Bayerischer Landtag
15. Wahlperiode
Drucksache 15/**2096**
23.11.2004

Gesetzentwurf

der Staatsregierung

zur Änderung des Polizeiaufgabengesetzes und des Parlamentarischen Kontrollgremium-Gesetzes

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 Kommuni-

kationsstrukturen einen wichtigen Ansatzpunkt für die Abwehr drohender Gefahren und 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 modernste Telekommunikationstechnik nutzen.

Ferner hat die polizeiliche Praxis seit geraumer Zeit dargelegt, dass die Erhebung von Telekommunikationsverkehrsdaten nicht nur zur Abwehr der genannten Gefahren unverzichtbar ist, sondern auch 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 zur Bekämpfung schwerwiegender Straftaten 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 verschiedenen Artikeln des III. Abschnitts des Gesetzes geregelt sind, werden die Art. 33, 38 und 46 ergänzt.

2. In das Polizeiaufgabengesetz werden Art. 34a und 34b 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. 34c 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 Telekommunikationsverkehrsdaten 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. 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, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, Verwendungsverboten und einer Löschenspflicht. 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 besonderen Vertrauensbeziehungen zusätzlich über generelle Abhörverbote für Vertrauenspersonen sowie über die Verpflichtung, eine laufende Maßnahme abzubrechen, wenn erkennbar wird, dass ein Eingriff in den Kernbereich privater Lebensgestaltung erfolgt. Dabei findet eine Erweiterung des Schutzes statt, um Berufsgeheimnisträger ebenfalls zu schützen. Die generelle richterliche Kontrolle der Verwertbarkeit stellt eine weitere Verfahrenssicherung dar, die den Grundrechtsschutz zusätzlich 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

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

1. Die voraussichtlichen künftigen Kosten des Einsatzes der präventiven Wohnraumüberwachung sind nicht konkret bezifferbar, da sie 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 anderseits – aufgrund der erheblichen Einengung des Anwendungsbereichs – insgesamt mit einem Rückgang der Fallzahlen zu rechnen ist, so dass eventuelle Kostensteigerungen dadurch kompensiert werden.

2. 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.

Bayerischer Landtag
15. Wahlperiode
Drucksache 15/**2096**
23.11.2004

Gesetzentwurf

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) [1]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 Abs. 1 und 2, §§ 176a, 177, 180b, 181, 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 des Waffengesetzes 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 Genehmigung oder behördliche Erlaubnis erteilt werden kann, und
   10. Straftaten nach § 30a oder § 30b des Betäubungsmittelgesetzes, soweit offensichtlich ist, dass keine Genehmigung oder behördliche Erlaubnis erteilt werden kann.

   [2]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 Betäubungsmittelgesetzes,
   4. § 96 des Aufenthaltsgesetzes."

2. Der Wortlaut in Art. 33 Abs. 2 wird Satz 1; es werden folgende Sätze 2 und 3 angefügt:

   „[2]Darüber hinaus kann die Polizei unbeschadet des Art. 30 Abs. 3 Satz 2 durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme in den Fällen des Art. 13 Abs. 1 Nrn. 1 bis 5 Kennzeichen von Kraftfahrzeugen erfassen und sie mit dem Fahndungsbestand abgleichen. [3]Der Abgleich mit anderen polizeilichen Dateien ist nur zulässig, soweit die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehenden Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist."

3. Art. 34 erhält folgende Fassung:

   „Besondere Bestimmungen über
   den Einsatz technischer Mittel in Wohnungen

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

   1. über die für eine Gefahr Verantwortlichen, wenn dies erforderlich ist zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, oder
   2. über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass diese Personen eine schwerwiegende Straftat begehen werden.

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

1. die dort genannten Gefahren nicht anders abgewehrt oder die dort genannten Straftaten nicht anders verhütet oder abgewehrt werden können und
2. für den Fall, dass zu privaten Wohnzwecken genutzte Räumlichkeiten betroffen sind, in denen sich die Person, gegen die sich die Maßnahme richtet, allein oder ausschließlich mit engsten Familienangehörigen, mit in gleicher Weise Vertrauten oder mit Berufsgeheimnisträgern nach §§ 53, 53a StPO aufhält,
   a) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gespräche geführt werden, die einen unmittelbaren Bezug zu den in Satz 1 Nrn. 1 und 2 genannten Gefahren oder Straftaten haben, ohne dass über ihren Inhalt das Zeugnis als Geistlicher, Verteidiger, Rechtsanwalt, Arzt, Berater für Fragen der Betäubungsmittelabhängigkeit, Psychologischer Psychotherapeut oder Kinder- und Jugendlichenpsychotherapeut nach §§ 53, 53a StPO verweigert werden könnte, oder
   b) die Maßnahme sich auch gegen die Familienangehörigen, Vertrauten oder Berufsgeheimnisträger richtet, und
3. für den Fall, dass sich die Maßnahme gegen einen Berufsgeheimnisträger nach §§ 53, 53a StPO selbst richtet und die zu seiner Berufsausübung bestimmten Räumlichkeiten betroffen sind, die Voraussetzungen der Nr. 2 Buchst. a vorliegen.

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

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

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

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

(4) [1]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 unverzüglich eine Bestätigung der Maßnahme durch einen Richter einzuholen. [2]Für die richterliche Anordnung ist Art. 24 Abs. 1 Satz 3 entsprechend anzuwenden; zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. [3]In der schriftlichen Anordnung sind Adressat, Art, Umfang und Dauer der Maßnahme zu bestimmen und die wesentlichen Gründe anzugeben. [4]Die Maßnahme ist auf höchstens einen Monat zu befristen und kann um jeweils nicht mehr als einen Monat verlängert werden. [5]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.

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

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

[3]Daten, bei denen sich nach Auswertung herausstellt, dass

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

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

(6) [1]Die Betroffenen sind von Maßnahmen nach Abs. 1 Satz 1 zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht of-

fen ermittelnden Beamten oder der in Abs. 1 Satz 1 genannten Rechtsgüter geschehen kann. [2]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. [3]Erfolgt die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. [4]Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. [5]Eine Unterrichtung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

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

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

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

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

sind zu sperren, wenn sie zum Zweck der Information der Betroffenen und zur gerichtlichen Überprüfung der Erhebung oder Verwendung der Daten noch benötigt werden; andernfalls sind sie zu löschen. [3]Im Fall der Unterrichtung des Betroffenen sind die Daten zu löschen, wenn der Betroffene sich nicht innerhalb eines Monats nach seiner Benachrichtigung mit Rechtsbehelf gegen die Maßnahme gewendet hat; auf diese Frist ist in der Benachrichtigung hinzuweisen. [4]Im Fall eines Rechtsbehelfs nach Satz 2 sind die Daten nach Abschluss des Rechtsbehelfsverfahrens zu löschen.

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

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

(10) 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) [1]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 Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist, oder
2. über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass
   a) sie eine schwerwiegende Straftat begehen werden oder
   b) sie für Personen nach Buchst. a oder nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder weitergeben oder
   c) die unter Buchst. a oder Nr. 1 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.

[2]Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. [3]Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Datenerhebung insoweit unzulässig, es sei denn, die Maßnahme richtet sich gegen den Berufsgeheimnisträger selbst oder ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich.

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

1. zur Vorbereitung einer Maßnahme nach Abs. 1 spezifische Kennungen, insbesondere die Geräte- und Kartennummer von Mobilfunkendgeräten, sowie

2. den Standort eines Mobilfunkendgerätes zu ermitteln.

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

(3) [1]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.

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

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

Art. 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) [1]Die Polizei kann unter den Voraussetzungen des Art. 34a Abs. 1 Satz 1 oder Abs. 3 Satz 1 Diensteanbieter verpflichten,

1. ihr vorhandene Telekommunikationsverkehrsdaten der in Art. 34a Abs. 1 Satz 1 und Abs. 3 Satz 1 genannten Personen zu übermitteln,
2. Auskunft über deren zukünftige Telekommunikationsverkehrsdaten zu erteilen oder
3. ihr die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer mitzuteilen.

[2]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 aussichtslos oder wesentlich erschwert wäre. [3]Die Daten sind der Polizei unverzüglich zu übermitteln.

(3) Telekommunikationsverkehrsdaten 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, Kartennummer, 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.

(4) Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden, soweit nicht eine Entschädigung nach dem Telekommunikationsgesetz zu gewähren ist.

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

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

(2) [1]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 Landeskriminalamts angeordnet werden. [2]Diese können die Anordnungsbefugnis auf besonders Beauftragte übertragen.

(3) [1]Anordnungen nach den Abs. 1 und 2 sind schriftlich zu erlassen und zu begründen. [2]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 Gefahr für Leib, Leben oder Freiheit einer Person genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation. [3]In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. [4]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.

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

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

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

[3]Daten, bei denen sich nach Auswertung herausstellt, dass

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

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

(5) [1]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.

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

(6) [1]Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind unverzüglich zu löschen; die Löschung ist zu dokumentieren. [2]Die durch eine Maßnahme nach 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. [3]Art. 34 Abs. 7 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) [1]Die nach Art. 33 Abs. 2 Sätze 2 und 3 erfassten Kennzeichen sind nach Durchführung des Datenabgleichs unverzüglich zu löschen. [2]Soweit ein Kennzeichen in der abgeglichenen Datei enthalten und seine 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 und 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) [1]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 Europäi-

schen Union, völkerrechtlicher Vereinbarungen oder sonstiger internationaler Verpflichtungen der Bundesrepublik Deutschland ermächtigt ist oder

3. zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich erscheint.

[2]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:

„[4]Abfragen, die mittels automatisierter Kennzeichenerkennungssysteme durchgeführt werden, 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:

„[2]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. 9" ersetzt.

2. In Art. 3 Abs. 2 Satz 1 werden die Worte „Art. 34 Abs. 6" durch die Worte „Art. 34 Abs. 9" ersetzt.

§ 3
In-Kraft-Treten

Dieses Gesetz tritt am …… 2005 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 Kennzeichenerfassung 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, zu den Kernstrukturen 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. Diese Notwendigkeit ergibt sich auch bei anderen schweren Straftaten. 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 zur Bekämpfung schwerwiegender Straftaten 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. Der Schutz wird auch auf Berufsgeheimnisträger ausgedehnt. 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 zu Zwecken 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 Abwehr 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, Straftaten aus dem Bereich des politischen Extremismus sowie die 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 Entscheidungen 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 Berufsgeheimnisträgern wie Anwälten, Ärzten, Geistlichen und Journalisten. Soweit Abhörmaßnahmen in eine solche Vertrauensbeziehung eingreifen, sind sie unzulässig. Stellt sich das Bestehen eines Vertrauensverhältnisses erst im Lauf der Maßnahme heraus, greifen Verwendungsverbote und die unverzügliche Löschenspflicht ein. Die Vertrauensbeziehungen zu anderen Personen werden ebenfalls durch Verwendungsverbote geschützt. Dadurch werden vertrauenswürdige und geheimhaltungsbedürftige Telekommunikationsdaten dem sicherheitsbehördlichen Zugriff bzw. der Verwertung grundsätzlich entzogen.

Nach Art. 73 Nr. 7 GG hat der Bund die ausschließliche Gesetzgebungskompetenz 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. Von dieser Kompetenzverteilung geht auch das Telekommunikationsgesetz (TKG; BGBl. I 2004, S. 1190) aus, das landesgesetzliche Regelungen zur Telekommunikationsüberwachung nicht nur voraussetzt (vgl. § 110 Abs. 9 Satz 1 Nr. 1 TKG), sondern auch klarstellt, dass diese unberührt bleiben (vgl. § 110 Abs. 1 Satz 6 TKG und die Begründung BR-Drs. 755/03, S. 126).

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. von Münch/Kunig Grundgesetz-Kommentar, 5. Auflage, Art. 10, Rn. 29). Daher bleibt es dem Landesgesetzgeber unbenommen, Beschränkungen des Fernmeldegeheimnisses zum Zweck der Gefahrenabwehr bereichsspezifisch zu regeln.

Die konkrete technische Abwicklung der landesgesetzlich zugelassenen Telekommunikationsüberwachung richtet sich nach den Regelungen des Telekommunikationsgesetzes und der darauf gestützten Rechtsverordnungen, auf die im Wege einer dynamischen Verweisung Bezug genommen wird. Die Entschädigung der Diensteanbieter bestimmt sich bis zum Inkrafttreten der auf § 110 Abs. 9 TKG beruhenden Rechtsverordnung, die auch die Entschädigung bei Maßnahmen aufgrund landesgesetzlicher Vorschriften zum Gegenstand hat, nach dem Justizvergütungs- und -entschädigungsgesetz.

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. Eine solche Beschränkung kann allerdings nicht generell angenommen werden, wenn es lediglich um die Möglichkeit geht, ein auf den Landesbereich beschränktes Gesetz wirksam zu vollziehen (BVerwG vom 19.05.1988, Az.: 7 C 37.87, BVerwGE 79, 339 ff.). Vielmehr werden auch solche Diensteanbieter, deren Firmensitz sich außerhalb Bayerns befindet, zur Unterstützung der Polizei nach Art. 34b Abs. 1 und 2 verpflichtet. Maßgeblicher Anknüpfungspunkt ist, dass sie auch in Bayern ihre Dienste anbieten und damit auch in Bayern den Adressaten einer Maßnahme nach Art. 34a die Möglichkeit eröffnen, Telekommunikationsdienste zu nutzen, die durch die polizeiliche Maßnahme überwacht werden sollen. Darin ist eine ausreichende Rechtfertigung für die Auferlegung von Mitwirkungspflichten für außerbayerische Unternehmen zu sehen.

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 Sicherheit 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, 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 vielfach nicht ohne weiteres als Gefahren für die öffentliche Sicherheit und Ordnung benannt werden können, deren Schutz aber in besonderem Maße geboten ist. Dabei wird der Bekämpfung von Straftaten, die bandenmäßig, gewerbsmäßig oder gewohnheitsmäßig begangen werden sowie der Straftaten, die im Zusammenhang mit den Erscheinungsformen der Organisierten Kriminalität und des internationalen Terro-

rismus stehen, ein besonderes Gewicht beigemessen. Voraussetzung ist jedoch, dass es sich um ausreichend gewichtige Straftaten handelt, die den Bereich der mittleren Kriminalität überschreiten oder zumindest an dessen Obergrenze liegen. Abzustellen ist dabei auf das jeweilige Grunddelikt sowie auf benannte besonders schwere Fälle in Form von Regelbeispielen, da andernfalls aus der ex-ante Sicht nicht erkennbar ist, ob ein minder schwerer oder ein besonders schwerer Fall im Sinn des Strafgesetzbuchs vorliegt. Bei Straftaten, die mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt sind, kann von einer besonderen Schwere ausgegangen werden. Soweit in Art. 30 Abs. 5 Satz 1 Delikte aufgenommen wurden, die diesen Strafrahmen unterschreiten, handelt es sich um Straftaten, die einen besonderen Bezug zur Organisierten Kriminalität aufweisen, so bei der Bildung krimineller Vereinigungen und dem Menschenhandel, oder bei denen bereits aufgrund der besonderen Schutzwürdigkeit sowie des hohen Ranges der geschützten Rechtsgüter eine Aufnahme in den Straftatenkatalog gerechtfertigt ist, so bei der Verbreitung von Kinderpornographie und der Vorbereitung eines Explosionsverbrechens. Bei der Gefahrenabwehr kann nicht das Strafmaß allein ausschlaggebend sein, da es wesentlich von den Tatfolgen bestimmt wird. Vielmehr sind die Gefahren, die für die öffentliche Sicherheit und Ordnung von den jeweiligen Straftaten ausgehen, maßgeblicher Gesichtspunkt in der Abwägung. Ziel ist gerade die Verhinderung schwerer Folgen. Das Bundesverfassungsgericht hat dementsprechend dargelegt, dass sich die Schwere einer Straftat grundsätzlich nur auf begangene Taten beziehen kann, nicht auf erst zukünftig zu erwartende (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 235).

Bei den schwerwiegenden Straftaten handelt es sich um Delikte, deren Bekämpfung im jeweiligen Einzelfall den Einsatz besonderer Ermittlungsbefugnisse erforderlich machen kann. Rechtstatsächliche Untersuchungen belegen, dass die Maßnahmen der Telekommunikationsüberwachung, aber auch der Wohnraumüberwachung, zur Abwehr unterschiedlicher Deliktsgruppen zum Einsatz kommen, wenn auch zum Teil in geringer Anzahl. Im Bereich des Sicherheitsrechts spielt der Grundsatz der effektiven Gefahrenabwehr eine besondere Rolle. Die Behörden müssen über die notwendigen Befugnisnormen verfügen, um Gefahren für bedeutsame Rechtsgüter auch bei nach außen stark abgeschotteten kriminellen Organisationsstrukturen bzw. bei konspirativer Begehungsweise im Einzelfall effektiv abwehren zu können.

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 gegeben sind.

Die bisherige Regelung über die Straftaten von erheblicher Bedeutung in Art. 30 Abs. 5 PAG wird zu Satz 2. Die Änderungen, die auch die Neufassung einzelner Straftatbestände sowie das Inkrafttreten des Zuwanderungsgesetzes berücksichtigen, sind lediglich redaktioneller Art. Die schwerwiegenden Straftaten nach Satz 1 sind ausnahmslos auch Straftaten von erheblicher Bedeutung.

Zu § 1 Nr. 2 (Art. 33 Abs. 2 Sätze 2 und 3)

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 Selbstbestimmung 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. Die neu geschaffenen Sätze 2 und 3 des Absatzes 2 gestatten 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 darüber hinaus die Speicherung der gewonnenen Daten und deren Abgleich mit anderen Datenbeständen. Den anlass- und verdachtsunabhängigen Abgleich mit beliebigen

Dateien ermöglicht die Vorschrift jedoch gleichwohl nicht. Generell zulässig ist der Abgleich nach der Neuregelung vielmehr nur mit dem Fahndungsbestand (Absatz 2 Satz 2). Ein darüber hinaus gehender Abgleich mit anderen polizeilichen Dateien kommt demgegenüber lediglich dann in Betracht, wenn die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehenden Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist (Absatz 2 Satz 3).

Voraussetzung ist also zunächst eine bestimmte Qualität der Dateien, die zur Abwehr konkreter oder solcher abstrakter Gefahren, die im Hinblick auf bestimmte Ereignisse bestehen, errichtet worden sein müssen. Ersteres wäre beispielsweise der Fall, wenn eine Datei speziell zur Bekämpfung einer konkreten Serie von Brandstiftungen angelegt wurde, letzteres trifft etwa auf die Datei „Gewalttäter Sport“ zu, die zur Abwehr abstrakter wie konkreter Gefahren im Zusammenhang mit bestimmten Sportereignissen errichtet wurde. Hier ermöglicht die Neuregelung den Kennzeichenabgleich schon im Vorfeld konkreter Gefahren, z. B. auf den Zubringerautobahnen zu einem Fußballstadion. Dagegen scheidet ein Abgleich der Kennzeichen mit Dateien der Vorgangsverwaltung oder dem Kriminalaktennachweis aus, da diesen Dateien der nötige Bezug zu bestimmten Ereignissen fehlt.

Darüber hinaus ist der Abgleich mit Dateien in dem genannten Sinn aber nur dann zulässig, wenn er zur Abwehr einer dem Errichtungszweck der Datei entsprechenden Gefahr erforderlich ist. Dies bedeutet zum Beispiel, dass der Abgleich mit der Datei „Gewalttäter Sport“ nicht generell, sondern nur im Zusammenhang mit einem Fußballspiel erfolgen darf, bei dem auch mit der Anreise von so genannten Hooligans zu rechnen ist.

Die über die Regelung der Datenerhebung und des Datenabgleichs 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 sie in der abgeglichenen Datei enthalten sind und 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 umfängliche 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. Die Befugnisnorm des Art. 34 PAG wird an die Vorgaben des Urteils des Bundesverfassungsgerichts zur repressiven Wohnraumüberwachung vom 03.03.2004 (Az.: 1 BvR 2378/98, 1 BvR 1084/99) und des Beschlusses zur 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 3.3.2004, 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). Gleichwohl ist eine fortlaufende Prüfung durch den Gesetzgeber erforderlich, die weiterhin 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 bisherige Regelung in Art. 34 Abs. 1 Satz 1 Nr. 1 über die nicht verantwortlichen Personen gemäß Art. 10 PAG entfällt. Maßnahmen gegen diesen Personenkreis können im Interesse des verstärkten Schutzes von Berufsgeheimnisträgern, aber auch von anderen Unbeteiligten, künftig nur unter den Voraussetzungen des Absatzes 3 gerichtet werden.

      Durch die Einschränkung der Gesundheitsgefahren auf die Gefahr für Leib und Leben wird klargestellt, dass nicht jede einfache Körperverletzung die Voraussetzungen für eine Wohnraumüberwachung eröffnen kann. Die Sachgefahr wird dahingehend konkretisiert, dass nur gemeine Gefahren erfasst werden. Das Bundesverfassungsgericht hat die Rechtsgüter der erheblichen Sach- und Vermögenswerte als ausreichend anerkannt, wenn das typische Gefahrenpotential einer gemeinen Gefahr im Sinn von Art. 13 Abs. 4 GG gegeben ist (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 345). Voraussetzung ist dafür, dass die Gefahr im Einzelfall für eine unbestimmte Vielzahl von Sachen droht, die einen erheblichen Wert haben.

      Dringende Gefahren im Sinn von Art. 13 Abs. 4 GG, die eine präventive Wohnraumüberwachung rechtfertigen, können nach Absatz 1 Satz 1 Nr. 2 auch bevorstehende schwerwiegende Straftaten sein. Der Gesetzgeber muss insbesondere dann, wenn wie im Waffen- oder im Betäubungsmittelrecht 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 ausreichendes Gewicht aufweisen. Daher wird auf die abschließend im Polizeiaufgabengesetz definierten schwerwiegenden Straftaten (Art. 30 Abs. 5 Satz 1) Bezug genommen, was eine erhebliche 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, der Schwere der drohenden Rechtsgutsverletzungen oder der banden-, gewohnheits- oder gewerbsmäßigen Begehungsweise 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 durchgehend angezeigt. Im Bereich des Rechtsgüterschutzes geht es nicht nur um die Ahndung von Unrecht, die sich im Wesentlichen am Strafrahmen orientiert, sondern um die Verhinderungen von Rechtsgutsbeeinträchtigungen. 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 konkrete Gefahr in Form der (drohenden) Begehung schwerwiegender Straftaten nach Absatz 1 Satz 1 Nr. 2 sind die Bestimmtheit der Tatsachen sowie die Begründetheit der Annahme, dass die Adressaten der Maßnahme die jeweiligen Taten begehen werden oder bereits begehen. 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 wahrscheinlich die Annahme sein muss, dass eine Straftat begangen wird, um den Eingriff zu rechtfertigen. Die Intensität des Grundrechtseingriffs (insbesondere die Schutzwürdigkeit 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 gesetzli-

che Einschränkungen und durch verfahrensrechtliche Sicherungen in Absatz 1 Satz 2 gewährleistet. Durch die Formulierung „wenn und soweit“ wird klargestellt, dass die Voraussetzungen bei Anordnung der Überwachungsmaßnahme nicht umfassend prognostiziert werden müssen, da insbesondere eine nach Ziffer 2 erforderliche Prognose, wer sich wann in den Räumlichkeiten aufhalten wird, in der Regel nicht möglich ist. Es handelt sich insofern um Anforderungen, die während der Durchführung zu beachten sind und nur soweit vorhersehbar bereits bei Maßnahmeanordnung vorliegen müssen.

- 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 aufgrund von Anhaltspunkten die Wahrscheinlichkeit dafür besteht, dass eine Verletzung des Kernbereichs erfolgt (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 135, 138f., 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 zu privaten Wohnzwecken genutzten Räumen 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 gegeben ist (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 138). Die Polizei hat durch geeignete Vorermittlungen oder durch parallelen Einsatz zusätzlicher Ermittlungsmaßnahmen Vorsorge zu tragen, dass in den konkreten Situationen keine unzulässigen Eingriffe erfolgen werden. Wer zu den engsten Vertrauten zählt, ist Frage des Einzelfalles. Grundsätzlich ist erforderlich, dass ein besonderes, den Kernbereich privater Lebensgestaltung betreffendes Vertrauensverhältnis besteht. Der Personenkreis, deren Gespräche zum Kernbereich privater Lebensgestaltung zu rechnen sind, stimmt nach Darlegung des Bundesverfassungsgerichts nicht mit dem Kreis der nach §§ 52, 53 und 53a StPO Zeugnisverweigerungsberechtigten überein (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 147f.). Der Kreis der besonderen Vertrauenspersonen ist einerseits enger, da nicht jedes Zeugnisverweigerungsrecht dem Kernbereichsschutz dient, andererseits aber weiter, da auch engste persönliche Freundschaften erfasst werden.

- Die Regelung in Satz 2 Nr. 2 schützt neben engsten Vertrauten und Familienangehörigen auch Berufsgeheimnisträger nach § 53 StPO sowie deren Hilfspersonen nach § 53a StPO; sie sind aufgrund der Bedeutung der Vertrauensverhältnisse ebenfalls schutzwürdig und werden daher vom Abhörverbot umfasst. Dadurch wird der Schutz vertrauenswürdiger Gespräche, die mit einem Berufsgeheimnisträger bzw. mit deren Hilfspersonen in privaten Wohnräumen geführt werden, umfassend gewährleistet.

  Die Schutzwirkungen greifen allerdings dann nicht ein, wenn Gespräche nach ihrem Inhalt die Begehung schwerwiegender Straftaten oder die Verursachung der in 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 richtet (Satz 2 Nr. 2 Buchst. b). Die Begehung von schwerwiegenden Straftaten und die Verursachung anderer Gefahren für gewichtige Rechtsgüter sind nicht schutzwürdig. Zu diesen Fallgruppen zählen auch Geiselnahmen durch engste Familienmitglieder, die den Einsatz der Wohnraumüberwachung erforderlich machen können.

  Eine Ausnahme von dem Grundsatz, dass Gespräche mit unmittelbarem Bezug zu Straftaten oder Gefahren im Sinn des Satzes 1 nicht schutzbedürftig sind, wird lediglich für die Gruppen von Berufsgeheimnisträgern gemacht, die aufgrund ihrer besonderen beruflichen Stellung selbst in derartigen Situationen gesetzlichen Schutz genießen (Satz 2 Nr. 2 Buchst. a). Dies ist der Fall, wenn ein gesprächstypischer Bezug zwischen den Gesprächen über mögliche Gefahren und ihrer Funktion als Berufsgeheimnisträger besteht. Das Zeugnisverweigerungsrecht nach § 53 StPO ist bei diesen Personen zugleich Ausdruck einer verfassungsrechtlichen Position, die einem Eingriff in das Vertrauensverhältnis entgegensteht, soweit es sich um Gespräche in einer besonders geschützten Umgebung handelt. Neben Geistlichen und Anwälten, denen sich der Adressat etwa im Zusammenhang mit bereits begangenen Straftaten anvertrauen kann, sind zu dieser Gruppe die Ärzte, Psychotherapeuten und Suchtberater zu rechnen. Der besondere Schutz greift aber nur soweit das Zeugnisverweigerungsrecht reicht. Ist der Berufsgeheimnisträger dagegen selbst an der Gefahrverursachung beteiligt, entfallen daher die Schutzwirkungen.

- Der Schutz wird in Satz 2 Nr. 3 auf Räumlichkeiten von Berufsgeheimnisträgern ausgedehnt, die zu deren Berufsausübung bestimmt sind. Zwar weisen Betriebs- und Geschäftsräume grundsätzlich eine geringere Schutzwürdigkeit auf, da sie typischerweise durch einen Sozialbezug geprägt sind. 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.). Dabei erfolgt keine Differenzierung zwischen den in § 53 StPO genannten Berufsgruppen, so dass auch Räume von Journalisten und Abgeordneten besonderen Schutz genießen. Wenn allerdings Hinweise dafür bestehen, dass der Berufsgeheimnisträger als Gefahrverursacher mit Dritten Gespräche führt, die nach ihrem Inhalt die Begehung schwerwiegender Straftaten oder die Verursachung der in Satz 1 Nr. 1 genannten Gefahren zum Gegenstand haben, besteht keine Schutzwürdigkeit des Vertrauensverhältnisses. Es gelten dann die Voraussetzungen der Nr. 2, Buchst. a), so dass Gespräche, die mit unbeteiligten Dritten geführt werden und die Gefahr nicht betreffen, ausgenommen sind.

b) Absatz 2 trifft Regelungen über die Art und Weise der Durchführung und die Unterbrechungspflicht. Wie vom Bundesverfassungsgericht in seiner Entscheidung vom 03.03.2004 (Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 151 f.) für die repressive Wohnraumüberwachung klargestellt, kann es der Grundrechtsschutz bei dem Abhören von Gesprächen aus einer Privatwohnung erforderlich machen, auf eine nur automatische Aufzeichnung der Gespräche zu verzichten, um die Maßnahme jederzeit unterbrechen zu können. Dieser Grundsatz ist auf die präventive Überwachung übertragbar. Daher werden durch den ersten Halbsatz die zu privaten Wohnzwecken genutzten Räumlichkeiten sowie die Räume der Berufsgeheimnisträger im Sinn der §§ 53, 53a StPO besonders geschützt. Eine automatisierte Aufzeichnung ist nur ausnahmsweise zulässig. Wenn keine hinreichenden äußeren Anzeichen für eine Kernbereichsverletzung vorliegen, so dass die Datenerhebung zulässig ist, und soweit die im ersten Halbsatz dargelegten Anforderungen beachtet werden, ist aus verfassungsrechtlicher Sicht eine Bewertung des Gesprächsinhalts im Rahmen einer ersten Sichtung dagegen nicht zu beanstanden (vgl. BVerfG vom 3.3.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, a.a.O.).

Im zweiten Halbsatz wird die Unterbrechung der Maßnahme angeordnet, wenn bei einer Wohnraumüberwachung erkennbar wird, dass es zu einem Kernbereichseingriff 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. 152). Das Verwendungsverbot und die Löschungspflicht für dennoch erfolgte Aufzeichnungen ergeben sich aus Absatz 5 bzw. aus Absatz 7. Die Dauer der Unterbrechung und die Zulässigkeit des erneuten Abhörens richten sich nach den Umständen des jeweiligen Einzelfalles. Nach einer Unterbrechung ist ein erneutes Abhören wieder zulässig, wenn anzunehmen ist, dass die Kernbereichssituation nicht mehr besteht. Aus Gründen des Grundrechtsschutzes kann ein „Hineinhören“ in die jeweilige Situation angebracht sein, wobei ohne Aufzeichnung zunächst die Gesprächssituation ermittelt wird. Stellt sich dabei heraus, dass entgegen der ursprünglichen Prognose immer noch Gespräche geführt werden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, ist eine neuerliche Unterbrechung erforderlich.

c) Die Regelung in Absatz 3 stellt klar, dass die Wohnraumüberwachung grundsätzlich nur in Wohnungen des Adressaten im Sinn von Absatz 1 Satz 1 Nrn. 1 und 2 durchgeführt werden darf. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn und solange anzunehmen ist, dass sich der Adressat dort aufhält (Satz 2 Nr. 1), und wenn Maßnahmen in seiner Wohnung nicht zur Gefahrenabwehr im Sinn des Absatz 1 Satz 1 ausreichen bzw. nicht möglich sind (Satz 2 Nr. 2). Zu diesen Fällen zählt auch die Ungeeignetheit von Maßnahmen in Wohnungen des Adressaten zur Abwehr der Gefahr. So dürfen bei einer Geiselnahme in Geschäftsräumen diese Räumlichkeiten zum Zweck der Gefahrenabwehr abgehört werden, ohne dass zuvor die Wohnung des Geiselnehmers überwacht werden müsste. Berufsgeheimnisträger werden in Satz 2 ausdrücklich ausgenommen, so dass in deren Räumen eine Überwachung nur dann zulässig ist, wenn sie selbst die Gefahren verursachen.

Satz 3 stellt klar, dass auch Dritte von der Maßnahme betroffen sein können, die nicht Adressat sind, wenn dies unvermeidbar ist.

d) Entsprechend der grundgesetzlichen Vorgaben in Art. 13 Abs. 4 GG wird die Maßnahme – wie nach bisheriger Rechtslage – durch einen Einzelrichter angeordnet (Absatz 4 Satz 1). 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.). Örtlich zuständig ist künftig das Amtsgericht des Behördensitzes, um bei Maßnahmen, die in verschiedenen Wohnungen durchgeführt werden, eine einheitliche Beschlussfassung zu gewährleisten und die gerichtliche Überwachung zu konzentrieren. In Eilfällen kann die Anordnung durch den Dienststellenleiter erfolgen; die gerichtliche Bestätigung ist entsprechend der grundgesetzlichen Vorgaben unverzüglich nachzuholen (Art. 13 Abs. 4 Satz 2 GG). Das Schriftlichkeitsgebot und die inhaltlichen Anforderungen an die Entscheidung gemäß Satz 3 dienen der Einhaltung der verfassungsrechtlichen Erfordernisse. Die Angaben zur Art der Maßnahme umfassen dabei insbesondere die Frage der automatisierten Aufzeichnung. Der Richter hat bei seiner Entscheidung die Vorgaben des Bundesverfassungsgerichts zu Aufgaben und Pflichten bei der gerichtlichen Prüfung zu beachten (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 275). Die Begrenzung auf einen Monat gewährleistet die regelmäßige gerichtliche Überprüfung 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.

e) In Absatz 5 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 anderen Zwecken, wie etwa der Strafverfolgung, stellt einen eigenen Grundrechtseingriff dar (vgl. 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. Ihre Zulässigkeit richtet sich nach den Maßgaben der Strafprozessordnung über die Verwendung von Daten, die im Rahmen einer präventiven Wohnraumüberwachung erhoben wurden (Satz 2 Nr. 2). Zwischen der Frage, ob eine Zweckänderung erfolgen darf und ob eine Verwendung 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 Verwendung sollen aber nach Absatz 5 Satz 2 Nr. 2 gleichlaufend sein.

Satz 3 regelt in Ergänzung zu den Erhebungsverboten die Verwendungsverbote. 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 den Kernbereich privater Lebensgestaltung vorliegt, unterliegen die Daten einem Verwendungsverbot und sind zu löschen.

Dementsprechend sieht Satz 3 Verwendungsverbote vor für Fälle, in denen sich nachträglich herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben (Nr. 1) bzw. dass die Daten aus einem nach Absatz 1 Satz 2 Nr. 2 a) besonders geschützten Vertrauensverhältnis zu Berufsgeheimnisträgern stammen (Nr. 2). Durch die Regelung in Ziffer 2 werden Gespräche mit den dort genannten Personen selbst dann geschützt, wenn sie einen unmittelbaren Bezug zu den Gefahren oder Straftaten nach Absatz 1 Satz 1 haben, soweit das Recht zur Zeugnisverweigerung reicht. Diese Schutzwirkungen enden allerdings, wenn ein Berufsgeheimnisträger selbst an der Verursachung der Gefahr beteiligt ist.

Schließlich dürfen auch Daten, die dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis zu sonstigen Berufsgeheimnisträgern zuzurechnen sind und keinen unmittelbaren Gefahrbezug haben, nicht verwendet werden (Nr. 3). Daten, die einen unmittelbaren Bezug zu Gefahren haben, sind grundsätzlich dem Sozialbereich zuzurechnen, so dass insofern nur eine Klarstellung erfolgt. Über die Erfordernisse des Kernbereichsschutzes hinaus werden auch Vertrauensverhältnisse zu Journalisten und anderen als den in Ziffer 2 genannten Gruppen von Berufsgeheimnisträgern, die nicht zu den engsten Vertrauten zählen, geschützt. Solange diese Gespräche keinen Gefahrbezug aufweisen, ist der Schutz durch die Vertrauensstellung gerechtfertigt. Sicherheitslücken sind nicht zu befürchten.

Im Bereich der Gefahrenabwehr ergeben sich allerdings Ausnahmen von den dargelegten Verwendungsverboten, 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 gegenüberstehen und in denen die Kollision nicht aufgelöst werden kann. Zu denken ist etwa an den Fall, dass bei der Auswertung eine Information gewonnen wird, die der Vereitelung eines unmittelbar drohenden terroristischen 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 Verwendungsverbote 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 umfassende richterliche Kontrolle nach Satz 4 gewährleistet. Bei Gefahr im Verzug kann die Entscheidung ausnahmsweise durch einen Dienststellenleiter getroffen werden. Die richterliche Entscheidung über die Zulässigkeit der Verwendung ist unverzüglich nachzuholen.

f) Absatz 6 hat die Benachrichtigungspflichten zum Gegenstand. 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 (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 290). Satz 1 regelt diese Unterrichtungspflicht. Zu den Betroffenen zählen neben den Adressaten und den Wohnungsinhabern grundsätzlich alle abgehörten Personen. Für die Inanspruchnahme gerichtlichen Rechtsschutzes gelten 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 30.4.1997, 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 selbst 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). Die bloße Gefährdung des künftigen Einsatzes nicht offen ermittelnder Beamter vermag die Zurückstellung dagegen nicht mehr zu rechtfertigen (vgl. BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 302). In Fällen, in denen die Daten zu Strafverfolgungszwecken 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 der Grundrechtseingriff bei der Zielperson oder bei dem zu benachrichtigenden Beteiligten vertieft würde (Nr. 1) oder wenn die Identitätsfeststellung bzw. die Ermittlung des Aufenthaltsortes nur unter unverhältnismäßigem Aufwand möglich ist (Nr. 2). Darin sind hinreichend gewichtige Gesichtspunkte zu sehen, die unter Beachtung der verfassungsrechtlichen Anforderungen eine Ausnahme rechtfertigen können (vgl. BVerfG vom 3.3.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 297).

g) Absatz 7 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 3.3.2004, 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 „ernsthaftes – grundsätzlich zu vermutendes – Interesse am Rechtsschutz oder an der Geltendmachung seines Datenschutzrechts“ haben kann, die Daten nicht gelöscht, sondern nur gesperrt werden (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 350). Die Sperrung hat zur Folge, dass die Daten zu keinem anderen Zweck als dem zur Information des Betroffenen verwendet werden dürfen und erst nachdem sichergestellt ist, dass sie für eine Überprüfung nicht mehr benötigt werden, zu löschen sind. Die Monatsfrist nach Satz 3 dient dem Betroffenen als Entscheidungsfrist darüber, ob er einen förmlichen oder einen sonstigen Rechtsbehelf einlegen 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.

   Daten, die aus dem Kernbereich privater Lebensgestaltung stammen und für die nach Absatz 5 Satz 3 ein Verwendungsverbot 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.

h) Absatz 8 hat den im bisherigen Absatz 3 geregelten Einsatz technischer Mittel zum Schutz verdeckter Ermittler zum Gegenstand. Diese Maßnahme 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 (Satz 5).

   Soweit dennoch eine Verwendung der Daten erfolgen soll, ist wie nach bisheriger Rechtslage eine richterliche Entscheidung über die Rechtmäßigkeit der Maßnahme erforderlich. Neu aufgenommen wurde Satz 4, der bei Verwendung der durch die technischen Mittel aufgezeichneten Daten auf die Verwendungsregelungen sowie die Löschungs- und Benachrichtigungspflichten in den Absätzen 5 bis 7 verweist.

i) Der bisherige Absatz 6, der die Unterrichtungspflicht des Landtages zum Gegenstand hat, wird zu Absatz 9. Es ergeben sich lediglich redaktionelle Änderungen.

j) Als Folge der neuen Befugnisse zur Telekommunikationsüberwachung in Art. 34a bis 34c wird die Klarstellung über den Umfang der Eingriffsbefugnis in Absatz 10 neu gefasst. In der bisherigen Fassung des Art. 34 Abs. 7 wurde klargestellt, dass das Vorliegen der Voraussetzungen, die zum Einsatz technischer Mittel in Wohnungen nach Art. 34 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 Polizeiaufgabengesetz 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, Übermittelns und Empfangens von Signalen 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. 22 und 23 TKG).

   a) Art. 34a Abs. 1 regelt die Erhebung personenbezogener Daten durch Überwachung und Aufzeichnung der Telekommunikation. Umfasst sind neben den Verkehrsdaten auch die Inhaltsdaten der Kommunikation. Adressaten der Maßnahme sind nach Satz 1 Nr. 1 die nach Art. 7 und 8 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 Leib, Leben 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 über entsprechende Befugnisse verfügt, folgt bereits aus der Generalklausel des Art. 11 Abs. 2 Satz 1 Nr. 1 Alt. 3. Darunter sind gem. Art. 11 Abs. 2 Satz 4 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. In Art. 34a Abs. 1 Satz 1 Nr. 1 werden einschränkend nur konkrete Gefahren für die Sicherheit oder den Bestand des Bundes oder eines Landes erfasst.

      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 wird. 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 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 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 wird, 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 oder ihnen ihre Kommunikationseinrichtungen zur Verfügung stellen, 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 besteht, 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 werden. Berufsgeheimnisträger sind in Buchst. b) besonders geschützt, soweit sie ein Recht zur Zeugnisverweigerung nach §§ 53, 53a StPO haben. Insoweit ist eine Überwachung unzulässig. Dies gilt jedoch nicht, wenn die entgegengenommenen Mitteilungen, die die Gefahrverursachung betreffen müssen, von ihnen weitergeleitet werden, sie also als Boten tätig sind, oder wenn die genannten Adressaten ihre Kommunikationseinrichtungen benutzen. Davon unberührt bleiben jedoch insbesondere die Verwendungsverbote.

Andere Personen als die in Nrn. 1 und 2 genannten können nach Absatz 1 dagegen 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, die den schwereren Grundrechtseingriff darstellt, subsidiär.

In Satz 3 wird ein Erhebungsverbot für Gespräche mit Berufsgeheimnisträgern angeordnet. Ein besonderer Schutz dieser Personengruppe wird angesichts der Vertrauensbeziehungen zu Ärzten, Apothekern, Anwälten, Geistlichen, Journalisten und anderen in § 53 StPO aufgezählten Berufsgruppen gewährt. Ausnahmen von der Unzulässigkeit der Datenerhebung sind in Fällen, in denen der Berufsgeheimnisträger selbst Adressat der Maßnahme ist, und bei der Abwehr gegenwärtiger Gefahren für Leib, Leben und Freiheit gerechtfertigt. Über die Regelung des Satzes 3 hinaus werden zum Schutz von Berufsgeheimnisträgern in Art. 34c Abs. 4 Verwendungsverbote und in Art. 34c Abs. 6 Löschenspflichten vorgesehen. Der Vorbehalt der Erkennbarkeit schließt Fälle aus, in denen erst bei Auswertung der Aufzeichnungen erkannt wird, dass ein Gespräch mit einem Berufsgeheimnisträger vorliegt. Welche Maßnahmen zu treffen sind, um die Erkennbarkeit sicherzustellen, richtet sich nach den Umständen des Einzelfalles. Ein live–Mithören wird in der Regel schon aus Gründen der Praktikabilität nicht möglich sein.

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 „verfassungsrechtlichen 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 Fernsprechnetz (eines Unternehmens) als Medium für die Fernkommunikation. 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 unmittelbare 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 (BVerfG vom 03.03.2004, Az.: 1 BvR 2378/98, 1 BvR 1084/99, Rn. 166), ist in diesem Zusammenhang einschlägig.

Ein Erhebungsverbot zum Schutz besonderer Vertrauensverhältnisse, die nicht auf einem Berufsgeheimnis beruhen, ist nicht vorgesehen. Eine Prognose, mit wem ein Telefongespräch zustande kommt und in welchem Verhältnis beide Gesprächspartner zueinander stehen, kann in der Regel gar nicht angestellt werden, angesichts der Häufigkeit und Vielgestaltigkeit von Telekommunikationsvorgängen. Vielfach lässt sich ohne weitere Auswertung nicht einmal feststellen, 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 Sinn 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, weil er die Voraussetzungen für eine Überwachung ebenfalls erfüllt.

Bei Vertrauensbeziehungen, die nicht auf einem Berufsgeheimnis beruhen, ist daher 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 Verwendungsverbote bzw. die Löschungspflichten in Art. 34c Abs. 4 und 6 gewährleistet.

b) Im Unterschied zur Überwachung und Aufzeichnung von Telekommunikationsdaten einschließlich der Telekommunikationsinhalte gewährt Absatz 2 die Befugnis zum Einsatz von technischen Mitteln 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 Kennungen oftmals über einen Provider nicht ermittelt werden können. Nachdem die Angabe der Rufnummer oder einer anderen Kennung aber Zulässigkeitsvoraussetzung für eine Anordnung der Telekommunikationsüberwachung 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 Kartennummer von Mobiltelefonen bzw. des Standortes von Mobilfunkendgeräten dienen (Absatz 2 Satz 1 Nr. 1), wird an die strengen Voraussetzungen des Art. 34a 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 Abwehr schwerwiegender Straftaten und zum Schutz der in Art. 34a Abs. 1 Satz 1 Nr. 1 genannten Rechtsgüter ebenfalls unverzichtbar. Erfasst wird auch die Aussendung von funktechnischen Signalen, um die Standortkennung eines Endgerätes zu erhalten. 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, sind diese unverzüglich zu löschen. Die Beeinträchtigungen für die Diensteanbieter sind aufgrund der technischen Fortschritte im Bereich der Überwachungsgeräte gering und daher zumutbar.

c) Die Suche nach vermissten oder hilflosen Personen, die sich in einer konkreten Gefahrenlage befinden, 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, dass sie zur Abwehr einer Gefahr für Leben oder Gesundheit der jeweils betroffenen Person erforderlich ist. Für den Einsatz technischer Geräte zur Ortung von Mobiltelefonen, die Vermisste bei sich tragen, bzw. für die Datenerhebung 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. Satz 2 stellt klar, dass die Mitwirkungspflichten der Diensteanbieter auch in den Fällen des Absatzes 3 bestehen und dass auf der Grundlage dieser Regelungen weitergehende Maßnahmen getroffen werden können, wenn die dort genannten Voraussetzungen gegeben sind.

d) In Anbetracht der Tatsache, dass die modernen Kommunikationstechniken gerade von terroristischen Netzwerken zur Begehung von Anschlägen genutzt werden, müssen der Polizei zur Abwehr 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. Die Sicherheitsbehörden können durch den Einsatz technischer Mittel, wie etwa des sog. „IMSI-Catchers“, die Telekommunikation der in Absatz 1 Satz 1 genannten Personen unterbrechen. Nicht erfasst sind dagegen Annordnungen gegenüber Diensteanbietern zur Unterbrechung des Telekommunikationsverkehrs. 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 Geiselnehmers mit Komplizen außerhalb des Tatorts über die Mobiltelefone Dritter unterbinden zu können. Voraussetzung ist eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person, die nicht anders abwendbar ist.

2. Die Mitwirkungspflichten der Diensteanbieter werden in Art. 34b geregelt. Diensteanbieter ist, wer ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder daran – auch als Vertriebspartner – mitwirkt (vgl. § 3 Nr. 6 TKG). 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, bei ihnen vorhandene oder künftig anfallende Telekommunikationsverkehrsdaten bzw. Daten über Kennungen, soweit diese vorliegen, zur Verfügung zu stellen. Absatz 3 enthält eine Aufzählung der bereitzustellenden Telekommunikationsverkehrsdaten, Absatz 4 eine Regelung für die Entschädigungspflicht.

a) Die Mitwirkungspflichten der Diensteanbieter bei der Telekommunikationsüberwachung sind angesichts der technischen Gegebenheiten unverzichtbar für die Durchführung der Maßnahmen. Dies gilt in besonderem Maß bei Festnetz-Telefonanschlüssen. Daher verpflichtet Absatz 1 die Diensteanbieter, der Polizei die Überwachung und Aufzeichnung der Telekommunikation nach Art. 34a 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 im für die technische Umsetzung von Telekommunikationsüberwachungsmaßnahmen maßgeblichen TKG festgeschrieben ist. In § 110 Abs. 1 Satz 6 TKG wird ausweislich der Begründung klargestellt, dass die landesgesetzlichen Regelungen zur präventiv-polizeilichen Telekommunikationsüberwachung nicht durch die Vorschrift des § 110 TKG eingeschränkt werden (BR-Drs. 755/03, S. 126). Daher ergeben sich keine kompetenzrechtlichen Bedenken gegen die Normierung landesgesetzlicher Verpflichtungen.

b) Ergänzend regelt Absatz 2 die Übermittlung der Telekommunikationsverkehrsdaten. 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, wenn eine konkrete Gefahr besteht. Die bisherige Praxis, die Befugnis zur Verpflichtung, entsprechende Daten zu übermitteln, auf den Rechtsgedanken des übergesetzlichen Notstandes (§ 34 StGB) zu stützen, wird von den Diensteanbietern immer wieder 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 Verkehrsdaten (Nr. 1) sowie die spezifischen Kennungen, die zur Ermittlung des Gerätestandortes erforderlich sind (Nr. 3), soweit sie bei den Diensteanbietern vorliegen. In Satz 1 Nr. 2 wird klargestellt, dass ebenso wie im Bereich der Strafverfolgung die Anordnung möglich ist, Auskunft über zukünftige Verkehrsdaten zu erteilen. Die Übermittlungspflicht betrifft die Daten der in Art. 34a Abs. 1 Satz 1 bzw. in Abs. 3 Satz 1 genannten Personen.

Nur soweit die Erforschung des Sachverhalts bzw. die Ermittlung des Aufenthaltsortes und damit die Abwehr der Gefahren bzw. der schwerwiegenden Straftaten auf andere Weise aussichtslos oder wesentlich erschwert ist, darf nach Satz 1 Nr. 1 i.V.m. Satz 2 die Übermittlung der im Wege eines Zielsuchlaufs gewonnenen Daten angeordnet werden. Satz 3 stellt die Unverzüglichkeit der Übermittlungspflicht für Daten nach Satz 1 und 2 klar.

c) Absatz 3 enthält eine Legaldefinition der Telekommunikationsverkehrsdaten, die von der Übermittlungspflicht erfasst werden. Da die technische Entwicklung noch weiter fortschreitet und möglicherweise derzeit verwendete Kennungen künftig durch andere den Diensteanbietern vorliegende Merkmale ersetzt werden, kann eine abschließende Aufzählung der Daten nicht erfolgen.

Die Einbeziehung der Verkehrsdaten, 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.

d) Zur Klarstellung der Entschädigungspflicht gegenüber den betroffenen Diensteanbietern verweist Absatz 4 auf die bundesrechtlichen Regelungen. Solange die Rechtsverordnung nach § 110 Abs. 9 TKG noch nicht erlassen wurde, richtet sich die Entschädigung nach § 23 des Justizvergütungs- und -entschädigungsgesetzes.

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 Verwendungsverbote, die Kennzeichnungs- und die Benachrichtigungspflicht sowie das Löschungsgebot 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 ausdrücklich 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. 4 – eine Anordnung durch hochrangige Dienststellenleiter (sog. Behördenleitervorbehalt) ausreichend. Es bedarf dann einer unverzüglichen Bestätigung der Entscheidung durch den Richter.

   b) In Absatz 2 wird eine entsprechende Regelung für die Fälle des Art. 34a Abs. 3 und die dafür erforderlichen Maßnahmen gegenüber den Diensteanbietern 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 Beweiswirkung eine Warnfunktion.

   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 Leib, Leben 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 durch unbekannte Täter zu denken, die dazu dient, die Kommunikation mit deren 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 sind in der Anordnung in jedem Fall genau zu bestimmen.

   Die zulässige Anordnungsdauer orientiert sich an der Regelung für die Wohnraumüberwachung. Durch die Monatsfrist wird eine effektive gerichtliche Kontrolle gewährleistet. Die Fristen für die Telekommunikationsunterbrechung und -verhinderung nach Art. 34a Abs. 4 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 Verwendung zur Strafverfolgung richtet sich die Zulässigkeit danach, ob die Daten zur Verfolgung von Straftaten nach § 100a Satz 1 StPO erforderlich sind.

   Das Verwendungsverbot in Satz 3 erfasst Datenerhebungen, bei denen sich nach Auswertung herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben (Nr. 1), sie Inhalte betreffen, über die das Zeugnis als Angehöriger der genannten Berufsgruppen verweigert werden kann (Nr. 2), oder dass sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis zu einem Berufsgeheimnisträger zuzuordnen sind und keinen unmittelbaren Bezug zu den in Art. 34a Abs. 1 Satz 1 Nrn. 1 und 2 Buchst. a) genannten Gefahren oder Straften haben (Nr. 3).

   Eine Verwertung ist entsprechend der Regelung in Art. 34 Abs. 5 Satz 3 allerdings ausnahmsweise zulässig, wenn dies zum Schutz hochwertigster Rechtsgüter vor gegenwärtigen Gefahren erforderlich ist (Satz 4). In derartigen Fällen ist unverzüglich eine richterliche Entscheidung über die Verwendung nachzuholen.

   e) Die Benachrichtigungspflicht (Absatz 5) 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. 6 dargelegten Grundsätze entsprechend.

f) Die Löschung von Daten, bei denen sich nach Auswertung ergibt, dass sie aus dem Kernbereich privater Lebensgestaltung stammen und dass für sie ein Verwendungsverbot besteht, ist in Absatz 6 Satz 1 geregelt. Die unverzügliche Löschenspflicht dient ebenso wie bei der Wohnraumüberwachung dem Schutz vor einer weiteren Vertiefung des Grundrechtseingriffs. Im Übrigen gelten dieselben Grundsätze wie bei Art. 34 Abs. 7.

Zu § 1 Nr. 5 (Art. 36 Abs. 1 Nr. 2)

Es handelt sich um eine redaktionelle Folgeänderung zu § 1 Nr. 1. Die bisherige Rechtslage bleibt unverändert.

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 Sätze 2 und 3 erfassten Kennzeichen – nach Durchführung des Datenabgleichs – grundsätzlich unverzüglich wieder zu löschen sind. Etwas anderes gilt nur dann, wenn sie in der abgeglichenen Datei enthalten sind und 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 Sätze 2 und 3 lediglich routinemäßigen Einsatzes automatisierter Kennzeichenerkennungssysteme nur dann eingreifen, wenn zunächst die in Absatz 3 Satz 2 im Einzelnen genannten „Hürden“ übersprungen werden können. Der Abgleich muss also untechnisch gesprochen zunächst einmal einen „Treffer“ ergeben haben und es muss für den jeweiligen Einzelfall belegbar sein, dass die Speicherung, Veränderung oder Nutzung des nach Art. 33 Abs. 2 Sätze 2 und 3 erfassten und abgeglichenen Kennzeichens 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 und 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 zeitlich befristeten Dokumentation, zur Vorgangsverwaltung oder zur vorbeugenden Bekämpfung von Straftaten in Betracht. Unberührt bleiben hier freilich auch spezielle, Absatz 1 verdrängende Regelungen über die Datennutzung, insbesondere die Zulässigkeit weiterer Datenabgleiche nach Art. 43. In allen anderen Fällen sind die erhobenen und abgeglichenen Kennzeichen unverzüglich wieder zu löschen.

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 geschaffener 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 stattdessen 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 Landesstraf- 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 verwahrlosten 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 Wortsinn 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 Empfängers) 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 nichtinnerstaatliche 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 zur bisherigen Nummer 1 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 Poli-

zei 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 verhältnismäßig 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 mittels 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 des Gesetzentwurfs.

Zu § 3 (In-Kraft-Treten):

Die Vorschrift regelt das In-Kraft-Treten.