Bayerischer Landtag
15. Wahlperiode

Drucksache 15/**10345**
02.04.2008

Änderungsantrag

der Abgeordneten **Georg Schmid, Dr. Jakob Kreidl, Peter Welnhofer, Herbert Ettengruber, Joachim Haedke, Hans Herold, Thomas Kreuzer, Christian Meißner, Thomas Obermeier, Rudolf Peterke, Angelika Schorer, Helga Weinberger, Dr. Manfred Weiß, Peter Winter, Otto Zeitler CSU**

zum Gesetzentwurf der Staatsregierung zur Änderung des Polizeiaufgabengesetzes
(Drs. 15/9460)

Der Landtag wolle beschließen:

1. § 1 wird wie folgt geändert:

   a) Die Anführung erhält folgende Fassung:

   „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 § 2 des Gesetzes vom 20. Dezember 2007 (GVBl S. 944), wird wie folgt geändert:“

   b) Nach der Anführung werden folgende Nrn. 1 bis 7 eingefügt:

   „1. In die Inhaltsübersicht werden folgende Art. 34d und 34e eingefügt:

   „Art. 34d
   Verdeckter Zugriff
   auf informationstechnische Systeme

   Art. 34e
   Notwendige Begleitmaßnahmen“

   2. Art. 34 wird wie folgt geändert:

      a) Abs. 1 Satz 1 wird wie folgt geändert:

         aa) In Nr. 1 werden die Worte „oder für Sachen, soweit eine gemeine Gefahr besteht,“ gestrichen.

         bb) In Nr. 2 werden nach dem Wort „Straftat“ die Worte „nach Art. 30 Abs. 5 Satz 1 Nrn. 1 bis 9“ eingefügt.

      b) In Abs. 5 Satz 5 werden die Worte „ein in Art. 33 Abs. 5 Sätze 1 und 2 genannter Dienststellenleiter“ durch die Worte „eine in Art. 33 Abs. 5 Sätze 1 und 2 genannte Stelle“ ersetzt.

   3. In Art. 34b Abs. 3 werden nach den Worten „erfasst werden,“ die Worte „einschließlich der nach § 113a des Telekommunikationsgesetzes gespeicherten Daten,“ eingefügt.

   4. Art. 34c wird wie folgt geändert:

      a) In Abs. 1 wird das Wort „Dienststellenleiter“ durch das Wort „Stellen“ ersetzt.

      b) In Abs. 4 Satz 2 Nr. 2 werden die Worte „Satz 1“ durch die Worte „Abs. 2“ ersetzt.

   5. Es werden folgende Art. 34d und 34e eingefügt:

   „Art. 34d
   Verdeckter Zugriff
   auf informationstechnische Systeme

   (1) [1]Die 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 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.

   [2]Daten dürfen unter den Voraussetzungen des Satzes 1 auch gelöscht oder verändert werden, gespeicherte Daten 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. [3]Eine 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. [4]Wird 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 oder ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. [5]Soweit 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. [6]Wird 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. [7]Maßnahmen nach den Sätzen 1 und 2 sind zu dokumentieren.

(2) [1]Die 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.

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

(3) [1]Art. 34 Abs. 4 Sätze 1 und 2 gelten entsprechend. [2]Bei 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. [3]Die Anordnung von Maßnahmen nach Abs. 1 und 2 ist schriftlich zu erlassen und zu begründen. [4]Die 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. [5]In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. [6]Die Anordnung ist auf höchstens drei Monate zu befristen. [7]Eine Verlängerung um jeweils nicht mehr als einen Monat ist möglich, soweit die Voraussetzungen fortbestehen. [8]Bestehen die in den Abs. 1 und 2 bezeichneten Voraussetzungen nicht fort, ist die Maßnahme unverzüglich zu beendigen; die Beendigung ist dem Richter mitzuteilen.

(4) [1]Bestehen 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. [2]Bei Gefahr in 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. [3]Die Löschung ist zu dokumentieren.

(5) [1]Die durch eine Maßnahme nach den Abs. 1 und 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. [2]Sie 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.

[3]Daten, 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 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. [4]Art. 34c Abs. 4 Sätze 4 und 5 gelten entsprechend.

(6) [1]Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren. [2]Die 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. [3]Art. 34 Abs. 7 Sätze 3 und 4 gelten entsprechend.

(7) [1]Von 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.

[2]Die 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. [3]Art. 34 Abs. 6 Sätze 2 bis 6 gelten entsprechend.

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

Art. 34e
Notwendige Begleitmaßnahmen

[1]Zur 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. [2]Für 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.“

6. In Art. 36 Abs. 3 Satz 1 werden die Worte „die in Art. 33 Abs. 5 genannten Dienststellenleiter“ durch die Worte „eine in Art. 33 Abs. 5 Sätze 1 und 2 genannte Stelle“ ersetzt.
7. Art. 44 erhält folgende Fassung:“

c) Es wird folgende Nr. 8 angefügt:

„8. In Art. 46 Abs. 2 Satz 2 werden die Worte „einer Anordnung der in Art. 33 Abs. 5 genannten Dienststellenleiter“ durch die Worte „der Anordnung einer in Art. 33 Abs. 5 Sätze 1 und 2 genannten Stelle“ ersetzt.“

2. Es wird folgender neuer § 2 eingefügt:

„§ 2

Durch dieses Gesetz wird in das Fernmeldegeheimnis nach Art. 10 des Grundgesetzes, Art. 112 Abs. 1 der Verfassung und das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 des Grundgesetzes, Art. 106 Abs. 3 der Verfassung eingegriffen.“

3. Der bisherige § 2 wird § 3.

Begründung:

Mit der Festnahme von Mitgliedern der „Islamic Jihad Union“ im September 2007 ist den Sicherheitsbehörden ein wichtiger Schlag gegen eine in Deutschland ansässige Terrorzelle gelungen. Konkret geplante Sprengstoffanschläge mit furchtbaren Folgen wurden abgewehrt. Diese Anschlagsplanungen haben nach den misslungenen Kofferbombenanschlägen von Köln im Jahr 2006 noch einmal deutlich gezeigt, dass die Bundesrepublik Deutschland nicht nur Rückzugsraum für den islamistischen Terrorismus ist. Vielmehr zählt Deutschland zu möglichen Anschlagszielen. Die Terroristen hätten dabei in menschenverachtender Art und Weise den Tod einer Vielzahl unschuldiger Opfer in Kauf genommen. Die aufgedeckten Terroranschläge haben zudem die internationale Vernetzung der Terrorzellen offen gelegt und verdeutlicht, dass die Attentäter hochkonspirativ arbeiten und modernste Technik nutzen, um sich systematisch gegen den Zugriff der Sicherheitsbehörden abzuschotten. Herkömmliche Ermittlungsmethoden unter Einsatz polizeilicher Standardmaßnahmen stoßen dabei schnell an ihre Grenzen.

Die Arbeit der Ermittlungsbehörden wird immer stärker von den neuen Technologien bestimmt. Internet, Miniaturisierung der Technologien, die nahezu grenzenlose Erhöhung des Speichervolumens und die Schnelligkeit der Informationsverarbeitung und -verbreitung haben sich auch Straftäter nutzbar gemacht. Islamistische Extremisten verbreiten im Internet ihre Propaganda oder

drohen Terroranschläge an, detaillierte Bombenbauanleitungen werden für jedermann zugänglich eingestellt, Amokläufe werden angedroht und einschlägige Foren und Tauschbörsen bieten einen Tummelplatz für Pädophilie zur Vorbereitung des sexuellen Missbrauchs von Kindern sowie zur Verbreitung inkriminierter kinderpornografischer Darstellungen.

Der Trend zur Professionalisierung des Kommunikationsverhaltens des polizeilichen Gegenübers ist unübersehbar und erschwert zunehmend sowohl die präventivpolizeiliche Gefahrenabwehr als auch die Strafverfolgung. Deutlich zeigte sich dies bei den Ermittlungen, die schließlich zur Festnahme von Mitgliedern der „Islamic Jihad Union“ im September 2007 führten. Es gibt deutliche Hinweise, dass die Beschuldigten gezielt bezüglich ihres Kommunikationsverhaltens geschult wurden. Es ist davon ausgehen, dass die Kenntnisse der Täter hinsichtlich neuester Technologien bzw. Kommunikationsmittel weiter zunehmen werden. Hierbei steht zu befürchten, dass die frei zugänglichen, höchst wirksamen Kryptierungsverfahren, die Anonymisierung und Zugangssicherung (z. B. durch die Verschleierung von IP-Adressen oder die Verwendung von Passwörtern) die klassischen polizeilichen Ermittlungsinstrumentarien zur Informationserhebung und Beweissicherung künftig weitgehend ins Leere laufen lassen.

So reicht etwa die herkömmliche offene physische Beschlagnahme von Computern oder Festplatten gerade im Bereich des Terrorismus, aber auch bei anderen hoch konspirativen kriminellen Netzwerken, nicht mehr aus, um dringende Gefahren oder schwerwiegende Straftaten abzuwehren. Die Beschlagnahme führt oftmals dazu, dass Mittäter gewarnt werden, da die polizeilichen Maßnahmen offen erfolgen. Vor allem im Zusammenhang mit terroristischen Attentaten kann dies fatale Folgen haben. Darüber hinaus ist – anders als noch vor wenigen Jahren – aufgrund der fortschreitenden Technisierung nicht mehr gewährleistet, dass die Daten nach einer Beschlagnahme ausgewertet werden können. Insbesondere der Fortschritt auf dem Gebiet der Verschlüsselungstechniken bereitet zum Teil unüberwindbare Hindernisse bei der Datenauswertung. Mit fortschreitender technischer Entwicklung wird sich diese Problematik noch ganz erheblich verschärfen.

Vor diesem Hintergrund ist im Einzelfall der Einsatz technischer Mittel zum verdeckten Zugriff auf informationstechnische Systeme notwendig, um Gefährdungslagen für überragend wichtige Rechtsgüter, wie Leib, Leben und Freiheit, rechtzeitig erkennen und Täter- und Tatstrukturen soweit aufklären zu können, dass offene Maßnahmen ohne Gefährdung des Ermittlungserfolges ermöglicht werden.

Das Bundesverfassungsgericht anerkennt in diesem Zusammenhang die Notwendigkeit staatlichen Handelns. In seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, führt das Gericht in Absatz-Nr. 220 aus: „Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen (vgl. BVerfGE 49, 24 <56 f.>; 115, 320 <346>). Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG (vgl. BVerfGE 115, 118 <152>). Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschließen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen (vgl. zur Strafverfolgung BVerfGE 115, 166 <193>).“

Der verdeckte Einsatz von technischen Mitteln, um auf informationstechnische Systeme zugreifen und Zugangsdaten und gespeicherte Daten erheben sowie im Einzelfall zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person auch auf dem Zielrechner löschen und verändern zu können, zählt angesichts des rasanten technischen Fortschritts zu den unverzichtbaren Instrumenten der Polizei zum Schutz überragend wichtiger Rechtsgüter. Der Polizei muss daher auch in Zukunft das notwendige Instrumentarium zur Verfügung stehen, um in hoch konspirative kriminelle Netze eindringen zu können und drohende Gefahren für überragend wichtige Rechtsgüter effektiv abwehren zu können. Andernfalls besteht aufgrund des schnellen Fortschrittes in der Informationstechnologie und der steigenden Konspirativität der Täter die Gefahr unverantwortbarer Sicherheitslücken und de facto rechtsfreier Räume. Dies ist vor dem Hintergrund der Abwehr dringender Gefahren für überragend wichtige Rechtsgüter und schwerwiegender Straftaten nicht akzeptabel.

Ziel des Änderungsantrags ist es, Umfang und Qualität der bisherigen Instrumente zur verdeckten Datenerhebung auch unter den erheblich verschlechterten Ausgangsbedingungen zumindest teilweise zu erhalten. Die durch die moderne Technik verursachten Erschwernisse für die Gefahrenabwehr sollen in Teilen kompensiert werden. Im Vordergrund steht nicht die Ausweitung der Überwachungsbefugnisse, sondern die Schaffung von Ausgleichsmaßnahmen, um auch künftig dringende Gefahren effektiv abwehren zu können. Hierfür bedarf es einer Anpassung des Bayerischen Polizeiaufgabengesetzes (PAG).

Darüber hinaus bedarf es einer Ergänzung des Polizeiaufgabengesetzes infolge des mit Wirkung vom 1. Januar 2008 geänderten Telekommunikationsgesetzes (TKG), das in § 113b TKG nunmehr eine landesrechtliche Zitierklausel fordert, um Telekommunikationsverkehrsdaten nicht nur im Bereich der Strafverfolgung, sondern auch zur Gefahrenabwehr verwenden zu können.

Außerdem erfolgen redaktionelle Klarstellungen bei den Anordnungskompetenzen für bestimmte Maßnahmen, die infolge der Änderung von Art. 33 Abs. 5 PAG durch das Gesetz zur Änderung des Polizeiorganisationsgesetzes vom 21. Dezember 2007 (GVBl S. 944) notwendig wurden.

Zu § 1 Buchstabe b):

Nr. 1

Es handelt sich um eine redaktionelle Änderung.

Nr. 2

Buchstabe a)

Bei der Wohnraumüberwachung nach Art. 34 soll die bislang in Nr. 1 enthaltene „gemeine Sachgefahr“ künftig nicht mehr als Eingriffsanlass ausreichen. Anlasstaten nach Nr. 2 sind künftig nur noch schwerwiegende Straftaten im Sinne von Art. 30 Abs. 5 Satz 1 Nr. 1 bis 9. Damit werden die Anordnungsvoraussetzungen der Wohnraumüberwachung mit denen der Online-Durchsuchung im neuen Art. 34d harmonisiert.

Buchstabe b)

Im Zuge der Novelle des Polizeiorganisationsgesetzes zur Umsetzung der Polizeiorganisationsreform wurde auch Art. 33 Abs. 5 geändert. Die dort bisher normierte Anordnungskompetenz wurde auf die Leiter der Polizeipräsidien und den Leiter des Landeskriminalamts reduziert, wobei jedoch in Satz 2 eine Delegationsmöglichkeit auf Beamte des höheren Polizeivollzugsdienstes eröffnet wurde. Für die Anordnungskompetenz zur Verwendung von Daten aus der Wohnraumüberwachung bei Gefahr im Verzug verweist Art. 34 Abs. 5 Satz 5 in der bisherigen Fassung auf die in Art. 33 Abs. 5 Satz 1 und 2 genannten „Dienststellenleiter“. Mit der Änderung wird klargestellt, dass bei Gefahr im Verzug auch die nach Art. 33 Abs. 5 Satz 2 besonders hierzu beauftragten Beamten des höheren Dienstes anordnungsbefugt sind.

Nr. 3

Die präventive Telekommunikationsüberwachung hat sich seit ihrer Einführung im PAG im Jahr 2006 als wirksame Maßnahme erwiesen, die zur Gefahrenabwehr und zum Schutz hochrangiger Rechtsgüter unverzichtbar ist. Dies gilt insbesondere für die Vermisstensuche. Das Instrument ist aber auch im Zusammenhang mit dem Kampf gegen die Organisierte Kriminalität und der Terrorbekämpfung unverzichtbar. Bei der Aufdeckung der Terrorzelle der „Islamischen Jihad Union“ im September 2007 und der Verhinderung furchtbarer Anschläge in Deutschland hat sich erneut gezeigt, dass die Ermittlungsbehörden die präventive Telekommunikationsüberwachung zur Abwehr schwerwiegender Straftaten und dringender Gefahren unbedingt benötigen. Die nach Auskunft des Staatsministeriums des Innern relativ geringe Zahl von Inhaltsüberwachungen belegt dabei, dass die Polizei nur in ausgewählten Fällen und unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes von dieser Befugnis Gebrauch macht.

Die Erhebung von Inhaltsdaten, die Ortung von Telekommunikationsendgeräten und die Verkehrsdatenerhebung sind aus dem polizeilichen Instrumentarium zum Schutz bedeutender Rechtsgüter, wie Leib, Leben und Freiheit, heute nicht mehr wegzudenken. Für die effektive Gefahrenabwehr sind sie unverzichtbar.

Der Bundesgesetzgeber hat durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. S. 3198) mit Wirkung vom 1. Januar 2008 Mindestspeicherfristen für Verkehrsdaten in § 113a des Telekommunikationsgesetzes (TKG) eingeführt sowie in § 113b TKG Übermittlungspflichten geregelt. Das Bundesverfassungsgericht hat im Beschluss vom 11. März 2008, Az.: 1 BvR 256/08 eine Aussetzung des Vollzugs von § 113a TKG abgelehnt (BVerfG, a.a.O, Absatz-Nr. 147 ff.). § 113b Satz 1 Nr. 1 TKG, der die Übermittlung von Verkehrsdaten zur Verfolgung von Straftaten regelt, wurde teilweise für die Fälle außer Kraft gesetzt, in denen die Daten nicht zur Verfolgung solcher Straftaten benötigt werden, anlässlich derer auch eine Telekommunikationsüberwachung nach § 100a Abs. 1 und 2 StPO hätte angeordnet werden dürfen. Die Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 bezieht sich ausschließlich auf die Verwendung der Verkehrsdaten für Strafverfolgungszwecke und nicht für die Verwendung im Gefahrenabwehrbereich. Nach § 113b Satz 1 Nr. 2 TKG dürfen Verkehrsdaten auch zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit an die zuständigen Stellen übermittelt werden, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a TKG vorgesehen ist. Der Begriff der erheblichen Gefahr in § 113b Satz 1 Nr. 2 TKG stimmt mit dem der dringenden Gefahr, wie er im PAG verwendet wird, überein (so Schmidbauer/Steiner, PAG, 2. Auflage, Art. 11 Rd.-Nr. 48 f., auf den die Gesetzesbegründung ausdrücklich verweist, dazu BT-Drs. 16/5846, S. 74). Da der Zugriff auf Telekommunikationsverkehrsdaten gemäß Art. 34a Abs. 1 Satz 1 bzw. Abs. 3 Satz 1 i.V.m. Art. 34b Abs. 2 Satz 1 nur zur Abwehr erheblicher Gefahren zulässig ist, wäre eine Datenübermittlung durch das PAG an sich gedeckt. In § 113b Satz 1 TKG ist allerdings eine Zitierklausel vorgesehen, wonach das jeweilige Landesgesetz eine Bezugnahme auf § 113a TKG enthalten muss, an der es im PAG bisher fehlt. Obwohl der Bundesrat gefordert hat, diese Regelung ersatzlos zu streichen, ist dem der Deutsche Bundestag nicht gefolgt. In der Stellungnahme des Bundesrates (BT-Drs. 16/5846, S. 87 f.) wird dargelegt, dass die Zitierklausel unzweckmäßig ist und „zu erheblichen Sicherheitslücken sowie zu Wertungswidersprüchen führen“ kann.

Um künftig derartige Sicherheitslücken sowie drohende Wertungswidersprüche zu vermeiden und um den Erfordernissen eines effektiven Rechtsgüterschutzes zu genügen, wird eine entsprechende Zitierung in Art. 34b Abs. 3 eingefügt. Ohne diese dürften die Diensteanbieter der Polizei in Zukunft nur die Daten zur Abwehr dringender Gefahren übermitteln, die zu Abrechnungszwecken gespeichert wurden, nicht dagegen die auf der Grundlage des § 113a TKG gespeicherten Verkehrsdaten. Es käme daher bei der Gefahrenabwehr im Ergebnis entscheidend auf die Tarifgestaltung zwischen Diensteanbietern und Kunden an. Soweit eine pauschalierte Abrechnung vertraglich vereinbart wurde (sog. Flatrate-Tarife), dürfte selbst dann, wenn die Kenntnis von gespeicherten und damit vorhandenen Verkehrsdaten zur Abwehr von Lebensgefahren unerlässlich ist, keine Auskunft erteilt werden. Sogar in Vermisstenfällen, in denen die Gefahr dem Nutzer selbst droht, würde es an der ausdrücklichen Zitierung des § 113a TKG im PAG fehlen. Bei der Abwehr von erheblichen Gefahren kann die Art der Abrechnung von Telekommunikationsleistungen und die Frage, ob die vorhandenen Daten zu diesem Zweck oder auf der Grundlage des § 113a TKG gespeichert wurden, allerdings kein Kriterium dafür sein, ob die zur Gefahrenabwehr erforderlichen Daten an die Polizei übermittelt werden dürfen.

Die Einbeziehung der Daten, die aufgrund von § 113a TKG gespeichert werden, ist erforderlich, um die effektive Gefahrenabwehr künftig sicher zu stellen. Dies gilt insbesondere vor dem Hintergrund, dass die Verbreitung von Flatrate-Tarifen noch erheblich zunehmen wird. Mildere Mittel sind nicht ersichtlich, da die Daten nicht auf anderem Weg erlangt werden können. Die Regelung ist auch angemessen. Die Rechtsgüter, die in Art. 34a Abs. 1 Satz 1 Nr. 1 und Abs. 3 ausdrücklich bzw. in Abs. 1 Satz 1 Nr. 2 durch den Verweis auf die strafrechtlich geschützten Güter abschließend normiert sind, sind gewichtig genug, um den Eingriff in Art. 10 Abs. 1 GG zu rechtfertigen. Es handelt sich durchgehend um die hochrangigen Rechtsgüter, wie sie auch die Überwachung und Aufzeichnung der Telekommunikation voraussetzt (vgl. zur Strafverfolgung BVerfG, a.a.O., Absatz-Nr. 167 f.). Wenngleich sich der im einstweiligen Anordnungsverfahren ergangene Beschluss des Bundesverfassungsgerichts vom 11. März 2008 ausschließlich auf die Übermittlung der Verkehrsdaten im repressiven Bereich bezieht, entspricht die vorgesehene Regelung im PAG der Intention des Bundesverfassungsgerichts, wonach eine Übermittlungspflicht jedenfalls in den Fällen besteht, in denen auch eine Telekommunikationsüberwachung hätte angeordnet werden dürfen und somit ein Eingriff in Art. 10 GG gerechtfertigt wäre. Die Angemessenheit ergibt sich im Hinblick auf Art. 34a Abs. 3 nicht zuletzt daraus, dass die Datenerhebung gerade auch dem Schutz der Kunden selbst dienen kann. Die Übermittlung an die Polizei erfolgt zudem nur dann, wenn die Voraussetzungen von Art. 34a Abs. 1 Satz 1 bzw. Abs. 3 Satz 1, jeweils i.V.m. Art. 34b Abs. 2 Satz 1 vorliegen. Danach bedarf es einer konkreten Gefahr für die dort genannten, hochrangigen

Rechtsgüter. Die Voraussetzungen an die Anordnungskompetenz aus Art. 34c Abs. 1 und 2 sowie die Regelungen über Verwendung, Benachrichtigung und Löschung erhobener Daten gelten ebenfalls uneingeschränkt. Schließlich ist zu berücksichtigen, dass es sich nicht um Telekommunikationsinhalte, sondern um Verkehrsdaten handelt.

Nr. 4

Buchtstabe a)

Für die Anordnungskompetenz im Zusammenhang mit Maßnahmen der Telekommunikationsüberwachung verweist Art. 34c Abs. 1 in der bisherigen Fassung auf die in Art. 33 Abs. 5 Satz 1 und 2 genannten „Dienststellenleiter“. Mit der Änderung wird klargestellt, dass die in Art. 33 Abs. 5 Satz 1 und 2 genannten Stellen, einschließlich der besonders hierzu beauftragten Beamten des höheren Dienstes, anordnungsbefugt sind.

Buchstabe b)

Nach Art. 34 c Abs. 4 Satz 2 Nr. 2 dürfen präventiv erlangte Daten für Zwecke der Strafverfolgung verwendet werden, wenn sie zur Verfolgung von Straftaten im Sinn des § 100a Satz 1 StPO benötigt werden. § 100a Satz 1 StPO enthielt bislang die schweren Straftaten, zu deren Verfolgung eine Telekommunikationsüberwachung angeordnet werden darf. Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. S. 3198) wurde § 100a StPO dergestalt geändert, dass die Aufzählung der schweren Straftaten nunmehr in Absatz 2 enthalten ist. Insofern erfolgt die redaktionelle Anpassung an die bundesrechtliche Gesetzeslage.

Nr. 5

Mit der Vorschrift des Art. 34d wird der verdeckte Zugriff auf informationstechnische Systeme auf eine gesetzliche Grundlage gestellt. Der Änderungsantrag orientiert sich dabei an den verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, für den Schutz des vom allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfassten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgestellt hat. Er berücksichtigt ferner die vom Bundesverfassungsgericht bereits früher für Maßnahmen der verdeckten Datenerhebung aufgestellten Maßstäbe, insbesondere in den Entscheidungen vom 3. März 2004 zur akustischen Wohnraumüberwachung, Az. 1 BvR 2378/98, 1 BvR 1084/99, und zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz, Az. 1 BvF 3/92, sowie im Urteil vom 27. Juli 2005 zum niedersächsischen Sicherheits- und Ordnungsgesetz, Az.: 1 BvR 668/04. Der Grundrechtsschutz orientiert sich durchweg an den dargelegten Erfordernissen.

Die Befugnis ist in ihrer Systematik eng an die Befugnisse zur Wohnraumüberwachung nach Art. 34 PAG und zur Telekommunikationsüberwachung nach Art. 34a PAG angelehnt. Damit spiegelt sich bei den staatlichen Eingriffsbefugnissen im PAG die vom Bundesverfassungsgericht dargelegte Systematik auf der Grundrechtsseite wieder. Denn das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt 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. Februar 2008, a.a.O., Absatz-Nr. 167).

1. Ziel der Maßnahme ist der verdeckte Zugriff auf informationstechnische Systeme zur Erhebung von Daten, soweit dies für die Abwehr dringender Gefahren für überragend wichtige Rechtsgüter bzw. schwerwiegender Straftaten erforderlich ist. In Ausnahmefällen zur Abwehr einer gegenwärtigen Gefahr für die existentiellen Rechtsgüter Leib, Leben oder Freiheit der Person können gespeicherte Daten auf dem Zielsystem auch gelöscht oder verändert werden. Zielobjekt der Maßnahme sind stets informationstechnische Systeme. Nach der Definition des Bundesverfassungsgerichts (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 202 f.) sind darunter Systeme zu verstehen, „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.“ Auch solche Mobiltelefone und elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können, fallen darunter.

   Der Zugriff auf informationstechnische Systeme bedeutet, dass die notwendigen technischen Maßnahmen ergriffen werden, um eine Datenerhebung zu ermöglichen. Die Regelung unterscheidet zunächst zwischen Zugangsdaten und gespeicherten Daten. 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 wäre hiervon erfasst. Die Regelung ermöglicht der Polizei damit auch die Erfassung von Tastatureingaben, um dann später mit Hilfe des erhobenen Kennwortes auf kryptierte oder anderweitig vor Zugriff besonders geschützte Daten zugreifen zu können. Eine gesetzliche Regelung ist erforderlich, weil 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 Tatstatur (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 205). Der Einsatz von Keyloggern kann insbesondere notwendig sein, um später entweder die eigentlich zur Gefahrenabwehr erforderlichen Daten im Rahmen einer verdeckten Maßnahme zu erheben oder im Wege der offenen Sicherstellung die Datenträger, die gegen den Zugriff Dritter besonders gesichert sind, in Gewahrsam zu nehmen und auszuwerten. Angesichts der zunehmenden Verbreitung von im Internet als Freeware herunterladbarer Kryptier- bzw. Verschlüsselungsprogramme, ermöglicht die verdeckte Erhebung von Zugangsdaten eine nachfolgende offene Beschlagnahme und Auswertung des Speichermediums. Obwohl die Erfassung von Zugangsdaten gegenüber der Erhebung von gespeicherten Daten regelmäßig die weniger eingriffsintensive Maß-

nahme darstellen wird, gelten auch hier die gleich strengen Voraussetzungen. Werden nur Zugangsdaten erhoben, gelöscht oder verändert, so besteht keine Unterrichtungspflicht nach Abs. 8. Gespeicherte Daten sind sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten (vgl. BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 205).

Bei den Daten darf es sich um keine Telekommunikationsdaten handeln. Soweit sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, trifft Art. 34a eine Sonderregelung. Dies gilt auch für die sogenannte „Quellen-Telekommunikationsüberwachung“, soweit durch technische und rechtliche Vorgaben sichergestellt ist, dass die Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt ist. Dies wurde so vom Bundesverfassungsgericht bestätigt (vgl. BVerfG vom 27 Februar 2008, a.a.O., Absatz-Nr. 190). Entsprechendes gilt für die Wohnraumüberwachung. Soweit eine Überwachungsmaßnahme darauf abzielt, keine Zugangsdaten eines informationstechnischen Systems oder darin gespeicherte Daten, sondern Lebensäußerungen aus einer Wohnung zu erheben, ist Art. 34 spezieller. Umgekehrt greift Art. 34d auch dann ein, wenn sich das informationstechnische System in einer Wohnung im Sinn von Art. 13 GG, Art. 106 Abs. 3 BV befindet.

Eingriffshandlung nach Satz 1 ist das Erheben von Daten. Das Erheben von Zugangsdaten betrifft insbesondere die Erhebung von Benutzerkennungen und Passwörtern, nicht aber schon die Erhebung von besonders gesicherten Daten. Das Erheben von gespeicherten Daten umfasst die bloße Sichtung, aber auch das Kopieren von Datenbeständen unter Belassung der Datenbestände auf dem Zielsystem.

Nicht erfasst von der Befugnis sind allgemeine Recherchen im Internet durch die Polizei, auch wenn Beamte nicht als Polizeibeamte und unter ihrem eigenen Namen auftreten. Hier liegt in der Regel kein Grundrechtseingriff vor (vgl. auch insoweit BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 311), sodass es keiner Rechtsgrundlage bedarf.

a) Die materiellen Voraussetzungen für einen verdeckten Zugriff mit technischen Mitteln auf informationstechnische Systeme orientieren sich an denen für die verdeckte Erhebung von Telekommunikationsinhaltsdaten, tragen aber insbesondere den Anforderungen des Bundesverfassungsgerichts im Urteil vom 27. Februar 2008 Rechnung. Die Befugnisnorm setzt das Bestehen einer konkreten Gefahr für ein überragend wichtiges Rechtsgut voraus. Die Polizei ist daher nicht zu Maßnahmen im „Gefahrenvorfeld“ berechtigt, andererseits ist es nicht erforderlich, dass die Gefahr schon in näherer Zukunft eintritt.

   Art. 34d Abs. 1 Satz 1 Nr. 1 sieht als Adressaten der Maßnahme die nach Art. 7 und 8 für eine Gefahr verantwortlichen Personen vor. Voraussetzung ist, dass eine konkrete Gefahr für die abschließend aufgezählten überragend wichtigen Rechtsgüter vorliegt. Zu diesen zählen neben Leib, Leben und Freiheit einer Person auch der Bestand und die Sicherheit des Bundes oder eines Landes. Das Bundesverfassungsgericht hat anerkannt, dass nicht nur Leib, Leben und Freiheit der Person sondern auch solche Güter der Allgemeinheit überragend wichtig sind, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 247). Letztere werden in der gesetzlichen Regelung von der Sicherheit des Bundes und des Landes umfasst. Durch die Einschränkung, dass es sich um eine dringende Gefahr handeln muss, stellt das Gesetz die Bedeutung der Rechtsgüter nochmals ausdrücklich klar.

b) Die Maßnahme der Gefahrenabwehr kann sich nach Satz 1 Nr. 2 auch 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 begehen werden. Im konkreten Einzelfall ist unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit und der Einschränkungen, die hinsichtlich der Tatsachengrundlage und der Begründetheit der Gefahrprognose gesetzlich vorgesehen sind, eine Abwägung zu treffen. Dabei ist wie im gesamten Gefahrenabwehrrecht zu berücksichtigen, dass das Gewicht des durch die Strafnorm geschützten Rechtsguts und die Anforderungen an die Wahrscheinlichkeit des Eintritts der Rechtsgutsverletzung in einem umgekehrten Verhältnis stehen. Die in Art. 30 Abs. 5 Satz 1 Nr. 1 - 9 genannten Straftaten dienen dem Schutz überragend wichtiger Rechtsgüter. Die Bezugnahme auf die schwerwiegenden Straftaten ist – ebenso wie bei der Wohnraumüberwachung – erforderlich, um Gefahren für schützenswerte überragend wichtige Rechtsgüter zu erfassen, die nicht ohne weiteres nach Nr. 1 benannt werden können. Diese Schwierigkeit wird auch aus der Urteilsbegründung des Bundesverfassungsgerichts ersichtlich, wenn die „Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“, nur sehr vage beschrieben werden können. Darüber hinaus dient die Bezugnahme auf die Straftatbestände im Bereich der nach Nr. 1 benannten Rechtsgüter zur Eingrenzung und Konkretisierung des Gefahrenbegriffs.

   Besondere Bedeutung kommt der ausdrücklich im Gesetz normierten Voraussetzung zu, dass die Tat auch im ganz konkreten Einzelfall schwer wiegen muss, Art. 30 Abs. 5 Satz 1 a.E. Auch durch sie wird im Rahmen des Art. 34d im Einzelfall der konkrete Bezug zur Abwehr einer Gefahr für ein überragend wichtiges Rechtsgut hergestellt. Einzubeziehen ist jeweils auch die Eingriffsintensität. So bedeutet beispielsweise die verdeckte Erhebung eines Passwortes, mit dessen Hilfe nach einer sich anschließenden offenen Durchsuchung und Beschlagnahme des Computers die Möglichkeit zur Auswertung eröffnet wird, im Hinblick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Vergleich zu einer verdeckten Erhebung von auf dem informationstechnischen System gespeicherten Daten den weniger intensiven Eingriff.

c) Kontakt- und Begleitpersonen, die für die in Satz 1 Nr. 1 und Nr. 2 aufgezählten Störer Botentätigkeiten wahrnehmen oder ihnen ihre informationstechnischen Systeme zur Verfügung stellen, können unter den einschränkenden Voraussetzungen des Satzes 1 Nr. 3 Buchst. a) und b) Adressaten der Maßnahme sein, wenn auf der Grundlage von bestimmten Tatsachen die begründete Annahme besteht, dass es sich um Kontaktpersonen handelt oder um Personen, die ihre informationstechnischen Systeme den in Nr. 1 und 2 genannten Adressaten in der Vergangenheit zur Verfügung gestellt haben oder zur Verfügung stellen. Berufsgeheimnisträger sind in

Buchst. a) besonders geschützt, soweit sie ein Recht zur Zeugnisverweigerung nach §§ 53, 53a StPO haben. Insoweit ist eine Überwachung unzulässig. Dies gilt jedoch nicht, wenn die entgegengenommenen Mitteilungen, die die Gefahrverursachung betreffen müssen, von ihnen weitergeleitet werden, sie also als Boten tätig sind, oder wenn die genannten Adressaten ihre informationstechnischen Systeme benutzen oder benutzt haben.

d) Nach Satz 2 dürfen in eng begrenzten Ausnahmefällen gespeicherte Daten auch gelöscht oder verändert werden, wenn dies 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 der Datenentzug gegenüber dem Maßnahmeadressaten, während unter Verändern das Hinzufügen, Weglassen oder sonstige Ändern von Informationen zu verstehen ist. So kann es beispielsweise erforderlich sein, bestimmte bereits gespeicherte Datenbestände (z.B. detaillierte Beschreibungen von Anschlagszielen, Bombenbauanleitungen, chemische Formeln von giftigen Substanzen, die zu Zwecken eines terroristischen Anschlags hergestellt werden sollen etc.) auf dem informationstechnischen System des Betroffenen gänzlich zu löschen oder zu verändern, um eine unmittelbar bevorstehende oder bereits teilweise realisierte Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren. Zugangsdaten dürfen unter den Voraussetzungen des Satzes 1 gelöscht oder verändert werden, um im Einzelfall beispielsweise zu verhindern, dass der Gefährder Zugang zu den auf dem informationstechnischen System gespeicherten Daten erhält.

e) Der Zugriff auf informationstechnische Systeme ist gegenüber anderen Maßnahmen subsidiär. Dies stellt Art. 34d Abs. 1 Satz 3 klar. Bei wortgetreuer Auslegung der Vorschriften, die eine mit Art. 34d Abs. 1 Satz 3 identische Subsidiaritätsklausel haben (Art. 34 Abs. 1 Satz 2 Nr. 1, 34a Abs. 1 Satz 2), entstünde ein Ringverweis zwischen denjenigen Normen, die die Aussichtslosigkeit anderer Ermittlungsmaßnahmen als Subsidiaritätsmerkmal enthalten. Während das Bundesverfassungsgericht in seinem Urteil zur repressiven Wohnraumüberwachung vom 3. März 2004, Az. 1 BvR 2378/98, 1 BvR 1084/99, die akustische Wohnraumüberwachung als letztes Mittel der Strafverfolgung bezeichnete (Absatz-Nr. 223), wird man im Lichte der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 so ein Verhältnis beim verdeckten Zugriff auf informationstechnische Systeme nicht von vornherein annehmen können. So wird die Erhebung von Zugangsdaten mittels eines Keyloggers regelmäßig der gegenüber einer optischen Wohnraumüberwachung weniger intensive Eingriff sein, wenn die Maßnahme beispielsweise darauf gerichtet ist, ein Passwort zu erhalten.

f) Der Schutz von Berufsgeheimnisträgern wird in Art. 34d Abs. 1 Satz 4 parallel zu Art. 34a Abs. 1 Satz 3 ausgestaltet. Der Schutz der Berufsgeheimnisträger in Art. 34a entspricht den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zur akustischen Wohnraumüberwachung vom 3. März 2004, a.a.O., gemacht hat. Die Entscheidung zur Online-Durchsuchung vom 27. Februar 2008 enthält hierzu keine weiteren Ausführungen, so dass eine unveränderte Übernahme beim verdeckten Zugriff auf informationstechnische Systeme angezeigt ist.

g) Art. 34d Abs. 1 Satz 5 dient dem verfassungsrechtlich gebotenen Kernbereichsschutz. Nach der jüngsten Rechtsprechung des Bundesverfassungsgerichts (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 280) lässt sich dieser durch ein zweistufiges Schutzkonzept verwirklichen. Durch Art. 34d Abs. 1 Satz 5 wird auf der ersten Stufe darauf hingewirkt, dass soweit dies informationstechnisch und ermittlungstechnisch möglich ist, mittels geeigneter Vorkehrungen sicherzustellen ist, dass bereits die Erhebung von kernbereichsrelevanten Daten unterbleibt. Dabei sind entsprechend den Ausführungen des Bundesverfassungsgerichts „verfügbare“ informationstechnische Sicherungen einzusetzen (vgl. BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 281). Satz 5 steht unter dem Vorbehalt des informationstechnisch und ermittlungstechnisch Möglichen, indem die Sicherstellung in der Erhebungsphase voraussetzt, dass geeignete Vorkehrungen vorhanden und einsetzbar sind. Auch das Bundesverfassungsgericht stellt in seiner Entscheidung vom 27. Februar 2008 fest, dass es bei einem heimlichen Zugriff auf ein informationstechnisches System praktisch unvermeidbar sei, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann (Absatz-Nr. 277). Weiter heißt es in der Entscheidung, dass „technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten … nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig [arbeiten], dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte“ (Absatz-Nr. 278). Art. 34d Abs. 1 Satz 6 betrifft den Fall, dass trotz entsprechender informationstechnischer Sicherungen oder mangels entsprechender Möglichkeiten bereits in der Phase der Datenerhebung erkennbar wird, dass gerade erhobene Daten dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Dies entspricht der vom Bundesverfassungsgericht auch in seiner jüngsten Entscheidung bestätigten Rechtsprechung, dass die Datenerhebung zu unterbleiben hat, wenn im Einzelfall konkrete Anhaltspunkte für die Kernbereichsrelevanz vorliegen (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 281). Die Datenerhebung ist nach Art. 34d Abs. 1 Satz 6 insoweit unzulässig. Eine Ausnahme besteht jedoch in den Fällen, in denen Anhaltspunkte bestehen, dass kernbereichsrelevante Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen. Das Bundesverfassungsgericht hat anerkannt, dass von dem grundsätzlichen Erhebungsverbot kernbereichsrelevanter Daten eine Ausnahme zu machen ist, wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 281). Der Schutz des Kernbereichs privater Lebensgestaltung wird darüber hinaus über die bereits in der Sichtungsphase bestehende Löschungspflicht bzw. Vorlagemöglichkeit an den Richter bei Zweifel über die Zulässigkeit der Verwendung nach Art. 34d Abs. 4 sowie die Löschungspflicht im Verlauf der weiteren Auswertung nach Art. 34d Abs. 6 Satz 1 i.V.m. Abs. 5 Satz 2 gewährleistet.

h) Art. 34d Abs. 1 Satz 7 ordnet schließlich die Dokumentation der Maßnahmen nach den Sätzen 1 und 2 an. Die Einfügung einer Dokumentationspflicht ist zum Schutz des vom Bundesverfassungsgericht in der Entscheidung vom 27. Februar 2008 beschriebenen „Computer-Grund-

rechts“ in seiner besonderen Ausprägung eines Grundrechts auf Gewährleistung der Integrität informationstechnischer Systeme erforderlich (vgl. Absatz-Nr. 239 ff.). Da es zu einer effektiven Gefahrenabwehr im Einzelfall auch erforderlich werden kann, auf dem Zielrechner gespeicherte Daten durch gezielte Manipulationen zu löschen, zu verändern oder neu anzulegen (vgl. insoweit auch Absatz-Nr. 240), ist es notwendig, den ursprünglichen Zustand sowie die Auswirkungen der polizeilichen Maßnahmen umfassend zu dokumentieren. Durch die Dokumentation der einzelnen Schritte der Maßnahme wird die Nachvollziehbarkeit aller getroffenen Maßnahmen gewährleistet und werden die Interessen der Betroffenen verfahrensrechtlich abgesichert.

2. Im Unterschied zum Zugriff auf informationstechnische Systeme zur Erhebung von Zugangsdaten oder gespeicherten Daten normiert Art. 34d Abs. 2 die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von informationstechnischen Systemen. Diese Regelung ist angesichts der Entwicklungen auf dem Gebiet der Informationstechnik erforderlich, da bei der Planung und Begehung von schwerwiegenden Straftaten, die überragend wichtige Rechtsgüter bedrohen, insbesondere von Angehörigen gewaltbereiter extremistischer Gruppen zunehmend informationstechnische Systeme eingesetzt werden, deren spezifische Kennungen und Standort den Sicherheitsbehörden nicht bekannt sind. Eine Spezifizierung der informationstechnischen Systeme ist allerdings im Regelfall Voraussetzung für die Durchführung einer Maßnahme nach Abs. 1. Daneben ist die Bezeichnung des informationstechnischen Systems Voraussetzung für eine Anordnung des Zugriffs auf informationstechnische Systeme zur Datenerhebung, so dass der Polizei die Befugnis zur Ermittlung der erforderlichen Daten eingeräumt werden muss. Gleiches gilt für die Bestimmung des Standorts eines informationstechnischen Systems. Der Einsatz von Geräten, wie etwa des sog. „WLAN-Catchers“ zur Bestimmung von spezifischen Kennungen bzw. des Standortes eines informationstechnischen Systems wird an die strengen Voraussetzungen des Abs. 1 geknüpft, da er in der Regel zur Vorbereitung einer der dort genannten Maßnahmen dient. Dies gilt auch für die Subsidiaritätsregelung in Abs. 1 Satz 3. Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, sind diese unverzüglich zu löschen.

3. Zur Anordnung einer Maßnahme nach Art. 34d bedarf es einer richterlichen Entscheidung; dies stellt der Verweis auf Art. 34 Abs. 4 Sätze 1 und 2 in Abs. 3 Satz 1 klar. Durch die Kontrolle einer unabhängigen und neutralen Instanz wird der Grundrechtsschutz zusätzlich abgesichert (vgl. zur Online-Durchsuchung BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 258). Bei Gefahr im Verzug besteht eine nach der regelmäßigen Eingriffstiefe differenzierte Anordnungskompetenz. Das Bundesverfassungsgericht lässt für Eilfälle ausdrücklich eine Ausnahme vom grundsätzlichen Erfordernis einer vorherigen Kontrolle durch eine geeignete neutrale Stelle zu (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 261). Bei Maßnahmen nach Abs. 2 (Ermittlung von Kennungen und des Standortes) und bei der bloßen Erhebung von Zugangsdaten ist nach Abs. 3 Satz 2 eine Anordnung durch die in Art. 33 Abs. 5 Satz 2 genannten Stellen ausreichend, im übrigen sind in Eilfällen nur der Leiter eines Polizeipräsidiums der Landespolizei oder des Landeskriminalamts anordnungsbefugt. In jedem Fall bedarf es einer unverzüglichen Bestätigung der Entscheidung durch den Richter.

Nach Satz 3 haben Anordnungen nach Art. 34d Abs. 1 und 2 schriftlich zu ergehen und sind zu begründen. Auf das Erfordernis der schriftlichen Begründung nach vorausgegangener eingehender Prüfung der Rechtmäßigkeit der Maßnahme durch den Richter weist das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 nochmals ausdrücklich hin (vgl. Absatz-Nr. 259). Satz 4 bestimmt, dass die Anordnung den Namen und die Anschrift des Betroffenen enthalten muss, soweit dies möglich ist. Die Einschränkung „soweit möglich“ trägt dem Umstand Rechnung, dass nicht stets vollständige Angaben zur Person des Betroffenen bekannt sind. Damit ist die Vorschrift der durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. S. 3198) neu gefassten Regelung in § 100b Abs. 2 Satz 2 Nr. 1 StPO angepasst. Es gibt durchaus Fallkonstellationen, bei denen die Polizei den Gefährder als Maßnahmeadressaten nur über das informationstechnische System ermitteln kann. So sind Fälle denkbar, in denen ein ausländischer E-Mail-Provider genutzt wird, bei dem E-Mail-Konten anonymisiert erstellt werden können und der Versand über öffentliche drahtlose Internetzugriffspunkte (z.B. WLAN-Hotspot) erfolgt. Hier kann bei der Auswertung der relevanten Verkehrsdaten die E-Mail keiner bestimmten Person oder spezifischen Kennung eines informationstechnischen Systems zugeordnet werden. In diesen Fällen sind Namen und Anschrift des Betroffenen nicht bekannt, so dass der Vorbehalt in Satz 4 erforderlich ist. In der Anordnung ist auch das informationstechnische System, auf das zugegriffen werden soll, zu bezeichnen. Art, Umfang und Dauer der Maßnahme sind nach Satz 5 in der Anordnung zu bestimmen. Damit wird eine exakte Eingrenzung der polizeilichen Maßnahme sichergestellt. Die zulässige Höchstdauer für eine Anordnung legt Satz 6 auf drei Monate fest. Dies trägt dem Umstand Rechnung, dass in der Praxis die Durchführung einer Maßnahme nach den Abs. 1 und 2 regelmäßig langwieriger Vorbereitungen bedarf. Eine kürzere Anordnungshöchstdauer würde in diesen Fällen die Beantragung einer erneuten Anordnung erfordern, bevor mit der eigentlichen Maßnahme begonnen worden ist. Da es sich um eine Bestimmung der Höchstdauer handelt, kann das anordnende Gericht je nach Lage des Einzelfalls die Maßnahme auch für eine kürzere Frist anordnen. Eine effektive gerichtliche Kontrolle bleibt daher gewährleistet. Nach Satz 7 besteht die Möglichkeit der Verlängerung der Maßnahmen um jeweils nicht mehr als einen Monat. In Konkretisierung des Verhältnismäßigkeitsgrundsatzes wird in Satz 8 Halbsatz 1 klargestellt, dass die jeweiligen Maßnahmen zu beenden sind, wenn die Voraussetzungen entfallen. Die Mitteilungspflicht bei Beendigung gemäß Satz 8, Halbsatz 2 stellt eine zusätzliche verfahrensrechtliche Sicherung dar.

4. Das Bundesverfassungsgericht misst dem Schutz des Kernbereichs der privaten Lebensgestaltung auch beim verdeckten Zugriff auf informationstechnische Systeme für die Verfassungsmäßigkeit einer gesetzlichen Eingriffsermächtigung entscheidende Bedeutung zu. Auf der ersten Stufe des im Urteil vom 27. Februar 2008 entwickelten zweistufigen Schutzkonzepts wird durch Abs. 1 Sätze 5 und 6 sichergestellt, dass bereits die Erhebung kernbereichsrelevanter Daten soweit wie möglich unterbleibt. Abs. 4 regelt die zweite Stufe des vom Bundesverfassungsgericht entwickelten Schutzkonzepts. Das Gericht führt aus, dass sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht immer klären lassen wird (Absatz-Nr. 282). Deshalb hat der Gesetzgeber durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater

Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben. Entscheidende Bedeutung für den Schutz des Betroffenen hat insoweit „die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte [...], für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt“ (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nr. 283). Ein solches geeignetes Verfahren wird in Abs. 4 geregelt. Bestehen anlässlich der Durchsicht Anhaltspunkte dafür, dass kernbereichsrelevante Daten erhoben wurden, so sind diese nach Satz 1 Nr. 1 entweder unverzüglich zu löschen oder aber – bei Zweifeln über die Kernbereichsrelevanz der Daten – dem für die Anordnung der Maßnahme zuständigen Richter vorzulegen; dieser entscheidet dann über ihre weitere Verwendung. Die Regelung gilt auch für Daten, die möglicherweise Inhalte betreffen, über die das Zeugnis als besonders privilegierter Berufsgeheimnisträger verweigert werden könnte (Satz 1 Nr. 2) bzw. solche Daten, die dem Vertrauensverhältnis mit einem anderen Berufsgeheimnisträger zuzuordnen sind (Satz 1 Nr. 3). Bestehen im letzteren Fall Anhaltspunkte, dass die Daten einen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben, kann der Richter ihre Verwendung (vgl. Abs. 5 Satz 3 Nr. 3) zulassen. In Eilfällen kann die Entscheidung nach Satz 2 auch vom Leiter eines Präsidiums der Landespolizei oder des Landeskriminalamts getroffen werden. Eine richterliche Entscheidung ist in diesen Fällen unverzüglich nachzuholen. Die Löschung ist nach Satz 3 zu dokumentieren.

5. Abs. 5 Sätze 1 bis 3 entsprechen Art. 34c Abs. 4 Sätze 1 bis 3. Satz 1 regelt die Kennzeichnungspflicht. Satz 2 Nr. 1 bestimmt, dass die erlangten personenbezogenen Daten zu den Zwecken, zu denen sie erhoben wurden, verwendet werden dürfen. Einer Zweckänderung durch Verwendung zur Strafverfolgung steht derzeit die Vorschrift des § 161 Abs. 2 StPO entgegen, die bestimmt, dass die nach anderen Gesetzen als der StPO erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden können, zu deren Aufklärung eine solche Maßnahme nach der StPO hätte angeordnet werden dürfen. Da die StPO einen verdeckten Zugriff auf informationstechnische Systeme zum Zwecke der Erhebung von Zugangsdaten oder von gespeicherten Daten nach der derzeitigen Gesetzeslage nicht vorsieht, läuft Satz 2 Nr. 2 bis zur Schaffung einer entsprechenden strafprozessualen Befugnis leer. Das Bundesverfassungsgericht hat festgestellt, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos gewährleistet ist und dass Eingriffe auch zur Strafverfolgung gerechtfertigt sein können (vgl. BVerfG, a.a.O., Absatz-Nr. 207). Ein Verwendungsverbot besteht gemäß Satz 3 für Datenerhebungen, bei denen sich nach Auswertung herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben, sie Inhalte betreffen, über die das Zeugnis als Angehöriger bestimmter Berufsgruppen verweigert werden kann, oder dass sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis zu einem Berufsgeheimnisträger zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben. Durch die Verweisung in Satz 4 auf Art. 34c Abs. 4 Sätze 4 und 5 ist eine Verwertung allerdings ausnahmsweise zulässig, wenn dies zum Schutz hochwertigster Rechtsgüter vor gegenwärtigen Gefahren erforderlich ist. In derartigen Fällen ist unverzüglich eine richterliche Entscheidung über die Verwendung nachzuholen. Eine Verwendung von Kernbereichsdaten in diesen Fällen ist auch bei der Wohnraumüberwachung (Art. 34 Abs. 5 Satz 3) und bei der Telekommunikationsüberwachung (34c Abs. 4 Satz 4) ganz ausnahmsweise zulässig. Dabei ist allerdings zunächst zu berücksichtigen, dass Daten, die einen unmittelbaren Bezug zu Gefahren haben, grundsätzlich dem Sozialbereich zuzurechnen sind und somit in aller Regel schon gar nicht kernbereichsrelevant sind (vgl. zu Gesprächen, die Angaben über begangene Straftaten enthalten BVerfG, Urteil vom 3. März 2004, Az.: 1 BvR 2378/98 und 1 BvR 1084/99, Absatz-Nr. 137). Gleichwohl sind Situationen nicht auszuschließen, in denen sich absolut geschützte Rechtsgüter gegenüberstehen und in denen die Kollision nicht aufgelöst werden kann. Zu denken ist etwa an den Fall, dass bei der Auswertung eine Information gewonnen wird, die der Vereitelung eines unmittelbar drohenden terroristischen (Selbstmord-)Anschlags und damit dem Schutz höchster Rechtsgüter dient. Dann stehen sich die Vertiefung des Eingriffs in den Kernbereich privater Lebensgestaltung durch die Verwendung der Daten und die staatliche Schutzpflicht für Leib, Leben und Freiheit gegenüber. Der Gesetzgeber hat sich bei der Novellierung des PAG im Jahre 2005 dafür entschieden, den Konflikt in derartigen Extremkonstellationen zu Gunsten des Schutzes hochwertigster Rechtsgüter und zu Lasten des Kernbereichs zu lösen (vgl. gesetzliche Begründung zu Art. 34 Abs. 5, Drs. 15/2096). Wenn das BVerfG in seinem Urteil zur repressiven Wohnraumüberwachung vom 3. März 2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, ausführt, dass der absolute Schutz des Kernbereichs die Verwertung solcher Daten ausschließe, so lehnt das Gericht damit eine Abwägung zwischen Kernbereichsschutz und Strafverfolgungsinteressen ab. Die Aussagen beziehen sich nicht auf den präventiven Bereich der Gefahrenabwehr, wo es – wie eben dargelegt – zu Kollisionen zwischen absolut geschützten Rechtsgütern durchaus kommen kann. Entsprechend sind auch die Aussagen des Bundesverfassungsgerichts im Urteil vom 27. Februar 2008 zur Online-Durchsuchung zu verstehen, dass eine Weitergabe oder Verwertung kernbereichsrelevanter Daten auszuschließen ist (Absatz-Nrn. 277, 283); das Gericht verweist in diesem Zusammenhang auf das zum repressiven Bereich ergangene Urteil vom 3. März 2004 und schließt somit eine Verwendung im präventiven Bereich nicht von vornherein aus.

6. Die Vorschrift des Abs. 6 entspricht Art. 34c Abs. 6. Die Löschung von Daten, bei denen sich ergibt, dass sie aus dem Kernbereich privater Lebensgestaltung stammen und dass für sie ein Verwendungsverbot besteht, ist in Abs. 7 Satz 1 geregelt. Die Löschungspflicht auf der zweiten Stufe des vom Bundesverfassungsgerichts entwickelten zweistufigen Schutzkonzepts (BVerfG vom 27. Februar 2008, a.a.O., Absatz-Nrn. 280 ff.) gilt stets, unabhängig vom Zeitpunkt einer eindeutigen Zuordnung erhobener Daten zum Kernbereich der privaten Lebensgestaltung. Die Löschung ist zu dokumentieren. Satz 2 Halbsatz 1 betrifft die Sperrung und Halbsatz 2 die Löschung in den sonstigen Fällen, in denen die Verwendung zu den Erhebungszwecken nicht erforderlich ist oder in denen ein Verwendungsverbot besteht. Die in Satz 3 enthaltene entsprechende Anwendbarkeit von Art. 34 Abs. 7 Sätze 3 und 4 bezieht sich auf die Löschung im Falle der Unterrichtung des Betroffenen.

7. Die Benachrichtigungspflicht nach Abs. 7 Satz 1 erfasst die Adressaten der Maßnahme. Als Rechtfertigungsgründe für die Zurückstellung der Benachrichtigung kommen nach Satz 2 die Gefährdung des Untersuchungszwecks und der eingesetzten, nicht offen ermittelnden Beamten selbst in Be-

tracht. Gleiches gilt bei einer Gefährdung der öffentlichen Sicherheit hinsichtlich der durch Absatz 1 Satz 1 Nrn. 1 und 2 geschützten Rechtsgüter. Im Übrigen verweist Satz 3 hinsichtlich der Nachholung der Unterrichtung bei strafrechtlichem Ermittlungsverfahren sowie hinsichtlich der Zurückstellung und Unterbleiben der Unterrichtung auf Art. 34 Abs. 6 Sätze 2 bis 6.

8. Obwohl die Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 zur Online-Durchsuchung dies nicht fordert, sieht Abs. 8 entsprechend der Regelung für die Wohnraumüberwachung in Art. 34 Abs. 9 eine jährliche Unterrichtungspflicht der Staatsregierung gegenüber dem Landtag für die nach Abs. 1 erfolgten Zugriffe auf informationstechnische Systeme zum Zwecke der Erhebung, Löschung oder Veränderung von gespeicherten Daten vor (Satz 1). Die Staatsregierung hat dem Parlamentarischen Kontrollgremium zu berichten (Satz 2). Eine Unterrichtungspflicht besteht nicht für die grundsätzlich weniger eingriffstiefe Erhebung, Löschung oder Veränderung von Zugangsdaten (Abs. 1 Satz 1 Alt. 1, Satz 2 Alt. 1) und die Ermittlung spezifischer Kennungen bzw. des Standorts eines informationstechnischen Systems nach Abs. 2.

9. Art. 34e enthält die Ermächtigung zur Durchführung notwendiger Begleitmaßnahmen. Die „Hauptmaßnahmen“ wären ohne die notwendigen Begleitmaßnahmen nach Satz 1 (Durchsuchung von Sachen, Betreten und Durchsuchung der Wohnung des Betroffenen) vielfach gar nicht möglich. Zu diesen Begleitmaßnahmen zählen etwa im Rahmen der Wohnraumüberwachung nach Art. 34 regelmäßig das Betreten der Wohnung und die Installation der erforderlichen Abhörtechnik. Im Zusammenhang mit der Überwachung kryptierter Telekommunikation kann es etwa erforderlich sein, Gespräche direkt am Endgerät auszuleiten. Derartige Maßnahmen sind nach Art. 34e Satz 1 ebenfalls zulässig, wenn kein milderes Mittel zur Durchführung der Überwachung und Aufzeichnung im Sinn von Art. 34a Abs. 1 besteht. Gleiches gilt für den verdeckten Zugriff auf informationstechnische Systeme nach Art. 34d Abs. 1. Mit umfasst ist dabei auch die heimliche Durchsuchung der Wohnung zur Auffindung eines Notebooks und das Anbringen von Hardwarekomponenten oder das Einbringen spezifischer Software, wenn dies unerlässliche Begleitmaßnahme ist. Für die Anordnung der Begleitmaßnahmen gelten nach Satz 2 die gleichen Vorschriften wie für die Hauptmaßnahme, insbesondere besteht zur verfahrensmäßigen Absicherung der Rechte des Betroffenen ein Richtervorbehalt und in der richterlichen Anordnung sind Art, Umfang und Dauer der Maßnahme genau zu bestimmen. Auch für die Unterrichtung gelten dieselben Regeln wie bei der Hauptmaßnahme.

Nr. 6

Die Ausschreibung zur Polizeilichen Beobachtung kann gemäß Art. 36 Abs. 3 Satz 1 in der bisherigen Fassung durch die in Art. 33 Abs. 5 Satz 1 und 2 genannten „Dienststellenleiter“ angeordnet werden. Mit der Änderung wird klargestellt, dass die in Art. 33 Abs. 5 Satz 1 und 2 genannten Stellen, einschließlich der besonders hierzu beauftragten Beamten des höheren Dienstes, anordnungsbefugt sind.

Zu § 1 Buchstabe c):

Protokollbestände, die nach Abfrage im automatisierten Abrufverfahren gemäß Art. 46 eingerichtet wurden, können zu Zwecken der Kriminalitätsbekämpfung und der Datensicherung ausgewertet werden. Die Auswertung bedarf einer Anordnung der in Art. 33 Abs. 5 genannten „Dienststellenleiter“. Mit der Änderung wird klargestellt, dass die in Art. 33 Abs. 5 Satz 1 und 2 genannten Stellen, einschließlich der besonders hierzu beauftragten Beamten des höheren Dienstes, anordnungsbefugt sind.

Zu § 2:

Nach dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG kann ein Gesetz nur dann verfassungsrechtlich gerechtfertigt sein, wenn es das eingeschränkte Grundrecht unter Angabe des Artikels nennt. Da das Fernmeldegeheimnis in Art. 10 GG und das Grundrecht auf Unverletzlichkeit der Wohnung in Art. 13 GG unter einen ausdrücklichen Gesetzesvorbehalt gestellt werden, ist ein Hinweis auf deren Einschränkung erforderlich.