

# Gesetzentwurf

## zur Änderung des Polizeiaufgabengesetzes

### A) Problem

1. Der technische Fortschritt eröffnet der Polizei fortlaufend Möglichkeiten zur Optimierung ihrer Aufgabenerfüllung durch den Einsatz neuer Technologien. Dazu zählen die verschiedenen Formen automatisierter Kennzeichenerkennungssysteme, durch die die Kennzeichen von Kraftfahrzeugen erfasst und mit dem INPOL-Fahndungsbestand oder im Einzelfall auch sonstigen Dateien abgeglichen werden können.

Das geltende Recht ermöglicht den Einsatz solcher Systeme unter Berücksichtigung des Umstandes, dass hiermit ein Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG einhergeht, jedoch nur in sehr eingeschränktem Umfang. Ein erfolgreich abgeschlossener Pilotversuch der Bayerischen Polizei zum Einsatz solcher Systeme kann daher ohne gesetzliche Änderungen nicht in einen regulären Betrieb überführt werden. Auch der Bayerische Landtag hat mit Beschlüssen vom 28. Januar 2004 (LT-Drs. 15/238, 15/239 und 15/241) die Schaffung einer gesetzlichen Regelung zum Einsatz automatisierter Kennzeichenerkennungssysteme gefordert. Als wichtigstes Tor Deutschlands und Westeuropas und als Transitland nach Ost- und Südosteuropa hat Bayern eine besondere sicherheitspolitische Verantwortung. Dabei gilt es einem möglichen Kriminalitätsimport und Gefahrentransit zu begegnen und so einen nachhaltigen Beitrag zur Ausgestaltung Europas als Raum der Freiheit, der Sicherheit und des Rechts zu leisten. Dies kann ohne den Einsatz neuer technischer Möglichkeiten zur Kriminalitätsbekämpfung nicht gelingen. Darüber hinaus kann nur so dem internationalen Terrorismus begegnet und den Schengen-Vorgaben für effektive Grenzkontrollen entsprochen werden.

2. Durch die Ereignisse des 11. September 2001 und die nachfolgenden weltweiten Terroranschläge, nicht zuletzt durch das Attentat am 11. März 2004 in Madrid, hat sich die Sicherheitslage in Europa grundlegend gewandelt. Neben der globalen Bedrohung durch den internationalen Terrorismus stellt auch die Bekämpfung grenzüberschreitend organisierter Banden die europäischen Sicherheitsbehörden vor neue Herausforderungen. Es hat sich gezeigt, dass diese Erscheinungsformen der Kriminalität von einem hohen Maß an Konspirativität geprägt sind und auf einen technisch hoch entwickelten Unterstützungsapparat zurückgreifen können. Die bisherigen polizeilichen Befugnisse genügen langfristig nicht, um den neuen Bedrohungen effektiv begegnen zu können. Die Erforschung der terroristischen Netzwerke und der Strukturen der Organisierten Kriminalität stößt ebenso wie die Bekämpfung anderer Formen der grenzüberschreitenden Kriminalität, insbesondere im Bereich des Menschenhandels und der Kinderpornografie, auf die Schwierigkeit, dass ein Einschleusen von Kräften der Sicherheitsbehörden vielfach unmöglich ist. Aufgrund der Vernetzung der Täter bieten allerdings die Kommunikationsstrukturen einen wichtigen Ansatzpunkt für die Abwehr drohender Gefahren und die Verhütung von Straftaten.

Den Sicherheitsbehörden dürfen daher die Instrumente, die ihnen für die Strafverfolgung seit langem zur Verfügung stehen, nicht länger vorenthalten werden. Den präventiven Maßnahmen zur Überwachung des Telekommunikationsverkehrs kommt dabei eine besondere Bedeutung zu. Der Schutz von Leib, Leben, Freiheit und anderer hochwertiger Rechtsgüter darf nicht davon abhängen, dass bereits ein strafbares Handeln vorliegt. Hinzu kommt das sicherheitspolitische Erfordernis neuartige Befugnisse einzuführen, etwa zur Kommunikationsunterbrechung bei Geisellagen oder bei unmittelbar bevorstehenden Sprengstoffanschlägen. Die jüngsten Attentate von Madrid haben gezeigt, dass internationale Terroristen zur Durchführung modernster Telekommunikationstechnik nutzen.

Ferner hat die polizeiliche Praxis seit geraumer Zeit dargelegt, dass die Erhebung von Telekommunikationsverbindungsdaten unverzichtbar ist, um bei Unglücksfällen, bei Suizidankündigungen sowie bei der Fahndung und Lokalisation von Vermissten einen oftmals lebensrettenden Fahndungsansatz zu gewährleisten. Derzeit können diese Maßnahmen nur hilfsweise auf die Rechtsnorm des rechtfertigenden Notstandes (§ 34 StGB) gestützt werden, so dass die Übermittlung erforderlicher Kennungen durch Mobilfunknetzbetreiber

letztendlich von deren Kooperationsbereitschaft abhängt. Für einen ggf. notwendigen weiteren Einsatz technischer Mittel zur Nahbereichslokalisierung fehlt es ebenfalls an der erforderlichen Befugnisnorm.

3. Die Wohnraumüberwachung zu präventiven Zwecken stellt in Zeiten wachsender Bedrohung durch den internationalen Terrorismus und durch die Erscheinungsformen der Organisierten Kriminalität weiterhin eine wichtige Befugnis zur Gefahrenabwehr dar. Um Ermittlungen in den inneren Kreis krimineller Organisationen zu tragen reichen herkömmliche Befugnisse vielfach nicht aus. Dies ist aber unerlässlich, um künftige Gefahren effektiv abzuwehren und Straftaten zu verhindern bzw. zu unterbinden. Das Bundesverfassungsgericht hat in seinem Urteil vom 3. März 2004 zur repressiven Wohnraumüberwachung (Az.: 1 BvR 2378/98, 1 BvR 1084/99) die Erforderlichkeit der Eingriffe in das Grundrecht aus Art. 13 Abs. 1 GG anerkannt und das Instrument der Wohnraumüberwachung im Grundsatz für verfassungsmäßig erklärt. Unmittelbar wurde in dem Urteil nur über die Verfassungsmäßigkeit der §§ 100c ff. StPO entschieden. Verfahrensgegenstand war lediglich die repressive Wohnraumüberwachung und nicht der Bereich der Gefahrenabwehr, zu dem sich das Bundesverfassungsgericht nur ansatzweise geäußert hat. Dennoch ergeben sich aus den dargelegten Grundsätzen für Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung Auswirkungen, die auch im Zusammenhang mit der Ausgestaltung der präventiven Wohnraumüberwachung nach Art. 34 PAG zu beachten sind und eine Novellierung der Befugnisnorm erforderlich machen.

4. Polizeiliche Gefahrenabwehr und Strafverfolgung wurden in Deutschland und Europa in der Vergangenheit lange als nahezu ausschließlich interne Angelegenheit eines Staates begriffen.

Nicht zuletzt unter dem Eindruck der neuen terroristischen Bedrohungslage nach den Anschlägen des 11. September 2001 in den USA und des 11. März 2004 in Spanien, verstärkt international agierender Strukturen der Organisierten Kriminalität, aber auch des weitgehenden Zusammenwachsens grenznaher Regionen zu einheitlichen kriminal- und gefahrengeografischen Räumen als Folge des Wegfalls der systematischen Kontrollen an den Schengen-Binnengrenzen hat sich das

praktische Erfordernis eines effektiven Zusammenwirkens der europäischen Polizeien beständig entwickelt. Wesentliches Kernelement der Zusammenarbeit ist dabei stets der Austausch personenbezogener Daten, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung erforderlich ist. Auf völkerrechtlicher Ebene hat der Bund eine Vielzahl von Verträgen zur Polizeikooperation geschlossen, die u. a. den Austausch von Informationen und personenbezogenen Daten vorsehen (vgl. die Vereinbarungen z. B. mit der Schweiz, Österreich, der Tschechischen Republik, Polen und den Niederlanden), oder im Rahmen der Europäischen Union entsprechenden Rechtsinstrumenten zugestimmt. Die strengen Voraussetzungen des Polizeiaufgabengesetzes für eine Datenübermittlung an nichtinnerstaatliche Stellen entsprechen heute jedoch nicht mehr den in den bilateralen Kooperationsvereinbarungen sowie in den Rechtsakten der Europäischen Union verankerten Anforderungen an einen effektiven Datenaustausch zur Bekämpfung der grenzüberschreitenden Kriminalität und zur Schaffung eines Europäischen Raums der Freiheit, der Sicherheit und des Rechts. So ist eine Initiativübermittlung personenbezogener Daten an nichtinnerstaatliche Stellen bei streng am Wortlaut der Absätze 2 und 3 des Art. 40 orientierter Auslegung bislang nur zur Erfüllung eigener Aufgaben der Bayerischen Polizei möglich, nicht aber zur Erfüllung von Aufgaben der ausländischen bzw. der über- oder zwischenstaatlichen Empfängerdienststelle. Auf Ersuchen der ausländischen bzw. über- oder zwischenstaatlichen Stelle kommt eine Datenübermittlung außer zur Abwehr einer erheblichen Gefahr durch den Empfänger nach Art. 40 Abs. 5 nur dann in Betracht, wenn die Polizei hierzu auf Grund über- oder zwischenstaatlicher Vereinbarungen ausdrücklich verpflichtet ist. Eine bloße Ermächtigung, wie sie in modernen Kooperationsvereinbarungen üblich ist, reicht demzufolge nicht aus.

## **B) Lösung**

1. Für den Einsatz automatisierter Kennzeichenerkennungssysteme wird eine spezielle gesetzliche Regelung geschaffen. Da beim Einsatz solcher Systeme sowohl Aspekte der Datenerhebung wie auch der Datenspeicherung und des Datenabgleichs betroffen sind, diese unterschiedlichen Eingriffsformen aber in verschie-

denen Artikeln des III. Abschnitts des Gesetzes geregelt sind, werden die Art. 33, 38 und 46 ergänzt.

2. In das Polizeiaufgabengesetz werden Art. 34 a und b eingefügt, die es der Polizei ermöglichen, zum Schutz hochwertiger Rechtsgüter und zur Verhütung schwerwiegender Straftaten unter engen Voraussetzungen den Telekommunikationsverkehr zu überwachen. Die Anbieter von Telekommunikationsdienstleistungen trifft hierbei eine Mitwirkungspflicht. Ein ebenfalls in das Polizeiaufgabengesetz eingefügter Art. 34 c regelt die formellen Voraussetzungen und gewährleistet den verfahrensrechtlichen Grundrechtsschutz.

Der Polizei wird neben der Befugnis zur Überwachung des netzgebundenen und netzungebundenen Telekommunikationsverkehrs auch eine Befugnis zur Anforderung von Telekommunikationsverbindungsdaten eingeräumt. Maßnahmen zur Identifikation und Lokalisation von Telekommunikationsteilnehmern mittels technischer Geräte werden ebenso geregelt wie die Befugnis, in besonderen Gefahrenlagen Telekommunikationsverbindungen zu unterbrechen oder zu verhindern.

Das Grundrecht aus Art. 10 GG wird durch umfassende Schutzvorkehrungen für Vertrauensverhältnisse abgesichert, die über die grundgesetzlichen Mindeststandards hinausgehen. Berufsgeheimnisträger wie Geistliche, Ärzte, Apotheker und Anwälte, aber auch Journalisten und Abgeordnete werden durch ein Erhebungsverbot geschützt. Darüber hinaus unterliegen die Gespräche mit diesen Personengruppen ebenso wie diejenigen mit engsten Familienangehörigen und Vertrauten Verwertungsverboten und einem Lösungsgebot. Die verfahrensrechtliche Absicherung wird durch weitgehende Richtervorbehalte gewährleistet. Obwohl die gerichtliche Prüfung für Eingriffe in das Fernmeldegeheimnis in Art. 10 GG, anders als bei der Wohnraumüberwachung, nicht vorgesehen ist, muss ein Richter der Telekommunikationsüberwachung grundsätzlich vorab zustimmen. Den Belangen des Datenschutzes wird darüber hinaus auch durch die Kennzeichnungspflichten und durch die Einschränkungen für Zweckänderungen entsprochen. Das Rechtsschutzgebot wird durch die Sperrung derjenigen Daten, die für eine gerichtliche Überprüfung erforderlich sind, und die Benachrichtigung der Betroffenen gewährleistet.

3. Die Regelungen über die präventive Wohnraumüberwachung werden den verfassungsrechtlichen Erfordernissen angepasst und denselben strengen Voraussetzungen unterworfen. Da die Maßnahme eine stärkere Eingriffsintensität als die Telekommunikationsüberwachung aufweist, erfolgt der Schutz der Privatsphäre und der genannten Vertrauensbeziehungen zusätzlich über generelle Abhörverbote für Vertrauenspersonen sowie über die Verpflichtung, eine laufende Maßnahme abubrechen, wenn erkannt wird, dass ein Eingriff in den Kernbereich bzw. in besondere Vertrauensverhältnisse erfolgt. Dabei findet eine Erweiterung des Schutzes über die Anforderungen hinaus, die das Bundesverfassungsgericht vorgegeben hat, statt, da Abgeordnete und Journalisten in gleicher Weise geschützt werden wie andere Berufsgruppen. Die richterliche Kontrolle der Verwertbarkeit stellt eine weitere Verfahrenssicherung dar, die den Grundrechtsschutz ebenfalls verstärkt.
  
4. Um die neuen Möglichkeiten des polizeilichen Datenaustausches mit nichtinnerstaatlichen Stellen, die die vom Bund im Einvernehmen mit den Ländern ratifizierten zwischen- und überstaatlichen Rechtsinstrumente vorsehen, in das nationale Polizeirecht zu transformieren, werden die Vorschriften über die Datenübermittlung innerhalb des öffentlichen Bereichs (Art. 40 und 42) überarbeitet.

### **C) Alternativen**

Keine

### **D) Kosten und Nutzen**

1. Für die Kennzeichenerkennungsanlagen sind im Haushalt 2004 1,2 Mio. € (Nachtragshaushalt 0,7 Mio. €, Ausgabereste 2003 0,5 Mio. €) eingestellt. Bei der Inbetriebnahme werden im Einzelfall Betriebskosten anfallen, deren Höhe derzeit jedoch noch nicht bezifferbar ist. Die Kosten des Betriebs sind aller Voraussicht nach mit den zur Verfügung stehenden Haushaltsmitteln abzudecken.

2. Die voraussichtlichen Kosten des Einsatzes der präventiven Maßnahmen zur Überwachung der Telekommunikation sind nicht konkret bezifferbar, da sie insbesondere maßgeblich davon abhängen, in welchem Umfang präventive Telekommunikationsüberwachung erfolgt und welcher personelle Aufwand für die Durchführung der Überwachung sowie die Auswertung der Erkenntnisse erforderlich ist. Für die präventive Telefonüberwachung kann jedoch zumindest in Teilbereichen auf die bereits vorhandene technische Ausstattung der bayerischen Polizei, die bereits bisher Überwachungsaufgaben als Strafverfolgungsbehörde nach §§ 100 a, 100 g bis 100 i StPO wahrnimmt, zurückgegriffen werden
  
3. Die voraussichtlichen künftigen Kosten des Einsatzes der präventiven Wohnraumüberwachung sind nicht konkret bezifferbar, da sie insbesondere maßgeblich davon abhängen, welchen Umfang die präventive Wohnraumüberwachung künftig einnehmen wird. Da die präventive Wohnraumüberwachung schon bislang im Bayerischen Polizeiaufgabengesetz normiert war, werden in der Summe keine Kostensteigerungen erwartet, da zwar einerseits - bedingt durch die Komplexität der Regelungen - die Kosten für einzelne Maßnahmen und der administrative Aufwand ansteigen dürften, jedoch andererseits - aufgrund der erheblichen Einengung des Anwendungsbereichs - insgesamt mit einem Rückgang der Fallzahlen zu rechnen ist, so dass eventuelle Kostensteigerungen dadurch kompensiert werden.
  
4. Auf Grund der Änderung der Vorschriften über die Datenübermittlung im öffentlichen Bereich sind zusätzliche monetäre Ausgabepositionen oder Einsparungen, die im Ansatz des Staatshaushaltes zu berücksichtigen wären, nicht zu erwarten. Beim Vollzug der Vorschriften können im Einzelfall Kosten (Telefonentgelte u. ä.) anfallen, deren Höhe zurzeit jedoch nicht bezifferbar ist. Die Kosten des Vollzugs sind aller Voraussicht nach mit den zur Verfügung stehenden Haushaltsmitteln abzudecken.

Ein Mehrbedarf an Personal oder Personaleinsparungen stehen nicht zu erwarten.

5. Die voraussichtlichen Kosten für die Beschaffung von Elektroimpulsgeräten und die dafür notwendige Aus- und Fortbildung sind derzeit nicht konkret zu beziffern, da sie maßgeblich vom späteren Ausstattungsumfang abhängig sind. Weil jedoch nicht vorgesehen ist, Elektroimpulsgeräte in größere Stückzahlen zu beschaffen und ihr Einsatz insbesondere bei den Polizeidirektionen Spezialeinheiten der Bayerischen Polizei angedacht ist, sind die Kosten aller Voraussicht nach mit den zur Verfügung stehenden Haushaltsmitteln abzudecken.

**2012-1-1-I, 12-4-I**

**Gesetz**  
**zur Änderung des Polizeiaufgabengesetzes**  
**und des Parlamentarischen Kontrollgremium - Gesetzes**

**§ 1**  
**Änderung des Polizeiaufgabengesetzes**

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 Gesetz vom 24. Juli 2001 (GVBl S. 348), wird wie folgt geändert:

1. Art. 30 Abs. 5 erhält folgende Fassung:

„(5) <sup>1</sup>Schwerwiegende Straftaten im Sinn dieses Gesetzes sind

1. Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80, 81, 82, §§ 94, 96 Abs. 1, jeweils auch in Verbindung mit § 97b, §§ 97a, 98 Abs. 1 Satz 2, § 99 Abs. 2, §§ 100, 100a Abs. 4 StGB),
2. Straftaten gegen die öffentliche Ordnung (§§ 129 bis 129b StGB),
3. Straftaten gegen die sexuelle Selbstbestimmung (§§ 176, 176a, 177, 180b, 181, 181a Abs. 1, § 184b Abs. 1 bis 3 StGB),
4. Straftaten gegen das Leben (§§ 211, 212 StGB, § 6 Völkerstrafgesetzbuch),
5. Straftaten gegen die persönliche Freiheit (§§ 234, 234a Abs. 1, §§ 239a, 239b StGB),
6. gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306b, 307 Abs.1 und 2, § 308 Abs.1, § 309 Abs.1, § 310 Abs.1, §§ 313, 314, 315 Abs. 3, 315b Abs. 3, §§ 316a, 316c StGB),

7. Verbrechen gegen die Menschlichkeit (§ 7 Völkerstrafgesetzbuch),  
Kriegsverbrechen (§§ 8 bis 12 Völkerstrafgesetzbuch),
8. Straftaten nach § 51 Abs. 1 in Verbindung mit Abs. 2, § 52 Abs. 1 Nr. 1 in  
Verbindung mit Abs. 5 Waffengesetz oder nach § 19 Abs. 2, § 20 Abs. 1,  
jeweils auch in Verbindung mit § 21, des Gesetzes über die Kontrolle von  
Kriegswaffen,
9. Straftaten nach § 22a Abs. 1 in Verbindung mit Abs. 2 des Gesetzes über  
die Kontrolle von Kriegswaffen, soweit offensichtlich ist, dass keine Ge-  
nehmigung oder behördliche Erlaubnis erteilt werden kann, und
10. Straftaten nach § 30a oder § 30b des Betäubungsmittelgesetzes, soweit  
offensichtlich ist, dass keine Genehmigung oder behördliche Erlaubnis er-  
teilt werden kann.

<sup>2</sup>Straftaten von erheblicher Bedeutung sind über die in Satz 1 genannten  
hinaus insbesondere Verbrechen, die in § 138 StGB genannten Vergehen  
sowie die gewerbs- oder bandenmäßig begangenen Vergehen nach

1. den §§ 243, 244, 253, 260, 263a, 265b, 266, 283, 283a, 291 oder 324  
bis 330a StGB,
2. § 52 Abs. 1 Nr. 1 des Waffengesetzes,
3. § 29 Abs. 3 Satz 2 Nr. 1 oder § 29a Abs. 1 Nr. 2 des Betäubungsmit-  
telgesetzes,
4. § 92a des Ausländergesetzes.“

2. Der Wortlaut in Art. 33 Abs. 2 wird Satz 1; es wird folgender Satz 2 angefügt:

„<sup>2</sup>Darüber hinaus kann die Polizei unbeschadet des Art. 30 Abs. 3 Satz 2  
durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssys-  
teme in den Fällen des Art. 13 Abs. 1 Nrn. 1 bis 5 Kennzeichen von Kraft-  
fahrzeugen zum Zweck des Datenabgleichs nach Art. 43 erfassen.“

3. Art. 34 wird wie folgt geändert:

- a) Der Wortlaut in Abs. 1 wird Satz 1 und wie folgt geändert:

aa) In Nr. 1 werden die Worte „oder für Sachen, deren Erhaltung im öffentlichen Interesse geboten erscheint,“ durch die Worte „oder für Sachen, soweit eine gemeine Gefahr besteht,“ ersetzt.

bb) Nr. 2 erhält folgende Fassung:

„2. Über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass diese Personen eine schwerwiegende Straftat begehen wollen.“

cc) Es werden folgende Sätze 2 bis 4 angefügt:

„<sup>2</sup>Eine Maßnahme nach Satz 1 ist nur zulässig, wenn

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 Berufsheimnisträgern nach § 53 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 oder
  - b) die Maßnahme sich auch gegen die Familienangehörigen, Vertrauten oder Berufsheimnisträger richtet oder richten könnte, und
3. für den Fall, dass sich die Maßnahme gegen einen Berufsheimnisträger selbst richtet und die ausschließlich zu seiner Berufsausübung dienenden Räumlichkeiten betroffen sind, die Voraussetzungen der Nr. 2 Buchst. a vorliegen.

<sup>3</sup>Eine Maßnahme nach Satz 1 ist unverzüglich zu unterbrechen, falls erkennbar wird, dass Gespräche mit engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsheimnisträgern geführt werden und die in Satz 2 Nr. 2 Buchst. a oder b genannten Voraussetzungen nicht vorliegen.

<sup>4</sup>Die Erhebung personenbezogener Daten über andere als die in Satz 1 ge-

nannten Personen ist nur zulässig, soweit sie unvermeidliche Folge einer Maßnahme nach Satz 1 ist.“

b) Abs. 2 erhält folgende Fassung:

„(2) <sup>1</sup>Eine 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 eine richterliche Entscheidung unverzüglich nachzuholen; für die richterliche Anordnung sind Art. 24 Abs. 1 Sätze 2 und 3 entsprechend anzuwenden. <sup>2</sup>Die Maßnahme ist schriftlich anzuordnen. <sup>3</sup>In der Anordnung sind Adressat, Umfang und Dauer der Maßnahme zu bestimmen. <sup>4</sup>Die Maßnahme ist auf höchstens einen Monat zu befristen und kann um jeweils nicht mehr als einen Monat verlängert werden. <sup>5</sup>Ungeachtet 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.“

c) Es werden folgende neue Abs. 3 und 4 eingefügt:

„(3) <sup>1</sup>Die durch eine Maßnahme nach Abs. 1 Satz 1 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. <sup>2</sup>Sie dürfen nur verwendet werden

1. zu den in Abs. 1 Satz 1 genannten Zwecken sowie
2. zu Zwecken der Strafverfolgung, wenn die Voraussetzungen der Strafprozessordnung für die Verwertung der Daten vorliegen oder für die Datenerhebung bei der Erhebung vorgelegen haben, eine Zweckänderung ist festzustellen und zu dokumentieren.

<sup>3</sup>Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie einem Vertrauensverhältnis zwischen engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit 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 Verhütung einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. <sup>4</sup>Vor einer Verwendung der Daten ist über deren Zulässigkeit ei-

ne richterliche Entscheidung herbeizuführen. <sup>5</sup>Bei Gefahr im Verzug kann die Entscheidung auch ein in Art. 33 Abs. 5 genannter Dienststellenleiter treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. <sup>6</sup>Für die richterliche Entscheidung sind Art. 24 Abs. 1 Satz 2 und 3 entsprechend anzuwenden.

(4) <sup>1</sup>Die 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. <sup>2</sup>Ist 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. <sup>3</sup>Erfolgt die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. <sup>4</sup>Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. <sup>5</sup>Eine Unterrichtung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

1. die Voraussetzungen des Satzes 1 auf Dauer nicht vorliegen oder
2. überwiegende Interessen eines Betroffenen entgegenstehen oder
3. die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden können.

<sup>6</sup>Die gerichtliche Zuständigkeit und das Verfahren richten sich im Fall des Satzes 2 nach den Regelungen der Strafprozessordnung, im Übrigen gelten Art. 24 Abs. 1 Satz 2 und 3 entsprechend.“

d) Der bisherige Abs. 3 wird Abs. 6 und wie folgt geändert:

aa) In Satz 2 werden nach den Worten „der Gefahrenabwehr“ die Worte „oder der Strafverfolgung“ eingefügt.

bb) Es wird folgender neuer Satz 4 eingefügt:

„<sup>4</sup>Die Abs. 3 bis 5 gelten im Fall der Verwendung der Daten entsprechend.“

cc) Der bisherige Satz 4 wird Satz 5.

e) Der bisherige Abs. 4 wird aufgehoben.

f) Abs. 5 erhält folgende Fassung:

„(5) <sup>1</sup>Daten, die einem Vertrauensverhältnis zwischen engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Abs. 1 Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben, sind unverzüglich zu löschen, es sei denn ihre Verwendung ist zur Verhütung einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. <sup>2</sup>Die durch eine Maßnahme nach Abs. 1 Satz 1 erlangten personenbezogenen Daten,

1. deren Verwendung zu den in Abs. 3 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. <sup>3</sup>Im Fall der Unterrichtung des Betroffenen sind die Daten zu löschen, wenn der Betroffene nach Ablauf eines Monats nach seiner Benachrichtigung keine Klage erhebt; auf diese Frist ist in der Benachrichtigung hinzuweisen. <sup>4</sup>Im Fall einer gerichtlichen Überprüfung sind die Daten nach deren Abschluss zu löschen.“

g) Der bisherige Abs. 6 wird Abs. 7 und wie folgt geändert:

Die Worte „nach Absatz 3“ werden durch die Worte „nach Abs. 6“ ersetzt.

h) Abs. 7 wird Abs. 8 und erhält folgende Fassung:

„(8) Das Brief- und das Postgeheimnis bleiben unberührt.“

4. Es werden folgende Art. 34a bis 34c eingefügt:

„Art. 34a

Datenerhebung und Eingriffe in den Telekommunikationsbereich

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

1. über die für eine Gefahr Verantwortlichen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist,
2. über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass
  - a) sie eine schwerwiegende Straftat begehen wollen oder
  - b) sie für Personen nach Buchst. a oder nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben oder
  - c) die unter Buchst. a oder Nr. 1 genannten Personen ihre Kommunikationseinrichtungen benutzen.

<sup>2</sup>Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise gefährdet oder erheblich erschwert wäre. <sup>3</sup>Datenerhebungen werden unzulässig, wenn in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, es sei denn die Maßnahme richtet sich gegen den Berufsgeheimnisträger selbst, könnte sich gegen diesen richten oder ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich.

(2) <sup>1</sup>Die 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.

<sup>2</sup>Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. <sup>3</sup>Solche Daten dürfen über den Datenabgleich zur Ermittlung spezifischer Kennungen hinaus nur verwendet werden, um Straftaten zu verfolgen oder schwerwiegende Straftaten

zu verhüten oder zu unterbinden. <sup>4</sup>Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen, soweit sie nicht nach Satz 3 benötigt werden.

- (3) <sup>1</sup>Die 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.

<sup>2</sup>Weitergehende Maßnahmen nach Art. 34b Abs. 1 und 2 bleiben unberührt.

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

#### Art. 34b

##### Mitwirkungspflichten der Diensteanbieter

(1) Ist eine Datenerhebung nach Art. 34a Abs. 1 oder Abs. 3 Satz 1 Nr. 1 angeordnet, hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in der jeweils geltenden Fassung der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.

(2) <sup>1</sup>Die Polizei kann unter den Voraussetzungen des Art. 34a Abs. 1 Satz 1 oder Abs. 3 Satz 1 Diensteanbieter verpflichten,

1. ihr vorhandene Telekommunikationsverbindungsdaten der in Art. 34a Abs. 1 Satz 1 und Abs. 3 Satz 1 genannten Personen zu übermitteln,

2. Daten über deren zukünftige Telekommunikationsverbindungen zu speichern und ihr zu übermitteln oder
3. ihr die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartenummer mitzuteilen.

<sup>2</sup>Die Übermittlung von Daten über Telekommunikationsverbindungen, die zu diesen Personen hergestellt worden sind, darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung ihres Aufenthaltsorts auf andere Weise erheblich erschwert wäre. <sup>3</sup>Die Daten sind der Polizei unverzüglich oder innerhalb der in der Anordnung bestimmten Zeitspanne sowie auf dem darin bestimmten Übertragungsweg zu übermitteln.

(3) Telekommunikationsverbindungsdaten sind alle nicht inhaltsbezogenen Daten, die im Zusammenhang mit einer Telekommunikation auch unabhängig von einer konkreten Telekommunikationsverbindung technisch erhoben und erfasst werden, insbesondere

1. Berechtigungskennung, Kartenummer, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,
2. Beginn und Ende der Verbindung nach Datum und Uhrzeit,
3. vom Kunden in Anspruch genommene Telekommunikationsdienstleistung,
4. Endpunkte fest geschalteter Verbindungen, ihr Beginn und Ende nach Datum und Uhrzeit.

#### Art. 34c

Verfahrensregelungen, Verwertungsverbote, Zweckbindung, Benachrichtigung und Löschung

(1) <sup>1</sup>Maßnahmen nach Art. 34a und Art. 34b dürfen nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 33 Abs. 5 Sätze 1 und 2 genannten Dienststellenleiter. <sup>2</sup>Die Anordnung eines Dienststellenleiters tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem

Richter bestätigt wird. <sup>3</sup>Art. 24 Abs. 1 Satz 3 findet entsprechende Anwendung. <sup>4</sup>Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat.

(2) <sup>1</sup>Soweit 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 Nr. 1 bis 3 POG genannten Dienststellen oder des Landeskriminalamtes angeordnet werden.

<sup>2</sup>Diese können die Anordnungsbefugnis auf besonders Beauftragte übertragen.

(3) Anordnungen nach den Abs. 1 und 2 sind schriftlich zu erlassen und zu begründen; bei Gefahr im Verzug ist ausreichend, wenn eine mündliche Anordnung unverzüglich unter Angabe der für sie maßgeblichen Gründe schriftlich bestätigt wird. <sup>2</sup>Die 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 erheblichen Gefahr für Leben, Gesundheit oder Freiheit einer Person genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation. <sup>3</sup>In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. <sup>4</sup>Die 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.

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

(4) <sup>1</sup>Die durch eine Maßnahme nach Art. 34a und 34b erlangten personenbezogenen Daten sind besonders zu kennzeichnen. <sup>2</sup>Sie dürfen nur verwendet werden

1. zu den Zwecken, zu denen sie erhoben wurden sowie

2. zu Zwecken der Strafverfolgung, wenn die Voraussetzungen der Strafprozessordnung für die Verwertung der Daten vorliegen oder für die Datenerhebung bei der Erhebung vorgelegen haben; eine Zweckänderung ist festzustellen und zu dokumentieren.

<sup>3</sup>Daten, bei denen sich nach Auswertung herausstellt, dass

1. die Voraussetzungen für ihre Erhebung nicht vorgelegen haben oder
2. sie einem Vertrauensverhältnis zwischen engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 Buchst. a genannten Gefahren oder Straftaten haben, dürfen nicht verwendet werden, es sei denn ihre Verwendung ist zur Verhütung einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich.

(5) <sup>1</sup>Von 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.

<sup>2</sup>Die 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 Buchst. a genannten Rechtsgüter geschehen kann. <sup>3</sup>Art. 34 Abs. 4 Sätze 2 bis 6 gelten entsprechend.

(6) <sup>1</sup>Daten, die einem Vertrauensverhältnis zwischen engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsheimnisträgern zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 Buchst. a genannten Gefahren oder Straftaten haben, sind unverzüglich zu löschen, es sei denn ihre Verwendung ist zur Verhütung einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. <sup>2</sup>Die 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. <sup>2</sup>Art. 34 Abs. 5 Sätze 3 und 4 gelten entsprechend.“
5. In Art. 36 Abs. 1 Nr. 2 werden die Worte „im Sinn von Art. 30 Abs. 5“ durch die Worte „von erheblicher Bedeutung“ ersetzt.
6. Art. 38 wird wie folgt geändert:
- a) Es wird folgender neuer Abs. 3 eingefügt:

„(3) <sup>1</sup>Die durch den Einsatz automatisierter Kennzeichenerkennungssysteme nach Art. 33 Abs. 2 Satz 2 erlangten personenbezogenen Daten sind nach Durchführung des Datenabgleichs unverzüglich zu löschen. <sup>2</sup>Soweit ihre Speicherung, Veränderung oder Nutzung im einzelnen Fall zur Verfolgung von Straftaten, von Ordnungswidrigkeiten, zur Abwehr einer Gefahr oder im Rahmen einer längerfristigen Observation oder polizeilichen Beobachtung erforderlich ist, gelten abweichend hiervon die Vorschriften der Strafprozessordnung, des Gesetzes über Ordnungswidrigkeiten sowie die Abs. 1 und 2.“
  - b) Die bisherigen Abs. 3 und 4 werden Abs. 4 und 5.
7. Art. 40 wird wie folgt geändert:
- a) In Abs. 2 werden nach den Worten „öffentliche Stellen“ das Komma und die Worte „sowie an Behörden und sonstige Stellen außerhalb des Geltungsbereichs des Grundgesetzes und an über- und zwischenstaatliche Stellen“ gestrichen.

- b) In Abs. 3 wird das Wort „Gefahrenabwehr“ durch die Worte „Abwehr von Gefahren“ ersetzt.
- c) In Abs. 4 wird das Wort „ist“ durch das Wort „erscheint“ ersetzt.
- d) Abs. 5 erhält folgende Fassung:

„(5) <sup>1</sup>Die Polizei kann von sich aus oder auf Ersuchen personenbezogene Daten an Behörden und Stellen mit polizeilichen Aufgaben und sonstige Behörden und Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen übermitteln, soweit dies

1. zur Erfüllung polizeilicher Aufgaben erforderlich ist,
2. zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint und die Polizei hierzu auf Grund von Rechtsvorschriften der Europäischen Union, völkerrechtlicher Vereinbarungen oder sonstiger internationaler Verpflichtungen der Bundesrepublik Deutschland ermächtigt ist oder
3. zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich erscheint.

<sup>2</sup>Die Datenübermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass sie gegen den Zweck eines Bundes- oder Landesgesetzes verstoßen würde oder schutzwürdige Interessen des Betroffenen beeinträchtigt würden.“

- 8. In Art. 42 Abs. 3 wird das Wort „sonstige“ durch die Worte „Stellen mit polizeilichen Aufgaben und sonstige Behörden und“ ersetzt.

- 9. Dem Art. 46 Abs. 2 wird folgender Satz 4 angefügt:

„<sup>4</sup>Abfragen anlässlich des Einsatzes automatisierter Kennzeichenerkennungssysteme dürfen nicht protokolliert werden.“

10. Art. 61 wird wie folgt geändert:

- a) Der Wortlaut in Abs. 4 wird Satz 1 und nach dem Wort „Schlagstock,“ werden die Worte „Elektroimpulsgerät und vergleichbare Waffen,“ eingefügt.
- b) Es wird folgender Satz 2 angefügt:  
„<sup>2</sup>Waffen können auf Anordnung des Staatsministeriums des Innern zeitlich befristet als Einsatzmittel erprobt werden.“

11. In Art. 74 werden nach den Worten „Unverletzlichkeit der Wohnung“ die Worte „und das Fernmeldegeheimnis“, nach den Worten „Art. 2 Abs. 2 Sätze 1 und 2,“ die Worte „Art. 10,“ und nach den Worten „Art. 106 Abs. 3“ die Worte „ , Art. 112 Abs. 1“ eingefügt.

## **§ 2**

### **Änderung des Parlamentarischen Kontrollgremium - Gesetzes**

Das Gesetz zur parlamentarischen Kontrolle der Staatsregierung hinsichtlich der Maßnahmen nach Art. 13 Abs. 3 bis 5 des Grundgesetzes sowie der Tätigkeit des Landesamts für Verfassungsschutz (Parlamentarisches Kontrollgremium - Gesetz – PKGG) in der Fassung und Bekanntmachung vom 10. Februar 2000 (GVBl S. 40, BayRS 12-4-I), zuletzt geändert durch § 1 Nr. 6 des Gesetzes vom 7. August 2003 (GVBl S. 497), wird wie folgt geändert:

1. In Art. 1 Abs. 1 Satz 1 werden die Worte „Art. 34 Abs. 6“ durch die Worte „Art. 34 Abs. 7“ ersetzt.
2. In Art. 3 Abs. 2 Satz 1 werden die Worte „Art. 34 Abs. 6“ durch die Worte „Art. 34 Abs. 7“ ersetzt.

**§ 3**

**In-Kraft-Treten**

Dieses Gesetz tritt am \_\_\_\_.2004 in Kraft.

## **Begründung:**

### **A. Allgemeines**

1. Die im Zuge der allgemeinen Internationalisierung der Personen-, Waren-, Dienstleistungs- und Finanzströme zunehmende grenzüberschreitende Kriminalität, die fortschreitende europäische Integration und die Bedrohungen durch den internationalen Terrorismus zwingen dazu, das polizeiliche Handeln immer effizienter zu gestalten. Das gilt insbesondere für die Möglichkeiten, verschiedenste Arten von Kontrollen zu vereinfachen und zu beschleunigen, aber auch für die Durchführung von Schutz-, Überwachungs- und Ermittlungsmaßnahmen.

Der technische Fortschritt eröffnet der Polizei fortlaufend Möglichkeiten zur Optimierung ihrer Aufgabenerfüllung, indem er neue Technologien zur Verfügung stellt. Dazu zählen die verschiedenen Formen automatisierter Kennzeichenerkennungssysteme, durch die die Kennzeichen von Kraftfahrzeugen erfasst und mit dem Fahndungsbestand oder im Einzelfall auch sonstigen Dateien abgeglichen werden können.

Mit drei Beschlüssen vom 28. Januar 2004 (LT-Drs. 15/238, 15/239 und 15/241) hat der Bayerische Landtag nach dem erfolgreichen Abschluss eines Pilotversuchs der Bayerischen Polizei an den Grenzübergängen Schirnding und Waidhaus-Autobahn sowie auf der BAB 8 München-Salzburg die Schaffung einer gesetzlichen Regelung zum Einsatz automatisierter Kennzeichenerkennungssysteme gefordert. Als wichtigstes Tor Deutschlands und Westeuropas und als Transitland nach Ost- und Südosteuropa hat Bayern eine besondere sicherheitspolitische Verantwortung. Dabei gilt es einem möglichen Kriminalitätsimport und Gefahrentransit zu begegnen und so einen nachhaltigen Beitrag zur Ausgestaltung Europas als Raum der Freiheit, der Sicherheit und des Rechts zu leisten. Dies kann ohne den Einsatz neuer technischer Möglichkeiten zur Kriminalitätsbekämpfung nicht gelingen. Darüber hinaus kann nur so dem internationalen Terrorismus begegnet und den Schengen-Vorgaben für effektive Grenzkontrollen entsprochen werden.

Da es sich bei Kraftfahrzeugkennzeichen wegen ihrer Zuordnung zu einem bestimmten Kraftfahrzeughalter um personenbezogene Daten handelt und durch die Kenn-

zeichenerfassung zunächst festgehalten wird, dass sich das Fahrzeug einer bestimmten Person zu einer bestimmten Zeit an einem bestimmten Ort befindet, stellt der Einsatz solcher Systeme einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG dar. Ein solcher Eingriff ist nach der Rechtsprechung des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) zulässig, wenn er im überwiegenden Allgemeininteresse unter Beachtung des Gebots der Normenklarheit und des Grundsatzes der Verhältnismäßigkeit erfolgt.

Der vorliegende Gesetzentwurf schafft die rechtlichen Voraussetzungen, um automatisierte Kennzeichenerkennungssysteme unter Beachtung der Erfordernisse des Datenschutzes in der polizeilichen Praxis effektiv einsetzen zu können. Da beim Einsatz automatisierter Kennzeichenerkennungssysteme sowohl Aspekte der Datenerhebung wie auch der Datenspeicherung und des Datenabgleichs betroffen sind, diese unterschiedlichen Eingriffsformen aber in verschiedenen Artikeln des III. Abschnitts des Gesetzes geregelt sind, werden die Art. 33, 38 und 46 ergänzt.

2. Die Wohnraumüberwachung zu präventiven Zwecken stellt in Zeiten wachsender Bedrohung durch den internationalen Terrorismus und durch die Erscheinungsformen der Organisierten Kriminalität eine wichtige Befugnis zur Gefahrenabwehr dar. Es ist erforderlich, die Ermittlungen in den inneren Kreis krimineller Organisationen zu tragen, um eine wirksame Prävention zu gewährleisten. Herkömmliche Befugnisse reichen vielfach nicht aus, um bei arbeitsteilig vorgehenden Banden, die sich fast völlig nach außen abschotten, in den Kernbereich vorzudringen. Dies ist aber unerlässlich, um künftige Gefahren, die durch die Formen schwerwiegender und grenzüberschreitend agierender Kriminalität drohen, abzuwehren und Straftaten zu verhindern bzw. zu unterbinden. Das Bundesverfassungsgericht hat in seinem Urteil vom 3. März 2004 zur repressiven Wohnraumüberwachung (Az.: 1 BvR 2378/98, 1 BvR 1084/99) die Erforderlichkeit der Eingriffe in das Grundrecht aus Art. 13 Abs. 1 GG anerkannt und das Instrument der Wohnraumüberwachung im Grundsatz für verfassungsmäßig erklärt. Unmittelbar wurde in dem Urteil nur über die Verfassungsmäßigkeit der §§ 100c ff. StPO entschieden. Verfahrensgegenstand war lediglich die repressive Wohnraumüberwachung und nicht der Bereich der Gefahrenabwehr, zu

dem sich das Bundesverfassungsgericht nur ansatzweise geäußert hat. Dennoch ergeben sich aus den dargelegten Grundsätzen für Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung Auswirkungen, die auch im Zusammenhang mit der Ausgestaltung der präventiven Wohnraumüberwachung nach Art. 34 PAG zu beachten sind.

Dabei ist allerdings zu berücksichtigen, dass der Prävention im Vergleich zur Strafverfolgung jedenfalls in Bezug auf hinreichend gewichtige Rechtsgüter ein grundsätzlich höheres verfassungsrechtliches Gewicht im Rahmen der Rechtsgüterabwägung zukommt, da Ziel der Rechtsgüterschutz und nicht lediglich die Ahndung begangener Straftaten ist. Für die Wohnraumüberwachung folgt dies bereits aus den unterschiedlichen verfassungsrechtlichen Regelungen in Art. 13 Abs. 3 und Abs. 4 GG. Während Art. 13 Abs. 3 GG für die repressive Wohnraumüberwachung den Verdacht besonders schwerer Straftaten verlangt, reicht für die präventive Wohnraumüberwachung nach Art. 13 Abs. 4 GG eine Gefahr für die öffentliche Sicherheit aus, die allerdings eine dringende sein muss. Der Menschenwürdegehalt des Art. 13 Abs. 1 GG gebietet jedoch einen umfassenden Schutz des Kernbereichs privater Lebensgestaltung, auch im Bereich der präventiven Befugnisse zur Wohnraumüberwachung.

Zusätzlich wird der Schutz auf Berufsgeheimnisträger ausgedehnt. Zu diesen zählen insbesondere Ärzte, Anwälte und Geistliche. Die Schutzwirkungen gehen über die verfassungsrechtlichen Mindestanforderungen hinaus, um auch die zu Journalisten und Abgeordneten bestehenden Vertrauensverhältnisse zu schützen. Bei der Zweckbindung der Daten und der damit in Zusammenhang stehenden Kennzeichnungspflicht sind zusätzliche verfahrensrechtliche Sicherungen vorzusehen. Das Spannungsfeld zwischen Löschung der Daten und den Interessen am effektiven Rechtsschutz ist unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts zu einem neuen Ausgleich zu bringen.

3. Die Sicherheitslage hat sich in Europa durch die Ereignisse des 11. September 2001 und die nachfolgenden Terroranschläge, nicht zuletzt durch das Attentat von Madrid am 11. März 2004, grundlegend geändert. Neben der zunehmenden „Globalisierung“ des (internationalen) Terrorismus stellt auch die Bekämpfung grenzüberschreitend organisierter krimineller Banden die europäischen Sicherheitsbehörden vor neue Herausforderungen. Diese Erscheinungsformen der Kriminalität sind von

einem hohen Maß an Konspirativität geprägt. Die oftmals über Ländergrenzen hinaus vernetzt arbeitenden Täter treffen vielfach Absprachen über das Telefon und über andere moderne Telekommunikationsmittel.

Zur Bekämpfung dieser Bedrohungen ist es erforderlich, der Polizei die Instrumente, die sie im Bereich der Strafverfolgung bereits seit geraumer Zeit erfolgreich einsetzt, im Bereich der Gefahrenabwehr nicht länger vorzuenthalten. Den präventiven Maßnahmen kommt eine eigenständige Bedeutung zu, da der Schutz von Leib, Leben, Freiheit und anderen hochwertigen Rechtsgütern nicht allein davon abhängen kann, dass bereits ein strafbares Handeln vorliegt. Sicherheitspolitisch ist es nicht vertretbar, der Polizei zur Verhütung schwerwiegender Straftaten Mittel vorzuenthalten, die ihr nach begangener Tat zur Aufklärung zur Verfügung stehen. Voraussetzung ist dabei allerdings, dass die Verletzung hinreichend gewichtiger Rechtsgüter bzw. die Begehung schwerwiegender Straftaten droht und dass eine ausreichende Wahrscheinlichkeit für eine Gefährdungslage vorliegt.

Die präventivpolizeiliche Telekommunikationsüberwachung ist nicht nur zur Bekämpfung der Organisierten Kriminalität und des Terrorismus sondern auch zur Verhinderung und Unterbindung anderer schwerwiegender Straftaten unverzichtbar. Zu nennen sind insbesondere Geisellagen und Entführungen, die Bekämpfung des Schleuserwesens, des politischen Extremismus sowie der Verbreitung von Kinderpornografie über das Internet. Zur präventiven Bekämpfung dieser Deliktsfelder muss der Polizei die Überwachung der Telekommunikation ermöglicht werden, da auch in diesem Bereich die Tätergruppierungen unter Verwendung von Telekommunikationsmitteln professionell arbeitsteilig und stark abgeschottet zusammenwirken.

Angesichts der rasch fortschreitenden technischen Entwicklung ist es auch erforderlich, dass die Sicherheitsbehörden in Extremsituationen Telekommunikationsverbindungen unterbrechen oder verhindern können, wenn etwa die Zündung von Sprengkörpern über Mobiltelefone erfolgen soll. Die Anschläge von Madrid haben gezeigt, dass zur Durchführung von Attentaten auf modernste Telekommunikationstechnik zurückgegriffen wird. Einen wichtigen Anwendungsfall für die Praxis stellt auch der Einsatz von Ortungsgeräten, wie des sog. „IMSI-Catchers“, dar, insbesondere bei der Standortbestimmung vermisster oder hilfloser Personen.

Die Befugnisnormen orientieren sich ebenso wie die verfahrensrechtlichen Sicherungen sowohl an den verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht in seinen Urteilen vom 3. März 2004 zur repressiven Wohnraumüberwachung

(Az.: 1 BvR 2378/98, 1 BvR 1084/99) und zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz (Az.: 1 BvF 3/92) aufgezeigt hat, als auch an den datenschutzrechtlichen Erfordernissen. Dabei wurden die Besonderheiten des Gefahrenabwehrrechts einbezogen.

Besonders geschützt sind die Vertrauensverhältnisse zwischen dem Adressaten der Maßnahme und Berufsheimnisträgern wie Anwälten, Ärzten, Geistlichen und Journalisten. Über die verfassungsrechtlichen Erfordernisse hinaus werden diese Vertrauensverhältnisse von der Überwachung ausgenommen. Abhörmaßnahmen, die in eine solche Vertrauensbeziehung eingreifen, sind unzulässig. Stellt sich das Bestehen des Vertrauensverhältnisses erst im Lauf der Maßnahme heraus, dürfen die Daten nicht verwertet werden. Zusätzlich bestehen ebenso wie bei Vertrauensbeziehungen zu anderen Personen Verwertungsverbote. Dadurch werden vertrauenswürdige und geheimhaltungsbedürftige Telekommunikationsdaten dem sicherheitsbehördlichen Zugriff bzw. der Verwertung entzogen. Der Schutz ist nicht erforderlich, wenn die Maßnahme (auch) gegen die jeweiligen Vertrauenspersonen gerichtet ist. Darüber hinaus sind Ausnahmen nur dann vorgesehen, wenn es kein milderes Mittel zur Abwehr einer gegenwärtigen Gefahr für die besonders wichtigen Rechtsgüter Leib, Leben und Freiheit einer Person gibt.

Nach Art. 73 Nr. 7 GG hat der Bund die ausschließliche Gesetzgebungszuständigkeit auf dem Gebiet der Telekommunikation. Unter Telekommunikation in diesem Sinn sind die entsprechenden Kommunikationsdienste und -dienstleistungen einschließlich der in diesem Zusammenhang zu regelnden Fragen der Technik, Organisation, Rechtsverhältnisse der Beteiligten u.ä. zu verstehen. Die Länder sind hingegen nach Art. 70 Abs. 1 GG für den Bereich des Gefahrenabwehr- und damit des Polizeirechts zuständig.

Der Text des Art. 10 Abs. 2 Satz 1 GG verzichtet darauf, die einschränkenden Gesetze dem Bundesgesetzgeber vorzubehalten; aus der Formulierung „aufgrund eines Gesetzes“ folgt, dass auch der Landesgesetzgeber die Grundrechte aus Art. 10 GG einschränkende Gesetze erlassen darf (vgl. v. Münch/Kunig Grundgesetz-Kommentar, 5. Auflage, Art. 10, Rn. 29). Daher bleibt es dem Landesgesetzgeber unbenommen, Beschränkungen des Fernmeldegeheimnisses zum Zwecke der Gefahrenabwehr bereichsspezifisch zu regeln.

Die konkrete Abwicklung einer landesgesetzlich zugelassenen Telekommunikationsüberwachung unterliegt hingegen der ausschließlichen Gesetzgebungszuständigkeit des Bundes: Die hierzu ergangene, auf § 88 des Telekommunikationsgesetzes (TKG; BGBl. I 1996, S. 1120) gestützte, Telekommunikations-Überwachungsverordnung (TKÜV; BGBl. I 2002, S. 458) gilt jedoch derzeit ausdrücklich nur für die namentlich genannten Bundesgesetze (§ 1 Nr. 1 TKÜV), obwohl die Ermächtigungsgrundlage eine solche Differenzierung nicht vornimmt. Auf die bundesrechtlichen Regelungen wird im Wege einer dynamischen Verweisung Bezug genommen.

Grundsätzlich beschränkt sich die Gesetzgebungshoheit des Freistaats Bayern auf dessen Staatsgebiet, so dass landesrechtlich begründete Pflichten regelmäßig nur die natürlichen oder juristischen Personen treffen, die zum Landesgebiet einen rechtserheblichen Bezug – je nach Rechtsmaterie etwa tatsächlichen Aufenthalt, Wohn- oder Unternehmenssitz o.ä. – haben. Allerdings hat das Bundesverwaltungsgericht entschieden, dass eine solche Beschränkung nicht generell angenommen werden kann, wenn es lediglich um die Möglichkeit geht, ein auf den Landesbereich beschränktes Gesetz wirksam zu vollziehen (BVerwGE 79, 339 ff.). Dementsprechend ist zu unterscheiden zwischen der Maßnahme zum Vollzug eines Landesgesetzes und den der Durchsetzung dieser Maßnahme dienenden Hilfsmaßnahmen. Aus der Entscheidung des Bundesverwaltungsgerichts kann der Schluss gezogen werden, dass auch natürliche oder juristische Personen mit Sitz außerhalb Bayerns Adressaten landesrechtlich begründeter Pflichten sein können, wenn die Maßnahme als solche, zu deren Durchsetzung sie in Anspruch genommen werden, in die Gesetzgebungskompetenz des Landesgesetzgebers fällt. Daher können auch solche Diensteanbieter, deren Firmensitz sich außerhalb Bayerns befindet, zur Unterstützung der Polizei nach Art. 34 b Abs. 1 und 2 verpflichtet werden. Maßgeblicher Anknüpfungspunkt ist, dass die verpflichteten Diensteanbieter auch in Bayern ihre Dienste anbieten und damit auch in Bayern den Adressaten einer Maßnahme nach Art. 34 a die Möglichkeit eröffnen, Telekommunikationsdienste zu nutzen, die durch die polizeiliche Maßnahme überwacht werden sollen. Aus diesem Grund ist es auch gerechtfertigt, sie zur Unterstützung polizeilicher Maßnahmen in Anspruch zu nehmen.

4. Polizeiliche Gefahrenabwehr und Strafverfolgung wurden in Deutschland und Europa in der Vergangenheit lange als nahezu ausschließlich interne Angelegenheit eines Staates begriffen.

Nicht zuletzt unter dem Eindruck der neuen terroristischen Bedrohungslage nach den Anschlägen des 11. September 2001 in den USA und des 11. März 2004 in Spanien, verstärkt international agierender Strukturen der Organisierten Kriminalität, aber auch des weitgehenden Zusammenwachsens grenznaher Regionen zu einheitlichen kriminal- und gefahrengeografischen Räumen als Folge des Wegfalls der systematischen Kontrollen an den Schengen-Binnengrenzen hat sich das praktische Erfordernis eines effektiven Zusammenwirkens der europäischen Polizeien beständig entwickelt. Wesentliches Kernelement der Zusammenarbeit ist dabei stets der Austausch personenbezogener Daten, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung erforderlich ist. Auf völkerrechtlicher Ebene hat der Bund eine Vielzahl von Verträgen zur Polizeikooperation geschlossen, die u. a. den Austausch von Informationen und personenbezogenen Daten vorsehen (vgl. die Vereinbarungen z. B. mit der Schweiz, Österreich, der Tschechischen Republik, Polen und den Niederlanden), oder im Rahmen der Europäischen Union entsprechenden Rechtsinstrumenten zugestimmt.

Soweit diese vom Bund im Einvernehmen mit den Ländern ratifizierten Rechtsinstrumente neue Möglichkeiten des polizeilichen Datenaustausches mit nichtinnerstaatlichen Stellen vorsehen, ist deren Transformation in das Polizeirecht sicherzustellen. Hierzu werden die Vorschriften über die Datenübermittlung innerhalb des öffentlichen Bereichs (Art. 40 und 42) überarbeitet.

## **B. Zwingende Notwendigkeit einer normativen Regelung**

Mit dem vorliegenden Gesetzentwurf soll die Polizei in erster Linie diejenigen neuen Befugnisse erhalten, auf die sie auf Grund aktueller Entwicklungen im Bereich der Organisierten Kriminalität und des internationalen Terrorismus, aber auch im Hinblick auf die fortschreitende Entwicklung Europas zu einem Raum der Freiheit, der Si-

cherheit und des Rechts zur Aufrechterhaltung der inneren Sicherheit nicht länger verzichten kann. Daneben werden aber auch bestehende Befugnisse überarbeitet, etwa um Vorgaben gerecht werden zu können, die sich für die Bundesrepublik Deutschland aus Rechtsakten der Europäischen Union, völkerrechtlichen Vereinbarungen über Polizeikooperationen oder sonstigen internationalen Verpflichtungen ergeben. Macht die Polizei von solchen Befugnissen Gebrauch, so greift sie in die Grundrechte der hiervon betroffenen Personen ein, was nach dem Grundsatz vom Vorbehalt des Gesetzes das Vorliegen einer entsprechenden gesetzlichen Ermächtigung voraussetzt. Die Schaffung zusätzlicher bzw. die Modifizierung bestehender präventiver Eingriffsbefugnisse für die Polizei kann daher aus verfassungsrechtlichen Gründen nur durch eine Ergänzung bzw. Änderung des Polizeiaufgabengesetzes erfolgen.

### **C. Begründung der einzelnen Vorschriften**

Zu § 1 Änderung des Polizeiaufgabengesetzes

Zu § 1 Nr. 1 (Art. 30 Abs. 5)

In Absatz 5 Satz 1 werden die schwerwiegenden Straftaten, zu deren Verhinderung Grundrechtseingriffe insbesondere in Art. 10 Abs. 1 und Art. 13 Abs. 1 GG zulässig sind, abschließend aufgezählt. Die Delikte sind bestimmt genug und vom Strafmaß ausreichend gewichtig. Die aufgeführten Katalogtaten dienen dem Schutz wichtiger Rechtsgüter, die nicht ohne weiteres als Gefahren für die Öffentliche Sicherheit und Ordnung benannt werden können, deren Schutz aber in besonderem Maße geboten ist. Dabei wurde der Bekämpfung von Straftaten, die bandenmäßig, gewerbsmäßig oder gewohnheitsmäßig begangen werden sowie der Straftaten, die im Zusammenhang mit den Erscheinungsformen der Organisierten Kriminalität stehen, ein besonderes Gewicht beigemessen. Voraussetzung war jedoch, dass es sich auch nach dem oberen Strafraum um schwerwiegende Straftaten handelt, die den Bereich der mittleren Kriminalität überschreiten oder zumindest an dessen Obergrenze liegen. Bei der Gefahrenabwehr sind neben dem Strafmaß aber die Gefahren, die für

die Öffentliche Sicherheit und Ordnung von den jeweiligen Straftaten ausgehen, in die Abwägung einzubeziehen. Soweit die Strafbarkeit vom Nichtvorliegen einer Gestattung oder von verwaltungsrechtlichen Vorfragen abhängt, wird klargestellt, dass die Erteilung offensichtlich nicht in Betracht kommen darf. Dadurch wird die Bestimmtheit der Eingriffsregelung trotz der Verwaltungsakzessorietät gewährleistet. Offensichtlichkeit liegt dann vor, wenn keine vernünftigen Zweifel daran bestehen können, dass die verwaltungsrechtlichen Voraussetzungen für die Strafbarkeit vorliegen.

Die bisherige Regelung des Art. 30 Abs. 5 PAG wird zu Satz 2. Die schwerwiegenden Straftaten sind ausnahmslos auch Straftaten von erheblicher Bedeutung.

Zu § 1 Nr. 2 (Art. 33 Abs. 2 Satz 2)

Mit dieser Vorschrift wird der Einsatz automatisierter Kennzeichenerkennungssysteme auf eine rechtliche Grundlage gestellt.

Die spezielle Regelung des Einsatzes automatisierter Kennzeichenerkennungssysteme ist notwendig, da das geltende Recht diesen nur in eingeschränktem Umfang ermöglicht. So setzt beispielsweise Art. 43 Abs. 1 Satz 3 für einen Abgleich mit dem Fahndungsbestand voraus, dass die personenbezogenen Daten von der Polizei im Rahmen ihrer Aufgabenerfüllung erlangt wurden. Dies ermöglicht zwar bereits jetzt den Abgleich von Kennzeichen, die bei der Verfolgung einer Verkehrsordnungswidrigkeit – etwa einer Geschwindigkeitsüberschreitung – gemäß § 46 Abs. 1 OWiG i. V. m. § 100c Abs. 1 Nr. 1 lit. a) StPO erhoben wurden, nicht aber den Abgleich an einem Grenzübergang, einer sonstigen Kontrollstelle, vor einem besonders gefährdeten Objekt oder auf einer Durchgangsstraße, da das Kennzeichen hier allein zum Zweck des Abgleichs erfasst wird und das Datum daher nicht im Rahmen der (anderweitigen) Aufgabenerfüllung der Polizei erlangt wurde. Auch der im Wege eines „argumentum a maiore ad minus“ zu erwägende Rückgriff auf die Vorschrift des Art. 13 über die viel umfangreichere Identitätsfeststellung, in deren Rahmen gemäß Absatz 3 die Vorlage des Fahrzeugscheins verlangt und das daraus ersichtliche Kennzeichen mit dem Fahndungsbestand abgeglichen werden könnte, erweist sich wegen der andersartigen Eingriffsqualität und Zielrichtung des automatisierten Kennzeichenabgleichs sowie des für Eingriffe in das Recht auf informationelle Selbstbestim-

mung im Besonderen geltenden Gebots der Normenklarheit als unzureichend. Art. 33 Abs. 2 wiederum lässt zwar bereits jetzt den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder –aufzeichnungen zu, setzt hierfür aber Hürden, die einem Einsatz automatisierter Kennzeichenerkennungssysteme allein zum Zweck des Datenabgleichs entgegenstehen. Schließlich ist die Schaffung gesetzlicher Regeln für den Einsatz automatisierter Kennzeichenerkennungssysteme aber auch aus Gründen der Bereichsspezifität zu befürworten. Dabei ist ein angemessener Ausgleich zwischen der an polizeilichen Bedürfnissen orientierten Ergänzung der präventiven Befugnisse einerseits und der Wahrung des erforderlichen Grundrechtsschutzes andererseits vorzunehmen.

Automatisierte Kennzeichenerkennungssysteme sind ohne Weiteres als technische Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen im Sinn des Absatzes 1 Nr. 2 und damit als besondere Mittel der Datenerhebung anzusehen. Absatz 2 erlaubt den Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und –aufzeichnungen bislang dann, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise gefährdet oder wesentlich erschwert würde. Damit ist es zwar beispielsweise möglich, zur Abwehr einer Gefahr Bildaufnahmen von einer bestimmten Örtlichkeit anzufertigen und so mit Hilfe der erfassten Kennzeichen festzustellen, ob ein bestimmtes Fahrzeug diese Örtlichkeit auffallend häufig passiert. Die Vorschrift schließt jedoch den Einsatz automatisierter Kennzeichenerkennungssysteme allein zum Zweck des Datenabgleichs aus. Der neu geschaffene Absatz 2 Satz 2 gestattet nunmehr die Erhebung personenbezogener Daten durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme unter den für die Vornahme einer Identitätsfeststellung geltenden Voraussetzungen des Art. 13 Abs. 1 Nrn. 1 bis 5 auch zu diesem Zweck. Die einschränkenden Vorgaben des Art. 30 Abs. 3 Satz 2 für die Zulässigkeit einer verdeckten Datenerhebung gelten insoweit nicht. Auch der Dienststellenleitervorbehalt des Absatzes 5 findet keine Anwendung, da es sich lediglich um Bildaufnahmen im Sinn des Absatzes 1 Nr. 2 handelt.

Die Norm ermöglicht die Erhebung personenbezogener Daten sowohl durch stationäre als auch durch mobile Systeme. Das hinter automatisierten Kennzeichenerkennungssystemen stehende Prinzip beinhaltet die optische Erfassung und anschließende Abbildung dreidimensionaler Gegenstände, in der Regel in digitaler Form. Automatisierte Kennzeichenerkennungssysteme gestatten in technischer Hinsicht dar-

über hinaus die Speicherung der gewonnenen Daten und deren Abgleich mit anderen Datenbeständen. Der Datenabgleich mit dem INPOL-Fahndungsbestand wird dabei in der täglichen Praxis den Regelfall darstellen. Die Vorschrift stellt daher klar, dass die Datenerhebung „zum Zwecke des Abgleichs nach Art. 43“ erfolgt. Insoweit handelt es sich um eine Rechtsgrundverweisung. Dies bedeutet, dass für den Datenabgleich die Tatbestandsvoraussetzungen des Art. 43 vorliegen müssen. Danach ist der routinemäßige Abgleich mit dem Fahndungsbestand immer möglich, da die Daten auf Grund der ausdrücklichen Ermächtigung in dem neuen Absatz 2 Satz 2 nunmehr als „im Rahmen der polizeilichen Aufgabenerfüllung erlangt“ anzusehen sind (Art. 43 Abs. 1 Satz 3). Ein darüber hinaus gehender Abgleich mit anderen polizeilichen Dateien ist dagegen nur bei Störern zulässig (Art. 43 Abs. 1 Satz 1), bei Nichtstörern nur ausnahmsweise, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist (Art. 43 Abs. 1 Satz 2). Letzteres wäre beispielsweise der Fall, wenn bei Vorfeldkontrollen zu Großveranstaltungen ein Abgleich mit polizeilichen Dateien über bekannte Störer (etwa der Datei „Gewalttäter Sport“ bei Fußballspielen) vorgenommen werden soll. Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben freilich unberührt (Art. 43 Abs. 2). Die über die Regelung der Datenerhebung hinaus erforderlichen Änderungen hinsichtlich der Datenspeicherung erfolgen in der hierfür einschlägigen Norm des Art. 38.

Die Datenerhebung wird in verdeckter Form zugelassen. Die Vorschrift trägt dem polizeilichen Bedürfnis Rechnung, präventive Wirkung nicht nur durch offenes Auftreten erzielen zu können, sondern auch durch die Erzeugung von Ungewissheit bei potentiellen Störern darüber, ob die Polizei möglicherweise verdeckt agiert. Gerade gegenüber der kriminellen Szene mit ihren vielfältigen Abschottungsmechanismen ist es zwingend geboten, der Polizei nicht nur offene, sondern auch verdeckte Maßnahmen zu gestatten. Die getroffene Regelung gestattet dem Grundsatz „a maiore ad minus“ folgend aber selbstverständlich auch die offene, also gegenüber dem Betroffenen ausdrücklich kenntlich gemachte Datenerhebung, ohne dass dies einer eigenständigen Regelung bedürfte.

Die Datenerhebung ist neben den bereits bislang von Absatz 2 gedeckten Fällen nunmehr unter den in Art. 13 Abs. 1 Nrn. 1 bis 5 genannten Voraussetzungen auch zum alleinigen Zweck des Datenabgleichs zulässig. Sie bezieht sich damit auf die

präventive Identitätsfeststellung, der eine der Datenerhebung durch automatisierte Kennzeichenerkennungssysteme ähnliche Zielrichtung zu Grunde liegt. Es handelt sich um eine in die Gesetzgebungskompetenz der Länder fallende Maßnahme der Gefahrenabwehr, was aus den Zwecken des Art. 13 Abs. 1 Nrn. 1 bis 5, auf die Bezug genommen wird, folgt. Zwar trifft es zu, dass insbesondere ein verdachtsunabhängiger Kennzeichenabgleich in den Fällen des Art. 13 Abs. 1 Nr. 5 wie die Schleierfahndung in seiner praktischen Anwendung auch Ergebnisse bringt, die dem repressiv-polizeilichen Sektor zuzurechnen sind, was sich beispielsweise dann zeigt, wenn der Kennzeichenabgleich zur Festnahme eines gesuchten Straftäters führt, der sich ins Ausland absetzen wollte. Dies ändert aber nichts an der vom Grundsatz her präventiven Zweckbestimmung der Maßnahme. Sie dient ohne konkretes Anlassverfahren der Vorsorge zur Verfolgung von bzw. der Verhütung von Straftaten. Solche Vorfeldbefugnisse sind der Gefahrenabwehr und nicht der Strafverfolgung zuzurechnen. Ferner werden durch die Maßnahme auch bereits eingetretene Störungen der öffentlichen Sicherheit beseitigt, was einen Unterfall der Gefahrenabwehr darstellt. Ausgenommen ist die Verweisung auf Art. 13 Abs. 1 Nr. 6, da es an einem Bedürfnis hierfür mangelt. In diesem Zusammenhang ist darauf hinzuweisen, dass die automatisierte Erhebung personenbezogener Daten durch Kennzeichenerkennungssysteme sich zwar im Vergleich zu bisher möglichen und zulässigen Verfahrensweisen auf eine Mehrzahl von Betroffenen beziehen kann, diesen aber nur geringe Eingriffe in ihre Grundrechte abverlangt und darüber hinaus eine Vielzahl von andernfalls in der Regel erforderlichen Kontrollen insbesondere zur Identitätsfeststellung überflüssig macht. Dabei ist auch zu berücksichtigen, dass die Daten nach Durchführung des Abgleichs unverzüglich gelöscht werden, es sei denn, dass ihre Speicherung, Nutzung oder Veränderung zu den in Art. 38 Abs. 3 Satz 2 genau benannten Zwecken (insbesondere zur Gefahrenabwehr und zur Strafverfolgung) erforderlich ist.

Die Datenerhebung zum Zweck der Abwehr einer konkreten Gefahr im Sinn des Art. 13 Abs. 1 Nr. 1 findet ihre Anwendung beispielsweise, wenn es Fahrtstrecken gefährdeter Personen zu überprüfen gilt. Hier kann eine mobile Kennzeichenerkennung zur schnellen Überprüfung der an der Strecke abgestellten Kraftfahrzeuge dienen. Andere Anwendungsfälle sind die Überwachung von Einkaufszentren, Parkplätzen und anderen Örtlichkeiten im Zusammenhang mit Überfällen oder Anschlagsdrohungen oder die Verhütung illegaler Autorennen.

Der Einsatz von automatisierten Kennzeichenerkennungssystemen an so genannten gefährlichen Orten im Sinn des Art. 13 Abs. 1 Nr. 2 wie beispielsweise Bahnhöfen, Gebäudepassagen, bestimmten Straßen oder Plätzen sowie Bordellen soll gegenüber dem an solchen Orten verkehrenden Personenkreis in erster Linie abschreckend wirken.

Insbesondere vor dem Hintergrund der Gefahren des internationalen Terrorismus vermögen Kontrollen, Schutz- und Überwachungsmaßnahmen mittels automatisierter Kennzeichenerkennungstechniken einen effektiven Schutz der in Art. 13 Abs. 1 Nr. 3 genannten gefährdeten Örtlichkeiten zu bewirken. Zu denken ist hier beispielsweise an Flughäfen, Bahnhöfe, öffentliche Verkehrsmittel, militärische Einrichtungen, Kernkraftwerke oder sonstige gefährdete Objekte wie Konsulate ausländischer Staaten, die auf Grund der aktuellen Gefährdungseinschätzung besonderen Schutzes bedürfen.

Darüber hinaus gestattet die Befugnisnorm den Einsatz automatisierter Kennzeichenerkennungssysteme in den Fällen des Art. 13 Abs. 1 Nr. 4, also an polizeilichen Kontrollstellen zur Verhinderung von Straftaten im Sinn von § 100a StPO oder § 27 des Versammlungsgesetzes. Die Vorschrift ermöglicht beispielsweise die Kennzeichenerfassung zum Zwecke des Abgleichs mit polizeilichen Dateien bekannter Störer von Demonstrationen. Auf diese Art und Weise lassen sich sonst erforderliche umfangreiche Kontrollen im Interesse der davon ebenfalls betroffenen friedlichen Versammlungsteilnehmer zeitlich minimieren.

Schließlich kommt die Nutzung von automatisierten Kennzeichenerkennungssystemen auch zur wirkungsvollen Unterstützung der Schleierfahndung gemäß Art. 13 Abs. 1 Nr. 5 in Frage. Damit wird insbesondere der automatisierte Kennzeichenabgleich auf Bundesautobahnen und Grenzübergängen möglich. Letzteres ermöglicht es der Polizei auch, ihre Verpflichtungen aus Art. 6 des Schengener Durchführungsübereinkommens effektiv zu erfüllen.

Zu § 1 Nr. 3 (Art. 34)

1. Art 34 PAG wird an die Vorgaben des Urteils des Bundesverfassungsgerichts zur repressiven Wohnraumüberwachung vom 3. März 2004 (Az.: 1 BvR 2378/98, 1 BvR

1084/99) und des Urteils zur Verfassungsmäßigkeit der Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz vom 3. März 2004 (Az.: 1 BvF 3/92) angepasst. Das Bundesverfassungsgericht hat klargestellt, dass die wirksame Aufklärung schwerer Straftaten und der Schutz der Bevölkerung vor der Begehung derartiger Delikte wesentlicher Auftrag eines rechtsstaatlichen Gemeinwesens sind (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 200). Die Bekämpfung der Organisierten Kriminalität und des (internationalen) Terrorismus spielen dabei eine besondere Rolle. Ziel ist die Eindringung in die Strukturen und in den Innenbereich der Organisationen, um die Begehung weiterer Straftaten zu verhindern. Eingriffe in Form der Wohnraumüberwachung sind grundsätzlich zu diesem Zweck geeignet und erforderlich, da mildere Mittel in Form der herkömmlichen Ermittlungsmethoden regelmäßig nicht ausreichen. Das hat auch das Bundesverfassungsgericht bestätigt (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 217). Angesichts der verbleibenden Unsicherheit ist eine fortlaufende Prüfung durch den Gesetzgeber erforderlich, die durch die Berichtspflichten gegenüber dem Bayerischen Landtag sichergestellt wird.

2. Ziel der Wohnraumüberwachung ist die Erhebung personenbezogener Daten. Die Erforschung des Aufenthaltsortes ist bei Einhaltung der übrigen Voraussetzungen ebenfalls zulässig.

- a. Die Sachgefahr wird dahingehend konkretisiert, dass gemeine Gefahren im Sinn von Art. 13 Abs. 4 GG erfasst werden. Es muss sich um Gefahren für erhebliche Sachwerte handeln. Das Bundesverfassungsgericht hat die Rechtsgüter der erheblichen Sach- und Vermögenswerte als ausreichend anerkannt, wenn das typische Gefahrenpotential einer gemeinen Gefahr gegeben ist (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 345).

Dringende Gefahren im Sinn von Art. 13 Abs. 4 GG, die eine präventive Wohnraumüberwachung rechtfertigen, können auch bevorstehende schwerwiegende Straftaten sein. Der Gesetzgeber muss insbesondere dann, wenn wie im Waffen-, Betäubungsmittel- oder Ausländerrecht die geschützten Güter nicht ohne weiteres benannt werden können, zum Zweck des präventiven Rechtsgüterschutzes auf die Verhinderung von Straftaten abstellen.

Voraussetzung ist dabei, dass die geschützten Rechtsgüter ein gewisses Gewicht aufweisen. Daher wird auf die abschließend im Polizeiaufgabengesetz definierten schwerwiegenden Straftaten (Art. 30 Abs. 5 Satz 1) Bezug genommen, was eine Einschränkung im Verhältnis zur bisherigen Rechtslage zur Folge hat. Das Strafmaß dieser Delikte bildet einen Anhaltspunkt für die Bedeutung des jeweils geschützten Rechtsguts. Darüber hinaus ist die Gefährdung der Öffentlichen Sicherheit und Ordnung einzubeziehen. Die erfassten Güter sind danach ausreichend gewichtig. Es handelt sich um Delikte, die aufgrund der besonderen Bedeutung der Rechtsgüter oder aufgrund der banden- bzw. gewohnheits- oder gewerbsmäßigen Begehensweise einen besonderen Unrechtsgehalt aufweisen und zugleich eine erhöhte Gefährdung für die Allgemeinheit mit sich bringen.

Eine strikte Beachtung der vom Bundesverfassungsgericht für die Wohnraumüberwachung zu Zwecken der Strafverfolgung aufgezeigten Anforderungen an den Deliktskatalog, insbesondere der Voraussetzungen für das obere Strafmaß, ist nicht angezeigt. Im Bereich des Rechtsgüterschutzes geht es nicht nur um die Ahndung von Unrecht, die sich im wesentlichen am Strafraumen orientiert, sondern um die Verhinderungen von Rechtsgüterschädigungen. Daher kommt den präventiven Maßnahmen jedenfalls in Bezug auf hinreichend gewichtige Rechtsgüter grundsätzlich ein höheres Gewicht zu. Der unterschiedliche Wortlaut des Art. 13 Abs. 4 GG – öffentliche Sicherheit – im Gegensatz zu Art. 13 Abs. 3 GG – durch Gesetz einzeln bestimmte besonders schwere Straftaten – legt deshalb einen anderen Maßstab nahe. Die öffentliche Sicherheit beinhaltet eine Vielzahl von Gefahren. Durch die Verwendung dieses Begriffs hat der verfassungsändernde Gesetzgeber bewusst an das allgemeine Sicherheitsrecht angeknüpft. Selbst bei Berücksichtigung der einschränkenden Auslegung, die verfassungsrechtlich erforderlich ist und die sich am Begriff der dringenden Gefahr sowie an den Regelbeispielen orientiert, ist der Anwendungsbereich des Art. 13 Abs. 4 GG in Bezug auf die zugrundeliegenden Straftaten weiter gefasst. Der Verhinderung von Straftaten kommt ein größeres Gewicht zu, als dem bloßen staatlichen Strafverfolgungsinteresse, das allenfalls als Annex und losgelöst vom jeweiligen Einzelfall die Unterbindung von Straftaten bzw. die Verhinderung der Begehung weiterer Straftaten

zum Ziel hat. Der Rechtsgüterschutz ist im Bereich der Gefahrenabwehr unmittelbar und nicht nur mittelbar betroffen.

Einschränkende Merkmale für die drohenden Gefahr in Form der Begehung schwerwiegender Straftaten sind die Bestimmtheit der Tatsachen sowie die Begründetheit der Annahme, dass die Adressaten der Maßnahme die jeweiligen Taten begehen wollen. Das Erfordernis von Tatsachen sagt aus, dass bloße Vermutungen und polizeiliche Erfahrungswerte nicht ausreichend sind. Im Einzelfall ist durch die Polizei und die Gerichte abzuwägen, wie konkret die Tatsachen sein müssen und wie begründet die Annahme sein muss, um den Eingriff zu rechtfertigen. Die Intensität des Eingriffs (insbesondere die Schwere der Verletzung der Wohnung und der zu erwartenden Situationen) und die Bedeutung der durch die Strafnorm im jeweiligen Fall geschützten Rechtsgüter sind in die Abwägung einzubeziehen.

Die Einhaltung der verfassungsrechtlichen Grenzen für die Wohnraumüberwachung wird durch weitere gesetzliche Einschränkungen und durch verfahrensrechtliche Sicherungen gewährleistet.

- Satz 2 Nr. 1 regelt die Subsidiarität der Wohnraumüberwachung gegenüber allen anderen Arten der Datenerhebung, einschließlich der Telekommunikationsüberwachung. Sie folgt aus der Schwere des Eingriffs (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 224).
- Der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung muss bei Maßnahmen der Wohnraumüberwachung gewährleistet sein. Ein Überwachungsverbot ist dann erforderlich, wenn die Wahrscheinlichkeit besteht, dass eine Verletzung des Kernbereichs erfolgt (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 177). Die Überwachungsmaßnahme ist daher nach Satz 2 Nr. 2 unzulässig, wenn aus der ex-ante Sicht eine Situation gegeben ist, in der sich derjenige, gegen den die Maßnahme gerichtet ist, allein oder ausschließlich mit Personen seines engsten Vertrauens in Wohnräumen aufhält und in denen keine tatsächlichen Anhaltspunkte dafür gegeben sind, dass ein

unmittelbarer Bezug zwischen den Gesprächen und den zu verhütenden Gefahren bzw. den schwerwiegenden Straftaten besteht. Die Polizei hat durch geeignete Vorermittlungen oder durch parallelen Einsatz zusätzlicher Ermittlungsmaßnahmen eine gesicherte Prognose anzustellen, dass keine derartigen Eingriffe erfolgen werden. Wer zu den engsten Vertrauten zählt, ist Frage des Einzelfalles. Grundsätzlich ist erforderlich, dass ein besonderes, den Kernbereich betreffendes Vertrauensverhältnis besteht.

Die Regelung in Satz 2 Nr. 2 geht aber über den verfassungsrechtlich gebotenen Kernbereichsschutz hinaus. Es werden auch Berufsgeheimnisträger nach § 53 Abs. 1 Satz 1 Nr. 4 und 5 StPO geschützt. Zeugnisverweigerungsrechte von Journalisten und Abgeordneten weisen zwar grundsätzlich keinen Bezug zum Kernbereich privater Lebensgestaltung auf (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 148). Sie sind aber aufgrund der Bedeutung der Vertrauensverhältnisse ebenfalls schutzwürdig und werden daher vom Abhörverbot umfasst. Dadurch wird der Schutz vertrauenswürdiger Gespräche, die mit einem Berufsgeheimnisträger in privaten Wohnräumen geführt werden, gewährleistet. Die Schutzwirkungen greifen allerdings dann nicht ein, wenn Gespräche nach ihrem Inhalt die Begehung schwerwiegender Straftaten oder die Verursachung der in Absatz 1 Satz 1 Nr. 1 genannten anderen Gefahren zum Gegenstand haben (Satz 2 Nr. 2 Buchst. a) oder wenn sich die Maßnahme zugleich gegen den Gesprächspartner wendet bzw. gegen diesen wenden könnte (Satz 2 Nr. 2 Buchst. b). Die Begehung von schwerwiegenden Straftaten und die Verursachung anderer Gefahren für gewichtige Rechtsgüter ist nicht schutzwürdig. Hierbei ist aus der Ex-Ante-Sicht eine Prognose anzustellen.

- Der Schutz wird in Satz 2 Nr. 3 auf Räumlichkeiten ausgedehnt, die von Berufsgeheimnisträgern ausschließlich zu deren Berufsausübung genutzt werden. Zwar genießen Betriebs- und Geschäftsräume grundsätzlich einen geringeren Schutz, da sie typischerweise einen Sozialbezug aufweisen, dies gilt aber nicht, wenn sie der Ausübung von Berufen dienen, die ein besonderes Vertrauensverhältnis voraussetzen, das

den Bereich des Höchstpersönlichen betrifft (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 142 f.). Wenn allerdings Hinweise dafür bestehen, dass der Berufsgeheimnisträger mit Dritten Gespräche führt, die nach ihrem Inhalt die Begehung schwerwiegender Straftaten oder die Verursachung der in Absatz 1 Satz 1 Nr. 1 genannten Gefahren zum Gegenstand haben, besteht keine Schutzwürdigkeit des Vertrauensverhältnisses.

- Satz 3 ordnet die Unterbrechung der Maßnahme an, wenn erkennbar wird, dass es zu einem Kernbereichseingriff bzw. zu einem Eingriff in ein besonderes Vertrauensverhältnis kommt, weil unerwartet eine Situation eingetreten ist, die dem absolut geschützten Bereich unterfällt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 184 f.). Soweit keine hinreichenden äußeren Anzeichen für eine Kernbereichsverletzung vorliegen, ist aus verfassungsrechtlicher Sicht eine Bewertung des Gesprächsinhalts im Rahmen einer ersten Sichtung nicht zu beanstanden (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 151). Dabei ist allerdings größtmögliche Zurückhaltung zu üben. Es kann daher erforderlich sein, die Möglichkeit einer Unterbrechung zu gewährleisten, für den Fall, dass eine Situation eintritt, die dem absolut geschützten Kernbereich zuzurechnen ist. Sobald dies erkannt wird, ist die Überwachung abubrechen. Das Verwertungsverbot und die Löschungspflicht für die dabei erfolgten Aufzeichnungen ergibt sich aus Absatz 3 bzw. aus Absatz 5.
- Satz 4 dient der Klarstellung, dass auch Dritte von der Maßnahme betroffen sein können. Eine Datenerhebung bei Kontakt- und Begleitpersonen zur Verhütung von Straftaten ist allerdings auch weiterhin nicht zulässig. Durch die Formulierung „unvermeidbar betroffen“ wird klargestellt, dass die Überwachung Dritter, die sich in der Wohnung der Zielperson aufhalten und selbst nicht Adressat einer Maßnahme nach Art. 34 PAG sind, unvermeidbar sein muss.

- b. Entsprechend der grundgesetzlichen Vorgaben in Art. 13 Abs. 4 GG wird die Maßnahme – wie nach bisheriger Rechtslage – durch einen Einzelrichter angeordnet. Ein Spruchkörpervorbehalt ist gemäß Art. 13 Abs. 3 Satz 3 GG nur

bei der Wohnraumüberwachung zu repressiven Zwecken erforderlich. Nach Art. 13 Abs. 4 GG genügt die richterliche Entscheidung (vgl. Papier, in: Maunz/Dürig, Grundgesetz, Art. 13, Rn. 98). Aus der Rechtsprechung des Bundesverfassungsgerichts ergeben sich insofern keine Bedenken gegen die bisherige Regelung (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 270 f.). In Eilfällen erfolgt die Anordnung durch den Dienststellenleiter; die gerichtliche Entscheidung ist unverzüglich nachzuholen. Das Schriftlichkeitsgebot und die inhaltlichen Anforderungen an die Entscheidung dienen der Einhaltung der verfassungsrechtlichen Erfordernisse. Die Begrenzung auf einen Monat gewährleistet die regelmäßige gerichtliche Überprüfung der Maßnahme und damit eine der Tiefe des Grundrechtseingriffs angemessene Überwachung durch eine weisungsunabhängige Instanz (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 281). Die Regelung in Satz 5, 1. Halbsatz dient der Klarstellung. Das Übermaßverbot ist in jedem Fall zu wahren. Die Mitteilungspflicht bei Beendigung gemäß Halbsatz 2 ist erforderlich, da der Richter die Maßnahme nicht nur anordnet, sondern auch überwacht.

- c. In Absatz 3 wird das Zweckbindungsgebot und die damit verbundene Kennzeichnungspflicht geregelt (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 328 ff.). Die Verwendung der erhobenen Daten zu Zwecken der Strafverfolgung stellt einen eigenen Grundrechtseingriff dar (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 333; Papier, in: Maunz/Dürig, Grundgesetz, Art. 13, Rn. 104). Die Zweckänderung ist daher zu dokumentieren. Die Zulässigkeit richtet sich nach den Maßgaben der Strafprozessordnung über die Verwertung der Daten, soweit solche nicht bestehen über diejenigen zur Datenerhebung zu strafprozessualen Zwecken (Satz 2 Nr. 2). Zwischen der Frage, ob eine Zweckänderung erfolgen darf und ob eine Verwertung im Prozess zulässig ist, muss zwar grundsätzlich unterschieden werden (Papier, in: Maunz/Dürig, Grundgesetz, Art. 13, Rn. 106). Die Voraussetzungen für die Zweckänderung und die Verwertung sollen aber nach Absatz 3 Satz 2 gleichlaufend sein. Ziel ist es, eine Umgehung der engeren Voraussetzungen des Art. 13 Abs. 3 GG zu verhindern. Besondere Verwertungsverbote werden durch Landesrecht nicht angeordnet.

Satz 3 regelt in Ergänzung zu den Erhebungsverboten das Verwertungsverbot für Fälle, in denen sich nachträglich herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben (Nr. 1) und in denen Daten gewonnen wurden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (Nr. 2). Die Pflicht zur Löschung dieser Daten ergibt sich aus Absatz 5.

Das Bundesverfassungsgericht hat anerkannt, dass es Fälle geben kann, in denen eine eindeutige Zuordnung nach dem sozialen Umfeld nicht möglich ist oder in denen sich im Vorhinein nicht feststellen lässt, ob es sich um Gespräche mit möglichen Tatbeteiligten handelt (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 185). Verfassungsrechtlich ist bei Einhaltung der Erhebungsvoraussetzungen eine nachträgliche Bewertung des Gesprächsinhalts grundsätzlich nicht ausgeschlossen (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 151). Wenn sich dabei jedoch aus der Ex-Post-Sicht herausstellt, dass ein Eingriff in ein besonders geschütztes Vertrauensverhältnis vorliegt, unterliegen die Daten einem Verwertungsverbot und sind zu löschen. Dies gilt unabhängig davon, ob das besondere Vertrauensverhältnis mit dem Kernbereich privater Lebensgestaltung übereinstimmt. Über die verfassungsrechtlichen Erfordernisse hinaus werden durch das Verwertungsverbot auch Vertrauensverhältnisse geschützt, die nicht dem Kernbereich zuzuordnen sind. Das Gesetz geht insbesondere im Interesse des Schutzes von Journalisten und anderen Gruppen von Berufsheimnisträgern, die nicht zu den engsten Vertrauten zählen, über die Anforderungen des Bundesverfassungsgerichts hinaus.

Im Bereich der Gefahrenabwehr ergeben sich Ausnahmen vom Verwertungsverbot für Daten, die aus einem besonderen Vertrauensverhältnis stammen bzw. bei denen die Erhebungsvoraussetzungen nicht gegeben waren, wenn eine Verwendung zum Schutz hochwertigster Rechtsgüter erforderlich ist. Das Bundesverfassungsgericht hat sich in seiner Entscheidung nur mit den absoluten strafprozessualen Verwertungsverboten befasst (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 121; 184 f.). Eine Abwägung zwischen Kernbereichsschutz und Strafverfolgungsinteressen ist dabei abgelehnt worden (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 121). Im Bereich der Gefahrenabwehr können allerdings Situationen eintreten, in denen sich absolut geschützte Rechtsgüter gegenüberste-

hen und in denen die Kollision nicht aufgelöst werden kann. Zu denken ist etwa an den Fall, dass eine Information gewonnen wird, die der Vereitelung eines unmittelbar drohenden terroristischen Anschlags und damit dem Schutz höchster Rechtsgüter dient. Dann stehen sich die Vertiefung des Eingriffs durch die Verwendung der Daten und die staatliche Schutzpflicht für Leib, Leben und Freiheit gegenüber, die eine Verwertung der Informationen gebietet. Der Konflikt wird in derartigen Extremkonstellationen zugunsten des Schutzes hochwertigster Rechtsgüter aufgelöst.

Die Beachtung der verfassungsrechtlichen Verwertungsverbote für Eingriffe aus dem Kernbereich ist von einer unabhängigen Stelle zu überprüfen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 194). Dies wird durch die erneute richterliche Kontrolle gewährleistet.

Absatz 4 regelt die Benachrichtigungspflichten. In den Fällen heimlicher Datenerhebung gebietet Art. 13 Abs. 1 GG in Verbindung mit dem Erfordernis des effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) grundsätzlich eine Benachrichtigung der Betroffenen. Für die Inanspruchnahme gerichtlichen Rechtsschutzes gelten im übrigen die allgemeinen Grundsätze. Nach der Rechtsprechung des Bundesverfassungsgerichts besteht bei schwerwiegenden Grundrechtseingriffen das Rechtsschutzinteresse grundsätzlich auch nach Beendigung der Maßnahme fort, wenn sich die direkte Belastung nach dem typischen Verfahrensverlauf auf eine Zeitspanne beschränkt, in welcher der Betroffene die gerichtliche Entscheidung kaum erlangen kann (BVerfG vom 30.04.1997, BVerfGE 96, 27/40; BVerfG vom 05.12.2001, BVerfGE 104, 220/232 f.). Daher kann auch nach der Erledigung der Maßnahme entsprechend den Regelungen des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit Beschwerde gegen den richterlichen Anordnungsbeschluss erhoben werden.

Als Rechtfertigungsgründe für die Zurückstellung der Benachrichtigung kommen die Gefährdung des Untersuchungszwecks und der eingesetzten, nicht offen ermittelnden Beamten in Betracht. Gleiches gilt bei einer Gefährdung der öffentlichen Sicherheit hinsichtlich der durch Absatz 1 Satz 1 Nrn. 1 und 2 geschützten Rechtsgüter (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 301). In Fällen, in denen die Daten zu Strafverfolgungszwe-

cken genutzt werden, erfolgt die Benachrichtigung in Absprache mit der Staatsanwaltschaft nach den strafprozessualen Regelungen.

Vor dem Hintergrund des effektiven Grundrechtsschutzes ist bei jeder mehr als sechsmonatigen Zurückstellung nach Beendigung der Maßnahme eine gerichtliche Entscheidung erforderlich. Danach erfolgt grundsätzlich eine jährliche Überprüfung, es sei denn der Richter hat eine abweichende Frist bestimmt. Verfahren und gerichtliche Zuständigkeit richten sich in Fällen, in denen die Daten zu Strafverfolgungszwecken verwendet werden, nach den jeweiligen Regelungen der Strafprozessordnung, im übrigen gelten die Regelungen für die Anordnung der Maßnahme entsprechend.

Ausnahmsweise kann die Benachrichtigung nach Satz 5 mit richterlicher Zustimmung auf Dauer unterbleiben, wenn die Voraussetzungen für eine Zurückstellung dauerhaft gegeben sind (Nr. 1), wenn der Grundrechtseingriff bei der Zielperson oder bei dem zu benachrichtigenden Beteiligten vertieft würde (Nr. 2) oder wenn die Feststellung der Identität eines Betroffenen nur unter unverhältnismäßigem Aufwand möglich ist (Nr. 3). Darin sind hinreichend gewichtige Gesichtspunkte zu sehen, die eine Ausnahme rechtfertigen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 297).

- d. Der im bisherigen Absatz 3 geregelte Einsatz technischer Mittel zum Schutz verdeckter Ermittler unterliegt weniger strengen Anforderungen, da der Ermittler selbst von den Vorgängen in der Wohnung Kenntnis erlangt. Die verfassungsrechtlichen Voraussetzungen ergeben sich aus Art. 13 Abs. 5 GG. Grundsätzlich sind die Aufzeichnungen nach Beendigung der Maßnahme zu löschen.

Soweit darüber hinaus Zufallsergebnisse erzielt werden, etwa weil in einer fremden Sprache oder unter Verwendung einer Chiffrierung gesprochen wurde, die die geschützte Person nicht verstanden hat, ist eine richterliche Entscheidung über die Verwertung erforderlich, unabhängig ob diese zu präventiven oder zu repressiven Zwecken erfolgt. Absatz 3 ist dabei zu beachten. Für die Benachrichtigung der Betroffenen und die Pflicht zur Sperrung bzw. Löschung von Daten wird auf die allgemeinen Regelungen verwiesen.

- e. Die Löschung von Daten ist künftig in Absatz 6 geregelt.

- f. Absatz 5 regelt die Sperrung und die Löschung der Daten. Der Schutz des Art. 13 Abs. 1 GG erstreckt sich auch auf die weiteren Phasen der Datenverarbeitung. Grundsätzlich sind daher Daten zu vernichten, sobald sie für den festgelegten oder einen anderen zulässigen Zweck nicht mehr benötigt werden. Diese Verpflichtung muss aber zugleich dem Gebot des effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG genügen (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 349).

Daher ist eine Abstimmung zwischen der Löschungspflicht und dem Gebot des effektiven Rechtsschutzes dergestalt erforderlich, dass in Fällen, in denen der Betroffene ein „ernsthafte – grundsätzlich zu vermutendes – Interesse am Rechtsschutz bzw. an der Geltendmachung des Datenschutzes“ haben kann, die Daten nicht gelöscht, sondern nur gesperrt werden (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, a.a.O.). Die Sperrung hat zur Folge, dass die Daten zu keinem anderen Zweck als zur Information des Betroffenen verwendet werden dürfen und erst nachdem sichergestellt ist, dass sie für eine gerichtliche Überprüfung nicht mehr benötigt werden, zu löschen sind. Die Monatsfrist nach Satz 3 dient dem Betroffenen als Entscheidungsfrist darüber, ob er Klage erheben will oder ob er mit der Löschung der Daten einverstanden ist. Die Fristsetzung ist erforderlich, um Rechtsklarheit über die Vernichtung der Daten zu schaffen. Die Fristberechnung richtet sich nach den allgemeinen Regelungen. Wenn eine Benachrichtigung ausnahmsweise unterbleibt oder kein Betroffener rechtzeitig Klage erhebt, erfolgt die endgültige Löschung.

Daten, die aus dem Kernbereich privater Lebensgestaltung oder aus einem besonders geschützten Vertrauensverhältnis stammen und keinen unmittelbaren Bezug zu den in Absatz 1 Satz 1 genannten Gefahren oder Straftaten aufweisen und für die daher nach Absatz 3 Satz 3 ein Verwertungsverbot besteht, sind dagegen unverzüglich zu löschen. Auch das Gebot des effektiven Rechtsschutzes steht dem nicht entgegen (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 186). Dies wird durch Satz 1 klargestellt.

- g. Folgeänderung zu § 1 Nr. 3 d des Gesetzentwurfs.

- h. Die Änderung ist Folge der Einführung der Befugnisse zur Telekommunikationsüberwachung in Art. 34a bis 34c. In der bisherigen Fassung des Art. 34 Abs. 7 PAG wurde klargestellt, dass das Vorliegen der Voraussetzungen, die zum Einsatz technischer Mittel in Wohnungen nach Art. 34 PAG ermächtigen, nicht zugleich auch Eingriffe in das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 GG zulässt. Mangels spezieller Befugnisse, die Eingriffe in das Fernmeldegeheimnis ermöglichten, konnte bisher nach dem PAG keine Telekommunikationsüberwachung durchgeführt werden.

Durch die Einfügung der speziellen Befugnisnormen entfällt hinsichtlich des Fernmeldegeheimnisses die Notwendigkeit für die klarstellende Regelung. Soweit die Voraussetzungen der Art. 34a bis 34c vorliegen, sind künftig auch Telekommunikationsüberwachungsmaßnahmen möglich. In Bezug auf das durch Art. 10 GG geschützte Brief- und Postgeheimnis bleibt die Klarstellung auch weiterhin erforderlich.

#### Zu § 1 Nr. 4 (Art. 34a bis 34c)

1. In Art. 34a Abs. 1 wird der Polizei die Befugnis zur Datenerhebung durch Telekommunikationsüberwachung eingeräumt, um Gefahren für hochwertige Rechtsgüter abzuwehren. Unter Telekommunikation ist hierbei der technische Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (Telekommunikationsanlage) zu verstehen (vgl. § 3 Nr. 16 und 17 TKG).

- a. Art. 34a Abs. 1 regelt die Erhebung personenbezogener Daten durch Überwachung und Aufzeichnung der Telekommunikation. Umfasst sind die Inhaltsdaten der Kommunikation. Adressaten der Maßnahme sind nach Satz 1 Nr. 1 die nach Art. 7 und 8 PAG für eine Gefahr verantwortlichen Personen. Voraussetzung für die Maßnahme ist, dass eine konkrete Gefahr für die genannten besonders schutzwürdigen Rechtsgüter vorliegt. Zu diesen zählen entsprechend der Regelung in Art. 34 Abs. 1 Satz 1 Nr. 1 neben Leben, Gesundheit und

Freiheit einer Person sowie Sachen, soweit eine gemeine Gefahr besteht, auch der Bestand und die Sicherheit des Bundes oder eines Landes. Dass die Polizei auch die Aufgabe hat, verfassungsfeindliche Handlungen zu verhüten, und bei konkreten Gefahren auch über entsprechende Befugnisse verfügt, folgt bereits aus der Generalklausel des Art. 11 Abs. 2 Satz 1 Nr. 1 Alt. 3 PAG. Darunter sind gem. Art. 11 Abs. 2 Satz 4 PAG Handlungen zu verstehen, die darauf gerichtet sind, die verfassungsmäßige Ordnung der Bundesrepublik Deutschland oder eines ihrer Länder auf verfassungswidrige Weise zu stören oder zu ändern, ohne eine Straftat oder Ordnungswidrigkeit zu verwirklichen. Soweit eine derartige Handlung mit Strafe bedroht ist bzw. eine Ordnungswidrigkeit verwirklicht wird, greift bereits Art. 11 Abs. 2 Satz 1 Nr. 1 Alt. 1 und 2 PAG ein. In Art. 34a Abs. 1 Satz 1 Nr. 1 werden einschränkend nur die Gefahren für die Sicherheit oder den Bestand des Bundes oder eines Landes erfasst. Voraussetzung ist dabei das Vorliegen einer konkreten Gefahr.

Nach Satz 1 Nr. 2 Buchst. a kann sich die Maßnahme der Gefahrenabwehr auch gegen potentielle Straftäter richten. Dann müssen bestimmte Tatsachen vorliegen, die die begründete Annahme rechtfertigen, dass die Person eine schwerwiegende Straftat begehen will. Bei den schwerwiegenden Straftaten nach Art. 30 Abs. 5 Satz 1 handelt es sich um hinreichend gewichtige Delikte, die den Bereich der mittleren Kriminalität überschreiten oder zumindest an dessen Obergrenze liegen und die daher abstrakt geeignet sind, im Interesse der Verhinderung einer Straftat einen Eingriff in die Fernmeldefreiheit zu rechtfertigen. Im konkreten Einzelfall ist unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit gemäß Art. 4 PAG 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. Bei überragend wichtigen Gütern genügen daher geringere Anhaltspunkte, während bei einem weniger bedeutsamen Rechtsgut, das etwa durch eine geringere Strafandrohung geschützt wird, höhere Anforderungen an die Begründetheit der Annahme, dass die Straftat verwirklicht werden soll, zu stellen sind. Dabei ist jeweils die Eingriffsintensität einzubeziehen.

Kontakt- und Begleitpersonen, die für die in Satz 1 Nr. 1 und Nr. 2 Buchst. a aufgezählten Störer Botentätigkeiten wahrnehmen, können unter den einschränkenden Voraussetzungen des Satzes 1 Nr. 2 Buchst. b und c Adressaten der Maßnahme sein. Voraussetzung ist, dass die begründete Annahme auf der Grundlage von bestimmten Tatsachen gerechtfertigt ist, dass es sich um Kontaktpersonen handelt oder um Personen, die ihre Kommunikationseinrichtungen den in Satz 1 Nr. 1 und 2 Buchst. a genannten Adressaten zur Verfügung stellen.

Andere Personen können keine Adressaten sein und dürfen daher nur dann von der Maßnahme betroffen werden, wenn dies unvermeidbar ist, weil sie Kommunikationspartner des Adressaten sind. Die Erhebung von Inhaltsdaten ist nach Satz 2 gegenüber anderen Maßnahmen, mit Ausnahme der Wohnraumüberwachung, subsidiär.

In Satz 3 wird ein Erhebungsverbot für Gespräche mit Berufsheimnisträgern angeordnet. Ein besonderer Schutz dieser Personengruppe ist zwar verfassungsrechtlich nicht geboten, wird aber angesichts der Besonderheiten der Vertrauensbeziehungen zu Ärzten, Apothekern, Anwälten, Geistlichen, Journalisten und anderen in § 53 StPO aufgezählten Berufsgruppen gewährt. Stellt sich nachträglich das Bestehen eines Vertrauensverhältnisses heraus, greift das Verwertungsverbot nach Art. 34c Abs. 4 Satz 3 Nr. 1 ein. Die darüber hinausgehenden Verwertungsverbote in Art. 34c Abs. 4 Satz 3 Nr. 2 gewährleisten ebenso wie die Löschungs- und Sperrungspflichten nach Art. 34c Abs. 6 einen zusätzlichen Schutz.

Der Schutz des Kernbereichs privater Lebensgestaltung erfolgt im übrigen nicht in gleicher Weise wie bei der Wohnraumüberwachung antizipiert. Der Grundsatz, dass durch geeignete Maßnahmen im Vorfeld die zu erwartende Kommunikationssituation ermittelt werden muss, ist nicht übertragbar. Das Bundesverfassungsgericht hat hinsichtlich des Zusammenhangs von Art. 13 GG und der Menschenwürde betont, dass die Privatwohnung als „letztes Refugium“ ein „Mittel zur Wahrung der Menschenwürde“ sei. Diese Aussage lässt sich für die Telekommunikation nur eingeschränkt treffen.

Der besondere Bezug der Unverletzlichkeit der Wohnung zur Menschenwürde und der enge Zusammenhang des Grundrechts mit dem „verfassungsrechtli-

chen Gebot unbedingter Achtung einer Sphäre des Bürgers für eine ausschließlich private – eine höchstpersönliche – Entfaltung“ ist ungeachtet der Bedeutung des Fernmeldegeheimnisses nicht in gleicher Weise bei Eingriffen in die Fernmeldefreiheit gegeben. Das Grundrecht aus Art. 10 GG gewährleistet die freie Entfaltung der Persönlichkeit und schützt damit zugleich die Menschenwürde (BVerfG vom 03.03.2004, Az.: 1 BvF 3/92, Rn. 105). Demgegenüber erfolgt durch Art. 13 GG eine Konkretisierung des Menschenwürdeschutzes. Der Einzelne benötigt für seine Entfaltung einen geeigneten Freiraum in Form der Privatwohnung, in dem er das Verhalten, das zum absolut geschützten Kernbereich privater Lebensgestaltung gehört, ausüben kann. Die Teilnahme am Fernmeldeverkehr ist nicht in gleichem Maße essentiell, wie die Innehabung eines Wohnraumes, wenn es um den Rückzug in die Privatsphäre geht.

Zudem begibt sich die Person durch die Nutzung der Telekommunikationsmittel „in die Öffentlichkeit“. Sie benutzt ein öffentliches Fernsprechnet (eines Unternehmens) als Medium für die Fernkommunikation. Es bedarf für Dritte, auch wenn sie nicht hoheitlich Handelnde sind, keiner übermäßig großen Anstrengungen, um Fernsprechverbindungen abzuhören. Unter Umständen können bereits Funktionsstörungen zu einem Mithören von Gesprächen führen. Dies gilt bei Festnetzverbindungen, um so mehr aber bei Mobilfunk- und bei Internetverbindungen. Auch die Gefahr, dass Dritte mit Zustimmung des Gesprächspartners Kenntnis von den Inhalten der Kommunikation erlangen, ist anders als bei einem Gespräch in der eigenen Wohnung nicht auszuschließen. Daher ist die Aufnahme einer solchen Verbindung ein bewusster Schritt aus dem unabdingbar geschützten Bereich. Die absolut geschützte Sphäre wird verlassen. Der vom Bundesverfassungsgericht angeführte Rechtsgedanke, dass der Betroffene weniger schutzwürdig ist, wenn er den Schutz seiner Privatwohnung als räumliches Substrat höchstpersönlicher Lebensgestaltung nicht nutzt, etwa weil er ermöglicht, dass die Kommunikation nach außen dringt und ohne technische Mittel hörbar ist (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 166), ist in diesem Zusammenhang einschlägig.

Hinzu kommt, dass in diesem Bereich eine Prognose, mit wem ein Telefongespräch zustande kommt und in welchem Verhältnis beide Gesprächspartner

zueinander stehen, in der Regel gar nicht angestellt werden kann. Angesichts der Häufigkeit und Vielgestaltigkeit von Telekommunikationsvorgängen ist dies regelmäßig nicht möglich. Selbst während der Durchführung einer Überwachungsmaßnahme kann vielfach ohne weitere Auswertung nicht einmal festgestellt werden, mit welcher Person gesprochen wird, etwa wenn keine Namensnennung erfolgt oder weil es sich um eine fremdsprachige Kommunikation handelt. Dies gilt um so mehr in Fällen, in denen ein Störer im Sinne des Art. 34a Abs. 1 Satz 1 gezielt eine Überwachung ausschließen oder erschweren will, indem er Vertrauensverhältnisse vortäuscht oder indem in Absprache mit den jeweiligen Kommunikationspartnern eine Vielzahl von Verbindungen, insbesondere im Bereich der Mobiltelefone, genutzt wird. Gerade bei international operierenden Kriminellen, etwa im Bereich der Organisierten Kriminalität oder des internationalen Terrorismus, dürfte es ohne weiteres möglich sein, durch entsprechende Chiffrierung bei jedem Gespräch, das die Begehung einer Straftat oder die Verursachung einer Gefahr für hochrangige Rechtsgüter betrifft, ein Vertrauensverhältnis oder eine familiäre Bindung zu fingieren. Vor allem bei Gesprächen mit Auslandsbezug wird es den Ermittlungsbehörden in der Regel nicht möglich sein, zu überprüfen, ob es sich tatsächlich um einen engsten Vertrauten handelt oder ob dies durch geschickte Wahl der Kommunikationsinhalte, etwa eine persönliche Anrede, nur vorgetäuscht wird. Bei sonstigen Vertrauten kann der Kommunikationspartner nicht wie bei den Gesprächen mit Berufsgeheimnisträgern, die regelmäßig nur über eine begrenzte Zahl an Kommunikationsverbindungen verfügen und bei denen der ständige Wechsel der Anschlüsse nicht in Betracht kommt, relativ genau identifiziert werden. Bei Ärzten, Anwälten, Journalisten und den anderen in § 53 StPO genannten Berufsgruppen besteht zudem eine weitaus geringere Missbrauchsgefahr. Anders als bei undifferenzierten Personenkontakten kann davon ausgegangen werden, dass der Gesprächspartner seine besondere Vertrauensstellung nicht ausnutzt, um mit dem Adressaten bei der Begehung schwerwiegender Straftaten oder der Verursachung von Gefahren zusammenzuwirken. Sollte dies ausnahmsweise doch der Fall sein, greift die Sonderregelung in Art. 34a Abs. 1 Satz 3 ein, wonach keine Schutzwürdigkeit besteht, wenn ein Berufsgeheimnisträger selbst Maßnahmeadressat ist oder sein könnte, weil er die Voraussetzungen für eine Überwachung ebenfalls erfüllt.

Bei Vertrauensbeziehungen, die nicht auf einem Berufsgeheimnis beruhen, ist daher grundsätzlich eine erste Sichtung von Gesprächsinhalten erforderlich. Dies ist nach der Rechtsprechung des Bundesverfassungsgerichts selbst bei der Wohnraumüberwachung zulässig, wenn nicht von vornherein ein Eingriff in den Kernbereich in Betracht kommt. Dementsprechend erfolgt eine Überprüfung der Gesprächsinhalte und der Schutzbedürftigkeit im Rahmen der Auswertung der gewonnenen Daten. Der Schutz des Kernbereichs privater Lebensgestaltung wird über die Verwertungsverbote bzw. die Löschungspflichten in Art. 34c Abs. 4 und 6 gewährleistet.

- b. Im Unterschied zur Überwachung und Aufzeichnung von Telekommunikationsinhalten gewährt Absatz 2 die Befugnis zum Einsatz von Geräten zur Identifikation und Lokalisation von Telekommunikationsteilnehmern. Diese Regelung ist angesichts der erheblichen Fortschritte auf dem Gebiet der Telekommunikationstechnik erforderlich. Bei der Planung und Begehung von schwerwiegenden Straftaten werden insbesondere von Angehörigen gewaltbereiter extremistischer Gruppen zunehmend Mobiltelefone eingesetzt, deren Herkunft den Sicherheitsbehörden nicht bekannt ist, weshalb auch die Telefonnummer oftmals über einen Provider nicht ermittelt werden kann. Nachdem die Angabe der Telefonnummer aber Zulässigkeitsvoraussetzung für eine Anordnung der Telekommunikationsüberwachung nach Art. 34a Abs. 1 ist, muss der Polizei die Befugnis zur Ermittlung der erforderlichen Daten eingeräumt werden. Der Einsatz von Geräten, wie etwa des sog. „IMSI-Catchers“, die zur Bestimmung der Geräte- und Kartenummer von Mobiltelefonen bzw. des Standortes von Mobilfunkendgeräten dienen (Absatz 2 Satz 1 Nr. 1), wird an die strengen Voraussetzungen des Art. 34 a Abs. 1 geknüpft, da er in der Regel zur Vorbereitung einer Telekommunikationsüberwachungsmaßnahme dient. Dies gilt insbesondere auch für die Subsidiaritätsregelung in Absatz 1 Satz 2. Absatz 2 Satz 1 Nr. 2 enthält die Befugnis zur Ermittlung des Standortes eines Mobilfunkendgerätes. Die Maßnahme ist zur Verhütung schwerwiegender Straftaten und zum Schutz der in Art. 34a Abs. 1 Satz 1 Nr. 1 geschützten Rechtsgüter ebenfalls unverzichtbar. Erfasst wird auch die Aussendung von funktechnischen Signalen, um die Standortkennung eines Endgerätes zu aktivieren. Zulässigkeitsvoraussetzung für Maßnahmen nach Absatz 2 ist nicht,

dass sich das Telekommunikationsgerät im Sendebetrieb befindet. Ausreichend ist der „Stand-By-Betrieb“.

Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, unterliegen diese grundsätzlich einem Verwendungsverbot und sind unverzüglich zu löschen. Die Verwendung dieser Daten ist ausnahmsweise zu dem Zweck der Verhütung von schwerwiegenden Straftaten oder zur Strafverfolgung zulässig. Im letztgenannten Fall sind die allgemeinen Einschränkungen für die Zweckänderung zu beachten, die sich aus Art. 34c Abs. 4 ergeben.

- c. Die Suche nach vermissten oder hilflosen Personen wird durch Standortbestimmungsmaßnahmen nach Absatz 3 wesentlich erleichtert. Durch erheblichen Zeitgewinn können gerade bei Unglücksfällen oder bei Suizidgefahr Leben gerettet werden. Voraussetzung für die Maßnahme ist dabei stets eine Gefahr für Leben oder Gesundheit. Für den Einsatz technischer Geräte zur Ortung von Mobiltelefonen, die Vermisste bei sich tragen, fehlt es bisher an einer Rechtsgrundlage. Der Einsatz kann lediglich auf den in § 34 StGB (rechtfertigender Notstand) niedergelegten Rechtsgedanken des übergesetzlichen Notstandes gestützt werden, der Lösungsansätze zur Reaktion auf außerordentliche, unvorhersehbare Interessenkollisionen bietet. Die Polizei benötigt aber eine eindeutige Rechtsgrundlage, um künftig zum Schutz von Leben und Gesundheit die vorhandenen technischen Möglichkeiten nutzen zu können. Diese wird ihr durch Absatz 3 gewährt.
  
- d. In Anbetracht der Tatsache, dass die modernen Kommunikationstechniken gerade von terroristischen Netzwerken zur Begehung von Anschlägen genutzt werden, müssen der Polizei zur Verhütung von Gefahren für hochrangige Rechtsgüter und zur Verhinderung von schwerwiegenden Straftaten neuartige Befugnisse eröffnet werden. Die Anschläge von Madrid haben gezeigt, dass Mobiltelefone im Zusammenhang mit Zündmechanismen für Sprengstoffe Verwendung finden. Darüber hinaus sind Fallgestaltungen bekannt, in denen eine Telekommunikation zur Abwehr von Gefahren oder zum Zweck der Verhinderung und Unterbindung von Straftaten unterbrochen oder gänzlich verhindert werden muss.

An Befugnisnormen für die Unterbrechung oder Verhinderung von Kommunikationsverbindungen fehlt es bisher. Diese sicherheitsrechtliche Lücke wird durch Absatz 4 geschlossen. Der Eingriff ist an die strengen Voraussetzungen des Absatzes 1 geknüpft.

Die Unterbrechung oder Verhinderung einer Telekommunikationsverbindung Unbeteiligter ist nur unter noch engeren Voraussetzungen zulässig, die spezielle Ausprägungen des Grundsatzes der Verhältnismäßigkeit sind. Solche Maßnahmen können bei sog. Sprengstofffallen erforderlich sein, wenn die Polizei davon Kenntnis erlangt, dass ein Sprengkörper über ein Mobilfunkgerät ferngesteuert gezündet werden soll. Gleiches muss bei Geisellagen gelten, um die Kommunikation des Geiselnahmers mit Komplizen außerhalb des Tatorts über die Mobiltelefone Dritter zu unterbinden. Voraussetzung ist eine gegenwärtige erhebliche Gefahr für Leben, Gesundheit oder Freiheit einer Person, die nicht anders abwendbar ist.

2. Die Mitwirkungspflichten der Diensteanbieter werden in Art. 34b geregelt. Diensteanbieter ist, wer geschäftsmäßig Telekommunikationsdienste anbietet, erbringt oder daran – auch als Vertriebspartner – mitwirkt. Die Pflicht zur Ermöglichung der Telekommunikationsüberwachung ist als notwendige Ergänzung der Befugnisnormen in Art. 34a Abs. 1 und Abs. 3 Satz 1 Nr. 1 geregelt. Nach Absatz 2 können Diensteanbieter verpflichtet werden, Telekommunikationsverbindungsdaten zur Verfügung zu stellen. Absatz 3 enthält eine Legaldefinition der Telekommunikationsverbindungsdaten.

a. Die Mitwirkungspflichten der Diensteanbieter bei der Telekommunikationsüberwachung sind angesichts der technischen Gegebenheiten unverzichtbar für die Durchführung der Maßnahmen. Dies gilt in besonderem Maße bei Festnetz-Telefonanschlüssen. Daher verpflichtet Absatz 1 die Diensteanbieter, der Polizei die Überwachung und Aufzeichnung der Telekommunikation nach Art. 34 a Abs. 1 und Abs. 3 Satz 1 Nr. 1 zu ermöglichen.

Dies schließt deren Verpflichtung ein, die zur Umsetzung der Telekommunikationsüberwachung notwendigen technischen Voraussetzungen zu schaffen. Die konkreten Pflichten ergeben sich aus dem Telekommunikationsgesetz

(TKG) und der zu dessen Durchführung erlassenen Rechtsverordnungen. Die den Diensteanbietern dadurch auferlegte Belastung geht nicht über diejenige hinaus, die ihnen nach der vergleichbaren Regelung in der Strafprozessordnung obliegt und die zudem bundeseinheitlich im für die technische Umsetzung von Telekommunikationsüberwachungsmaßnahmen maßgeblichen TKG festgeschrieben ist.

- b. Ergänzend regelt Absatz 2 die Übermittlung der Telekommunikationsverbindungsdaten. Ohne die Übermittlung dieser Informationen ist es der Polizei vielfach nicht möglich, Verflechtungen und Zusammenhänge im unübersichtlichen und vielschichtigen Bereich der Organisierten Kriminalität und des (internationalen) Terrorismus zu erkennen und effektive Maßnahmen zur Gefahrenabwehr zu treffen. Gerade bei stark nach außen abgeschotteten Gruppen und konspirativ angelegten Strukturen ist die Kenntnis dieser Daten unbedingt erforderlich.

Auch in Fällen des Art. 34a Abs. 3 Satz 1 ist die Übermittlungsbefugnis notwendig. Durch die Kenntnis der letzten Gesprächsdaten können entscheidende Hinweise zur Auffindung einer vermissten oder hilflosen Person gewonnen werden. Zu denken ist auch an Suizidgefährdete oder an Personen, die Hilferufe absetzen, ohne ausreichende Angaben zu ihrem Aufenthaltsort machen zu können. Die bisherige Praxis, die Befugnis zur Verpflichtung, entsprechende Daten zu übermitteln, auf den Rechtsgedanken des übergesetzlichen Notstandes (§ 34 StGB) zu stützen, wird zunehmend von den Diensteanbietern in Frage gestellt. Eine eindeutige Rechtsgrundlage ist im Interesse der geschützten Rechtsgüter aber unverzichtbar.

Die Befugnis ist an die jeweiligen Voraussetzungen des Art. 34a Abs. 1 Satz 1 bzw. des Abs. 3 Satz 1 geknüpft. Gegenstand der Übermittlung sind vorhandene Daten (Nr. 1) sowie die spezifischen Kennungen, die zur Ermittlung des Gerätestandortes erforderlich sind (Nr. 3). In Satz 1 Nr. 2 wird klargestellt, dass auch die Anordnung möglich ist, zukünftige Verbindungsdaten zu übermitteln. Die Übermittlungspflicht betrifft nur die Daten der in Art. 34a Abs. 1 Satz 1 bzw. in Abs. 3 Satz 1 genannten Personen.

Soweit die Erforschung des Sachverhalts und damit die Abwehr der Gefahren bzw. die Verhinderung schwerwiegender Straftaten auf andere Weise erheb-

lich erschwert wäre, darf nach Satz 2 die Übermittlung der im Wege einer Umkehrsuche gewonnenen Daten angeordnet werden. In Fällen, in denen es erforderlich ist, die letzten Gesprächspartner vermisster Personen zu ermitteln, kann die Übermittlung der Daten aus einem derartigen Zielsuchlauf entscheidende Hinweise zur Gefahrenabwehr liefern. Gleiches gilt für die Fallgruppen des Art. 34a Abs. 1 Satz 1. Die Art und Weise der Datenübermittlung regelt Satz 3.

- c. Absatz 3 enthält eine Legaldefinition der Telekommunikationsverbindungsdaten. Da die technische Entwicklung noch weiter fortschreitet und möglicherweise derzeit verwendete Kennungen künftig durch andere Merkmale ersetzt werden, kann eine abschließende Aufzählung der Daten nicht erfolgen.

Die Einbeziehung der Verbindungsdaten, die während des „Stand-By-Betriebs“ eines Mobilfunkendgerätes erhoben werden, ist im Interesse einer effektiven Gefahrenabwehr unerlässlich. Die Abfrage der Standortkennung eines Mobiltelefons im „Stand-By-Betrieb“ greift nicht stärker in die Telekommunikationsfreiheit ein, als die Abfrage der Standortkennung eines Mobiltelefons, mit dem aktuell telefoniert wird. Demgegenüber ist die Maßnahme beispielsweise in Fällen des Art. 34a Abs. 3 notwendig, wenn die vermisste oder hilflose Person keine Anrufe entgegennehmen oder tätigen kann. Auch in den Fällen des Art. 34a Abs. 1 ist es erforderlich, im Interesse der geschützten Rechtsgüter und der Verhinderung schwerwiegender Straftaten, Daten zu erheben, während Mobilfunkendgeräte nicht in Sendebetrieb sind.

3. Die Regelung über das Verfahren zur Datenerhebung bei der Telekommunikationsüberwachung in Art. 34c orientiert sich an den entsprechenden Maßgaben in der Strafprozessordnung. Durch die besonderen verfahrensrechtlichen Absicherungen wird den Vorgaben des Bundesverfassungsgerichts folgend den datenschutzrechtlichen Erfordernissen entsprochen. Darüber hinaus werden die Verwertungsverbote, die Kennzeichnungs- und die Benachrichtigungspflicht sowie das Lösungsgebot geregelt.

- a. Zur Anordnung einer Maßnahme nach Art. 34a und 34b bedarf es, in Anbetracht der hohen Bedeutung des Fernmeldegeheimnisses, einer richterlichen

Entscheidung, auch wenn diese in Art. 10 GG nicht zwingend vorgesehen ist. Durch die Kontrolle einer unabhängigen Instanz wird der Grundrechtsschutz zusätzlich abgesichert.

Bei Gefahr im Verzug ist – in Anlehnung an Art. 24 Abs. 1 PAG bzw. Art. 34 Abs. 2 – eine Anordnung durch hochrangige Dienststellenleiter (sog. Behördenleitervorbehalt) ausreichend. Nach Satz 2 ist in diesen Fällen die richterliche Bestätigung binnen drei Tagen nachzuholen. Wird die Maßnahme nicht fristgerecht durch den Richter bestätigt oder versagt der Richter die Bestätigung, tritt die Anordnung mit ex-nunc-Wirkung außer Kraft. Entfällt die Gefahr im Verzug erkennbar vor Ablauf der Drei-Tages-Frist, muss die Anordnung des Dienststellenleiters unverzüglich aufgehoben und nötigenfalls eine neue Anordnung durch den Richter beantragt werden.

- b. In Absatz 2 wird eine entsprechende Regelung für die Fälle des Art. 34a Abs. 3 und die dafür erforderlichen Maßnahmen gegenüber den Diensteanbieter nach Art. 34b Abs. 1 und 2 getroffen. Ein Richtervorbehalt ist nicht geboten, da die Maßnahme regelmäßig besonders eilbedürftig ist und im Interesse des Betroffenen liegt. Zudem ist der Umfang der Maßnahme auf die Ermittlung des Aufenthaltsortes beschränkt.
- c. Absatz 3 regelt die formellen Anforderungen an die Anordnungen nach Absatz 1 und 2. Die Schriftlichkeit erfüllt neben der Beweiskraft eine Warnfunktion. Ausnahmen vom Schriftlichkeitserfordernis sind lediglich bei Gefahr im Verzug gemacht, wenn die schriftliche Niederlegung dazu führen würde, dass die Erreichung des polizeilichen Zwecks aufgrund des zeitlichen Verzuges gefährdet wäre. Die inhaltlichen Anforderungen an die Maßnahme bleiben hiervon unberührt.

Grundsätzlich ist die genaue Bezeichnung des Betroffenen sowie die Angabe der Rufnummer oder einer anderen Kennung des Endgeräts oder des Anschlusses erforderlich. Liegt allerdings eine gegenwärtige Gefahr für Leben, Gesundheit oder Freiheit einer Person vor und ist andernfalls die Sachverhaltsermittlung oder die Zweckerreichung erheblich erschwert, ist es gerechtfertigt, eine räumlich und zeitlich hinreichend genaue Bezeichnung der zu überwachenden Telekommunikation genügen zu lassen. Als Beispiel ist etwa

an die Unterbrechung des Mobilfunkverkehrs bei einer Geiselnahme zu denken, um die Kommunikation mit Komplizen zu verhindern. Unter diesen engen Voraussetzungen ist auch ein sog. „Funkzellenabgleich“ zulässig, bei dem bei konkreten Anhaltspunkten, dass sich ein Störer zu bestimmten Zeiten innerhalb bestimmter Funkzellen aufhält, alle Positionsmeldungen innerhalb des festgelegten Ortes und der festgesetzten Zeit erfasst werden und durch späteren Abgleich die Identität der Zielperson ermittelt werden kann. Der Kreis der Betroffenen muss dabei räumlich möglichst genau bezeichnet werden. Art, Umfang und Dauer der Maßnahme müssen in der Anordnung in jedem Fall genau bestimmt sein.

Die Befristung orientiert sich an der Regelung für die Wohnraumüberwachung. Durch die Monatsfrist wird eine effektive gerichtliche Kontrolle gewährleistet. Die Fristen für die Telekommunikationsunterbrechung und -verhinderung sind vor dem Hintergrund des Übermaßverbotes kürzer. Darüber hinaus besteht nach Satz 5 die Möglichkeit der Verlängerung der Maßnahmen. In Konkretisierung des Verhältnismäßigkeitsgrundsatzes wird in Satz 6, 1. Halbsatz klargestellt, dass die jeweiligen Maßnahmen zu beenden sind, wenn die Voraussetzungen entfallen. Die Mitteilungspflicht bei Beendigung gemäß Halbsatz 2 ist erforderlich, da der Richter die Maßnahme nicht nur anordnet, sondern auch überwacht.

- d. Die Zweckbindungs- und Kennzeichnungspflichten sind in Absatz 4 geregelt. Bei einer Zweckänderung durch Weitergabe der Daten an die Strafverfolgungsbehörden richtet sich die Zulässigkeit nach den Regelungen der Strafprozessordnung für die Verwertung der Daten, hilfsweise nach den Befugnissen für die Erhebung von Daten durch Telekommunikationsüberwachung bzw. für die sonstigen Maßnahmen.

Das Verwertungsverbot in Satz 3 erfasst Datenerhebungen, bei denen sich nach Auswertung herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben bzw. dass sie aus besonders geschützten Vertrauensverhältnissen stammen und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 Buchst. a genannten Gefahren oder Straften haben. Eine Verwertung ist entsprechend der Regelung in Art. 34 Abs. 3 Satz 3 zulässig,

wenn dies zum Schutz hochwertigster Rechtsgüter vor gegenwärtigen Gefahren erforderlich ist.

- e. Die Benachrichtigungspflicht erfasst neben den Adressaten der Maßnahme die Personen, deren Daten zu den Zwecken der Gefahrenabwehr oder der Strafverfolgung verwendet wurden. Aus dem Rechtsgedanken heraus, dass die grundrechtliche Betroffenheit mit den Interessen des jeweiligen Adressaten abzuwägen ist und dass die Benachrichtigung nicht zu Vertiefungen der Eingriffe führen darf, ist eine Einschränkung des Kreises der zu benachrichtigenden Personen gerechtfertigt. Für die Zurückstellung der Benachrichtigung und die näheren Bestimmungen über das Verfahren gelten die zu Art. 34 Abs. 4 dargelegten Grundsätze entsprechend.
- f. Die Löschung von Daten, bei denen sich nach Auswertung ergibt, dass sie aus Vertrauensverhältnissen zu engsten Familienangehörigen, zu besonderen Vertrauten oder zu Berufsgeheimnisträgern stammen und keinen Bezug zu den abzuwehrenden Gefahren bzw. den zu verhütenden schwerwiegenden Straftaten haben, ist in Absatz 6 Satz 1 geregelt. Für sonstige Daten gilt der Vorrang der Sperrung, wenn sie für die gerichtliche Überprüfung noch benötigt werden.

Zu § 1 Nr. 5 (Art. 36 Abs. 1 Nr. 2)

Es handelt sich um eine Folgeänderung zu § 1 Nr. 1.

Zu § 1 Nr. 6 (Art. 38 Abs. 3)

Im Volkszählungsurteil hat das Bundesverfassungsgericht für Eingriffe in das Recht auf informationelle Selbstbestimmung auch organisatorische und verfahrensrechtliche Vorkehrungen gefordert, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Dem trägt der neu eingefügte Absatz 3 für den Einsatz automatisierter Kennzeichenerkennungssysteme Rechnung.

Befürchtungen, die durch den Einsatz automatisierter Kennzeichenerkennungssysteme mögliche massenhafte Erhebung von Daten führe zu einer unzulässigen Ausweitung polizeilicher Datenbestände, ist zunächst zu entgegnen, dass die Erhebung der Daten abgesehen von den wenigen bislang schon möglichen Fällen nur unter den nunmehr gesetzlich genannten Voraussetzungen zulässig ist, die sich an der Befugnisnorm zur Identitätsfeststellung orientieren. Darüber hinaus wird durch die Regelung des neu eingefügten Absatzes 3 sichergestellt, dass ein den Maßgaben des Bundesverfassungsgerichts entsprechender verhältnismäßiger Umgang mit den erhobenen Daten erfolgt. So verlangt Satz 1, dass die durch den Einsatz automatisierter Kennzeichenerkennungssysteme nach Art. 33 Abs. 2 Satz 2 erhobenen Daten – nach Durchführung des gemäß Art. 33 Abs. 2 Satz 2 i. V. m. Art. 43 möglichen Datenabgleichs – grundsätzlich unverzüglich wieder zu löschen sind. Etwas anderes gilt nur dann, wenn ihre Speicherung, Veränderung oder Nutzung im einzelnen Fall zur Verfolgung von Straftaten, von Ordnungswidrigkeiten, zur Abwehr einer konkreten Gefahr (vgl. die Legaldefinition in Art. 11 Abs. 1) oder im Rahmen einer längerfristigen Observation nach Art. 33 Abs. 1 Nr. 1, Abs. 2 Satz 1 oder einer polizeilichen Beobachtung im Sinn des Art. 36 erforderlich ist. In diesem Fall finden – insoweit bundesrechtlich vorgegeben – die Vorschriften der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten sowie die Absätze 1 und 2 über die Speicherung, Veränderung und Nutzung von Daten Anwendung. Durch diese Regelung wird erreicht, dass die vergleichsweise großzügigen Möglichkeiten der Absätze 1 und 2 für die Speicherung, Veränderung oder Nutzung von Daten in den Fällen des nach Art. 33 Abs. 2 Satz 2 lediglich routinemäßigen Einsatzes automatisierter Kennzeichenerkennungssysteme nur dann eingreifen, wenn zunächst die in Absatz 3 Satz 2 im Einzelnen genannten „Hürden“ übersprungen werden können. Es muss also für den jeweiligen Einzelfall belegbar sein, dass die Speicherung, Veränderung oder Nutzung der nach Art. 33 Abs. 2 Satz 2 erhobenen Daten zur Verfolgung von Straftaten, von Ordnungswidrigkeiten, zur Abwehr einer konkreten Gefahr oder im Rahmen einer längerfristigen Observation oder polizeilichen Beobachtung erforderlich ist. Ist dies der Fall, dann – aber auch nur dann – gelten die herkömmlichen Regelungen der Strafprozessordnung, des Gesetzes über Ordnungswidrigkeiten sowie die Absätze 1 und 2 über die Zulässigkeit der Speicherung, der Veränderung und Nutzung der Daten. Nur in diesen Fällen kommt dann beispielsweise auch eine Speicherung zur zeit-

lich befristeten Dokumentation, zur Vorgangsverwaltung oder zur vorbeugenden Bekämpfung von Straftaten in Betracht.

Die Regelung verbietet somit im Ergebnis jegliche willkürliche Vorratsdatenspeicherung über unbescholtene Personen und schließt insoweit auch die Erstellung von Bewegungsbildern aus.

Zu § 1 Nr. 7 (Art. 40)

Mit dieser Vorschrift werden die Regelungen über die Datenübermittlung innerhalb des öffentlichen Bereichs überarbeitet.

Dies ist deshalb notwendig, weil die Polizei andernfalls den ständig zunehmenden internationalen Verpflichtungen der Bundesrepublik Deutschland zur grenzüberschreitenden Polizeikooperation nur unzureichend nachkommen könnte. So ist eine Initiativübermittlung personenbezogener Daten an nichtinnerstaatliche Stellen bei streng am Wortlaut der Absätze 2 und 3 des Art. 40 orientierter Auslegung bislang nur zur Erfüllung eigener Aufgaben der Bayerischen Polizei möglich, nicht aber zur Erfüllung von Aufgaben der ausländischen bzw. der über- oder zwischenstaatlichen Empfängerdienststelle. Auf Ersuchen der aus- bzw. über- oder zwischenstaatlichen Stelle kommt eine Datenübermittlung außer zur Abwehr einer erheblichen Gefahr durch den Empfänger nach Art. 40 Abs. 5 nur dann in Betracht, wenn die Polizei hierzu auf Grund über- oder zwischenstaatlicher Vereinbarungen ausdrücklich verpflichtet ist. Diese noch von Misstrauen gegenüber dem Ausland geprägten engen Voraussetzungen entsprechen heute nicht mehr den in den bilateralen Kooperationsvereinbarungen sowie den Rechtsakten der Europäischen Union verankerten Anforderungen an einen effektiven Datenaustausch zur Bekämpfung der grenzüberschreitenden Kriminalität und zur Schaffung eines Europäischen Raums der Freiheit, der Sicherheit und des Rechts.

- a. Der polizeilichen Übermittlung von personenbezogenen Daten an Empfänger außerhalb des Geltungsbereichs des Grundgesetzes sowie an zwischen- oder überstaatliche Organisationen kommt angesichts einer Vielzahl neu geschaf-

fener einschlägiger völkerrechtlicher Vereinbarungen eine neue Qualität und besondere Bedeutung zu. Deshalb, aber auch aus Gründen einer besseren Übersichtlichkeit und Anwendbarkeit des Gesetzes, werden die bisher in mehreren Absätzen des Art. 40 angesiedelten Varianten der Datenübermittlung an nichtinnerstaatliche Datenempfänger künftig in Absatz 5 zusammengeführt und, soweit erforderlich, neu geregelt. Als Folge hiervon wird die bisher in Absatz 2 enthaltene Regelung zur Initiativübermittlung an solche Stellen gestrichen und statt dessen in einen neuen Absatz 5 überführt.

- b. Mit der Ersetzung des Begriffs „Gefahrenabwehr“ durch den Terminus „Abwehr von Gefahren“ in Absatz 3 wird einer bisher bestehenden Problematik begegnet, die in der Vergangenheit des Öfteren zu Schwierigkeiten bei der Rechtsanwendung geführt hat. Der bisherige Wortlaut stellt bei enger Auslegung auf den Status einer Behörde oder öffentlichen Stelle als Gefahrenabwehrbehörde, mithin als „Sicherheitsbehörde“, ab. Welche Behörden darunter zu subsumieren sind, ist an verschiedenen Stellen gesetzlich geregelt (vgl. insbesondere die Auflistung der „allgemeinen“ Sicherheitsbehörden in Art. 6 des Landesstraft- und Verordnungsgesetzes – LStVG).

Rechtlich zweifelhaft war die Datenübermittlung immer dann, wenn eine Behörde oder öffentliche Stelle bei der Polizei vorhandene personenbezogene Daten benötigt, um im Einzelfall Gefahren abzuwehren, ohne dass sie selbst den formalen Status einer Sicherheitsbehörde besitzt. Dies trifft zum Beispiel auf Sozialämter, Jugendämter oder Schulbehörden zu, die zwar keine allgemeinen oder besonderen Sicherheitsbehörden sind, denen im Einzelfall aber trotzdem auch die Abwehr von Gefahren obliegen kann (Unterstützung einer verwaorlosten Person, deren Gesundheit in Gefahr ist; notorischer „Schulschwänzer“, der fortwährend mit dem Gesetz in Konflikt zu kommen droht etc.).

Mit der Neuformulierung stellt das Gesetz nicht mehr auf den Status der handelnden Behörde, sondern auf die Abwehr einer Gefahr für die öffentliche Sicherheit durch eine hierzu berufene Stelle ab, ohne dass deren Status als „Sicherheitsbehörde im engeren Sinn“ entscheidend wäre.

Für die Beschränkung der Zulässigkeit einer Datenübermittlung ausschließlich auf solche Behörden oder öffentliche Stellen, die im engen Wortsinne und primär für die Gefahrenabwehr zuständig sind, besteht kein einleuchtender Grund. Diese Einschätzung wird dadurch gestützt, dass auch Art. 9 Abs. 1 Halbsatz 1 des Polizeiorganisationsgesetzes – POG – auf die Zusammenarbeit mit „... andere(n) Stellen, denen die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung“ obliegt, abstellt und nicht nur auf die Sicherheitsbehörden im engeren Sinn. Gegen eine derart restriktive Auslegung spricht im Übrigen schon der sich aus der Ausstrahlungswirkung der Grundrechte ergebende staatliche Schutzauftrag, dessen Erfüllung im Einzelfall nicht am formalen Status der zuständigen Behörde scheitern darf.

- c. Die bisherige Regelung der Anlassübermittlung an inländische (nichtpolizeiliche) Stellen zur Erfüllung der Aufgaben des Empfängers in Absatz 4 verlangte, dass die Datenübermittlung an die datenempfangende Stelle erforderlich „ist“. Dieser Maßstab ist in den Fällen einer Datenübermittlung zur Erfüllung inländischer polizeilicher Aufgaben (Absätze 1, 2 und 5 Nr. 1 neu) gerechtfertigt, da die Polizei hier auf Grund eigener Sach- und Rechtskenntnis (auch die Tätigkeiten der Polizeien der anderen Länder und die hierfür geltenden Rechtsvorschriften sind im Wesentlichen gleich) die nötige Beurteilung vornehmen kann, welche Daten zur Erfüllung inländischer polizeilicher Aufgaben an welche Stellen übermittelt werden müssen. Soll die Aufgabenerfüllung, der die Datenübermittlung dient, aber durch eine sonstige (nichtpolizeiliche) Stelle erfolgen, liegt es in der Natur der Sache, dass es der übermittelnden polizeilichen Stelle unmöglich ist, die absolute Erforderlichkeit der Datenübermittlung zu prüfen oder gar festzustellen. Vielmehr kann sich die Prüfung nur auf die Frage erstrecken, ob die Erforderlichkeit der Datenübermittlung zur Erfüllung der Aufgaben des Empfängers fachlich und rechtlich plausibel erscheint. Dem trägt die nunmehrige Formulierung „... erforderlich erscheint“ Rechnung. Darüber hinaus wird mit dieser Änderung die Kongruenz zu Absatz 3 (Initiativübermittlung an inländische nichtpolizeiliche Stellen zur Erfüllung der Aufgaben des Empfängers) sowie Absatz 5 Nrn. 2 und 3 neu (Initiativ- und Anlassübermittlung an nichtinnerstaatliche Stellen zur Erfüllung der Aufgaben des Empfän-

gers) gewahrt, denen eine vergleichbare Ausgangslage zu Grunde liegt. Die Anpassung des Absatzes 4 ist insoweit systematisch konsequent.

- d. Absatz 5 Satz 1 nimmt mit seiner Neufassung zur Gänze die Vorschriften über die Übermittlung personenbezogener Daten an Datenempfänger außerhalb des Geltungsbereichs des Grundgesetzes und an zwischen- oder überstaatliche Stellen auf und ersetzt die bisherige verstreute Regelung der Absätze 2 und 5. Absatz 5 umfasst in seiner neuen Fassung sowohl die Initiativ- als auch die Anlassübermittlung personenbezogener Daten an nichtinnerstaatliche Stellen.

Mit dem neu formulierten Satz 1 sind die Vorschriften über die Datenübermittlung auf Ersuchen und über die so genannte Initiativübermittlung nun in Regelungsinhalt und -umfang parallel ausgestaltet. Die bisherige Bindung der einzelnen Übermittlungsarten an qualitativ deutlich voneinander abweichende Erfordernisse ist der Sache nach nicht geboten, da in beiden Fallgestaltungen das Bedürfnis des Datenempfängers, Gefahren abzuwehren, regelmäßig als gleichwertig anzunehmen ist und im Übrigen die Entscheidung zur Datenweitergabe uneingeschränkt bei der datenführenden Stelle der Bayerischen Polizei liegt. Darüber hinaus behandeln die einschlägigen völkervertraglichen Vorschriften zur Polizeikooperation beide Varianten regelmäßig gleich, so dass auch aus diesem Gesichtspunkt kein Anlass besteht, Initiativ- und Anlassübermittlung differenziert zu regeln. Mit der Zusammenführung beider Übermittlungsarten in Absatz 5 ist jeweils der Kreis der möglichen Datenempfänger identisch ausgestaltet. Dies ist aus den vorgenannten Gründen ebenfalls sachgerecht.

Die grenzüberschreitende Datenübermittlung ist insbesondere für die Aufrechterhaltung der Inneren Sicherheit in einheitlichen kriminal- und gefahrengeografischen Räumen wichtig, wie sie sich längst beiderseits der Staatsgrenzen entwickelt haben. Darüber hinaus ist sie Voraussetzung für die Schaffung eines Europäischen Raumes der Freiheit, der Sicherheit und des Rechts. Die aus der bisherigen Formulierung der Absätze 2 und 3 herrührende Problematik, dass die Initiativübermittlung bei streng am Wortlaut orientierter Auslegung

an sich lediglich zur Erfüllung der eigenen Aufgaben der Bayerischen Polizei, nicht aber auch zur Aufgabenerfüllung der ausländischen (oder zwischen- oder überstaatlichen) datenempfangenden Stelle möglich ist, wird beseitigt. Die Gesetzesanpassung bringt insofern eine Klarstellung und zeichnet dabei bestehende Datenübermittlungsregelungen der Europäischen Union und bilateraler völkervertraglicher Vereinbarungen nach.

Personenbezogene Daten können an nichttinnerstaatliche Stellen übermittelt werden, soweit zusätzlich zu den genannten Voraussetzungen wenigstens eine der vom Gesetz enumerativ genannten Bedingungen vorliegt.

Die Nummer 1 enthält den Regelungsgehalt des bisherigen zweiten Halbsatzes des Absatzes 2.

Im Gegensatz zu Nummer 1 alt fordert die korrespondierende neue Nummer 2 als Voraussetzung der Datenübermittlung nun nicht mehr eine völkervertragliche Verpflichtung, sondern stellt auf das Vorliegen einer völkervertraglichen Ermächtigung ab. Geboten ist dies deshalb, weil die einschlägigen völkerrechtlichen Vereinbarungen regelmäßig nicht eine Pflicht, sondern eine Möglichkeit zur Datenübermittlung normieren. Dies ist auch sinnvoll, weil die letzte Entscheidung über die Datenweitergabe – entsprechend weiterer Vorgaben des Gesetzes – stets bei der datenführenden Stelle verbleibt. Sonstige internationale Verpflichtungen der Bundesrepublik Deutschland können insbesondere Rechtsakte der Vereinten Nationen, etwa zur Einrichtung von VN-Polizeimissionen mit exekutiven Aufgaben in Krisengebieten, sein.

Auch wenn keine einschlägigen völkerrechtlichen Instrumente bestehen oder keine eigene Aufgabe der inländischen Polizei zu erfüllen ist, soll doch im Einzelfall und unter bestimmten Voraussetzungen zum Zwecke der Gefahrenabwehr die Übermittlung von personenbezogenen Daten an nichtdeutsche staatliche und über- oder zwischenstaatliche Stellen möglich sein. Allerdings wird gerade im Falle des Fehlens völkerrechtlicher Vereinbarungen – und damit von ausdrücklich erklärten Garantien des Empfangsstaates – in besonderem Maße einzelfallspezifisch zu prüfen sein, in wie weit eine Datenübermittlung verhält-

nismäßig ist. Dieses Erfordernis manifestiert sich in der Formulierung des Gesetzestextes. So stellt Nummer 3 im Vergleich zu den Nummern 1 und 2 erhöhte tatbestandliche Anforderungen und sieht ausdrücklich vor, dass die Datenübermittlung als erforderlich erscheinen muss, um eine erhebliche Gefahr abzuwehren. Diese bereits bislang vorgesehene Steigerung ist sachgerecht und daher zu erhalten. Demgegenüber wird – wie auch im Fall der Nummer 2 – die Anforderung an den Nachweis der Erforderlichkeit der Datenübermittlung zur Gefahrenabwehr durch die nichtinnerstaatliche Behörde leicht abgesenkt. Die bisherige Regelung verlangte, dass die Datenübermittlung an die nichtinnerstaatliche Stelle erforderlich „ist“. Besteht die abzuwehrende Gefahr aber außerhalb des Zuständigkeitsbereiches der inländischen Polizei, deren Tätigkeit die Bayerische Polizei fachlich und auch rechtlich beurteilen kann, liegt es in der Natur der Sache, dass es der übermittelnden Stelle unmöglich ist, die absolute Erforderlichkeit der Datenübermittlung zu prüfen oder gar festzustellen. Vielmehr kann sich die Prüfung nur darauf erstrecken, ob die Erforderlichkeit der Datenübermittlung zur Erfüllung der Aufgaben des Empfängers fachlich und rechtlich plausibel erscheint. Dem trägt die nunmehrige Formulierung „... erforderlich erscheint“ Rechnung (vgl. hierzu auch die Begründung oben zu Absatz 4).

Die Grenzen der Übermittlung und eventuelle Übermittlungshindernisse ergeben sich insbesondere aus Satz 2, dessen Inhalt durch die Verankerung der Initiativübermittlung in Satz 1 nun auch für diese maßgeblich ist. Die vorgenommene Änderung des Textes – Streichung des Wortes „durch“ – ist rein redaktioneller Natur.

Zu § 1 Nr. 8 (Art. 42 Abs. 3)

Insoweit handelt es sich lediglich um eine Klarstellung, dass auch Polizeidienststellen zum Kreis der ersuchten ausländischen Stellen gehören können.

Zu § 1 Nr. 9 (Art. 46 Abs. 2)

Die Anfügung eines neuen Satzes 4 in Absatz 2 ergänzt als weitere Schutzvorkehrung die Regelung des Art. 38 Abs. 3, indem die Protokollierung von Abfragen, die anlässlich des Einsatzes automatisierter Kennzeichenerkennungssysteme vorgenommen werden, ausdrücklich untersagt wird. Auch insoweit bleibt also die Erstellung von Bewegungsbildern unmöglich.

Zu § 1 Nr. 10 (Art. 61 Abs. 4)

Die zulässigen Waffen nach Art. 61 Abs. 4 PAG werden um das drahtgestützte Elektroimpulsgerät, das aus der Distanz eingesetzt werden kann und beim Betroffenen zu Handlungsunfähigkeit führt, ergänzt. Insbesondere bei den Spezialeinheiten der Bayerischen Polizei besteht das Bedürfnis, Geräte wie den sogenannten "Advanced Taser" einzusetzen. Die Erfahrungen aus anderen Ländern belegen den hohen Einsatzwert und zeigen, dass die Waffe eine Alternative darstellt, um den Einsatz der Schusswaffe und damit Verletzungen des Angreifers zu vermeiden. Durch die Bezugnahme auf vergleichbare Waffen wird der Einsatz von Geräten, die zwar nicht drahtgestützt arbeiten, aber in technisch ähnlicher Weise wirken und gleichartige Folgen bei einem Angreifer hervorrufen, ermöglicht. Angesichts der rasch fortschreitenden Entwicklung dieser Waffengattung ist eine Festlegung auf ein drahtgestütztes Gerät nicht zweckmäßig. Unter dem Gesichtspunkt der Verhältnismäßigkeit stellen derartige Waffen ein milderes Mittel zum Schusswaffeneinsatz dar.

Forschung und Technik ermöglichen im Bereich der Waffentechnik auch über die Elektroschockwaffen hinaus Neuentwicklungen, die ebenfalls darauf ausgerichtet sind, Angreifer handlungsunfähig zu machen. Für die Polizei ist es unerlässlich, derartige Neuerungen zu beobachten und ggf. hinsichtlich ihrer Einsatzmöglichkeit für allgemeine Einsatzzwecke oder für besondere Einheiten zu prüfen. Der neu angefügte Satz 2 ermöglicht es auf Anordnung des Staatsministeriums des Innern Waffen auf ihre Einsatztauglichkeit zu erproben. Erfasst werden dabei nur solche Waffen, deren Einsatz unter Beachtung des Verhältnismäßigkeitsgrundsatzes in Betracht kommen. Maßstab ist die Eingriffsintensität der vom Gesetzgeber in Satz 1 zugelassenen Waffen.

Zu § 1 Nr. 11 (Art. 74)

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 von Art. 10 Abs. 1 GG unter einen ausdrücklichen Gesetzesvorbehalt gestellt wird, ist die Aufnahme in den Katalog der nach dem PAG einschränkbaren Grundrechte erforderlich.

Zu § 2 Änderung des Parlamentarischen Kontrollgremium - Gesetzes:

Folgeänderung zu § 1 Nr. 3 g des Gesetzentwurfs.

Zu § 3 (In-Kraft-Treten):

Die Vorschrift regelt das In-Kraft-Treten.