

GESETZENTWURF

der Fraktionen der SPD und Linkspartei.PDS

Entwurf eines Vierten Gesetzes zur Änderung des Sicherheits- und Ordnungsgesetzes

1. Problem

Das Bundesverfassungsgericht hat mit seinem Urteil vom 3. März 2004 (Az.: 1BvR 2378/98) Grundsätze für akustische Wohnraumüberwachungsmaßnahmen aufgestellt, die im Rahmen der Strafverfolgung durchgeführt werden. Für diese Maßnahmen ist Artikel 13 Abs. 3 Grundgesetz (GG) maßgeblich. Die Regelungen der Strafprozessordnung (StPO), die die Grundgesetzänderung einfachgesetzlich umsetzen, wurden teilweise für verfassungswidrig erklärt. Zwar hat das Bundesverfassungsgericht unmittelbar nur über die Verfassungsmäßigkeit der Bestimmungen der §§ 100c ff. StPO entschieden, dennoch ergibt sich aus der Urteilsbegründung auch gesetzlicher Änderungsbedarf hinsichtlich der Ausgestaltung der präventiven Wohnraumüberwachung im SOG M-V.

Auch zwingen die allgemeine Internationalisierung der Personen-, Waren-, Dienstleistungs- und Finanzströme, die zunehmende grenzüberschreitende Kriminalität sowie die fortschreitende europäische Integration und die Bedrohungen durch den internationalen Terrorismus dazu, das polizeiliche Handeln immer effizienter zu gestalten. Das gilt insbesondere für die Durchführung von Überwachungs- und Ermittlungsmaßnahmen.

2. Lösung

Um den Grundsätzen des Bundesverfassungsgerichts Rechnung zu tragen, erfolgt die Ergänzung der Regelungen zur Wohnraumüberwachung aus Gründen der Übersichtlichkeit in einem neu geschaffenen § 34b SOG M-V. Im Gefahrenabwehrbereich sichert die erarbeitete Befugnisnorm nunmehr den unantastbaren Kernbereich privater Lebensgestaltung und trifft spezielle Regelungen zur Verarbeitung und Nutzung der diesbezüglich erlangten Daten. Es wird darauf hingewiesen, dass die Entscheidung des Landesverfassungsgerichtes M-V vom 18. Mai 2000 zu § 33 Abs. 4 und 6 SOG M-V (polizeiliche Überwachung von Wohnungen und bei Datenerhebungen aus dem Bereich geschützter Vertrauensverhältnisse) bereits bei einer der letzten Gesetzesnovellen berücksichtigt worden ist und insoweit keine Änderungen vorzunehmen waren.

Spätestens mit den Terroranschlägen am 7. Juli 2005 in London ist ebenso eine Novellierung der Regelungen zur Videoüberwachung öffentlich zugänglicher Orte im SOG M-V dringend geboten. Die Handhabe der Bildaufzeichnung ist im Land Mecklenburg-Vorpommern im Vergleich zu anderen Länderregelungen nur in einem sehr eingeschränkten Umfang möglich. Unter Berücksichtigung der aktuellen Rechtsprechung zur Videoüberwachung öffentlich zugänglicher Orte (Urteil des VGH Mannheim vom 21. Juli 2003) und bereits bestehender Regelungen in anderen Bundesländern soll die Befugnisnorm zur Bildbeobachtung und Aufzeichnung neu gefasst werden. Mit der neu geschaffenen Regelung sind die Ordnungsbehörden und die Polizei zur Bildbeobachtung öffentlich zugänglicher Orte befugt, wenn dies zur Aufgabenerfüllung nach § 1 Abs. 1 SOG M-V erforderlich ist. Darüber hinaus ist die Bildaufzeichnung an öffentlich zugänglichen Orten möglich, an denen wiederholt Straftaten begangen worden sind (sog. Kriminalitätsschwerpunkte) und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist. Des Weiteren wird eine Rechtsgrundlage für Bild- und Tonaufzeichnungen an oder in so genannten gefährdeten Objekten gemäß § 29 Abs. 1 Satz 2 Nr. 2 und 3 geschaffen.

Zum Zwecke der Verbesserung der Eigensicherung der Polizeibeamten ist die Möglichkeit der Videodokumentation von Anhalte- und Kontrollsituationen in das SOG M-V aufzunehmen. Wie z. B. in Nordrhein-Westfalen und Rheinland-Pfalz wird nun auch die Polizei in Mecklenburg-Vorpommern ermächtigt, zum Zwecke der Eigensicherung bei Personen- oder Fahrzeugkontrollen Bildaufnahmen und -aufzeichnungen durch den Einsatz von Videotechnik in und an Fahrzeugen der Polizei herzustellen.

Die Telekommunikationsüberwachung zu präventiven Zwecken stellt in Zeiten wachsender Bedrohung durch den internationalen Terrorismus und durch die Erscheinungsform der Organisierten Kriminalität eine wichtige Befugnis zur Gefahrenabwehr dar. Insofern ist es erforderlich eine diesbezügliche Regelung in das SOG M-V aufzunehmen.

Unter Berücksichtigung der am 27. Juli 2005 ergangenen Entscheidung des Bundesverfassungsgerichts (Az.: 1BvR 668/04) in Bezug auf die im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung enthaltene Regelung zur präventiven Telekommunikationsüberwachung (TKÜ) knüpft die diesbezüglich erarbeitete Befugnisnorm zur präventiven TKÜ inklusive Standortermittlung an die Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes - und damit an besonders hochrangige Rechtsgüter - an. Darüber hinaus wird mit der neu geschaffenen Regelung die Maßnahme der präventiven TKÜ in Suizid- und Unglücksfällen zugelassen.

Zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung sind Vorkehrungen aufgenommen und weitere spezielle Vorschriften zur Verarbeitung und Nutzung der im Rahmen einer präventiven TKÜ erlangten personenbezogenen Daten geschaffen worden.

Der technische Fortschritt eröffnet der Polizei fortlaufend Möglichkeiten zur Optimierung ihrer Aufgabenerfüllung, indem er neue Technologien zur Verfügung stellt. Dazu zählt u. a. das Automatische Kfz-Kennzeichen-Lesesystem (AKLS), welches die Kennzeichen vorbeifahrender Kraftfahrzeuge erfasst und die Überprüfung dieser Ergebnisse mit Hilfe von Datenbanken oder das Speichern der Daten für spätere Recherchen ermöglicht. Dabei kann sowohl eine gezielte Suche nach einem speziell eingegebenen Kfz-Kennzeichen als auch ein Abgleich der gelesenen Kfz-Kennzeichen mit dem Sachfahndungsbestand erfolgen. Der vorliegende Gesetzentwurf schafft die rechtlichen Voraussetzungen, um das automatisierte Kfz-Kennzeichen-Lesesystem unter Beachtung der Erfordernisse des Datenschutzes in der polizeilichen Praxis effektiv einsetzen zu können. Durch den Einsatz dieser Technik werden die Polizeibeamten in ihrer Arbeit entlastet, da der aufwändige manuelle Abgleich entfällt.

Auf Empfehlung der Innenministerkonferenz wurde die Tatbestandsvoraussetzung für die Rasterfahndung, welche bisher das Vorliegen einer „gegenwärtigen Gefahr“ forderte, dahingehend verändert, dass die Durchführung der Rasterfahndung nunmehr zur Abwehr einer „erheblichen Gefahr“ zulässig ist. Zudem wird der Anwendungsbereich der Maßnahme auf den Bereich der Bekämpfung von Straftaten von erheblicher Bedeutung, z. B. der Organisierten Kriminalität, ausgedehnt.

Zum Schutz von Personen, die einem erhöhten Infektionsrisiko ausgesetzt sind, wie etwa Opfer von Gewalttaten oder im Dienst verletzte Polizeibeamte wird mit der vorgeschlagenen Änderung die Möglichkeit der präventiven Blutentnahme geschaffen.

Für die Regelungen zur Videoüberwachung, zur präventiven Telekommunikationsüberwachung und zum Einsatz des Kfz-Kennzeichen-Lesesystems wurde eine Befristung von fünf Jahren geschaffen, um die Wirksamkeit der Maßnahmen in diesem Zeitraum prüfen zu können.

Durch Ergänzungen, Klarstellungen sowie Vereinfachung des Gesetzestextes sollen die gewandelten Gegebenheiten Berücksichtigung finden, die Verständlichkeit und Handhabung des allgemeinen Gefahrenabwehrrechts verbessert sowie die Rechtssicherheit für Bürger und Behörden erhöht werden.

3. Alternativen

Keine.

4. Notwendigkeit der Regelung

Mit dem vorliegenden Gesetzentwurf soll die Polizei in erster Linie diejenigen neuen Befugnisse erhalten, auf die sie aufgrund 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. 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 Sicherheits- und Ordnungsgesetzes erfolgen.

5. Kosten

5.1 Kosten der öffentlichen Hand ohne Vollzugaufwand

Für die Wohnraumüberwachung, die präventive Telekommunikationsüberwachung, die Automatische Kennzeichenlesung und die Rasterfahndung kann auf vorhandene Technik zurückgegriffen werden. Ob der verfügbare Bestand den zukünftigen Bedarf abdeckt, kann derzeit noch nicht eingeschätzt werden. Für die präventive Telekommunikationsüberwachung werden weitere laufende Kosten (Entschädigung der Diensteanbieter) anfallen. Da nicht absehbar ist, in welchem Umfang diese rechtliche Möglichkeit genutzt werden muss, können die kostenmäßigen Auswirkungen nicht eingeschätzt werden. Für die Videoüberwachung zur Eigensicherung werden zusätzliche Kosten für die Beschaffung entstehen. Ferner wird die Ermöglichung der präventiven Blutprobenentnahme zusätzliche Kosten verursachen. Auch wenn von Kosten pro Blutprobenentnahme und -untersuchung von ca. 100 Euro ausgegangen werden kann, so sind doch die Fallzahlen nicht bekannt, sodass zu den kostenmäßigen Auswirkungen bei der präventiven Blutprobenentnahme keine Aussage gemacht werden kann.

Eventuelle Mehrbedarfe werden im Rahmen der verfügbaren Haushaltsmittel abgesichert.

Es ist weiter beabsichtigt, anstelle des inzwischen aufgehobenen Gesetzes über die Entschädigung von Sachverständigen und Zeugen (ZSEG) das Justizvergütungs- und -entschädigungsgesetz (JVEG) bei Entschädigungsregelungen nach dem SOG für entsprechend anwendbar zu erklären. Es wird davon ausgegangen, dass bei einer sachgerechten Anwendung des JVEG durch die Polizeibehörden, hier insbesondere durch Vergütungsvereinbarungen nach § 14 JVEG, Mehrausgaben im Polizeihaushalt nicht entstehen bzw. geringfügige Mehrausgaben im Rahmen der Deckungsfähigkeit ausgeglichen werden können. Eine Umfrage bei den Landkreisen (Ordnungsbehörden) hat ergeben, dass die Anwendung der Entschädigungsregelung kaum praktische Relevanz besitzt. Beispielsweise wurde vom Landkreis Müritzt mitgeteilt, dass in den vergangenen Jahren lediglich 1995 eine Vergütung erfolgte. Insofern dürfte nicht von einer nennenswerten finanziellen Mehrbelastung der Ordnungsbehörden auszugehen sein.

5.2 Vollzugsaufwand

Maßnahmen werden durch das vorhandene Personal getroffen.

5.3 Sonstige Kosten

Keine.

ENTWURF

eines Vierten Gesetzes zur Änderung des Sicherheits- und Ordnungsgesetzes

Der Landtag hat folgendes Gesetz beschlossen:

Artikel 1

Das Sicherheits- und Ordnungsgesetz in der Fassung der Bekanntmachung vom 25. März 1998 (GVOBl. M-V S. 335), zuletzt geändert durch das Gesetz vom 18. Mai 2004 (GVOBl. M-V S. 178) wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 34 werden folgende Angaben eingefügt:

„§ 34a Datenerhebung durch Überwachung der Telekommunikation
§ 34b Wohnraumüberwachung mit technischen Mitteln“.

b) Nach der Angabe zu § 43 wird folgende Angabe eingefügt:

„§ 43a Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen“.

c) Die Angabe zu § 44 wird wie folgt neu gefasst:

„§ 44 Rasterfahndung“.

d) Nach der Angabe zu § 45 wird die Angabe zu Unterabschnitt 3 wie folgt neu gefasst:

„Unterabschnitt 3
Prüffristen und Beschreibung von Verfahren (§§ 46, 47)“.

e) Die Angabe zu § 47 wird wie folgt neu gefasst:

„§ 47 Verfahren“.

f) Die Angabe zu § 53 wird wie folgt neu gefasst:

„§ 53 Durchsuchung und Untersuchung von Personen“.

g) Die Angabe zu § 116 wird wie folgt neu gefasst:

„§ 116 Außer-Kraft-Treten“.

2. Nach § 27 Abs. 4 Satz 1 werden folgende Sätze 2, 3 und 4 angefügt:

„Im Übrigen ist eine Aufzeichnung von Anrufen zulässig, soweit sie zur polizeilichen Aufgabenerfüllung erforderlich ist. Die Aufzeichnungen nach Satz 1 sind spätestens sechs Monate nach ihrer Erhebung, die Aufzeichnungen nach Satz 2 spätestens nach einer Woche zu löschen. Dies gilt nicht, sofern die Daten zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Erfüllung der in § 1 bezeichneten Aufgaben benötigt werden.“

3. § 32 wird wie folgt geändert:

- a) Absatz 3 wird wie folgt neu gefasst:

„(3) Öffentlich zugängliche Orte dürfen offen mit technischen Mitteln zur Bildüberwachung beobachtet werden, wenn dies zur Aufgabenerfüllung gemäß § 1 Abs. 1 erforderlich ist. Darüber hinaus dürfen offen Bilder aufgezeichnet werden, soweit an diesen Orten wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort künftig mit der Begehung von Straftaten zu rechnen ist. Bild- und Tonaufzeichnungen dürfen offen an oder in den in § 29 Abs. 1 Satz 2 Nr. 2 und 3 genannten Objekten angefertigt werden, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind. Die Maßnahmen nach Satz 1 bis 3 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind. Sie bedürfen der Anordnung durch den Behördenleiter. Über die Anordnung nach Satz 2 oder 3 ist der Landesbeauftragte für den Datenschutz unverzüglich zu unterrichten.“

- b) Nach Absatz 3 werden folgende Absätze 4 und 5 angefügt:

„(4) Bild- und Tonaufzeichnungen nach Absatz 3 Satz 2 und 3 sind spätestens eine Woche nach ihrer Erhebung zu löschen. Dies gilt nicht, wenn sie zur Verfolgung von Straftaten benötigt werden oder im Fall des Absatzes 3 Satz 3 Tatsachen die Annahme rechtfertigen, dass die Person künftig vergleichbare Straftaten oder Straftaten von erheblicher Bedeutung (§ 49) begehen wird.“

(5) Die Polizei kann zur Eigensicherung bei Personen- oder Fahrzeugkontrollen Bildaufnahmen und -aufzeichnungen durch den Einsatz optisch-technischer Mittel in oder an Fahrzeugen der Polizei herstellen. Der Einsatz der optisch-technischen Mittel ist, falls nicht offenkundig, durch geeignete Maßnahmen erkennbar zu machen oder der betroffenen Person mitzuteilen. Die Bildaufzeichnungen sind unverzüglich, spätestens am Ende der Dienstschicht, zu löschen. Dies gilt nicht, wenn die Aufzeichnungen zur Verfolgung von Straftaten benötigt werden.“

4. § 33 wird wie folgt geändert:

- a) In Absatz 1 Nr. 2 werden die Wörter „der durch Verwaltungsvorschrift des Innenministeriums zugelassenen“ gestrichen und das Wort „technischen“ durch das Wort „technischer“ ersetzt.
- b) Absatz 4 Satz 1 und 2 wird aufgehoben.
- c) Absatz 6 Satz 1 wird wie folgt neu gefasst:

„Aus einem mittels Amts- oder Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne der §§ 53, 53a der Strafprozessordnung kann die Polizei personenbezogene Daten mit technischen Mitteln über Personen erheben, die für eine Gefahr verantwortlich sind, und unter den Voraussetzungen des § 71 Abs. 1 über andere Personen, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist.“

5. § 34 wird wie folgt geändert:

- a) Absatz 2 wird wie folgt neu gefasst:

„(2) Daten, die ausschließlich über andere als die in § 33 Abs. 2, 3 oder 6 genannten Personen erhoben worden sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die nach § 33 Abs. 2 erhobenen Daten zur Verfolgung von Straftaten benötigt werden. Satz 1 gilt ferner nicht, soweit die nach § 33 Abs. 6 erhobenen Daten im Sinne des § 100d Abs. 6 der Strafprozessordnung verwendet werden dürfen.“

- b) In Absatz 3 Satz 1 werden die Wörter „in oder aus Wohnungen nach § 33 Abs. 4 oder“ gestrichen.
- c) In Absatz 5 Satz 3 wird die Angabe „4 und“ gestrichen.
- d) Absatz 7 Satz 2 wird wie folgt neu gefasst:

„Entsprechend unterrichtet das Justizministerium dieses Gremium über die nach § 100c der Strafprozessordnung erfolgten Maßnahmen.“

6. Nach § 34 werden folgende §§ 34a und 34b eingefügt:

„§ 34a

Datenerhebung durch Überwachung der Telekommunikation

(1) Die Polizei kann personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben über

1. die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben, Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes erforderlich ist,
2. Personen, wenn deren Leben oder Gesundheit gefährdet ist.

Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. Personenbezogene Daten Dritter dürfen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zweckes unvermeidbar ist. § 33 Abs. 6 gilt entsprechend.

(2) Eine Datenerhebung nach Absatz 1 kann sich auf

1. die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte,
2. die Telekommunikationsverbindungsdaten gemäß § 100g Abs. 3 der Strafprozessordnung oder
3. die Standortkennung einer Mobilfunkendeinrichtung beziehen.

(3) Die Polizei kann zur Vorbereitung einer Maßnahme nach Absatz 1 auch technische Mittel einsetzen, um die Geräte- und Kartenummer eines Mobilfunkendgerätes zu ermitteln, wenn die Durchführung der Maßnahme ohne die Ermittlung der Geräte- oder Kartenummer unmöglich oder wesentlich erschwert wäre. Durch den Einsatz technischer Mittel können unter den Voraussetzungen des Absatzes 1 Nr. 1 Telekommunikationsverbindungen unterbrochen oder verhindert werden. Kommunikationsverbindungen Dritter dürfen dabei nur unterbrochen oder verhindert werden, soweit dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist.

(4) Für die Anordnung der Maßnahmen nach Absatz 1 oder Absatz 3 gilt § 34 Abs. 3 entsprechend mit der Maßgabe, dass die Anordnung den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, oder die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten muss. Die Anordnung ergeht schriftlich, sie ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen des Absatzes 1 fortbestehen.

(5) Unter den Voraussetzungen des Absatzes 1 Nr. 1 kann die Polizei auch Auskunft über die Telekommunikation in einem zurückliegenden Zeitraum verlangen. Für die Anordnung der Maßnahme gilt Absatz 4 entsprechend.

(6) Aufgrund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 3 Abs. 2 des Gesetzes vom 7. Juli 2005 (BGBl. I S. 170), und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung, Aufzeichnung, Unterbrechung und Verhinderung von Telekommunikation zu ermöglichen sowie Auskünfte über nähere Umstände der Telekommunikation zu erteilen. Die in Anspruch genommenen Diensteanbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 716, 776), das zuletzt durch Artikel 5 des Gesetzes vom 16. August 2005 (BGBl. I S. 2437) geändert worden ist, entschädigt.

(7) Sind die nach dieser Vorschrift durchgeführten Maßnahmen abgeschlossen, sind die Betroffenen zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann. Erfolgt die Unterrichtung nicht innerhalb von sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Unterrichtung der richterlichen Zustimmung. Entsprechendes gilt nach Ablauf von jeweils weiteren sechs Monaten. Ist wegen des die Maßnahme auslösenden Sachverhaltes ein strafrechtliches Ermittlungsverfahren gegen einen Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Mit Ausnahme der Personen, gegen die sich die Maßnahme richtete, kann eine Unterrichtung mit richterlicher Zustimmung unterbleiben, wenn sie nur mit unverhältnismäßigen Ermittlungen möglich wäre oder wenn ihr überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Im Fall des Satzes 4 gelten die Regelungen der Strafprozessordnung; im Übrigen gilt für die gerichtliche Zuständigkeit und das Verfahren § 34 Abs. 3 Satz 3 bis 5 entsprechend.

(8) Die durch Maßnahmen nach dieser Vorschrift erlangten personenbezogenen Daten sind besonders zu kennzeichnen. Sie dürfen nur verwendet werden zu den Zwecken, zu denen sie erhoben wurden, sowie zu dem Zweck der Verfolgung von Straftaten, die nach der Strafprozessordnung die Überwachung und Aufzeichnung der Telekommunikation rechtfertigen. Die Zweckänderung ist festzustellen und zu dokumentieren. Personenbezogene Daten Dritter sind nach Beendigung der Maßnahme unverzüglich zu löschen. Daten, bei denen sich nach Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung zuzuordnen sind, dürfen nicht verwendet werden; sie sind unverzüglich zu löschen. Im Übrigen findet für die erlangten personenbezogenen Daten § 45 Abs. 2, 3 und 4 Nr. 1 und 2 Anwendung. Wird eine Löschung nach den Sätzen 4, 5 oder 6 vorgenommen, ist diese zu dokumentieren.

(9) § 34 Abs. 7 gilt entsprechend.

§ 34b
Wohnraumüberwachung mit technischen Mitteln

(1) In oder aus Wohnungen von Personen, die für eine Gefahr verantwortlich sind, kann die Polizei personenbezogene Daten mit technischen Mitteln über Personen erheben, die für eine Gefahr verantwortlich sind, und unter den Voraussetzungen des § 71 Abs. 1 über andere Personen, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. In oder aus Wohnungen von Personen, die nicht für eine Gefahr verantwortlich sind, ist die Datenerhebung nur zulässig, wenn die Gefahrenabwehr auf andere Weise nicht oder nicht rechtzeitig möglich wäre und dabei überwiegende Rechte und Pflichten der Personen nicht verletzt werden.

(2) Die Maßnahme nach Absatz 1 darf nur angeordnet werden, soweit nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Daten erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Abzustellen ist dabei insbesondere auf die Art der zu überwachenden Räumlichkeiten und das Verhältnis der dort anwesenden Personen zueinander. Gespräche in Betriebs- oder Geschäftsräumen sind in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen. Das Gleiche gilt für Gespräche über begangene Straftaten und Äußerungen, mittels derer Straftaten begangen werden.

(3) Die Bild- und Tonüberwachung sowie die Aufzeichnung und die Auswertung der erhobenen Daten durch die Polizei sind unverzüglich zu unterbrechen, sofern sich tatsächliche Anhaltspunkte dafür ergeben, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen, sie dürfen nicht verwertet werden. Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu dokumentieren. Ist die Maßnahme nach Satz 1 unterbrochen worden, so darf sie unter den in Absatz 2 genannten Voraussetzungen fortgeführt werden.

(4) Für die Datenerhebung aus einem mittels Amts- oder Berufsgeheimnis geschützten Vertrauensverhältnis im Sinne der §§ 53, 53a der Strafprozessordnung gilt § 33 Abs. 6 entsprechend.

(5) Die Datenerhebung nach Absatz 1 bedarf der richterlichen Anordnung. Bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person kann der Behördenleiter die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. § 34 Abs. 3 Satz 3 bis 5 gilt entsprechend. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. soweit bekannt Name und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
3. Art, Umfang und Dauer der Maßnahme,
4. die Wohnung oder Räume, in oder aus denen die Daten erhoben werden sollen, und
5. die Art der durch die Maßnahme zu erhebenden Daten

zu bestimmen. Sie ist auf höchstens zwei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die in den Absätzen 1 und 2 bezeichneten Voraussetzungen vorliegen.

- (6) Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Aufhebung der Datenerhebung an. Polizeiliche Maßnahmen nach Absatz 3 können durch das anordnende Gericht jederzeit aufgehoben, geändert oder angeordnet werden. Soweit ein Verwertungsverbot nach Absatz 3 Satz 2 in Betracht kommt, hat die Polizei unverzüglich eine Entscheidung des anordnenden Gerichts über die Verwertbarkeit der erlangten Erkenntnisse herbeizuführen.
- (7) Nach Absatz 1 erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrecht zu erhalten. Die erlangten Daten dürfen nur verwendet werden zu Zwecken, zu denen sie erhoben wurden, sowie zu dem Zweck der Verfolgung von Straftaten, die nach der Strafprozessordnung die Wohnraumüberwachung rechtfertigen. Die Zweckänderung ist festzustellen und zu dokumentieren.
- (8) Sind die nach dieser Vorschrift durchgeführten Maßnahmen abgeschlossen, sind die Betroffenen zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann. Erfolgt die Unterrichtung nicht innerhalb von sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Unterrichtung der richterlichen Zustimmung. Entsprechendes gilt nach Ablauf von jeweils weiteren sechs Monaten. Ist wegen des die Wohnraumüberwachung auslösenden Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen einen Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Mit Ausnahme der Personen, gegen die sich die Maßnahme richtete, kann eine Unterrichtung mit richterlicher Zustimmung unterbleiben, wenn sie nur mit unverhältnismäßigen Ermittlungen möglich wäre oder wenn ihr überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Gegenüber solchen Personen, die sich als Gast oder sonst zufällig in der überwachten Wohnung aufgehalten haben, kann die Benachrichtigung auch unterbleiben, wenn die Überwachung keine verwertbaren Ergebnisse erbracht hat. Im Fall des Satzes 4 gelten die Regelungen der Strafprozessordnung; im Übrigen gilt für die gerichtliche Zuständigkeit und das Verfahren § 34 Abs. 3 Satz 3 bis 5 entsprechend.
- (9) § 34 Abs. 7 gilt entsprechend.“
7. In § 40 Abs. 4 Satz 1 werden die Wörter „die vom Innenministerium durch Verwaltungsvorschrift bestimmten“ gestrichen und das Wort „ausländischen“ durch das Wort „ausländische“ ersetzt.
8. In § 42 Abs. 2 Satz 1 werden die Wörter „Das Verfahrensverzeichnis“ durch die Wörter „Die Beschreibung“ ersetzt.

9. Nach § 43 wird folgender § 43a eingefügt:

**„§ 43a
Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen**

(1) Die Polizei kann unter den Voraussetzungen der §§ 27a, 29, 32 oder 33 Abs. 1 Nr. 1 im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben. Eine verdeckte Datenerhebung ist nur unter den Voraussetzungen des § 26 Abs. 2 Satz 2 zulässig. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind.

(2) Der Abgleich erhobener Kennzeichendaten mit anderen polizeilichen Dateien ist nur zulässig, soweit die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist.

(3) Erfasste Kennzeichendaten, die nach Durchführung des Datenabgleichs nicht im Fahndungsbestand oder in einer Datei gemäß Absatz 2 enthalten sind, sind unverzüglich zu löschen.“

10. § 44 wird wie folgt geändert:

a) Die Überschrift wird wie folgt neu gefasst:

„§ 44
Rasterfahndung“.

b) Absatz 1 Satz 1 wird wie folgt neu gefasst:

„Die Polizei kann von Behörden, anderen öffentlichen Stellen und von Stellen außerhalb der öffentlichen Verwaltung zur Abwehr einer erheblichen Gefahr oder zur Bekämpfung von Straftaten von erheblicher Bedeutung gemäß § 49 Nr. 1 und 3 die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen (Rasterfahndung), wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr oder zur Bekämpfung der Straftaten erforderlich ist.“

c) Absatz 3 Satz 1 wird wie folgt neu gefasst:

„Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen personenbezogenen Daten auf dem Datenträger zu löschen und die Unterlagen zurückzugeben oder zu vernichten, soweit sie nicht zur Abwehr einer erheblichen Gefahr oder für ein mit dem Sachverhalt zusammenhängendes Strafverfahren erforderlich sind.“

11. Nach § 45 wird die Überschrift zu Unterabschnitt 3 wie folgt neu gefasst:

„Unterabschnitt 3
Prüffristen und Beschreibung von Verfahren“.

12. § 47 wird wie folgt geändert:

a) Die Überschrift wird wie folgt neu gefasst:

„§ 47
Verfahren“.

b) Absatz 2 wird wie folgt neu gefasst:

„(2) Für jedes automatisierte Verfahren ist eine Beschreibung zu erstellen, in der neben den Vorgaben des § 18 des Landesdatenschutzgesetzes zusätzlich Prüffristen nach § 46 anzuordnen sind.“

c) In Absatz 3 Satz 2 werden die Wörter „Das Verzeichnisse“ durch die Wörter „Die Beschreibung“ ersetzt.

13. § 49 Nr. 3 wird wie folgt geändert:

a) In Buchstabe b wird die Angabe „§ 53 Abs. 1 Satz 1 Nr. 1 und 2“ durch die Angabe „§ 52 Abs. 1 Nr. 2 Buchstabe c und d“ ersetzt.

b) In Buchstabe d wird die Angabe „§ 92 Abs. 2 des Ausländergesetzes“ durch die Angabe „§ 95 Abs. 2 des Aufenthaltsgesetzes“ ersetzt.

14. In § 50 Abs. 6 werden die Wörter „Gesetz über die Entschädigung von Zeugen und Sachverständigen“ durch die Wörter „Justizvergütungs- und -entschädigungsgesetz“ ersetzt.

15. § 52 Abs. 2 wird wie folgt geändert:

a) Satz 1 wird wie folgt neu gefasst:

„Die Polizei kann eine Person ihrer Wohnung und des unmittelbar angrenzenden Bereichs verweisen, wenn dies erforderlich ist, um eine gegenwärtige Gefahr für Leib, Leben oder Freiheit von Bewohnern derselben Wohnung abzuwenden.“

b) Nach Satz 4 werden folgende Sätze 5 und 6 angefügt:

„Im Falle eines Antrags auf zivilrechtlichen Schutz nach dem Gewaltschutzgesetz vom 11. Dezember 2001 (BGBl. I S. 3513) mit dem Ziel des Erlasses einer einstweiligen Anordnung, endet die nach Satz 1 oder 2 verfügte polizeiliche Maßnahme bereits mit dem Tag der Wirksamkeit der gerichtlichen Entscheidung. Das Gericht informiert die Polizei über seine Entscheidung.“

16. § 53 wird wie folgt geändert:

a) Die Überschrift wird wie folgt neu gefasst:

„§ 53
Durchsuchung und Untersuchung von Personen“.

b) Nach Absatz 3 wird folgender Absatz 4 angefügt:

„(4) Bei einer lebenden oder verstorbenen Person, von der sich ergibt oder anzunehmen ist, dass sie krank, krankheitsverdächtig, ansteckungsverdächtig ist oder war, können Entnahmen von Blutproben und andere körperliche Eingriffe zur Feststellung des Infektionsstatus angeordnet werden, wenn Tatsachen die Annahme rechtfertigen, dass es zu einer Übertragung von Krankheitserregern, wie insbesondere Hepatitis B, Hepatitis C oder Humanes Immundefizienzvirus (HIV) auf eine andere Person gekommen ist und bei dieser Person dadurch eine Gefahr für das Leben oder eine schwerwiegende Gesundheitsgefährdung besteht und die Kenntnis des Infektionsstatus zur Abwehr der Gefahr erforderlich ist. Körperliche Untersuchungen und Eingriffe dürfen nur von einem Arzt nach den Regeln der ärztlichen Kunst durchgeführt werden. Vor einer Blutentnahme soll eine ärztliche Konsultation erfolgen. Körperliche Untersuchungen und Eingriffe sind ohne Einwilligung des Betroffenen zulässig, wenn kein Nachteil für seine Gesundheit zu befürchten ist. Die Maßnahme bedarf der richterlichen Anordnung. Bei Gefahr im Verzug kann die Polizei die Maßnahme anordnen. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Die bei der Untersuchung erhobenen personenbezogenen Daten dürfen über den Zweck dieses Gesetzes hinaus nur zum Schutz vor oder zur Abwehr von schwerwiegenden Gesundheitsgefährdungen verarbeitet und genutzt werden.“

17. § 64 Abs. 1 Nr. 2 wird wie folgt neu gefasst:

„2. die empfangsberechtigte Person die Sache innerhalb einer Frist von sechs Wochen nach schriftlich ergangener Aufforderung nicht in Empfang nimmt oder“.

18. § 116 wird wie folgt neu gefasst:

**„§ 116
Außer-Kraft-Treten**

§ 32 Abs. 3 und 4, § 34a und § 43a treten mit Ablauf des <einsetzen: Datum des Tages, der dem Tag vorhergeht, der durch seine Benennung oder seine Zahl dem Tag des Inkraft-Tretens dieses Gesetzes nach 5 Jahren entspricht.> außer Kraft.“

Artikel 2

Aufgrund dieses Gesetzes können das Recht auf körperliche Unversehrtheit (Artikel 2 Abs. 2 Satz 1 des Grundgesetzes), das Recht der Freiheit der Person (Artikel 2 Abs. 2 Satz 2 des Grundgesetzes), das Recht auf Wahrung des Fernmeldegeheimnisses (Artikel 10 Abs. 1 des Grundgesetzes), das Recht der Freizügigkeit (Artikel 11 des Grundgesetzes) und das Recht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt werden.

Artikel 3

Das Innenministerium kann den Wortlaut des Sicherheits- und Ordnungsgesetzes in der vom In-Kraft-Treten dieses Gesetzes an geltenden Fassung im Gesetz- und Verordnungsblatt für Mecklenburg-Vorpommern bekannt machen.

Artikel 4

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Volker Schlotmann und Fraktion

Angelika Gramkow und Fraktion

Begründung:

A. Allgemeine Begründung

Mit dem vorliegenden Gesetzentwurf soll die Polizei in erster Linie diejenigen neuen Befugnisse erhalten, auf die sie aufgrund 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. 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 Sicherheits- und Ordnungsgesetzes erfolgen.

Das Bundesverfassungsgericht hat mit seinem Urteil vom 3. März 2004 (Az.: 1BvR 2378/98) Grundsätze für akustische Wohnraumüberwachungsmaßnahmen aufgestellt, die im Rahmen der Strafverfolgung durchgeführt werden. Für diese Maßnahmen ist Art. 13 Abs. 3 Grundgesetz (GG) maßgeblich. Die Regelungen der Strafprozessordnung (StPO), die die Grundgesetzänderung einfachgesetzlich umsetzen, wurden teilweise für verfassungswidrig erklärt. Zwar hat das Bundesverfassungsgericht unmittelbar nur über die Verfassungsmäßigkeit der Bestimmungen der §§ 100c ff. StPO entschieden, dennoch ergibt sich aus der Urteilsbegründung auch gesetzlicher Änderungsbedarf hinsichtlich der Ausgestaltung der präventiven Wohnraumüberwachung im SOG M-V.

Um den Grundsätzen des Bundesverfassungsgerichts Rechnung zu tragen, erfolgt die Ergänzung der Regelungen zur Wohnraumüberwachung aus Gründen der Übersichtlichkeit in einem neu geschaffenen § 34b SOG M-V. Im Gefahrenabwehrbereich sichert die erarbeitete Befugnisnorm nunmehr den unantastbaren Kernbereich privater Lebensgestaltung und trifft spezielle Regelungen zur Verarbeitung und Nutzung der diesbezüglich erlangten Daten. Es wird darauf hingewiesen, dass die Entscheidung des Landesverfassungsgerichtes M-V vom 18. Mai 2000 zu den landesrechtlichen Regelungen zur polizeilichen Überwachung von Wohnungen und bei Datenerhebungen aus dem Bereich geschützter Vertrauensverhältnisse bereits bei einer der letzten Gesetzesnovellen berücksichtigt worden ist und insoweit keine Änderungen vorzunehmen waren.

Spätestens mit den Terroranschlägen am 7. Juli 2005 in London ist ebenso eine Novellierung der Regelungen zur Videoüberwachung öffentlich zugänglicher Orte im SOG M-V dringend geboten. Die Handhabe der Bildaufzeichnung ist im Land Mecklenburg-Vorpommern im Vergleich zu anderen Länderregelungen nur in einem sehr eingeschränkten Umfang möglich. Unter Berücksichtigung der aktuellen Rechtsprechung zur Videoüberwachung öffentlicher Räume (Urteil des VGH Mannheim vom 21. Juli 2003) und bereits bestehender Regelungen in anderen Bundesländern soll die Befugnisnorm zur Bildbeobachtung und -aufzeichnung neu gefasst werden. Mit der neu geschaffenen Regelung sind die Ordnungsbehörden und die Polizei zur Bildbeobachtung öffentlich zugänglicher Orte befugt, wenn dies zur Aufgabenerfüllung nach § 1 Abs. 1 SOG M-V erforderlich ist. Darüber hinaus ist die Bildaufzeichnung an öffentlich zugänglichen Orten möglich, an denen wiederholt Straftaten begangen worden sind (sog. Kriminalitätsschwerpunkte) und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist.

Zum Zwecke der Verbesserung der Eigensicherung der Polizeibeamten ist die Möglichkeit der Videodokumentation von Anhalte- und Kontrollsituationen in das SOG M-V aufzunehmen. Wie z. B. in Nordrhein-Westfalen wird nun auch die Polizei in Mecklenburg-Vorpommern ermächtigt, zum Zwecke der Eigensicherung bei Personen- oder Fahrzeugkontrollen Bildaufnahmen und -aufzeichnungen durch den Einsatz von Videotechnik in und an Fahrzeugen der Polizei herzustellen.

Die Telekommunikationsüberwachung zu präventiven Zwecken stellt in Zeiten wachsender Bedrohung durch den internationalen Terrorismus und durch die Erscheinungsform der Organisierten Kriminalität eine wichtige Befugnis zur Gefahrenabwehr dar. Insofern ist es erforderlich eine diesbezügliche Regelung in das SOG M-V aufzunehmen.

Unter Berücksichtigung der am 27. Juli 2005 ergangenen Entscheidung des Bundesverfassungsgerichts (Az.: 1BvR 668/04) in Bezug auf die im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung enthaltene Regelung zur präventiven Telekommunikationsüberwachung (TKÜ) knüpft die diesbezüglich erarbeitete Befugnisnorm zur präventiven TKÜ inklusive Standortermittlung an die Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes - und damit an besonders hochrangige Rechtsgüter - an. Darüber hinaus wird mit der neu geschaffenen Regelung die Maßnahme der präventiven TKÜ in Suizid- und Unglücksfällen zugelassen. Zudem sind Vorkehrungen zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung aufgenommen und weitere spezielle Vorschriften zur Verarbeitung und Nutzung der im Rahmen einer präventiven TKÜ erlangten personenbezogenen Daten geschaffen worden.

Der technische Fortschritt eröffnet der Polizei fortlaufend Möglichkeiten zur Optimierung ihrer Aufgabenerfüllung, indem er neue Technologien zur Verfügung stellt. Dazu zählt u.a. das Automatische Kfz-Kennzeichen-Lesesystem (AKLS), welches die Kennzeichen vorbeifahrender Kraftfahrzeuge erfasst und die Onlineüberprüfung dieser Ergebnisse mit Hilfe von Datenbanken oder das Speichern der Daten für spätere Recherchen ermöglicht. Dabei kann sowohl eine gezielte Suche nach einem speziell eingegebenen Kfz-Kennzeichen als auch ein Abgleich der gelesenen Kfz-Kennzeichen mit dem Sachfahndungsbestand erfolgen. Der vorliegende Gesetzentwurf schafft die rechtlichen Voraussetzungen, um das automatisierte Kfz-Kennzeichen-Lesesystem unter Beachtung der Erfordernisse des Datenschutzes in der polizeilichen Praxis effektiv einsetzen zu können. Durch den Einsatz dieser Technik werden die Polizeibeamten in ihrer Arbeit entlastet, da der aufwändige manuelle Abgleich entfällt.

Entsprechend der Empfehlung der ad-hoc-Arbeitsgruppe des AK II „Rasterfahndung“ wird mit der Änderung des Absatzes 1 Satz 1 des § 44 eine Herabsetzung der bisher normierten Eingriffsvoraussetzungen vorgenommen. Dieser Bericht wurde am 6. Juni 2002 von der Innenministerkonferenz zustimmend zur Kenntnis genommen. Es wird nicht mehr an die Gegenwärtigkeit der Gefahr angeknüpft, sondern das Vorliegen einer „erheblichen Gefahr“ gemäß § 3 Abs. 3 SOG M-V vorausgesetzt. Mit dem Rückgriff auf die in § 3 Abs. 3 SOG M-V enthaltene Legaldefinition geht gleichzeitig eine Erweiterung der bisher geschützten, bedeutsamen Rechtsgüter einher. Andere Bundesländer haben diese Herabsetzung der Eingriffsvoraussetzungen bereits vorgenommen.

§ 53 wird ergänzt um die Befugnis zur Anordnung einer Blutentnahme. Diese Vorschrift soll dem Schutz von Opfern von Gewalttaten, von Polizeibeamten und anderen Berufsgruppen dienen, die mit Personen in Kontakt gekommen sind, bei denen beispielsweise der Verdacht auf Aids oder Hepatitis besteht. Eine Infektion ist kurze Zeit nach dem Kontakt zwischen Verursacher und Opfer gerade bei den o.g. schweren Viruserkrankungen beim Opfer noch nicht nachzuweisen. Eine wirksame medizinische Maßnahme hat jedoch zumeist direkt nach der Virenübertragung zu erfolgen. Der Infektionsstatus, der durch eine Blutuntersuchung festgestellt werden kann, ist somit von eminenter Wichtigkeit für die weitere Behandlung des Opfers. Für diese körperliche Untersuchung (Blutentnahme) ist grundsätzlich eine richterliche Anordnung erforderlich, bei Gefahr im Verzug darf die Anordnung durch die Polizei erfolgen.

B. Zu den einzelnen Vorschriften

Zu Artikel 1

Zu Nummer 1 (Inhaltsübersicht)

Wegen der Änderung der Überschriften der §§ 44, 47 und 53 sowie der Einfügung der §§ 34a, 34b und 43a wird die Inhaltsübersicht geändert. Im Übrigen wird die Überschrift des Abschnittes 3 Unterabschnitt 3 angepasst.

Zu Nummer 2 (§ 27)

Gemäß § 27 Abs. 4 können die Polizei und Behörden, die Aufgaben der Hilfs- und Rettungsdienste wahrnehmen, fernmündlich an sie gerichtete Notrufe und über die Notrufeinrichtungen eingehende sonstige Mitteilungen auf einen Tonträger aufnehmen.

In den Polizeidienststellen des Landes werden jedoch auch Anrufe, die keinen Notrufcharakter haben, in einem Drohanrufsystem digital zwischengespeichert. Das Drohanrufsystem ist ein Dokumentationssystem, das an dem Vermittlungsplatz der Polizeibehörden installiert ist. Jeder Anruf wird dort digital zwischengespeichert. Bei sog. Drohanrufen kann aus Gründen der Gefahrenabwehr mittels Knopfdruck der gesamte Gesprächsinhalt aus dem digitalen Zwischenspeicher auf ein Magnetband übertragen werden. Ansonsten werden die Gespräche fortlaufend überschrieben und sind nur mit erheblichem technischen Aufwand aus dem Zwischenspeicher rekonstruierbar. Bei den Drohanrufen handelt es sich z. B. um die Ankündigung von Straftaten (Bombendrohungen, Erpressermeldungen) oder sonstige Tatbestände, die aus Gründen der Gefahrenabwehr ein Einschreiten der Polizei erforderlich machen. Bisher existiert für die digitale Zwischenspeicherung von Anrufen keine rechtliche Grundlage im SOG M-V. Auf Anregung des Landesbeauftragten für den Datenschutz wird eine solche Regelung nunmehr aufgenommen.

Für die neue Speicherungsmöglichkeit ist allerdings eine kürzere Lösungsfrist vorgesehen.

Zu Nummer 3 (§ 32)

Die Ständige Konferenz der Innenminister und -senatoren der Länder hat bereits im Jahre 2000 die offene Videoüberwachung an Kriminalitätsbrennpunkten als geeignetes Mittel bezeichnet, die polizeiliche Gefahrenabwehr zu verbessern. Durch Videoüberwachung könne die Prävention gestärkt, Straftaten verhindert und die polizeiliche und ordnungsbehördliche Gefahrenabwehr verbessert werden. Dieser Forderung wurde nach den terroristischen Anschlägen in London am 7. Juli 2005 wieder Nachdruck verliehen. Bundesweit wird eine Ausweitung der Videoüberwachung für erforderlich gehalten, um die Wahrnehmung der polizeilichen Aufgaben im Rahmen der Gefahrenabwehr und der Verhütung von Straftaten auch im Bereich der allgemeinen Kriminalität noch wirksamer unterstützen zu können.

Während allgemein zugängliche Flächen und Räume bisher mit technischen Mitteln zur Bildübertragung beobachtet werden durften, wenn dies zur Aufgabenerfüllung nach § 1 erforderlich war, ist die Möglichkeit der Bildaufzeichnung im Land Mecklenburg-Vorpommern im Vergleich zu anderen Länderregelungen nur in sehr eingeschränktem Umfang zugelassen worden. So stellte man bisher bei der Bildaufzeichnung auf die in § 49 normierten Straftaten von erheblicher Bedeutung ab und forderte das Vorliegen tatsächlicher Anhaltspunkte für deren Begehung. Mit der neuen Vorschrift soll eine Rechtsgrundlage für Bildübertragungen und Aufzeichnungen an öffentlich zugänglichen Orten sowie an gefährdeten Objekten ermöglicht werden. Durch diese Neuregelungen sollen die Gefahrenabwehrbehörden in die Lage versetzt werden, bei diesen neuen Anforderungen wirksam der Entstehung von Gefahren entgegenzutreten. Zu denken ist hierbei u. a. an den Schutz wichtiger Infrastruktureinrichtungen (Heizkraftwerke, Energieanlagen, Verkehrseinrichtungen) vor Sabotageanschlägen durch Einsatz von Videotechnik. Die demnächst in Mecklenburg-Vorpommern stattfindenden Veranstaltungen, wie G8-Gipfel mit einem Massenaufkommen an zu schützenden Personen und Veranstaltungen, wie auch die Übertragung von Fußball-WM-Spielen auf Großbildschirmen verlangen das Vorhandensein bestimmter Eingriffsmöglichkeiten für die Gefahrenabwehrbehörden. Ob diese Eingriffsgrundlagen letztlich genutzt werden müssen, ist eine andere Frage. Erfahrungen mit dem Einsatz von Videotechnik in der Bundesrepublik haben bisher durchweg positive Ergebnisse gezeigt. Schon aufgrund des Abschreckungseffektes durch den offenen Einsatz können regelmäßig ein Rückgang der Kriminalität verzeichnet und somit Straftaten verhütet werden. Gleichzeitig wird das subjektive Sicherheitsgefühl der Bürger verbessert.

Unter Berücksichtigung der aktuellen Rechtsprechung zur Videoüberwachung öffentlicher Räume (Urteil des VGH Mannheim vom 21. Juli 2003; NVwZ 2004 S. 498) und bereits bestehender Regelungen in anderen Bundesländern wird die Befugnisnorm zur Bildbeobachtung und -aufzeichnung neu gefasst. Da beide Formen der Videoüberwachung in das Recht auf informationelle Selbstbestimmung eingreifen, werden die Überwachungsmaßnahmen nur in bestimmten Fällen zugelassen:

Zu a)

In Satz 1 wurde die Zulässigkeit der Bildbeobachtung durch die Ordnungsbehörden und die Polizei zur Verdeutlichung des primären Ziels der Maßnahme, nämlich Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren, auf die Aufgabenerfüllung gemäß § 1 Abs. 1 beschränkt.

Mit der vorgeschlagenen Neuregelung ist über die bloße Bildbeobachtung hinaus eine Bildaufzeichnung an öffentlich zugänglichen Orten möglich, an denen wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist. Diese so genannten Kriminalitätsbrennpunkte sind aufgrund von objektiv nachvollziehbaren ortsbezogenen Lageerkenntnissen zu ermitteln. Neben der Qualifizierung des überwachten Ortes als Kriminalitätsbrennpunkt setzt die Durchführung der Videoüberwachung voraus, dass aufgrund konkreter Anhaltspunkte - also auf Grund der tatsächlichen Geschehnisse an diesem Ort - die Annahme gerechtfertigt ist, dass dort in Zukunft weitere Straftaten begangen werden und dass die Videoüberwachung zu deren Bekämpfung erforderlich ist (Gefahrenprognose).

Darüber hinaus wird mit der vorgeschlagenen Änderung eine Rechtsgrundlage für Bild- und Tonaufzeichnungen an oder in Verkehrs- oder Versorgungsanlagen oder -einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden und in deren unmittelbarer Nähe und an oder in besonders gefährdeten Objekten geschaffen. Eine Videoüberwachung ist an oder in diesen Objekten nur dann zulässig, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind.

Die Befugnisse zur Datenerhebung nach Absatz 3 gelten nicht bei öffentlichen Versammlungen, da diese abschließend im Versammlungsgesetz geregelt sind. Der Einsatz technischer Mittel zur Bildüberwachung bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen, die nicht dem Versammlungsgesetz unterliegen (Bsp. Fußballspiele, Volksfeste, Rockertreffen), ist bereits in Absatz 1 des § 32 geregelt.

Mit dem neuen Absatz 3 wird zudem eindeutig geregelt, dass die Videoüberwachung an den v. g. öffentlich zugänglichen Orten und den genannten Objekten offen (d. h. die Tatsache der Überwachung der v. g. Örtlichkeiten muss für den Betroffenen erkennbar sein) zu erfolgen hat. Die Maßnahme der Videoüberwachung bedarf nunmehr der Anordnung durch den Behördenleiter. Soweit Aufzeichnungsmaßnahmen angeordnet werden, ist der Landesbeauftragte für den Datenschutz unverzüglich zu unterrichten.

Zu b)

Mit dem Absatz 4 wird für die neu geregelte Videoüberwachung nach Absatz 3 eine spezielle Regelung zur Verarbeitung und Nutzung der bei der Bild- und Tonaufzeichnung erhobenen Daten geschaffen. So sind die nach dem neuen Absatz 3 angefertigten Bild- und Tonaufzeichnungen spätestens 1 Woche nach ihrer Erhebung zu löschen, wenn sie nicht zur Verfolgung von Straftaten benötigt werden oder im Fall des Absatzes 3 Satz 3 Tatsachen die Annahme rechtfertigen, dass die Person künftig vergleichbare Straftaten oder Straftaten von erheblicher Bedeutung (§ 49) begehen wird. Soweit die Bild- und Tonaufzeichnungen daher zur Verfolgung von Ordnungswidrigkeiten benötigt werden, ist eine Aufbewahrung über die Wochenfrist hinaus nicht zulässig.

Die festgelegte Wochenfrist ist eine Höchstfrist. Sie unterschreitet deutlich die in § 32 Abs. 2 enthaltene Monatsfrist zur Löschung der nach Absatz 1 bei oder in Zusammenhang mit Veranstaltungen oder Ansammlungen erhobenen Daten und auch die festgelegten Lösungsfristen zu Bild- und Tonaufzeichnungen in den meisten Polizeigesetzen der anderen Bundesländer. Die Festlegung einer kürzeren Lösungsfrist für die Bild- und Tonaufzeichnungen nach Absatz 3 ist insbesondere mit Blick auf die benötigte Zeit für den Fall der notwendigen Auswertung von Tonaufzeichnungen nicht angezeigt.

Die Anwendung der neu geregelten Absätze 3 und 4 des § 32 wird zunächst auf 5 Jahre begrenzt (vgl. Regelung in § 116). Die zeitliche Begrenzung der Befugnisnorm zur Videoüberwachung bestimmter Örtlichkeiten soll dazu führen, dass eine Aus- bzw. Bewertung des Einsatzes und der Auswirkungen der Maßnahme stattfindet und dann eine Entscheidung über den Fortbestand der Regelung getroffen werden kann.

Zu c)

Zum Zwecke der Verbesserung der Eigensicherung ist die Möglichkeit der Videodokumentation von Anhalte- und Kontrollsituationen in das SOG aufzunehmen. Wie z. B. in Nordrhein-Westfalen und Rheinland-Pfalz wird nun auch die Polizei in Mecklenburg-Vorpommern ermächtigt, zum Zwecke der Eigensicherung bei Personen- oder Fahrzeugkontrollen Bildaufnahmen und -aufzeichnungen durch den Einsatz von Videotechnik in und an Fahrzeugen der Polizei herzustellen. Der Einsatz von Videotechnik muss, soweit er nicht offenkundig ist, durch geeignete Maßnahmen erkennbar gemacht oder der betroffenen (kontrollierten) Person mitgeteilt werden. Durch diese Regelungen soll die kontrollierte Person von Angriffen gegen Polizeibeamte abgeschreckt werden.

Die Bildaufzeichnungen sind unverzüglich, spätestens am Ende der Dienstschicht, zu löschen - außer wenn die Aufzeichnungen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden. Durch das unverzügliche Löschen wird ein Missbrauch der Aufzeichnungen zum Zwecke der Mitarbeiterkontrolle durch Vorgesetzte verhindert. Durch die enge Begrenzung der Verwendung der Aufzeichnung und die kurze Frist bis zur Löschung handelt es sich bei der Maßnahme um einen nur geringen Eingriff in das Recht auf informationelle Selbstbestimmung der kontrollierten Person. Einem solch geringen Eingriff in die Rechte des Betroffenen steht die gefährdete Unversehrtheit von Leib und Leben der kontrollierenden Polizeibeamten gegenüber. Eine Rechtsgüterabwägung muss hier zu dem Ergebnis kommen, dass das Interesse der Polizisten an der körperlichen Unversehrtheit und damit der Eigensicherung überwiegt.

Zu Nummer 4 (§ 33)

§ 33 Abs. 1 Nr. 2 gestattet bisher den verdeckten Einsatz technischer Mittel, insbesondere zur Bild- und Tonüberwachung oder Bild- und Tonaufzeichnung, soweit diese Mittel durch eine Verwaltungsvorschrift des Innenministeriums zugelassen sind. Vor dem Hintergrund der schnell voranschreitenden technischen Entwicklungen ist festzustellen, dass eine solche Verwaltungsvorschrift nicht zweckdienlich ist, da sie stetig erneuert werden müsste. Die Streichung des Absatzes 4 Satz 1 und 2 und die Neufassung des Absatz 6 Satz 1 sind Folgeänderungen der Neuregelung der Wohnraumüberwachung in § 34b.

§ 33 listet in Absatz 1 die besonderen Mittel der Datenerhebung auf. Die Regelungen in den folgenden Absätzen beinhalten allgemeine Vorschriften, die sich auf alle besonderen Mittel der Datenerhebung beziehen, auch auf die in den §§ 34 a und b normierten.

Zu Nummer 5 (§ 34)

Die Änderungen ergeben sich aus der Neufassung der Wohnraumüberwachung in § 34b und der Neufassung der Strafprozessordnung.

Zu Nummer 6 (§ 34a)

Nach derzeitiger Rechtslage ist die Telekommunikationsüberwachung in den §§ 100a ff. der Strafprozessordnung (StPO) geregelt. Nach diesen Regelungen können Telefonate abgehört, E-Mails überprüft und Telekommunikationsverbindungsdaten gesammelt werden. Beim Einsatz von Mobilfunktelefonen kann auch der Standort des Benutzers festgestellt werden. Diese Regelungen in der StPO haben sich in der polizeilichen Praxis zwar bewährt, zwingende Voraussetzung für ihre Anwendung ist aber immer das Vorliegen eines qualifizierten Anfangsverdachts im Sinne des § 152 Abs. 2 StPO. Das bedeutet, dass Überwachungsmaßnahmen der Telekommunikation nach der StPO nur dann durchgeführt werden können, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine bestimmte, katalogartig erfasste Straftat begangen hat. Erst dann können Überwachungsmaßnahmen der Telekommunikation nach der StPO durchgeführt werden.

Da sich die Kommunikationsmöglichkeiten in den letzten Jahren grundlegend verändert - insbesondere erweitert - haben, können immer mehr Menschen unabhängig von ihrem Standort und ihrer momentan ausgeführten Tätigkeit weltweit miteinander kommunizieren. Da die modernen Kommunikationstechnologien zunehmend auch von Straftätern - insbesondere aus den Bereichen des Terrorismus und der Organisierten Kriminalität - genutzt werden, ist es zur Gewährleistung einer effektiven Gefahrenabwehr dringend erforderlich, dass die Polizei Befugnisse zur Durchführung der Telekommunikationsüberwachung zu präventiven Zwecken erhält. Dies erscheint insbesondere vor dem Hintergrund, dass unter bestimmten Voraussetzungen zwar das Abhören von Gesprächen in Wohnungen im Gefahrenabwehrbereich zulässig ist, die weniger einschneidende Überwachung der Telekommunikation jedoch nicht, geboten.

Auch der AK II der IMK hat sich bereits auf seiner Sitzung am 5./6. November 2002 mit der Notwendigkeit der Telekommunikationsüberwachung befasst und befunden, dass Regelungen zur präventiven Telekommunikationsüberwachung in allen Bundesländern erforderlich sind. Denn das Fehlen entsprechender Befugnisse im polizeilichen Gefahrenabwehrrecht führt zu dem unbefriedigenden Zustand, dass nach dem bisher geltenden Recht zwar Straftaten effektiv verfolgt, nicht aber entsprechend effektiv verhindert werden können und der Schutz der Bevölkerung somit nicht angemessen gewährleistet ist.

In Mecklenburg-Vorpommern ist die Polizei bisher nicht befugt, Telekommunikationsüberwachungsmaßnahmen zu präventiven Zwecken durchzuführen. Die polizeiliche Praxis im Land hat jedoch deutlich werden lassen, dass diese Maßnahmen ein unverzichtbares Mittel zur Gefahrenabwehr darstellen. So leistet beispielsweise die Möglichkeit der Ortung von Mobilfunkbenutzern bereits heute schon bei Unglücksfällen, bei Suizidankündigungen sowie bei der Fahndung und Lokalisierung von Vermissten (Kinder, hilflose Personen, die ärztlicher Hilfe bedürfen usw.) einen oftmals lebensrettenden Fahndungsansatz. Begünstigend trägt der Umstand dazu bei, dass Mobiltelefone im Zuge des technologischen Fortschritts mit steigender Tendenz Verbreitung in allen Bevölkerungsgruppen finden. Gestützt wurden diese Maßnahmen der Ortung in Unglücksfällen bisher auf § 34 StGB, der grundsätzlich auch auf staatliches Handeln anwendbar ist. Eine Heranziehung des § 34 StGB kommt aber nur dort in Betracht, wo ein atypischer Interessenkonflikt vorliegt, der für den Gesetzgeber aufgrund seiner Ungewöhnlichkeit nicht vorhersehbar ist oder seiner Natur nach einer abstrakt-generellen Regelung nicht zugänglich ist. Es muss sichergestellt sein, dass § 34 StGB nur in ganz außergewöhnlichen Konstellationen angewendet wird. In den vergangenen Jahren ist eine Vielzahl von Fällen verzeichnet worden, in denen suizidgefährdete Personen aufgrund von Mobilfunkortung ausfindig gemacht wurden. Eine Rechtfertigung über § 34 StGB ist daher auf lange Sicht nicht möglich. Die Bewältigung solcher Lagen muss auf eine spezifische Rechtsgrundlage gestellt werden.

Darüber hinaus ist die Möglichkeit der präventiven Telekommunikationsüberwachung ein wichtiger Schritt zur wirkungsvollen und nachhaltigen Bekämpfung des internationalen Terrorismus und der Organisierten Kriminalität. So hat sich die Sicherheitslage in Europa seit den Anschlägen am 11. September 2001 in New York, dem Attentat am 11. März 2004 in Madrid und den Londoner Anschlägen am 7. Juli 2005 grundlegend gewandelt. Neben der globalen Bedrohung durch den internationalen Terrorismus stellt auch die Bekämpfung der grenzüberschreitenden Organisierten Kriminalität die europäischen Sicherheitsbehörden vor neue Herausforderungen. Diese Erscheinungsformen der Kriminalität sind von einem hohen Maß an Konspirativität geprägt. Gleichzeitig können sie auf einen technisch hoch entwickelten Unterstützungsapparat zurückgreifen. Die bisherigen polizeilichen Befugnisse genügen nicht, um den neuen Bedrohungen effektiv zu begegnen. Die Erforschung der Strukturen terroristischer Netzwerke und der Organisierten Kriminalität gerät oft schnell an ihre Grenzen, da ein Einschleusen von Kräften der Sicherheitsbehörden in die Tätergruppen vielfach unmöglich ist. Die Polizei stößt bei ihrer Ermittlungsarbeit in vielen Fällen auf weit verzweigte internationale Strukturen und Netzwerke, auf abgeschottete Gruppen, die modernste Kommunikationsmittel nutzen. Häufig können die Straftäter im Verborgenen agieren, sodass es für die Polizei nach bisheriger Rechtslage schwierig ist, einen Anfangsverdacht für die Einleitung von Telekommunikationsüberwachungsmaßnahmen nach den Maßgaben der StPO zu begründen. Die Ermittlungen müssen oft überhaupt erst grundsätzliche Erkenntnisse über Zusammenhänge, Methoden und Kontakte erbringen, bevor gegen bestimmte Personen vorgegangen werden kann. Ein frühzeitiges Eindringen in diese Organisationen mit dem Ziel der Informationsbeschaffung und -auswertung ist für die Gefahrenabwehr von elementarer Bedeutung. Um Bedrohungslagen rechtzeitig erkennen und Straftaten verhüten zu können, ist es erforderlich, der Polizei Instrumente, die ihr zu Zwecken der Strafverfolgung bereits seit geraumer Zeit zur Verfügung stehen, im Gefahrenabwehrbereich zur Verfügung zu stellen.

Mit dem § 34a wird daher nunmehr eine Rechtsgrundlage für die polizeilichen Maßnahmen der Telekommunikationsüberwachung und -aufzeichnung, der Verkehrsdatenabfrage, der Standortermittlung sowie der Verbindungsunterbrechung und -verhinderung der Telekommunikation geschaffen. Damit wird ein Maßnahmenkatalog geschaffen, der der Polizei in Mecklenburg-Vorpommern eine effektive Gefahrenabwehr ermöglichen soll.

Bei der Schaffung einer Regelung zur präventiven Telekommunikationsüberwachung war jedoch zu beachten, dass die berechtigten Schutzinteressen der Allgemeinheit und der Schutz der Grundrechte der Betroffenen in Einklang gebracht werden. Insbesondere Berücksichtigung fand die Entscheidung des Bundesverfassungsgerichtes vom 27. Juli 2005 (1 BvR 668/04) über die sich gegen § 33a Abs. 1 Nr. 2 und 3 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) und damit gegen die Ermächtigung der Polizei, personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation zur Vorsorge für die Verfolgung und zur Verhütung einer Straftat von erheblicher Bedeutung zu erheben, richtende Verfassungsbeschwerde. In seinem Urteil kommt das Bundesverfassungsgericht zu dem Schluss, dass die angegriffenen Regelungen formell verfassungswidrig sind, weil

- im Änderungsgesetz der nach Art. 19 Abs. 1 Satz 2 GG (Zitiergebot) erforderliche Hinweis auf die Einschränkung des Artikel 10 Abs. 2 Satz 1 GG (Fernmeldegeheimnis) fehlt und
- der niedersächsische Gesetzgeber die Regelungen nicht nur auf die Verhütung von Straftaten beschränkt, sondern in § 33a Abs. 1 Nr. 2 und 3 Nds. SOG auch die Vorsorge für die Verfolgung von Straftaten als eigenständiges Tatbestandsmerkmal vorgesehen hat. Der Sachbereich der Verfolgungsvorsorge gehört zum gerichtlichen Verfahren im Sinne des Artikel 74 Abs. 1 Nr. 1 GG und daher zur konkurrierenden Gesetzgebung. Von der konkurrierenden Gesetzgebung zur Strafverfolgung hat jedoch der Bundesgesetzgeber im Bereich der Telekommunikation abschließend Gebrauch gemacht, sodass der niedersächsische Gesetzgeber seine Gesetzgebungskompetenz überschritten hat.

Das Bundesverfassungsgericht hält die angegriffenen Normen auch in materieller Hinsicht für nicht mit der Verfassung vereinbar, weil

- die Ermächtigungen des § 33a Abs. 1 Nr. 2 und 3 Nds. SOG dem Bestimmtheitsgebot nicht gerecht werden. Insbesondere enthält das Gesetz keine einschränkenden Tatbestandsmerkmale, die die - gerade im Bereich der Vorfeldermittlung schwierige - Abgrenzung eines harmlosen von dem in einer Straftatenbegehung mündenden Verhaltens ermöglichen. Zudem sind die Regelungen zur Überwachung von Kontakt- und Begleitpersonen nicht hinreichend bestimmt.
- die angegriffenen Normen nicht den Anforderungen genügen, die der Verhältnismäßigkeitsgrundsatz an die Angemessenheit eines grundrechtsbeschränkenden Gesetzes im Sinne von Art. 10 Abs. 1 Satz 2 GG stellt. Da das Gesetz keine näher eingegrenzten Tatsachen enthält, die die Annahme einer künftigen Straftat rechtfertigen, kann der schwere Eingriff in die Telekommunikationsüberwachung nur dann als angemessen bewertet werden, wenn der zu schützende Gemeinwohlbelang überragend wichtig ist. Zudem trägt das Tatbestandsmerkmal der „Straftaten von erheblicher Bedeutung“ den Anforderungen an das besondere Gewicht des zu verfolgenden Rechtsguts nicht Rechnung.
- das Gesetz keine hinreichenden Vorkehrungen zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung enthält.

Der Landesgesetzgeber besitzt nach der Entscheidung des Bundesverfassungsgerichtes somit zwar keine Kompetenz zur Schaffung einer Telekommunikationsüberwachungsregelung zur Vorsorge für die spätere Verfolgung von Straftaten, jedoch liegt die Verhütung einer Straftat in der Gesetzgebungskompetenz der Länder für die Gefahrenabwehr, und zwar auch dann, wenn sie vorbeugend für den Zeitraum vor dem Beginn einer konkreten Straftat vorgesehen wird. Schafft der Landesgesetzgeber in diesem Kompetenzbereich eine Befugnisnorm zur Telekommunikationsüberwachung, so ist der schwere Eingriff in das Telekommunikationsgeheimnis nach der Entscheidung des Bundesverfassungsgerichtes nur zulässig, wenn er sich auf den Schutz besonders hochrangiger Rechtsgüter bezieht und beschränkt sowie eine durch konkrete Anhaltspunkte gekennzeichnete Lage gegeben ist, die auf einen unmittelbaren Bezug zur künftigen Begehung der Straftat schließen lässt. Erforderlich sind dann Regelungen zur Sicherung, dass Kommunikationsinhalte des höchstpersönlichen Bereiches nicht verwertet werden dürfen und dass sie unverzüglich zu löschen sind, wenn es ausnahmsweise zu ihrer Erhebung gekommen sein sollte.

Die nunmehr geschaffene polizeiliche Befugnisnorm zur Datenerhebung durch Telekommunikationsüberwachungsmaßnahmen orientiert sich ebenso wie die verfahrensrechtlichen Sicherungen an den verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht in seiner Entscheidung vom 27. Juli 2005 aufgezeigt hat, als auch an den datenschutzrechtlichen Erfordernissen.

Zu den Regelungen im Einzelnen

Zu Absatz 1

Absatz 1 regelt die Erhebung personenbezogener Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation. Der Begriff Telekommunikation ist bereits in § 3 Nr. 22 Telekommunikationsgesetz definiert. Danach ist Telekommunikation der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen.

Satz 1 ermächtigt die Polizei, personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation zu erheben über die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes erforderlich ist (Absatz 1 Nr. 1). Der schwere Eingriff in das Telekommunikationsgeheimnis ist demnach nur zulässig, wenn er sich auf den Schutz besonders hochrangiger Rechtsgüter bezieht und beschränkt. Zudem muss eine im einzelnen Falle bevorstehende Gefahr - also eine Sachlage, bei der bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens ein die öffentliche Sicherheit der Ordnung schädigendes Ereignis im konkreten Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit eintreten wird, - für die genannten Rechtsgüter gegeben sein (vgl. Legaldefinition in § 3 Abs. 3 Nr. 1).

Des Weiteren ist die Polizei auch zur Datenerhebung - insbesondere solcher der Standortkennung einer Mobilfunkeinrichtung (vgl. Abs. 2) - durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation befugt über Personen, wenn deren Leben oder Gesundheit gefährdet ist (Absatz 1 Nr. 2). Damit wird die bisher fehlende eindeutige polizeiliche Rechtsgrundlage geschaffen, um u. a. bei Unglücksfällen, bei Suizidankündigungen sowie bei der Fahndung und Lokalisierung von Vermissten (Kinder, hilflose Personen, die ärztlicher Hilfe bedürfen usw.) unter Nutzung technischer Mittel einen oftmals lebensrettenden Fahndungsansatz zu gewährleisten.

Nur unter diesen jeweils in Nummer 1 oder 2 festgelegten Voraussetzungen und wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre, ist der Eingriff in die Grundrechte - insbesondere in das Fernmeldegeheimnis des Artikel 10 GG - der Betroffenen durch Telekommunikationsüberwachungsmaßnahmen gerechtfertigt. Die Polizei muss sich also in einem so genannten „Ermittlungsnotstand“ befinden, bevor die Maßnahmen nach Satz 1 zulässig sind. Auf welche Bereiche sich die Datenerhebung konkret beziehen kann, ist in Absatz 2 normiert (s. u.).

Darüber hinaus wird mit Satz 3 sichergestellt, dass personenbezogene Daten Dritter im Rahmen von Telekommunikationsüberwachungsmaßnahmen nur erhoben werden dürfen, wenn dies aus technischen Gründen unvermeidbar ist. Zum Schutz der Rechte Dritter enthält Absatz 8 Satz 4 (s. u.) die Verpflichtung, dass erhobene personenbezogene Daten Dritter unverzüglich nach Beendigung der Maßnahme zu löschen sind.

Ein Eingriff in das Beichtgeheimnis ist durch den Verweis auf § 33 Abs. 6 SOG MV unzulässig. Durch den Verweis unterliegt die Telekommunikationsüberwachung bezüglich mittels Amts- oder Berufsgeheimnis geschützter Vertrauensverhältnisse besonderen Anforderungen (Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person).

Zu Absatz 2

Absatz 2 benennt die für die polizeiliche Gefahrenabwehr bedeutungsvollen drei Bereiche, auf die sich eine Datenerhebung nach Absatz 1 beziehen kann.

Zum einen kann die Polizei Gespräche zwischen zwei Personen überwachen. Eine solche Maßnahme richtet sich in erster Linie auf die Gesprächsinhalte. Gleichzeitig werden bei dieser Überwachung auch automatisch Verkehrsdaten an die Polizei übermittelt. Die Ermittler erhalten so genaue Informationen über den Inhaber des Anschlusses.

Zum anderen können auch Mailboxen überprüft werden, die in einem Datenspeicher innerhalb des Telekommunikationsnetzes abgelegt werden.

Ein dritter Bereich der Telekommunikationsüberwachung ist die Ortung eines Mobilfunktelefons. Das Mobiltelefon nimmt automatisch Verbindung zu der nächstgelegenen Funkzelle auf. Bei der Überwachung des Mobiltelefons ist daher auch immer der (zumindest ungefähre) Standort des Benutzers bekannt bzw. ermittelbar. Dies gilt sowohl für den Fall, dass mit dem Mobiltelefon ein Gespräch geführt wird, als auch für den Fall, dass sich das Mobiltelefon lediglich im Stand-By-Modus befindet. Die polizeilichen Erfahrungen mit telefonisch angekündigten Suizidabsichten zeigen, dass eine schnelle Standortbestimmung unerlässlich ist, um den Suizidgefährdeten von seiner Tat abzuhalten.

Auch die Ortung hilfloser Personen, die verunglückt sind und sich nicht mehr über ihren genauen Standort äußern können oder vermisster Kinder, ist mittels Standortermittlung von ggf. mitgeführten Mobiltelefonen möglich.

Zu Absatz 3

Die Polizei wird ebenfalls ermächtigt, zur Vorbereitung einer Maßnahme nach Absatz 1 technische Mittel einzusetzen, um die Geräte- und Kartennummer eines Mobilfunkendgerätes zu ermitteln, wenn die Durchführung der Maßnahme ohne die Ermittlung der Geräte- oder Kartennummer unmöglich oder wesentlich erschwert wäre.

Der Einsatz von Geräten, wie etwa des so genannten „IMSI-Catchers“, die zur Bestimmung der Geräte- und Kartennummer von Mobiltelefonen dienen, wird damit zur Vorbereitung einer Telekommunikationsüberwachungsmaßnahme nach Absatz 1 für polizeilich-präventive Zwecke möglich.

Für die richterliche Anordnung ist gem. § 34a Abs. 4 bei Mobiltelefonen zumindest die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses anzugeben. Die Erfahrungen aus der polizeilichen Praxis zeigen die Notwendigkeit der Überwachung von Mobiltelefonen. Sie ergibt sich aus der Tatsache, dass zur Vorbereitung bzw. Durchführung terroristischer Anschläge bzw. im Bereich der Organisierten Kriminalität zunehmend Mobiltelefone genutzt werden, deren Herkunft nicht bekannt ist, sodass die Rufnummer nur mittels eines technischen Gerätes - wie z. B. dem „IMSI-Catcher“ - zu ermitteln ist. Daneben agieren die Täter häufig auch mit mehreren Chipkarten, was die Ermittlungen zusätzlich erschwert und den Einsatz von technischen Geräten zur Ermittlung der Geräte- und Kartennummer eines Mobiltelefons erforderlich macht.

Mit Hilfe eines Gerätes wie z. B. dem „IMSI-Catcher“ lässt sich die so genannte International Mobile Subscriber Identity (IMSI) eines Handys und damit letztlich den Anschlussinhaber eines Mobiltelefons feststellen. Bei der IMSI handelt es sich um eine weltweit eindeutige Kennung, die den Teilnehmer - Vertragspartner eines Netzbetreibers - eindeutig identifiziert und die auf der Chipkarte (sog. SIM-Karte) gespeichert ist, die der Mobilfunkteilnehmer bei Abschluss eines Vertrages erhält.

Der Gesetzentwurf schafft darüber hinaus die Rechtsgrundlage für eine Verbindungsunterbrechung bzw. -verhinderung durch den Einsatz technischer Mittel. Mit dieser Maßnahme sollen Telekommunikationsverbindungen unter den Voraussetzungen des Absatzes 1 Nr. 1 - und damit nur zur Abwehr von einer im einzelnen Falle bevorstehenden Gefahr für die dort genannten besonders hochrangigen Rechtsgüter - unterbrochen und künftige Verbindungen verhindert werden. So kann z. B. über ein Mobiltelefon der Zündmechanismus einer Bombe ausgelöst werden. Darüber hinaus kann potenziellen Straftätern die Planung und Durchführung ihrer Vorhaben wesentlich erschwert werden. Die Polizei kann so die nötige Zeit gewinnen, um andere Maßnahmen zu ergreifen, mittels derer die Gefahr endgültig beseitigt werden kann.

Die Unterbrechung oder Verhinderung der Kommunikationsverbindung wird auch gegenüber Dritten ermöglicht. Wegen des dadurch entstehenden erheblichen Grundrechtseingriffs ist dies aber nur zur Abwehr einer gegenwärtigen Gefahr zulässig. Der Begriff der gegenwärtigen Gefahr ist bereits in § 3 Abs. 3 Nr. 2 legal definiert.

Zu Absatz 4

Absatz 4 enthält die verfahrensrechtlichen Anforderungen. Die Maßnahmen nach den Absätzen 1 oder 3 stehen danach wegen der hohen Bedeutung des Fernmeldegeheimnisses unter einem richterlichen Anordnungsvorbehalt. Nur in Ausnahmefällen, nämlich bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person, darf die Maßnahme durch den Behördenleiter angeordnet werden; eine richterliche Entscheidung ist in diesem Fall jedoch unverzüglich nachzuholen.

Die Anordnung ist schriftlich zu erlassen und hat Namen und Anschrift des Betroffenen oder die Rufnummer oder eine andere Kennung des betroffenen Telekommunikationsanschlusses zu enthalten. Eine Verbindung von Namen und Anschrift des Betroffenen sowie der entsprechenden Rufnummer (oder einer anderen Kennung des Anschlusses) entsprechend der diesbezüglichen Regelungen in der StPO ist nicht vorgesehen. Die gewählte Alternativregelung basiert auf folgender Überlegung: Das Erfordernis Namen, Anschrift und auch Rufnummer des Betroffenen angeben zu müssen, kann in Fällen präventiver Telekommunikationsüberwachung nicht zielführend und unter Umständen sogar äußerst hinderlich sein. So dürften bei gefordertem Vorliegen von Namen, Anschrift und Rufnummer der Standort eines Verunglückten, der per Mobiltelefon einen Hilferuf an die Polizei abgibt ggf. nicht ermittelt werden, wenn der Verunglückte nicht mehr in der Lage ist, seinen Namen zu nennen. Ähnliche Fälle sind bei Suizidankündigungen, in denen die betroffene Person ihren Namen nicht nennt, denkbar. Der Polizei wäre in solchen Fällen nur die angezeigte Rufnummer des Telefons bekannt.

Die in Absatz 4 enthaltene Regelung zur Befristung der Maßnahmen orientiert sich an den entsprechenden Regelungen zur Telekommunikationsüberwachung im strafprozessualen Bereich. Die Dreimonatsfrist stellt eine Höchstfrist dar. Die volle Ausschöpfung der Frist wird in der Regel bei der Unterbrechung oder Verhinderung der Telekommunikation wegen der erheblichen Eingriffsintensität und des mit der Maßnahme verfolgten Zweckes nicht angemessen sein. Bei diesen Maßnahmen wird die Anordnung daher grundsätzlich mit einer wesentlich geringeren Frist zu versehen sein. Zudem wird die Möglichkeit der Verlängerung der in der Anordnung gesetzten Frist um nicht mehr als jeweils weitere drei Monate unter der Bedingung, dass die Maßnahmevoraussetzungen weiterhin vorliegen, geschaffen.

Zu Absatz 5

Absatz 5 stellt klar, dass Auskunftersuchen der Polizei auch über einen zurückliegenden Zeitraum möglich sind. Diese Maßnahme bedarf ebenfalls der richterlichen Anordnung (vgl. Absatz 4).

Welche Daten durch den Diensteanbieter erhoben und über welche Zeitspanne und in welcher Form diese gespeichert werden dürfen, bestimmt sich nach dem Telekommunikationsgesetz (TKG) und der Telekommunikationsdatenschutzverordnung (TDSV). § 7 Abs. 3 TDSV lässt derzeit die Speicherung bestimmter Verbindungsdaten für bis zu sechs Monate nach Rechnungslegung zu.

Zu Absatz 6

Absatz 6 regelt die Mitwirkungspflichten derjenigen, die geschäftsmäßig Telekommunikationsdienstleistungen erbringen oder daran mitwirken (Diensteanbieter). Der Absatz enthält einen Verweis auf die Regelungen des TKG und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung, da darin detailliert geregelt ist, inwiefern die Diensteanbieter Vorkehrungen zu treffen haben, um der Polizei die erforderlichen Auskünfte erteilen zu können.

Die Diensteanbieter haben einen Anspruch auf Entschädigung der ihnen aus Anlass der präventiv-polizeilichen Telekommunikationsüberwachung entstandenen Kosten. Sie richtet sich, wie die Entschädigung für eine strafprozessuale Maßnahme, nach § 23 des Justizvergütungs- und Entschädigungsgesetzes (JVEG).

Zu Absatz 7

Absatz 7 enthält Regelungen zur Unterrichtung der durch die Maßnahmen nach § 34a Betroffenen. Grundsätzlich hat die Unterrichtung der Betroffenen nach Abschluss der Maßnahme zu erfolgen, sobald dies ohne Gefährdung des Zwecks der Maßnahme möglich ist. Wird nach Prüfung eine Gefährdung des Maßnahmensezwecks auch sechs Monate nach Beendigung der Maßnahme immer noch angenommen, ist für eine über diesen Zeitraum hinausgehende Zurückstellung der Unterrichtung die richterliche Zustimmung einzuholen. Die richterliche Zustimmung ist erneut nach Ablauf von jeweils weiteren sechs Monaten einzuholen.

Satz 4 eröffnet die Möglichkeit des Hinausschiebens der Unterrichtung, wenn sich an den die präventive Telekommunikationsüberwachung auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren gegen einen Betroffenen anschließt. Die Unterrichtung ist in diesem Fall jedoch in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Es gelten die Regelungen der StPO.

Das Unterbleiben der Unterrichtung einer anderen von der Maßnahme nach § 34a betroffenen Person - nicht die von der Maßnahme betroffene Person selbst - wird mit richterlicher Zustimmung ausnahmsweise zugelassen, wenn deren Unterrichtung nur mit unverhältnismäßigen Ermittlungen möglich wäre oder wenn ihr überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen.

Mit Satz 6 wird klargestellt, dass die im § 34 Abs. 3 Satz 3 bis 5 bereits enthaltenen Verfahrensvorschriften über die gerichtliche Zuständigkeit und das Verfahren beim Einsatz besonderer Mittel der Datenerhebung auch für das Unterrichtungsverfahren - mit Ausnahme des in Satz 4 des Absatzes 7 dargestellten Falles - für Maßnahmen nach § 34a entsprechend gelten.

Zu Absatz 8

In Absatz 8 wird das Kennzeichnungsgebot der durch die Telekommunikationsmaßnahmen erlangten personenbezogenen Daten geregelt. Die Kennzeichnung dieser Daten dient der Gewährung der Zweckbindung, da auf diese Weise sichergestellt wird, dass auch nach der Informationserhebung erkennbar bleibt, dass es sich um entsprechend sensible Daten handelt.

Eine Zweckänderung der im Rahmen einer Telekommunikationsmaßnahme erlangten personenbezogenen Daten ist nur unter engen Voraussetzungen zugelassen. So wird die Verwendung der Daten zu dem Zweck der Verfolgung von Straftaten, die nach der StPO die Überwachung und Aufzeichnung der Telekommunikation rechtfertigen, ermöglicht. In diesem Fall ist eine formale Feststellung in Form einer Dokumentation erforderlich.

Gemäß § 34a Absatz 1 dürfen personenbezogene Daten Dritter nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zweckes unvermeidbar ist. Zum Schutz der Rechte Dritte wird in Absatz 8 Satz 4 ausdrücklich die Pflicht aufgenommen, dass solche ausnahmsweise erhobenen Daten nach Beendigung der Maßnahme unverzüglich zu löschen sind.

Da bei der Anordnung bzw. Durchführung einer Telekommunikationsüberwachungsmaßnahme nicht sicher vorhersehbar ist, welchen Inhalt die Gespräche haben werden, ist das Risiko nicht auszuschließen, dass beim Abhören Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst wird. Unter Beachtung des Urteils des Bundesverfassungsgerichtes vom 27. Juli 2005 wird in Satz 5 der Schutz des absolut geschützten Kernbereiches privater Lebensgestaltung sichergestellt, indem die diesem Bereich zuzuordnenden Daten in keinem Fall verwendet werden dürfen und unverzüglich zu löschen sind, wenn es ausnahmsweise zu ihrer Erhebung gekommen sein sollte.

Es wird zudem klargestellt, dass für die übrigen erlangten personenbezogenen Daten die bereits in § 45 Abs. 2, 3 und 4 Nr.1 und 2 enthaltenen Regelungen zur Löschung und Sperrung Anwendung finden - jedoch mit der zusätzlichen Maßgabe, dass jede vorgenommene Löschung zu dokumentieren ist. Durch den Verweis auf die Regelungen in § 45 tritt in bestimmten Fällen an Stelle der Löschung die Sperrung, sodass die (nachträgliche) Inanspruchnahme von Rechtsschutz möglich ist.

Zu Absatz 9

Bei den Maßnahmen nach § 34a handelt es sich um besondere Mittel der Datenerhebung, sodass die in § 34 Abs. 7 festgelegten Berichtspflichten des Innenministeriums an den Landtag auch für die nach § 34a erfolgten Einsätze technischer Mittel gelten sollen.

Zu Nummer 6 (§ 34b)

Das Bundesverfassungsgericht hat mit Urteil vom 3. März 2004 - 1 BvR 2378/98, 1 BvR 1084/99 - die Schaffung einer verfassungsrechtlichen Grundlage für die akustische Wohnraumüberwachung zur Strafverfolgung in Art. 13 Abs. 3 Grundgesetz für mit der Verfassung im Einklang erklärt. Die Regelungen der Strafprozessordnung, die die Grundgesetzänderung einfachgesetzlich umsetzen, wurden jedoch teilweise für verfassungswidrig erklärt.

Das Urteil des Bundesverfassungsgerichtes betrifft zunächst nur die Verfassungsmäßigkeit der Bestimmungen der §§ 100c ff. StPO. Dennoch ergibt sich aus der Urteilsbegründung gesetzlicher Änderungsbedarf hinsichtlich der Ausgestaltung der präventiven Wohnraumüberwachung. Die Ausführungen des Bundesverfassungsgerichts zu den grundrechtlichen Schranken der Maßnahmen beruhen im Wesentlichen auf der Auslegung des Grundrechts der Menschenwürde gemäß Artikel 1 Abs. 1 GG und dem Grundrecht der Unverletzlichkeit der Wohnung gemäß Artikel 13 Abs. 1 GG. Da die vom Bundesverfassungsgericht untersuchte Problematik der Gemengelage unterschiedlicher Gesprächsinhalte und Verhaltensweisen jeder Wohnraumüberwachung immanent ist und sich nicht nur auf Artikel 13 Abs. 3 GG, sondern auch auf Artikel 13 Abs. 4 (Wohnraumüberwachung zur Gefahrenabwehr) GG bezieht, ist die Anerkennung eines absolut geschützten Kernbereichs für die repressive Wohnraumüberwachung in gleicher Weise auch auf die Präventivüberwachung anzuwenden. Mit der Anerkennung eines auch für Präventivüberwachungen absolut geschützten Kernbereichs sind konsequenterweise auch die zur Verwirklichung des Grundrechtsschutzes vom Bundesverfassungsgericht aufgestellten Überwachungs- und Erhebungsverbote sowie Verwertungsverbote und Löschungspflichten zu schaffen.

Um den Grundsätzen des Bundesverfassungsgerichts Rechnung zu tragen, erfolgt die Einführung des § 34b (Wohnraumüberwachung mit technischen Mitteln) sowie eine Anpassung der §§ 33 und 34, die jeweils Regelungen zur Wohnraumüberwachung enthalten. Zum Schutz privater Lebensgestaltung werden Erhebungs-, Überwachungs- und Verwertungsverbote sowie maßnahmenspezifische Löschungspflichten aufgenommen. Weiterhin werden die Verfahrensrechte Betroffener gestärkt. Wesentliche Neuerung ist dabei die Aufnahme einer begleitenden gerichtlichen Kontrolle der Maßnahme, um einen effektiven Rechtsschutz zu gewährleisten.

Aufgrund der Entscheidung des Landesverfassungsgerichts Mecklenburg-Vorpommern vom 18. Mai 2000 wurde die Vorschrift zur Wohnraumüberwachung im SOG M-V bereits anhand des Artikels 13 GG i. V. m. Artikel 5 Abs. 3 der Verfassung des Landes Mecklenburg-Vorpommern auf seine Verfassungsmäßigkeit hin überprüft. Das Landesverfassungsgericht hat in diesem Urteil die Wohnraumüberwachung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person für verfassungsgemäß erachtet. Dementsprechend wurde das SOG M-V durch das Erste Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes vom 24. Oktober 2001 angepasst. Die Problematik, welche Rechtsgüter durch eine Wohnraumüberwachung geschützt werden dürfen, stellte sich daher - im Gegensatz zu einigen anderen Bundesländern - in Mecklenburg-Vorpommern wegen der bereits hierzu getroffenen Entscheidung des Landesverfassungsgerichtes nicht.

Zu den einzelnen Bestimmungen

Zu Absatz 1

Absatz 1 enthält wörtlich die Regelungen des § 33 Abs. 4 Satz 1 und 2, die sich auf die Wohnraumüberwachung beziehen.

Zu Absatz 2

Absatz 2 definiert nach den Vorgaben des Bundesverfassungsgerichtes den absolut geschützten Kernbereich privater Lebensgestaltung, der durch die Maßnahme nicht tangiert werden darf. Es handelt sich hierbei um eine richterliche Prognoseentscheidung, die auf tatsächlichen Anhaltspunkten beruhen muss. Die Polizei hat dabei durch geeignete Maßnahmen im Vorfeld abzuklären, ob solche tatsächlichen Anhaltspunkte vorliegen und diese dem Gericht mitzuteilen. Wesentlich sind hierbei die Art der zu überwachenden Räumlichkeiten und das Verhältnis der anwesenden Personen zueinander. Die Formulierung benennt die maßgeblichen Indikatoren, die sich aus dem Urteil des Bundesverfassungsgerichtes ergeben (Absätze 139 ff., 169 ff.), und anhand derer die Prognose zu erfolgen hat. Der Begriff des Kernbereichs privater Lebensgestaltung ist auslegungsfähig und -bedürftig und muss in Anbetracht des jeweils zu beurteilenden Sachverhaltes erfolgen. Der Schutzbedarf von Räumlichkeiten hängt von ihrer konkreten Nutzung ab. Die Anforderungen an die Rechtmäßigkeit der Maßnahme sind umso höher, je größer die Wahrscheinlichkeit ist, dass mit ihr Gespräche höchstpersönlichen Inhalts erfasst werden. Eine derartige Wahrscheinlichkeit ist beim Abhören von Gesprächen mit Familienangehörigen und sonstigen engsten Vertrauten gegeben. Bei diesem Personenkreis darf eine Überwachung nur erfolgen, wenn konkrete Anhaltspunkte dafür bestehen, dass die Gesprächsinhalte zwischen dem Adressat der Maßnahme und diesen Personen keinen absoluten Schutz erfordern. So gehören Gespräche über begangene Straftaten ihrem Inhalt nach beispielsweise nicht in den Kernbereich privater Lebensgestaltung (BVerfG, aaO Abs. 137). Eine typisierende Betrachtungsweise bei der Einschätzung der als privat anzusehenden Räume wird vom Bundesverfassungsgericht ausdrücklich akzeptiert (BVerfG, aaO Abs. 142). Die in Betriebs- und Geschäftsräumen geführten Gespräche haben i. d. R. Sozialbezug und betreffen nicht den Menschenwürdegehalt des Grundrechts. Anderes gilt regelmäßig für in Privaträumen geführte Gespräche.

Zu Absatz 3

In Absatz 3 wird die Pflicht zur Unterbrechung der Maßnahme normiert. Sie dient dem Schutz des Kernbereichs. Die Überwachungsmaßnahme ist unverzüglich abubrechen, wenn unerwartet (trotz sorgfältiger Prognose) eine Situation eintritt, die den absolut geschützten Kernbereich berührt. Um die Maßnahme jederzeit abbrechen zu können, kann es erforderlich sein, auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, wenn Anhaltspunkte dafür vorliegen, dass die Gefahr einer Erfassung von dem Kernbereich zuzurechnenden Äußerungen eintreten könnte (BVerfG, aaO Abs. 151). Sofern eine derartige Gefahr nicht gegeben ist, ist ein Mithören durch das Überwachungspersonal in Echtzeit hingegen nicht zwingend erforderlich. Aufzeichnungen solcher Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, müssen unverzüglich gelöscht werden.

Etwaige der Vernichtung entgegenstehende Belange des Rechtsschutzes sind nach Auffassung des Bundesverfassungsgerichts unerheblich, da der Menschenwürdebezug der Aufzeichnungen und die daraus folgende Pflicht zur unverzüglichen Vernichtung dieser Belange überwiegt. Das Risiko einer Vertiefung der Persönlichkeitsverletzung (durch eine Sperrung etwa) muss ausgeschlossen werden (BVerfG, aaO Abs. 186). Ferner besteht ein absolutes Verwertungsverbot für solche Aufzeichnungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind (vgl. BVerfG, aaO Abs. 184). Um die nachträgliche Überprüfung der Rechtmäßigkeit der Maßnahme zu gewährleisten, ist die Tatsache der Erfassung der dem Kernbereich zuzurechnenden Äußerungen und die Vernichtung entsprechender Aufzeichnungen zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn die Voraussetzungen des Absatzes 2 vorliegen, d. h. wenn keine tatsächlichen Anhaltspunkte für eine Verletzung des Kernbereichs privater Lebensgestaltung (mehr) vorliegen. Das ist je nach der Sachlage im Einzelfall festzulegen. Anhaltspunkte hierfür können sein, dass bestimmte Personen die betreffende Wohnung verlassen, andere Personen diese betreten oder Gespräche sich räumlich verlagern.

Zu Absatz 4

In Absatz 4 wird die bisher schon für die Wohnraumüberwachung einschlägige Regelung in § 33 Abs. 6 weiterhin für anwendbar erklärt.

Zu Absatz 5

Absatz 5 betrifft die Anordnung der Maßnahme. Neben den bisher geltenden, in § 34 Abs. 4 enthaltenen Regelungen, werden die Anforderungen an den Inhalt der Anordnung präzisiert. Außerdem wird die Regelung ergänzt um eine Frist für die erstmalige Anordnung und eine Frist hinsichtlich der Verlängerungsmöglichkeit. Die Einführung dieser ausdrücklich benannten Fristen dient der Gewährleistung der verfahrensmäßigen Absicherung des Grundrechtsschutzes der Betroffenen. Danach darf die Maßnahme für eine Dauer von höchstens bis zu zwei Monaten angeordnet und jeweils um nicht mehr als einen Monat verlängert werden. Diese Fristen geben einen überschaubaren Zeitrahmen, der den Vorgaben des Bundesverfassungsgerichts genügt (BVerfG, aaO Abs. 281). Bei der Festlegung der Fristen ist auch zu berücksichtigen, dass die Schaffung der technischen Voraussetzungen zur Durchführung der Wohnraumüberwachung schon mehrere Wochen dauern kann.

Zu Absatz 6

Absatz 6 regelt die begleitende Kontrolle durch das anordnende Gericht. Nach der Urteilsbegründung des Bundesverfassungsgerichts (aaO Abs. 279) ist von der Anordnungs-kompetenz des Gerichts auch die Befugnis erfasst, den durchführenden Stellen eine in bestimmten Abständen erfolgende Unterrichtung über den Verlauf der Maßnahme aufzugeben, um gegebenenfalls korrigierend zur Wahrung des Grundrechtsschutzes eingreifen zu können. Diese Befugnis wird nunmehr klarstellend als Verpflichtung der Polizei im Gesetz geregelt. Zwecks Einhaltung des Verwertungsverbot wird geregelt, dass die Polizei eine Entscheidung des Gerichts herbeizuführen hat, soweit ein Verwertungsverbot in Betracht kommt.

Hiermit wird der Forderung des Bundesverfassungsgerichts Rechnung getragen, das die Prüfung der Verwertbarkeit von erlangten Informationen durch eine unabhängige Stelle verlangt (BVerfG aaO Abs. 194). Für das Gefahrenabwehrrecht ist diese Pflicht allerdings zu modifizieren. Eine Pflicht zur richterlichen Überprüfung aller erlangten Informationen würde dem Grundsatz der effektiven Gefahrenabwehr zuwiderlaufen und kann daher nur bei der Strafverfolgung zur Anwendung gelangen. Im Bereich der Wohnraumüberwachung zur Gefahrenabwehr gilt es, die Realisierung der Gefahr für hochrangige Schutzgüter zu verhindern. Hier verbleibt möglicherweise zu wenig Zeit, um alle Informationen vor ihrer Verwendung auf ihre Verwertbarkeit gerichtlich überprüfen zu lassen. Diesen Unterschieden trägt auch Art. 13 mit dem Aufstellen unterschiedlich strenger Voraussetzungen für die repressive und die präventive Wohnraumüberwachung Rechnung. Im Übrigen ist durch die Unterrichtung des Gerichts über den Verlauf der Maßnahme und die Ergebnisse eine ständige Kontrolle gewährleistet, das Gericht kann jederzeit Anordnungen treffen.

Zu Absatz 7

Absatz 7 regelt die Kennzeichnungspflicht der durch die Wohnraumüberwachung erlangten personenbezogenen Daten. Diese Kennzeichnung ist auch nach Übermittlung der Daten aufrecht zu halten. Dadurch wird sichergestellt, dass die Herkunft der Daten, der Zweck ihrer Erhebung erkennbar bleiben. Eine Zweckänderung ist nur unter engen Voraussetzungen möglich. Hierfür ist eine formale Feststellung in Form einer Dokumentation erforderlich.

Zu Absatz 8

Absatz 8 hat die Pflicht zur Benachrichtigung der Betroffenen von der Wohnraumüberwachung zum Regelungsgegenstand. Sie wurde entsprechend der Regelungen zur Unterrichtung über die Telekommunikationsüberwachung in § 34a Abs. 7 abgefasst. Auf die Ausführungen in der dortigen Begründung wird verwiesen. Nach Satz 6 kann von der Benachrichtigung der Gäste oder anderer Personen, die sich zufällig in der überwachten Wohnung befunden haben, abgesehen werden. Der Grundrechtseingriff bei der in erster Linie betroffenen Zielperson der Maßnahme soll nicht noch weiter vertieft werden, wenn die Überwachung keine verwertbaren Erkenntnisse erbracht hat. Diese Vorgabe folgt den Ausführungen des Bundesverfassungsgerichts (aaO Abs. 297).

Zu Absatz 9

Absatz 9 regelt durch Verweis die Berichtspflichten des Innenministeriums an den Landtag.

Zu Nummer 7 (§ 40)

Die in Absatz 4 vorgesehene Verwaltungsvorschrift wurde bisher nicht erlassen und ist auch nicht notwendig. Grundlage der Datenübermittlung an ausländische Polizeidienststellen sind die entsprechenden völkerrechtlichen Abkommen, die unmittelbar geltendes Recht sind. Eine Aufzählung aller ggf. betroffenen Polizeidienststellen der Vertragsstaaten, wie sie die Regelung in § 40 bisher vorsieht, ist nicht sinnvoll, da sich die Rechtslage fortentwickelt und zudem der jeweilige Übermittlungsweg (direkt oder über zentrale Dienststellen) zu berücksichtigen ist.

Zu Nummer 8 (§ 42)

Mit der vorgesehenen Änderung wird eine Angleichung der Begrifflichkeiten des SOG an die des Landesdatenschutzgesetzes (hier insbesondere § 18) erreicht.

Zu Nummer 9 (§ 43a)

Mit dem Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen (AKLS) wird das polizeiliche Ziel verfolgt, Kennzeichen von Kraftfahrzeugen zu erfassen und diese online mit Hilfe von Datenbanken abzugleichen oder die erfassten Kennzeichendaten erst für spätere Recherchen zu speichern. Durch die automatische Erfassung von Kraftfahrzeugkennzeichen und den Abgleich dieser mit vorhandenen Datenbeständen wird z. B. eine wirksame Kontrolle des fließenden und ruhenden Verkehrs u. a. an Grenzübergängen, an so genannten gefährdeten Objekten oder gefährlichen Orten erwartet.

Die Erfassung von Kennzeichendaten und deren Abgleich mit vorhandenen Datenbeständen stellt keine grundsätzlich neue polizeiliche Methode dar. Das gestiegene Verkehrsaufkommen sowie die steigende Anzahl von zur Fahndung ausgeschriebenen Kraftfahrzeugen und die Ausweitung der zur Verfügung stehenden Fahndungsdaten durch den Zugriff auf das Schengener Informationssystem erfordern jedoch eine Optimierung der polizeilichen Aufgabenerfüllung. Da es sich bei AKLS um eine neue Möglichkeit für technisch unterstützte Fahndungsmaßnahmen handelt, liegt es auf der Hand, dass durch deren Einsatz eine Verbesserung bei der polizeilichen Aufgabenerfüllung eintreten wird.

Der Einsatz solcher Systeme ist nach geltendem Recht jedoch nur im eingeschränkten Umfang im repressiven Bereich möglich. Nach einem Prüfbericht des UA RV, der vom AK II am 6./7. Mai 2004 zustimmend zur Kenntnis genommen wurde, bedarf es für den Einsatz des AKLS im präventiv-polizeilichen Bereich der Schaffung einer speziellen Eingriffsnorm im jeweiligen Polizei- bzw. Sicherheitsgesetz eines Bundeslandes.

Einige Bundesländer haben sich bereits für den Einsatz von AKLS im präventiv-polizeilichen Bereich entschieden und die Schaffung von speziellen Eingriffsbefugnissen in ihren Polizei- bzw. Sicherheitsgesetzen vorgenommen oder beabsichtigen diese.

Im Sicherheits- und Ordnungsgesetz des Landes Mecklenburg-Vorpommern gibt es zum Einsatz von AKLS bisher keine spezielle Befugnisnorm. Mit der Aufnahme des § 43a soll diese spezielle Regelung nunmehr geschaffen werden, da das geltende Recht den Einsatz von AKLS bisher in nur sehr eingeschränktem Umfang ermöglicht:

So ist in der zurzeit geltenden Fassung des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern bereits ein Abgleich erlangter personenbezogener Daten mit dem Fahndungsbestand gem. § 43 Abs. 1 Satz 3 möglich, jedoch ist dieser Abgleich an die Voraussetzung geknüpft, 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 Ordnungswidrigkeit - etwa einer Geschwindigkeitsüberschreitung - erhoben wurden. Die Vorschrift ermöglicht jedoch z. B. keinen Abgleich von Kennzeichen, die an einem Grenzübergang, einer Kontrollstelle vor einem besonders gefährdeten Objekt erhoben worden sind, da hier das Kennzeichen allein zum Zweck des Datenabgleichs erfasst und daher nicht im Rahmen der Aufgabenerfüllung der Polizei erlangt worden wäre. Auch § 32 lässt einen Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen zu, jedoch wird die Erfassung von Kennzeichendaten allein zum Zwecke des Abgleichs mit dem Fahndungsbestand oder ggf. anderen Dateien von § 32 nicht - auch nicht in Verbindung mit § 43 - erfasst.

Vor diesem Hintergrund wird jetzt mit dem neu in das Gesetz eingefügten § 43a eine ausreichende rechtliche Grundlage für den Einsatz von AKLS zum Zwecke des Datenabgleichs in Mecklenburg-Vorpommern geschaffen. Bei der Schaffung der speziellen Befugnisnorm fand vor allem Folgendes Beachtung:

AKLS sind technische Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen und damit besondere Mittel der Datenerhebung. Mit der Erhebung von Kraftfahrzeugkennzeichen mittels AKLS wird erfasst, dass sich das Fahrzeug einer bestimmten Person zu einer bestimmten Zeit an einem bestimmten Ort befindet. Da sich aus dem Kraftfahrzeugkennzeichen u. a. der Halter des Fahrzeugs ohne Weiteres bestimmen lässt, werden mithin personenbezogene Daten erhoben. Der Einsatz von AKLS stellt daher einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG dar.

Eingriffe in das Recht auf informationelle Selbstbestimmung sind nur zulässig, wenn diese im überwiegenden Allgemeininteresse erfolgen und dem rechtsstaatlichen Gebot der Normenklarheit und Normenbestimmtheit sowie dem Grundsatz der Verhältnismäßigkeit genügen. Soweit daher ein Gesetzgeber einen Eingriff in die grundrechtlich geschützten Freiheiten normiert, hat er einen angemessenen Ausgleich zwischen Allgemein- und Individualinteressen herbeizuführen. Bei der Schaffung von Ermächtigungen zu Überwachungsmaßnahmen ist mithin zu beachten, dass diese Maßnahmen nur dann durchgeführt werden können, wenn zwingende Gründe des Allgemeinwohls dies erfordern. Mit Blick auf den Freiheitsanspruch des Einzelnen ist dieser von polizeilichen Maßnahmen zu verschonen, die nicht durch eine hinreichende Beziehung zwischen ihm und einer Gefährdung eines zu schützenden Rechtsguts oder eine entsprechende Gefahrennähe legitimiert ist (so Landesverfassungsgericht M-V im Urteil vom 21. Oktober 1999 zur Schleierfahndung).

Vor diesem Hintergrund verbietet sich ein genereller anlassunabhängiger Einsatz von AKLS zum Zwecke des Datenabgleichs (z. B. im Rahmen einer allgemeinen Verkehrskontrolle nach § 36 Abs. 5 StVO). In diesem Zusammenhang scheidet regelmäßig eine auf Dauer installierte Anlage aus.

Da mit dem Einsatz von AKLS die Kontrolle einer Vielzahl von Bürgern einhergeht, die zu dem Informationseingriff und der möglicherweise anschließenden Datenspeicherung keinen Anlass gegeben haben, ist die Befugnisnorm also so zu bestimmen, dass betroffene Personen grundsätzlich erkennen können, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist.

Zu Absatz 1

Mit dem in das Gesetz neu eingefügten § 43a Abs. 1 wird in Mecklenburg-Vorpommern eine Rechtsgrundlage für den Einsatz von AKLS zum Zwecke des Datenabgleichs im präventiv-polizeilichen Bereich geschaffen. Die Polizei kann zukünftig unter den Voraussetzungen der §§ 27a, 29, 32 oder 33 Abs. 1 Nr. 1 im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben.

Aufgrund dieser Regelung ist der Einsatz von AKLS zum Abgleich mit dem Fahndungsbestand insbesondere im Rahmen von Anhalte- und Sichtkontrollen im öffentlichen Verkehrsraum zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung (§ 27a Nr. 1) zulässig, soweit die Anordnung der Maßnahme auf polizeilichen Lagekenntnissen basiert. Darüber hinaus kann AKLS auch unter den in § 29 normierten Voraussetzungen zur Identitätsfeststellung sowie unter den Voraussetzungen, die für die Vornahme der in § 32 (Einsatz technischer Mittel zur Bildüberwachung sowie zur Bild- und Tonaufzeichnung) oder § 33 Abs. 1 Nr. 1 (Observation) genannten Eingriffsmaßnahmen gelten, zum Einsatz kommen.

Bei den vorgenannten Maßnahmen handelt es sich in Gänze um anlassbezogene Maßnahmen. Mithin findet der Einsatz von AKLS im Rahmen dieser Maßnahmen ebenfalls immer anlassbezogen statt.

Ein Einsatz von AKLS zum Zwecke des Abgleichs mit dem Fahndungsbestand wird ohne konkreten Anlass ausschließlich für polizeiliche Anhalte- und Sichtkontrollen gemäß § 27a Nr. 2 (Kontrollen im Grenzgebiet bis zu einer Tiefe von 30 m zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität und zur Unterbindung des unerlaubten Aufenthaltes) zugelassen. Folglich ist außer bei Maßnahmen nach § 27a Nr. 2 ein anlassunabhängiger Einsatz von AKLS zum Zweck des Abgleichs mit dem Fahndungsbestand - wie etwa im Rahmen einer allgemeinen Verkehrskontrolle gemäß § 36 Abs. 5 StVO - rechtlich nicht zulässig.

Unter Beachtung des § 26 Abs. 2, der die offene Datenerhebung als Grundsatz normiert, ist auch der Einsatz von AKLS zum Zwecke des Abgleichs mit dem Fahndungsbestand grundsätzlich offen durchzuführen. Eine verdeckte Datenerhebung mittels AKLS kommt nur ausnahmsweise dann in Betracht, wenn sonst die Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erheblich gefährdet werden würde oder wenn anzunehmen ist, dass dies im Interesse der Betroffenen ist. Ein Einsatz von AKLS zum Zwecke des Datenabgleichs in verdeckter Form wäre demnach z. B. im Rahmen geplanter Raub- und Sexualdelikte oder Kindesentführungen möglich. Es wird darauf hingewiesen, dass die Vorschrift zur verdeckten Datenerhebung mittels AKLS inhaltlich vollumfänglich der in § 26 Abs. 2 Satz 2 enthaltenen Regelung für die verdeckte Erhebung anderer personenbezogener Daten entspricht.

Zu Absatz 2

In Absatz 2 wird die Ausnahme zu dem in Absatz 1 des § 43a zugelassenen Regelfall des Abgleichs mit dem Fahndungsbestand normiert. Mit der Regelung in Absatz 2 wird unter den Voraussetzungen der §§ 27a, 29, 32 oder 33 Abs. 1 Nr. 1 im öffentlichen Verkehrsraum ein Abgleich mit anderen Dateien nur dann zugelassen, wenn die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist.

Aufgrund dieser Regelung ist es z. B. möglich, zur Abwehr konkreter Gefahren Kennzeichendaten auf Zubringerstraßen zu einem Fußballstadion mittels AKLS zu erheben und einen Abgleich mit der Datei „Gewalttäter Sport“ vorzunehmen, wenn mit der Anreise von so genannten Hooligans zu rechnen ist. Denn die Datei „Gewalttäter Sport“ wurde eigens zur Abwehr von abstrakten als auch konkreten Gefahren im Zusammenhang mit bestimmten Sportgroßereignissen (z. B. Fußballspiele) errichtet.

Bei einem Abgleich von Kennzeichen mit anderen Dateien als dem Fahndungsbestand ist aber immer sicherzustellen, dass dieser zur Abwehr einer dem Errichtungszweck der Datei entsprechenden Gefahr erforderlich ist und in Bezug zu einem bestimmten Ereignis steht. Mit der Regelung wird also nur in einem äußerst beschränkten Umfang ein Abgleich der erfassten Kennzeichen mit anderen Datenbeständen zugelassen und ein beliebiger Abgleich mit vorhandenen Datenbeständen ausgeschlossen.

Zu Absatz 3

Absatz 3 regelt, dass erfasste Kennzeichendaten, die nach Durchführung des Datenabgleichs nicht im Fahndungsbestand oder in Dateien gemäß Absatz 2 enthalten sind, unverzüglich zu löschen sind. Es wird damit sichergestellt, dass nur die Kennzeichendaten, die nach dem Abgleich zu einem so genannten „Trefferfall“ geführt haben, weiter gespeichert und verarbeitet werden dürfen. Hierzu sind die bestehenden Vorschriften im Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern zur Nutzung, Verarbeitung und Löschung erhobener personenbezogener Daten zu beachten.

Die Vorschrift schließt mithin eine willkürliche Vorratsdatenspeicherung von Daten unbescholtener Personen aus.

Zu Nummer 10 (§ 44)**Zu a)**

Die Änderung der Überschrift des § 44 „Besondere Formen des Datenabgleichs“ wurde aus folgenden Gründen erforderlich:

Beim Abgleich von Personendatenbeständen mit dem Ziel, diese zu reduzieren, um die Personen herauszufiltern, die zuvor festgelegte Prüfmerkmale erfüllen (so genannte Rasterfahndung), handelt es sich um eine besondere Form des Datenabgleichs. Die neu aufgenommene Regelung zur Erkennung von Kraftfahrzeugkennzeichen stellt ebenfalls eine besondere Form des Datenabgleichs dar, sodass diese - der Systematik der geltenden Fassung des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommerns folgend - auch in § 44 aufzunehmen wäre. Da beide polizeilichen Maßnahmen aber weiterer spezieller, nicht identischer Regelungen (z. B. zur Löschung der erhobenen Daten) bedürfen, empfiehlt sich mit Blick auf die Wahrung der Übersichtlichkeit die Schaffung einer jeweils gesonderten Vorschrift. Aus diesem Grund ist für den Datenabgleich zur Erkennung von Kraftfahrzeugkennzeichen § 43a neu in das Gesetz eingefügt worden. Folglich sind in § 44 nicht (mehr) alle besonderen Formen des Datenabgleichs - wie dessen derzeitige Überschrift vorgibt - normiert, sondern „nur“ die polizeiliche Maßnahme der Rasterfahndung. Um Unklarheiten bei der Gesetzesanwendung zu vermeiden, bedarf es daher der Änderung der Überschrift des § 44 in „Rasterfahndung“.

Zu b)

Die Polizei kann aufgrund der derzeit bestehenden gesetzlichen Regelung in § 44 Abs. 1 Satz 1 von Behörden, anderen Stellen und von Stellen außerhalb der öffentlichen Verwaltung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zwecke des Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist.

Nach den Anschlägen vom 11. September 2001 wurde in Mecklenburg-Vorpommern auf der Grundlage dieser Regelung die so genannte Rasterfahndung durchgeführt. Mit Blick auf das Ziel einer Rasterfahndung, welches gerade darin besteht, Anschläge zu verhindern und nicht erst dann eine Rasterfahndung zuzulassen, nachdem es schon zu Anschlägen gekommen ist, erwies sich das Tatbestandsmerkmal der „gegenwärtigen Gefahr“, welches nicht nur in Mecklenburg-Vorpommern, sondern auch in den Polizei- bzw. Sicherheitsgesetzen anderer Bundesländer zum Zeitpunkt der Durchführung der Rasterfahndung als Voraussetzung normiert war, als problematisch.

So war die nach den Ereignissen vom 11. September 2001 durchgeführte Rasterfahndung in mehreren Bundesländern - nicht in Mecklenburg-Vorpommern - Gegenstand von gerichtlichen Verfahren. Aufgrund der differierenden Gerichtsentscheidungen, die im Wesentlichen auf die nicht einheitliche Auslegung des Begriffes „gegenwärtige Gefahr“ durch die Gerichte zurückzuführen sind, und der damit einhergehenden Rechtsunsicherheit in Bezug auf die polizeiliche Maßnahme der Rasterfahndung bat der UA RV in seiner Sitzung am 6./7. März 2002 die vom AK II eingesetzte ad-hoc-Arbeitsgruppe „Rasterfahndung“ darum, Möglichkeiten der bundesweiten Vereinheitlichung gesetzlicher Voraussetzungen für die Durchführung der Rasterfahndung zu untersuchen. Der von der Arbeitsgruppe diesbezüglich vorgelegte Bericht enthält u. a. die Empfehlung, in den Landesgesetzen nicht (mehr) an die Gegenwartigkeit einer Gefahr anzuknüpfen, weil die Maßnahme ihrem Charakter nach im Vorfeld konkreter Ereignisse ansetzen müsse. Der Bericht wurde am 31. Mai 2002 vom AK II und am 6. Juni 2002 von der IMK zustimmend zur Kenntnis genommen.

Mit Blick auf die bereits erwähnte bundesweit unterschiedliche Rechtsprechung bei der Auslegung des Begriffes „gegenwärtige Gefahr“ und der Erkenntnis, dass die Rasterfahndung ein notwendiges und effektives Instrument der Gefahrenabwehr gegen den internationalen Terrorismus bietet, wurde nun mit der Änderung des Absatzes 1 Satz 1 des § 44 entsprechend der Empfehlung der Arbeitsgruppe des AK II „Rasterfahndung“ eine Herabsetzung der dort normierten Eingriffsvoraussetzungen vorgenommen.

Die Mehrheit der Bundesländer, die zum Zeitpunkt der Durchführung der Rasterfahndung im Herbst 2001 in ihren Polizei- bzw. Sicherheitsgesetzen die „gegenwärtige Gefahr“ oder „unmittelbar bevorstehende Gefahr“ als Tatbestandsmerkmal für die Durchführung der Rasterfahndung normiert hatten, haben inzwischen ebenfalls eine dahingehende Änderung ihrer Polizei- bzw. Sicherheitsgesetze vorgenommen, dass nunmehr nicht mehr an die Gegenwartigkeit der Gefahr angeknüpft wird.

Mit der Änderung des Absatzes 1 Satz 1 wird zukünftig auch in Mecklenburg-Vorpommern für die Durchführung einer Rasterfahndung das Vorliegen einer „erheblichen Gefahr“ vorausgesetzt. Der Begriff „erhebliche Gefahr“ wird bereits in § 3 Abs. 3 Nr. 3 des Gesetzes definiert. Danach ist eine „erhebliche Gefahr, eine Gefahr für ein bedeutsames Rechtsgut, wie Leib, Leben oder Freiheit einer Person, wesentliche Sach- und Vermögenswerte oder den Bestand des Staates“. Aufgrund dieser Legaldefinition werden die einzelnen, bedeutsamen Rechtsgüter im Satz 1 des Absatzes 1 nicht mehr einzeln benannt. Mit dem Rückgriff auf die in § 3 Abs. 3 Nr. 3 enthaltene Begriffsdefinition geht gleichzeitig eine Erweiterung der bisher geschützten, bedeutsamen Rechtsgüter einher. So ist die Durchführung der polizeilichen Maßnahme der Rasterfahndung gegenüber der bisher geltenden Fassung des Absatzes 1 Satz 1 zukünftig u. a. auch zur Abwehr einer Gefahr für den Bestand des Staates oder für wesentliche Sach- und Vermögenswerte möglich. Diese Erweiterung der zu schützenden, bedeutsamen Rechtsgüter ist u. a. mit Blick auf mögliche Anschläge auf Industrieanlagen (z. B. biochemische Anlagen) oder Infrastruktureinrichtungen (z. B. Umspannwerke) und der diesbezüglich drohenden Gefahren angezeigt.

Zudem wird mit der vorgenommenen Änderung der Anwendungsbereich der Rasterfahndung auf den Bereich der Bekämpfung von Straftaten von erheblicher Bedeutung gem. § 49 Nr. 1 und 3 ausgedehnt. Der Datenabgleich stellt im Einzelfall ein wirksames Mittel dar, um Erkenntnisse zur Verhütung weiterer Straftaten im Bereich der schweren Kriminalität zu gewinnen. Die Rasterfahndung dient dazu, aus einer unbestimmten Anzahl von Gefährdern durch Datenabgleich verschiedener, sich im Einzelfall ergebender Rasterkriterien (z. B. Datenabgleich von Melde-, Flug- oder Kfz-Daten) den Kreis soweit zu verdichten, dass entweder der Gefährder unmittelbar festgestellt wird oder der Kreis zumindest soweit eingegrenzt wird, dass gezielte Folgemaßnahmen (z. B. Observation, Befragungen) möglich werden.

Eine solche Vorgehensweise kann sich bei allen schweren Kriminalitätsformen ergeben. So belegen polizeiliche Erfahrungen, dass insbesondere auch schwerwiegende Raubstraftaten von hochspezialisierten, zum Teil international agierenden Tätergruppen begangen werden, die insoweit auch OK-Bezug haben können. Dabei wird häufig nach einem bestimmten modus operandi verfahren, der im Zuge der Ermittlungen, genutzt werden kann, um die sich daraus ergebenden Rasterkriterien für die o. a. eingrenzende Gefährderbestimmung zu verwenden. In diesem Zusammenhang sind regelmäßig Kfz- und Telekommunikationsdaten von besonderer Bedeutung. Welche Rasterkriterien im Einzelfall zielführend sind, lässt sich generell nicht entscheiden.

Sexualstraftäter sind nach allgemeinen gesicherten kriminologischen Erkenntnissen aufgrund ihrer Persönlichkeitsstruktur häufig Serienstraftäter. Dies gilt insbesondere auch bei Sexualstraftaten zum Nachteil von Kindern. Aus diesem Erfahrungswissen heraus und unter Berücksichtigung des Einzelfalles lässt sich ein spezifisches Täterprofil erstellen, das es ermöglicht, entsprechende zielgerichtete Abgleiche durchzuführen. Insoweit ist die Möglichkeit der Rasterfahndung auch ein notwendiger Beitrag zum Opferschutz.

Im zunehmenden Maße wird des Weiteren das Internet zur Begehung von Straftaten genutzt. Dabei werden u. a. über so genannte Internet-Auktionshäuser, wie z. B. ebay, aus Straftaten herrührende Gegenstände zum Kauf angeboten. Gezielte Datenabgleiche ermöglichen in diesen Fällen die Feststellung von Tatzusammenhängen und die Eingrenzung des Kreises von Tatverdächtigen sowie deren Ermittlung und damit auch die Verhinderung weiterer Straftaten.

Aufgrund dieser Fallgestaltungen wird deutlich, dass eine Erweiterung der Datenabgleichsmöglichkeiten mit Blick auf § 7 Abs. 1 Nr. 4 des Gesetzes, in dem als eine der wesentlichen Aufgaben der Polizei die Verhütung von Straftaten normiert wird, geboten ist. Allerdings ist bei den geschilderten Fällen zu berücksichtigen, dass es sich nicht um sog. Alltagskriminalität handelt. Es handelt sich vielmehr um wenige, herausragende Einzelfälle, die allerdings mit der Verletzung hochrangiger Rechtsgüter bzw. hohem Schaden einhergehen. In diesen Fällen kann der Datenabgleich die Arbeit der Polizei wesentlich erleichtern. In Anwendung des Grundsatzes der Verhältnismäßigkeit kommt die Rasterfahndung nur dann in Betracht, wenn andere Möglichkeiten der Erkenntnisgewinnung nicht zur Verfügung stehen bzw. keinen Erfolg versprechen.

Die vorgenommene Gesetzesänderung orientiert sich an bestehenden Regelungen in anderen Landespolizei- bzw. Sicherheitsgesetzen.

Zu c)

Absatz 3 Satz 1 in der derzeit geltenden Fassung regelt, dass in den Fällen, in denen der Zweck der polizeilichen Maßnahme der Rasterfahndung erreicht ist oder sich zeigt, dass der Zweck der Maßnahme nicht erreicht werden kann, die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen personenbezogenen Daten auf dem Datenträger zu löschen und die Unterlagen zurückzugeben oder zu vernichten sind, soweit sie nicht zur Abwehr einer anderen gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder für ein mit dem Sachverhalt zusammenhängendes Strafverfahren erforderlich sind.

Behielte man für die weitere Speicherung/Verwendung von übermittelten und im Zuge der Rasterfahndung zusätzlich angefallenen personenbezogenen Daten die derzeit normierte Voraussetzung „Abwehr einer anderen gegenwärtigen Gefahr“ in Absatz 3 bei, würde diese aufgrund der vorgenommenen Änderungen in Absatz 1 leer laufen. Wären nämlich die im Zuge einer nach Absatz 1 neue Fassung durchgeführten Rasterfahndung übermittelten und zusätzlich angefallenen personenbezogenen Daten zur Abwehr einer erheblichen Gefahr erforderlich, würde die in Absatz 1, 1. Alternative neue Fassung normierte Voraussetzung zur Anordnung einer (neuen) Rasterfahndung vorliegen. Folglich ließe der neu gefasste Absatz 1 die derzeitige Voraussetzung „Abwehr einer anderen gegenwärtigen Gefahr“ in Absatz 3 nicht mehr greifen.

Aus diesem Grund ist eine Anpassung der festgelegten Voraussetzungen für die weitere Speicherung/Verwendung der im Rahmen der Maßnahme Rasterfahndung übermittelten und zusätzlich angefallenen personenbezogenen Daten dahingehend angezeigt, dass nunmehr auf die „Abwehr einer erheblichen Gefahr“ abgestellt wird. Zum Begriff der „erheblichen Gefahr“ wird auf die Begründung zu Absatz 1 verwiesen.

Zu Nummer 11 (Überschrift des Abschnittes 3 Unterabschnitt 3)

Siehe Begründung zu 7. (§ 42).

Zu Nummer 12 (§ 47)

Siehe Begründung zu 7. (§ 42).

Zu Nummer 13 (§ 49)

Aufgrund der am 1. April 2003 in Kraft getretenen Novellierung des Waffengesetzes ist die Änderung unter a) notwendig.

Die Änderung unter b) ergibt sich aus der Novellierung des Aufenthaltsrechts und dem daraus resultierenden Aufenthaltsgesetz vom 30. Juli 2004.

Zu Nummer 14 (50)

Durch das Kostenrechtsmodernisierungsgesetz wurde das Gesetz über die Entschädigung von Zeugen und Sachverständigen aufgehoben und gleichzeitig das Justizvergütungs- und Entschädigungsgesetz in Kraft gesetzt. In § 107 OWiG wurde die Änderung bereits realisiert. Im Landesverwaltungsverfahrensgesetz und im Verwaltungskostengesetz des Landes Mecklenburg-Vorpommern soll der Verweis entsprechend geändert werden. Folgerichtig ist die Änderung somit auch im SOG M-V nachzuvollziehen.

Zu Nummer 15 (§ 52)

Die Änderung dient der Klarstellung. Aufgrund der ursprünglichen Formulierung in Satz 1 „bis zu einer richterlichen Entscheidung über zivilrechtliche Schutzmöglichkeiten“ wurde der Antrag auf zivilrechtlichen Schutz nach Hinweisen des Interventionsprojektes CORA und der Frauen- und Gleichstellungsbeauftragten der Landesregierung M-V missverständlich als Tatbestandsvoraussetzung für die Wegweisung angesehen. Das hieße, das Opfer müsste schon im Moment der Wegweisung entscheiden, zivilrechtlichen Schutz in Anspruch nehmen zu wollen. Dies ist nicht Intention des Gesetzgebers. Die Regelung soll lediglich festlegen, dass die polizeilich verfügte Wegweisung mit Ablauf der von der Polizei gesetzten Frist endet, oder, soweit das Opfer zivilrechtlichen Schutz beantragt hat und die Entscheidung darüber vor Ablauf der von der Polizei gesetzten Frist ergeht, die Wegweisung im Zeitpunkt der Gerichtsentscheidung endet.

Die Verpflichtung der Gerichte, die Polizei über getroffene Entscheidungen zu informieren, ist dringend erforderlich. Dadurch wird die Polizei in Kenntnis gesetzt, ob sie an der von ihr getroffenen Maßnahme festhalten muss/kann oder diese bereits aufgrund einer gerichtlichen Entscheidung obsolet geworden ist.

Zu Nummer 16 (§ 53)**Zu a)**

Die Änderung der Überschrift des § 53 „Durchsuchung von Personen“ in „Durchsuchung und Untersuchung von Personen“ wurde aufgrund der Einfügung von Absatz 4 erforderlich, der die Untersuchung von Personen zum Inhalt hat.

Zu b)

Medizinischer Fortschritt hat es möglich gemacht, die Wahrscheinlichkeit einer Infektion mit HIV zu vermindern, wenn unmittelbar nach Übertragung der Viren spezifische medizinische Maßnahmen erfolgen (Postexpositionsprophylaxe; kurz PEP). Die Nebenwirkungen der bei der PEP eingesetzten Medikamente sind für den Betroffenen - z. B. für das Opfer einer Straftat, das vom Täter verletzt und einer Infektionsgefahr ausgesetzt wurde - belastend, sodass deren Durchführung vom Vorliegen eines tatsächlichen Infektionsrisikos abhängt. Dies setzt unter anderem voraus, dass der HIV-Serostatus (med. Definition: Resultat der Untersuchung einer Blutprobe auf spezifische Antikörper) des Verursachers der Gefahr bekannt ist, das heißt, eine HIV-Infektion in dessen Blut festzustellen ist.

Bei Hepatitis B (HBV) hängt das weitere Vorgehen vom Serostatus sowohl des Betroffenen als auch des Verursachers ab. Dies gilt insbesondere für die nachträgliche Impfung. Bei einer drohenden Infektion mit Hepatitis C (HCV) richten sich weitere Untersuchungen beim Betroffenen nach dem Ergebnis der Blutuntersuchung beim Verursacher. Eine PEP steht hier nicht zur Verfügung. Die Notwendigkeit von therapeutischen Maßnahmen richtet sich nach der Entwicklung der Untersuchungsbefunde beim Betroffenen.

Als mögliche, zu erweiternde Rechtsgrundlage für die Anordnung einer Blutentnahme durch die Polizei und Veranlassung einer mikrobiologischen Blutuntersuchung zur Prüfung des Krankheitsstatus des Verursachers einer konkreten Infektionsgefahr (HIV, HCV und HBV) wurde von den Gremien der IMK bislang § 25 f Infektionsschutzgesetz (IfSG) angenommen. Im Rahmen der Befassung der Gremien der IMK und der GMK mit dem Thema Blutentnahme zur Gefahrenabwehr wurden jedoch von den Bundesministerien für Gesundheit und Soziale Sicherung, Justiz sowie des Inneren Zweifel an der Anwendbarkeit des IfSG geäußert, da § 25 IfSG in erster Linie dem Schutz der Bevölkerung zum Schutz vor Infektionen diene. Der Schutz der Allgemeinheit sei der eigentliche Gesetzeszweck, weniger der Schutz des Einzelnen und dessen Behandlung.

Eine interministerielle Sonder-Arbeitsgruppe von GMK und IMK unter Beteiligung des BMI und des BMGS konnte jedoch keine Einigung hinsichtlich der rechtlichen Verankerungsmöglichkeiten etwaiger Zwangsmaßnahmen erzielen. Die Arbeitsgruppe wurde aufgelöst und die weitere Klärung den Innen- und Justizressorts überantwortet. Angesichts dieser Sachlage und der Vorbehalte des Bundes gegen eine Regelung im Bundesrecht ist in absehbarer Zeit mit einer bundeseinheitlichen gesetzlichen Regelung, die wünschenswert wäre, nicht zu rechnen.

Zur Herstellung von Rechtssicherheit für die anordnenden Beamten und mit den Untersuchungen betrauten Ärzten ist daher eine landesrechtliche Regelung erforderlich. Zwar hat der Bund die konkurrierende Gesetzgebungszuständigkeit nach Artikel 74 Absatz 1 Nummer 19 GG für „Maßnahmen gegen gemeingefährliche und übertragbare Krankheiten“. Darunter sind alle Infektionskrankheiten zu verstehen, so dass alle Krankheiten im Sinne des § 2 Nummer 3 IfSG erfasst werden. Mit dem Infektionsschutzgesetz hat der Bund im Sinne des Artikels 72 Absatz 1 GG von seiner Gesetzgebungszuständigkeit Gebrauch gemacht. Die Tatsache, dass der Bundesgesetzgeber eine spezifische Vorschrift der Blutentnahme zur Gefahrenabwehr (Individualprophylaxe) verbunden mit einer entsprechenden klar definierten Datenweitergabe bisher nicht geregelt hat, zeigt, dass er in dieser speziellen Frage von seiner Gesetzgebungszuständigkeit nicht abschließend Gebrauch gemacht hat, sodass das IfSG eine landesrechtlichen Regelung im Polizeirecht nicht sperrt. Darüber hinaus hat der Bund während der Arbeit in den Gremien deutlich gemacht, dass er sich für dieses Thema nicht zuständig sieht.

Mit dem neuen Absatz 4 soll daher eine Regelung geschaffen werden, die insbesondere die unverzügliche Blutentnahme beim Verursacher einer Infektionsgefahr gegen dessen Willen erlaubt, um dessen Serostatus bzgl. HIV, aber auch Hepatitis B und C, als eine Voraussetzung für die Einleitung bzw. Fortführung medizinischer Maßnahmen feststellen zu können. Da eine Infektion kurze Zeit direkt nach dem Kontakt zwischen Verursacher und Opfer beim Opfer nicht nachweisbar ist, für die medizinische Behandlung jedoch geklärt sein sollte, ob und welche Viren das Opfer infiziert haben könnten, kann eine Untersuchung des Verursacherbluts die notwendigen Erkenntnisse für die ärztliche Entscheidungsfindung bringen.

Zu betonen ist, dass in jedem Fall die freiwillige Mitwirkung des Verursachers und seine Einwilligung in die Blutuntersuchung anzustreben ist. Fehlt diese, kann bei einer Gefahr für das Leben des Opfers oder einer schwerwiegenden Gesundheitsgefährdung jedoch nicht auf die zwangsweise Durchsetzung der Maßnahme verzichtet werden. Die Vorschrift kommt allen Personen zugute, die aus ärztlicher Sicht einer Infektionsgefährdung ausgesetzt waren, insbesondere Opfern von Gewaltdelikten, aber auch beispielsweise medizinisches Personal oder Polizeivollzugsbeamte.

Die körperliche Untersuchung ist darauf gerichtet, den Zustand und die Beschaffenheit des Körpers sowie seiner Bestandteile für die Zwecke der Gefahrenabwehr festzustellen. Für im Rahmen der Strafverfolgung vorzunehmende Untersuchungen gelten die §§ 81a bis 81d StPO. § 81a StPO kommt als Rechtsgrundlage für den hier angestrebten Zweck der Gefahrenabwehr nicht in Betracht. Die Regelung bezieht sich beim gegenwärtigen Stand der medizinischen und epidemiologischen Wissenschaft auf folgende Krankheitserreger:

- Human Immunodeficiency Virus (Menschliches Immun-Schwäche-Virus, HIV),
- Hepatitis C (HCV),
- Hepatitis B (HBV).

Von einer Infektionsgefahr durch die v. g. Erreger wird auszugehen sein bei:

- Stich- und Schnittverletzungen mit möglicherweise infektiös verunreinigten Gegenständen, z. B. Hohladeln,
- Benetzung offener Wunden und Schleimhäute mit Blut, Speichel oder Sperma,
- Bissverletzungen,
- Augenkontakt mit möglicherweise infektiösen Körperflüssigkeiten,
- Aufnahme möglicherweise infektiöser Körperflüssigkeiten in Nasen-/Mundraum,
- ungeschütztem Geschlechtsverkehr (Vergewaltigungsfälle).

Ein rechtswidriges und schuldhaftes Verhalten ist im Zusammenhang mit der Verursachung der Infektionsgefahr nicht zu fordern. Gemäß den allgemeinen Grundsätzen des Gefahrenabwehrrechts ist ausschließlich die unmittelbare Verursachung der Gefahrenlage entscheidend. Eine Einschränkung des Kreises der von der Norm zu schützenden Personen ist nicht geboten. Jedermann kann einer Infektionsgefahr im hier zu regelnden Sinne ausgesetzt sein. Neben Vollzugspersonal und medizinischem Personal, das regelmäßig zu ansteckungsverdächtigen Personen Kontakt hat, sind in zahlreichen Fällen auch Bürger als Opfer von Straftaten einer Infektionsgefahr ausgesetzt worden. Das Herausgreifen einzelner Berufsgruppen aufgrund einer statistisch erhöhten Wahrscheinlichkeit einer Infektion und die Versagung einer Schutzmaßnahme für z. B. Opfer von Straftaten wäre nicht sachgerecht und insbesondere angesichts der erheblichen Gefahren für Leib und Leben der Betroffenen mit dem Gleichbehandlungsgebot aus Artikel 3 GG unvereinbar.

Für eine körperliche Untersuchung ist grundsätzlich eine richterliche Anordnung erforderlich. Bei Gefahr im Verzug darf die Anordnung durch die Polizei erfolgen. Mit einer HIV-PEP ist möglichst innerhalb von 2 Stunden nach der Exposition zu beginnen. Vor diesem Hintergrund ist es erforderlich, auch derjenigen Behörde, die mit den vorliegenden Fällen ohnehin aufgrund ihrer Zuständigkeit für die Verfolgung von Straftaten und für die allgemeine Gefahrenabwehr konfrontiert ist, die Anordnung und Koordination des weiteren Verfahrens zu überlassen. Standards zur Beurteilung eines Übertragungsrisikos und zum weiteren diagnostisch-/therapeutischen Vorgehen sind in der medizinischen Literatur beschrieben.

So kann auf die Deutsch-Österreichischen Empfehlungen zur postexpositionellen Prophylaxe der HIV-Infektion, Mai 2002, Bezug genommen werden. Die Beurteilung einer konkreten Infektionsgefahr, die weitergehende Untersuchungen und Maßnahmen gegenüber dem Verursacher rechtfertigt, setzt spezifisches medizinisches Fachwissen voraus. Vor der richterlichen Anordnung oder der Anordnung durch die Polizei ist deshalb die Einschätzung eines Arztes mit entsprechenden Fachkenntnissen einzuholen, ob im konkreten Fall eine Infektionsgefahr vorliegt. Diese Risikoeinschätzung, die Vorbereitung und die Durchführung des körperlichen Eingriffs und die sich anschließende Beratung und Behandlung liegen ausschließlich in der Verantwortung des Arztes.

Die Nutzung der durch die Untersuchung erhobenen Befunddaten richtet sich für den untersuchenden und behandelnden Arzt nach den allgemeinen Bestimmungen.

Ein weiterer Anwendungsbereich der Vorschrift kann gegebenenfalls in der Untersuchung des Gefährdeten selbst liegen. Körperliche Untersuchungseingriffe, auch ohne oder gegen den Willen des Betroffenen, können im Einzelfall zum Schutz von Leib und Leben und damit zu dessen Rettung, z. B. bei einer konkreten Vergiftungsgefahr durch verschluckte Drogenbehältnisse, erforderlich werden.

Es kann erforderlich sein, Hinweise auf ansteckende Krankheiten über die Einleitung medizinischer Maßnahmen hinaus im Einzelfall zur Abwehr zukünftiger Gefahren zu nutzen. Es handelt sich um Fälle, in denen Verursacher, die rechtswidrige Taten begangen haben und von denen weitere Straftaten zu erwarten sind, eine Infektionsgefahr herbeigeführt haben. Erbringt eine Blutuntersuchung hier ein positives Ergebnis, so können mit Nutzung dieses Befundes zukünftige Infektionsgefahren verhindert werden. So besteht in der polizeilichen Personendatei INPOL die Möglichkeit, einen direkten Hinweis auf die konkrete übertragbare Krankheit aufzunehmen. INPOL dient der Aufklärung von Straftaten und der Gefahrenabwehr, einschließlich der vorbeugenden Bekämpfung von Straftaten. Gespeichert werden u. a. Personen, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist und bei denen wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht. Die Aufnahme eines Hinweises auf z. B. eine HIV-Infektion bei diesem Personenkreis, der zudem eine konkrete Infektionsgefahr verursacht hat und dessen Blut mit positivem Ergebnis untersucht wurden, kann bei einer Wiederholungstat und der neuen Situation einer Ansteckungsgefahr für einen Dritten den zunächst entscheidenden Hinweis geben, dass überhaupt eine Ansteckungsgefahr droht. Ein derartiger Hinweis kann die Notfallbehandlung beschleunigen. So kann zunächst auch ohne Abnahme einer Blutprobe beim Verursacher (Fälle, in denen der Täter flüchtig ist oder sich massiv gegen die Blutentnahme wehrt) und die Durchführung des Schnelltests mit der Behandlung des Verletzten begonnen werden. Darüber hinaus kann der Hinweis „Ansteckungsgefahr“ Einsatzkräfte warnen und weitere Infektionsgefahren vermeiden.

Zu Nummer 17 (§ 64)

Die Änderung dient der Klarstellung, dass empfangsberechtigte Personen sechs Wochen Zeit haben, verwahrte Sachen nach einer schriftlich erfolgten Aufforderung in Empfang zu nehmen. Die empfangsberechtigte Person sollte in dem Aufforderungsschreiben auf diese Frist hingewiesen werden. Nach Ablauf der Frist ist die Vernichtung der verwahrten Sache zulässig. Mit der Regelung wird Rechtssicherheit hergestellt.

Zu Nummer 18 (§ 116)

Mit der Befristung der Regelungen zur Videoüberwachung, zur Telekommunikationsüberwachung und zum Einsatz des Kfz-Kennzeichen-Lesesystems in § 116 soll eine Überprüfung der Wirksamkeit der Regelung einhergehen.

Zu Artikel 2

Mit Artikel 2 wird dem verfassungsrechtlichen Zitiergebot gemäß Artikel 19 Abs. 1 Satz 2 des Grundgesetzes Rechnung getragen.

Zu Artikel 3

Die Verständlichkeit und Handhabbarkeit der Gesetzesänderungen können durch Bekanntmachung der geltenden Fassung verbessert werden. Hierzu wird das Innenministerium ermächtigt.

Zu Artikel 4

Artikel 4 regelt das In-Kraft-Treten.