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

Mannheim, den 1. August 2017

Bayerischer Verfassungsgerichtshof
80097 München

Popularklage

1. der Frau Katharina Schulze,
   Maximilianeum, 81627 München,
2. des Herrn Ludwig Hartmann,
   Maximilianeum, 81627 München,
3. des Herrn Jürgen Mistol,
   [redacted]

– Klägerin und Kläger –

g e g e n

Art. 5 Abs. 1 Satz 1,

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. 20 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)

sowie

Art. 30 Abs. 3 des Bayerischen Datenschutzgesetzes vom 23. Juli 1993, zuletzt geändert durch Gesetz vom 22. Dezember 2015 (BayGVBl S. 458),

und

Meinungsverschiedenheit

der Fraktion BÜNDNIS 90/DIE GRÜNEN im Bayerischen Landtag,
vertreten durch die Vorsitzenden Katharina Schulze und Ludwig Hartmann,
Maximilianeum, 81627 München,

– Antragstellerin –

g e g e n

1. die CSU-Fraktion im Bayerischen Landtag,
   vertreten durch den Vorsitzenden Thomas Kreuzer,
   Maximilianeum, 81627 München,
2. die Bayerische Staatsregierung,
   vertreten durch den Ministerpräsidenten Horst Seehofer,
   Bayerische Staatskanzlei,
   Franz-Josef-Strauß-Ring 1, 80539 München.

– Antragsgegnerinnen –

Namens und in beigefügter Vollmacht **(Anlage 1)** der Klägerin, der Kläger und der Antragstellerin beantrage ich, die oben genannten Vorschriften des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Datenschutzgesetzes für nichtig zu erklären, weil und soweit sie die Verfassung des Freistaates Bayern verletzen. Im Einzelnen rüge ich Verletzungen von Art. 2, Art. 3 Abs. 1 Satz 1, Art. 100, Art. 101, Art. 106 Abs. 3 und Art. 118 Abs. 1 BV.

Hilfsweise für den Fall, dass der Verfassungsgerichtshof den Antrag im Verfahren der Meinungsverschiedenheit ganz oder teilweise für unzulässig hält, erkläre ich für die Antragstellerin den Beitritt zu der Popularklage, soweit das Verfahren der Meinungsverschiedenheit unzulässig ist.

Gliederung

A. Sachverhalt

Die Popularklage und die Meinungsverschiedenheit richten sich gegen Regelungen des am 1. August 2016 in Kraft getretenen Bayerischen Verfassungsschutzgesetzes (im Folgenden: BayVSG). Gegenstände dieser Regelungen sind Ermächtigungen zu verschiedenen verdeckten Überwachungsmaßnahmen und damit zusammenhängende Verfahrensvorgaben, Ermächtigungen zur Übermittlung personenbezogener Daten sowie die Ermächtigung zur Speicherung personenbezogener Daten über Minderjährige.

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 Bundesverfassungsgerichts folgenden verfassungsrechtlichen Anforderungen umsetzen,

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

Gegenstand der Popularklage und der Meinungsverschiedenheit sind verschiedene Ermächtigungen des Bayerischen Landesamts für Verfassungsschutz (im Folgenden: Landesamt), durch verdeckte Überwachungsmaßnahmen und Datenübermittlungen an andere Stellen in Grundrechte einzugreifen. Zudem erstrecken sich die Anträge auf Verfahrensregelungen und Kontrollvorgaben, die mit diesen Ermächtigungen zusammenhängen. Schließlich richten sich die Anträge gegen die weitreichende Ermächtigung des Landesamts zur Verarbeitung und Nutzung personenbezogener Daten über Minderjährige.

Im Einzelnen richten sich die Popularklage und die Meinungsverschiedenheit gegen die gesetzlichen Ermächtigungen zu folgenden Überwachungsmaßnahmen:

- Einsatz nachrichtendienstlicher Mittel (Art. 8 BayVSG),
- Wohnraumüberwachung (Art. 9 BayVSG),
- „Online-Durchsuchung“ (Art. 10 BayVSG),
- Ortung von Mobilfunkendgeräten (Art. 12 BayVSG),
- „Quellen-Telekommunikationsüberwachung“ (Art. 13 BayVSG),

- Auskunftsersuchen betreffend Transaktionsdaten aus den Bereichen Post, Telemedien und Telekommunikation (Art. 15 Abs. 2 und Abs. 3 BayVSG),
- Auskunftsersuchen betreffend Transaktionsdaten aus den Bereichen Luftfahrt und Kreditwesen (Art. 16 BayVSG),
- Einsatz Verdeckter Mitarbeiter (Art. 18 BayVSG),
- Einsatz von Vertrauensleuten (Art. 19 BayVSG).

Gegenstand der Rügen sind die materiellen Eingriffsschwellen dieser Regelungen sowie zugehörige Verfahrensregelungen zum Schutz besonders sensibler Äußerungen und zur Gewährleistung von Transparenz und effektivem Rechtsschutz. Hinsichtlich der Ermächtigungen zu „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ sind auch die technisch-sozialen Modalitäten der Infiltration informationstechnischer Systeme zur Durchführung von Überwachungen von den Anträgen umfasst.

Darüber hinaus richten sich die Popularklage und die Meinungsverschiedenheit gegen folgende weitere Regelungen:

- die allgemeine Ermächtigung des Landesamts zur Verarbeitung und Nutzung personenbezogener Daten, soweit sie sich auf Daten über Minderjährige erstreckt (Art. 5 Abs. 1 Satz 1 BayVSG),
- die gesetzlichen Verpflichtungen des Staatsministeriums des Innern und des Parlamentarischen Kontrollgremiums zur Berichterstattung über bestimmte Überwachungsmaßnahmen des Landesamts (Art. 20 Abs. 1 BayVSG),
- bestimmte Beschränkungen des Auskunftsanspruchs des von Datenverarbeitungen des Landesamts Betroffenen (Art. 23 BayVSG),
- 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 einige Regelungen des BayVSG verweisen) und
- die Verteilung der aufsichtlichen Kontrolle des Landesamts zwischen der G 10-Kommission des Bayerischen Landtags und dem Bayerischen Landesbeauftragten für den Datenschutz (Art. 30 Abs. 3 BayDSG sowie Art. 2 AGG 10, auf den einige Regelungen des BayVSG verweisen).

II. Antragstellerin, Klägerin und Kläger

Die Antragstellerin im Verfahren der Meinungsverschiedenheit ist eine Fraktion des 2013 zusammengetretenen 17. Bayerischen Landtags.

Die Klägerin zu 1 im Popularklageverfahren ist Doktorandin an der Ludwig-Maximilians-Universität München. Sie ist seit 2013 Abgeordnete des Bayerischen Landtags und gehört der Antragstellerin an.

Der Kläger zu 2 im Popularklageverfahren ist Kommunikationsdesigner. Er ist seit 2008 Abgeordneter des Bayerischen Landtags und gehört der Antragstellerin an.

Der Kläger zu 3 im Popularklageverfahren ist examinierter Krankenpfleger. Er ist seit 2013 Abgeordneter des Bayerischen Landtags und gehört der Antragstellerin an.

Die Klägerin und die Kläger erheben die Popularklage nicht in ihrer Eigenschaft als Landtagsabgeordnete, sondern als natürliche Personen.

III. Vorbringen der Antragstellerin im Gesetzgebungsverfahren

Die Antragstellerin hat während des Gesetzgebungsverfahrens wiederholt gerügt, dass die seinerzeit geplanten und nunmehr in Kraft getretenen Regelungen des BayVSG in weitem Umfang Grundrechte verletzen.

Bereits in der ersten Lesung des Entwurfs des neuen BayVSG im Bayerischen Landtag brachte die innenpolitische Sprecherin der Antragstellerin – die Popularklägerin zu 1 – verfassungsrechtliche Bedenken gegen den Entwurf vor,

> vgl. Plenarprotokoll 17/66 vom 25. Februar 2016 **(Anlage 2)**, S. 5562 f.

Im weiteren Verlauf des Gesetzgebungsverfahrens führten die Ausschüsse für Kommunale Fragen, Innere Sicherheit und Sport sowie für Verfassung, Recht und Parlamentsfragen des Bayerischen Landtags am 27. April 2016 – maßgeblich auf Betreiben der Antragstellerin – eine gemeinsame öffentliche Anhörung von Sachverständigen zu dem geplanten Gesetz durch. Den Stellungnahmen der Sachverständigen lag ein Fragenkatalog zugrunde, den die Ausschüsse zuvor zusammengestellt hatten und der in vielfacher Hinsicht Fragen der Vereinbarkeit der geplanten Eingriffsermächtigungen mit höherrangigem Recht zum Gegenstand hatte,

> vgl. Wortlautprotokoll der öffentlichen Anhörung vom 27. April 2016 **(Anlage 3)**, S. 4 ff.

Im Rahmen der Anhörung wurde von mehreren der geladenen Sachverständigen in vielfacher Hinsicht eine verfassungsrechtlich begründete Kritik an dem Gesetzentwurf geübt. Die innenpolitische Sprecherin der Antragstellerin griff diese Kritik in ihrer Wortmeldung auf und spitzte sie teils zu,

> vgl. Wortlautprotokoll der öffentlichen Anhörung vom 27. April 2016, S. 29 f.

Die innenpolitische Sprecherin der Antragstellerin wiederholte und vertiefte ihre Kritik sowohl in der abschließenden Sitzung des Innenausschusses,

> vgl. Protokoll der Sitzung des Innenausschusses vom 8. Juni 2016 **(Anlage 4)**, S. 19 ff.,

als auch bei der zweiten Lesung des Gesetzes im Plenum des Bayerischen Landtags,

> vgl. Plenarprotokoll 17/78 vom 7. Juli 2016 **(Anlage 5)**, S. 6693 ff.

B. Zulässigkeit

Sowohl die Popularklage (unten I) als auch der Antrag im Verfahren der Meinungsverschiedenheit (unten II) sind zulässig. Hilfsweise für den Fall, dass der Verfassungsgerichtshof den Antrag im Verfahren der Meinungsverschiedenheit ganz oder teilweise für unzulässig hält, tritt die Antragstellerin der Popularklage bei (unten III).

I. Popularklage

Die Klägerin und die Kläger sind gemäß Art. 55 Abs. 1 Satz 1 VfGHG als natürliche Personen antragsberechtigt.

Antragsgegenstand im Sinne von Art. 55 Abs. 1 Satz 1 VfGHG sind die im Rubrum aufgezählten Regelungen des BayVSG. Soweit das BayVSG auf Vorschriften des Bundesrechts verweist – insbesondere auf das G 10 –, überführt es diese Normen in bayerisches Landesrecht, das mit der Popularklage angegriffen werden kann,

> VerfGH, Entscheidung vom 23. Juli 2014 – Vf. 10-VII-13 –, juris, Rn. 17.

Die Klägerin und die Kläger rügen eine Verletzung der Grundrechte aus Art. 100, Art. 101, Art. 106 Abs. 3 und Art. 118 Abs. 1 BV. Im Rahmen dieser Rügen machen sie auch Verletzungen des Demokratieprinzips des Art. 2 BV sowie des Rechtsstaatsprinzips des Art. 3 Abs. 1 Satz 1 BV geltend, was nach ständiger Rechtsprechung des Verfassungsgerichtshofs zulässig ist,

> näher Lindner, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 3 Rn. 10 f., m.w.N.

Es besteht ein objektives Klarstellungsinteresse für die Popularklage. Dies gilt auch insoweit, als sich die Popularklage gegen Art. 15 Abs. 3 BayVSG richtet, der dem Landesamt 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 1. August 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 ebenfalls zumindest möglich, dass die Ermächtigung des Art. 15 Abs. 3 BayVSG in näherer Zukunft faktische Belastungswirkungen für Einzelne zeitigen wird. Zur Bejahung eines objektiven Klarstellungsinteresses reicht dies aus, da ein solches Interesse nur zu verneinen ist, wenn eine Inanspruchnahme staatlicher Rechtsschutzinstanzen unter keinem Aspekt sinnvoll erscheint,

> vgl. Wolff, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 98 Rn. 50.

Eine Klagefrist besteht nicht. Gründe für eine Verwirkung des Klagerechts der Klägerin und der Kläger sind nicht ersichtlich,

> vgl. zu den hohen Anforderungen an eine Verwirkung VerfGH, Entscheidung vom 12. Juni 2013 – Vf. 11-VII-11 –, juris, Rn. 102 ff.

II. Meinungsverschiedenheit

Die Antragstellerin ist als Fraktion des Bayerischen Landtags gemäß Art. 49 Abs. 2 Satz 1 VfGHG antragsberechtigt, da sie als Teil des Landtags in der Verfassung mit eigenen Rechten ausgestattet wird,

> vgl. VerfGHE 47, 241 (252).

Die Antragsgegnerin zu 1 als Mehrheitsfraktion im Landtag, mit deren Stimmen das BayVSG erlassen wurde,

> vgl. Plenarprotokoll 17/78 vom 7. Juli 2016, S. 6698,

und die Antragsgegnerin zu 2, die den ursprünglichen Gesetzentwurf in das Gesetzgebungsverfahren eingebracht hat, sind taugliche Antragsgegner.

Streitgegenstand des Verfahrens ist die Meinungsverschiedenheit der Antragstellerin und der Antragsgegnerinnen darüber, ob die angegriffenen Regelungen des BayVSG mit Art. 2, Art. 3 Abs. 1 Satz 1, Art. 100, Art. 101, Art. 106 Abs. 3 und Art. 118 Abs. 1 BV in Einklang stehen.

Diese Meinungsverschiedenheit hat sich bereits im Gesetzgebungsverfahren herausgebildet und ist in diesem erkennbar geworden,

> vgl. zu diesem Erfordernis VerfGHE 47, 241 (252 f.); Möstl, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 75 Rn. 13.

Die innenpolitische Sprecherin der Antragstellerin hat in sämtlichen Stadien des Gesetzgebungsverfahrens ihre Überzeugung von der Verfassungswidrigkeit der Überwachungsermächtigungen des BayVSG wie auch der zugehörigen Verfahrens- und Kontrollregelungen – mit unterschiedlichen Akzenten in ihren einzelnen Stellungnahmen – hervorgehoben. Die Regelungen über Datenübermittlungen sind mit diesen Überwachungsermächtigungen eng verknüpft. Eine detailliertere Ausarbeitung aller Einzelrügen in den Redebeiträgen der innenpolitischen Sprecherin der Antragstellerin hätte den Usancen der politischen Auseinandersetzung widersprochen und kann für die Zulässigkeit des Verfahrens nicht gefordert werden.

Die Verfassungswidrigkeit der hier angegriffenen Normen wurde zudem bereits im Gesetzgebungsverfahren von mehreren der Sachverständigen, wel-

che die Ausschüsse für Kommunale Fragen, Innere Sicherheit und Sport sowie für Verfassung, Recht und Parlamentsfragen des Bayerischen Landtags angehört haben, im Einzelnen begründet,

> vgl. neben dem Wortprotokoll der Anhörung die schriftlichen Stellungnahmen der Sachverständigen Bäcker, Kuhn, Löffelmann und Petri **(Anlagen 6 bis 9).**

Auf die Stellungnahmen dieser Sachverständigen hat sich die innenpolitische Sprecherin der Antragstellerin in ihren späteren Redebeiträgen wiederholt bezogen und sie sich damit zu Eigen gemacht.

Der Antrag im Verfahren der Meinungsverschiedenheit ist nicht fristgebunden. Gründe für eine Verwirkung des Antragsrechts sind nicht ersichtlich.

III. Hilfsweise: Beitritt der Antragstellerin zu der Popularklage

Lediglich hilfsweise für den Fall, dass der Verfassungsgerichtshof den Antrag im Verfahren der Meinungsverschiedenheit – insbesondere mangels hinreichender Rügen durch die Antragstellerin während des Gesetzgebungsverfahrens – für ganz oder teilweise unzulässig hält, erkläre ich für die Antragstellerin den Beitritt zu der Popularklage.

Die Antragstellerin ist im Verfahren der Popularklage gemäß Art. 55 Abs. 1 Satz 1 VfGHG antragsberechtigt. Der Jedermannsbegriff in dieser Norm umfasst nach der Rechtsprechung des Verfassungsgerichtshofs neben natürlichen Personen und juristischen Personen des Privatrechts auch juristische Personen des öffentlichen Rechts,

> etwa VerfGHE 51, 1 (13); weitere Nachweise bei Wolff, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 98 Rn. 14.

Als Fraktion des Bayerischen Landtags ist die Antragstellerin nicht lediglich eine unselbstständige Untergliederung dieses Verfassungsorgans, sondern zugleich selbst Trägerin von Rechten und Pflichten. Dementsprechend bestimmt Art. 1 Abs. 2 Satz 1 FraktG, dass die Fraktionen am allgemeinen Rechtsverkehr teilnehmen und unter ihrem Namen klagen und verklagt werden können. Die Fraktionen sind damit als rechtsfähig anzusehen, was für ihre Antragsbefugnis im Verfahren der Popularklage ausreicht.

Einem Beitritt zu der Popularklage steht nicht entgegen, dass die Antragstellerin jedenfalls dem Grunde nach antragsberechtigt im Verfahren der Meinungsverschiedenheit ist. Zwischen diesen beiden Verfahren besteht kein

Spezialitätsverhältnis dergestalt, dass ein tauglicher Antragsteller im Verfahren der Meinungsverschiedenheit keine Popularklage erheben könnte. Gegen ein solches Spezialitätsverhältnis spricht bereits der unterschiedliche Prüfungsmaßstab in beiden Verfahren: Während mit der Popularklage gemäß Art. 98 Satz 4 BV nur Grundrechtsverletzungen geltend gemacht werden können, kann im Verfahren der Meinungsverschiedenheit die Verfassungswidrigkeit einer Norm umfassend gerügt werden. Es muss den rechtsfähigen potenziellen Antragstellern im Verfahren der Meinungsverschiedenheit daher freistehen, gegebenenfalls unter Verzicht auf die weitergehende Prüfungsbefugnis zumindest wie jedermann die Grundrechtswidrigkeit eines Gesetzes vor dem Verfassungsgerichtshof mittels einer Popularklage zu rügen.

C. Begründetheit

Die Popularklage und die Meinungsverschiedenheit sind begründet, da die angegriffenen Regelungen des BayVSG die in der Verfassung des Freistaates Bayern verbürgten Grundrechte und weitere verfassungsrechtliche Vorgaben verletzen: Die Ermächtigung zum Abruf bevorrateter Telekommunikations-Verkehrsdaten verletzt Bundesrecht und verstößt daher gegen das Rechtsstaatsprinzip (unten I). Die gesetzlichen Eingriffsschwellen der übrigen angegriffenen Überwachungsermächtigungen 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 Bayern und darüber hinaus und verletzen so objektiv-rechtliche Grundrechtsgehalte (unten IV). Das BayVSG enthält daneben keine verfassungsrechtlich hinreichenden transparenzschaffenden Vorgaben (unten V). Die Ermächtigungen des Landesamts zu Datenübermittlungen an andere öffentliche und nicht-öffentliche Stellen stehen nicht mit den grundrechtlichen Anforderungen in Einklang (unten VI). Das BayVSG gestaltet die parlamentarische, öffentliche und aufsichtliche Kontrolle der Überwachungstätigkeit des Landesamts unzureichend aus (unten VII). Schließlich ermöglicht das Gesetz dem Landesamt in zu großem Ausmaß, personenbezogene Daten über Minderjährige zu verarbeiten und zu nutzen (unten VIII).

I. Verletzung des Rechtsstaatsprinzips durch Art. 15 Abs. 3 BayVSG

Die Ermächtigung in Art. 15 Abs. 3 BayVSG, bevorratete Telekommunikations-Verkehrsdaten abzurufen, bildet die Grundlage für Eingriffe in das aus Art. 101 i.V.m. Art. 100 BV abzuleitende Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung,

> vgl. zur Ableitung dieses Rechts etwa VerfGHE 40, 7 (12); 50, 226 (246); 57, 113 (119).

Diese Ermächtigung ist daher auch im Verfahren der Popularklage nicht nur auf ihre Vereinbarkeit mit materiellen Grundrechtsgehalten, sondern vollumfänglich auf ihre Verfassungsmäßigkeit zu überprüfen,

> vgl. etwa VerfGHE 52, 47 (56); 55, 1 (6).

Dabei beschränkt sich der Prüfungsmaßstab des Verfassungsgerichtshofs auf die Verfassung des Freistaates Bayern. Vorschriften des Bundesrechts sind

von diesem Prüfungsmaßstab für sich genommen nicht umfasst. Jedoch überprüft der Verfassungsgerichtshof die Vereinbarkeit von Normen des bayerischen Gesetzesrechts mit dem Bundesrecht mittelbar am Maßstab des Rechtsstaatsprinzips des Art. 3 Abs. 1 Satz 1 BV. Das Rechtsstaatsprinzip ist verletzt, wenn der Verstoß gegen Bundesrecht offen zutage tritt und auch inhaltlich schwer wiegt,

> vgl. etwa VerfGHE 50, 76 (98); weitere Nachweise bei Wolff, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 98 Rn. 66.

Die Datenerhebungsermächtigung in Art. 15 Abs. 3 BayVSG verstößt offenkundig und schwerwiegend gegen Bundesrecht. Die in dieser Norm angeordnete Pflicht der Anbieter von Telekommunikationsdiensten, bevorratete Verkehrsdaten an das Landesamt zu übermitteln, widerspricht § 113c Abs. 1 Nr. 2 TKG, der die maßgebliche Übermittlungserlaubnis enthält. Sie weicht damit die für die verfassungsrechtliche Rechtfertigung der Vorratsdatenspeicherung zentrale Entscheidung des Bundesgesetzgebers, den Zugriff auf Vorratsdaten eng zu begrenzen, fundamental auf.

Um den Widerspruch zwischen Art. 15 Abs. 3 BayVSG und § 113c Abs. 1 Nr. 2 TKG zu erkennen, müssen die Regelungsbefugnisse und Regelungsaufträge von Bundes- und Landesgesetzgebern im Zusammenhang mit der Bevorratung von Telekommunikationsdaten einander zugeordnet werden. Das Bundesverfassungsgericht hat diese Zuordnung in seinem Urteil zu der ersten Vorratsdatenspeicherung vom 2. März 2010 klar durchgeführt.

Danach sind die Kompetenzen zur Regelung von Bevorratung, Übermittlung und Abruf von Telekommunikations-Verkehrsdaten 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 neben der eigentlichen Bevorratungspflicht auch Regelungen zum Bevorratungszweck. Bei der Vorratsdatenspeicherung liegt dieser Zweck darin, die bevorrateten Daten an Sicherheitsbehörden zu übermitteln. Der Bund kann (und muss) daher Übermittlungserlaubnisse für die bevorratungspflichtigen Diensteanbieter schaffen. Diese Erlaubnisse müssen insbesondere normenklar und hinreichend restriktiv regeln, an welche Behörden aus welchen Anlässen und zu welchen Verfahrenszielen die Diensteanbieter die Vorratsdaten *übermitteln* dürfen. Demgegenüber kann der Bund die behördlichen Ermächtigungen zum *Abruf* der bevorrateten Daten nur insoweit regeln, als ihm aus

einem anderen Kompetenztitel als Art. 73 Abs. 1 Nr. 7 GG die Regelungsbefugnis für das Fachrecht der abrufenden Behörden zusteht,

BVerfGE 125, 260 (314 ff.).

In seinem Beschluss zur Bevorratung und zur sicherheitsbehördlichen Verwendung von Telekommunikations-Bestandsdaten hat das Bundesverfassungsgericht die Kompetenzrechtslage weiter präzisiert. Danach ist untrennbarer Bestandteil des Datenabrufs die Auskunftspflicht des angefragten Diensteanbieters. Der Bund darf (und muss) also nur die Übermittlungs*erlaubnis* für die Diensteanbieter durchweg regeln. Die Regelungskompetenz für die Frage, ob darüber hinaus eine *Pflicht* zur Übermittlung besteht, richtet sich hingegen nach der Gesetzgebungsbefugnis für das Fachrecht der Behörde, welche die Auskunft begehrt. Dementsprechend bedarf es für die behördliche Erhebung von Telekommunikations-Verkehrsdaten einer Rechtsgrundlage im behördlichen Fachrecht, die neben der Datenerhebung selbst auch die korrespondierende Auskunftspflicht des Diensteanbieters regelt,

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 Landesamts, Vorratsdaten zu erheben, auch eine korrespondierende Mitwirkungspflicht der Diensteanbieter. Dem Wortlaut der Norm, nach dem das Landesamt „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 Landesamts 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 Übermittlung von Vorratsdaten verpflichtet, zu der sie gemäß § 113c Abs. 1 Nr. 2

TKG 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 Bundesverfassungsgericht 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 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 Aufklärung in die polizeiliche oder ordnungsbehördliche 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

Die materiell-grundrechtlichen Maßstäbe für die Eingriffsschwellen von Überwachungsermächtigungen im Verfassungsschutzrecht lassen sich aus der Rechtsprechung des Bundesverfassungsgerichts ableiten, die zumindest weitgehend auf die Grundrechte der Verfassung des Freistaates Bayern übertragbar sind (unten 1). Auf der Grundlage dieser Maßstäbe verfehlen fast alle Überwachungsermächtigungen des BayVSG die grundrechtlichen Anforderungen (unten 2 bis 7).

1. Verfassungsrechtliche Maßstäbe

Die Überwachungsermächtigungen des BayVSG regeln überwiegend Eingriffe in das Recht auf informationelle Selbstbestimmung, das durch Art. 101 i.V.m. Art. 100 BV gewährleistet wird. Die Ermächtigung zu Wohnraumüberwachungen in Art. 9 BayVSG ermöglicht einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 106 Abs. 3 BV.

Diese Ermächtigungen müssen, um verfassungsrechtlich gerechtfertigt zu sein, einen angemessenen Ausgleich zwischen Individual- und Allgemeininteresse herstellen und das Gebot der Normenklarheit wahren,

VerfGHE 50, 226 (246); 59, 29 (35).

Im Einzelnen sind die grundrechtlichen Anforderungen an der jüngeren Rechtsprechung des Bundesverfassungsgerichts zu orientieren. Dieser Rechtsprechung lassen sich präzise und differenzierte Kriterien für Überwachungsermächtigungen im Verfassungsschutzrecht entnehmen.

a) Leitbildfunktion der jüngeren Rechtsprechung des Bundesverfassungsgerichts

Der Verfassungsgerichtshof hat seit geraumer Zeit keinen Anlass mehr gehabt, die verfassungsrechtlichen Maßstäbe zu konkretisieren, die sich aus der Verfassung des Freistaates Bayern für Ermächtigungen der Sicherheitsbehörden zu verdeckten Überwachungsmaßnahmen ergeben. Insgesamt liegen, soweit ersichtlich, bislang lediglich zwei Entscheidungen zu diesem Thema vor: Die erste befasste sich mit den Datenerhebungs- und Datenverarbeitungsregelungen des Polizeiaufgabengesetzes,

VerfGHE 47, 241,

die zweite hatte Vorschriften des Datenschutzgesetzes und des Verfassungsschutzgesetzes zum Gegenstand,

VerfGHE 50, 226.

Ferner hat der Verfassungsgerichtshof zwei Entscheidungen zur polizeilichen Schleierfahndung gefällt,

VerfGHE 56, 28 und VerfGHE 59, 29,

die allerdings als offene Ermittlungsmaßnahme in ermittlungstaktischem Zweck und Modalitäten erheblich von den hier verfahrensgegenständlichen Überwachungsmaßnahmen abweicht. Der Erkenntniswert dieser Entscheidungen für das vorliegende Verfahren ist daher begrenzt.

Auch die beiden Entscheidungen zum Polizeiaufgabengesetz sowie zum Datenschutz- und zum Verfassungsschutzgesetz haben für das vorliegende Verfahren nurmehr geringe Aussagekraft. Sie stammen aus den Jahren 1994 und 1997, befinden sich nicht mehr auf dem Stand der Diskussion und können daher allenfalls in engen Grenzen und mit großer Vorsicht herangezogen werden, um die grundrechtlichen Vorgaben an Überwachungsermächtigungen zu konkretisieren. Hierfür sprechen ein Sachgrund und ein Rechtsgrund:

In sachlicher Hinsicht ist zu beachten, dass sich die Eingriffsintensität verdeckter Überwachungsmaßnahmen seit 1997 drastisch erhöht hat. Seit diesem Zeitpunkt ist das Arsenal staatlicher Überwachungsmethoden erheblich angewachsen. Beispielhaft seien „Online-Durchsuchungen“ und „Quellen-Telekommunikationsüberwachungen“ genannt (Art. 10 und Art. 13 BayVSG). Auch etwa die technischen Mittel, die zu Observationszwecken eingesetzt werden können (Art. 8 BayVSG), sind heute ungleich leistungsstärker als vor 20 Jahren. Die soziale und technische Entwicklung hat zudem dazu geführt, dass über die Einzelnen ein damals noch unvorstellbares Ausmaß an elektronisch codierten Informationen zur Verfügung steht, das die Sicherheitsbehörden erschließen können. Beispielhaft sei auf die zahlreichen Metadaten (Verkehrs- und Nutzungsdaten) verwiesen, die bei der Nutzung von Telekommunikationsdiensten und Telemedien anfallen und die weitreichende Schlüsse etwa auf Bewegungsverhalten, Vorlieben und soziale Einbindung des Betroffenen ermöglichen (vgl. zur Erhebung dieser Daten Art. 15 BayVSG). Schließlich hat der Fortschritt der Informationstechnik die Fähigkeiten der Sicherheitsbehörden erheblich zunehmen lassen, erhobene Daten zu analysieren und miteinander zu verknüpfen, um aus ihnen neue Informationen zu gewinnen, etwa über Eigenschaften, Verhalten oder soziale Vernetzungen einer Person. We-

gen dieses Fortschritts der Auswertungstechnik sind auch hergebrachte Überwachungsmaßnahmen wie Observationen (Art. 8 BayVSG), Wohnraumüberwachungen (Art. 9 BayVSG) oder der Einsatz Verdeckter Mitarbeiter (Art. 18 BayVSG) heute neu zu bewerten.

In rechtlicher Hinsicht ist zu beachten, dass sich die verfassungsjuristische Diskussion über verdeckte Überwachungsmaßnahmen der Sicherheitsbehörden seit 1997 beträchtlich fortentwickelt hat. Hauptgrund hierfür ist die Rechtsprechung des Bundesverfassungsgerichts. Das Bundesverfassungsgericht hat seit der „Initialzündung“ im zweiten G 10-Urteil von 1999,

> BVerfGE 100, 313,

in einer Vielzahl von Entscheidungen aus den Grundrechten des Grundgesetzes ein mittlerweile dicht gewirktes Sicherheitsverfassungsrecht entwickelt, das es fortlaufend an die sozialen und technischen Veränderungen der staatlichen Sicherheitsgewähr angepasst hat. Die Rechtsprechung des Bundesverfassungsgerichts ist mittlerweile in vielen zentralen Punkten konsolidiert. Hierzu hat insbesondere die bislang letzte Entscheidung beigetragen, das Urteil zum BKA-Gesetz,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09; eine Auflistung der zwischen 1999 und 2015 ergangenen Entscheidungen des Bundesverfassungsgerichts zum Sicherheitsverfassungsrecht findet sich bei Bäcker, Kriminalpräventionsrecht, 2015, S. 1, Fn. 3.

Das Bundesverfassungsgericht hat in seiner zwischenzeitlich ergangenen Rechtsprechung die grundrechtlichen Anforderungen an verdeckte Überwachungsmaßnahmen weitaus präziser und detaillierter bestimmt als dies dem Verfassungsgerichtshof in seinen lediglich zwei Entscheidungen möglich war. Darüber hinaus fallen die Anforderungen nach der Rechtsprechung des Bundesverfassungsgerichts deutlich restriktiver aus. Für die Auslegung von Art. 101 i.V.m. Art. 100 und von Art. 106 Abs. 3 BV ist dies bedeutsam, weil der Verfassungsgerichtshof in ständiger Rechtsprechung betont, dass der Schutzgehalt des grundrechtlichen Informationsschutzes nach der Verfassung des Freistaates Bayern nicht hinter den inhaltsgleichen Gewährleistungen des Grundgesetzes zurückbleibt. Dementsprechend kann die Rechtsprechung des Bundesverfassungsgerichts zu diesen Gewährleistungen zumindest in ihren

Grundaussagen zur Auslegung der Grundrechte der Bayerischen Verfassung herangezogen werden,

> VerfGHE 40, 7 (12); 47, 241 (254); 50, 226 (246); 57, 113 (119); 59, 29 (34).

Daher sind im Folgenden auf der Grundlage des weitgehenden Gleichlaufs zwischen dem grundrechtlichen Informationsschutz nach der Verfassung des Freistaates Bayern und nach dem Grundgesetz die grundrechtlichen Maßstäbe für Überwachungsermächtigungen im Verfassungsschutzrecht anhand der jüngeren Rechtsprechung des Bundesverfassungsgerichts zu konkretisieren.

b) Überwachungsermächtigungen des Verfassungsschutzrechts im Lichte der Rechtsprechung des Bundesverfassungsgerichts

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,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 104 ff.

Für die weitere Konkretisierung der verfassungsrechtlichen Maßstäbe ist insbesondere bedeutsam, ob und inwieweit auf die Rechtsprechung des Bundesverfassungsgerichts zu präventivpolizeilichen Überwachungsmaßnahmen zurückgegriffen werden kann, um auch Ermächtigungen im Verfassungsschutzrecht zu beurteilen. Insbesondere stellt sich die Frage nach der Relevanz der

Maßstäbe, die das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz herausgearbeitet hat, für das Verfassungsschutzrecht.

Im Ausgangspunkt hat das Bundesverfassungsgericht 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 Bundesverfassungsgericht 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 Bundesverfassungsgericht 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.).

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 Bundesverfassungsgericht eingriffsintensive Überwachungsmaßnahmen an das Erfordernis einer konkreten Gefahr für ein bedeut-

sames Rechtsgut als einheitliche Mindesteingriffsschwelle gebunden. Zugleich hat das Gericht den verfassungsrechtlichen Begriff der konkreten Gefahr von dem hergebrachten 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 Bundesverfassungsgericht 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 macht deutlich, was den Kern der Erweiterung des (verfassungsrechtlichen) Gefahrbegriffs ausmacht: Während der hergebrachte polizeirechtliche Gefahrbegriff die *situationsbezogene* Prognose eines Schadensereignisses erfordert, zielt der erweiterte verfassungsrechtliche Gefahrbegriff auf eine *personenbezogene* Aussage über die „Gefährlichkeit“ eines Individuums. Ein konkretes Schadensereignis muss hierfür nicht absehbar sein. Allerdings muss die personenbezogene Gefährlichkeitsprognose auf hinreichend aussagekräftigen Tatsachen beruhen,

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

Dieser erweiterte verfassungsrechtliche Gefahrbegriff ist gerade 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 ermöglicht, bevor eine klar konturierte schadensträchtige Situation entstanden ist. Die personenbezogene Gefährlichkeitsprognose kann so die fortlaufende Beobachtung bestimmter Personen oder Gruppierungen anleiten, die typisch für die nachrichtendienstliche Tätigkeit ist.

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 Bundesverfassungsgericht umrissene personenbezogene Gefährlichkeitsprognose eignet sich daher besonders dazu, personengerichtete Überwachungsmaßnahmen der Nachrichtendienste im benötigten Umfang zu ermöglichen und sie zugleich hinreichend trennscharf zu begrenzen. Darum 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. Insoweit sind die verfassungsrechtlichen Maßstäbe, die für das Handeln der Polizeibehörden gelten, nach wie vor nicht auf die Nachrichtendienste zu über-

tragen. Soweit die Nachrichtendienste sich auf solche Aufklärungsmaßnahmen beschränken, kommt vielmehr ihr deutlich weitergehender Aufklärungsauftrag vollumfänglich zum Tragen.

Zweitens sind hingegen personengerichtete Überwachungsmaßnahmen hoher Eingriffsintensität auch im Nachrichtendienstrecht an eine situationsbezogene Schadens- oder eine personenbezogene Gefährlichkeitsprognose zu binden, wie sie das Bundesverfassungsgericht 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 Bundesverfassungsgericht 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,

> vgl. 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,

anders noch VerfGHE 50, 226 (260).

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. VerfGHE 59, 29 (35).

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 verstößt Art. 8 Abs. 1 Satz 1 BayVSG gegen Art. 101 i.V.m. Art. 100 BV.

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. Sie verletzen daher Art. 106 Abs. 3 bzw. Art. 101 i.V.m. Art. 100 BV.

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 hat für „Online-Durchsuchungen“ und mit Blick auf die Grundrechte des Grundgesetzes das Bundesverfassungsgericht bereits ausgeführt,

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

> vgl. 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 Nr. 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. Das Landesamt 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. 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 1. August 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 des Freistaates 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 Bayern oder auch nur in einem der Größe nach nicht völlig vernachlässigbaren Teil Bayerns 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., 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 zum insoweit gleichlautenden § 8a Abs. 2 Satz 1 Nr. 2, Abs. 3 Nr. 1 BVerfSchG-a.F. 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 – hier 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 Bundesverfassungsgerichts 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 Bundesverfassungsgerichts einer Neubewertung. Das Bundesverfassungsgericht 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 BayVSG

Die in Art. 13 BayVSG enthaltene Ermächtigung zu „Quellen-Telekommunikationsüberwachungen“ weist in zweifacher Hinsicht verfassungsrechtliche Defizite auf: Erstens verletzt sie das aus Art. 101 i.V.m. Art. 100 BV abzuleitende Gebot der Normenklarheit und das Demokratieprinzip des Art. 2 BV, 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. Zweitens genügt der in Bezug genommene § 3 Abs. 1 G 10 seinerseits nicht den grundrechtlichen Anforderungen an Ermächtigungen zu Telekommunikationsüberwachungen, so dass Art. 13 BayVSG auch materiell gegen Art. 101 i.V.m. Art. 100 BV verstößt.

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. Diese Bezugnahme ist als dynamische Verweisung auf die Bezugsnorm in ihrer jeweils geltenden Fassung 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 Gebots der Normenklarheit und des Demokratieprinzips. Nach der Rechtsprechung des Verfassungs-

gerichtshofs sind dynamische Verweisungen zwar nicht schlechthin unzulässig. Dies gilt auch, wenn eine Norm des bayerischen Landesrechts auf eine bundesrechtliche Norm verweist. 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. Insbesondere wenn eine Regelung einen Grundrechtseingriff vorsieht, muss sie Art und Ausmaß der Grundrechtsbeeinträchtigung selbst festlegen und rechtfertigen. Nur in diesem Rahmen kann sie auf andere Vorschriften auch dynamisch Bezug nehmen,

> vgl. zur grundsätzlichen Zulässigkeit und zu den Grenzen dynamischer Verweisungen allgemein VerfGH, Entscheidung vom 23. Juli 2014 – Vf. 10-VII-13 –, juris, Rn. 23; Lindner, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 3 Rn. 30; ferner aus der Rechtsprechung des Bundesverfassungsgerichts etwa BVerfGE 47, 285 (312); 67, 348 (363).

Aus den Grundrechten sowie 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. VerfGHE 59, 29 (35); ferner aus der Rechtsprechung des Bundesverfassungsgerichts 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, die durch die dynamische Verweisung in Art. 13 Abs. 2 BayVSG in bayerisches Landesrecht transformiert wurden und deshalb an den Grundrechten der Verfassung des Freistaates Bayern zu messen sind, 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 Nachrichten-

dienste, 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 Stadium 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. zur grundrechtlichen Problematik einer Einbeziehung des Planungsstadiums 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, 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 Straftatenkatalog 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 *(Dual Use)* 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. Aufgrund von Art. 13 Abs. 2 BayVSG i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10 kann das Landesamt 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 persönlichen 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 auf 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 Satz 1 und Satz 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 politisch 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 1. August 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 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

höchst private 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, 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, der als Überwachungsanlass eine konkrete Gefahr (im verfassungsrechtlichen Sinne) vorgibt und die möglichen Zielpersonen des Einsatzes präzise und restriktiv beschreibt. 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

Die Garantie der Unantastbarkeit der Menschenwürde aus Art. 100 BV und die allgemeine Handlungsfreiheit des Art. 101 BV umfassen den Schutz eines Kernbereichs privater Lebensgestaltung, der absolut geschützt ist und von staatlichen Eingriffen freibleiben muss,

> vgl. VerfGHE 32, 121 (128); 57, 161 (166).

Der Kernbereich privater Lebensgestaltung ist insbesondere bei der Durchführung staatlicher Überwachungsmaßnahmen zu beachten. Selbst gewichtige Aufklärungsinteressen können ein Eindringen in diesen Kernbereich nicht rechtfertigen.

Das Bundesverfassungsgericht hat in seiner jüngeren Rechtsprechung seit dem Urteil zur akustischen Wohnraumüberwachung,

BVerfGE 109, 279,

aus der grundgesetzlichen Menschenwürdegarantie des Art. 1 Abs. 1 GG neben dem materiell-grundrechtlichen Verbot einer Kernbereichsverletzung auch prozedurale Vorgaben für Überwachungsmaßnahmen abgeleitet. In seinem Urteil zum BKA-Gesetz hat es diese Vorgaben gebündelt und präzisiert. Danach muss der Gesetzgeber Ermächtigungen zu Überwachungsmaßnahmen, die eine gesteigerte Kernbereichssensibilität aufweisen, mit verfahrensrechtlichen Schutzvorkehrungen verbinden, die das Risiko einer Kernbereichsverletzung reduzieren. Diese Vorkehrungen müssen auf zwei Stufen ansetzen: Auf der ersten Stufe der eigentlichen Überwachung ist ein Eindringen in den Kernbereich privater Lebensgestaltung nach Möglichkeit zu vermeiden. Auf der zweiten Stufe der Auswertung der durch die Überwachung gewonnenen Erkenntnisse ist zu gewährleisten, dass im Fall einer Erfassung des Kernbereichs zumindest die Folgen für den Betroffenen abgemildert werden. Hierzu sind Anforderungen an das Auswertungsverfahren zu stellen und Dokumentations- und Löschungspflichten vorzusehen,

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

Wegen des Gleichlaufs der Gewährleistungen der Menschenwürde und der informationellen Selbstbestimmung in der Verfassung des Freistaates Bayern und im Grundgesetz,

siehe oben II. 1. a),

liegt es nahe, diese Rechtsprechung auf Art. 100 und Art. 101 BV zu übertragen.

Das BayVSG verfehlt die Anforderungen an den prozeduralen Kernbereichsschutz, wie sie sich aus der jüngeren Rechtsprechung des Bundesverfassungsgerichts ergeben. 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,

> vgl. zu Art. 1 Abs. 1 GG 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. Diese Vorgabe reicht jedoch nicht aus, um den gebotenen prozeduralen Grundrechtsschutz zu gewährleisten. Denn aus dem Demokratieprinzip des Art. 2 BV und dem Rechtsstaatsprinzip des Art. 3 Abs. 1 BV folgt, dass das Parlament als unmittelbar demokratisch legitimiertes Staatsorgan wesentliche Fragen selbst durch formelles Gesetz entscheiden muss,

> VerfGHE 31, 99 (127); 34, 82 (93); 47, 276 (302).

Der prozedurale Kernbereichsschutz ist als derartige wesentliche Frage anzusehen, da er dem Risiko einer Verletzung der Menschenwürdegarantie und damit der fundamentalen grundrechtlichen Gewährleistung in besonders sensiblen Lagen vorbeugen soll. Dementsprechend hat das Bundesverfassungsgericht in seiner Rechtsprechung zu Art. 1 Abs. 1 GG 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.

Der prozedurale Schutz der Menschenwürde kann mithin 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 auf der Grundlage der jüngeren Rechtsprechung des Bundesverfassungsgerichts 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. So ist jedoch nicht gewährleistet, 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,

> vgl. 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 Überwachung. Zum einen besteht für Gespräche in Wohnrümen eine verfassungsrechtliche Vermutung, dass sie dem Kernbereich zuzuordnen sind und daher nicht überwacht werden dürfen. Diese Vermutung ist positiv zu entkräften, damit eine Wohnung überwacht werden darf. Dem trägt § 3a G 10 nicht Rechnung. Zum anderen ermöglicht diese Norm eine automatische Daueraufzeichnung der Überwachungsergebnisse, die jedoch im Rahmen von Wohnraumüberwachungen wegen der besonderen Kernbereichssensibilität dieser Maßnahme nicht zugelassen werden darf,

> vgl. zu Art. 1 Abs. 1 GG 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. Auch diese Vorgabe trägt der besonderen Kernbereichssensibilität der Wohnraumüberwachung nicht hinreichend Rechnung,

> 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. zu diesem Gebot 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

Über den Schutz des Kernbereichs privater Lebensgestaltung hinaus bedarf gemäß Art. 101 i.V.m. Art. 100 BV auch die vertrauliche Kommunikation mit Berufsgeheimnisträgern eines besonderen Schutzes. Diese Kommunikation muss zwar – soweit sie nicht dem Kernbereich unterfällt – nicht vollständig frei von staatlichen Einblicken gehalten werden. Es bedarf jedoch gesetzlicher Schutzregelungen, die der besonderen Sensibilität der Berufsgeheimnisse

Rechnung tragen, wenngleich der Gesetzgeber hierbei über einen beträchtlichen Gestaltungsspielraum verfügt,

> vgl. zu den Grundrechten des Grundgesetzes 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 des Art. 118 Abs. 1 BV nicht in Einklang,

> vgl. zu Art. 3 Abs. 1 GG und zu dem mit § 3b G 10 weitgehend identischen § 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

Das Recht auf informationelle Selbstbestimmung aus Art. 101 i.V.m. Art. 100 BV gebietet im Zusammenwirken mit der aus Art. 3 Abs. 1 BV herzuleitenden Rechtsschutzgarantie,

> vgl. zu dieser Ableitung VerfGHE 59, 219 (227),

dass verdeckte eingriffsintensive Überwachungsmaßnahmen grundsätzlich einer Vorabkontrolle durch eine unabhängige Stelle unterworfen werden, um die Rechte des Betroffenen bereits im behördlichen Verfahren zur Geltung zu bringen und so irreparable Schäden durch rechtswidrige Maßnahmen möglichst zu vermeiden. Es ist Sache des Gesetzgebers, eine solche Kontrolle verbindlich vorzugeben. Damit die Vorabkontrolle tatsächlich wirksam ist und sich nicht in bloßen Routinen und Formeln erschöpft, muss der Gesetzgeber zudem strenge Anforderungen an den Inhalt und die Begründung der Entscheidung der Kontrollinstanz errichten,

> vgl. zu den Grundrechten des Grundgesetzes BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 117 f.; anders noch VerfGHE 47, 241 (262 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-Kommission des Bayerischen Landtags mit der Kontrolle zu befassen. Voraussetzung dafür ist allerdings, dass diese anderen 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 das Landesamt selbst oder der Innenminister als 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 § 10 Abs. 2 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). Diese Regelung ist allerdings auf Telekommunikationsüberwachungen zugeschnitten. Der Verweis auf sie 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 BayVSG nicht vor.

IV. Übermäßige Folgerisiken für die Integrität informationstechnischer Systeme

Die Ermächtigungen zu „Online-Durchsuchungen“ und zu „Quellen-Telekommunikationsüberwachungen“ erzeugen über die individuellen Grundrechtseingriffe hinaus nicht mehr hinnehmbare Risiken für die IT-Sicherheit in Bayern und darüber hinaus. Das Gesetz schirmt diese Risiken nicht hinreichend ab,

da es keine begrenzenden Vorgaben dafür enthält, in welcher Weise die Zielsysteme solcher Überwachungen infiltriert werden dürfen.

Verfassungsrechtlicher Maßstab für die Vorgaben über die Infiltration des Zielsystems ist das aus Art. 101 i.V.m. Art. 100 BV folgende Recht auf informationelle Selbstbestimmung in seiner objektiv-rechtlichen Dimension. Der Verfassungsgerichtshof hat, soweit ersichtlich, diese Grundrechtsdimension mit Blick auf die IT-Sicherheit in seiner Rechtsprechung noch nicht ausgelotet. Demgegenüber hat das Bundesverfassungsgericht in seinem Urteil zu „Online-Durchsuchungen“ aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (IT-Grundrecht) abgeleitet,

> BVerfGE 120, 274 (302 ff.).

Das IT-Grundrecht erweitert den hergebrachten Schutz der Vertraulichkeit personenbezogener Daten, den das Recht auf informationelle Selbstbestimmung vermittelt, in zweifacher Hinsicht:

Erstens umfasst es mit der Integrität informationstechnischer Systeme ein weiteres Schutzanliegen. Der Begriff der Integrität entstammt der informationstechnischen Terminologie. Daten sind integer, wenn sie nicht von Nichtberechtigten verändert werden können (starke Integrität) oder Veränderungen zumindest für den Berechtigten erkennbar sind (schwache Integrität),

> vgl. Hansen/Pfitzmann, in: Roggan, Online-Durchsuchungen, 2008, S. 131 (132).

Das IT-Grundrecht gewährleistet die Integrität informationstechnischer Systeme unabhängig davon, ob aus einem infiltrierten System später Daten erhoben und so die Vertraulichkeit des Systems beeinträchtigt wird. Hinsichtlich des subjektiv-rechtlichen Grundrechtsgehalts verlagert die Integritätskomponente des IT-Grundrechts den Grundrechtsschutz damit zeitlich vor. Da zudem ein einmal infiltriertes System aus technischer Sicht als vollständig kompromittiert anzusehen ist, gebietet der grundrechtliche Schutz der Integrität informationstechnischer Systeme, den Integritätsbruch durch begrenzende Verfahrensregelungen zu flankieren, wie sie Art. 10 Abs. 2 und Art. 13 Abs. 1 BayVSG enthalten.

Zweitens enthält das IT-Grundrecht neben einem subjektiven Abwehrrecht einen objektiv-rechtlichen Gewährleistungsauftrag für die Integrität informationstechnischer Systeme. Dies ergibt sich aus dem Begriff der „Gewährleistung“,

den das Bundesverfassungsgericht zur Bezeichnung des IT-Grundrechts verwendet. Die objektiv-rechtliche Dimension des IT-Grundrechts ist in dem Urteil zu „Online-Durchsuchungen“ nicht konkretisiert worden, dieses argumentierte vielmehr rein subjektiv-rechtlich. Sie bildet allerdings den Anknüpfungspunkt, um über subjektive Abwehrrechte hinaus einen grundrechtlichen Gestaltungsauftrag zu begründen: 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.

Angesichts des Gleichlaufs zwischen dem grundrechtlichen Informationsschutz aus Art. 101 i.V.m. Art. 100 BV und den entsprechenden Grundrechten des Grundgesetzes erscheint es angezeigt, auch das bayerische Landesgrundrecht auf informationelle Selbstbestimmung um diesen objektiv-rechtlichen Gewährleistungsauftrag zu erweitern.

Die Infiltration informationstechnischer Systeme zu Überwachungszwecken kann neben dem individuellen Eingriff in Grundrechte der Zielperson und dritter Betroffener auch die objektiv-rechtliche Dimension des grundrechtlichen Informationsschutzes und insbesondere die Integrität der IT-Infrastruktur in Bayern und darüber hinaus empfindlich treffen. Risiken weit über den Einzelfall hinaus können sich dann ergeben, wenn zum Zweck der Infiltration eines informationstechnischen Systems Software-Sicherheitslücken ausgenutzt werden (sogenannte Exploits). Insbesondere stellt es eine schwerwiegende Bedrohung der IT-Sicherheit 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 die staatliche Gewalt 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 soeben 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 Einschätzung 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 1. August 2017).

Es liegt fern, dass das Landesamt die bei ihm vorhandenen Informationen über Software-Sicherheitslücken bedeutend besser schützen kann als die NSA. Mit vergleichbaren Vorfällen infolge einer Sammlung solcher Sicherheitslücken bei dieser Behörde wäre daher 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 Bayern und darüber hinaus nicht legitimieren, die von einer Sammlung von Sicherheitslücken bei dem Landesamt 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 Bundesverfassungsgerichts entwickelten und auf das bayerische Verfassungsrecht übertragbaren subjektiv-abwehrrechtlichen Anforderungen an diese Überwachungsmaßnahmen,

> vgl. 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 zu manipulieren, oder Zugriffspasswörter durch eine Messung der elektromagnetischen Abstrahlungen des Zielsystems zu ermitteln. Solche Zugriffe führen nur zur Kompromittierung des Zielsystems, begründen aber keine besonderen Infiltrationsrisiken für andere informationstechnische Systeme. 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 grundrechtlichen Integritätsschutzes aus Art. 101 i.V.m. Art. 100 BV 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 Grundrechtsdimension 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

Aus dem Recht auf informationelle Selbstbestimmung gemäß Art. 101 i.V.m. Art. 100 BV sowie aus der Rechtsschutzgarantie des Art. 3 Abs. 1 BV ergeben sich verfassungsrechtliche Anforderungen an die Transparenz eingriffsintensiver verdeckter Überwachungsmaßnahmen. Der Verfassungsgerichtshof hat diese Anforderungen in seinen Entscheidungen zum Polizeiaufgabengesetz und zum alten Verfassungsschutzgesetz grundsätzlich anerkannt, allerdings Ausnahmen von der Transparenz verdeckter Überwachungsmaßnahmen in weitem Umfang für zulässig gehalten,

vgl. VerfGHE 47, 241 (263 f.); 50, 226 (262 f.).

Auch in diesem Punkt befinden sich diese Entscheidungen allerdings nicht mehr auf dem Stand der Diskussion und können nicht mehr herangezogen werden, um die grundrechtlichen Maßstäbe zu konkretisieren,

> vgl. zu den Anforderungen an den Tatbestand von Überwachungsermächtigungen oben II. 1. a).

Insbesondere hat das Bundesverfassungsgericht in seiner Rechtsprechungslinie seit dem zweiten G 10-Urteil von 1999 aus dem Grundgesetz weit strengere und detailliertere Maßstäbe auch für transparenzschaffende Regelungen abgeleitet als sie der Verfassungsgerichtshof seinerzeit entwickelt hat,

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

Wegen des prinzipiellen Gleichlaufs des grundrechtlichen Informationsschutzes nach der Verfassung des Freistaates Bayern und nach dem Grundgesetz sind die grundrechtlichen Anforderungen an transparenzschaffende Vorkehrungen heute an der jüngeren Rechtsprechung des Bundesverfassungsgerichts und nicht mehr an den Entscheidungen des Verfassungsgerichtshofs zum Polizeiaufgabengesetz und zum alten Verfassungsschutzgesetz zu orientieren.

Auf der Grundlage dieser Rechtsprechung enthält das BayVSG 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 Bundesverfassungsgerichts Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen generell durch Benachrichtigungspflichten flankieren,

> anders für verdeckte Überwachungsmaßnahmen der Polizei mit Ausnahme der Wohnraumüberwachung noch VerfGHE 47, 214 (264).

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, wie sie sich aus der Rechtsprechung des Bundesverfassungsgerichts ergeben, 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 zu der verfassungsrechtlichen Benachrichtigungspflicht 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,

> vgl. 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 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 Bundesverfassungsgerichts zur strategischen Telekommunikationsüberwachung nach dem G 10 vom 14. Juli 1999 entnommen ist,

> vgl. BVerfGE 100, 313 (398).

Das Bundesverfassungsgericht ist – ebenso wie der Verfassungsgerichtshof – keine Rechtsetzungsinstanz, sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Es kann sinnvoll oder wegen des Demokratieprinzips sogar angezeigt sein, im Rahmen verfassungsgerichtlicher Entscheidungen 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 verfassungsgerichtlichen Rechtsprechung 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, Datenschutzrecht in Bund und Ländern, 2013, § 19 BDSG Rn. 1.

Das Bundesverfassungsgericht hat insbesondere die zentrale Bedeutung dieses Anspruchs für den Grundrechtsschutz betont, wenn eine staatliche Stelle – wie das Landesamt – 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); hingegen hat der Verfassungsgerichtshof im Jahr 1997 die Auskunftserteilung noch als Ausnahmefall gekennzeichnet, VerfGHE 50, 226 (262).

Gerade in solchen Fallkonstellationen bestehen hohe Anforderungen an Einschränkungen des Auskunftsanspruchs. Eine Einschränkung muss gegenläufigen 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,

> vgl. zu dieser Wurzel des Rechts auf informationelle Selbstbestimmung etwa VerfGHE 50, 226 (246); 57, 113 (120).

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 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 ermessensfehlerfreie 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, wie dies bei den weitgehend verdeckt durchgeführten Datenverarbeitungen des Landesamts der Fall ist,

> vgl. BVerfGE 120, 351 (364); anders noch VerfGHE 50, 226 (262).

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 wie das Landesamt. Die Verfassungsschutzbehörden

des Bundes und der Länder 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 grundsätzlich nur auf Daten, die strukturiert in automatisierten Dateien gespeichert sind. Eine Auskunft zu anderen gespeicherten Daten setzt voraus, dass der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und dass der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht.

Der prinzipielle Anspruchsanschluss für Daten außerhalb strukturierter Dateien reicht zu weit, weil unter heutigen informationstechnischen Bedingungen insbesondere auch unstrukturierte Datenbestände – etwa 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,

> unter anderen technischen Rahmenbedingungen noch anders VerfGHE 50, (262).

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.

Zwar hat der Verfassungsgerichtshof in seinen Entscheidungen zum Polizeiaufgabengesetz und zum alten Verfassungsschutzgesetz derartige Übermittlungsermächtigungen selbst bei sehr weiter Fassung der Übermittlungstatbestände gebilligt,

> VerfGHE 47, 241 (258 f., 261 f.); 50, 226 (264 f.).

Auch in diesem Punkt sind diese Entscheidungen jedoch durch die seitdem ergangene Rechtsprechung des Bundesverfassungsgerichts überholt und lassen sich allenfalls in engen Grenzen heranziehen, um die grundrechtlichen

Anforderungen an die Übermittlungsermächtigungen des BayVSG zu bestimmen,

> vgl. zu den Anforderungen an Überwachungungsermächtigungen oben II. 1. a).

Wegen des Gleichlaufs des grundrechtlichen Informationsschutzes nach der Verfassung des Freistaates Bayern und nach dem Grundgesetz sind an die Übermittlungsermächtigungen des BayVSG vielmehr primär die verfassungsrechtlichen Maßstäbe anzulegen, die das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz unter Konsolidierung und Präzisierung seiner Rechtsprechung herausgearbeitet hat,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 275 ff.

Verfassungswidrig sind auf dieser Grundlage zum einen die meisten 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 Bundesverfassungsgericht 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, die zu unterschiedlichen Verteilungen von Datenerhebungs- und Zwangsbefugnissen führen. 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 Bundesverfassungsgericht 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 Bundesverfassungsgerichts 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, da die verfassungsrechtlichen Anforderungen an die Übermittlung personenbezogener Daten von der Eingriffsintensität der Datenerhebung abhängen,

> näher Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 249 ff.

Für die sensibleren Daten, die das Landesamt mit nachrichtendienstlichen Mitteln erhoben hat, 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 Datenübermittlung 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 personenbezogene Daten 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 zur Verfolgung die-

ser Straftaten erlangt werden dürften. Unerheblich ist insoweit, ob die übermittelten Daten 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 Datenübermittlung 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 Kriminalprävention 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 Verhütung 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., 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 Daten übermittelt werden können, die durch eingriffsintensive Überwachungsmaßnahmen wie Tonaufnahmen außerhalb von Wohnungen oder den Einsatz von Verdeckten Mitarbeitern oder Vertrauensleuten gewonnen wurden,

> vgl. zu dem 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 ge-

währleistet 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 Überwachungsmaßnahmen 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,

> anders zu der Vorgängervorschrift des Art. 14 BayVSG-a.F. noch VerfGHE 50, 226 (264 f.).

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 Bundesverfassungsgericht in seinem Urteil zur Antiterrordatei getroffen hat. Das Bundesverfassungsgericht 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 Bundesverfassungsgerichts 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 genügen, 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.; ansatzweise bereits VerfGHE 50, 226 (265).

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 Telekommunikationsüber-

wachung 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).

VII. Unzureichende Vorgaben für die Kontrolle der Überwachungstätigkeit Landesamts

Die im BayVSG vorgesehene parlamentarische, öffentliche und aufsichtsbehördliche Kontrolle der eingriffsintensiven Überwachungsmaßnahmen des Landesamts und der nachfolgenden Datenverarbeitungen genügt gleichfalls nicht den grundrechtlichen Anforderungen.

Zur Konkretisierung dieser Anforderungen ist wiederum auf die jüngere Rechtsprechung des Bundesverfassungsgerichts zurückzugreifen, da es an aktuellen Maßstäben in der Rechtsprechung des Verfassungsgerichtshofs fehlt,

> siehe oben II. 1. a).

Danach sieht das Gesetz nur unzureichende Pflichten zur parlamentarischen und öffentlichen Berichterstattung über Überwachungsmaßnahmen und nachfolgende Datenverarbeitungen vor (unten 1), enthält nicht die grundrechtlich

gebotenen Dokumentationspflichten zur Gewährleistung einer wirksamen Datenschutzkontrolle (unten 2) und teilt die aufsichtliche Kontrolle des Landesamts in dysfunktionaler Weise zwischen der G 10-Kommission des Bayerischen Landtags und dem Bayerischen Landesbeauftragten für den Datenschutz auf (unten 3).

1. Unzureichende Berichtspflichten

Die in Art. 20 Abs. 1 BayVSG enthaltenen Pflichten zur Berichterstattung über verdeckte Überwachungsmaßnahmen reichen nicht weit genug, um den grundrechtlichen Anforderungen zu genügen.

Nach der Rechtsprechung des Bundesverfassungsgerichts müssen Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen durch Pflichten zur Berichterstattung an Parlament und Öffentlichkeit flankiert werden, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Ermächtigungen gestützten Datenerhebungen und nachfolgenden Datenverarbeitungen zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen,

> BVerfGE 133, 277 (372); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 142 f.

Die Berichtspflichten müssen neben den Überwachungsmaßnahmen selbst auch den weiteren Umgang mit den dadurch erlangten personenbezogenen Daten umfassen. Insbesondere muss auch über Datenübermittlungen berichtet werden,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 340, 354.

Art. 20 Abs. 1 BayVSG enthält zwei Berichtspflichten: Zum einen ist das Bayerische Staatsministerium zur Information des Parlamentarischen Kontrollgremiums verpflichtet (Art. 20 Abs. 1 Satz 1 BayVSG), zum anderen muss das Parlamentarische Kontrollgremium an das Plenum des Landtags berichten (Art. 20 Abs. 1 Satz 2 BayVSG). Die gesetzliche Ausgestaltung dieser Berichtspflichten verfehlt jedoch die grundrechtlichen Maßstäbe aus drei Gründen:

Erstens umfassen die Berichtspflichten nicht alle Vorgänge, über die eine Berichterstattung geboten ist.

Die Berichtspflicht des Staatsministeriums des Innern an das Parlamentarische Kontrollgremium aus Art. 20 Abs. 1 Satz 1 BayVSG erstreckt sich nicht auf den Einsatz nachrichtendienstlicher Mittel gemäß Art. 8 BayVSG, obwohl

diese Norm auch eingriffsintensive Maßnahmen wie Tonaufnahmen außerhalb von Wohnungen oder längerfristige Observationen abdecken soll. Über „Quellen-Telekommunikationsüberwachungen“ gemäß Art. 13 BayVSG ist das Kontrollgremium gleichfalls nicht zu informieren. Eine Berichtspflicht ergibt sich insoweit auch nicht aus Art. 13 Abs. 2 BayVSG, da diese Vorschrift nicht auf Art. 3 AGG 10 verweist, der eine Berichtspflicht gegenüber dem Kontrollgremium errichtet.

Die Berichtspflicht des Parlamentarischen Kontrollgremiums an den Landtag aus Art. 20 Abs. 1 Satz 2 BayVSG erstreckt sich darüber hinaus auch nicht auf den Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten.

Schließlich umfassen die Berichtspflichten des Art. 20 Abs. 1 BayVSG generell nicht den weiteren Umgang mit den personenbezogenen Daten, die durch eingriffsintensive Überwachungsmaßnahmen erlangt wurden. Insbesondere eine Berichtspflicht über Datenübermittlungen fehlt.

Zweitens reichen die Berichtspflichten des Art. 20 Abs. 1 BayVSG inhaltlich nicht weit genug. Art. 20 Abs. 1 Satz 2 BayVSG lässt sich entnehmen, dass beide Berichtspflichten sich zumindest auf die Durchführung sowie Art, Umfang und Anordnungsgründe der durchgeführten Maßnahmen erstrecken. Damit fehlt es jedoch an der gleichfalls gebotenen Pflicht zur Berichterstattung darüber, inwieweit die Betroffenen über diese Maßnahmen benachrichtigt wurden,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 268.

Drittens sieht Art. 20 Abs. 1 Satz 2 BayVSG nicht vor, dass die Berichte des Parlamentarischen Kontrollgremiums an den Bayerischen Landtag zu veröffentlichen sind. Die gebotene Berichterstattung an die Öffentlichkeit ist damit generell nicht sichergestellt.

2. Unvollständige Dokumentation intensiver Grundrechtseingriffe

Ermächtigungen zu schwerwiegenden verdeckten Grundrechtseingriffen müssen durch eine hinreichend wirksame aufsichtliche Kontrolle flankiert werden. Zur wirksamen Ausgestaltung der Kontrolle zählen umfassende Dokumentationspflichten, die sich sowohl auf eingriffsintensive Überwachungsmaßnahmen als auch auf den weiteren Umgang mit den dadurch erlangten personenbezogenen Daten, insbesondere auf Datenübermittlungen erstrecken müssen,

> BVerfGE 133, 277 (370); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 141.

Die allgemeinen Regeln zur Aktenführung reichen nicht aus, um die verfassungsrechtliche Dokumentationspflicht zu erfüllen, da sie nicht gerade darauf ausgerichtet sind, die datenschutzrechtlichen Anforderungen an eine wirksame Kontrolle zu gewährleisten. Gleiches gilt für Regelungen, die eine Überwachungsmaßnahme an eine vorherige Entscheidung einer neutralen Stelle binden, selbst wenn die Entscheidungsgründe zu protokollieren sind,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 267.

Im BayVSG finden sich jedoch lediglich punktuelle und vereinzelte Dokumentationspflichten, etwa zur Löschung von Daten in § 4 Abs. 1 Satz 3 G 10 i.V.m. Art. 11 Abs. 2 Satz 3, Art. 13 Abs. 2 und Art. 17 Abs. 2 Satz 1 BayVSG. Eine umfassende Pflicht zur Dokumentation intensiver Grundrechtseingriffe fehlt hingegen.

3. Sachwidrige Zersplitterung der Datenschutzkontrolle

Eine wirksame aufsichtliche Kontrolle des Landesamts ist darüber hinaus wegen einer dysfunktionalen Aufspaltung der Kontrollaufgabe nicht gewährleistet.

Eine wirksame Aufsicht kann nicht nur an mangelhafter Ausstattung oder an unzureichenden Befugnissen der Aufsichtsbehörde scheitern, sondern auch daran, dass diese Behörde kein vollständiges Bild von den Tätigkeiten der kontrollierten Behörden erlangen kann. Das Bundesverfassungsgericht hat dementsprechend in seinem Urteil zur Antiterrordatei eine Kooperation der zuständigen Aufsichtsbehörden angemahnt, um eine effektive Kontrolle dieser Verbunddatei von Bund und Ländern sicherzustellen,

> vgl. BVerfGE 133, 277 (370).

Zur Kontrolle einiger Überwachungsmaßnahmen nach dem BayVSG ist die G 10-Kommission des Bayerischen Landtags zuständig. Im Einzelnen betrifft dies „Quellen-Telekommunikationsüberwachungen“ gemäß Art. 13 Abs. 2 BayVSG i.V.m. Art. 2 AGG 10 sowie die in Art. 15 Abs. 2 und 3 sowie in Art. 16 BayVSG geregelten Datenabrufe gemäß Art. 17 Abs. 2 Satz 1 BayVSG i.V.m. Art. 2 AGG 10.

Die Tätigkeit der Kommission erschöpft sich nicht in der – mit der Aufgabe eines Vorbehaltsrichters vergleichbaren – Vorabprüfung vorgesehener Überwachungsmaßnahmen nach Art. 2 Abs. 1 Satz 1 und Satz 2 AGG 10. Die Kommission ist darüber hinaus – ähnlich wie eine Datenschutzbehörde – gemäß Art. 2 Abs. 1 Satz 3 und Abs. 2 AGG 10 berufen, umfassend über die

Zulässigkeit und Notwendigkeit von Überwachungsmaßnahmen wie auch aller nachfolgenden Verarbeitungsschritte zu entscheiden. Hierzu räumt ihr Art. 2 Abs. 5 Satz 1 AGG 10 umfängliche Kontrollbefugnisse ein. Werden die Überwachungsmaßnahmen, die der Kontrolle der G 10-Kommission unterliegen, isoliert betrachtet, so genügt dieser gesetzliche Kontrollmechanismus zumindest im Ansatz den verfassungsrechtlichen Anforderungen,

> vgl. demgegenüber zum früheren, defizitären Befugniskreis der G 10-Kommission mit Blick auf strategische Beschränkungen durch den Bundesnachrichtendienst BVerfGE 100, 313 (401).

Die Kontrolle ist gleichwohl defizitär ausgestaltet, weil sich die Kontrollbefugnisse der G 10-Kommission auf bestimmte Überwachungsmaßnahmen und die nachgelagerten Datenverarbeitungen beschränken. Die anderen Überwachungsmaßnahmen des Landesamts unterliegen nicht der Kontrolle durch die Kommission. Diese Begrenzung der Kontrollaufgabe der G 10-Kommission hat zur Folge, dass die Kommission sich kein umfassendes Bild von den Aufklärungsaktivitäten des Landesamts machen kann. Ein Gesamtbild ist aber erforderlich, um die Maßnahmen, zu deren Kontrolle die Kommission berufen ist, umfassend zu würdigen.

So hängt die Erforderlichkeit einer Überwachungsmaßnahme immer auch davon ab, ob und welche Erkenntnisse das Landesamt mit anderen, weniger eingriffsintensiven Maßnahmen gewinnen könnte. Der Ertrag einer solchen Überwachung und die Erforderlichkeit einer (weiteren) Speicherung der Überwachungsergebnisse lassen sich nur dann vollständig bemessen, wenn der gesamte Erkenntnisstand des Landesamts vorliegt. Auch die Entscheidung darüber, die Benachrichtigung des Betroffenen einer Überwachungsmaßnahme zurückzustellen, kann von weiteren Erkenntnissen abhängen, auf welche die Kommission nicht aus eigener Initiative und nicht vollständig zugreifen kann. Schließlich gebietet die Menschenwürdegarantie des Art. 100 BV in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts, das Gesamtniveau hoheitlicher Überwachungsmaßnahmen gegenüber bestimmten Betroffenen begrenzt zu halten,

> vgl. zuletzt BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 130.

Diese „Überwachungs-Gesamtrechnung“,

> so die griffige Bezeichnung von Roßnagel, NJW 2010, S. 1238,

setzt voraus, dass zumindest die Kontrolle einer einzelnen Behörde, die zu eingriffsintensiven Überwachungsmaßnahmen ermächtigt ist, die Gesamtheit dieser Überwachungsmaßnahmen umfassen muss. Ansonsten kann die Kontrollstelle das additive Überwachungsniveau nicht zuverlässig einschätzen.

Dieses Defizit der Kontrollaufgabe der G 10-Kommission wird nicht durch andere Vorkehrungen zur Gewährleistung einer wirksamen Kontrolle kompensiert. Insbesondere kann eine hinreichend wirksame Kontrolle nicht durch ein Zusammenwirken der G 10-Kommission mit dem Bayerischen Landesbeauftragten für den Datenschutz erreicht werden.

Auch der Landesbeauftragte für den Datenschutz ist nicht umfassend zur Kontrolle des Landesamts berufen. Seine Kontrollaufgabe erstreckt sich gemäß Art. 30 Abs. 3 BayDSG grundsätzlich nicht auf personenbezogene Daten, die der Kontrolle durch die G 10-Kommission unterliegen. Diese Regelung führt somit zu einer weitgehend unverbundenen Zweiteilung der Kontrolle mit der Folge, dass keine Kontrollstelle den Erkenntnisstand und die Überwachungstätigkeit des Landesamts umfassend nachvollziehen kann.

Zwar kann die G 10-Kommission gemäß Art. 30 Abs. 3 BayDSG den Landesbeauftragten für den Datenschutz um begrenzte Kontrollmaßnahmen ersuchen. Diese Befugnis der Kommission bleibt jedoch auf ihren eigenen Aufgabenbereich bezogen und ermöglicht ihr daher nicht, sich ein Gesamtbild von der Überwachungstätigkeit des Landesamts zu machen,

> vgl. zu der Parallelvorschrift in § 24 Abs. 2 Satz 3 BDSG Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2014, § 24 Rn. 9.

Umgekehrt hat der Landesbeauftragte für den Datenschutz überhaupt keine Möglichkeit, die G 10-Kommission um die Kontrolle von Überwachungsmaßnahmen des Landesamts, die in ihrem Zuständigkeitsbereich liegen, oder von nachgelagerten Verarbeitungsschritten zu ersuchen, selbst wenn dies für seine eigene Kontrollaufgabe bedeutsam wäre.

Ein rechtfertigender Grund für die dysfunktionale Aufspaltung der Kontrolle ist nicht erkennbar. Anders als im Fall der Antiterrordatei, über den das Bundesverfassungsgericht zu entscheiden hatte, lassen sich für diese Aufspaltung keine bundesstaatlichen Gründe anführen. Es geht vielmehr hier allein um die Aufsicht über eine einzige Behörde eines einzigen Landes mit einer einheitlichen gesetzlichen Aufgabe. Diese Kontrollaufgabe ließe sich ohne weiteres gleichfalls vereinheitlichen. Beispielsweise könnte die Kontrollaufgabe der

G 10-Kommission auf eine richterähnliche Vorabprüfung bestimmter Überwachungsmaßnahmen beschränkt und die gesamte Ex-post-Kontrolle bei dem Landesbeauftragten für den Datenschutz konzentriert werden. Dies wäre auch im Anwendungsbereich von Art. 10 Abs. 2 Satz 2 GG möglich, da der Landesbeauftragte gemäß Art. 29 Abs. 1 Satz 1 BayDSG vom Bayerischen Landtag gewählt wird und damit gleichfalls ein von der Volksvertretung bestelltes Organ im Sinne dieser Norm ist,

> vgl. BVerfGE 67, 157 (185); BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, Rn. 45.

Insoweit besteht ein erheblicher Gestaltungsspielraum des Gesetzgebers, der jedoch endet, wenn – wie gegenwärtig – insgesamt eine wirksame Kontrolle des Landesamts nicht zuverlässig gewährleistet ist.

VIII. Verarbeitung und Nutzung personenbezogener Daten über Minderjährige

Die allgemeine Regelung in Art. 5 Abs. 1 Satz 1 BayVSG, die das Landesamt zur Verarbeitung und Nutzung erhobener personenbezogener Daten ermächtigt, ist insoweit verfassungswidrig, als sie sich unmodifiziert auch auf personenbezogene Daten über Minderjährige erstreckt.

Die Verarbeitung personenbezogener Daten über Minderjährige stellt einen besonders intensiven Eingriff in deren Recht auf informationelle Selbstbestimmung aus Art. 101 i.V.m. Art. 100 BV dar. Denn zu den allgemeinen Schutzzielen dieses Grundrechts tritt bei Minderjährigen das Anliegen hinzu, ihnen eine ungestörte Persönlichkeitsentwicklung zu ermöglichen. Eine Beobachtung des Verhaltens von Minderjährigen und insbesondere von Kindern durch staatliche Stellen kann deren Persönlichkeitsentfaltung empfindlicher stören als dies bei Erwachsenen anzunehmen ist. Dementsprechend muss dieser Personenkreis in weitergehendem Ausmaß vor einer solchen Beobachtung geschützt werden,

> vgl. zum Schutz des allgemeinen Persönlichkeitsrechts von Kindern in unterschiedlichen Fallkonstellationen BVerfGE 24, 119 (144); 57, 361 (383) 101, 361 (385).

Dieses Schutzbedürfnis erstreckt sich auf die Bevorratung und Nutzung personenbezogener Daten Minderjähriger. Eine solche Weiterverarbeitung erhobener Daten begründet das Risiko, dass Minderjährige ohne Rücksicht auf die

Spezifika ihrer Persönlichkeitsentwicklung mittel- oder sogar langfristig mit „Jugendsünden“ konfrontiert werden und so in ihrer weiteren Entwicklung erheblich beeinträchtigt werden.

Die Verarbeitung und Nutzung erhobener personenbezogener Daten über Minderjährige durch eine Verfassungsschutzbehörde ist danach verfassungsrechtlich zwar nicht schlechthin ausgeschlossen. Sie muss aber insbesondere für Kinder durch besondere Schutzregelungen auf Ausnahmefälle beschränkt werden, in denen ein besonders gewichtiges Beobachtungsbedürfnis es rechtfertigt, den prinzipiell gebotenen Minderjährigenschutz ausnahmsweise einzuschränken. Dabei ist es verfassungsrechtlich zulässig, den grundrechtlich gebotenen Minderjährigenschutz nach Altersstufen und nach der generellen Eingriffsintensität behördlicher Datenverarbeitungen abzuschichten. Ein Beispiel für einen solchen abgestuften Schutzansatz bildet § 11 BVerfSchG. Diese Regelung unterscheidet zum einen zwischen Kindern (§ 11 Abs. 1 BVerfSchG) und Jugendlichen unter 16 Jahren (§ 11 Abs. 2 BVerfSchG), die unterschiedlich stark geschützt werden. Zum anderen unterscheidet § 11 Abs. 1 BVerfSchG für Kinder zwischen Datenspeicherungen in Personenakten, die ausnahmsweise zulässig sind, und Datenspeicherungen in Dateien, die vollständig ausgeschlossen werden. Dies ist ein verfassungsrechtlich zumindest im Ansatz tragfähiges Schutzkonzept.

Das BayVSG trägt dem besonderen Schutzbedarf von Minderjährigen und insbesondere von Kindern demgegenüber nur unzureichend Rechnung. Insbesondere ermächtigt Art. 5 Abs. 1 Satz 1 BayVSG das Landesamt umfassend zur Verarbeitung und Nutzung personenbezogener Daten auch dieses Personenkreises.

Im Gesetz finden sich lediglich besondere Regelungen über die Pflicht zur Datenlöschung (Art. 21 Abs. 1 Satz 3 BayVSG i.V.m. § 63 Abs. 1 BZRG) und über die Frist zur Überprüfung von Datenspeicherungen (Art. 21 Abs. 3 Satz 2 BayVSG). Diese Regelungen ändern jedoch nichts an der umfassenden Bevorratungs- und Nutzungsbefugnis des Landesamts. Zudem vermitteln sie selbst nur einen sehr unvollkommenen Schutz. So ermöglicht Art. 21 Abs. 1 Satz 3 BayVSG i.V.m. § 63 Abs. 1 BZRG ohne weitere Vorgaben eine Datenspeicherung bis zur Vollendung des 24. Lebensjahres. Der persönlichkeitsrechtlich besonders sensible Zeitraum der Persönlichkeitsentwicklung einer minderjährigen oder heranwachsenden Person wird durch diese Regelung mithin überhaupt nicht erfasst. Art. 21 Abs. 3 Satz 2 BayVSG verkürzt die allgemeine Überprüfungsfrist auf einen zweijährigen Turnus, errichtet jedoch

keine materiellen Vorgaben für die durchzuführende datenschutzrechtliche Prüfung.

(Prof. Dr. Bäcker, LL.M.)

Anlagen

1. Verfahrensvollmachten
2. Plenarprotokoll 17/66 vom 25. Februar 2016 (Auszug)
3. Wortlautprotokoll der öffentlichen Anhörung vom 27. April 2016
4. Protokoll der Sitzung des Innenausschusses des Bayerischen Landtags vom 8. Juni 2016
5. Plenarprotokoll 17/78 vom 7. Juli 2016 (Auszug)
6. Stellungnahme des Sachverständigen Prof. Dr. Matthias Bäcker für die öffentliche Anhörung am 27. April 2016
7. Stellungnahme des Sachverständigen Dr. Thomas Kuhn für die öffentliche Anhörung am 27. April 2016
8. Stellungnahme des Sachverständigen Dr. Markus Löffelmann für die öffentliche Anhörung am 27. April 2016
9. Stellungnahme des Sachverständigen Dr. Thomas Petri für die öffentliche Anhörung am 27. April 2016