

## Viertes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes (Auszug)

### § 33b

#### Datenerhebung durch Eingriffe in die Telekommunikation

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

1. dies zur Abwehr einer dringenden Gefahr für Leben, Leib oder Freiheit einer Person oder einer gemeinen Gefahr erforderlich ist oder
2. aufgrund tatsächlicher Anhaltspunkte, insbesondere aufgrund konkreter Informationen über Planungs- oder Vorbereitungshandlungen, anzunehmen ist, dass eine Straftat von erheblicher Bedeutung (§ 10 Abs. 3 Satz 1)<sup>1</sup> begangen werden soll, die auch im Einzelfall besonders schwer wiegt und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist

und wenn bestimmte Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse erlangt werden, die für die Gefahrenabwehr von Bedeutung sind.

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

1. spezifische Kennungen, insbesondere Geräte- und Kartenummer von Mobilfunkendgeräten, zu ermitteln, wenn dies für die Durchführung einer Maßnahme nach Satz 1 unerlässlich ist,
2. den Standort eines Mobilfunkendgerätes zu ermitteln oder
3. Telekommunikationsverbindungen zu unterbrechen oder zu verhindern.

(3) Eine Maßnahme nach Absatz 1 und 2 darf sich nur gegen

1. den für die Gefahr Verantwortlichen oder einen Notstandspflichtigen richten sowie
2. gegen Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass
  - a) sie für Personen nach Nummer 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a der Strafprozessordnung zu haben, oder weitergeben oder
  - b) die unter Nummern 1 genannten Personen ihre Telekommunikationseinrichtungen benutzen werden.

Wird erkennbar, dass in den Kernbereich privater Lebensgestaltung oder in ein durch ein Berufsgeheimnis nach §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenerhebung zu unterbrechen, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst. Äußerungen oder Mitteilungen, die einen unmittelbaren Bezug zu der in Absatz 1 genannten Gefahr haben, sind in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen.

---

<sup>1</sup> § 10 Abs. 3 S. 1 BbgPolG: Straftaten von erheblicher Bedeutung sind alle Verbrechen und alle weiteren in § 100a der Strafprozessordnung aufgeführten Straftaten.

(4) Bei Maßnahmen nach Absatz 1 und 2 dürfen personenbezogene Daten Dritter nur erhoben und Telekommunikationsverbindungen Dritter nur unterbrochen oder verhindert werden, wenn dies zu ihrer Durchführung unvermeidbar ist. Nach Beendigung der Maßnahme sind dabei erhobene Daten unverzüglich zu löschen.

(5) Die Maßnahme darf nur durch den Richter, bei Gefahr im Verzug auch durch den Behördenleiter angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. In der schriftlichen Anordnung sind anzugeben

1. soweit bekannt, der Name und die Anschrift des Adressaten, gegen den sich die Maßnahme richtet,
2. eine Kennung des Telekommunikationsanschlusses oder Endgerätes,
3. die Art der Maßnahme sowie
4. die tragenden Erkenntnisse für das Vorliegen der Gefahr nach Absatz 1 und die Begründung der Verhältnismäßigkeit der Maßnahme.

Die Anordnung ist auf den nachfolgend genannten Zeitraum zu befristen:

1. im Falle des Absatzes 2 Nr. 2 höchstens zwei Wochen,
2. im Falle des Absatzes 2 Nr. 3 höchstens drei Tage und
3. in allen anderen Fällen höchstens einen Monat.

Eine Verlängerung um jeweils den jeweils gleichen Zeitraum ist zulässig, sofern die Anordnungsvoraussetzungen fortbestehen. Anderenfalls ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht darüber zu benachrichtigen.

(6) Eine Anordnung nach Absatz 5 verpflichtet jeden, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in der jeweils geltenden Fassung der Polizei die Überwachung und Aufzeichnung zu ermöglichen. Die Polizei kann Diensteanbieter unter den Voraussetzungen des Absatzes 1 verpflichten, unverzüglich Auskunft über vorhandene und künftige Verkehrsdaten der dort genannten Personen sowie über die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartenummer sowie die Zellinformationen, zu erteilen. Die Entschädigung richtet sich nach § 23 des Justizvergütungsgesetzes, soweit nicht eine Entschädigung auf Grund des Telekommunikationsgesetzes zu gewähren ist.

(7) Die Unterrichtung des Betroffenen richtet sich nach § 29 Absatz 6 und 7<sup>2</sup>. Wird wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingelei-

---

<sup>2</sup> § 29 Abs. 6 BbgPolG: Werden Daten beim oder über den Betroffenen ohne seine Kenntnis erhoben, so ist er davon zu benachrichtigen, sobald der Zweck der Datenerhebung dadurch nicht mehr gefährdet wird. Eine Benachrichtigung unterbleibt, wenn zu ihrer Durchführung in unverhältnismäßiger Weise weitere Daten erhoben werden müssten. Ist die zu benachrichtigende Person minderjährig, treten die Personensorgeberechtigten an ihre Stelle. Von der Benachrichtigung kann abgesehen werden, solange zu besorgen ist, dass sie zu erheblichen Nachteilen für den Minderjährigen führt.

§ 29 Abs. 7 BbgPolG-E: Im Falle von verdeckten Datenerhebungen, die nur auf Grund richterlicher Anordnung zulässig sind, erfolgt die Benachrichtigung spätestens sechs Monate nach Beendigung der Maßnahme. Eine weitere Zurückstellung bedarf der richterlichen Zustimmung. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit ent-

C:\Dokumente und Einstellungen\K.Schlberg\Lokale Einstellungen\Temporary Internet Files\OLK211\§ 33b BbgPolG-E.doc

tet, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Die Unterrichtung kann unterbleiben, wenn der Betroffene im Rahmen des Ermittlungsverfahrens von der Maßnahme Kenntnis erlangt.

(8) Die auf Grund einer Maßnahme nach Absatz 1, 2 und 6 Satz 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. Sie dürfen für andere Zwecke verwendet werden, wenn dies zur Abwehr einer in Absatz 1 genannten dringenden Gefahr für die öffentliche Sicherheit oder für die Verfolgung von Straftaten nach § 100a Satz 1 der Strafprozessordnung erforderlich ist. Eine solche Änderung der Zweckrichtung ist festzustellen und zu dokumentieren.

(9) Daten, bei denen sich nach der Auswertung herausstellt, dass die Voraussetzungen für ihre Erhebung nicht vorlagen, dürfen nicht verwendet werden und sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich einzuholen; Absatz 5 gilt entsprechend. Im Übrigen sind die auf Grund von Maßnahmen nach Absatz 1, 2 und 6 Satz 2 erlangten personenbezogenen Daten unverzüglich zu sperren, wenn sie nicht mehr erforderlich sind. Sie dürfen ausschließlich für eine gerichtliche Überprüfung verwendet werden und sind unverzüglich zu löschen, wenn sie hierfür nicht benötigt werden, spätestens jedoch zwei Wochen nach Unterrichtung der Betroffenen. Auf diese Frist ist in der Unterrichtung hinzuweisen. Die Löschung von Daten nach Satz 1 und 4 und nach Absatz 4 Satz 2 ist zu dokumentieren.“

## **Auszug aus der Begründung für das Vierte Gesetz zur Änderung des Brandenburgischen Polizeigesetzes**

### § 33b - Datenerhebung durch Eingriffe in die Telekommunikation

Mit dieser Norm wird in das Polizeigesetz die Befugnis zur Datenerhebung durch Überwachung der Telekommunikation eingefügt. Hierdurch ist die Polizei erstmals ermächtigt, nicht nur repressiv als Strafverfolgungsbehörde, sondern auch zur Gefahrenabwehr verdeckt die Telekommunikation zu überwachen. Sie kann ferner technische Geräte zur Identifikation, Lokalisation von Telekommunikationsteilnehmern (zum Beispiel den sog. „IMSI-Catcher“, ein Gerät zur Ermittlung der Geräte- und Kartennummer aktiv geschalteter Mobilfunkendgeräte und auf dieser Basis auch zur Lokalisation von deren Standort) und zur Unterbrechung bzw. Verhinderung von Telekommunikation einsetzen.

Der Einsatz von Ortungsgeräten, wie der sog. „IMSI-Catcher“, stellt einen wichtigen Anwendungsfall in der Praxis dar. Dies gilt insbesondere bei der Standortbestimmung vermisster oder hilfloser Personen. Die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen durch die Polizei kann dann erforderlich werden, wenn Telekommunikationstechnik beispielsweise zur Ausführung von Sprengstoffanschlägen – wie beim Anschlag in Madrid – oder bei Geisellagen zum Einsatz kommt.

---

sprechend. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. Eine Unterrichtung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn

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

Der Lageeinschätzung des Bundeskriminalamtes zu Folge diene Deutschland in der Vergangenheit verschiedenen islamistischen Gewalttätern nicht nur als Aufenthaltsort sowie Ruhe- und Rückzugsraum, sondern auch als Vorbereitungsraum von Terroranschlägen. Die Bundesrepublik Deutschland ist Teil eines beinahe weltweiten Gefahrenraums und liegt somit auch im Zielspektrum terroristischer Gruppierungen. Von der Existenz bislang noch unbekannter islamistischer Netzwerke bzw. Zellen, die in grenzüberschreitende funktionsfähige Strukturen eingebunden sind und die weitestgehend in eigener Regie und unter Berücksichtigung eigener Fähigkeiten und Tatmittel Anschlagplanungen vornehmen könnten, ist auszugehen.

Von dieser Gesamteinschätzung ist auch das Land Brandenburg erfasst. Zwar liegen den Sicherheitsbehörden gegenwärtig keine Erkenntnisse über konkrete Bedrohungen oder Anschlagplanungen vor. Insbesondere das Einsatzführungskommando der Bundeswehr in Schwielowsee (ehemals Geltow) und der internationale Flughafen Schönefeld bleiben jedoch herausragende potenzielle Anschlagziele. Daneben ist die Sicherheitslage Brandenburgs durch die unmittelbare Nähe zur Bundeshauptstadt Berlin sowie durch den starken Transitverkehr von und nach Berlin sowie aus und in osteuropäische Staaten gekennzeichnet. Die Vielzahl potenzieller Ziele für terroristische Anschläge in Berlin lassen es nicht unwahrscheinlich erscheinen, dass Brandenburg als Planungs-, Vorbereitungs- oder Rückzugsraum in Betracht gezogen wird. Zudem kann nicht ausgeschlossen werden, dass auch in Brandenburg weitere relevante Anschlagziele, etwa durch den Besuch von Staatsgästen, entstehen. Der versuchte Anschlag auf den damaligen irakischen Ministerpräsidenten Allawi in Berlin im Dezember 2004 zeigt, auch nach Auffassung des Präsidenten des Bundesnachrichtendienstes (BND): „In dem Augenblick, wo ein relevantes Ziel in Deutschland auftaucht, versuchen islamistische Terroristen auch hier zuzuschlagen“ (Interview mit dem Präsidenten des BND, Ernst Uhrlau, in der Berliner Morgenpost vom 24. Juli 2006).

Insbesondere die Vielzahl von Staatsbesuchen in der Landeshauptstadt Potsdam (oder in Rheinsberg, wie zuletzt durch den französischen Staatspräsidenten Jacques Chirac), aber auch zahlreiche Staatsbesuche in der Bundeshauptstadt, die über den internationalen Flughafen Schönefeld erfolgen, Regierungstagungen an Konferenzorten in Brandenburg (z.B. Neu Hardenberg, Genshagen) lassen dieses Szenario auch in Brandenburg wahrscheinlich werden.

Daneben findet auch hier Organisierte Kriminalität mit Bezug auf Straftaten von erheblicher Bedeutung statt. Zieht man die geografische Lage Brandenburgs in Betracht, nimmt dieser Umstand noch an Bedeutung zu. In Berlin und Brandenburg bilden sich häufig länderübergreifende kriminelle Strukturen heraus. Daneben spielt auch die Nähe zum Nachbarn Polen und die damit verbundene Gefahr grenzüberschreitender und international organisierter Kriminalität eine nicht nur untergeordnete Rolle.

Die brandenburgische Polizei wird sich daher zukünftig verstärkt auch mit länder- und grenzübergreifenden kriminellen und terroristischen Organisationen befassen müssen, die nicht nur durch eine besondere Abschottung nach außen, sondern auch dadurch gekennzeichnet sind, dass sie die zur Verfügung stehenden modernen Informations- und Kommunikationsmittel professionell nutzen. Ihr müssen daher Mittel und Befugnisse in die Hand gegeben werden, die ihr die Abwehr dringender Gefahren und von Straftaten von erheblicher Bedeutung oft erst ermöglichen. Die Telekommunikationsüberwachung und die Ermittlung spezifischer Kennungen sowie von Standorten von Mobilfunkgeräten haben sich als Mittel zur Strafverfolgung auch in Brandenburg bewährt. Der Einsatz solcher Mittel sollte jedoch nicht erst dann möglich sein, wenn Straftaten von erheblicher Bedeutung stattgefunden haben und Schäden an hochrangigen Rechtsgütern bereits eingetreten sind. Benötigt werden diese Mittel vielmehr bereits zur vorbeugenden Bekämpfung solcher Straftaten und zur Abwehr von Gefahren für hochrangige Rechtsgüter. Dabei spielt keine Rolle, ob der zu erwartende Schaden in Brandenburg selbst, im benachbarten Berlin oder anderenorts eintritt. Entscheidend ist, dass die Mittel für Eingriffe in die Telekommunikation dort und dann eingesetzt werden, wo die Gefahr wirksam abgewehrt werden kann.

Die Befugnisnorm § 33b orientiert sich ebenso wie die verfahrensrechtlichen Sicherungen sowohl an den verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht in seinen Entscheidungen vom 3. März 2004 zur repressiven Wohnraumüberwachung (Az.: 1 BvR 2378/98, 1 BvR 1084/99), vom 27. Juli 2005 zur vorbeugenden Telefonüberwachung im Niedersächsischen Polizeigesetz (1 BvR 668/04) und zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz (Az.: 1 BvF 3/92) aufgezeigt hat, als auch an den datenschutzrechtlichen Erfordernissen. Dabei wurden die Besonderheiten des Gefahrenabwehrrechts einbezogen.

Einen besonderen Schutz genießen der Kernbereich privater Lebensgestaltung und die Vertrauensverhältnisse zwischen dem Adressaten der Maßnahme und Berufsheimnisträgern wie Anwälten, Ärzten, Geistlichen und Journalisten, soweit das Wesen der Überwachung und Aufzeichnung von Telekommunikation dies zulässt. Abhörmaßnahmen, die erkennbar in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis oder in den Kernbereich privater Lebensgestaltung eingreifen, sind grundsätzlich unzulässig und deshalb zu unterbrechen. Im Bereich der Gefahrenabwehr ist jedoch der Schutz von Vertrauensverhältnissen zu Berufsheimnisträgern dann nicht der Abwägung gegen andere hochrangige Rechtsgüter entzogen, wenn sich die Überwachung der Telekommunikation gegen den Berufsheimnisträger selbst richtet. Derartig hohe Rechtsgüter, wie die körperliche Unversehrtheit, das Leben und die Freiheit einer Person, die einen besonderen Schutz genießen, den der Staat in seiner Garantstellung für den Einzelnen zu gewährleisten hat, müssen in diesem Falle bei der gesetzlichen Abwägung gegen geschützte Vertrauensverhältnisse überwiegen.

Zwar hat der Bund gemäß Artikel 73 Nr. 7 Grundgesetz die ausschließliche Gesetzgebungskompetenz auf dem Gebiet der Telekommunikation. Dies betrifft jedoch nur die technische Seite der Übermittlung des Kommunikationsvorgangs. Die Länder sind hingegen nach Artikel 70 Abs. 1 Grundgesetz für den Bereich der Gefahrenabwehr zuständig. Daher steht dem Landesgesetzgeber die Befugnis zu, zum Zweck der Gefahrenabwehr bereichsspezifische Regelungen zur Beschränkung des Fernmeldegeheimnisses zu erlassen. Die konkrete technische Abwicklung der Telekommunikationsüberwachung erfolgt nach den Regelungen des Telekommunikationsgesetzes und der darauf gestützten Rechtsverordnungen.

Dies gilt auch für die Mitwirkungspflichten der Diensteanbieter. Die Gesetzgebungshoheit des Landes Brandenburg ist grundsätzlich auf sein Staatsgebiet beschränkt. Folglich können landesrechtlich begründete Pflichten nur die natürlichen oder juristischen Personen betreffen, die zum Landesgebiet einen rechtlichen Bezug, wie z.B. durch den tatsächlichen Aufenthalt oder den Unternehmenssitz, haben. Maßgeblicher Anknüpfungspunkt für eine Verpflichtung eines Diensteanbieters, dessen Firmensitz sich außerhalb Brandenburgs befindet, zur Unterstützung der brandenburgischen Polizei ist, dass sie ihre Dienste auch in Brandenburg anbieten und damit auch in Brandenburg den Adressaten einer Maßnahme nach § 33b Abs.1 die Möglichkeit eröffnen, Telekommunikationsdienste zu nutzen. Dies ist eine ausreichende Rechtfertigung für die Auferlegung von Mitwirkungspflichten auf Unternehmen außerhalb Brandenburgs.

#### Absatz 1

Absatz 1 regelt die Befugnis der Polizei zur Erhebung personenbezogener Daten durch die Überwachung und die Aufzeichnung von Telekommunikation im Sinne des Telekommunikationsgesetzes zur Abwehr von Gefahren für hochwertige Rechtsgüter. Unter Telekommunikation ist hierbei der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (Telekommunikationsanla-

ge), zu verstehen (vgl. § 3 Nr. 22 und 23 TKG). Von der Befugnis werden sowohl Inhalts- als auch Verkehrsdaten erfasst.

Voraussetzung für die Maßnahme ist, dass eine dringende Gefahr für die genannten besonders schutzwürdigen Rechtsgüter vorliegt. Analog zur neuen Regelung über die präventive Wohnraumüberwachung wird auch im Rahmen der Telekommunikationsüberwachung der Begriff „dringende Gefahr“ verwendet. Hierdurch wird gewährleistet, dass maßgebliches Kriterium für die Beurteilung der Zulässigkeit der Telekommunikationsüberwachung nicht der zeitliche Faktor, sondern die Wahrscheinlichkeit und das Ausmaß des Schadens, insbesondere die Hochrangigkeit des gefährdeten Rechtsgutes ist (vgl. BVerfGE 17, 232, 251 f., BVerwGE 47, 31, 40). So wird sichergestellt, dass die Telekommunikationsüberwachung nur zur Abwehr von Gefahren für besonders hochrangige Rechtsgüter zulässig ist. Zu diesem Zweck dürfen Datenerhebungen nur durchgeführt werden, wenn dies für die Gefahrenabwehr erforderlich ist. Die präventive Telekommunikationsüberwachung ist dementsprechend gegenüber allen anderen polizeilichen Maßnahmen der Gefahrenabwehr, mit Ausnahme der Wohnraumüberwachung, subsidiär. Zudem wird sichergestellt, dass die abzuwehrenden Gefahren einen engen Bezug zur Telekommunikation haben. Präventive Eingriffe in die Telekommunikation sind nur dann zulässig, wenn erkennbar ist, dass sich damit die Gefahr beseitigen lässt oder dass Erkenntnisse gewonnen werden können, die für die Gefahrenabwehr von Bedeutung sind.

Damit wird einer wichtigen Maßgabe des Bundesverfassungsgerichts in seiner Entscheidung zum niedersächsischen Polizeigesetz vom 27. Juli 2005 (1 BvR 668/04) entsprochen und das gesetzgeberische Konzept für die vorbeugende Telekommunikationsüberwachung verdeutlicht. Die Einschränkung gilt nicht nur für die Überwachung und Aufzeichnung von Telekommunikation, sondern auch für Maßnahmen nach Absatz 2, also die Ermittlung spezifischer Gerätekennungen, die Standortermittlung und die Unterbrechung oder Verhinderung von Kommunikationsverbindungen.

Nach Nummer 2 kann die Maßnahme zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung durchgeführt werden. Dann müssen tatsächliche Anhaltspunkte vorliegen, die die begründete Annahme rechtfertigen, dass eine Straftat von erheblicher Bedeutung begangen werden soll. Der Gesetzgeber vermutet solche Anhaltspunkte insbesondere bei Informationen über Vorbereitungs- und Planungshandlungen. Der Begriff der Straftat von erheblicher Bedeutung ist bereits in § 10 Abs. 3 Satz 1 definiert. Er umfasst alle Verbrechen und alle weiteren in § 100a StPO aufgeführten Straftaten. Bei den Verbrechen handelt es sich um hinreichend gewichtige Delikte, die den Bereich der mittleren Kriminalität überschreiten und die daher geeignet sind, im Interesse der Verhinderung einer Straftat einen Eingriff in die Fernmeldefreiheit zu rechtfertigen. Dabei ist wie im gesamten Gefahrenabwehrrecht zu berücksichtigen, dass das Gewicht des durch die Strafnorm geschützten Rechtsguts und die Anforderungen an die Wahrscheinlichkeit des Eintritts der Rechtsgutsverletzung in einem umgekehrten Verhältnis stehen. Bei überragend wichtigen Gütern genügen daher geringere Anhaltspunkte, während bei einem weniger bedeutsamen Rechtsgut, das etwa durch eine geringere Strafandrohung geschützt wird, höhere Anforderungen an die Begründetheit der Annahme, dass die Straftat verwirklicht wird, zu stellen sind. § 100a StPO ist zudem die einschlägige Befugnisnorm für Beschränkungen des Fernmeldegeheimnisses im Rahmen der Strafverfolgung. Die Auswahl dieser Delikte wird daher den besonderen Anforderungen einer Telekommunikationsüberwachung gerecht.

## Absatz 2

Im Unterschied zur Überwachung und Aufzeichnung von Telekommunikationsdaten einschließlich der Telekommunikationsinhalte gewährt Absatz 2 die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von Telekommunikationsteilnehmern sowie zur Unterbrechung oder Verhinderung der Kommunikation. Diese Regelung ist angesichts der erheblichen Fortschritte auf dem

Gebiet der Telekommunikationstechnik erforderlich. Bei der Planung und Begehung von schweren Straftaten werden insbesondere von Angehörigen gewaltbereiter extremistischer Gruppen aber auch im Bereich der Organisierten Kriminalität zunehmend Mobiltelefone eingesetzt, deren Herkunft den Sicherheitsbehörden nicht bekannt ist, weshalb auch die Kennungen oftmals über einen Provider nicht ermittelt werden können. Nachdem die Angabe der Rufnummer oder einer anderen Kennung aber Zulässigkeitsvoraussetzung für eine Anordnung der Telekommunikationsüberwachung ist, muss der Polizei die Befugnis zur Ermittlung der erforderlichen Daten eingeräumt werden.

Der Einsatz von Geräten, wie etwa des sog. „IMSI-Catchers“, die zur Bestimmung der Geräte- und Kartennummern von Mobiltelefonen bzw. des Standortes von Mobilfunkendgeräten dienen, wird an die strengen Voraussetzungen des Absatzes 1 geknüpft, da er in der Regel zur Vorbereitung einer Telekommunikationsüberwachungsmaßnahme dient. Dies gilt insbesondere auch für die Subsidiaritätsregelung in Absatz 1.

Absatz 2 Nr. 2 enthält die Befugnis zur Ermittlung des Standortes eines Mobilfunkendgerätes. Die Maßnahme ist zur Abwehr von Straftaten von erheblicher Bedeutung und zum Schutz der in Absatz 1 Nr. 1 genannten Rechtsgüter ebenfalls unverzichtbar. Erfasst wird auch die Aussendung von funktechnischen Signalen, um die Standortkennung eines Endgerätes zu erhalten. Zulässigkeitsvoraussetzung für Maßnahmen nach Nummer 2 ist nicht, dass sich das Telekommunikationsgerät im Sendebetrieb befindet. Ausreichend ist der „Stand-By-Betrieb“.

Insbesondere die Suche nach vermissten oder hilflosen Personen, die sich in einer konkreten Gefahrenlage befinden, wird durch Standortbestimmungsmaßnahmen nach Absatz 2 Nr. 2 wesentlich erleichtert. Durch erheblichen Zeitgewinn können gerade bei Unglücksfällen oder bei Suizidgefahr Leben gerettet werden. Voraussetzung für die Maßnahme ist dabei stets, dass sie zur Abwehr einer Gefahr für Leben oder Gesundheit der jeweils betroffenen Person erforderlich ist. Für den Einsatz technischer Geräte zur Ortung von Mobiltelefonen, die Vermisste bei sich tragen, bzw. für die Datenerhebung fehlt es bisher an einer Rechtsgrundlage. Der Einsatz kann lediglich auf den in § 34 des Strafgesetzbuches (rechtfertigender Notstand) niedergelegten Rechtsgedanken des übergesetzlichen Notstandes gestützt werden, der Lösungsansätze zur Reaktion auf außerordentliche, unvorhersehbare Interessenkollisionen bietet. Die Polizei benötigt aber eine eindeutige Rechtsgrundlage, um künftig zum Schutz von Leben und Gesundheit die vorhandenen technischen Möglichkeiten nutzen zu können. Im Schnitt werden durch die Polizei monatlich sechs Suizidenten gesucht, die mittels Mobilfunkortung wesentlich schneller gerettet werden können. Der Einsatz eines IMSI-Catchers ist auch im UMTS-Netz technisch ohne weiteres möglich

In Anbetracht der Tatsache, dass die modernen Kommunikationstechniken gerade von terroristischen Netzwerken zur Begehung von Anschlägen genutzt werden, aber auch vor dem Hintergrund der zunehmenden technischen Vernetzung der Beteiligten bei organisierter Kriminalität, müssen der Polizei zur Abwehr von Gefahren für hochrangige Rechtsgüter und zur Verhinderung von schwerwiegenden Straftaten neuartige Befugnisse eröffnet werden. Die Anschläge von Madrid haben gezeigt, dass Mobiltelefone im Zusammenhang mit Zündmechanismen für Sprengstoffe Verwendung finden. Darüber hinaus sind Fallgestaltungen bekannt, in denen eine Telekommunikation zur Abwehr von Gefahren oder zum Zweck der Verhinderung und Unterbindung von Straftaten unterbrochen oder gänzlich verhindert werden muss. An Befugnisnormen für die Unterbrechung oder Verhinderung von Kommunikationsverbindungen fehlt es bisher. Diese sicherheitsrechtliche Lücke wird durch Absatz 2 Nr. 3 geschlossen. Die Sicherheitsbehörden können durch den Einsatz technischer Mittel, wie etwa des sogenannte „IMSI-Catchers“ oder von Störsendern, so genannten „Jammern“, die Telekommunikation der in Absatz 3 genannten Personen unterbrechen oder verhindern. Nicht erfasst sind dagegen Anordnungen gegenüber Diensteanbietern zur Unterbrechung des Telekommunikationsverkehrs. Auch dieser Eingriff ist an

die strengen Voraussetzungen des Absatzes 1 geknüpft. Die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen ist nicht gleichzusetzen mit der Abschaltung ganzer Mobilfunknetze. Der Arbeitskreis II - Innere Sicherheit - der Ständigen Konferenz der Innenminister und Senatoren der Länder hat sich mit diesem Thema während seiner Sitzung am 25./26. Oktober 2005 befasst und unter anderem die folgenden Beschlüsse gefasst:

*„1. Der AK II nimmt den Bericht der Projektgruppe des UA FEK (FF), des UA luK, des UA RV und des BKA zur „Abschaltung von Mobilfunknetzen der Provider in konkreten Bedrohungs- und Anschlaglagen (Stand: 01.09.2005)“ sowie die hierzu ergangenen Beschlüsse des UA FEK vom 14.09.2005, des UA luK vom 21.09.05 und des UA RV vom 16.09.05 zur Kenntnis.*

*2. Er ist der Auffassung, dass die Möglichkeit einer „regionalen Totalabschaltung der Mobilfunknetze durch die Netzbetreiber“ zur Verhinderung von Anschlägen aufgrund der aus technischer und einsatztaktischer Sicht bestehenden Bedenken, angesichts bestehender Zweifel an der Erforderlichkeit der Maßnahme im Hinblick auf den Verhältnismäßigkeitsgrundsatz sowie wegen der Tatsache, dass auch diese Maßnahme eine Auslösung nicht bekannter unkonventioneller Spreng- und Brandvorrichtungen (USBV) nicht zuverlässig verhindern kann, derzeit nicht weiter verfolgt werden sollte.*

*3. Der AK II stellt ebenso fest, dass die im Bericht beschriebene „Nichtweiterleitung von Anrufen in bestimmte Funkzellen“ im Vergleich zu einer „regionalen Totalabschaltung der Mobilfunknetze durch die Netzbetreiber“ das unter dem Gesichtspunkt der Verhältnismäßigkeit mildere Mittel darstellt und daher genauer auf ihre technische und finanzielle Machbarkeit geprüft werden sollte. Er bittet daher den UA luK gemeinsam mit den Netzbetreibern zu prüfen, ob bzw. wie die „Nichtweiterleitung von Anrufen in bestimmte Funkzellen“ als Maßnahme zur Verhinderung von Anschlägen realisiert werden kann.*

*4. Der AK II ist der Ansicht, dass die in dem Bericht „Abschaltung von Mobilfunknetzen der Provider in konkreten Bedrohungs- und Anschlaglagen“ beschriebenen Maßnahmen „Priorisierung berechtigter Teilnehmer“, „Sperrung verdächtiger Teilnehmer“, „Einsatz von Jammern“ sowie „Einsatz von IMSI-Catchern“ im Einzelfall potentiell erfolgreiche taktische Einsatzvarianten im Umfeld von Anschlägen darstellen können. Er empfiehlt daher den Bundesländern, die Schaffung der für die Umsetzung dieser Maßnahmen notwendigen Voraussetzungen zu prüfen.“*

Diese Überprüfung hat für Brandenburg ergeben, dass der IMSI-Catcher, dessen Einsatz sich bei der Verfolgung von Straftaten bereits bewährt hat, für die Ermittlung spezifischer Gerätekennungen, für die Lokalisierung von Mobilfunkendgeräten sowie für die Verhinderung von bestimmten Telekommunikationsverbindungen geeignet ist. Der Einsatz von angemessen dimensionierten Störsendern, so genannten „Jammern“ eignet sich, um Mobilfunkverbindungen zu unterbrechen oder zu verhindern. Mit dem vorliegenden Gesetz werden die rechtlichen Voraussetzungen für den Einsatz dieser technischen Mittel geschaffen.

Die Standortermittlung, die Ermittlung von spezifischen Gerätekennungen sowie das Verhindern von Telekommunikation durch Mobilfunkgeräte kann mit Hilfe des IMSI-Catchers nahezu ohne Beeinträchtigung der Telekommunikation Dritter stattfinden, weil solche Maßnahmen sich technisch auf das vom Adressaten der Maßnahme benutzte Endgerät beschränken lassen.

Eine Beeinträchtigung der Mobilfunkkommunikation Dritter kann beim Einsatz von Störsendern hingegen zwar den örtlichen Gegebenheiten entsprechend minimiert werden, indem sie z.B. auf bestimmte Gebäude beschränkt wird. Sie kann aber nicht völlig ausgeschlossen werden. In Anbetracht des Ausmaßes der abzuwehrenden Gefahr erscheint aber die, zudem räumlich eng begrenzte Beeinträchtigung

Dritter hinnehmbar, insbesondere wenn diese auf andere Fernkommunikationsmittel, wie z.B. Festnetzverbindungen, ausweichen können.

### Absatz 3

Adressaten der Maßnahme sind nach Satz 1 Nr. 1 die nach den §§ 5 und 6 für eine Gefahr verantwortlichen Personen sowie – unter den engen Voraussetzungen des § 7 – gegen den Notstandspflichtigen. Die Einbeziehung dieses Adressatenkreises ist bereits bei der Wohnraumüberwachung zulässig (VerfGBbg, Urteil vom 30. Juni 1999 - VfGBbg: 3/98 -, D.IV.2.c.bb. [1]). Ihre Zulässigkeit bei Eingriffen in die Telekommunikation ergibt sich aus der Subsidiarität der Wohnraumüberwachung gegenüber der Telekommunikationsüberwachung.

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

Berufsheimnisträger sind besonders geschützt, soweit sie ein Recht zur Zeugnis-Verweigerung nach §§ 53, 53a StPO haben. Insoweit ist eine Überwachung unzulässig und zieht Verwendungseinschränkungen oder -verbote nach sich. Dies gilt jedoch nicht, wenn die entgegengenommenen Mitteilungen, die die Gefahrverursachung betreffen müssen, von ihnen weitergeleitet werden, sie also als Boten tätig sind, oder wenn die genannten Adressaten ihre Telekommunikationseinrichtungen benutzen. In Satz 2 wird ein Erhebungsverbot für Gespräche mit Berufsheimnisträgern angeordnet. Das Erhebungsverbot greift jedoch dann nicht, wenn der Berufsheimnisträger selbst Adressat der Maßnahme ist.

Durch Standortbestimmungsmaßnahmen nach Absatz 2 Nr. 2 soll insbesondere die Suche nach vermissten oder hilflosen Personen, die sich in einer konkreten Gefahrenlage befinden, erleichtert werden. Durch die Einbeziehung dieser Personen in den Anwendungsbereich von Abs. 3 als Störer oder Notstandspflichtige ist diese Grundlage geschaffen.

Andere Personen als die in Satz 1 Nr. 1 und 2 genannten können dagegen keine Adressaten sein und dürfen daher nur dann von der Maßnahme betroffen werden, wenn dies unvermeidbar ist, weil sie Kommunikationspartner des Adressaten oder aus technischen Gründen unvermeidlich betroffene Dritte sind (vgl. Absatz 4).

Der Schutz des Kernbereichs privater Lebensgestaltung wird in ähnlicher Weise wie bei der Wohnraumüberwachung gewährleistet und zwingt bei dessen drohender Verletzung zur Unterbrechung der Maßnahme.

Auf die ausdrückliche Normierung von Verwendungsverböten wurde verzichtet. Aus der Unzulässigkeit einer erkennbar in geschützte Vertrauensverhältnisse oder in den Kernbereich privater Lebensgestaltung eingreifenden Überwachung der Telekommunikation ergibt sich unmittelbar aus Artikel 20 Abs. 3 Grundgesetz zugleich das Verbot, die dadurch gewonnen Daten zu verwenden. Der Vorbehalt der Erkennbarkeit trägt den Besonderheiten der Telekommunikationsüberwachung Rechnung. Anders als bei der Wohnraumüberwachung ist nicht in jedem Falle sofort ersichtlich, in welchem Verhältnis die Kommunizierenden zueinander stehen. Zudem sind Fälle ausgeschlossen, in denen erst bei (nachträglicher) Auswertung der Aufzeichnungen erkannt wird, dass ein Gespräch vorliegt, dessen Aufzeichnung unzu-

lässig war. Welche Maßnahmen zu treffen sind, um die Erkennbarkeit sicherzustellen, richtet sich nach den Umständen des Einzelfalles.

Ein Erhebungsverbot zum Schutz besonderer Vertrauensverhältnisse, die nicht auf einem Berufsgeheimnis beruhen, ist nicht vorgesehen. Eine Prognose, mit wem ein Telefongespräch zustande kommt und in welchem Verhältnis beide Gesprächspartner zueinander stehen, kann in der Regel gar nicht angestellt werden, angesichts der Häufigkeit und Vielgestaltigkeit von Telekommunikationsvorgängen. Vielfach lässt sich ohne weitere Auswertung nicht einmal feststellen, mit welcher Person gesprochen wird, etwa wenn keine Namensnennung erfolgt oder weil es sich um eine fremdsprachige Kommunikation handelt. Dies gilt umso mehr in Fällen, in denen ein Störer gezielt eine Überwachung ausschließen oder erschweren will, indem er Vertrauensverhältnisse vortäuscht oder indem in Absprache mit den jeweiligen Kommunikationspartnern eine Vielzahl von Verbindungen, insbesondere im Bereich der Mobiltelefone, genutzt wird. Gerade bei international operierenden Kriminellen, etwa im Bereich der Organisierten Kriminalität oder des internationalen Terrorismus, dürfte es ohne weiteres möglich sein, durch entsprechende Chiffrierung bei jedem Gespräch, das die Begehung einer Straftat oder die Verursachung einer Gefahr für hochrangige Rechtsgüter betrifft, ein Vertrauensverhältnis oder eine familiäre Bindung zu fingieren.

Vor allem bei Gesprächen mit Auslandsbezug wird es den Ermittlungsbehörden in der Regel nicht möglich sein, zu überprüfen, ob es sich tatsächlich um einen engsten Vertrauten handelt oder ob dies durch geschickte Wahl der Kommunikationsinhalte, etwa eine persönliche Anrede, nur vorgetäuscht wird. Bei sonstigen Vertrauten kann der Kommunikationspartner nicht wie bei den Gesprächen mit Berufsgeheimnisträgern, die regelmäßig nur über eine begrenzte Zahl an Kommunikationsverbindungen verfügen und bei denen der ständige Wechsel der Anschlüsse nicht in Betracht kommt, relativ genau identifiziert werden. Bei Ärzten, Anwälten, Journalisten und den anderen in § 53 StPO genannten Berufsgruppen besteht zudem eine weitaus geringere Missbrauchsgefahr. Anders als bei undifferenzierten Personenkontakten kann davon ausgegangen werden, dass der Gesprächspartner seine besondere Vertrauensstellung nicht ausnutzt, um mit dem Adressaten bei der Begehung schwerwiegender Straftaten oder der Verursachung von Gefahren zusammenzuwirken. Sollte dies ausnahmsweise doch der Fall sein, greift die Sonderregelung in Satz 2 ein, wonach keine Schutzwürdigkeit besteht, wenn ein Berufsgeheimnisträger selbst Maßnahmedressat ist, weil er die Voraussetzungen für eine Überwachung ebenfalls erfüllt. Bei Vertrauensbeziehungen, die nicht auf einem Berufsgeheimnis beruhen, ist daher eine erste Sichtung von Gesprächsinhalten erforderlich. Dies ist nach der Rechtsprechung des Bundesverfassungsgerichts selbst bei der Wohnraumüberwachung zulässig, wenn nicht von vornherein ein Eingriff in den Kernbereich in Betracht kommt. Dementsprechend erfolgt eine Überprüfung der Gesprächsinhalte und der Schutzbedürftigkeit im Rahmen der Auswertung der gewonnenen Daten. Eine entsprechende Schutzfunktion entfaltet Absatz 9 Satz 1 und 2.

#### Absatz 4

Absatz 4 regelt den Schutz unbeteiligter Dritter bei Maßnahmen der Telekommunikationsüberwachung, -unterbrechung und -verhinderung. Die Unterbrechung oder Verhinderung von Telekommunikationsverbindungen Dritter kann bei sogenannten Sprengstofffallen erforderlich sein, wenn die Polizei davon Kenntnis erlangt, dass ein Sprengkörper über ein Mobilfunkgerät ferngesteuert gezündet werden soll. Gleiches muss bei Geisellagen gelten, um die Kommunikation des Geiselnahmens mit Komplizen außerhalb des Tatorts über die Mobiltelefone Dritter unterbinden zu können. Die insoweit nicht auszuschließende Inanspruchnahme Dritter ist bei Abwägung ihrer Rechtspositionen mit den durch die polizeiliche Maßnahme zu schützenden Rechtsgütern angemessen und verhältnismäßig. Insbesondere bei einer Unterbrechung von Mobilfunkverbindungen verbleiben den betroffenen Dritten zudem auch noch andere Kommunikations- und Fernkommunikationsmittel, wie das Internet oder ein Festnetz-

Telefonanschluss. Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, sind diese unverzüglich zu löschen. Die Beeinträchtigungen für die Diensteanbieter sind aufgrund der technischen Fortschritte im Bereich der Überwachungsgeräte gering und daher zumutbar.

#### Absatz 5

Die Regelung über das Verfahren zur Datenerhebung bei der Telekommunikationsüberwachung in Absatz 5 orientiert sich an den entsprechenden Maßgaben in der Strafprozessordnung. Durch die besonderen verfahrensrechtlichen Absicherungen wird den Vorgaben des Bundesverfassungsgerichts folgend den datenschutzrechtlichen Erfordernissen entsprochen.

Zur Durchführung der Maßnahme ist gemäß Satz 1 die richterliche Entscheidung notwendig, um dem Schutz des Fernmeldegeheimnisses aus Artikel 10 Grundgesetz Rechnung zu tragen. Zwar wird der Richtervorbehalt in Artikel 10 Grundgesetz nicht ausdrücklich gefordert, jedoch gewährleistet er in besonderer Weise die Überwachung der Maßnahme und bietet angemessenen Grundrechtsschutz durch Verfahren. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Behörde ihren Sitz hat. Anders als bei der Wohnraumüberwachung ist die richterliche Anordnung bei Eingriffen in die Telekommunikation nicht einem Kollegialgericht übertragen. Auch damit wird die Subsidiarität der Wohnraumüberwachung gegenüber den in § 33b genannten Maßnahmen deutlich zum Ausdruck gebracht.

Lediglich bei Gefahr im Verzug kann die Anordnung, wie bei der Wohnraumüberwachung, durch den Behördenleiter erfolgen. Behördenleiter ist dabei der Leiter einer Polizeibehörde, nicht also etwa die nach der Polizeistrukturereform mit weitgehender Selbständigkeit ausgestatteten Leiter der Schutzbereiche der Polizeipräsidien. Der Begriff „Behördenleiter“ bezeichnet die Funktion und nicht die Person. Die Anordnungsbefugnis erstreckt sich daher auch immer auf den jeweiligen Vertreter im Amt. Die richterliche Bestätigung ist bei Behördenleiteranordnungen unverzüglich nachzuholen.

Satz 2 regelt die örtliche und sachliche Zuständigkeit für das Anordnungsverfahren. Sachlich zuständig ist das Amtsgericht. Örtlich zuständig ist das Gericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat.

In Satz 4 werden die formellen Anforderungen an die Anordnungen nach Satz 1 normiert. Diese haben schriftlich zu erfolgen. Dies hat vor allem Beweis- und Warnfunktion.

Die zulässige Anordnungsdauer in Satz 5 orientiert sich an der Regelung für die Wohnraumüberwachung. Durch die Monatsfrist wird eine effektive gerichtliche Kontrolle gewährleistet. Die Fristen für die Telekommunikationsunterbrechung und -verhinderung nach Absatz 2 Nr. 3 sind vor dem Hintergrund des Übermaßverbotes kürzer.

Darüber hinaus besteht nach Satz 6 die Möglichkeit der Verlängerung der Maßnahmen. In Konkretisierung des Verhältnismäßigkeitsgrundsatzes wird in Satz 7, 1. Halbsatz klargestellt, dass die jeweiligen Maßnahmen zu beenden sind, wenn die Voraussetzungen entfallen. Die Mitteilungspflicht bei Beendigung gemäß Halbsatz 2 ist erforderlich, da der Richter die Maßnahme nicht nur anordnet, sondern auch überwacht.

#### Absatz 6

Die Mitwirkungspflichten der Diensteanbieter werden in Absatz 6 geregelt. Diensteanbieter ist, wer ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder daran – auch als Vertriebspartner – mitwirkt (vgl. § 3 Nr. 6 TKG). Die Pflicht zur Ermöglichung der Telekommunikationsüberwa-

chung ist als notwendige Ergänzung der Befugnisnormen in Absatz 1 geregelt. Die Mitwirkungspflichten der Diensteanbieter bei der Telekommunikationsüberwachung sind angesichts der technischen Gegebenheiten unverzichtbar für die Durchführung der Maßnahmen. Dies gilt in besonderem Maße bei Festnetz-Telefonanschlüssen. Die den Diensteanbietern dadurch auferlegte Belastung geht nicht über diejenige hinaus, die ihnen nach der vergleichbaren Regelung in der Strafprozessordnung obliegt und die im für die technische Umsetzung von Telekommunikationsüberwachungsmaßnahmen maßgeblichen TKG festgeschrieben ist. In § 110 Abs. 1 Satz 6 TKG wird ausweislich der Begründung klargestellt, dass die landesgesetzlichen Regelungen zur präventiv-polizeilichen Telekommunikationsüberwachung nicht durch die Vorschrift des § 110 TKG eingeschränkt werden (BR-Drs. 755/03, S. 126). Daher ergeben sich keine kompetenzrechtlichen Bedenken gegen die Normierung landesgesetzlicher Verpflichtungen.

Nach Satz 2 können Diensteanbieter verpflichtet werden, bei ihnen vorhandene oder künftig anfallende Telekommunikationsverkehrsdaten zur Verfügung zu stellen. Ohne die Übermittlung dieser Informationen ist es der Polizei vielfach nicht möglich, Verflechtungen und Zusammenhänge im unübersichtlichen und vielschichtigen Bereich der Organisierten Kriminalität und des (internationalen) Terrorismus zu erkennen und effektive Maßnahmen zur Gefahrenabwehr zu treffen. Gerade bei stark nach außen abgeschotteten Gruppen und konspirativ angelegten Strukturen ist die Kenntnis dieser Daten unbedingt erforderlich. Auch bei der Suche nach vermissten, hilflosen oder suizidgefährdeten Personen ist die Übermittlungsbefugnis notwendig.

Durch die Kenntnis der letzten Gesprächsdaten können entscheidende Hinweise zur Auffindung einer vermissten oder hilflosen Person gewonnen werden, wenn eine konkrete Gefahr besteht. Gegenstand der Übermittlung sind vorhandene und - ebenso, wie im Bereich der Strafverfolgung möglich - zukünftige Verkehrsdaten soweit sie bei den Diensteanbietern vorliegen sowie über die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartenummer sowie die Zellinformationen, ohne die eine Lokalisation des Mobilfunktelefons nicht möglich wäre. Die Übermittlungspflicht betrifft die Daten der in den zitierten Vorschriften genannten Personen.

Zur Klarstellung der Entschädigungspflicht gegenüber den betroffenen Diensteanbietern verweist Satz 3 auf die bundesrechtlichen Regelungen. Solange die Rechtsverordnung nach § 110 Abs. 9 TKG noch nicht erlassen wurde, richtet sich die Entschädigung nach § 23 des Justizvergütungs- und -entschädigungsgesetzes.

#### Absatz 7

Die Benachrichtigungspflicht erfasst neben den Adressaten der Maßnahme die Personen, deren Daten zu den Zwecken der Strafverfolgung verwendet wurden. Aus dem Rechtsgedanken heraus, dass die grundrechtliche Betroffenheit mit den Interessen des jeweiligen Adressaten abzuwägen ist und dass die Benachrichtigung nicht zu Vertiefungen der Eingriffe führen darf, ist eine Einschränkung des Kreises der zu benachrichtigenden Personen gerechtfertigt.

Da die nachträgliche Unterrichtung Betroffener schon in der allgemeinen datenschutzrechtlichen Vorschrift des § 29 Abs. 6 und 7 geregelt ist, wird zur Vermeidung von Doppelbestimmungen deklaratorisch auf diese Norm verwiesen. Für die Zurückstellung der Benachrichtigung und die näheren Bestimmungen über das Verfahren gelten die zu § 29 Abs. 7 dargelegten Grundsätze entsprechend.

Abweichend von dieser Unterrichtung nach § 29 Abs. 6 und 7 wird für Fälle, in denen im Anschluss an die präventivpolizeiliche Wohnraumüberwachung ein strafrechtliches Ermittlungsverfahren eingeleitet wurde, bestimmt, dass die Unterrichtung der hiervon Betroffenen in Absprache mit der Staatsanwalt-

schaft erfolgt und zudem unterbleiben kann, wenn der Betroffene aus dem Ermittlungsverfahren Kenntnis über die Maßnahme erhält. Diese Verfahrensweise zeichnet die übliche Verteilung der Befugnisse zur Erteilung von Auskünften in strafrechtlichen Ermittlungsverfahren gemäß § 475 Abs. 1 StPO nach.

#### Absatz 8

Die Zweckbindungs- und Kennzeichnungspflichten sind in Absatz 8 geregelt. Sie gewährleisten, dass die gewonnenen Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden. Abweichend hiervon ist eine Zweckrichtungsänderung vorgesehen, wenn der Schutz hochwertiger Rechtsgüter dies erforderlich macht.

Eine solche Zweckrichtungsänderung ist vom Bundesverfassungsgericht anerkannt, wenn sie „durch Allgemeinbelange gerechtfertigt ist, die die grundrechtlich geschützten Interessen überwiegen“ (BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98, 1 BvR 1084/99 -, Rn. 334). Dem trägt die Vorschrift durch die Bezugnahme auf eine dringende Gefahr Rechnung. Bei einer Zweckänderung durch Verwendung zur Strafverfolgung richtet sich die Zulässigkeit danach, ob die Daten zur Verfolgung von Straftaten nach § 100a Satz 1 StPO erforderlich sind. Dies bedeutet aber auch, dass die Daten nur zur Verfolgung solcher Straftaten übermittelt werden dürfen, die selbst Voraussetzung für eine Wohnraumüberwachung nach § 100a StPO sind.

#### Absatz 9

Das Verwendungsverbot in Satz 1 erfasst Datenerhebungen, bei denen sich nach Auswertung herausstellt, dass die Erhebungsvoraussetzungen nicht vorgelegen haben. Eine Verwertung ist allerdings ausnahmsweise zulässig, wenn dies zum Schutz hochwertigster Rechtsgüter vor gegenwärtigen Gefahren erforderlich ist. In derartigen Fällen ist unverzüglich eine richterliche Entscheidung über die Verwendung nachzuholen.

Sind rechtmäßig erhobene Daten nicht mehr erforderlich, sind sie zu sperren, d.h. die weitere Verarbeitung der Daten ist zu verhindern (vgl. § 3 Abs. 2 Nr. 5 BbgDSG). Diese Bestimmung stärkt die Rechtsstellung der Betroffenen bei der nachträglichen gerichtlichen Überprüfung einer abgeschlossenen Maßnahme. Hierfür steht dem Betroffenen, ebenso wie bei der Wohnraumüberwachung gemäß 33a Abs. 8 Satz 5, eine Frist von zwei Wochen zur Verfügung. Spätestens wenn die Daten auch für eine gerichtliche Überprüfung nicht erforderlich sind, bzw. nach Ablauf der 2-Wochenfrist, sind sie nachweislich zu löschen.