

Dr. Rosemarie Will

Universitätsprofessorin
Landesverfassungsrichterin
des Landes Brandenburg a. D.

Marchlewski Str. 31
10243 Berlin
☎ 030 2930 95 35
0174 33 277 32

An das
Bundesverfassungsgericht

Postfach 1771
76006 Karlsruhe

Berlin, 18.09.2008

Verfassungsbeschwerde

- 1) der Frau Bärbel Narnhammer
Beethovenstraße 23
85622 Feldkirchen

- 2) des Herrn Florian Ritter
Dachauer Straße 187
80637 München

- 3) der Frau Adelheid Rupp
Daiserstraße 27
81371 München

- 4) des Herrn Franz Schindler
Friedrich-Ebert-Straße 49
92421 Schwandorf

- Beschwerdeführer -

alle vertreten durch

Prof. Dr. Rosemarie Will, Marchlewski Str. 31, 10243 Berlin

- Prozessbevollmächtigte -

gegen

1. das Bayerische Verfassungsschutzgesetz (BayVSG) in der Fassung der Bekanntmachung vom 10. April 1997 (GVBl S. 70, BayRS 12-1-I), zuletzt geändert durch § 1 des Gesetzes vom 8. Juli 2008 (GVBl S. 357)

und

2. das Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz - PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl S. 397, BayRS 2012-1-1-I), zuletzt geändert durch Art. 27 Abs. 1 des Gesetzes vom 22. Juli 2008 (GVBl S. 421)

Ich zeige an, dass die vier Beschwerdeführer mich beauftragt haben, ihre Interessen vor dem Bundesverfassungsgericht wahrzunehmen und mir Vollmacht erteilt haben.

Die vier Vollmachten lege ich vor als

Anlagen B 1 – B 4.

Namens und im Auftrag der Beschwerdeführer erhebe ich

Verfassungsbeschwerde

gegen

1. Art. 6a, 6b ,6d, 6e, 6f, 6g

des Bayerischen Verfassungsschutzgesetzes (BayVSG) in der Fassung der Bekanntmachung vom 10. April 1997 (GVBI S. 70, BayRS 12-1-I), zuletzt geändert durch § 1 des Gesetzes vom 8. Juli 2008 (GVBI S. 357)

2. Art. 34, 34a, 34c, 34d, 34e

des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz - PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBI S. 397, BayRS 2012-1-1-I), zuletzt geändert durch Art. 27 Abs. 1 des Gesetzes vom 22. Juli 2008 (GVBI S. 421).

Es wird beantragt,

1. die Verfassungswidrigkeit der genannten Vorschriften festzustellen

sowie

2. der Staatskasse die notwendigen Auslagen der Beschwerdeführer aufzuerlegen.

Gerügt wird die Verletzung von:

- Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – in seiner Ausprägung als Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme,
- Art. 1 Abs. 1 GG in seiner Ausprägung als Kernbereich privater Lebensgestaltung,
- Art. 13 GG.

Inhalt der Beschwerdeschrift:

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Gegenstand der Verfassungsbeschwerde | 6 |
| A. Sachverhalt | 6 |
| I. Die angegriffenen Normen | 6 |
| 1) BayVSG | 6 |
| Art. 6a Einsatz technischer Mittel im Schutzbereich des Art. 13 Grundgesetz | 6 |
| Art. 6b Verfahrensregelungen für Maßnahmen nach Art. 6a BayVSG | 8 |
| Art. 6d Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes..... | 10 |
| Art. 6e Verdeckte Online-Datenerhebung | 11 |
| Art. 6f Verfahrensvorschriften | 11 |
| Art. 6g Notwendige Begleitmaßnahmen | 13 |
| 2) PAG | 13 |
| Art. 34 Besondere Bestimmungen über den Einsatz technischer Mittel in Wohnungen..... | 13 |
| Art. 34a Datenerhebung und Eingriffe in den Telekommunikationsbereich..... | 16 |
| Art. 34c Verfahrensregelungen, Verwendungsverbote, Zweckbindung, Benachrichtigung und Löschung..... | 17 |
| Art. 34d Verdeckter Zugriff auf informationstechnische Systeme..... | 19 |
| Art. 34e Notwendige Begleitmaßnahmen | 22 |
| II. Die Beschwerdeführer | 22 |
| Benutzung informationstechnischer Systeme..... | 23 |
| Kontakte zu Organisationen, die vom Verfassungsschutz observiert werden..... | 23 |
| B. Zulässigkeit | 25 |
| I. Beschwerdefähigkeit..... | 25 |
| II. Beschwerdebefugnis bezüglich der Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 13 GG und Art. 1 Abs. 1 GG | 25 |
| III. eigene Beschwer | 26 |
| IV. gegenwärtige Beschwer | 27 |
| V. unmittelbare Betroffenheit | 27 |
| VI. Frist..... | 28 |
| VII. Subsidiarität..... | 28 |
| C. Begründetheit..... | 29 |
| I. Verfassungswidrigkeit der Online-Durchsuchung in Art. 34d PAG und in Art. 6e BayVSG | 29 |
| 1) Die verfassungsrechtlichen Maßstäbe für einen verdeckten Zugriff mit technischen Mitteln auf informationstechnische Systeme | 29 |
| 2) Die Verfassungswidrigkeit des verdeckten Zugriffs auf informations- technische Systeme nach Art. 34d PAG..... | 31 |
| (a) Die Verfassungswidrigkeit der in Art. 34d Abs. 1 Satz 1 Nr. 2 PAG formulierten Eingriffsschwelle | 31 |
| (b) Verfassungswidrige Eingriffsdifferenzierung in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zwischen der Erhebung von Zugangsdaten und der Erhebung von gespeicherten Daten | 34 |
| (c) Befugnis zur Datenänderung und Datenlöschung als Mittel der Gefahrenabwehr nach Art. 34d Abs. 1 Satz 2 PAG..... | 35 |
| (d) Unzureichender Richtervorbehalt in Art. 34d Abs. 3 PAG | 36 |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| (e) Zweckänderung nach Art. 34d Abs. 5 Satz 2 Nr. 2 PAG | 37 |
| 3) Die Verfassungswidrigkeit der Online Datenerhebung nach Art. 6e BayVSG .. | 38 |
| (a) Verfassungswidrige Eingriffsermächtigung in Art. 6e Abs. 1 Satz 1 BayVSG | 38 |
| (b) Fehlender eigenständiger Richtervorbehalt | 40 |
| 4) Unterschreiten der staatlichen Gewährleistungspflichten für die Vertraulichkeit und Integrität informationstechnischer Systeme in Art. 34d PAG und Art. 6e BayVSG | 41 |
| II. Verfassungswidrigkeit der Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG | 43 |
| 1) Begleit- und Hauptmaßnahmen | 43 |
| 2) Art. 13 GG als eigenständiger Maßstab für die Prüfung der Begleitmaßnahmen in Art. 6g VSG und Art. 34e PAG | 47 |
| 3) Grundsatz der Offenheit der Durchsuchung in Art. 13 Abs. 2 GG | 49 |
| (a) Durchsuchungsbegriff | 49 |
| (b) Offenheit der Durchsuchung | 50 |
| (c) Fehlende Offenheit der Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG | 51 |
| 4) Heimliches Betreten als verfassungswidrige Begleitmaßnahme einer präventiven Wohnungsüberwachung mit technischen Mitteln nach Art. 13 Abs. 4 GG | 52 |
| (a) Anordnungsvoraussetzungen nach Art. 13 Abs. 4 GG | 52 |
| (b) Verstoß gegen die Maßstäbe von Art. 13 Abs. 4 GG durch Art. 6g BayVSG und Art. 34e PAG | 53 |
| III. Die Verfassungswidrigkeit der den Kernbereich privater Lebensgestaltung schützenden Regelungen | 54 |
| 1) Die neuen kernbereichsschützenden Regelungen | 54 |
| (a) Die neuen kernbereichsschützenden Regelungen im BayVSG | 54 |
| (b) Die neuen kernbereichsschützenden Regelungen im PAG | 56 |
| 2) Die verfassungsrechtlichen Vorgaben für den Kernbereichsschutz bei verdeckten Datenerhebungen | 59 |
| (a) Die Absolutheit des Kernbereichsschutzes | 59 |
| (b) Das 2-stufige Schutzkonzept | 59 |
| (c) Die Einheitlichkeit des Schutzstandards für den Kernbereich privater Lebensgestaltung bei Neuregelungen zur verdeckten Datenerhebung | 60 |
| 3) Die Verfassungswidrigkeit der neuen Kernbereichsregelungen | 61 |
| (a) Keine ausreichende Regelung von Anhaltspunkten für eine drohende Kernbereichsverletzung (unzureichendes Schutzkonzept auf der ersten Stufe) | 61 |
| (b) Unzureichende Bestimmtheit der Regelungen über das „Vortäuschen kernbereichszugehöriger Kommunikation zur Überwachungs- verhinderung“ | 63 |
| (c) Verfassungsrechtlich unzureichendes Schutzkonzept auf der zweiten Stufe | 64 |

Gegenstand der Verfassungsbeschwerde

Die Verfassungsbeschwerde betrifft die in das Bayerische Polizeiaufgabengesetz und in das Bayerische Verfassungsschutzgesetz zum 01.08.2008 neu aufgenommenen Onlinedurchsuchungsbefugnisse, die neu eingeführten Begleitmaßnahmen zum heimlichen Betreten und Durchsuchen von Wohnungen zum Zwecke der verdeckten Datenerhebung und die neu geregelten Maßnahmen zum Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen.

A. Sachverhalt

I. Die angegriffenen Normen

Die Verfassungsbeschwerde richtet sich gegen die folgenden Normen des BayVSG und des PAG (Die angegriffenen Neuregelungen sind fett und kursiv gedruckt.).

1) BayVSG

Die Neufassungen der Art. 6a und 6b:

Art. 6a
Einsatz technischer Mittel im
Schutzbereich des Art. 13 Grundgesetz

(1) Das Landesamt für Verfassungsschutz darf technische Mittel im Schutzbereich des Art. 13 des Grundgesetzes als nachrichtendienstliche Mittel im Sinn des Art. 6 Abs. 1 unter besonderer Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach Art. 6 Abs. 3 nur unter den nachfolgenden Voraussetzungen einsetzen.

(2) ¹Maßnahmen nach Abs. 1 sind nur zulässig, sofern tatsächliche Anhaltspunkte für den Verdacht vorliegen, dass jemand Bestrebungen oder Tätigkeiten nach Art. 3 Abs. 1 Satz 1 durch die Planung oder Begehung von Straftaten verfolgt, die im Einzelfall geeignet sind, den Bestand oder die Sicherheit des Bundes oder eines Landes oder in erheblichem Maße Leib, Leben oder Freiheit von Personen zu gefährden. ²Solche Straftaten sind:

- 1. Straftaten des Friedensverrats, Hochverrats und Landesverrats (§§ 80, 81, 82, 94 Strafgesetzbuch - StGB),***
- 2. Straftaten gegen die öffentliche Ordnung (§§ 129a, 129b StGB),***

3. **Straftaten gegen das Leben (§§ 211, 212 StGB, § 6 Völkerstrafgesetzbuch),**
4. **Straftaten gegen die persönliche Freiheit (§§ 232, 233, 233a Abs. 2, §§ 234, 234a Abs. 1, §§ 239a, 239b StGB),**
5. **Gemeingefährliche Straftaten in den Fällen der §§ 306a, 306b, 307 Abs. 1 und 2, § 308 Abs. 1, § 309 Abs. 1, § 310 Abs. 1, § 313 Abs. 1, § 314 Abs. 1, § 315 Abs. 3, § 315b Abs. 3, § 316c StGB und**
6. **Straftaten nach dem Waffengesetz (WaffG) und dem Gesetz über die Kontrolle von Kriegswaffen (§ 51 Abs. 1 in Verbindung mit Abs. 2, § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5 WaffG; § 19 Abs. 2, § 20 Abs. 1, jeweils auch in Verbindung mit § 21 des Gesetzes über die Kontrolle von Kriegswaffen; § 22a Abs. 1 in Verbindung mit Abs. 2 des Gesetzes über die Kontrolle von Kriegswaffen).**

(3) ¹Maßnahmen nach Abs. 1 sind nur zulässig, wenn und soweit

1. **die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und**
2. **für den Fall, dass zu privaten Wohnzwecken genutzte Räumlichkeiten betroffen sind, in denen sich die Person, gegen die sich die Maßnahme richtet, allein oder ausschließlich mit engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsgeheimnisträgern nach §§ 53, 53a der Strafprozessordnung (StPO) in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl I S. 1074, 1319) in der jeweils geltenden Fassung aufhält,**
 - a) **tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gespräche geführt werden, die einen unmittelbaren Bezug zu den im Abs. 2 genannten Bestrebungen oder Tätigkeiten haben, ohne dass ein Gesprächsteilnehmer über ihren Inhalt das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigern könnte, oder**
 - b) **die Maßnahme sich auch gegen die Familienangehörigen, Vertrauten oder Berufsgeheimnisträger richtet, und**
3. **für den Fall, dass sich die Maßnahme gegen einen Berufsgeheimnisträger nach §§ 53, 53a StPO selbst richtet und die zu seiner Berufsausübung bestimmten Räumlichkeiten betroffen sind, die Voraussetzungen der Nr. 2 Buchst. a vorliegen.**

²**In den Fällen des Satzes 1 Nrn. 2 und 3 ist eine nur automatische Aufzeichnung zulässig, wenn bei Anordnung der Maßnahme abzusehen ist, dass keine Gespräche geführt werden, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind; wird bei einer Maßnahme nach Abs. 1 erkennbar, dass solche Gespräche geführt werden und bestehen keine Anhaltspunkte dafür, dass sie dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Datenerhebung unverzüglich und so lange erforderlich zu unterbrechen.**

(4) ¹Maßnahmen nach Abs. 1 dürfen im Fall des Abs. 3 Satz 1 Nr. 2 nur in Wohnungen des in der Anordnung bezeichneten Adressaten durchgeführt werden. ²In Wohnungen anderer Personen sind die Maßnahmen zulässig, wenn es nicht Wohnungen von Berufsgeheimnisträgern nach §§ 53, 53a StPO sind und auf Grund bestimmter Tatsachen anzunehmen ist, dass

- 1. der Adressat sich dort aufhält und**
- 2. die Maßnahme in Wohnungen des Adressaten allein zur Erforschung des Sachverhalts nicht möglich oder nicht ausreichend ist.**

³Die Erhebung personenbezogener Daten über andere als die in Satz 1 genannten Personen ist zulässig, soweit sie unvermeidliche Folge einer Maßnahme nach Abs. 1 ist.

**Art. 6b
Verfahrensregelungen für
Maßnahmen nach Art. 6a**

(1) ¹Der Einsatz technischer Mittel nach Art. 6a bedarf einer richterlichen Anordnung auf Antrag des Präsidenten des Landesamts für Verfassungsschutz oder dessen Stellvertreters. ²Bei Gefahr im Verzug kann der Präsident des Landesamts für Verfassungsschutz oder dessen Vertreter die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen. ³In der schriftlichen Anordnung sind Adressat, Art, Umfang und Dauer der Maßnahme zu bestimmen und die wesentlichen Gründe zu benennen. ⁴Die Anordnung ist auf längstens einen Monat zu befristen; Verlängerungen um jeweils nicht mehr als einen Monat sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. ⁵Liegen die Voraussetzungen nicht mehr vor oder ist der verdeckte Einsatz technischer Mittel nicht mehr erforderlich, so ist die Maßnahme ungeachtet des in der Anordnung genannten Zeitraums unverzüglich zu beenden. ⁶Die Beendigung ist dem Richter mitzuteilen. ⁷Ein Bediensteter des Landesamts für Verfassungsschutz mit Befähigung zum Richteramt beaufsichtigt den Vollzug der Anordnung und eventuelle Datenübermittlungen.

(2) ¹Die durch Maßnahmen nach Art. 6a erhobenen Daten sind als solche zu kennzeichnen. ²Nach einer Übermittlung hat der Empfänger die Kennzeichnung aufrecht zu erhalten; darauf ist dieser hinzuweisen. ³Daten aus Maßnahmen nach Art. 6a dürfen nur verwendet werden

- 1. zur Abwehr und Aufklärung der in Art. 6a Abs. 2 genannten Gefahren,**
- 2. zur Verfolgung von Straftaten, wenn die Voraussetzungen der Strafprozessordnung für die Datenerhebung bei der Erhebung vorgelegen haben und bei der Übermittlung noch vorliegen,**
- 3. zur Abwehr dringender Gefahren für Leib, Leben oder Freiheit von Menschen.**

⁴Das Landesamt für Verfassungsschutz prüft unverzüglich und dann in Abständen von sechs Monaten, ob die durch Maßnahmen nach Art. 6a erhobenen personenbezogenen Daten allein oder zusammen mit bereits vorliegenden Daten für die Zwecke des Satzes 3 erforderlich sind. ⁵Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art 6a Abs. 2 genannten Bestrebungen oder Tätigkeiten haben,

dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich und Daten im Sinn der Nr. 2 oder 3 sind nicht betroffen. ⁶Über eine Übermittlung von Daten aus einer Maßnahme nach Art. 6a an Stellen außerhalb des Verbunds der Verfassungsschutzbehörden entscheidet der Richter. ⁷Bei Gefahr im Verzug kann die Entscheidung auch der Präsident des Landesamts für Verfassungsschutz oder dessen Vertreter treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen.

(3) ¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen. ²Die durch eine Maßnahme nach Art. 6a Abs. 1 erlangten personenbezogenen Daten, deren Verwendung zu den in Abs. 2 Satz 3 genannten Zwecken nicht erforderlich ist oder für die ein Verwendungsverbot besteht, sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen; soweit die Daten für eine Mitteilung an den Betroffenen oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können, sind sie zu sperren. ³Die gesperrten Daten dürfen nur zu den in Satz 2 Halbsatz 2 genannten Zwecken verwendet werden. ⁴Im Fall der Mitteilung an den Betroffenen sind die Daten erst zu löschen, wenn der Betroffene nach Ablauf eines Monats nach seiner Benachrichtigung keine Klage erhebt; auf diese Frist ist in der Mitteilung hinzuweisen. ⁵Im Fall einer gerichtlichen Überprüfung sind die Daten nach deren Abschluss zu löschen. ⁶Die Löschung von Daten ist zu protokollieren.

(4) ¹Das Landesamt für Verfassungsschutz teilt den in der Anordnung bezeichneten Personen sowie denjenigen, deren personenbezogene Daten erhoben und zu den Zwecken des Abs. 2 Satz 3 verwendet wurden, Maßnahmen nach Art. 6a Abs. 1 nach ihrer Einstellung, frühestens jedoch dann mit, wenn eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. ²Erfolgt die Mitteilung nicht binnen sechs Monaten nach Einstellung der Maßnahmen, bedarf ihre weitere Zurückstellung der richterlichen Zustimmung. ³Dem Gericht sind die Gründe mitzuteilen, die einer Mitteilung an den Betroffenen entgegenstehen. ⁴Die richterliche Entscheidung ist jeweils nach einem Jahr erneut einzuholen, wenn das Gericht keine andere Frist bestimmt. ⁵Eine Mitteilung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

1. *überwiegende Interessen eines Betroffenen entgegenstehen,*
2. *die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann oder*
3. *die Voraussetzungen für eine Mitteilung auch nach fünf Jahren nach Beendigung der Maßnahme nicht eingetreten sind, sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden und die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger der Daten vorliegen.*

(5) ¹Der verdeckte Einsatz technischer Mittel im Schutzbereich des Art. 13 des Grundgesetzes ausschließlich zum Schutz der für den Verfassungsschutz in diesem Bereich tätigen Personen bedarf der Anordnung des Präsidenten des Landesamts für Verfassungsschutz oder eines von ihm bestellten Beauftragten. ²Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse ist nur zulässig, wenn zuvor der Richter festgestellt hat, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des Art. 6a Abs. 2 vorliegen; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. ³Soweit Erkenntnisse verwendet werden, gelten für die Datenverarbeitung, die Löschung der Daten und die Mitteilung an den Betroffenen Abs. 2 bis 4 entsprechend. ⁴Im Übrigen sind die Daten unverzüglich zu löschen.

(6) ¹Zuständiges Gericht zur Entscheidung nach den Abs. 1, 2, 4 und 5 ist das Amtsgericht am Sitz des Landesamts für Verfassungsschutz. ²Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit (BGBl III 315-1), zuletzt geändert durch Art. 3 des Gesetzes vom 26. März 2008 (BGBl I S. 441), entsprechend.

(7) ¹Die Staatsregierung unterrichtet den Landtag jährlich über die gemäß Art 6a und, soweit richterlich überprüfungsbedürftig, nach Abs. 5 angeordneten Maßnahmen. ²Das Parlamentarische Kontrollgremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus.

Die Neuregelungen der Art. 6d bis 6g:

Art. 6d
Abhören und Aufzeichnen des
nichtöffentlich gesprochenen Wortes

Das Landesamt für Verfassungsschutz darf außerhalb von Wohnungen und außerhalb des Anwendungsbereichs des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) vom 26. Juni 2001 (BGBl I S. 1254, 2298) in der jeweils geltenden Fassung das nichtöffentlich gesprochene Wort unter besonderer Berücksichtigung des Grundsatzes der Verhältnismäßigkeit nach Art. 6 Abs. 3 mit dem verdeckten Einsatz technischer Mittel abhören und aufzeichnen.

Art. 6e
Verdeckte Online-Datenerhebung

(1) ¹Das Landesamt für Verfassungsschutz kann bei Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut unter den Voraussetzungen des Art. 6a Abs. 2 im Einzelfall mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben. ²Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. ³Sie darf sich nur gegen Verdächtige und ihre Nachrichtenmittler richten. ⁴Gegen Nachrichtenmittler darf sich die Maßnahme nur insoweit richten, als sie kein Recht zur Verweigerung des Zeugnisses nach den §§ 53, 53a StPO haben. ⁵Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Maßnahme insoweit unzulässig, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst. ⁶Soweit informationstechnisch und ermittlungstechnisch möglich, sind alle Maßnahmen zu ergreifen, mit denen die Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, vermieden werden kann. ⁷Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die weitere Datenerhebung insoweit unzulässig.

(2) ¹Zur Vorbereitung einer Maßnahme nach Abs. 1 dürfen auch technische Mittel eingesetzt werden, um spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln. ²Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, soweit dies aus technischen Gründen unvermeidbar ist. ³Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

Art. 6f
Verfahrensvorschriften

(1) ¹Maßnahmen nach Art. 6c Abs. 4 sowie Auskünfte nach Art. 6c Abs. 2 bedürfen eines Antrags, der durch den Präsidenten des Landesamts für Verfassungsschutz oder seinen Vertreter schriftlich zu stellen und zu begründen ist. ²Über den Antrag entscheidet das Staatsministerium des Innern.

(2) ¹Die Anordnung einer Maßnahme nach Art. 6c Abs. 4 sowie eines Auskunftersuchens nach Art. 6c Abs. 2 über künftig anfallende Daten ist auf höchstens drei Monate zu befristen. ²Eine Verlängerung um jeweils nicht mehr als drei Monate ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. ³Anordnungen über Auskunftersuchen nach Art. 6c Abs. 2 sind dem Verpflichteten insoweit schriftlich mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtung zu ermöglichen. ⁴Das Auskunftersuchen und die übermittelten Daten darf der Verpflichtete dem Betroffenen oder Dritten nicht mitteilen.

(3) ¹Im Fall der Anordnung eines Auskunftersuchens nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 sowie bei Maßnahmen nach Art. 6c Abs. 4 unterrichtet das Staatsministerium des Innern monatlich die nach Art. 2 des Ausführungsgesetzes Art. 10-Gesetz (AGG 10) gebildete Kommission über die Anordnungen vor deren Vollzug. ²Bei Gefahr im Verzug kann es den Vollzug der Anordnung auch bereits vor der Unterrichtung der Kommission anordnen. ³Die Kommission prüft von Amts wegen oder auf Grund von

Beschwerden, ob die Anordnung zulässig und notwendig ist. ⁴§ 15 Abs. 5 G 10 ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach Art. 6c Abs. 2 Satz 1 Nrn. 3 bis 5 und Abs. 4 erlangten personenbezogenen Daten erstreckt. ⁵Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt hat, hat das Staatsministerium des Innern unverzüglich aufzuheben. ⁶Die Daten unterliegen in diesem Fall einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. ⁷Für die Verarbeitung der erhobenen Daten ist § 4 G 10 entsprechend anzuwenden. ⁸Für die Mitteilung an den Betroffenen finden § 12 Abs. 1 und 3 G 10 entsprechende Anwendung.

(4) ¹Die Erhebung und Verwendung von Daten nach Art. 6d bedarf der Genehmigung des Präsidenten des Landesamts für Verfassungsschutz oder seines Stellvertreters. ²Soweit bei Maßnahmen nach Art. 6d Daten erhoben wurden, bei denen sich nach Auswertung herausstellt, dass

- 1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder**
- 2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder**
- 3. sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 6a Abs. 2 genannten Bestrebungen oder Tätigkeiten haben,**

dürfen sie nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich und Daten im Sinn der Nr. 2 oder 3 sind nicht betroffen. ³Daten, die nicht verwendet werden dürfen, sind unverzüglich zu löschen.

(5) ¹Bei Maßnahmen nach Art. 6e gelten Art. 6b Abs. 1 bis 4 und 6 entsprechend. ²Die schriftliche Anordnung der Maßnahme muss soweit möglich Namen und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sowie die Bezeichnung des informationstechnischen Systems, auf das zugegriffen werden soll, enthalten und ist bei der erstmaligen Anordnung abweichend von Art. 6b Abs. 1 Satz 4 auf höchstens drei Monate zu befristen. ³Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten

- 1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind oder**
- 2. Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder**
- 3. einem Vertrauensverhältnis mit anderen Berufsheimlichkeitsgeheimnisträgern zuzuordnen sind,**

sind diese unverzüglich zu löschen oder dem zuständigen Richter zur Entscheidung über die weitere Verwendung vorzulegen. ⁴Art. 6b Abs. 2 Satz 7 und Art. 6b Abs. 6 gelten im Fall des Satzes 3 entsprechend.

Art. 6g
Notwendige Begleitmaßnahmen

¹Zur Durchführung von Maßnahmen nach Art. 6a und 6e Abs. 1 und 2 kann das Landesamt für Verfassungsschutz verdeckt Sachen durchsuchen sowie die Wohnung des Betroffenen ohne Einwilligung betreten und durchsuchen. ²Für die Anordnung dieser Begleitmaßnahmen und die Unterrichtung der Betroffenen finden die für die Maßnahmen nach Art. 6a und 6e Abs. 1 und 2 jeweils geltenden Vorschriften entsprechende Anwendung. ³Zur Durchführung von Maßnahmen nach dem Art. 10-Gesetz, kann das Landesamt für Verfassungsschutz verdeckt Sachen durchsuchen sowie bei Vorliegen einer dringenden Gefahr für die öffentliche Sicherheit und Ordnung die Wohnung des Betroffenen ohne Einwilligung betreten und durchsuchen. ⁴Für die Anordnung dieser Begleitmaßnahme und die Unterrichtung der Betroffenen finden die für Maßnahmen nach Art. 6e geltenden Vorschriften entsprechende Anwendung.

2) PAG

Die Verfassungsbeschwerde richtet sich weiter gegen folgende Normen des PAG:

Art. 34
Besondere Bestimmungen über den
Einsatz technischer Mittel in Wohnungen

(1) ¹Die Polizei kann durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (Art. 23 Abs. 1 Satz 2) personenbezogene Daten erheben

1. über die für eine Gefahr Verantwortlichen, wenn dies erforderlich ist zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder
2. über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat **nach Art. 30 Abs. 5 Satz 1 Nrn. 1, 2 (ohne § 129 Abs. 1 in Verbindung mit Abs. 4 StGB) bis 9** begehen werden.

²Eine Maßnahme nach Satz 1 ist nur zulässig, wenn und soweit

1. die dort genannten Gefahren nicht anders abgewehrt oder die dort genannten Straftaten nicht anders verhütet oder abgewehrt werden können und
2. für den Fall, dass zu privaten Wohnzwecken genutzte Räumlichkeiten betroffen sind, in denen sich die Person, gegen die sich die Maßnahme richtet, allein oder ausschließlich mit engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsgeheimnisträgern nach §§ 53, 53a StPO aufhält,

- a) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gespräche geführt werden, die einen unmittelbaren Bezug zu den in Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben, ohne dass über ihren Inhalt das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
 - b) die Maßnahme sich auch gegen die Familienangehörigen, Vertrauten oder Berufsheimnisträger richtet, und
3. für den Fall, dass sich die Maßnahme gegen einen Berufsheimnisträger nach §§ 53, 53a StPO selbst richtet und die zu seiner Berufsausübung bestimmten Räumlichkeiten betroffen sind, die Voraussetzungen der Nr. 2 Buchst. a vorliegen.

(2) In den Fällen des Abs. 1 Satz 2 Nrn. 2 und 3 ist eine nur automatische Aufzeichnung zulässig, wenn bei Anordnung der Maßnahme abzusehen ist, dass keine Gespräche geführt werden, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind; wird bei einer Maßnahme nach Abs. 1 Satz 1 erkennbar, dass solche Gespräche geführt werden **und bestehen keine Anhaltspunkte dafür, dass sie dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen**, ist die Datenerhebung unverzüglich und so lange erforderlich zu unterbrechen.

(3) ¹Die Maßnahme darf nur in den Wohnungen des Adressaten durchgeführt werden. ²In Wohnungen anderer Personen ist die Maßnahme zulässig, wenn es nicht Wohnungen von Berufsheimnisträgern nach §§ 53, 53a StPO sind und auf Grund bestimmter Tatsachen anzunehmen ist, dass

- 1. der in der Anordnung bezeichnete Adressat sich dort aufhält und
- 2. die Maßnahme in Wohnungen des Adressaten allein zur Abwehr der Gefahr oder der Straftat nicht möglich oder nicht ausreichend ist.

³Die Erhebung personenbezogener Daten über andere als die in Satz 1 genannten Personen ist zulässig, soweit sie unvermeidliche Folge einer Maßnahme nach Abs. 1 Satz 1 ist.

(4) ¹Eine Maßnahme nach Abs. 1 Satz 1 darf nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 33 Abs. 5 Satz 1 genannten Dienststellenleiter; in diesem Fall ist unverzüglich eine Bestätigung der Maßnahme durch einen Richter einzuholen. ²Für die richterliche Anordnung ist Art. 24 Abs. 1 Satz 3 entsprechend anzuwenden; zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. ³In der schriftlichen Anordnung sind Adressat, Art, Umfang und Dauer der Maßnahme zu bestimmen und die wesentlichen Gründe anzugeben. ⁴Die Maßnahme ist auf höchstens einen Monat zu befristen und kann um jeweils nicht mehr als einen Monat verlängert werden. ⁵Ungeachtet des in der Anordnung genannten Zeitraums ist die Maßnahme unverzüglich zu beenden, wenn die in Abs. 1 Satz 1 genannten Voraussetzungen nicht mehr fortbestehen; die Beendigung ist dem Richter mitzuteilen.

(5) ¹Die durch eine Maßnahme nach Abs. 1 Satz 1 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. ²Sie dürfen nur verwendet werden

- 1. zu den in Abs. 1 Satz 1 genannten Zwecken sowie
- 2. zu Zwecken der Strafverfolgung, wenn sie nach § 100d Abs. 6 Nr. 3 StPO verwendet werden dürfen; eine Zweckänderung ist festzustellen und zu dokumentieren.

³Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte oder
3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben,

dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich **und Daten im Sinn der Nr. 2 oder 3 sind nicht betroffen**. ⁴Vor einer Verwendung der Daten ist über deren Zulässigkeit eine richterliche Entscheidung herbeizuführen. ⁵Bei Gefahr im Verzug kann die Entscheidung auch **eine in Art. 33 Abs. 5 Sätze 1 und 2 genannte Stelle** treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. ⁶Für die richterliche Entscheidung ist Abs. 4 Satz 2 entsprechend anzuwenden.

(6) ¹Die Betroffenen sind von Maßnahmen nach Abs. 1 Satz 1 zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht offen ermittelnden Beamten oder der in Abs. 1 Satz 1 genannten Rechtsgüter geschehen kann. ²Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. ³Erfolgt die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. ⁴Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. ⁵Eine Unterrichtung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

1. überwiegende Interessen eines Betroffenen entgegenstehen oder
2. die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann.

⁶Die gerichtliche Zuständigkeit und das Verfahren richten sich im Fall des Satzes 2 nach den Regelungen der Strafprozessordnung, im Übrigen gilt Abs. 4 Satz 2 entsprechend.

(7) ¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren. ²Die durch eine Maßnahme nach Abs. 1 Satz 1 erlangten personenbezogenen Daten,

1. deren Verwendung zu den in Abs. 5 Satz 2 genannten Zwecken nicht erforderlich ist oder
2. für die ein Verwendungsverbot besteht,

sind zu sperren, wenn sie zum Zweck der Information der Betroffenen und zur gerichtlichen Überprüfung der Erhebung oder Verwendung der Daten noch benötigt werden; andernfalls sind sie zu löschen. ³Im Fall der Unterrichtung des Betroffenen sind die Daten zu löschen,

wenn der Betroffene sich nicht innerhalb eines Monats nach seiner Benachrichtigung mit Rechtsbehelf gegen die Maßnahme gewendet hat; auf diese Frist ist in der Benachrichtigung hinzuweisen. ⁴Im Fall eines Rechtsbehelfs nach Satz 2 sind die Daten nach Abschluss des Rechtsbehelfsverfahrens zu löschen.

(8) ¹Die Anordnung eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen obliegt den in Art. 33 Abs. 5 Sätze 1 bis 3 genannten Stellen. ²Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse zu Zwecken der Gefahrenabwehr oder der Strafverfolgung ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. ³Abs. 4 Satz 2 findet entsprechende Anwendung. ⁴Die Abs. 5 bis 7 gelten im Fall der Verwendung der Daten entsprechend. ⁵Aufzeichnungen aus einem solchen Einsatz sind unverzüglich nach Beendigung des Einsatzes zu löschen, soweit sie nicht zur Strafverfolgung oder Gefahrenabwehr benötigt werden.

(9) ¹Die Staatsregierung unterrichtet den Landtag jährlich über den nach Abs. 1 und, soweit richterlich überprüfungsbedürftig, nach Abs. 8 erfolgten Einsatz technischer Mittel. ²Ein vom Landtag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus.

(10) Das Brief- und das Postgeheimnis bleiben unberührt.

Art. 34a Datenerhebung und Eingriffe in den Telekommunikationsbereich

(1) ¹Die Polizei kann durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben

1. über die für eine Gefahr Verantwortlichen, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist, oder
2. über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat begehen werden oder
3. über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass
 - a) sie für Personen nach Nrn. 1 oder 2 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder weitergeben oder
 - b) die unter Nrn. 1 oder 2 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.

²Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. ³Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Datenerhebung insoweit unzulässig, es sei denn, die Maßnahme richtet sich gegen den Berufsgeheimnisträger selbst. ⁴**Wird erkennbar, dass dem Kernbereich privater Lebensgestaltung zuzurechnende Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Datenerhebung insoweit unzulässig.**

(2) ¹Die Polizei kann unter den Voraussetzungen des Abs. 1 auch technische Mittel einsetzen, um

1. zur Vorbereitung einer Maßnahme nach Abs. 1 spezifische Kennungen, insbesondere die Geräte- und Kartenummer von Mobilfunkendgeräten, sowie
2. den Standort eines Mobilfunkendgerätes zu ermitteln.

²Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. ³Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

(3) ¹Die Polizei kann bei Gefahr für Leben oder Gesundheit einer Person

1. durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten über diese Person erheben oder
2. technische Mittel einsetzen, um den Standort eines von ihr mitgeführten Mobilfunkendgerätes zu ermitteln.

²Weitergehende Maßnahmen nach Art. 34b Abs. 1 und 2 bleiben unberührt.

(4) ¹Die Polizei kann unter den Voraussetzungen des Abs. 1 Kommunikationsverbindungen der dort genannten Personen durch den Einsatz technischer Mittel unterbrechen oder verhindern. ²Kommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person durch andere Mittel nicht abgewehrt werden kann.

Art. 34c **Verfahrensregelungen, Verwendungsverbote** **Zweckbindung, Benachrichtigung und Löschung**

(1) Für Maßnahmen nach Art. 34a und Art. 34b gilt Art. 34 Abs. 4 Sätze 1 und 2 entsprechend; bei Gefahr im Verzug sind die in Art. 33 Abs. 5 Sätze 1 und 2 genannten **Stellen** anordnungsbefugt.

(2) ¹Soweit eine Maßnahme nach Art. 34a Abs. 3 ausschließlich dazu dient, den Aufenthaltsort einer dort genannten Person zu ermitteln, darf sie auch durch die Dienststellenleiter der in Art. 4 Abs. 2 Satz 1 Nrn. 1 und 2 POG genannten Dienststellen oder des Landeskriminalamts angeordnet werden. ²Diese können die Anordnungsbefugnis auf besonders Beauftragte übertragen.

(3) ¹Anordnungen nach den Abs. 1 und 2 sind schriftlich zu erlassen und zu begründen. ²Die Anordnung muss Namen und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sowie die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder des Endgerätes enthalten; im Falle einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation. ³In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. ⁴Die Anordnung ist auf den nachfolgend genannten Zeitraum zu befristen:

1. im Fall des Art. 34a Abs. 4 Satz 1 höchstens zwei Wochen,
2. im Fall des Art. 34a Abs. 4 Satz 2 höchstens drei Tage,
3. in allen anderen Fällen höchstens ein Monat.

⁵Eine Verlängerung um jeweils nicht mehr als den in Satz 4 genannten Zeitraum ist möglich, soweit die Voraussetzungen fortbestehen. ⁶Bestehen die in Art. 34a und 34b bezeichneten Voraussetzungen nicht fort, ist die Maßnahme unverzüglich zu beenden; die Beendigung ist dem Richter mitzuteilen.

(4) ¹Die durch eine Maßnahme nach Art. 34a und 34b erlangten personenbezogenen Daten sind besonders zu kennzeichnen.

²Sie dürfen nur verwendet werden

1. zu den Zwecken, zu denen sie erhoben wurden, sowie
2. zu Zwecken der Strafverfolgung, wenn sie zur Verfolgung von Straftaten im Sinn des § 100a **Abs. 2** StPO benötigt werden; eine Zweckänderung ist festzustellen und zu dokumentieren.

³Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte oder
3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben,

dürfen nicht verwendet werden. ⁴Dies gilt nicht, wenn ihre Verwendung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich ist **und Daten im Sinn der Nr. 2 oder 3 nicht betroffen sind**. ⁵In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich nachzuholen; Art. 34 Abs. 4 Satz 2 findet entsprechende Anwendung.

(5) ¹Von Maßnahmen nach Art. 34a Abs. 1, 2 und 4 sowie Art. 34b sind

1. die Personen zu unterrichten, gegen die die Maßnahme gerichtet war, sowie

2. diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme erhoben und zu den Zwecken des Abs. 4 Satz 2 verwendet wurden.

²Die Unterrichtung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht offen ermittelnden Beamten oder der in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 genannten Rechtsgüter geschehen kann. ³Art. 34 Abs. 6 Sätze 2 bis 6 gelten entsprechend.

(6) ¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren.

²Die durch eine Maßnahme nach Art. 34a oder 34b erlangten personenbezogenen Daten,

1. deren Verwendung zu den in Abs. 4 Satz 2 genannten Zwecken nicht erforderlich ist oder
2. für die ein Verwendungsverbot besteht,

sind zu sperren, wenn sie zum Zweck der Information der Betroffenen und zur gerichtlichen Überprüfung der Erhebung oder Verwendung der Daten noch benötigt werden; andernfalls sind sie zu löschen. ³Art. 34 Abs. 7 Sätze 3 und 4 gelten entsprechend.

Art. 34d Verdeckter Zugriff auf informationstechnische Systeme

(1) ¹Die Polizei kann mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben von Personen,

- 1. die für eine Gefahr verantwortlich sind, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist, oder**
- 2. wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat nach Art. 30 Abs. 5 Satz 1 Nrn. 1, 2 (ohne § 129 Abs. 1 in Verbindung mit Abs. 4 StGB) bis 9 begehen werden, oder**
- 3. soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass**
 - a) sie für Personen nach Nr. 1 oder 2 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder entgegengenommen haben, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder solche Mitteilungen weitergeben oder weitergegeben haben oder**
 - b) die unter Nr. 1 oder 2 genannten Personen ihre informationstechnischen Systeme benutzen oder benutzt haben.**

²Daten dürfen unter den Voraussetzungen des Satzes 1 auch gelöscht oder verändert werden, andere als Zugangsdaten jedoch nur, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und eine Erhebung zur Abwehr der Gefahr nicht ausreichend wäre. ³Eine Maßnahme nach den Sätzen 1 und 2 darf nur durchgeführt werden, wenn die Erfüllung einer polizeilichen

Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. ⁴Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Maßnahme insoweit unzulässig, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst. ⁵Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, hat die Polizei durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. ⁶Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Maßnahme insoweit unzulässig. ⁷Maßnahmen nach den Sätzen 1 und 2 sind zu dokumentieren.

(2) ¹Die Polizei kann unter den Voraussetzungen des Abs. 1 auch technische Mittel einsetzen, um

- 1. zur Vorbereitung einer Maßnahme nach Abs. 1 spezifische Kennungen sowie**
- 2. den Standort eines informationstechnischen Systems zu ermitteln.**

²Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. ³Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

(3) ¹Art. 34 Abs. 4 Sätze 1 und 2 gelten entsprechend. ²Bei Gefahr im Verzug sind bei Maßnahmen nach Abs. 2 und bei der Erhebung von Zugangsdaten auch die in Art. 33 Abs. 5 Satz 2 genannten Stellen anordnungsbefugt. ³Die Anordnung von Maßnahmen nach Abs. 1 und 2 ist schriftlich zu erlassen und zu begründen. ⁴Die Anordnung muss, soweit möglich, Namen und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sowie die Bezeichnung des informationstechnischen Systems, auf das zugegriffen werden soll, enthalten. ⁵In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. ⁶Die Anordnung ist auf höchstens drei Monate zu befristen. ⁷Eine Verlängerung um jeweils nicht mehr als einen Monat ist möglich, soweit die Voraussetzungen fortbestehen. ⁸Bestehen die in den Abs. 1 und 2 bezeichneten Voraussetzungen nicht fort, ist die Maßnahme unverzüglich zu beenden; die Beendigung ist dem Richter mitzuteilen.

(4) ¹Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten

- 1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind oder**
- 2. Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder**
- 3. einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind,**

sind diese unverzüglich zu löschen oder dem für die Anordnung nach Abs. 1 zuständigen Richter zur Entscheidung über ihre weitere Verwendung vorzulegen. ²Bei Gefahr im Verzug kann die Entscheidung auch eine in Art. 33 Abs. 5 Satz 1 genannte Stelle treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. ³Die Löschung ist zu dokumentieren.

(5) ¹Die durch eine Maßnahme nach den Abs. 1 und 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. ²Sie dürfen nur verwendet werden

- 1. zu den Zwecken, zu denen sie erhoben wurden, sowie**
- 2. zu Zwecken der Strafverfolgung hinsichtlich solcher Straftaten, zu deren Aufklärung eine solche Maßnahme nach der Strafprozessordnung hätte angeordnet werden dürfen; eine Zweckänderung ist festzustellen und zu dokumentieren.**

³Daten, bei denen sich nach der Auswertung herausstellt, dass

- 1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder**
- 2. sie Inhalte betreffen, über die das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder**
- 3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben,**

dürfen nicht verwendet werden. ⁴Dies gilt nicht, wenn ihre Verwendung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und Daten im Sinn der Nr. 2 oder 3 nicht betroffen sind. ⁵In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich nachzuholen; Art. 34 Abs. 4 Satz 2 findet entsprechende Anwendung.

(6) ¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren. ²Die durch eine Maßnahme nach den Abs. 1 und 2 erlangten personenbezogenen Daten,

- 1. deren Verwendung zu den in Abs. 5 Satz 2 genannten Zwecken nicht erforderlich ist, oder**
- 2. für die ein Verwendungsverbot besteht,**

sind zu sperren, wenn sie zum Zweck der Information der Betroffenen und zur gerichtlichen Überprüfung der Erhebung oder Verwendung der Daten noch benötigt werden; andernfalls sind sie zu löschen. ³Art. 34 Abs. 7 Sätze 3 und 4 gelten entsprechend.

(7) ¹Von Maßnahmen nach den Abs. 1 und 2 sind

- 1. die Personen zu unterrichten, gegen die die Maßnahme gerichtet war, sowie**
- 2. diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme erhoben, gelöscht oder verändert und zu den Zwecken des Abs. 5 Satz 2 verwendet wurden.**

²Die Unterrichtung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht offen ermittelnden Beamten oder der in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Rechtsgüter geschehen kann. ³Art. 34 Abs. 6 Sätze 2 bis 6 gelten entsprechend.

(8) ¹Die Staatsregierung unterrichtet den Landtag jährlich über die erfolgte Erhebung von Daten nach Abs. 1 Satz 1 mit Ausnahme von Zugangsdaten sowie die Löschung und die Veränderung solcher Daten nach Abs. 1 Satz 2. ²Art. 34 Abs. 9 Satz 2 gilt entsprechend.

Art. 34e **Notwendige Begleitmaßnahmen**

¹Zur Durchführung von Maßnahmen nach Art. 34 Abs. 1, Art. 34a sowie 34d Abs. 1 und 2 kann die Polizei verdeckt Sachen durchsuchen sowie die Wohnung des Betroffenen ohne Einwilligung betreten und durchsuchen. ²Für die Anordnung der Begleitmaßnahmen und die Unterrichtung der Betroffenen finden die für die Maßnahme nach Art. 34 Abs. 1, Art. 34a sowie 34d Abs. 1 und 2 jeweils geltenden Vorschriften entsprechende Anwendung.

II. Die Beschwerdeführer

Die vier Beschwerdeführer sind derzeit Abgeordnete des Bayerischen Landtags.

Alle vier sind Mitglieder des Arbeitskreises für Verfassungs-, Rechts- und Parlamentsfragen der SPD-Fraktion im Bayerischen Landtag. Die Beschwerdeführer sind ferner Mitglieder im Ausschuss für Verfassungs-, Rechts- und Parlamentsfragen des Bayerischen Landtags, dessen Vorsitzender der Beschwerdeführer Ziff. 4 ist. Sie sind weiter Mitglieder folgender Kommissionen und Landtagsausschüsse:

Die Beschwerdeführerin Ziff. 1 ist auch stellvertretende Vorsitzende der Datenschutzkommission, die beim Bayerischen Landtag gebildet wird. Sie gehört ferner dem Ausschuss für Eingaben und Beschwerden des Bayerischen Landtags an.

Der Beschwerdeführer Ziff. 2 gehört neben dem Ausschuss für Verfassungs-, Rechts- und Parlamentsfragen auch dem Ausschuss für Kommunale Fragen und Innere Sicherheit des Bayerischen Landtags an.

Die Beschwerdeführerin Ziff. 3 ist nicht nur Mitglied im Ausschuss für Verfassungs-, Rechts- und Parlamentsfragen; sie ist auch Mitglied im Ausschuss für Hochschule, Forschung und Kultur des Bayerischen Landtags.

Der Beschwerdeführer Ziff. 4 ist nicht nur Vorsitzender des Ausschusses für Verfassungs-, Rechts- und Parlamentsfragen, sondern auch rechtspolitischer Sprecher der SPD-Landtagsfraktion.

Die Beschwerdeführerin Ziff. 1 wird dem Bayrischen Landtag in dessen 16. Legislaturperiode nicht mehr angehören, da sie nicht mehr kandidieren wird.

Für sie und für alle Beschwerdeführer, also auch für die Beschwerdeführer Ziff. 2 – 4, gilt – für den Fall des Verlustes ihres Abgeordnetenstatus –, dass alle ausnahmslos weiterhin politisch aktiv bleiben werden. Auch an ehemalige Abgeordnete wenden sich Bürger. Dies ist im vorliegenden Fall erst recht wegen der von allen Beschwerdeführern in ihrer bisherigen Abgeordnetentätigkeit gesetzten Schwerpunkte zu erwarten, zumal die Beschwerdeführer sich weiter politisch engagieren und damit weiterhin in der Öffentlichkeit in Erscheinung treten. Erfahrungsgemäß muss also damit gerechnet werden, dass sich Bürger bei den Beschwerdeführern weiterhin über Maßnahmen und Verhalten von Polizei und Verfassungsschutz in Bayern beschweren und/oder in diesen Angelegenheiten um Rat fragen. Auch in diesem Kontext ist E-Mail- und Telefonverkehr zu erwarten.

Die vier Beschwerdeführer haben folgende Berufe:

Die Beschwerdeführerin Ziff. 1 ist gelernte Erzieherin.

Der Beschwerdeführer Ziff. 2 ist von Beruf Datenverarbeitungskaufmann. Er ist Selbständiger und im Handelsregister als Geschäftsführer einer Werbe- und Internetagentur eingetragen.

Die Beschwerdeführerin Ziff. 3 ist niedergelassene Rechtsanwältin.

Der Beschwerdeführer Ziff. 4 ist von Beruf Rechtsanwalt und übt diesen Beruf neben seinem Mandat auch aus.

Benutzung informationstechnischer Systeme:

Die Beschwerdeführerin Ziff. 1 nutzt sowohl in ihrer Eigenschaft als Abgeordnete als auch privat PC und Handy.

Der Beschwerdeführer Ziff. 2 nutzt sowohl dienstlich als auch privat PC, Notebook und Handy.

Die Beschwerdeführerin Ziff. 3 nutzt beruflich und privat PC, Notebook und Handy.

Der Beschwerdeführer Ziff. 4 nutzt sowohl beruflich als auch privat PC und Handy.

Kontakte zu Organisationen, die vom Verfassungsschutz observiert werden:

Die politischen Kontakte zu Organisationen oder zu Personen in Organisationen, die Objekte der Beobachtung durch das Landesamt für Verfassungsschutz in Bayern sind, ergeben sich aus den politischen Inhalten, mit denen die Beschwerdeführer befasst sind. Die vier Beschwerdeführer haben mit fast allen aktuellen Fragen zu tun, die im Zusammenhang mit den Freiheits- und Grundrechten stehen. Es kann daher vorkommen und ist bereits

vorgekommen, dass die Beschwerdeführer als Beauftragte oder Kontaktpersonen (z. B. der BayernSPD oder der SPD-Landtagsfraktion) mit Bündnissen (z. B. "Rettet die Grundrechte - Gegen den Notstand der Republik") zu tun haben, in die auch Organisationen, die vom Verfassungsschutz beobachtet werden, Mitglieder entsenden oder einen Aufruf (wie: "Wir brauchen unsere Versammlungsfreiheit, wir lassen sie uns nicht nehmen!") unterschreiben, den auch Organisationen unterzeichnen, die vom Verfassungsschutz beobachtet werden. Beispielfhaft wird den Beschwerdeführer Ziff. 2 verwiesen, der in politischem Kontakt zu Organisationen bzw. zu Mitgliedern in Organisationen steht, die vom Verfassungsschutz in Bayern beobachtet werden. Zu diesen Kontakten gehört beispielsweise die Partei DIE LINKE, DKP, VVN-BdA, Arbeiterbund für den Wiederaufbau der KPD (AB) etc. Es ist zwar nicht bekannt, dass der Beschwerdeführer Ziff. 2 jemals namentlich in einem Bericht des Verfassungsschutzes erwähnt worden ist. In den Verfassungsschutzinformationen für das 1. Halbjahr 2008 des Bayerischen Staatsministerium des Innern wird als ein Agitationsfeld der autonomen Szene in Bayern allerdings die Auseinandersetzung mit dem Bayerischen Versammlungsgesetz aufgeführt und es wird auf eine Demonstration am 31.05.2008 in München hingewiesen, an der der Beschwerdeführer Ziff. 2 teilgenommen und mit in vorderster Reihe den Demonstrationzug angeführt hat.

Der entsprechende Auszug aus den Verfassungsschutzinformationen Bayern für das 1. Halbjahr 2008 des Bayerischen Staatsministerium des Innern und ebenfalls ein Bericht der Süddeutschen Zeitung vom 02.06.2008 über die Demonstration am 31.05.2008 werden der Verfassungsbeschwerde als Anhänge 5 und 6 beigelegt.

Als Mitglieder des SPD-Arbeitskreises und des Landtagsausschusses, die sich beide mit Verfassungs-, Rechts- und Parlamentsfragen befassen, und auch allgemein in ihrer Eigenschaft als Abgeordnete sind die Beschwerdeführer Ziff. 1 – 4 zudem mit Eingaben befasst, in denen sich Bürger über Maßnahmen und Verhalten von Polizei und Verfassungsschutz in Bayern beschweren. Bei dem Beschwerdeführer Ziff. 4 kommt dies aufgrund seiner Eigenschaft als Vorsitzender des Ausschusses für Verfassungs-, Rechts- und Parlamentsfragen und als rechtspolitischer Sprecher der SPD-Landtagsfraktion besonders häufig vor.

B. Zulässigkeit

Die Verfassungsbeschwerden sind zulässig. Die Beschwerdeführer sind beschwerdefähig (I.) und beschwerdebefugt (II.). Sie werden durch die angegriffenen gesetzlichen Regelungen unmittelbar (V.), gegenwärtig (IV.) und selbst (III.) in ihren Grundrechten verletzt. Die angegriffenen Regelungen sind am 1. August 2008 in Kraft getreten.

I. Beschwerdefähigkeit

Die Beschwerdeführer zu 1) bis 4) sind als natürliche Personen Träger der gerügten Grundrechte und damit beschwerdefähig gemäß § 90 Abs. 1 BVerfGG.

II. Beschwerdebefugnis bezüglich der Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 13 GG und Art. 1 Abs. 1 GG

Die Beschwerdeführer sind auch beschwerdebefugt. Es besteht die Möglichkeit einer Verletzung von Grundrechten der Beschwerdeführer durch die öffentliche Gewalt. Von der Grundrechtsverletzung geht eine gegenwärtige, eigene und unmittelbare Beschwerde für die Beschwerdeführer aus.

Die Beschwerdeführer machen mit ihrer Verfassungsbeschwerde eine Verletzung durch die öffentliche Gewalt in ihrem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, aus Art. 13 GG und aus Art. 1 Abs. 1 GG in seiner Konkretisierung als Schutz des Kernbereichs privater Lebensgestaltung geltend. Sie sind damit im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt, da eine Grundrechtsverletzung der Beschwerdeführer durch die angegriffenen Gesetze möglich erscheint. Alle Beschwerdeführer nutzen regelmäßig und dauerhaft verschiedene von den gesetzlichen Regelungen erfasste informationstechnische Systeme wie PC, Notebook und auch Handy. Diese nutzen sie sowohl dienstlich als auch privat außerhalb und innerhalb ihrer privaten Wohnungen. Durch ihre beruflichen und politischen Tätigkeiten haben sie zudem häufig Kontakte zu Personen, gegen die die Polizei und auch der Verfassungsschutz verdeckt Daten erheben. Der Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist betroffen, da die angegriffenen Normen Befugnisse des Verfassungsschutzes sowie der Polizei regeln, die in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen. Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprä-

gung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der Grundrechtsschutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten (Urteil vom 27.02.2008, Rn. 205). In das Grundrecht aus Art. 13 GG wird durch die in den Gesetzen vorgesehenen Begleitmaßnahmen zur verdeckten Datenerhebung durch heimliches Betreten und Durchsuchen eingegriffen. Die in Art. 13 Abs. 1 GG gewährleistete Garantie der Unverletzlichkeit der Wohnung verbürgt dem Einzelnen mit Blick auf seine Menschenwürde sowie im Interesse der Entfaltung seiner Persönlichkeit einen elementaren Lebensraum, in den nur unter den besonderen Voraussetzungen von Art. 13 Abs. 2 bis 7 GG eingegriffen werden darf. Diese sehen ein heimliches Betreten und Durchsuchen nicht vor. Die in den angegriffenen Regelungen getroffenen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen verletzen zudem den durch Art. 1 Abs. 1 GG garantierten absoluten Schutz dieses Bereichs.

III. eigene Beschwer

Die Beschwerdeführer sind durch die angegriffenen Neuregelungen selbst betroffen. Für die eigene Betroffenheit genügt es,

„wenn ein Gesetz die Normadressaten bereits gegenwärtig zu später nicht mehr korrigierbaren Entscheidungen zwingt, oder schon jetzt zu Dispositionen veranlasst, die sie nach dem späteren Gesetzesvollzug nicht mehr nachholen können“
(BVerfGE 65, 1, 37; 75, 78, 95).

Ein entsprechender Fall liegt hier vor.

Für die Beschwerdeführer müssen sich aus den angegriffenen Regelungen Rechtswirkungen ergeben, die die Rechtspositionen der Beschwerdeführer zu ihrem Nachteil verändern (BVerfGE 60, 360, 371). Dies ist bei den angegriffenen Regelungen gegeben. Seit dem Inkrafttreten der angegriffenen Regelungen müssen die Beschwerdeführer befürchten, dass sie und die anderen Beteiligten ihrer Kommunikationsvorgänge ausgespäht, registriert, identifiziert und geortet werden und dass die dabei anfallenden Daten von staatlicher Seite ausgewertet und benutzt werden. Eine eigene Betroffenheit besteht auch hinsichtlich des Eingriffs in das Grundrecht aus Art. 13 GG durch die in den angegriffenen Regelungen vorgesehenen heimlichen Begleitmaßnahmen.

Sollte das Gericht weiteren Sachvortrag zur eigenen Beschwer der jeweiligen Beschwerdeführer für notwendig erachten, so bitte ich um einen entsprechenden Hinweis.

IV. gegenwärtige Beschwer

Die Beschwerdeführer von 1) bis 4) sind auch gegenwärtig durch die angegriffenen Vorschriften betroffen. Die angegriffenen Neuregelungen der verdeckten Ermittlungsmaßnahmen sind für beide Gesetze am 1. August 2008 in Kraft getreten. Seitdem werden diese verdeckten Maßnahmen durch Polizei und Verfassungsschutz durchgeführt bzw. könnten angewendet werden. Aufgrund der eindeutigen Regelung des Gesetzgebers ist die Betroffenheit nach Zeitpunkt und Auswirkung genau bestimmt, der Eingriff somit nicht lediglich „virtuell“. Für die Beschwerdeführer, die Nutzer informationstechnischer Systeme sind, ist zudem nicht erkennbar, welche Dienststellen von Polizei und Verfassungsschutz bereits derzeit von den neugeregelten Befugnissen Gebrauch machen.

V. unmittelbare Betroffenheit

Den Beschwerdeführern zu 1) bis 4) steht die Verfassungsbeschwerde unmittelbar gegen die von ihnen angegriffenen gesetzlichen Regelungen zu. Grundsätzlich ist Voraussetzung einer unmittelbaren Rechtsbeeinträchtigung, dass ein Akt der Rechtsanwendung zwischen die abstrakte gesetzliche Regelung und die Rechtssphäre der Beschwerdeführer tritt. Ein Beschwerdeführer, der das Gesetz selbst angreift, muss deshalb geltend machen können, gerade durch die angegriffene Rechtsnorm und nicht erst durch ihren Vollzug in seinen Rechten verletzt zu sein (vgl. BVerfGE 16, 147, 158 f.; 68, 287, 300). Setzt das Gesetz zu seiner Durchführung rechtsnotwendig oder auch nur nach der tatsächlichen staatlichen Praxis einen besonderen, vom Willen der vollziehenden Stelle beeinflussten Vollziehungsakt voraus, muss der Beschwerdeführer grundsätzlich zunächst diesen Akt angreifen und den gegen ihn eröffneten Rechtsweg erschöpfen, bevor er die Verfassungsbeschwerde erhebt (vgl. BVerfGE 1, 97, 102 f.). Die Verfassungsbeschwerde kann sich jedoch ausnahmsweise unmittelbar gegen ein vollziehungsbedürftiges Gesetz richten, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil es ihn nicht gibt (vgl. BVerfGE 67, 157, 170) oder weil er keine Kenntnis von der Maßnahme erlangt (vgl. BVerfGE 100, 313, 354). In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zu wie in jenen Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz selbst eintritt (vgl. BVerfGE 30, 1, 16 f.; 67, 157, 169 f.; 100, 313, 354). Bei den neugeregelten, angegriffenen Befugnisnormen handelt es sich durchweg um verdeckte Maßnahmen, von denen der Betroffene weder vor noch während der Durchführung etwas erfährt, so dass fachgerichtlicher Rechtsschutz insoweit nicht in Anspruch

genommen werden kann. Der Umstand, dass zum Teil nachträgliche Benachrichtigungen der Beteiligten von den getroffenen Maßnahmen vorgesehen sind, steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen. Ihre Erhebung unmittelbar gegen das Gesetz ist nicht nur dann zulässig, wenn nach der gesetzlichen Regelung die Betroffenen zu keinem Zeitpunkt Kenntnis von einem heimlichen Vollzugsakt erhalten, sondern darüber hinaus auch dann, wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber auf Grund von Ausnahmetatbeständen auch langfristig abgesehen werden kann. Unter diesen Umständen ist ebenfalls nicht gewährleistet, dass der Betroffene effektiven fachgerichtlichen Rechtsschutz erlangen kann. Solche Ausnahmetatbestände enthalten die angegriffenen Regelungen in Art. 34d Abs. 7 PAG und Art. 6b Abs. 4 Satz 5 BayVSG, nach denen die Benachrichtigung erst erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, bestimmter Rechtsgüter und der eingesetzten nicht offen ermittelnden Beamten, geschehen kann bzw. ganz unterbleiben kann. Daraus ergibt sich, dass die Voraussetzung der Unmittelbarkeit der Beschwer gegeben ist.

VI. Frist

Die Verfassungsbeschwerde ist fristgemäß erhoben. Da sich die Verfassungsbeschwerde gegen ein Gesetz richtet, gilt hier die einjährige Frist des § 93 Abs. 3 BVerfGG. Diese Frist beginnt mit dem Inkrafttreten des Gesetzes und ist hier offensichtlich gewahrt.

VII. Subsidiarität

Die Beschwerdeführer können nicht darauf verwiesen werden, vorab den ordentlichen Rechtsweg zu beschreiten.

Die Verfassungsbeschwerde ist von allgemeiner Bedeutung gemäß § 90 Abs. 2 Satz 2 BVerfGG. Die angegriffenen Regelungen betreffen die bayerischen Bürger in ihrer Gesamtheit. Nur eine verfassungsgerichtliche Entscheidung kann die erforderliche Klarheit über die Vielzahl der durch das Gesetz herbeigeführten Grundrechtseingriffe treffen (vgl. BVerfG NJW 93, 2367). Die Voraussetzungen des § 93a BVerfGG für die Zulässigkeit der Verfassungsbeschwerde liegen somit vor.

C. Begründetheit

Die Verfassungsbeschwerde ist begründet,

- weil die Online-Durchsuchung gem. den Art. 34d PAG und Art. 6e BayVSG verfassungswidrig sind (I.),
- weil die Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG verfassungswidrig sind (II.) und
- weil die den Kernbereich privater Lebensgestaltung schützenden Regelungen verfassungswidrig sind (III.).

I. Verfassungswidrigkeit der Online-Durchsuchung in Art. 34d PAG und in Art. 6e BayVSG

1) Die verfassungsrechtlichen Maßstäbe für einen verdeckten Zugriff mit technischen Mitteln auf informationstechnische Systeme

Die in Art. 34d PAG (dazu nachstehend **2**)) und in Art. 6e BayVSG (dazu nachstehend **3**)) enthaltenen Befugnisse zur verdeckten Online-Datenerhebung sind am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen, wie es das BVerfG in seinem Urteil vom 27.02.2008 aus dem allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG hergeleitet hat (BVerfG, Urteil vom 27.02.2008, Rn. 167, 201 – 206). Das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt informationstechnische Systeme vor staatlichen Eingriffen, soweit der Schutz nicht durch andere Grundrechte gewährleistet ist, insbesondere das Fernmeldegeheimnis (Art. 10 GG) oder das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) sowie das Recht auf informationelle Selbstbestimmung (BVerfG vom 27.02.2008, Rn.167). Informationstechnische Systeme sind nach der Definition des Bundesverfassungsgerichts Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden.“ (BVerfG vom 27.02.2008, Rn. 202 f.). Auch Mobiltelefone und elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können, fallen darunter.

Eingriffshandlungen in den Schutzbereich des Grundrechts sind alle Zugriffe auf persönliche Daten, die sich auf dem informationstechnischen System befinden bzw. für dessen Betrieb erforderlich sind. Das betrifft die Zugangsdaten, insbesondere die Erhebung von Benutzerkennungen und Passwörtern, ebenso wie die Erhebung von bereits gespeicherten Daten. Das Erheben von gespeicherten Daten umfasst die bloße Sichtung, aber auch das Kopieren von Datenbeständen unter Belassung der Datenbestände auf dem Zielsystem und jedwede Datenveränderung.

Verfassungsrechtlich ist die heimliche Infiltration eines informationstechnischen Systems nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Solche sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren (BVerfG, Urteil vom 27.02.2008, Rn. 247). Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen (BVerfG, Urteil vom 27.02.2008, Rn. 249 ff.).

Grundsätzlich steht die heimliche Online-Durchsuchung unter dem Vorbehalt der richterlichen Anordnung (BVerfG, Urteil vom 27.02.2008, Rn. 257 ff.). Das ermächtigende Gesetz muss außerdem Vorkehrungen enthalten, um den Kernbereich privater Lebensführung zu schützen (BVerfG, Urteil vom 27.02.2008, Rn. 267 ff.).

Darüber hinaus sind die vom Bundesverfassungsgericht bereits früher für Maßnahmen der verdeckten Datenerhebung aufgestellten Maßstäbe, insbesondere in den Entscheidungen vom 03.03.2004 zur akustischen Wohnraumüberwachung, Az. 1 BvR 2378/98 u. 1 BvR 1084/99, und zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz, Az. 1 BvF 3/92, sowie im Urteil vom 27.07.2005 zum niedersächsischen Sicherheits- und Ordnungsgesetz, Az. 1 BvR 668/04, zu beachten.

2) Die Verfassungswidrigkeit des verdeckten Zugriffs auf informationstechnische Systeme nach Art. 34d PAG

Gemessen an den Maßstäben des Urteils vom 27.02.2008 sind in Art. 34d PAG folgende Regelungen verfassungswidrig:

- Art. 34d Abs. 1 Satz 1 Nr. 2 PAG (vorbeugende Straftatenbekämpfung, Straftatenverhütung, dazu nachstehend unter **(a)**)
- Art. 34d Abs. 1 Satz 2 (Datenänderung und Datenlöschung, dazu nachstehend unter **(c)**)
- Art. 34d Abs. 3 Satz 1 und 2 (fehlender eigenständiger Richtervorbehalt, dazu nachstehend unter **(d)**)
- Art. 34d Abs. 5 Satz 2 Nr. 2 (Zweckänderung, Zufallsfundverwertung, dazu nachstehend unter **(e)**)
- Art. 34d Abs. 1 Satz 5 und 6 (Unzureichender Kernbereichsschutz dazu unter Abschnitt III. 3))

(a) Die Verfassungswidrigkeit der in Art. 34d Abs. 1 S. 1 Nr. 2 PAG formulierten Eingriffsschwelle

Während nach Art. 34d Abs. 1 Satz 1 Nr. 1 PAG für einen Eingriff in ein informationstechnisches System eine konkrete Gefahr für die aufgezählten Rechtsgüter vorliegen muss, kann sich der Eingriff nach Satz 1 Nr. 2 auch bereits gegen potentielle Straftäter richten, wenn bestimmte Tatsachen vorliegen, die die begründete Annahme rechtfertigen, dass diese eine schwerwiegende Straftat nach Art. 30 Abs. 5 Satz 1 Nr. 1 bis 9 PAG begehen werden. Damit wird für den konkreten Einzelfall ein Eingriff zugelassen, der nicht der Abwehr einer konkreten Gefahr dient, auch wenn dies in der Gesetzesbegründung anders dargestellt wird. Die Gesetzesbegründung geht zwar auch bzgl. Art. 34 d Abs. 1 Satz 1 Nr. 2 PAG davon aus, dass eine konkrete Gefahr vorliegen muss (Entwurfsbegründung S. 7, Drs. 15/10345), kann aber auf diese Weise den alternativ zu Nr. 1 formulierten Eingriffstatbestand in seinem Mehrwert zu Nr. 1 bzw. dessen Anwendungsbereich im Unterschied zu Nr. 1 nicht erklären. Unterscheidet man jedoch den Anwendungsbereich von Art. 34d Abs. 1 Satz 1 Nr. 2 PAG von dem des Art. 34d Abs. 1 Satz 1 Nr. 1 PAG wie es der Wortlaut nahe legt, wird die in Nr. 2 formulierte Eingriffsschwelle von der konkreten Gefahr weg in das Gefahrenvorfeld gelegt. Der in Nr. 2 alternativ zu Nr. 1 formulierte Eingriffstatbestand verlangt das Vorliegen einer konkreten Gefahr nicht und erfasst damit das Gefahrenvorfeld. In seiner Formulierung

entspricht er zudem anderen Normen im III. Abschnitt des PAG, die nach einer in der klassischen Gefahr-Störer-Dogmatik verbleibenden Nr. 1 eine offener formulierte Nr. 2 enthalten, die auch das Gefahrenvorfeld erfasst (z.B. Art. 33 Abs. 3 PAG). Damit aber unterschreitet die in Art. 34d Abs. 1 Satz 1 Nr. 2 PAG vorgesehene Eingriffsschwelle für den verdeckten Zugriff auf informationstechnische Systeme, die Eingriffsschwelle, die im Urteil vom 27.02.2008 vorgegebenen wurde und ist deshalb verfassungswidrig. Das Urteil vom 27.02.2008 fordert eine Prognose, die auf das Entstehen einer konkreten Gefahr bezogen ist, d.h. auf eine im Einzelfall bestehende hinreichende Wahrscheinlichkeit, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden verursacht wird.

„[251]... Die Tatsachen müssen 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.

[252] Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.

[253] Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur ein durch relativ diffuse Anhaltspunkte für mögliche Gefahren gekennzeichnetes Geschehen bekannt ist. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. zur Straftatenverhütung BVerfGE 110, 33, 59 = NJW 2004, 2213).“

Das Gericht formuliert demnach eine Eingriffsschwelle, die dadurch gekennzeichnet ist, dass eine absehbare konkrete Gefahr für die Schutzgüter der Norm existiert und die Identität der beteiligten Personen bekannt ist. Damit wird die zulässige Eingriffsschwelle für einen Eingriff in ein informationstechnisches System deutlich abgegrenzt von einer Eingriffsschwelle wie sie bei Eingriffen zur Straftatenverhütung im Gefahrenvorfeld vorliegt.

Art. 34d Abs. 1 Satz 1 Nr. 2 PAG regelt demgegenüber – auch nach der Gesetzesbegründung – eine präventive Maßnahme und keine repressive polizeiliche Maßnahme, bei der bereits ein strafrechtlicher Anfangsverdacht nach § 152 Abs. 2 StPO besteht. Hieraus folgend fragt es sich, welchen Anwendungsbereich Art. 34d Abs. 1 Satz 1 Nr. 2 PAG hat. Nach seinem Wortlaut und der gewählten Regelungssystematik muss Art. 34d Abs. 1 Satz 1 Nr. 2 PAG so verstanden werden, dass er bei personenbezogenen konkreten Verdachtslagen in Bezug auf die im Einzelnen näher bezeichneten drohenden Straftaten auch zum Eingriff im Gefahrenvorfeld berechtigt und damit die im Urteil vom 27.02.2008 gezogenen verfassungsrechtlichen Grenzen überschreitet. Die Regelung in Art. 34d Abs. 1 Satz 1 Nr. 2 PAG lässt bereits konkrete Vorbereitungshandlungen und gegebenenfalls weitere bestimmte Tatsachen als Verdachtsgrundlage für den Eingriff in ein informationstechnisches System zu. Sie verlangt keine Anhaltspunkte für einen Schadenseintritt bezogen auf die konkreten Schutzgüter der Norm. Es soll nur bereits ein (personenbezogener) Verdacht bezüglich einer künftigen Straftatenbegehung bestehen, der sich gegen bestimmte Personen richtet. Damit ist eine Eingriffsschwelle formuliert, die dem Bereich der Straftatenverhütung bzw. der Straftatenvorbeugung zuzurechnen ist. In der polizeirechtlichen Dogmatik besteht insoweit Einigkeit darüber, dass die präventive Mitwirkung der Polizei zur Straftatenverhütung die Eingriffsschwelle für polizeiliches Handeln vorverlagert und einen größeren zeitlichen Abstand zum prognostizierten Geschehen hat als es bei einer absehbaren konkreten Gefahr der Fall ist.

Für das Verständnis der Verhütung von Straftaten ist es wichtig, zu konstatieren,

„...dass die Verhinderung unmittelbar bevorstehender Straftaten, die unter die Abwehr konkreter Gefahren fällt, damit nicht gemeint und auch nicht darin eingeschlossen ist. ...“ (M. Albers, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001, S. 123f).

Die präventive Verhütung von Straftaten ist daher eine Verhütung der durch Straftaten entstehenden Gefahren. Sie zielt im Gefahrenvorfeld darauf ab, dass es nicht zu Straftaten kommt. Insgesamt werden damit Maßnahmen bezeichnet, die in einen konkreten Geschehensablauf eingreifen oder die Entstehungsbedingungen und Ursachenketten beeinflussen, so dass der Eintritt einer befürchteten Situation schon im Vorfeld verhütet wird. Agiert die Polizei in diesem Handlungskomplex, steht ihr das Mittel des verdeckten Zugriffs auf informationstechnische Systeme nach der im Urteil vom 27.02.2008 formulierten

Eingriffsschwelle nicht zu. Das vorgenannte Urteil fordert eine Gefahrverwirklichung bzw. deren zeitliche Nähe, die nicht nur einen individuellen Zugriff auf einen möglichen Straftäter zulässt, sondern auch eine erkennbare Gefährdung konkreter Rechtsgüter. Dies ist im Bereich der vorbeugenden Straftatenbekämpfung und -verhütung gerade nicht der Fall. Art. 34d Abs. 1 Satz 1 Nr. 2 PAG dient aber im Unterschied zu Nr. 1 der Straftatenverhütung bzw. -vorbeugung. Insoweit handelt es sich bei der in Nr. 2 formulierten Eingriffsschwelle um eine unzulässige Anknüpfung an das Vorfeldstadium einer konkreten Gefahr, die verfassungsrechtlich angesichts der Schwere eines verdeckten Eingriffs auf informationstechnische Systeme nicht hinnehmbar ist.

(b) Verfassungswidrige Eingriffsdifferenzierung in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zwischen der Erhebung von Zugangsdaten und der Erhebung von gespeicherten Daten

Sowohl Art. 34d Abs. 1 Satz 2 PAG als auch Art. 34d Abs. 3 Satz 2 Halbsatz 2 PAG sehen einen erleichtern Zugriff auf informationstechnische Systeme bei der Erhebung von Zugangsdaten im Vergleich zur Erhebung von bereits gespeicherten Daten vor. Art. 34d Abs. 1 Satz 2 PAG erlaubt unter den Voraussetzungen des Satzes 1 die Löschung und Veränderung von Zugangsdaten. Dies soll bei bereits gespeicherten Daten nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben und Freiheit einer Person möglich sein. Art. 34d Abs. 3 Satz 2, Halbsatz 2 PAG erlaubt die Erhebung von Zugangsdaten auf Anordnung von Beamten des höheren Polizeidienstes, ohne dass eine Gefahr im Verzug bestehen muss. Bei gespeicherten Daten trifft hingegen die Anordnung grundsätzlich der Richter.

Zugangsdaten sind meist nicht im informationstechnischen System abgelegt und dienen als Schlüssel, um den Zugang zu den gespeicherten Daten zu eröffnen. Zugangsdaten sind insbesondere Benutzerkennungen, Pass- und Kennwörter; aber auch die von einem informationstechnischen System geforderte Authentifizierung mittels Fingerprint. Gespeicherte Daten sind hingegen sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten (BVerfG vom 27.02.2008, Rn. 205).

Zugangsdaten sind in der Regel persönliche Daten, die der Träger des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in besonderer Weise schützt. Dies ist regelmäßig für die gespeicherten Daten nur in unterschiedlicher Weise der Fall. Bei den gespeicherten Daten in einem informationstechnischen System wird es vielmehr eine Gemengelage bei den Daten geben; sie werden in unter-

schiedlicher Weise für den Träger des Grundrechts wichtig sein. Insoweit leuchtet es nicht ein, dass für Zugangsdaten niedrigere Eingriffsschwellen gelten sollen.

Das Bundesverfassungsgericht unterscheidet nicht zwischen Eingriffen in „Zugangsdaten“ und bereits „gespeicherten Daten“. Das Gericht sieht vielmehr bei „*flüchtigen oder nur temporär gespeicherten Daten*“ wie Passwörtern eine „*besondere Relevanz für die Persönlichkeit*“ (Rn. 236). Bei beiden Datenarten handelt es sich um personenbezogene Daten, die durch das Grundgesetz gleichermaßen geschützt werden. Im Urteil zur Online-Durchsuchung des BVerfG wurde zudem ausdrücklich festgestellt, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität auch vor Datenerhebungen mit Mitteln schützt, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa beim Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur (BVerfG vom 27.02.2008, Rn. 205). Der Einsatz von Keyloggern ist oftmals notwendig, um den Zugang zu den für die eigentlich zur Gefahrenabwehr erforderlichen Daten zu erhalten. Angesichts der zunehmenden Verbreitung von im Internet als Freeware herunterladbarer Kryptier- bzw. Verschlüsselungsprogramme, ermöglicht deshalb vielfach erst die verdeckte Erhebung von Zugangsdaten eine nachfolgende Auswertung des Speichermediums. Das Bundesverfassungsgericht sieht die Eingriffsintensität dieser Maßnahmen deshalb auch als keineswegs geringer an, als bei solchen die bereits gespeicherte Daten betreffen. Es stellt sie vielmehr unter die gleichen strengen Voraussetzungen. Der erleichterte Zugriff auf Zugangsdaten in Art. 34d Abs. 1 Satz 2 PAG als auch in Art. 34d Abs. 3 Satz 2 Halbsatz 2 PAG ist deshalb ein Verstoß gegen das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.

(c) Befugnis zur Datenänderung und Datenlöschung als Mittel der Gefahrenabwehr nach Art. 34d Abs. 1 Satz 2 PAG

Nach Art. 34d Abs. 1 Satz 2 PAG dürfen Daten unter den Voraussetzungen von Abs. 1 auch gelöscht oder verändert werden. Gespeicherte Daten können dies im Unterschied zu Zugangsdaten nur, wenn es zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und die bloße Datenerhebung zur Gefahrenabwehr nicht ausreichen würde. Die Löschung ist dabei der Datenentzug gegenüber dem Maßnahmeadressaten, während unter Verändern das Hinzufügen, Weglassen oder sonstige Ändern von Informationen zu verstehen ist.

Die in Art. 34d Abs. 1 Satz 2 PAG vorgesehene Möglichkeit, im Wege der Online-Durchsuchung gespeicherte Daten zu löschen oder zu verändern, ist nicht gedeckt durch die vom Bundesverfassungsgericht gezogenen Schranken des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und daher verfassungswidrig. Das Bundesverfassungsgericht hat ausdrücklich dargelegt, dass das Gewicht des Eingriffes in das Grundrecht sich in Folge der Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch betroffener Dritter erhöht (vgl. Rn. 239 ff. Urteil BVerfG vom 27.02.2008).

Zwar hat das Bundesverfassungsgericht nach den Hinweisen der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen festgestellt,

“es könne nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht“ (Rn. 240 Urteil BVerfG vom 27.02.2008).

Aber es hat die Online-Durchsuchungsbefugnis gleichwohl nur als Datenerhebungs- und Datenverwendungsbefugnis für zulässig erklärt. Die in Art. 34d Abs. 1 Satz 2 PAG vorgesehene Möglichkeit, bei der Online-Durchsuchung gespeicherte Daten zu löschen oder zu verändern, geht deshalb über einen verfassungsrechtlich zulässigen Eingriff hinaus. Eine gezielte Manipulation von Zugangsdaten und gespeicherten Daten greift darüber hinaus in das Eigentumsgrundrecht des Betroffenen aus Art. 14 Abs. 1 Satz 1 GG ein.

(d) Unzureichender Richtervorbehalt in Art. 34d Abs. 3 PAG

Wer eine Online-Durchsuchung anordnen darf, regelt Art. 34 d Abs. 3 Satz 1 und 2 PAG.

- Art. 34d Abs. 3 Satz 1 PAG ordnet eine entsprechende Anwendung von Art. 34 Abs. 4 Satz 1 und 2 PAG an. Nach Art. 34 Abs. 4 Satz 1 PAG ordnet der Richter, bei Gefahr im Verzug auch der Leiter eines Polizeipräsidiums oder des LKA die Maßnahme an, jedoch ist unverzüglich eine Bestätigung der Maßnahme durch den Richter einzuholen.
- Nach Art. 34d Abs. 3 Satz 2 Halbsatz 1 PAG hingegen kann bei Maßnahmen, die nach Art. 34d Abs. 2 PAG die Online-Durchsuchung vorbereiten (Erhebung von spezifischen Gerätekennungen und Einsatz des sog. WLAN-Catchers zur Standortermittlung eines informationstechnischen Systems), bei Gefahr im Verzug die Anordnungsbefugnis nach

Art. 33 Abs. 5 Satz 2 PAG auf Beamte des höheren Polizeidienstes übertragen werden, ohne dass unverzüglich eine Bestätigung der Maßnahme durch den Richter einzuholen ist.

- Nach Art. 34d Abs. 3 Satz 2 Halbsatz 2 PAG kann die Erhebung von Zugangsdaten, ohne dass eine Gefahr im Verzug besteht, nach Art. 33 Abs. 5 Satz 2 PAG auf Beamte des höheren Polizeidienstes übertragen werden, ebenfalls ohne dass unverzüglich eine Bestätigung der Maßnahme durch den Richter einzuholen ist.

Dass die Formulierungen des Richtervorbehalts in Art. 34d Abs. 3 PAG auf eine entsprechende Anwendung von Art. 34 Abs. 4 und Art. 33 Abs. 5 PAG verweisen, dient nicht dem verfassungsrechtlichen Gebot der Normenklarheit. Art. 34 Abs. 4 PAG bezieht sich auf verdeckte Datenerhebungen im Schutzbereich von Art. 13 GG und Art. 33 Abs. 5 PAG regelt allgemein Anforderungen an besondere Datenerhebungen. Das Urteil vom 27.02.2008 hat aber nun gerade für den verdeckten Zugriff auf informationstechnische Systeme den Richtervorbehalt unabhängig von Art. 13 GG hergeleitet. Der Normenklarheit wäre gedient, wenn im Art. 34d PAG der Richtervorbehalt selbstständig für den Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme formuliert worden wäre. Verfassungswidrig aber wird die Regelung, wenn Teile der Online-Durchsuchung wie in Art. 34d Abs. 3 Satz 2 PAG geregelt, ohne richterliche Anordnung ergehen dürfen. Dass auch die Erhebung von Zugangsdaten ein Eingriff in den Schutzbereich des IT-Grundrechts ist, hat das BVerfG ausdrücklich festgestellt. Ebenso ist es von einem gleichwertigen Schutz von Zugangs- und bereits gespeicherten Daten ausgegangen (siehe unter C. I. 2) (b)).

(e) Zweckänderung nach Art. 34d Abs. 5 Satz 2 Nr. 2 PAG

In Art. 34d Abs. 5 Satz 2 Nr. 2 PAG ist eine Verwendung zur Strafverfolgung bei solchen Straftaten vorgesehen, bei denen eine solche Maßnahme nach der Strafprozessordnung zulässig gewesen wäre. Die Strafprozessordnung sieht zwar derzeit keine Online-Datenerhebung vor, wäre aber für den Fall der Einführung einer solchen repressiven Befugnisnorm verfassungswidrig. Die in Art. 34d Abs. 5 Satz 2 Nr. 2 PAG vorgesehene Möglichkeit, Zufallsfunde zu Zwecken der Strafverfolgung zu verwerten und die damit eröffnete Möglichkeit der Umwidmung (Zweckänderung) grundsätzlich aller zu präventiven Zwecken erhobenen persönlichen Daten, geht zu weit. Diese Möglichkeit der Zweckänderung unterläuft zu

mindestens gegenüber betroffenen Dritten die vom Bundesverfassungsgericht statuierten Eingriffsvoraussetzungen für den verdeckten Zugriff auf informationstechnische Systeme. Zudem lädt die Regelung zu ihrem Missbrauch ein, nämlich zur systematischen Suche nach Zufallsfunden im Wege der Online-Durchsuchung.

3) Die Verfassungswidrigkeit der Online-Datenerhebung nach Art. 6e BayVSG

Gemessen an den Maßstäben des Urteils vom 27.02.2008 sind in Art. 6e BayVSG folgende Regelungen verfassungswidrig:

- Art. 6e Abs. 1 Satz 1 BayVSG (konkrete Gefahrenabwehr, dazu nachstehend unter **(a)**)
- Art. 6e Abs. 1 Satz 1 BayVSG (fehlender eigenständiger Richtervorbehalt, dazu nachstehend unter **(b)**)
- Art. 6e Abs.1 Satz 6 und 7 BayVSG (Unzureichender Kernbereichsschutz dazu unter Abschnitt **III. 3**)).

(a) Verfassungswidrige Eingriffsermächtigung in Art. 6e Abs. 1 Satz 1 BayVSG

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Verfassungsschutzgesetz des Landes NRW grundsätzlich festgestellt, dass die verfassungsrechtlichen Anforderungen an die Regelung des tatsächlichen Eingriffsanlasses im Fall des heimlichen Zugriffs auf ein informationstechnisches System für alle Eingriffsermächtigungen mit präventiver Zielsetzung zu beachten seien.

„Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die Gleiche ist, besteht hinsichtlich seiner Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang.“

(Bundesverfassungsgericht, Urteil vom 27.02.2008, Rn. 254)

Die Zulässigkeit einer Online-Durchsuchung bemisst sich demnach ausschließlich an der Beeinträchtigung für die Betroffenen. Sie bleibt bei einer Online-Durchsuchung immer die Gleiche, unabhängig davon, ob Polizeibehörden oder Verfassungsschutzbehörden sie vornehmen. Die unterschiedlichen Aufgaben von Polizei- und Verfassungsschutzbehörden sind für die Rechtfertigung des Eingriffs einer Online-Durchsuchung ohne Belang. Gerechtfertigt kann die Eingriffstiefe, die in einer Online-Durchsuchung liegt, nur dadurch werden, dass sie der Abwehr einer konkreten Gefahr dient. Das Bundesverfassungsgericht hat deshalb für die Online-Durchsuchung des Verfassungsschutzes keine anderen Voraussetzungen formuliert als sie auch für die Polizei gelten. Angesichts der Eingriffsintensität einer Online-Durchsuchung hat das Bundesverfassungsgericht den Gesetzgeber auch bei der Regelung der Befugnisse von Sicherheitsbehörden, deren Aufgabe in der Vorfeldaufklärung besteht, an die dieselben verfassungsrechtlichen Vorgaben gebunden. Dies hat bezogen auf die Online-Durchsuchung dazu geführt, dass auch Verfassungsschutzbehörden zu diesem intensiven Grundrechtseingriff nur dann ermächtigt werden dürfen, wenn die erhöhten Anforderungen an die Regelung des Eingriffsanlasses gewahrt sind, die auch für die Polizei gelten.

„Auch wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern.“

(Bundesverfassungsgericht, Urteil vom 27.02.2008, Rn 256)

Art. 6e Abs.1 Satz 1 BayVSG fordert tatsächliche Anhaltspunkte für konkrete Gefahren als Eingriffsvoraussetzung. Damit wird der vom Gericht aufgestellten Forderung nach einer Prognose entsprochen, die auf das Entstehen einer konkreten Gefahr bezogen ist, d.h. auf eine im Einzelfall bestehende hinreichende Wahrscheinlichkeit, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden verursacht wird. Die Regelung in Art. 6e Abs. 1 Satz 1 BayVSG genügt dem scheinbar. Sie formuliert eine Eingriffsschwelle, die den vom Gericht gewählten Formulierungen entspricht. Allerdings fragt es sich wie der Verfassungsschutz eine vorliegende konkrete Gefahr abwehren kann. Die Übertragung einer Befugnis, die ihre Rechtfertigung aus der Abwehr einer konkreten Gefahr bezieht, ist nur dann verfassungsgemäß, wenn die Behörde die Befugnis zur Abwehr auch gebrauchen kann. Dass eine Behörde, der selber die Vornahme kausalverlaufsunterbrechender, gefahrenbeseitigender

Maßnahmen wegen der Trennung von polizeilichen und geheimdienstlichen Aufgaben untersagt ist (vgl. Art. 1 Abs. 4 BayVSG), eine Befugnis zur Gefahrenabwehr erhält, ist nicht nur eine Frage der Zweckmäßigkeit. Ermächtigungen in den Geheimdienstgesetzen, die ihre verfassungsrechtliche Rechtfertigung aus der Abwehr konkreter Gefahren für höchstrangige Rechtsgüter beziehen, ohne dass sie selbst die Gefahr abwehren können, sind daher verfassungswidrig. Wenn der Gesetzgeber, wie in Art. 6e Abs. 1 Satz 1 BayVSG, den Weg der Befugnisübertragung geht, ohne dass diese ernsthaft als Gefahrenabwehrmaßnahmen eingesetzt werden können, fehlt der Befugnisübertragung die verfassungsrechtliche Rechtfertigung. Dem Trennungsgebot folgend stehen dem bayerischen Verfassungsschutz selber keine rechtlichen Instrumentarien zur Gefahrenabwehr im Sinne einer unmittelbar kausalverlaufunterbrechenden Intervention zur Verfügung. Einziges Mittel auf eine Gefahr einzuwirken, ist die Datenübermittlung nach Art. 14 Abs. 1 BayVSG. Danach darf das Landesamt für Verfassungsschutz personenbezogene Daten an inländische Behörden übermitteln, wenn die empfangende Behörde diese Informationen für Zwecke der öffentlichen Sicherheit benötigt. Damit wird aber dem Verhältnismäßigkeitsgrundsatz nicht genügt, wenn eine befugte Behörde selber keine eigenen Kompetenzen zur Bewältigung der tatbestandlich vorausgesetzten Lage besitzt.

(b) Fehlender eigenständiger Richtervorbehalt

Das Bundesverfassungsgericht verlangt für die Online-Durchsuchung die richterliche Anordnung (Urteil vom 27.02.2008, Rn. 257). Der Richtervorbehalt soll gewährleisten, dass auf die Interessen des Betroffenen hinreichend Rücksicht genommen wird, da er selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorhinein nicht wahrnehmen kann. Die Kontrolle dient insoweit der „kompensatorischen Repräsentation“ der Interessen des Betroffenen im Verwaltungsverfahren.

Art. 6e des BayVSG enthält einen solchen Richtervorbehalt nicht. Der Verweis auf Art. 6a Abs. 2 BayVSG und die dort geregelten Voraussetzungen führt zu Art. 6b BayVSG. Nach dessen Abs. 1 bedarf der Einsatz technischer Mittel im Schutzbereich von Art. 13 einer richterlichen Anordnung auf Antrag des Präsidenten des Landesamts für Verfassungsschutz oder dessen Stellvertreter.

Da sich Art. 6a und 6b BayVSG ausdrücklich auf Eingriffe in den Schutzbereich des Art. 13 GG beziehen, ist der Richtervorbehalt im Wege verfassungskonformer Auslegung von Art. 6b Abs. 1 BayVSG nicht auf Art. 6e BayVSG übertragbar. Art. 6e BayVSG regelt die Eingriffsbefugnis in ein anderes Grundrecht, den Eingriff in das Grundrecht auf Gewähr-

leistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Von daher fehlt es an einer selbständigen Regelung des Richtervorbehalts in Art. 6e BayVSG.

4) Unterschreiten der staatlichen Gewährleistungspflichten für die Vertraulichkeit und Integrität informationstechnischer Systeme in Art. 34d PAG und Art. 6e BayVSG

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verlangt vom Gesetzgeber, der wie der bayerische Gesetzgeber in Art. 34d PAG und Art. 6e BayVSG staatliche Eingriffsbefugnisse in informationstechnische Systeme regelt, dass er den durch das Grundrecht statuierten Schutzpflichten für die Vertraulichkeit und Integrität informationstechnischer Systeme genügt.

„Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können aufgrund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen. Dies kann den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen.“

(Bundesverfassungsgericht, Urteil vom 27.02.2008, Rn. 240)

Weiter heißt es in dem Urteil

„Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Ziel-

konflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.“

(Bundesverfassungsgericht, Urteil vom 27.02.2008, Rn. 241)

Vor diesem Hintergrund ergeben sich für den Gesetzgeber Schutzpflichten, denen er mit entsprechenden gesetzlichen Regelungen inhaltlich zu genügen hat. So ist bei der Regelung der Eingriffsbefugnisse vorzusehen, dass

- an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und
- die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden,
- das eingesetzte technische Mittel nach dem aktuellen Stand von Wissenschaft und Technik gegen unbefugte Nutzung zu schützen ist und
- die kopierten Daten nach dem aktuellen Stand von Wissenschaft und Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind (vgl. § 20 k Abs. 2 BKAG-Entwurf, BT-Drs. 16/9588).

Darüber hinaus sollten ein effektiver Rechtsschutz des Betroffenen und eine effektive Datenschutzkontrolle ermöglicht werden durch die Formulierung von Protokollierungspflichten für insbesondere folgende Punkte (vgl. § 20k Abs. 3 BKAG-Entwurf, BT-Drs. 16/9588):

- die Bezeichnung des technischen Mittels und der Einsatzzeitpunkt
- Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen Veränderungen
- Angaben, die die Feststellung der erhobenen Daten ermöglichen und die Organisationseinheit und Personen, die die Maßnahme durchführen.

Die Dokumentationspflicht zum Schutz des „Computer-Grundrechts“ ist vom Bundesverfassungsgericht in der Entscheidung vom 27.02.2008 ausdrücklich benannt worden (Rn. 239 ff.).

Zwar ordnet Art. 34d Abs. 1 Satz 7 PAG die Dokumentation der Maßnahmen nach den Sätzen 1 und 2 an, sie wird aber in keiner Weise spezifiziert. Darüber hinausgehende Schutzvorkehrungen, um Schäden für die informationstechnischen Systeme zu vermeiden bzw. rückgängig zu machen, trifft der Gesetzgeber des PAG nicht. Im BayVSG fehlt es auch an der Regelung der Dokumentationspflicht. Von daher unterschreiten beide Gesetze die verfassungsrechtlich geforderte Schutzpflicht.

II. Verfassungswidrigkeit der Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG

Die Regelungen in Art. 34e PAG bzw. Art. 6g BayVSG, die als Begleitmaßnahmen für Online-Durchsuchungen, präventive Wohnraumüberwachungen (akustische und optische) und Telekommunikationsüberwachungen das heimliche Durchsuchen und Betreten von Wohnungen erlauben, sind verfassungswidrig. Sie sind als eigenständige Eingriffe selbstständig am Maßstab des Grundrechts auf Unverletzlichkeit der Wohnung in Art. 13 GG zu messen. (Dazu nachstehend **2**). Soweit die in Art. 6g BayVSG und Art. 34e PAG vorgesehenen verdeckten Begleitmaßnahmen Befugnisse zur heimlichen Wohnungsdurchsuchung sind, sind sie verfassungswidrig, weil sie als heimliche Maßnahmen nicht dem Merkmal der Offenheit entsprechen, dass Art. 13 Abs. 2 GG verlangt. (Dazu nachstehend **3**). Soweit die in Art. 6g BayVSG und Art. 34e PAG vorgesehenen verdeckten Begleitmaßnahmen Befugnisse zum heimlichen Betreten von Wohnungen sind und mit der technischen Überwachung von Wohnungen notwendigerweise verbundene, vorbereitende Maßnahmen darstellen, sind sie Schrankenregelung wie die Hauptmaßnahme, dass heißt Art. 13 Abs. 4 GG unterworfen. Die Regelungen in Art. 6a Abs. 2 Satz 1 BayVSG und Art. 34 Abs. 1 Satz 1 Nr. 2 PAG unterschreiten diese Schranken und sind deshalb verfassungswidrig (Dazu nachstehend unter **4**).

1) Begleit- und Hauptmaßnahmen

Die in Art. 6g BayVSG und Art. 34e PAG geregelten Eingriffsbefugnisse sind vorgesehen als verdeckte Begleitmaßnahmen zu verdeckten Hauptmaßnahmen, die ihrerseits in den Art. 6a und 6e BayVSG und den Art. 34 Abs. 1, 34a und 34d PAG geregelt sind. Für die Anordnung der Begleitmaßnahmen gelten nach Art. 6g Satz 2 BayVSG und Art. 34e Abs. 1 Satz 2 PAG die gleichen Vorschriften wie für die Hauptmaßnahme.

Für Art. 6g BayVSG stellt sich der Zusammenhang zwischen Begleitmaßnahme, Hauptmaßnahme und Anordnungsvoraussetzung wie folgt dar:

| Begleitmaßnahme | Hauptmaßnahme | Anordnungsvoraussetzung |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 6a BayVSG: Einsatz technischer Mittel im Schutzbereich des Art. 13 GG | Art. 6a Abs. 2 Satz 1 BayVSG: „... tatsächliche Anhaltspunkte für den Verdacht vorliegen dass jemand Bestrebungen oder Tätigkeiten nach Art. 3 Abs. 1 Satz 1 durch die Planung oder Begehung von Straftaten verfolgt, die im Einzelfall geeignet sind den Bestand oder die Sicherheit des Bundes oder eines Landes oder in erheblichem Maße Leib, Leben oder Freiheit von Personen zu gefährden.“ |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 6e Abs. 1 BayVSG: verdeckte Online-Datenerhebung | Art. 6e Abs. 1 Satz 1 BayVSG: „... bei Vorliegen tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut unter den Voraussetzungen des Art. 6a Abs. 2“ |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 6e Abs. 2 BayVSG: Vorbereitung einer Maßnahme nach Art. 6e Abs. 1 BayVSG | wie in Art. 6e Abs. 1 Satz 1 BayVSG |

Für Art. 34e PAG stellt sich der Zusammenhang zwischen Begleitmaßnahme, Hauptmaßnahme und Anordnungsvoraussetzung wie folgt dar:

| Begleitmaßnahme | Hauptmaßnahme | Anordnungsvoraussetzung |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34 Abs. 1 PAG: verdeckter Einsatz technischer Mittel zur Erhebung personenbezogener Daten in und aus Wohnungen | Art. 34 Abs. 1 Satz 1 Nr. 1 PAG: „... wenn dies erforderlich ist zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person“ Art. 34 Abs. 1 Satz 1 Nr. 2 PAG: „... über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat nach Art. 30 Abs. 5 Satz 1 Nr. 1, 2 (ohne § 129 Abs. 1 in Verbindung mit Abs. 4 StGB) bis 9 begehen werden.“ |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 1 PAG: Überwachung und Aufzeichnung der Telekommunikation | Art. 34a Abs. 1 Satz 1 Nr. 1 PAG: „... soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist“ Art. 34a Abs. 1 Satz 1 Nr. 2 PAG: „... wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat begehen werden“ |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 2 Satz 1 Nr. 1 PAG: zur Vorbereitung einer Maßnahme nach Art. 34a Abs. 1 PAG Ermittlung spezifischer Kennung | Voraussetzungen des Art. 34a Abs. 1 PAG |

| Begleitmaßnahme | Hauptmaßnahme | Anordnungsvoraussetzung |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 2 Satz 1 Nr. 2 PAG: Standortermittlung eines Mobilfunkendgerätes | Voraussetzungen des Art. 34a Abs. 1 PAG |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 3 Satz 1 Nr. 1 PAG: Überwachung und Aufzeichnung der Telekommunikation zur Erhebung personenbezogener Daten über eine Person, deren Leben oder Gesundheit in Gefahr ist | Bei Gefahr für Leben oder Gesundheit einer Person |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 3 Satz 1 Nr. 2 PAG: Standortermittlung eines Mobilfunkendgeräts einer Person nach Art. 34a Abs. 3 Satz 1 Nr. 1 PAG | Bei Gefahr für Leben oder Gesundheit einer Person |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34a Abs. 4 PAG: Unterbrechung von Kommunikationsverbindungen | Voraussetzungen des Art. 34a Abs. 1 PAG |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34d Abs. 1 Satz 1 PAG: verdeckter Zugriff auf informationstechnische Systeme | Art. 34d Abs. 1 Satz 1 Nr. 1 PAG: „... soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist“ Art. 34d Abs. 1 Satz 1 Nr. 2 PAG: „... wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat nach Art. 30 Abs. 5 Satz 1 Nr. 1, 2 (ohne § 129 Abs. 1 in Verbindung mit Abs. 4 StGB) bis 9 begehen werden“ |

| Begleitmaßnahme | Hauptmaßnahme | Anordnungsvoraussetzung |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34d Abs. 2 Satz 1 Nr. 1 PAG: verdeckter Zugriff auf spezifische Kennungen informationstechnischer Systeme zur Vorbereitung einer Maßnahme nach Art. 34d Abs. 1 PAG | Voraussetzungen des Art. 34d Abs. 1 PAG |
| verdeckte Durchsuchung von Sachen und Wohnungen und Betreten von Wohnungen ohne Einwilligung | Art. 34d Abs. 2 Satz 1 Nr. 2 PAG: verdeckte Standortermittlung einer informationstechnischen Systems | Voraussetzungen des Art. 34d Abs. 1 PAG |

Die Tabellen verdeutlichen, dass immer die selben Begleitmaßnahmen, verdeckte Durchsuchung von Sachen und Wohnungen und das Betreten von Wohnungen ohne Einwilligung, für eine Fülle unterschiedlicher Hauptmaßnahmen geregelt sind, die ihrerseits höchst unterschiedliche Eingriffsvoraussetzungen haben.

2) Art. 13 GG als eigenständiger Maßstab für die Prüfung der Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG

Die in Art. 6g BayVSG und in Art. 34e PAG vorgesehenen verdeckten Begleitmaßnahmen bezüglich des heimlichen Betretens und Durchsuchens von Wohnungen sind am Grundrecht der Unverletzlichkeit der Wohnung zu messen, auch dann, wenn die Hauptmaßnahme in ein anderes Grundrecht eingreift. Die in Art. 6g BayVSG und in Art. 34e PAG vorgesehenen Befugnisse müssen als selbständige Eingriffe in Art. 13 GG bewertet werden. Das heimliche Betreten und Durchsuchen der Wohnung ist nicht bereits durch die Eingriffsermächtigung zur Hauptmaßnahme gedeckt. Die vorgesehene Begleitmaßnahme „heimliches Betreten und Durchsuchen der Wohnung“ ist daher verfassungsrechtlich selbstständig, unabhängig von der Hauptmaßnahme, zu beurteilen. Das BVerfG hat dieses Nebeneinander von Eingriffen in verschiedene Grundrechte von Haupt- und Begleitmaßnahme bezogen auf die Online-Durchsuchung ausdrücklich festgestellt. Wird die Wohnung heimlich betreten und durchsucht als Begleit- oder Vorbereitungsmaßnahme für eine Online-Durchsuchung, ist die Hauptmaßnahme am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen; die Vorbereitungsmaßnahme aber am Grundrecht der Unverletzlichkeit der Wohnung.

So heißt es im Urteil des Bundesverfassungsgerichts vom 27.02.2008 wörtlich in Rn. 193:

„Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrophon oder eine Kamera dazu genutzt werden.“

Bei einer Hauptmaßnahme, bei der präventiv technische Mittel im Schutzbereich von Art. 13 GG nach Art. 34 Abs. 1 PAG und Art. 6a BayVSG eingesetzt werden, ist bereits im Zusammenhang mit der Einfügung von Art. 13 Abs. 4 GG ins Grundgesetz 1998 die Frage diskutiert worden, ob heimliches Betreten und Durchsuchen der Wohnung als vorbereitende Maßnahme zur Ermöglichung des präventiven Lausch und Spähangriffes ebenfalls an Art. 13 Abs. 4 oder aber weiter an Art. 13 Abs. 2 GG zu messen ist. (Nachweise zur Diskussion bei G. Hermes in Dreier, 1. Auflage, Bd. I, Art. 13 Rn. 52).

In der Literatur ist, weniger für den präventiven Lauschangriff als vielmehr für den repressiven Lauschangriff nach Art. 13 Abs. 3 GG, das heimliche Betreten der Wohnung, soweit es notwendig mit dem Abhören verbunden ist, von der Regelung der heimlichen Hauptmaßnahme als gedeckt angesehen worden (vgl. Ziekow/Guckelberger, Festschrift 73; Berkemann, in AK-GG, Okt. 2001 Art. 13 Rn. 130, m.w. N.; Papier, in Maunz/Dürig, GG, Art. 13 Rn. 47, 79, 89; Jarass/Pieroth, Art. 13 Rn. 19; Meyer/Hetzer, NJW 1998 S. 1017, 1026). Danach sind mit dem Abhören notwendigerweise verbundene Maßnahmen, z. B. heimliches Betreten der Wohnung zur Anbringung technischer Vorrichtungen, erlaubt. Bei der technischen Wohnraumüberwachung soll die Begleitmaßnahme der Installation der Abhörtechnik derselben Schrankenregelung wie die Hauptmaßnahme unterworfen sein (Stern, Handbuch des Staatsrechts, Bd. 4/1, 2006, S. 283 f.). Das Kennzeichen der Maßnahmen, die unter Art. 13 Abs. 3 bis 6 GG fallen, sei gerade deren Heimlichkeit und Anonymität, deshalb sei im Rahmen von Maßnahmen des Art. 13 Abs. 3 GG das Betreten der Wohnung des „Beschuldigten“, erlaubt, um darin technische Mittel anbringen zu können. Eine Ermächtigung zur akustischen Wohnraumüberwachung, im repressiven oder im präventiven Bereich, würde ins Leere laufen, wenn nicht zugleich mit der Maßnahme

einhergehende unerlässliche Vorbereitungs- bzw. Begleithandlungen zulässig wären (vgl. Heger, JR 1998, 164; Anhörung im Ausschuss für Kommunale Fragen und Innere Sicherheit des Bayerischen Landtags, 99. Sitzung am 27.05.2008, Anlage zum Wortprotokoll – Stellungnahme von Prof. Dr. Heckmann).

Damit wird zum einen dem Betreten der Wohnung die Heimlichkeit zugebilligt, die sie nach Art. 13 Abs. 2 GG nicht hätte, zugleich wird sie jedoch unter die erhöhten verfassungsrechtlichen Anforderungen von Art. 13 Abs. 4 GG gestellt.

Das soll aber für eine Durchsuchung nicht gelten, weil eine Durchsuchung - anders als das Betreten zur Installation von Abhörtechnik - nicht notwendigerweise mit dem Abhören verbunden ist.

Für Telekommunikationsüberwachungsmaßnahmen gilt eine Analogie zu Art. 13 Abs. 4 GG bezüglich der Begleitmaßnahmen jedoch nicht. Unabhängig von der Verfassungsmäßigkeit der Hauptmaßnahmen zur Telekommunikationsüberwachung nach Art. 34a PAG, die ihrerseits nach Art. 10 GG zu beurteilen sind, müssen die nach Art. 34e PAG möglichen Begleitmaßnahmen des heimlichen Betretens und Durchsuchens der Wohnung an den Schranken des Art. 13 Abs. 2 GG gemessen werden. Die Begleitmaßnahme ist auch hier wie bei der Online-Durchsuchung ein Eingriff in den Schutzbereich eines anderen Grundrechts, ein Eingriff in den Schutzbereich des Wohnungsgrundrechts. Auch eine Schrankenübertragung aus Art. 13 Abs. 4 GG scheidet aus grundsätzlichen Überlegungen aus.

3) Grundsatz der Offenheit der Durchsuchung in Art. 13 Abs. 2 GG

(a) Durchsuchungsbegriff

Handelt es sich bei den Begleitmaßnahmen nach Art. 6g BayVSG und Art. 34e PAG um Wohnungsdurchsuchungen, ist ihre Verfassungsmäßigkeit nach Art. 13 Abs. 2 GG zu prüfen. Art. 13 Abs. 2 GG ist die speziellere Vorschrift hinsichtlich der Rechtfertigung eines Eingriffs, der eine Durchsuchung darstellt (vgl. BVerwGE 28, 285, 286 f.; BVerwGE 47, 3, 36; BVerfGE 51, 97, 106 f.). Das BVerfG hat den Durchsuchungsbegriff nach Art. 13 Abs. 2 GG definiert als

„ziel- und zweckgerichtetes Suchen staatlicher Organe nach Personen oder Sachen oder zur Ermittlung eines Sachverhalts, um etwas aufzuspüren, was der Inhaber der Wohnung von sich aus nicht offen legen oder herausgeben will“ (BVerfGE 28, 235, 287 ff.; 47, 31, 36f; 76, 83, 89).

(b) Offenheit der Durchsuchung

Als Charakteristikum einer Durchsuchung im Sinne von Art. 13 Abs. 2 GG ist nach herrschender Auffassung das Merkmal der Offenheit der Maßnahme anzusehen (Kutscha, Die Legalisierung des Lauschangriffs, DuR 1992, S. 247-252). Die in Art. 13 Abs. 2 GG genannten Eingriffsmöglichkeiten „Betreten und Durchsuchen“ erfolgen gegenüber dem Betroffenen offen und nicht heimlich (Gornig, in: von Mangoldt/Klein/Starck, GG, Art. 13 Rn. 65; ebenso zur Parallelproblematik bei der Änderung von Art. 13 Abs. 3 GG anlässlich der akustischen Wohnraumüberwachung Papier, in: Maunz/Dürig, GG, Art. 13 Rn. 47). Der Grundrechtsträger soll bemerken, dass seine Wohnung Gegenstand einer staatlichen Ausforschung ist (vgl. Kühne, in: Sachs, GG, Art. 13 Rn.25). Der Betroffene soll erkennen, dass seine Wohnung durchsucht wird, um die Einhaltung der strengen Verfahrensvorschriften kontrollieren zu können.

Wegen der Heimlichkeit von Lausch- und Spähangriffen im Unterschied zu den Eingriffen in Art. 13 Abs. 2 und Abs. 7 GG, die nur zulässig sind, wenn sie offen erfolgen, musste 1998 das Grundgesetz geändert werden. Die Änderung des Grundgesetzes zur Einführung des „Großen Lauschangriffs“ war erforderlich, um eine heimliche technische Wohnraumüberwachung zu ermöglichen, wie das Bundesverfassungsgericht einleitend in seinem Urteil ausführte (vgl. Urteil vom 03.03.2004, Az. 1 BvR 2378/98 u. 1 BvR 1084/99 Rn. 3 f.). Durch die Änderung des Grundgesetzes wurde klargestellt, dass technische Überwachungsmaßnahmen nicht als Durchsuchung im Sinne von Art. 13 Abs. 2 GG angesehen werden können. Durch die Grundgesetzänderung wurden für die technische Überwachung von Wohnungen andere Voraussetzungen und Schranken als die, die für die Durchsuchung gelten, geregelt. Dabei ist die Offenheit der Durchsuchung das Abgrenzungskriterium zu den optischen und akustischen Überwachungsmaßnahmen nach Art. 13 Abs. 3 bis 5 GG. Dies wurde auch noch einmal in der BGH-Rechtsprechung zur Durchsuchung im strafprozessualen Sinne im Beschluss zur Online-Durchsuchung bestätigt.

„Die Durchsuchung gem. §§ 102, 103 StPO erfasst nach der Gesetzessystematik den grundsätzlich offenen körperlichen Zugriff auf Beweismittel (oder Einziehungsgegenstände usw.) bzw. die Träger von Beweismitteln. Demgegenüber findet der heimliche Zugriff mit technischen (elektronischen) Mitteln seine abschließende Grundlage in den §§ 100a bis 100i StPO.“ (12 BGH, MMR 2007, 175.)

Diese Ausführungen wurden durch Beschluss des BGH vom 31.01.2007 bestätigt.

„Das Bild der Strafprozessordnung von einer rechtmäßigen Durchsuchung ist dadurch geprägt, dass Ermittlungsbeamte am Ort der Durchsuchung körperlich anwesend sind und die Ermittlungen offenlegen (vgl. BVerfGE 115, 166 = NJW 2006, 976, 981)“. (BGH, Beschluss vom 31.01.2007 – StB 18/06, Rn. 5)

Mit der Rechtssprechung zum Lauschangriff und zur Online-Durchsuchung steht mithin fest, dass sich heimliche Maßnahmen nicht auf die Grundrechtsschranke des Art. 13 Abs. 2 GG stützen können.

(c) Fehlende Offenheit der Begleitmaßnahmen in Art. 6g BayVSG und Art. 34e PAG

Da das in Art. 6g BayVSG und Art. 34e PAG geregelte verdeckte Durchsuchen von Wohnungen als Begleitmaßnahmen dem Durchsuchungsbegriff des Art. 13 Abs. 2 GG unterfällt, ist festzustellen, dass sie der Schrankenregelung aus Art. 13 Abs. 2 GG wegen des Merkmals der Offenheit einer Durchsuchung nicht entsprechen. „Durchsuchungen“ sind zudem in Art. 13 Abs. 2 GG abschließend geregelt. Deshalb scheidet auch ein Rückgriff auf Art. 13 Abs. 7 GG aus. Hinzu kommt, dass nach herrschender Auffassung auch Art. 13 Abs. 7 GG nur offene Eingriffe erfassen soll (so auch: Kutscha, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2006, S. 58). Da es sich bei den in Art. 6g BayVSG und Art. 34e PAG geregelten Begleitmaßnahme um Durchsuchungen handelt, sind sie an Art. 13 Abs. 2 GG zu messen. Nach Art. 13 Abs. 2 GG sind aber Durchsuchungen von Wohnungen nur als offene und nicht als verdeckte Maßnahmen zulässig. Insoweit sind die in Art. 6g BayVSG und Art. 34e PAG vorgesehenen Begleitmaßnahmen, die nach der Rechtsprechung des Bundesverfassungsgerichts den Tatbestand des Betretens und Durchsuchens erfüllen, als heimliche Maßnahmen nach Art. 13 Abs. 2 GG nicht zulässig.

4) Heimliches Betreten als verfassungswidrige Begleitmaßnahme einer präventiven Wohnungsüberwachung mit technischen Mitteln nach Art. 13 Abs. 4 GG

(a) Anordnungsvoraussetzungen nach Art. 13 Abs. 4 GG

Auch für das in Art. 6g BayVSG und Art. 34e PAG vorgesehene heimliche Betreten von Wohnungen als Begleitmaßnahme zu einer Wohnungsüberwachung mit technischen Mitteln als Hauptmaßnahme sollen die Eingriffsvoraussetzungen der Hauptmaßnahme gelten. Diese sind an den verfassungsrechtlichen Maßstäben für eine präventive Wohnungsüberwachung mit technischen Mitteln des Art. 13 Abs. 4 Satz GG zu messen. Danach darf die technische Überwachung von Wohnungen nur zur Abwehr dringender Gefahren für die öffentliche Sicherheit als Schutzgut dienen. Andere Ziele sind – jedenfalls nach Art. 13 Abs. 4 GG – unzulässig. Art. 13 Abs. 4 GG betrifft nicht die konkrete Verbrechenverfolgung; er dient auch nicht der vorbeugenden Bekämpfung von Straftaten im Sinne polizeilicher (bzw. präventiver) Aufgabenzuweisung. Dabei können nur hochrangige Rechtsgüter der öffentlichen Sicherheit Schutzobjekt sein. Das Bestehen gemeiner Gefahr oder Lebensgefahr sind kraft Verfassung stets Fälle dringender Gefahren für die öffentliche Sicherheit. Leibes- oder Freiheitsschutz werden nicht genannt, sind aber nicht ausgeschlossen (vgl. Berkemann AK-GG, Oktober 200, Art. 13, Rn. 161). „Gemein“ ist die Gefahr, die sich auf eine unbestimmte Zahl von Personen oder Sachen bezieht. Die Gefahr muss konkret sein. Die vorsorgende Gefahrenverhütung ist ausgeschlossen. Die Gefahr muss dringend sein. Der Ausdruck „dringende Gefahr“ verbindet in Art. 13 Abs. 4 GG Elemente der Gefahrenlage und des gefährdeten Schutzgutes in einem qualitativen Sinne (vgl. BVerfGE 100, 313, 392 ff. zu Art. 10 GG). Der Eintritt des Schadens für das Gemeinwohl muss bei ungehindertem Ablauf mit hinreichender Wahrscheinlichkeit zu erwarten sein. Zugelassen ist der Einsatz aller technischen Mittel in der Wohnung, neben akustischen Mitteln auch optische Mittel. Die Verhältnismäßigkeit der technischen Überwachung ist zu beurteilen nach ihrer Geeignetheit und Erforderlichkeit, vor allem aber nach ihrer Verhältnismäßigkeit im engeren Sinne. Das „bloße“ Vorliegen einer dringenden Gefahr rechtfertigt für sich genommen noch keine Präventivüberwachung. Die Erforschung des beurteilungsbedürftigen Sachverhaltes darf anders als durch akustische oder optische Überwachung der Wohnung nicht erreichbar sein. Dem steht gleich, dass die Erforschung auf andere Weise unverhältnismäßig erschwert wäre (ultima ratio).

(b) Verstoß gegen die Maßstäbe von Art. 13 Abs. 4 GG durch Art. 6g BayVSG und Art. 34e PAG

Auch für das in Art. 6g BayVSG und Art. 34e PAG vorgesehene heimliche Betreten von Wohnungen als Begleitmaßnahme zu einer Wohnungsüberwachung mit technischen Mitteln als Hauptmaßnahme sollen die Eingriffsvoraussetzungen der Hauptmaßnahme gelten. Das heißt im Einzelnen:

- Für die Begleitmaßnahme nach Art. 6g BayVSG zu Art. 6a BayVSG als Hauptmaßnahme verlangt Art. 6a Abs. 2 Satz 1 BayVSG

„tatsächliche Anhaltspunkte für den Verdacht ..., dass jemand Bestrebungen oder Tätigkeiten nach Art. 3 Abs. 1 Satz 1 BayVSG durch die Planung oder Begehung von Straftaten verfolgt, die im Einzelfall geeignet sind, den Bestand oder die Sicherheit des Bundes oder eines Landes oder in erheblichem Maße Leib, Leben oder Freiheit von Personen zu gefährden.“

- Für die Begleitmaßnahme nach Art. 34e PAG zu Art. 34 PAG als Hauptmaßnahme verlangt

Art. 34 Abs. 1 Satz 1 Nr. 1 PAG

„...wenn dies erforderlich ist zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder für Leib, Leben oder Freiheit einer Person.“

und

Art. 34 Abs. 1 Satz 1 Nr. 2 PAG

„... , wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat nach Art. 30 Abs. 5 Satz 1 Nr. 1, 2 (ohne § 129 Abs. 1 in Verbindung mit Abs. 4 StGB) bis 9 begehen werden.“

Den verfassungsrechtlichen Maßstäben von Art. 13 Abs. 4 GG entsprechen nur die in Art. 34 Abs. 1 Satz 1 Nr. 1 PAG geregelten Eingriffsvoraussetzungen. Die Regelungen in Art. 6a

Abs. 2 Satz 1 BayVSG und Art. 34 Abs. 1 Satz 1 Nr. 2 PAG unterschreiten hingegen die Vorgaben des Art. 13 Abs. 4 GG. Beide Normen verlangen nicht eine konkrete Gefahr, sondern sind Maßnahmen der Gefahrenverhütung. Sie sind damit auch unter der Voraussetzung, dass heimliches Betreten als Begleitmaßnahme zur Wohnraumüberwachung mit technischen Mitteln akzeptiert wird, verfassungswidrig.

III. Die Verfassungswidrigkeit der den Kernbereich privater Lebensgestaltung schützenden Regelungen

Die neuen kernbereichsschützenden Regelungen im BayVSG und im PAG (dazu unter **1**) entsprechen nicht den verfassungsrechtlichen Vorgaben (dazu unter **2**) für den Kernbereichsschutz bei verdeckten Datenerhebungen. Für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes nach Art. 6d BayVSG enthält Art. 6f Abs. 4 Satz 2 Nr. 3 BayVSG keine kernbereichsschützenden Regelungen die dem Schutzkonzept auf der ersten Stufe zuzurechnen sind (dazu unter **3 (a)**). Bei den Neuregelungen des Kernbereichsschutzes für die Online-Durchsuchung im BayVSG und PAG, für Datenerhebungseingriffe in den Telekommunikationsbereich im PAG und für den Einsatz technischer Mittel im Schutzbereich des Art. 13 GG im BayVSG und PAG gibt es keine ausreichende Regelung von Anhaltspunkte für drohende Kernbereichsverletzungen (dazu unter **3 (a)**), dafür aber Regelungen über das „Vortäuschen kernbereichszugehöriger Kommunikation zur Überwachungsverhinderung“, die unzureichend bestimmt sind (dazu unter **3 (b)**). Auf der zweiten Stufe des Kernbereichsschutzes genügen die Neuregelungen für Kernbereichsdaten, die beim Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes nach Art. 6d BayVSG und bei Eingriffen in den Telekommunikationsbereich nach Art. 34a PAG erhoben werden, nicht dem vom Verfassungsgericht geforderten Schutzniveau (dazu unter **3 (c)**).

1) Die neuen kernbereichsschützenden Regelungen

(a) Die neuen kernbereichsschützenden Regelungen im BayVSG

Art. 6a BayVSG, der den Einsatz technischer Mittel im Schutzbereich des Art. 13 GG regelt, enthält folgende kernbereichsschützende Regelungen:

In Abs. 3 Satz 2:

„²In den Fällen des Satzes 1 Nrn. 2 und 3 ist eine nur automatische Aufzeichnung zulässig, wenn bei Anordnung der Maßnahme abzusehen ist, dass keine Gespräche geführt werden, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind; wird bei einer Maßnahme nach Abs. 1 erkennbar, dass solche Gespräche geführt werden und bestehen keine Anhaltspunkte dafür, dass sie dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Datenerhebung unverzüglich und so lange erforderlich zu unterbrechen.“

Art. 6b BayVSG, der die Verfahrensregelungen für Maßnahmen nach Art. 6a BayVSG regelt, enthält folgende kernbereichsschützende Regelungen:

In Abs. 2 Satz 5 Nr. 3:

„⁵Daten, bei denen sich nach Auswertung herausstellt, dass

- 3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 6a Abs. 2 genannten Bestrebungen oder Tätigkeiten haben, dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich und Daten im Sinn der Nr. 2 oder 3 sind nicht betroffen.“*

In Abs. 3 Satz 1:

„¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen.“

Für Maßnahmen nach Art. 6d BayVSG, der das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes regelt, enthält Art. 6f Abs. 4 Satz 2 Nr. 3, Satz 3 BayVSG folgende kernbereichsschützenden Regelungen:

„²Soweit bei Maßnahmen nach Art. 6d Daten erhoben wurden, bei denen sich nach Auswertung herausstellt, dass

- 3. sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 6a Abs. 2 genannten Bestrebungen oder Tätigkeiten haben,*

dürfen sie nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich und Daten

im Sinn der Nr. 2 oder 3 sind nicht betroffen. ³Daten, die nicht verwendet werden dürfen, sind unverzüglich zu löschen.“

Für die in Art. 6e BayVSG geregelte verdeckte Online-Datenerhebung sind folgende kernbereichsschützenden Regelungen vorgesehen:

In Art. 6e Abs. 1 Sätze 6 und 7:

„⁶Soweit informationstechnisch und ermittlungstechnisch möglich, sind alle Maßnahmen zu ergreifen, mit denen die Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, vermieden werden kann. ⁷Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die weitere Datenerhebung insoweit unzulässig.“

In Art. 6f Abs. 5 Satz 3 Nr. 1:

„³Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten
1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
sind diese unverzüglich zu löschen oder dem zuständigen Richter zur Entscheidung über die weitere Verwendung vorzulegen.“

(b) Die neuen kernbereichsschützenden Regelungen im PAG

In Art. 34 PAG, der die besonderen Bestimmungen über den Einsatz technischer Hilfsmittel in Wohnungen enthält, wurden die vorhandenen kernbereichsschützende Regelungen

in Abs. 2 durch einen neuen Halbsatz 2 wie folgt ergänzt (Ergänzung fett und kursiv gedruckt):

*„(2) In den Fällen des Abs. 1 Satz 2 Nrn. 2 und 3 ist eine nur automatische Aufzeichnung zulässig, wenn bei Anordnung der Maßnahme abzusehen ist, dass keine Gespräche geführt werden, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind; wird bei einer Maßnahme nach Abs. 1 Satz 1 erkennbar, dass solche Gespräche geführt werden **und bestehen keine Anhaltspunkte dafür, dass sie dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen**, ist die Datenerhebung unverzüglich und so lange erforderlich zu unterbrechen.“*

und

in Abs. 5 Satz 3 wie folgt ergänzt (Ergänzung fett und kursiv gedruckt):

„³Daten, bei denen sich nach Auswertung herausstellt, dass

3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben,

dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich **und Daten im Sinn der Nr. 2 oder 3 sind nicht betroffen.**“

In Art. 34a PAG, der die Datenerhebung und Eingriffe in den Telekommunikationsbereich regelt, wurde Abs. 1 Satz 4 wie folgt neu gefasst:

„⁴Wird erkennbar, dass dem Kernbereich privater Lebensgestaltung zuzurechnende Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Datenerhebung insoweit unzulässig.“

In Art. 34c PAG, der die allgemeinen Verfahrensregelungen, Verwendungsverbote, Zweckbindung, Benachrichtigung und Löschung für die Datenerhebung und Verarbeitung enthält, wurde in Abs. 4 Satz 4 folgende Kernbereichsregelung neu eingefügt (Einfügung fett und kursiv gedruckt):

„(4)

³Daten, bei denen sich nach Auswertung herausstellt, dass

3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben,

dürfen nicht verwendet werden. ⁴Dies gilt nicht, wenn ihre Verwendung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich ist **und Daten im Sinn der Nr. 2 oder 3 nicht betroffen sind.** ⁵In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich nachzuholen; Art. 34 Abs. 4 Satz 2 findet entsprechende Anwendung.“

In Art. 34d PAG, der neu den verdeckten Zugriff auf informationstechnische Systeme regelt, gibt es folgende kernbereichsschützende Regelungen:

In Abs. 1 Sätze 5 und 6:

„⁵Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, hat die Polizei durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. ⁶Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Maßnahme insoweit unzulässig.“

In Abs. 4 Satz 1 Nr.1:

„¹Bestehen bei der Durchsicht der Daten Anhaltspunkte dafür, dass Daten
1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
sind diese unverzüglich zu löschen oder dem für die Anordnung nach Abs. 1 zuständigen Richter zur Entscheidung über ihre weitere Verwendung vorzulegen. ²Bei Gefahr im Verzug kann die Entscheidung auch eine in Art. 33 Abs. 5 Satz 1 genannte Stelle treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. ³Die Löschung ist zu dokumentieren.“

In Abs. 5 Satz 3 Nr. 3 und Satz 4:

„³Daten bei denen sich nach der Auswertung herausstellt, dass
3. sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit anderen Berufsgeheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nr. 1 und 2 genannten Gefahren oder Straftaten haben,
dürfen nicht verwendet werden. ⁴Dies gilt nicht, wenn ihre Verwendung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist und Daten im Sinn der Nr. 2 oder 3 nicht betroffen sind.“

In Abs. 6 Satz 1:

„¹Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren.“

2) Die verfassungsrechtlichen Vorgaben für den Kernbereichsschutz bei verdeckten Datenerhebungen

(a) Die Absolutheit des Kernbereichsschutzes

Heimliche Ermittlungsmaßnahmen sind nur dann verfassungsrechtlich zulässig, wenn bei ihrem Einsatz der Kernbereich privater Lebensgestaltung absolut geschützt bleibt. Seit dem Elfes-Urteil geht das BVerfG in ständiger Rechtsprechung mit Blick auf die Menschenwürde davon aus, „dass dem einzelnen Bürger eine Sphäre privater Lebensgestaltung verfassungskräftig vorbehalten ist, also ein letzter unantastbarer Bereich menschlicher Freiheit besteht, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist“ (BVerfGE 6, 32, 41, zuletzt, Urteil vom 27.02.2008, Az. 1 BvR 370/07 u. 1 BvR 595/07, unter Hinweis auf BVerfGE 34, 238, 245 und 109, 279, 313). Aus der Absolutheit des Kernbereichsschutzes folgt, dass ein Eingriff in den Kernbereich nicht zu rechtfertigen ist. Deshalb trifft den Gesetzgeber eine Schutzpflicht zur Vermeidung von Eingriffen in den Kernbereich privater Lebensgestaltung.

(b) Das 2-stufige Schutzkonzept

Das BVerfG fordert seit seinem Lauschangriffsurteil (BVerfGE 109, 279, 309 ff.) ein sog. „2-stufiges Schutzkonzept“ (zuletzt BVerfG, NJW 2008, 822 ,833; ausführlich zu diesen zwei Kategorien von „Schutzschilden“ gegen heimlichen Ermittlungsmaßnahmen Zöller, StraFo 2008, 15 ,18 ff.). Danach werden auf der ersten Stufe Vorkehrungen gefordert, die schon im Vorhinein die Verletzung des Kernbereichs verhindern sollen. Dagegen sollen auf der zweiten Stufe bestimmte Regelungen die Kompensation eingetretener Kernbereichsverletzungen gewährleisten (Zöller, StraFo 2008, 15, 23 f.). Deutlich festgestellt wurde dies zuletzt im Online-Durchsuchungs-Urteil: „Ist es – wie bei dem heimlichen Zugriff auf ein informationstechnisches System – praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. [...] In vielen Fällen wird sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären lassen“ (BVerfG, NJW 2008, 822, 834).

Dass das BVerfG Kompensationsmaßnahmen auf der zweiten Stufe für erforderlich hält, macht deutlich, dass die vom Gericht anerkannte Absolutheit des Schutzes insofern durchbrochen wird, als dass Kernbereichsverletzungen scheinbar in Kauf genommen werden.

Daraus entsteht das Dilemma, dass man bei heimlichen Maßnahmen oft erst sicher wissen kann, ob ein Sachverhalt dem Kernbereich zuzuordnen ist, wenn man ihn kennt, die Kenntnisnahme aber bereits die Verletzung dieses Bereichs bedeutet (so bereits das Sondervotum in BVerfGE 109, 279, 383). Gleichwohl kann man nicht von einer naturgesetzlich vorgegebenen „Unvermeidbarkeit“ von Kernbereichsverletzungen ausgehen, sondern muss bereits auf der ersten Stufe entsprechende Schutzmaßnahmen ergreifen. Geschieht dies nicht bzw. ist dies gänzlich unmöglich, sind die den Kernbereich gefährdenden heimlichen Datenerhebungsbefugnisse mit dem Grundgesetz unvereinbar (so die Schlussfolgerung der Richterinnen Hohmann-Dennhardt und Jaeger im Sondervotum zum Lauschangriffsurteil, BVerfGE 109, 279, 382 ff.).

(c) Die Einheitlichkeit des Schutzstandards für den Kernbereich privater Lebensgestaltung bei Neuregelungen zur verdeckten Datenerhebung

Ausgangspunkt der Überlegungen zum Kernbereich privater Lebensgestaltung ist die Erkenntnis, dass alle heimlichen Maßnahmen staatlicher Stellen diesen zu verletzen imstande sind und deshalb dafür Sorge zu tragen ist, dass ihre Anwendung Art. 1 Abs. 1 GG nicht verletzt. Im Rahmen aller heimlichen Zugriffe auf Personen, auf deren persönliche Daten bzw. auf deren informationstechnische Systeme besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind. Deshalb genießen tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente ebenso wie etwa schriftliche Verkörperungen des höchstpersönlichen Erlebens einen absoluten Schutz (dazu BVerfGE 80, 367, 373 ff.; 109, 279, 319; BVerfG NJW 2008, 822, 833).

Das BVerfG hat dabei deutlich gemacht, dass die Frage des Kernbereichsschutzes keine (allein) an einzelnen Erhebungsmethoden oder Ermittlungskonstellationen festzumachende Problematik ist, sondern dass dieser Kernbereich umfassend Geltung gegenüber sämtlichen heimlichen Ermittlungsmaßnahmen präventiver wie repressiver (hierzu Lindemann, JR 2006, 191) Natur beansprucht. Überzeugend ist deshalb der Vorschlag von Zöller, den Kernbereichsschutz bei heimlichen strafprozessualen Maßnahmen „in einer allgemeinen, vor die Klammer gezogenen Norm“ zu regeln (StraFo 2008, 15, 22). Für die verfassungsrechtliche Prüfung der gerügten bayerischen Gesetze kann ebenso einheitlich vorgegangen werden. Die einzelnen kernbereichsschützenden Normen müssen einheitlich am Maßstab des Art. 1 Abs. 1 GG gemessen werden, d.h. auch einheitlich bezüglich ihres Schutzkonzeptes verfassungsrechtlich bewertet werden.

3) Die Verfassungswidrigkeit der neuen Kernbereichsregelungen

(a) Keine ausreichende Regelung von Anhaltspunkten für eine drohende Kernbereichsverletzung (unzureichendes Schutzkonzept auf der ersten Stufe)

Bereits auf der ersten Stufe müssen hinreichend konkrete Schutzregelungen erfolgen, damit der Kernbereich in der Lebenswirklichkeit geschützt bleibt. So hat das BVerfG im Urteil vom 27.02.2008 zuletzt festgestellt: Damit die Erhebung kernbereichsrelevanter Daten möglichst unterbleibe, seien „verfügbare informationstechnische Sicherungen einzusetzen“. Und weiter führt der Senat aus: „Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben.“ (BVerfG, NJW 2008, 822, 834) Daraus ergibt sich für den Gesetzgeber die Verpflichtung, ausreichend bestimmt diejenigen Anhaltspunkte zu regeln, bei deren Vorliegen regelmäßig eine Berührung des Kernbereichs droht. Zugleich muss der Gesetzgeber an das Vorliegen dieser Anhaltspunkte die Rechtsfolge knüpfen, die Datenerhebung zu unterlassen. Nur wenn der Gesetzgeber einerseits hinreichend konkret Anhaltspunkte aufzeigt, bei deren Vorliegen eine Verletzung des Kernbereiches droht und andererseits daran die Rechtspflicht knüpft, die Datenerhebung zu unterlassen, genügt er der Absolutheit des Kernbereichsschutzes. Besonders deutlich hat dies das BVerfG im Lauschangriffsurteil gemacht, wo es sich eingehend mit den Faktoren befasst hat, welche für eine Kernbereichsverletzung sprechen. Das BVerfG hat in dieser Entscheidung zum einen die Anwesenheit von Personen des höchstpersönlichen Vertrauens, zum anderen eine vertrauliche räumliche Situation als Anhaltspunkte für eine drohende Kernbereichsverletzung durch die akustische Wohnraumüberwachung herausgearbeitet (BVerfGE 109, 279, 320 ff.). Zu den Personen des höchstpersönlichen Vertrauens seien enge persönliche Freunde und engste Familienangehörige des Betroffenen sowie einige der nach § 53 StPO zur Zeugnisverweigerung Berechtigten, wie etwa der Geistliche und im Einzelfall auch der Strafverteidiger, zu zählen. Die Privatwohnung könne, mit Blick auf den Faktor der vertraulichen räumlichen Situation, als typischerweise dem Einzelnen als Rückzugsort dienender Bereich die Vermutung kernbereichsrelevanter Vorgänge in Anspruch nehmen. Dagegen fehle den Geschäfts- und Betriebsräumen regelmäßig diese Vertraulichkeit und Geborgenheit.

Diesen Kriterien lassen sich auch allgemeine Hinweise auf Anhaltspunkte entnehmen, bei denen mit einer drohenden Kernbereichsverletzung bei anderen heimlichen Datenerhebungsmaßnahmen zu rechnen ist (hierzu bei der Online-Durchsuchung Warntjen, Jura 2007, 581, 583 ff; auch die Beispiele bei Jahn/Kudlich, JR 2007, 57, 59).

Der Gesetzgeber des BayVSG und des PAG hat bei seinen Neuregelungen des Kernbereichsschutzes für die Online-Durchsuchung (Art. 6e Abs. 1 Satz 6 und 7 BayVSG, Art. 34d Abs. 5 PAG), für Datenerhebungseingriffe in den Telekommunikationsbereich (Art. 34a Abs. 1 Satz 4 PAG) und für den Einsatz technischer Mittel im Schutzbereich des Art. 13 GG (Art. 6a Abs. 3 Satz 2 BayVSG) versucht, auf der ersten Stufe ein Schutzkonzept für den Kernbereich privater Lebensgestaltung zu schaffen. Für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes nach Art. 6d BayVSG enthält Art. 6f Abs. 4 Satz 2 Nr. 3 BayVSG keine kernbereichsschützenden Regelungen, die einem Schutzkonzept auf der ersten Stufe zuzurechnen sind. Diese Regelungen setzen vielmehr sofort bei der Auswertung der gewonnenen Daten, also auf der zweiten Stufe an. Da der Gesetzgeber zu recht davon ausgeht, dass auch bei Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes der Kernbereich privater Lebensgestaltung verletzt werden kann, hat er es verfassungswidrig versäumt, ein Schutzkonzept für die erste Stufe zu entwickeln.

Aber auch bei seinen Neuregelungen des Kernbereichsschutzes für die Online-Durchsuchung (Art. 6e Abs.1 Satz 6 und 7 BayVSG, Art. 34d Abs. 5 PAG), für Datenerhebungseingriffe in den Telekommunikationsbereich (Art. 34a Abs. 1 Satz 4 PAG) und für den Einsatz technischer Mittel im Schutzbereich des Art. 13 GG (Art. 6a Abs. 3 Satz 2 BayVSG) genügt der Gesetzgeber dem geforderten Schutzniveau aus Art. 1 Abs. 1 GG nicht. Durchgängig hat er nicht hinreichend konkrete Anhaltspunkte aufgezeigt, bei deren Vorliegen eine Verletzung des Kernbereiches droht, sondern überlässt es dem Rechtsanwender, solche Anhaltspunkte selbstständig festzustellen. Insofern genügt er der Absolutheit des Kernbereichsschutzes mit seinen Neuregelungen nicht. Im Falle der kernbereichsschützenden Regelungen für die Online-Durchsuchung (Art. 6e Abs. 1 Satz 6 und 7 BayVSG, Art. 34d Abs. 5 PAG) hat er lediglich die abstrakte Feststellung des BVerfG aus dem Urteil vom 27.02.2008 in den Gesetzestext übernommen, wonach, „soweit dies informationstechnisch und ermittlungstechnisch möglich ist, durch geeignete Vorkehrungen sicherzustellen“, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Anhaltspunkte bei deren Vorliegen die Maßnahme zu unterbleiben hat, hat der Gesetzgeber nicht formuliert. Noch stärker wird der verfassungsrechtlich gebotene Schutzstandard der ersten Stufe für die Kernbereichsdaten bei Datenerhebungseingriffen im Telekommunikationsbereich (Art. 34a Abs. 1 Satz 4 PAG) unterschritten. Erst wenn erkennbar wird, dass Kernbereichsdaten betroffen sind, soll die Datenerhebung unzulässig sein. Damit wird zu spät angesetzt. Auf Anhaltspunkte zu achten, die von vornherein die Maßnahme ausschließen, wird hier nicht einmal mehr dem Ermittler bzw. dem Anordnenden der Maßnahme aufgetragen.

(b) Unzureichende Bestimmtheit der Regelungen über das „Vortäuschen kernbereichszugehöriger Kommunikation zur Überwachungsverhinderung“

Anknüpfend an die Pflicht, bei Anhaltspunkten für eine Berührung des Kernbereichs die Datenerhebung zu unterlassen, hat das BVerfG im Urteil vom 27.02.2008 zur Online-Durchsuchung ausgeführt: „Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.“ (BVerfG, NJW 2008, 822, 834). Soweit also die Ermittler den durch konkrete Anhaltspunkte begründeten Verdacht haben, dass die überwachte Kommunikation bzw. die überwachten Sachverhalte nur scheinbar kernbereichszugehöriger Natur sind, sie vielmehr absichtlich diesen Anschein erwecken sollen, um die Überwachung zu verhindern, soll die Datenerhebung nicht unterbleiben und auch nicht abgebrochen werden müssen. Mit dem BVerfG kann davon ausgegangen werden, dass in diesen Situationen selbstverständlich keine kernbereichszugehörigen Vorgänge stattfinden, so dass eine Überwachung – bei Einhaltung der sonstigen tatbestandlichen Voraussetzungen – legitim und nicht unzulässig ist. Allerdings muss auch für diese Fälle der Gesetzgeber dafür Sorge tragen, dass die Regelung hinreichend bestimmt ist. Tatsächlich hat der bayerische Gesetzgeber die Urteilspassage ohne weitere Konkretisierung in die neu geregelten Kernbereichsnormen für die Online-Durchsuchung (Art. 6e Abs. 1 Satz 6 und 7 BayVSG, Art. 34d Abs. 5 PAG), für Datenerhebungseingriffe in den Telekommunikationsbereich (Art. 34a Abs. 1 Satz 4 PAG) und für den Einsatz technischer Mittel im Schutzbereich des Art. 13 GG (Art. 6a Abs. 3 Satz 2 BayVSG) einfach nur abgeschrieben. Damit hat der Gesetzgeber unter einfacher Feststellung auf die vom BVerfG abstrakt ausgemachte Gefahr eines nur vorgetäuschten Kernbereichsbezugs eine Blankettnorm geschaffen. Unter Berufung auf diese Normen kann nun faktisch jede Ermittlungsmaßnahme auch bei Anhaltspunkten für einen dem Kernbereich zuzuordnenden Sachverhalt fortgesetzt werden. So hat der Gesetzgeber z. B. sich weder die Mühe gemacht, Regelbeispiele für den Rechtsanwender vorzugeben, noch hat er entsprechende Verfahrenssicherungen in die Gesetze aufgenommen. Auf diese Weise verletzt er seine von Art. 1 Abs. 1 GG gebotene Schutzpflicht.

(c) Verfassungsrechtlich unzureichendes Schutzkonzept auf der zweiten Stufe

Im Anschluss an eine Kernbereichsverletzung sind auf der zweiten Stufe des Kernbereichsschutzes vom Gesetzgeber Lösungs- und Benachrichtigungspflichten sowie ein umfassendes Verwertungsverbot für erhobene Kernbereichsdaten zu regeln. Diesbezüglich hat der bayerische Gesetzgeber unterschiedliche Schutzniveaus geschaffen, die die verfassungsrechtlich gebotene Einheitlichkeit des Schutzniveaus verletzen.

| Eingriffsbefugnis nach | Löschungspflicht für erhobene Kernbereichsdaten | Verwertungsverbot von erhobene Kernbereichsdaten | Benachrichtigungspflichten über erhobene Kernbereichsdaten | Pflicht zur Lifeüberwachung und Pflicht zum Abbruch |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------|
| Einsatz technischer Mittel im Schutzbereich des Art. 13 GG, Art. 6a BayVSG und Art. 34 PAG | Art. 6b Abs. 3 Satz 1 BayVSG | Art. 6b Abs. 2 Satz 5 Nr. 3 BayVSG und Art. 34 Abs. 5 Satz 3 PAG | | Art. 6a Abs. 3 Satz 2 BayVSG |
| Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes, Art. 6d BayVSG | Art. 6f Abs. 4 Satz 3 BayVSG | Art. 6f Abs. 4 Satz 2 Nr. 3 BayVSG | | |
| Onlinedurchsuchungen, Art. 6e BayVSG und 34d PAG | Art. 6f Abs. 5 Satz 3 BayVSG und 34d Abs. 4 Satz 1 Nr. 3 PAG | Art. 6f Abs. 4 Satz 2 Nr. 3 BayVSG und 34d Abs. 5 Satz 3 Nr. 3 und Satz 4 PAG | Art. 6f Abs. 5 Satz 1 BayVSG unter Verweis auf Art. 6b Abs. 4 BayVSG und 34d Abs. 7 PAG | |
| Überwachung der Telekommunikation, Art. 34a PAG | | Art. 34c Abs. 4 Satz 3 Nr. 3, Satz 4 PAG | | |

Zusammenfassend lässt sich feststellen, dass die Neuregelungen für Kernbereichsdaten, die beim Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes nach Art. 6d BayVSG und bei Eingriffe in den Telekommunikationsbereich nach Art. 34a PAG erhoben wurden, nicht dem vom Verfassungsgericht geforderten Schutzniveau der zweiten Stufe entsprechen.