) – Freiheitsstrafe von sechs Monaten bis zu zehn Jahren; § 129a Abs. 1 und 2 StGB (Bildung einer terroristischen Vereinigung) – Freiheitsstrafe von einem Jahr bis zu zehn Jahren.

Wird jedoch der materiell-strafrechtliche Vorfeldansatz mit den Regelungsmustern präventivpolizeilicher Eingriffsermächtigungen verbunden, so droht der Eingriffsanlass zu entgrenzen, indem die strafrechtliche Vorverlagerung noch ausgedehnt wird,

> vgl. zu der parallelen Problematik im Zusammenhang mit der Überwachungsermächtigung des Art. 13 BayVSG i.V.m. § 3 Abs. 1 G 10 oben II. 5. b).

Soweit ein eigenständiger Übermittlungstatbestand für Zwecke der polizeilichen Kriminalprävention in Art. 25 Abs. 2 Satz 1 BayVSG überhaupt erforderlich sein sollte, hätten die Straftaten, die eine Datenübermittlung rechtfertigen, nach spezifisch präventivpolizeilichen Kriterien ausgewählt und enumerativ aufgezählt werden müssen. Nur so hätte der Gesetzgeber gewährleisten können, dass der Übermittlung in jedem Fall ein verfassungsrechtlich hinreichender Ermittlungsansatz zugrunde liegt,

> vgl. allgemein zu den Bedenken gegen unreflektiert aus dem Strafprozessrecht übernommene Straftatenkataloge in präventivpolizeilichen Eingriffsermächtigungen BVerfGE 125, 260 (329); Bäcker, Kriminalpräventionsrecht, 2015, S. 349 ff.

Zweitens ermöglicht Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG Datenübermittlungen auch, um Straftaten zu verhüten. Der Begriff der Straftatverhütung soll nach der Gesetzesbegründung auf Bedrohungslagen im Vorfeld konkreter Gefahren verweisen,

> LT-Drs. 17/10014, S. 51.

Dieses Begriffsverständnis deckt sich mit weiten Teilen der Gesetzgebungspraxis, Rechtsprechung und Literatur zum Polizeirecht,

> vgl. nur Denninger, in: Lisken/ders. (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. D 1 ff., m.w.N.

Der unscharfe Begriff der Verhütung von Straftaten gewährleistet jedoch nicht in jedem Fall, dass der Übermittlung der verfassungsrechtlich erforderliche Ermittlungsansatz zugrunde liegt. Die verfassungsrechtlichen Grenzen sind daher zumindest insoweit überschritten, als auf dieser vagen Grundlage auch Informationen übermittelt werden können, die durch eingriffsintensive Überwachungsmaßnahmen wie Tonaufnahmen außerhalb von Wohnungen oder den Einsatz von Verdeckten Mitarbeitern oder Vertrauensleuten gewonnen wurden,

> vgl. zum insoweit gleichlautenden § 20v Abs. 5 Satz 1 Nr. 2 BKAG BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 313.

Bei der Übermittlung von Daten, die durch eine Wohnraumüberwachung oder eine „Online-Durchsuchung“ gewonnen wurden, ist neben Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG die besondere Zweckbestimmung in Art. 11 Abs. 3 BayVSG anzuwenden. Auch im Zusammenwirken beider Regelungen gewährleistet das Gesetz jedoch nicht durchweg, dass die besonders hohen verfassungsrechtlichen Anforderungen gewahrt werden, die an die zweckändernde Übermittlung solcher Daten zu stellen sind,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 291.

Defizitär ist insbesondere Art. 11 Abs. 3 Nr. 2 BayVSG, der im Zusammenwirken mit Art. 25 Abs. 2 Satz 1 Nr. 2 BayVSG eine Datenübermittlung pauschal zur Verhinderung oder Verhütung von Straftaten im Sinne von § 100c Abs. 2 StPO erlaubt. Insbesondere der unscharfe Begriff der Verhütung gewährleistet wiederum nicht, dass die Datenübermittlung an eine konkrete Gefahr im verfassungsrechtlichen Sinne gebunden wird, wie dies geboten ist. Zudem enthält der Straftatkatalog des § 100c Abs. 2 StPO auch strafrechtliche Vorfeldtatbestände wie § 89a oder § 129a StGB, deren bevorstehende Verwirklichung nicht zwingend auf eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut schließen lässt.

Verfassungsrechtlich unzulänglich ist schließlich die in Art. 25 Abs. 2 Satz 1 Nr. 3 BayVSG enthaltene Übermittlungsermächtigung. Diese Norm greift zwar

mit dem Kriterium der hypothetischen Datenneuerhebung einen Regelungsansatz auf, der grundsätzlich den verfassungsrechtlichen Anforderungen genügt. Zu beanstanden ist aber, dass Art. 25 Abs. 2 Satz 1 Nr. 3 BayVSG keinen eigenständigen Übermittlungstatbestand enthält, sondern für die hypothetische Datenneuerhebung auch auf Datenerhebungsermächtigungen aus dem Recht des Bundes oder anderer Länder als Bayern Bezug nimmt. Indem jedoch der bayerische Gesetzgeber dem Landesamt für Verfassungsschutz bestimmte Datenerhebungen erlaubt, übernimmt er eine grundrechtliche Regelungsverantwortung für den Umgang mit den erhobenen Daten,

vgl. BVerfGE 125, 260 (345 f.); 130, 1 (34).

Er muss daher die Voraussetzungen einer Datenübermittlung selbst abschließend und normenklar festlegen. Hingegen kann sich der bayerische Gesetzgeber seiner Regelungsverantwortung nicht dadurch entledigen, dass er in einer Übermittlungsermächtigung dynamisch auf Normen anderer Gesetzgeber verweist,

vgl. zu der parallelen Problematik dynamischer Verweisungen im Tatbestand von Überwachungsermächtigungen oben II. 5. a); spezifisch zu Übermittlungsermächtigungen Bäcker, Kriminalpräventionsrecht, 2015, S. 488.

cc) Informationübermittlung wegen Staatsschutzdelikten, Art. 25 Abs. 2 Satz 2 BayVSG

Gleichfalls zu weit gefasst ist die Übermittlungsermächtigung in Art. 25 Abs. 2 Satz 2 BayVSG mit ihrem Verweis auf § 20 BVerfSchG.

Nach diesen Normen muss das Landesamt Informationen an die Polizei- und Strafverfolgungsbehörden übermitteln, wenn die Informationen benötigt werden, um Staatsschutzdelikte zu verhindern oder zu verfolgen. Der damit maßgebliche Begriff des Staatsschutzdelikts wird in § 20 Abs. 1 Satz 2 BVerfSchG definiert. Er reicht viel zu weit und umfasst bei entsprechender Motivation des Täters auch Straftaten von geringem Gewicht wie Beleidigungen oder Sachbeschädigungen, deren Verhinderung oder Verfolgung die Übermittlung von Daten nicht rechtfertigen kann, die aus eingriffsintensiven Überwachungsmaß-

nahmen stammen. Nur am Rande sei angemerkt, dass andererseits befremdlicherweise nie eine Übermittlungspflicht bei Straftaten ohne Staatsschutzbezug besteht, selbst wenn es sich um schwerste Kriminalität handelt,

> eingehend zu den Bedenken gegen § 20 BVerfSchG Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 318 ff.

dd) Allgemeine Übermittlungsermächtigung, Art. 25 Abs. 1 BayVSG

Die allgemeine Übermittlungsermächtigung in Art. 25 Abs. 1 BayVSG begegnet insoweit keinen verfassungsrechtlichen Bedenken, als sie eine Übermittlung von Informationen ermöglicht, die das Landesamt ohne Rückgriff auf nachrichtendienstliche Mittel – insbesondere also durch die Auswertung öffentlich zugänglicher Quellen – erlangt hat. Der Gesetzgeber darf nach dem Kriterium der hypothetischen Datenneuerhebung der allenfalls geringen Eingriffsintensität einer solchen Informationserhebung Rechnung tragen, indem die Anforderungen an eine Übermittlung der Informationen gleichfalls abgesenkt werden.

Verfassungswidrig ist Art. 25 Abs. 1 BayVSG jedoch insoweit, als diese Norm unter niedrigen Voraussetzungen ausdrücklich auch eine Übermittlung von Informationen zulässt, die mit nachrichtendienstlichen Mitteln gewonnen wurden.

Art. 25 Abs. 1 Nr. 1 BayVSG erlaubt eine Übermittlung solcher Informationen generell für Zwecke der öffentlichen Sicherheit. Da der Begriff der öffentlichen Sicherheit die Integrität der gesamten Rechtsordnung umfasst und fast jede Behörde berufen ist, zur Wahrung der Rechtsordnung beizutragen, wird so eine Übermittlung an nahezu beliebige Empfangsbehörden ermöglicht, wenn die Übermittlung nur nützlich sein kann, damit diese Behörden ihre Aufgaben erfüllen können. Eine qualifizierte Übermittlungsschwelle hinsichtlich der zu schützenden Rechtsgüter oder des Übermittlungsanlasses fehlt auch für Informationen, die aus eingriffsintensiven Maßnahmen wie längerfristigen Film- und Tonaufzeichnungen außerhalb von Wohnungen oder dem Einsatz von Verdeckten Mitarbeitern stammen.

Dieser Regelung liegt ein zu enges Verständnis der Aussagen zugrunde, die das angerufene Gericht in seinem Urteil zur Antiterrordatei getroffen hat. Das angerufene Gericht hatte sich dort – entsprechend dem Zuschnitt der Antiterrordatei – unmittelbar allein mit einem Datenaustausch zwischen Nachrichtendiensten einerseits und Polizei- und Strafverfolgungsbehörden andererseits zu

befassen. Dementsprechend hat es das informationelle Trennungsprinzip ausdrücklich auf das Verhältnis dieser Behörden zueinander bezogen. Daraus lässt sich jedoch nicht folgern, dass hohe Übermittlungsschranken nur im Verhältnis der Nachrichtendienste zu Empfangsbehörden mit spezifisch polizeilichen Zwangsbefugnissen bestehen,

so aber anscheinend die Gesetzesbegründung, LT-Drs. 17/10014, S. 50 f.

Vielmehr muss der Ableitungszusammenhang des informationellen Trennungsprinzips einbezogen werden,

BVerfGE 133, 277 (324 ff.).

Die Ausführungen des angerufenen Gerichts gehen von den unterschiedlichen Aufgaben und Befugnissen der Nachrichtendienste einerseits und der anderen in dem Urteil behandelten Behörden andererseits aus. Eine Datenübermittlung von einem Nachrichtendienst an eine andere Behörde bewirkt dann und deshalb einen besonders schweren Grundrechtseingriff, wenn durch sie die weitreichenden Befugnisse der Nachrichtendienste zu verdeckten Informationserhebungen mit weitreichenden Befugnissen zu imperativen Grundrechtseingriffen verbunden werden. Dementsprechend nennt das Urteil als Behörden, deren Tätigkeit grundlegend anders zugeschnitten ist als die der Nachrichtendienste, neben Polizeibehörden ausdrücklich auch (sonstige) Sicherheitsbehörden,

BVerfGE 133, 277 (327).

Diese Erwägungen legen nahe, das informationelle Trennungsprinzip auf das Verhältnis der Nachrichtendienste zu Sonderordnungsbehörden zu übertragen, die gleichfalls über einschneidende imperative Befugnisse verfügen können. So können Eingriffsmaßnahmen von Gewerbeaufsichts- oder Ausländerbehörden aus Sicht der Betroffenen ebenso schwere, mitunter sogar schwerere Folgen haben als Eingriffsmaßnahmen der Polizei oder auch als eine strafrechtliche Verurteilung. Daher leuchtet es nicht ein, dass Informationsübermittlungen an solche Behörden den Nachrichtendiensten ohne signifikante Eingriffsschwelle möglich sein sollen, während Übermittlungen an Polizei- und Strafverfolgungsbehörden als besonders schwere Eingriffe nur ausnahmsweise unter restriktiven Bedingungen zulässig sein können.

Das Urteil zum BKA-Gesetz, welches das – teilweise modifizierte – Regelungskonzept der hypothetischen Datenneuerhebung als verfassungsrechtlich

gebotene Vorgabe für Zweckänderungen entfaltet hat, bestätigt diesen Befund. Denn danach muss die Eingriffsschwelle für eine Informationsübermittlung hinsichtlich der geschützten Rechtsgüter den Anforderungen an die Erhebung der Informationen genügen und ist ein hinreichend konkreter Übermittlungsanlass festzulegen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 287 ff.

Die in Art. 25 Abs. 1 Nr. 1 BayVSG vorgesehenen Tatbestände können daher eine Übermittlung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, zumindest in der Regel nicht legitimieren. Für die Übermittlung solcher Informationen sind enger begrenzte Eingriffsschwellen sowohl hinsichtlich der zu schützenden Rechtsgüter als auch hinsichtlich des Übermittlungsanlasses verfassungsrechtlich geboten.

Verfassungswidrig ist daneben auch der noch weiter gefasste Art. 25 Abs. 1 Nr. 2 BayVSG, der Datenübermittlungen auch zur Erfüllung anderer behördlicher Aufgaben erlaubt, wenn die Empfangsbehörde „zum Schutz der freiheitlichen demokratischen Grundordnung beizutragen oder Gesichtspunkte der öffentlichen Sicherheit oder auswärtige Belange zu würdigen hat“. Diese Formulierung gibt die Übermittlung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, praktisch vollständig frei, da so gut wie jede Behörde berufen ist, die genannten Belange zu beachten. Die in lit. b als Regelbeispiel genannte geplante Ordensvergabe, die eine Übermittlung von Informationen aus eingriffsintensiven verdeckten Überwachungsmaßnahmen auch ohne Einwilligung des Betroffenen rechtfertigen soll, illustriert dies.

b) Auslandsübermittlungen, Art. 25 Abs. 3 Nr. 2 BayVSG

Die in Art. 25 Abs. 3 Nr. 2 BayVSG enthaltene Ermächtigung zur Informationsübermittlung an ausländische, zwischen- und überstaatliche Stellen steht hinsichtlich von Informationen, die durch den Einsatz eingriffsintensiver nachrichtendienstlicher Mittel gewonnen wurden, gleichfalls nicht mit den verfassungsrechtlichen Anforderungen in Einklang.

Eine Ermächtigung zu Auslandsübermittlungen muss hinsichtlich der Übermittlungsschwelle den Anforderungen an eine Zweckänderungsermächtigung ge-

nügen, einen datenschutzrechtlich angemessenen Umgang mit den übermittelten Daten im Empfängerstaat voraussetzen und eine wirksame inländische Kontrolle ermöglichen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 329 ff.

Art. 25 Abs. 3 Nr. 2 BayVSG leistet nichts davon. Die Norm ermöglicht eine Übermittlung zur Wahrung unspezifischer „erheblicher Sicherheitsinteressen“ des Empfängers, ohne die zu schützenden Rechtsgüter oder den Übermittlungsanlass auch nur ansatzweise zu konkretisieren. Zu dem Datenschutzniveau bei der Empfangsstelle finden sich überhaupt keine Vorgaben. Zudem sind die vorgesehenen verfahrensrechtlichen Sicherungen viel zu schwach ausgestaltet. Sie beschränken sich im Wesentlichen auf den in Art. 25 Abs. 4 Satz 3 BayVSG vorgesehenen Vorbehalt einer „Bitte“ des Landesamts um Auskunft über die Verwendung der übermittelten Informationen.

c) Übermittlungen an nicht-öffentliche Stellen, Art. 25 Abs. 3 Nr. 3 BayVSG

Die Ermächtigung in Art. 25 Abs. 3 Nr. 3 BayVSG, Informationen an nicht-öffentliche Stellen zu übermitteln, verfehlt ebenfalls die verfassungsrechtlichen Anforderungen, soweit sie sich auf Informationen erstreckt, die mit nachrichtendienstlichen Mitteln gewonnen wurden.

Eine solche Übermittlung begründet ein gewichtiges Risiko, dass hochsensible Informationen durch Privatpersonen, die nicht den Bindungen und Kontrollen hoheitlicher Stellen unterliegen, versehentlich oder sogar missbräuchlich zweckfremd verwendet werden. Dieses Risiko ist nur in besonders gewichtigen Fällen hinnehmbar, die durch eine qualifizierte Eingriffsschwelle zu beschreiben sind. Hieran fehlt es in Art. 25 Abs. 3 Nr. 3 BayVSG, der eine Übermittlung letztlich generell zur Aufgabenerfüllung des Landesamts zulässt. Darüber hinaus fehlt es auch für Datenübermittlungen an nicht-öffentliche Stellen an geeigneten und hinreichend zuverlässigen verfahrensrechtlichen Sicherungen, um die besonderen Risiken solcher Übermittlungen für die Betroffenen einzuhegen.

2. Übermittlungen nach Maßgabe von § 4 Abs. 4 G 10

Sonderregelungen für Datenübermittlungen enthalten Art. 13 Abs. 2 und Art. 17 Abs. 2 Satz 1 BayVSG. Diese Regelungen verweisen hinsichtlich von Informationen, die durch die in Art. 13, Art. 15 Abs. 2 und Abs. 3 sowie Art. 16

BayVSG geregelten eingriffsintensiven Überwachungsmaßnahmen gewonnen wurden, auf die in § 4 Abs. 4 G 10 enthaltenen Übermittlungsermächtigungen.

Es liegt nahe, diese Verweisungen als dynamische Verweisungen auf § 4 Abs. 4 G 10 in seiner jeweils geltenden Fassung zu interpretieren. Jedoch ist die Regelung der Eingriffsschwellen für Datenübermittlungen als wesentliche Frage anzusehen, die der bayerische Landesgesetzgeber selbst zu regeln ist. Er kann seine grundrechtliche Regelungsverantwortung nicht durch eine dynamische Verweisung auf eine bundesrechtliche Vorschrift auf den Bundesgesetzgeber abwälzen,

siehe oben VI. 1. a) bb).

Darüber hinaus verfehlen die in § 4 Abs. 4 Nr. 1 und Nr. 2 G 10 enthaltenen Übermittlungsermächtigungen inhaltlich in weiten Teilen die verfassungsrechtlichen Anforderungen.

a) Datenübermittlungen zur Strafverfolgung, § 4 Abs. 4 Nr. 2 G 10

Dies gilt zunächst für § 4 Abs. 4 Nr. 2 G 10, der Datenübermittlungen zum Zweck der Strafverfolgung regelt. Die Norm setzt den Verdacht einer Straftat aus den Katalogen von § 3 Abs. 1 und Abs. 1a und § 7 Abs. 4 Satz 1 G 10 sowie mittelbar von § 100a Abs. 2 StPO voraus. Die Katalogtaten wiegen jedoch nicht durchweg schwer genug, um eine Übermittlung von Daten zu rechtfertigen, die durch die von Art. 13, Art. 15 Abs. 2 und Abs. 3 sowie Art. 16 BayVSG geregelten eingriffsintensiven Überwachungsmaßnahmen gewonnen wurden.

Nach dem Kriterium der hypothetischen Datenneuerhebung müssen die Anlasstaten der Datenübermittlung schwer genug wiegen, um auch die ursprüngliche Datenerhebungsmaßnahme zu rechtfertigen. Als Referenzmaßnahme für die hypothetische Datenneuerhebung ist hier die Telekommunikationsüberwachung heranzuziehen. Der ebenfalls erfasste Abruf von Telekommunikations-Verkehrsdaten steht der Inhaltsüberwachung hinsichtlich der Eingriffsintensität angesichts der heutigen Auswertungsmöglichkeiten nicht mehr nach.

Eine Telekommunikationsüberwachung kann im Strafverfahren verfassungsrechtlich nur gerechtfertigt werden, wenn sie dazu dient, eine schwere Straftat zu verfolgen. Dazu ist neben einer gesetzlichen Höchststrafe von mindestens fünf Jahren zu verlangen, dass die Tat besonders bedeutsame Rechtsgüter bedroht oder schädigt und auch im Einzelfall schwer wiegt,

vgl. BVerfGE 129, 208 (243 f.).

Nach diesem Maßstab wiegen zumindest die folgenden Katalogtaten angesichts ihrer niedrigen Strafrahmen nicht hinreichend schwer:

Straftatbestand	Katalogtat nach	Strafrahmen (Freiheitsstrafe)
§ 85 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis drei Jahre
§ 86 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis drei Jahre
§ 89b StGB	§ 7 Abs. 4 Satz 1 Nr. 1 lit. a G 10	Bis drei Jahre
§ 97 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Bis drei Jahre
§ 109g Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Bis zwei Jahre
§ 95 Abs. 1 Nr. 8 AufenthaltsG	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 7 G 10	Bis ein Jahr
§ 20 Abs. 1 Nr. 1-4 VereinsG	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis ein Jahr

Ob im Übrigen die weiteren Katalogtaten durchweg besonders bedeutsame Rechtsgüter schützen, erscheint zumindest fragwürdig. Schließlich verlangt § 4 Abs. 4 Nr. 2 G 10 nicht, dass die Tat auch im Einzelfall schwer wiegt.

b) Datenübermittlungen zu präventivpolizeilichen Zwecken, § 4 Abs. 4 Nr. 1 G 10

In noch weiterem Umfang verfassungswidrig ist die Ermächtigung zu Datenübermittlungen zu präventivpolizeilichen Zwecken in § 4 Abs. 4 Nr. 1 G 10. Diese Norm macht die Datenübermittlung von dem Verdacht abhängig, dass jemand eine Straftat aus den Katalogen von § 3 Abs. 1 und Abs. 1a sowie § 7 Abs. 4 Satz 1 G 10 plant oder begeht.

Zunächst ist wiederum zu bemängeln, dass sich diese Straftatenkataloge nicht durchweg auf schwere Straftaten beschränken, sondern auch Tatbestände der einfachen und vereinzelt sogar der Bagatellkriminalität enthalten.

Zudem gewährleistet diese Übermittlungsermächtigung mit der Ausdehnung des Eingriffsanlasses auf das Planungsstadium nicht durchweg, dass die Übermittlung an einen konkreten Ermittlungsansatz anknüpft. Überdies führen die in Bezug genommenen Straftatkataloge auch strafrechtliche Vorfeldtatbestände wie § 89a und § 129a StGB auf. Insbesondere wenn die Planungsalternative mit einem solchen Vorfeldtatbestand verbunden wird, kommt es zu einer fast vollständigen Entgrenzung des Übermittlungsanlasses in tatsächlicher Hinsicht, die das Erfordernis eines konkreten Ermittlungsansatzes weit verfehlt,

> vgl. zu der gleichartigen Tatbestandsfassung in der Überwachungsermächtigung des § 3 Abs. 1 G 10 und zur Kritik daran oben II. 5. b).

(Prof. Dr. Bäcker, LL.M.)