**SCHLESWIG-HOLSTEINISCHER LANDTAG** **Drucksache 16/2135**
16. Wahlperiode 2008-07-01

# Gesetzentwurf

der Landesregierung

**Entwurf eines Gesetzes zur Umsetzung der Terrorismusbekämpfungsgesetze und zur Stärkung der parlamentarischen Kontrolle**

**Federführend ist das Innenministerium**

## A. Problem

Der internationale Terrorismus hat sich seit den Anschlägen des 11. September 2001 zu einer weltweiten Bedrohung entwickelt. Wie die Festnahmen von unter Terrorismusverdacht stehenden Verdächtigten gezeigt haben, ist die neue Bedrohung auch in Schleswig-Holstein gegenwärtig. Um den Gefahren des internationalen Terrorismus wirksam begegnen zu können, gilt es, jene bereits im Vorfeld aufzuklären. Dabei kommt dem Verbund der Verfassungsschutzbehörden des Bundes und der Länder eine entscheidende Bedeutung zu. Die Zusammenarbeit der Verfassungsschutzbehörden setzt einen gemeinsamen rechtlichen Mindeststandard voraus, der mit dem Bundesverfassungsschutzgesetz vorgegeben ist. Vor diesem Hintergrund haben die Bundesländer das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) und zum Teil auch das Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) landesrechtlich umgesetzt. Allein in Schleswig-Holstein ist dies noch nicht geschehen.

## B. Lösung

Die Terrorismusbekämpfungsgesetze sind im hiesigen Landesverfassungsschutzgesetz umzusetzen. Dabei muss die Erweiterung verfassungsschutzbehördlicher Befugnisse mit einer Stärkung der parlamentarischen Kontrolle einhergehen.

Zur Umsetzung der Terrorismusbekämpfungsgesetze sind

- der Beobachtungsauftrag der Verfassungsschutzbehörde auf den internationalen Terrorismus zu erweitern,
- Auskunftspflichten von Privatunternehmen, insbesondere zu Passagier-, Konto- und Telekommunikationsdaten einzuführen und
- der Einsatz technischer Mittel zum Ausfindigmachen von Mobiltelefonen zu regeln.

Zur Stärkung der parlamentarischen Kontrolle sind

- ein parlamentarisches Kontrollgremium zu schaffen, in dem die Kontrolle über die Angelegenheiten des Verfassungsschutzes und über die verfassungsschutzbehördliche Durchführung der Post- und Fernmeldeüberwachung gebündelt wird, sowie
- die Unterrichtungspflichten der Verfassungsschutzbehörde nach Maßgabe des umzusetzenden Bundesrechts zu präzisieren.

Ziel muss es sein, das Verfassungsschutzrecht unter Berücksichtigung der konkreten Erfordernisse der Praxis in moderater Weise anzupassen. Die landesrechtliche Umsetzung der Terrorismusbekämpfungsgesetze soll sich auf deren essenziellen Kernbestand beschränken.

Gleichzeitig gilt es, den Grundrechtsschutz zu stärken. Besonderer Bedeutung kommt dabei der Bezeichnung und rechtlichen Ausgestaltung der bereits bestehenden nachrichtendienstlichen Mittel zu. Der Entwurf sieht nicht nur eine Präzisierung der Eingriffsvoraussetzungen, des Adressatenkreises und der zu beachtenden Verfahren vor. Überdies werden ein genereller Schutz des Kernbereichs

privater Lebensgestaltung und der Berufsgeheimnisträger gesetzlich verankert. Auf diese Weise wird den Grundsätzen der Verhältnismäßigkeit, Bestimmtheit und Rechtsklarheit Rechnung getragen.

## C. Alternativen

Alternativen bestehen keine. Ein Verzicht auf die Fortentwicklung des Landesverfassungsschutzrechts kommt angesichts der neuen Bedrohungslage und der Harmonisierungspflicht gegenüber dem Bund und den Ländern nicht in Betracht. Andererseits kann auch eine zusätzliche Verschärfung des Gesetzes derzeit nicht empfohlen werden.

## D. Kosten und Verwaltungsaufwand

### 1. Kosten

Keine.

### 2. Verwaltungsaufwand

Die Betätigung der erweiterten Befugnisse führt naturgemäß zu einem Mehr an Verwaltungsaufwand. Dem steht jedoch eine Entlastung bei der Anwendung bestehender nachrichtendienstlicher Mittel gegenüber. So können z. B. personalintensive und somit kostenträchtige Observationen effizienter durchgeführt werden, wenn von der neuen Befugnis des Ausfindigmachens von Mobiltelefonen Gebrauch gemacht werden kann. Insgesamt ist danach ein erhöhter Verwaltungsaufwand nicht zu erwarten.

### 3. Auswirkungen auf die private Wirtschaft

Die Privatwirtschaft wird durch die Auskunftspflichten der Luftfahrtunternehmen sowie der Finanz-, Post-, Telekommunikations- und Telemediendienstleister belastet. Ausgehend von der Vollzugspraxis des Bundesamtes für Verfassungsschutz ist aber anzunehmen, dass die Auskunftspflichten nur zurückhaltend angeordnet werden (BT-Drs. 16/5982, S. 4). Im Übrigen stehen der Belastung der Unternehmen Einsparungen gegenüber, die sich aus einer verbesserten Sicherheitslage und der ungestörten Entwicklung der Volkswirtschaft ergeben.

## E. Information des Landtages nach Artikel 22 der Landesverfassung in Verbindung mit dem Parlamentsinformationsgesetz

Der Landtag ist mit Schreiben vom 16. April 2008 über den Gesetzentwurf unterrichtet worden.

## F. Federführung

Federführend ist das Innenministerium.

**Gesetz zur Umsetzung der Terrorismusbekämpfungsgesetze und zur Stärkung der parlamentarischen Kontrolle**

**Vom**

Der Landtag hat das folgende Gesetz beschlossen:

## Artikel 1
## Änderung des Landesverfassungsschutzgesetzes

Das Landesverfassungsschutzgesetz vom 23. März 1991 (GVOBl. Schl.-H. S. 203), zuletzt geändert durch Gesetz vom 10. Dezember 2003 (GVOBl. Schl.-H. S. 651), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Nach § 8 werden die Angaben „§ 8 a Besondere Auskunftsverlangen“ und „§ 8 b Verfahren“ eingefügt.
   b) Die Angabe „§ 26 Parlamentarische Kontrollkommission“ wird durch die Angabe „§ 26 Parlamentarisches Kontrollgremium“ ersetzt.
   c) Nach § 26 wird die Angabe „§ 26 a G 10-Kommission“ eingefügt.

2. In § 5 Abs. 1 Nr. 3 wird der Punkt durch ein Komma ersetzt. Folgende Nummer 4 wird angefügt:

   „4. Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind.“

3. In § 6 Abs. 1 wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) In Satz 1 wird die Angabe „§ 5 Abs. 1 Nr. 1 und 3“ durch die Angabe „§ 5 Abs. 1 Nr. 1, 3 und 4“ ersetzt.
      bb) Folgender Satz 2 wird angefügt:

      „Verhaltensweisen von Einzelpersonen gelten als Bestrebungen im Sinne von Satz 1, wenn diese auf die Anwendung von Gewalt gerichtet

sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut des § 5 Abs. 1 schwerwiegend zu gefährden.“

b) In Absatz 3 wird wie folgt geändert:

aa) In Nummer 2 wird der Punkt durch ein Komma ersetzt und folgende Nummer 3 angefügt:

„3. Bestrebungen gegen den Gedanken der Völkerverständigung solche, die sich gegen die Erhaltung des Friedens, die Ächtung von Angriffskriegen und die allgemeinen Grundrechte der Staaten, insbesondere das Recht auf politische Unabhängigkeit sowie das Recht auf Selbsterhaltung, auf Gleichheit, Ehre und Teilnahme am völkerrechtlichen Verkehr richten.“

bb) Folgender Satz 2 wird angefügt:

„Ferner ist im Sinne des Gesetzes

1. Zielperson eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie

a) einer Bestrebung als Mitglied angehört,

b) sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht verfolgt,

c) als Einzelperson nach Absatz 1 Satz 2 einer Bestrebung gleichsteht oder

d) Bestrebungen oder Personen nach Buchstabe b und c nachdrücklich unterstützt.

2. Kontaktperson eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie zu der Zielperson

a) in näherer persönlicher oder geschäftlicher Beziehung steht,

b) über einen längeren Zeitraum Kontakt unterhält oder

c) Kontakt unter konspirativen Umständen hergestellt hat oder pflegt

und nicht zur Zielperson in einem gesetzlich geschützten Vertrauensverhältnis steht,

3. Nachrichtenmittler eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass

a) sie für die Zielperson bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt oder

b) die Zielperson ihre Adresse oder ihren Anschluss benutzt

und nicht zur Zielperson in einem gesetzlich geschützten Vertrauensverhältnis steht.“

4. § 8 wird wie folgt geändert:

a) Absatz 2 erhält folgende Fassung:

„(2) Die Verfassungsschutzbehörde darf Methoden und Gegenstände einschließlich technischer Mittel zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) anwenden. Nachrichtendienstliche Mittel sind insbesondere

1. die Verwendung fingierter biografischer, beruflicher oder gewerblicher Angaben (Legenden),

2. die Beschaffung, Erstellung und Verwendung von Tarnpapieren und Tarnkennzeichen,

3. die Beobachtung des Funkverkehrs auf nicht für den allgemeinen Empfang bestimmten Kanälen und

4. das heimliche Aufklären des Internets, soweit dadurch nicht nach § 1 Abs. 1 Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254), zuletzt geändert durch Artikel 5 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198), Telekommunikation überwacht oder aufgezeichnet wird, mit Ausnahme öffentlich zugänglicher Informationen.

Nachrichtendienstliche Mittel sind ferner

1. der Einsatz von verdeckten Ermittlerinnen und Ermittlern, Vertrauensleuten, Gewährspersonen und sonstigen geheimen Informantinnen und Informanten sowie von zum Zwecke der Spionageabwehr überworbenen Agentinnen und Agenten,

2. die Anfertigung verdeckter Bildaufnahmen oder -aufzeichnungen,

3. die planmäßig angelegte Beobachtung, welche

   a) innerhalb einer Woche länger als 24 Stunden oder

   b) über den Zeitraum einer Woche hinaus

vorgesehen ist oder tatsächlich durchgeführt wird (langandauernde Observation),

4. das Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel,

5. der Einsatz sonstiger besonderer, für Observationszwecke bestimmter, technischer Mittel zur Erforschung des Sachverhaltes oder zur Ermittlung des Aufenthaltsortes der Zielperson,

6. der Einsatz technischer Mittel zur Ermittlung

   a) der Geräte- und Kartennummer eines Mobilfunkendgerätes sowie

   b) des Standortes eines aktiv geschalteten Mobilfunkendgerätes

(Ausfindigmachen eines Mobilfunkendgerätes),

7. die Post- und Fernmeldeüberwachung nach dem Artikel 10-Gesetz.“

b) Die Absätze 4 und 5 werden durch folgende Absätze 4 bis 9 ersetzt:

„(4) Die Anwendung nachrichtendienstlicher Mittel ist unzulässig, wenn sich tatsächliche Anhaltspunkte dafür ergeben, dass dadurch allein solche Informationen erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Eine bereits laufende Datenerhebung sowie die Auswertung der erhobenen Daten ist in diesem Falle unverzüglich und solange wie erforderlich

zu unterbrechen. Sind bei der Anwendung nachrichtendienstlicher Mittel versehentlich Informationen aus dem Kernbereich privater Lebensgestaltung erhoben worden, sind diese unverzüglich zu löschen. Die Löschung ist zu dokumentieren. Informationen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, dürfen in keiner Weise verwertet oder übermittelt werden.

(5) Die Anwendung nachrichtendienstlicher Mittel nach Absatz 2 Satz 3 ist nur zulässig, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes der Zielperson auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre. Die Maßnahmen dürfen sich nur gegen Zielpersonen und Kontaktpersonen richten. Sie dürfen auch dann durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(6) Der Einsatz von verdeckten Ermittlerinnen und Ermittlern, Vertrauensleuten, Gewährspersonen und sonstigen geheimen Informantinnen und Informanten sowie von zum Zwecke der Spionageabwehr überworbenen Agentinnen und Agenten (Absatz 2 Satz 3 Nr. 1) und langandauernde Observationen (Absatz 2 Satz 3 Nr. 3) werden von der Leitung der Verfassungsschutzabteilung angeordnet. Im Falle der langandauernden Observation ist die Maßnahme auf höchstens drei Monate zu befristen. Die Verlängerung der Maßnahme bedarf der Anordnung durch die Innenministerin oder den Innenminister; § 8 b Abs. 1 Satz 1 bis 3 gilt entsprechend. Die Verlängerungsanordnung ist der betroffenen Person gemäß § 8 b Abs. 3 mitzuteilen; das Parlamentarische Kontrollgremium ist gemäß § 8 b Abs. 4 zu unterrichten.

(7) Der Einsatz technischer Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes (Absatz 2 Satz 3 Nr. 4) ist nur zulässig, wenn

1. die Voraussetzungen des § 8 a Abs. 2 vorliegen und

2. ohne den Einsatz der technischen Mittel die Ermittlung des Aufenthaltsortes der Zielperson auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Innerhalb von Wohnungen ist die Maßnahme unzulässig. Sie wird gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Die Anordnung ist der betroffenen Person gemäß § 8 b Abs. 3 mitzuteilen. Das Parlamentarische Kontrollgremium ist gemäß § 8 b Abs. 4 zu unterrichten. Für die Verarbeitung der erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden.

(8) Der Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (Absatz 2 Satz 3 Nr. 6) ist nur zulässig, wenn

1. die Voraussetzungen des § 8 a Abs. 2 vorliegen und

2. ohne den Einsatz der technischen Mittel die Ermittlung der Geräte- oder Kartennummer oder die Ermittlung des Standortes aussichtslos oder wesentlich erschwert wäre.

Die Maßnahme darf sich nur gegen Zielpersonen oder Nachrichtenmittler richten. Sie wird gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Über die Anordnung unterrichtet die Verfassungsschutzbehörde die G 10-Kommission (§ 8 b Abs. 2). Ferner teilt sie die Anordnung der betroffenen Person mit; § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung. Nach der Mitteilung steht der betroffenen Person der

Rechtsweg offen. Das Parlamentarische Kontrollgremium ist gemäß § 8 b Abs. 4 zu unterrichten. Für die Verarbeitung der erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden, wobei Daten, die von Dritten erhoben worden sind (Absatz 5 Satz 3), einem Verwendungsverbot unterliegen und nach Beendigung der Maßnahme unverzüglich zu löschen sind. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.

(9) Die Befugnis der Verfassungsschutzbehörde zur Post- und Fernmeldeüberwachung (Absatz 2 Satz 3 Nr. 7) ergibt sich aus dem Artikel 10-Gesetz, wobei die Beschränkungsmaßnahmen gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet werden. Zuständig für die Anordnung des Verzichts auf die Kennzeichnung von zu übermittelnden Daten, die durch eine Post- und Fernmeldeüberwachung gewonnen worden sind (§ 4 Abs. 3 Satz 1 des Artikel 10-Gesetzes), ist die Leitung der Verfassungsschutzabteilung; die für die Zustimmung zuständige Stelle ist die G 10-Kommission (§ 26 a)."

5. Folgende §§ 8 a und 8 b werden eingefügt:

„§ 8 a Besondere Auskunftsverlangen

(1) Die Verfassungsschutzbehörde darf im Einzelfall bei denjenigen, die geschäftsmäßig Postdienstleistungen, Telekommunikationsdienste oder Telemedien erbringen oder daran mitwirken, Auskunft über Daten einholen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien (Bestandsdaten) gespeichert worden sind, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die Verfassungsschutzbehörde darf im Einzelfall Auskunft einholen bei

1. Luftfahrtunternehmen zu Namen und Anschriften der Kundin oder des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg,

2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhaberinnen oder Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge,

3. denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken, zu den Umständen des Postverkehrs,

4. denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 4 und § 113 a des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198), und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten und

5. denjenigen, die geschäftsmäßig Telemedien erbringen oder daran mitwirken, zu

a) Merkmalen zur Identifikation der Nutzerin oder des Nutzers,

b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und

c) Angaben über die von der Nutzerin oder von dem Nutzer in Anspruch genommenen Telemedien,

soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 5 Abs. 1 genannten Schutzgüter vorliegen. Im Falle des § 5 Abs. 1 Nr. 1 gilt dies nur für Bestrebungen, die bezwecken oder auf Grund ihrer Wirkungsweise geeignet sind,

1. zu Hass oder Willkürmaßnahmen gegen Teile der Bevölkerung aufzustacheln oder deren Menschenwürde durch Beschimpfen, böswilliges Verächtlichmachen oder Verleumden anzugreifen und dadurch die Bereitschaft zur Anwendung von Gewalt zu fördern und den öffentlichen Frieden zu stören oder

2. Gewalt anzuwenden oder vorzubereiten, einschließlich dem Befürworten, Hervorrufen oder Unterstützen von Gewaltanwendung, auch durch Unterstützen von Vereinigungen, die Anschläge gegen Personen oder Sachen veranlassen, befürworten oder androhen.

(3) Die Auskunftsverlangen nach den Absätzen 1 und 2 sind gegenüber den zur Auskunft Verpflichteten schriftlich anzuordnen. Die Anordnung und die übermittelten Daten dürfen die Verpflichteten den Betroffenen oder Dritten nicht mitteilen.

(4) Anordnungen nach Absatz 2 dürfen sich nur gegen Zielpersonen sowie

1. bei Auskünften über Passagierdaten, Kontoverbindungsdaten und über Nutzungsdaten zu Telemedien (Absatz 2 Satz 1 Nr. 1, 2 und 5) gegen Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie die Leistung für die Zielperson in Anspruch nehmen, und

2. bei Auskünften über Post- und Telekommunikationsverkehrsdaten sowie über Nutzungsdaten von Telemedien (Absatz 2 Satz 1 Nr. 3 bis 5) gegen Nachrichtenmittler

richten. Satz 1 gilt für juristische Personen entsprechend.

(5) Auskunftspflichten zu Passagierdaten (Absatz 2 Satz 1 Nr. 1) werden von der Leitung der Verfassungsschutzabteilung angeordnet.

(6) Auskunftspflichten zu Kontoverbindungsdaten (Absatz 2 Satz 1 Nr. 2) werden gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Die Anordnung ist der betroffenen Person gemäß § 8 b Abs. 3 mitzuteilen.

(7) Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten von Telemedien (Absatz 2 Satz 1 Nr. 3 bis 5) werden gemäß § 8 b Abs. 1 von der Innenministerin oder dem Innenminister angeordnet. Über die Anordnung unterrichtet die Verfassungsschutzbehörde die G 10-Kommission (§ 8 b Abs. 2). Ferner teilt sie die Anordnung der betroffenen Person mit; § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung. Nach der Mitteilung steht der betroffenen Person der Rechtsweg offen. Für die Verarbeitung der erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.

(8) Über sämtliche Anordnungen nach Absatz 2 ist das Parlamentarische Kontrollgremium gemäß § 8 b Abs. 4 zu unterrichten. Das Innenministerium berichtet ferner dem Parlamentarischen Kontrollgremium des Bundes über Anordnungen nach Absatz 2; § 8 b Abs. 4 findet entsprechende Anwendung.

§ 8 b Verfahren

(1) Ist nach diesem Gesetz die Anordnung einer Maßnahme durch die Innenministerin oder den Innenminister vorgesehen, erfolgt jene auf Antrag der Leitung der Verfassungsschutzabteilung, im Falle der Verhinderung der Innenministerin oder des Innenministers durch die Vertreterin oder den Vertreter. Der Antrag ist schriftlich zu stellen und zu begründen. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(2) Ist nach diesem Gesetz eine Unterrichtung der G 10-Kommission (§ 26 a) vorgesehen, erfolgt jene durch die Verfassungsschutzbehörde vor dem Vollzug der Maßnahme. Bei Gefahr im Verzuge kann die Maßnahme auch bereits vor der Unterrichtung der Kommission vollzogen werden. Die G 10-Kommission prüft von Amts wegen oder auf Grund von Beschwerden die Zulässigkeit und Notwendigkeit der Maßnahme. § 15 Abs. 5 des Artikel 10-Gesetzes ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der durch die Maßnahme erlangten personenbezogenen Daten erstreckt. Anordnungen, die die G 10-Kommission für unzulässig oder nicht notwendig erklärt, sind unverzüglich aufzuheben. Die Daten unterliegen in diesem Falle einem absoluten Verwendungsverbot und sind unverzüglich zu löschen.

(3) Ist nach diesem Gesetz eine Mitteilung der betroffenen Person vorgesehen und nichts anderes bestimmt, erfolgt jene durch die Verfassungsschutzbehörde, sobald eine Gefährdung des Zwecks der Maßnahme ausgeschlossen werden kann. Einer Mitteilung bedarf es nicht, wenn diese Voraussetzung auch nach fünf Jahren noch nicht eingetreten ist. Sie unterbleibt ferner bei einem durch die Maßnahme unvermeidbar betroffenen Dritten im Sinne von § 8 Abs. 5 Satz 3, wenn die Mitteilung

1. nur mit unverhältnismäßigen Ermittlungen möglich wäre oder
2. überwiegende schutzwürdige Belange anderer betroffener Personen entgegenstehen.

Nach der Mitteilung steht der betroffenen Person der Rechtsweg offen.

(4) Ist nach diesem Gesetz eine Unterrichtung des Parlamentarischen Kontrollgremiums (§ 26) vorgesehen, erfolgt jene durch die Verfassungsschutzbehörde im Abstand von höchstens sechs Monaten. Dabei ist insbesondere ein Überblick über den Anlass, den Umfang, die Dauer, das Ergebnis und die Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben."

6. In § 10 Abs. 1 wird folgender Anstrich angefügt:

„- von Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen den Gedanken der Völkerverständigung (Arti-

kel 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 des Grundgesetzes) gerichtet sind,“

7. § 11 wird folgender Absatz 4 angefügt:

„(4) Die Verarbeitung der Daten darf zum Zwecke der Datenschutzkontrolle protokolliert werden. Die Protokolldaten dürfen auch zur Aufklärung eines Verdachts auf Datenmissbrauch verwendet werden.“

8. § 12 wird wie folgt geändert:

a) In Nummer 2 wird die Angabe „§ 5 Abs. 1 Nr. 1 oder 3“ durch die Angabe „§ 5 Abs. 1 Nr. 1, 3 oder 4“ ersetzt.

b) Es werden folgende Sätze angefügt:

„Personenbezogene Daten zu Minderjährigen, die das 14. Lebensjahr vollendet haben, dürfen nur gespeichert werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie eine der in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftaten planen, begehen oder begangen haben. Die Daten nach Satz 2 dürfen nicht in Dateien gespeichert werden.“

9. In § 13 Satz 3 wird die Angabe „§ 5 Abs. 1 Nr. 1 oder 3“ durch die Angabe „§ 5 Abs. 1 Nr. 1, 3 oder 4“ ersetzt.

10. In § 14 wird Absatz 3 gestrichen.

11. In § 15 werden die Worte „mit der oder dem Landesbeauftragten für den Datenschutz“ durch die Worte „mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein“ ersetzt.

12. In § 20 werden folgende Sätze angefügt:

„Abweichend von Satz 2 darf die Verfassungsschutzbehörde Informationen einschließlich personenbezogener Daten an die Nachrichtendienste von Mitgliedstaaten der EU, die an Schleswig-Holstein grenzen oder zu denen Fährverbindungen bestehen, übermitteln, wenn dies

1. zur Erfüllung der Aufgaben der Verfassungsschutzbehörde oder

2. zur Wahrung erheblicher Sicherheitsinteressen des Empfängers

erforderlich ist. Satz 3 gilt für das Königreich Norwegen entsprechend.“

13. § 23 wird wie folgt geändert:

a) In Absatz 1 wird folgender Satz 2 angefügt:

„Satz 1 gilt entsprechend für Ersuchen an die Behörden des Bundes und die bundesunmittelbaren juristischen Personen des öffentlichen Rechts

sowie für die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien des Bundes und anderer Länder.“

b) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 wird die Angabe „Absatz 1“ durch die Angabe „Absatz 1 Satz 1“ ersetzt.

bb) In Satz 3 wird die Angabe „§ 2 des Gesetzes zu Artikel 10 Grundgesetz“ durch die Angabe „§ 3 Abs. 1 des Artikel 10-Gesetzes“ ersetzt.

cc) Satz 5 erhält folgende Fassung:

„Auf die nach Satz 3 und 4 übermittelten Informationen findet § 4 des Artikel 10-Gesetzes entsprechende Anwendung.“

14. § 25 wird wie folgt geändert:

a) Absatz 1 werden folgende Sätze 2 und 3 angefügt:

„In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit die oder der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der oder dem Betroffenen geltend gemachten Informationsinteresse steht.“

b) Absatz 2 erhält folgende Fassung:

„(2) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der Aufgaben der Verfassungsschutzbehörde gefährden würde, insbesondere wenn die Gefahr einer Ausforschung der nachrichtendienstlichen Arbeitsmethoden und Mittel besteht,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.“

c) In § 25 Abs. 4 werden die Worte „an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz“ durch die Worte „an das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein“ ersetzt.

15. § 26 wird wie folgt geändert:

a) In der Überschrift werden die Worte „Parlamentarische Kontrollkommission“ durch die Worte „Parlamentarisches Kontrollgremium“ ersetzt.

b) In Absatz 1 werden folgende Sätze angefügt:

„Es nimmt überdies die Aufgabe des gleichnamigen Kontrollorgans nach § 14 des Artikel 10-Gesetzes wahr. § 14 Abs. 1 Satz 1 des Artikel 10-Gesetzes gilt entsprechend.“

c) In den Absätzen 1, 5 und 8 werden jeweils die Worte „die Parlamentarische Kontrollkommission“ durch die Worte „das Parlamentarische Kontrollgremium“ ersetzt.

d) In Absatz 2 und 6 Satz 1 sowie Absatz 9 werden jeweils die Worte „der Parlamentarischen Kontrollkommission“ durch die Worte „des Parlamentarischen Kontrollgremiums“ ersetzt.

e) In Absatz 2 wird das Wort „ihre“ durch das Wort „seine“ ersetzt.

f) In den Absätzen 2 und 7 werden jeweils die Worte „der Kommission“ durch die Worte „des Gremiums“ ersetzt.

g) In den Absätzen 4 und 6 Satz 2 und 3 werden jeweils die Worte „der Parlamentarischen Kontrollkommission“ durch die Worte „dem Parlamentarischen Kontrollgremium“ ersetzt.

h) In Absatz 8 Satz 2 wird das Wort „Sie“ durch das Wort „Es“ ersetzt.

16. Folgender § 26 a wird eingefügt:

„§ 26 a G 10-Kommission

(1) Die G 10-Kommission nimmt die Aufgaben des gleichnamigen Kontrollorgans nach § 15 des Artikel 10-Gesetzes wahr. § 15 Abs. 5 bis 7 des Artikel 10-Gesetzes gelten entsprechend. Sie ist ferner

1. beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (§ 8 Abs. 8) und

2. bei der Anordnung von Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten von Telemedien (§ 8 a Abs. 2 Nr. 3 bis 5)

zu beteiligen.

(2) Die Kommission besteht aus der oder dem Vorsitzenden, die oder der die Befähigung zum Richteramt besitzen muss, und zwei Beisitzern. Sie werden vom Landtag für die Dauer einer Wahlperiode mit der Maßgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der Kommission, spätestens jedoch drei Monate nach Ablauf der Wahlperiode, endet. Für jedes Mitglied der Kommission wird eine Vertreterin oder ein Vertreter bestellt, die oder der an den Sitzungen mit Rede- und Fragerecht teilnehmen kann. Die Mitglieder der Kommission sind in ihrer Amtsausführung unabhängig und Weisungen nicht unterworfen. Für die Geheimhaltung gilt § 26 Abs. 6 entsprechend. Die Kommission gibt sich eine Geschäftsordnung, die der Zustimmung des Parlamentarischen Kontrollgremiums (§ 26) bedarf.

17. § 27 wird wie folgt geändert:

a) In Satz 1 werden die Worte „Die Parlamentarische Kontrollkommission“ durch die Worte „Das Parlamentarische Kontrollgremium“ ersetzt.

b) In Satz 4 werden die Worte „der Parlamentarischen Kontrollkommission“ durch die Worte „dem Parlamentarischen Kontrollgremium“ ersetzt.

**Artikel 2**
**Inkrafttreten, Außerkrafttreten, Übergangsregelung**

(1) Das Gesetz tritt am Tage nach seiner Verkündung in Kraft. Gleichzeitig tritt das Gesetz zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz vom 17. Dezember 1968 (GVOBl. Schl.-H. S. 357), geändert durch Gesetz vom 2. November 1981 (GVOBl. Schl.-H. S. 248), Zuständigkeiten und Ressortbezeichnungen ersetzt durch Verordnung vom 24. Oktober 1996 (GVOBl. Schl.-H. S. 652), außer Kraft.

(2) Die auf der Grundlage des § 3 des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz gebildete G 10-Kommission bleibt für die Dauer ihrer Amtszeit bestehen.

(3) Das Gremium nach § 2 des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz bleibt bis zum Ablauf der laufenden Wahlperiode des Landtages bestehen und nimmt bis dahin seine bisherigen Aufgaben weiter wahr. Die übrigen Aufgaben, die dem Parlamentarischen Kontrollgremium nach dem Landesverfassungsschutzgesetz in der Fassung dieses Gesetzes übertragen wurden, nimmt die bestehende Parlamentarische Kontrollkommission unter ihrer neuen Bezeichnung Parlamentarisches Kontrollgremium wahr.

Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Kiel 2008

Peter Harry Carstensen
Ministerpräsident

Lothar Hay
Innenminister

## Begründung

## zum Entwurf eines Gesetzes zur Umsetzung der Terrorismusbekämpfungsgesetze und zur Stärkung der parlamentarischen Kontrolle

### A. Allgemeines

Das Landesverfassungsschutzgesetz (LVerfSchG) ist seit seinem Inkrafttreten im Jahre 1991 im Wesentlichen unverändert geblieben. Insbesondere sind das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) und das Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) nicht umgesetzt worden. Schleswig-Holstein ist das einzige Bundesland, in dem der Gesetzgeber nicht auf die neue Bedrohungslage infolge der Anschläge vom 11. September 2001 reagiert hat. Eine Fortschreibung des Landesverfassungsschutzgesetzes ist dringend erforderlich, um dem durch das Bundesverfassungsschutzgesetz (BVerfSchG) vorgegebenen Mindeststandard an die gemeinsame Aufgabenerfüllung der Verfassungsschutzbehörden des Bundes und der Länder (Art. 73 Nr. 10 Buchst. b und c des Grundgesetzes – GG) gerecht zu werden.

Mit der im Entwurf vorgesehenen Umsetzung der Terrorismusbekämpfungsgesetze werden die bestehenden Befugnisse der Verfassungsschutzbehörde erweitert und neue hinzugefügt:

- Erweiterung des Beobachtungsauftrages auf den internationalen Terrorismus (Art. 1 Nr. 2),
- Auskunftspflichten von Privatunternehmen, insbesondere zu Passagier-, Konto- und Telekommunikationsdaten (Art. 1 Nr. 5) sowie
- Einsatz von technischen Mitteln zum Ausfindigmachen von Mobiltelefonen (Art. 1 Nr. 4 Buchst. b).

Als Gegengewicht zu dieser Befugniserweiterung soll die parlamentarische Kontrolle der Verfassungsschutzbehörde gestärkt werden. Dazu wird die parlamentarische Kontrolle über die Angelegenheiten des Verfassungsschutzes sowie über die Durchführung der Post- und Fernmeldeüberwachung in einem Parlamentarischen Kontrollgremium zusammengefasst (Art. 1 Nr. 15). Die G 10-Kommission bleibt davon unberührt.

Neben der Umsetzung der Terrorismusbekämpfungsgesetze bedarf es in einzelnen Punkten einer Angleichung des Landesverfassungsschutzgesetzes an die sonstigen Vorschriften des Bundesverfassungsschutzgesetzes, so hinsichtlich der

- Erweiterung des dem Beobachtungsauftrag zugrunde liegenden Begriffs der Bestrebung um Einzelpersonen, die auf Gewalt gerichtet sind oder von denen eine schwerwiegende Gefahr für die verfassungsschutzrechtlichen Schutzgüter ausgeht (Art. 1 Nr. 3 Buchst. a Doppelbuchst. bb),
- Herabsetzung der Altersgrenze für die Speicherung von Daten zu Minderjährigen, falls von jenen eine Gefahr ausgeht, die eine Post- und Fernmeldeüberwachung rechtfertigt (Art. 1 Nr. 8 Buchst. b),

- Erweiterung des Kreises der auskunftspflichtigen Behörden (Art. 1 Nr. 13 Buchst. a).

Ferner werden der Forderung der Rechtsprechung folgend die nachrichtendienstlichen Mittel zur Rechtsklarheit im Einzelnen bezeichnet (Art. 1 Nr. 4 Buchst. a; BVerfG, Urteil vom 12. April 2005 - 2 BvR 581/01 - NJW 2005, 1338, 1340) und rechtlich ausgestaltet. Zur rechtlichen Ausgestaltung werden die Eingriffsvoraussetzungen und das einzuhaltende Verfahren bei der Anwendung der einzelnen nachrichtendienstlichen Mittel bestimmt, dies in Abhängigkeit der jeweiligen Intensität des Grundrechtseingriffs. Bei dieser Konkretisierung des Grundsatzes der Verhältnismäßigkeit orientiert sich der Entwurf an den Spezialbefugnissen des Polizei- und Strafprozessrechts. Darüber hinausgehend wird für die Anwendung sämtlicher nachrichtendienstlicher Mittel der Schutz des Kernbereichs privater Lebensgestaltung verankert (Art. 1 Nr. 4 Buchst. b; BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/99 - NJW 2004, 999, 1006; BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - NJW 2008, 822, 834). Die rechtliche Ausgestaltung der bestehenden Befugnis zur Anwendung nachrichtendienstlicher Mittel stellt ein Novum im Verfassungsschutzrecht des Bundes und der Länder dar und dient in besonderem Maße der Rechtssicherheit.

Zur besseren Lesbarkeit des Gesetzes und damit dem Grundsatz der Rechtsklarheit Rechnung tragend werden Legaldefinitionen zur Bestimmung des Adressatenkreises der Befugnisse eingeführt (Zielperson, Kontaktperson, Nachrichtenmittler). Dabei wird auch der Schutz der Berufsgeheimnisträger gesetzlich festgeschrieben (Art. 1 Nr. 3 Buchst. b).

Der besseren Lesbarkeit des Gesetzes dient weiterhin die Zusammenfassung des Verfahrensrechts in einer gesonderten Vorschrift, auf die aus den jeweiligen Befugnissen verwiesen wird (Art. 1 Nr. 4 Buchst. b). Es wird hier der Entwicklung des Strafprozessrechts gefolgt, trägt dies doch auch zu einer Harmonisierung des Verfahrensrechts bei.

Harmonisiert wird überdies der Auskunftsanspruch der Betroffenen. Auf Anraten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein orientiert sich der Entwurf dabei an § 19 des Bundesdatenschutzgesetzes.

Weiterhin wird klargestellt, dass als nachrichtendienstliches Mittel auch das Internet heimlich beobachtet und verdeckt genutzt werden kann, dies allerdings nur insoweit, wie die Brief-, Post- und Fernmeldefreiheit unberührt bleibt (Art. 1 Nr. 4 Buchst. a). Zu denken ist hier an die Überwachung extremistischer Webseiten und die legendierte Teilnahme an so genannten Chats. Eine Überwachung des E-Mail-Verkehrs ist nur nach den strengen Anforderungen des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, ber. S. 2298), zuletzt geändert durch Gesetz vom 18. Februar 2007 (BGBl. I S. 106), zulässig. Die Einführung der so genannten Online-Durchsuchung ist nicht vorgesehen.

Das Artikel 10-Gesetz ist mit dem Ausführungsgesetz zum Artikel 10-Gesetz i. d. F. d. B. vom 31. Dezember 1971 (GVOBl. Schl.-H. S. 182), zuletzt geändert durch Verordnung vom 24. Oktober 1996 (GVOBl. Schl.-H. S. 652), landesrechtlich ausgestaltet worden. Die Vorschrift ist nach der Neufassung des Artikel 10-Gesetzes veraltet. Die Regelungen werden fortgeschrieben und gehen im Sachzusammenhang der verfassungsschutzbehördlichen Befugnisse in das Landesverfassungsschutzgesetz ein (Art. 1 Nr. 4 Buchst. b). Dies erleichtert die Rechtsanwendung und macht eine weitere Rechtsvorschrift entbehrlich.

Im Übrigen soll der Informationsaustausch mit ausländischen Nachrichtendiensten im „Kleinen Grenzverkehr“, insbesondere mit Dänemark erleichtert werden (Art. 1 Nr. 12). Damit wird den Bedürfnissen der hiesigen Vollzugspraxis Rechnung getragen.

## B. Zu den Bestimmungen im Einzelnen

### Zu Artikel 1 (Änderung des Landesverfassungsschutzgesetzes)

#### Zu Nr. 1 (Inhaltsübersicht)

Folgeänderung zu Nr. 5, 15 und 16.

#### Zu Nr. 2 (§ 5 Abs. 1)

#### Satz 1 Nr. 4

Die Aufgabe der Verfassungsschutzbehörde wird um die Beobachtung von Bestrebungen im Geltungsbereich dieses Gesetzes erweitert, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind. Bestrebungen gegen den Gedanken der Völkerverständigung sind solche, die sich gegen

- die Erhaltung des Friedens,
- die Ächtung von Angriffskriegen und
- die allgemeinen Grundrechte der Staaten, insbesondere
    - o das Recht auf politische Unabhängigkeit sowie
    - o das Recht auf Selbsterhaltung, auf Gleichheit, Ehre und Teilnahme am völkerrechtlichen Verkehr

richten, so das vereinsrechtliche Begriffsverständnis (Schnorr, Öffentliches Vereinsrecht, 1965, Rn 21 zu § 3 VereinsG; VGH München, Urteil vom 4. August 1999 - 4 A 96.2675 - NVwZ-RR 2000, 496, 499), das auch im Landesverfassungsschutzgesetz zugrunde gelegt wird. Dies wird durch die Legaldefinition des § 6 Abs. 3 Nr. 3 klargestellt (Nr. 3 Buchst. b).

Dem Gedanken der Völkerverständigung zuwider läuft jedenfalls ein Verstoß gegen die Friedenspflicht des Art. 26 Abs. 1 GG. Zur Rechtsklarheit wird daher das „friedliche Zusammenleben der Völker“ als Regelbeispiel aufgenommen, zumal dies nicht nur dem Wortlaut des § 3 Abs. 1 Nr. 4 BVerfSchG, sondern auch dem der Verfassungsschutzgesetze anderer Länder (z. B. Niedersachsen, Mecklenburg-Vorpommern, Hamburg und Nordrhein-Westfalen) entspricht.

Die Aufgabenerweiterung trägt dem Umstand Rechnung, dass bei ausländerextremistischen Organisationen in Deutschland Bestrebungen zu beobachten sind, die sich gegen politische Gegner im Ausland richten (z. B. die HAMAS; Bundesministerium des Innern, Verfassungsschutzbericht 2006, S. 218). So nehmen die Anhänger von ausländerextremistischen Organisationen in Deutschland die Aktionen ihrer Organisation im Heimatland insbesondere durch das Internet oder Satellitenfernsehen sehr genau wahr. Dies gilt auch für Organisationen, die lediglich im Ausland gewalt-

tätig gegen politische Gegner vorgehen. Durch die räumliche Entfernung zum Heimatland, wie z. B. bei der HAMAS, den Taliban oder der Hizb Allah könnte bei einigen Anhängern der Wunsch bzw. innere Drang dazu entstehen, in irgendeiner Form aktiv für die Organisation tätig zu werden. Dieser Drang kann in einfachen Unterstützungshandlungen, wie z. B. Spenden von materiellen oder finanziellen Mitteln oder in der Verbreitung von Propagandamitteln enden. Allerdings besteht auch die Gefahr, dass je nach Grad der Emotionalisierung eine „günstige Gelegenheit“ genutzt wird, um einen terroristischen Anschlag auch in Deutschland durchzuführen. Ähnlich verhielt es sich bei den mutmaßlichen Attentätern des vereitelten Anschlages auf den ehemaligen irakischen Ministerpräsidenten Allawi im Dezember 2004 in Deutschland.

Die Beobachtung solcher Bestrebungen ist von dem Aufgabenkatalog des § 5 Abs. 1 und 2 nicht hinreichend abgedeckt. So setzen § 5 Abs. 1 Nr. 1 und 3 voraus, dass die innere Sicherheit oder die auswärtigen Belange der Bundesrepublik Deutschland bedroht sind. Den betreffenden Organisationen sind aber Gewaltanwendung oder entsprechende Vorbereitungshandlungen in Deutschland, die zugleich Auswirkungen auf die innere Sicherheit haben oder die auswärtigen Belange beeinträchtigen, nicht oder nur sehr schwer nachzuweisen. Gleichwohl bilden Bestrebungen, die sich gegen den Gedanken der Völkerverständigung oder gegen das friedliche Zusammenleben der Völker richten, einen Nährboden für die Entstehung extremistischer Auffassungen und schüren Hass, der auch vor terroristischer Gewaltanwendung nicht zurückschreckt. Es muss daher zulässig sein, dass die Verfassungsschutzbehörde solche Bestrebungen – auch unter Einsatz nachrichtendienstlicher Mittel – aufklärt, zumal sie bei der Ermittlung von Gründen für das Verbot völkerrechtswidriger Vereine beteiligt wird (§ 4 Abs. 1 Vereinsgesetz).

**Zu Nr. 3 (§ 6)**

**Abs. 1**

Durch die Änderung in Satz 1 erfolgt eine redaktionelle Anpassung an die Änderung in Nr. 2.

Der neue Satz 3 erweitert den Beobachtungsauftrag der Verfassungsschutzbehörde um Einzelpersonen, die auf Gewalt gerichtet sind oder von denen in anderer Weise eine schwerwiegende Gefahr für die verfassungsschutzrechtlichen Schutzgüter ausgeht. Es handelt sich um eine Anpassung an das Bundesrecht (§ 4 Abs. 1 Satz 4 BVerfSchG).

Bei der Aufklärung von Gefahren für die verfassungsschutzrechtlichen Schutzgüter stehen in erster Linie Organisationen und Gruppierungen im Blickfeld der Verfassungsschutzbehörde. Verfassungsschutzrechtliche Gefahren können aber auch von Einzelpersonen ausgehen, insbesondere von gewalttätigen und gewaltbereiten Einzeltätern. Zu denken ist hier vor allem an den Bereich des Islamismus (Bundesministerium des Innern, Verfassungsschutzbericht 2006, S. 201).

So handelte es sich z. B. bei den mutmaßlichen Attentätern der im Sommer 2006 fehlgeschlagenen Kofferbombenattentate auf zwei Regionalzüge in Nordrhein-Westfalen um Einzeltäter. Nach derzeitigem Erkenntnisstand gehörten sie keiner ausländerextremistischen Organisation an, auch wenn davon auszugehen ist, dass sie über eine entsprechende islamistische Grundeinstellung verfügten. Sie entschlossen sich letztlich aus einer inneren Betroffenheit über die so genannten Mohammed-Karikaturen heraus, folgenschwere Anschläge in Deutschland zu begehen.

Das notwendige Rüstzeug wurde aus einschlägigen Internet-Angeboten beschafft. Gerade die Al-Qaida setzt als Markenzeichen darauf, dass unter anderem lose Personenzusammenschlüsse oder aber auch Einzelpersonen sich von der Ideologie der Al-Qaida angesprochen und animiert fühlen, selbst im Sinne des weltweiten Jihads auch terroristisch aktiv zu werden.

Im Falle solcher Einzeltäter ist die Aufmerksamkeit des Verfassungsschutzes somit ebenso geboten wie beim organisierten Extremismus. Gleiches gilt für den Fall, in dem eine Einzelperson zwar nicht auf Gewalt gerichtet ist, von ihr aber eine schwerwiegende Gefahr für ein Schutzgut des § 5 Abs. 1 ausgeht. Hinsichtlich des Begriffs der schwerwiegenden Gefahr wird auf die Begründung zu Nr. 5 (§ 8 a) verwiesen.

**Abs. 3**

In Satz 1 werden Bestrebungen, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind, gemäß der Begründung zu Nr. 2 legaldefiniert. Im angefügten Satz 2 werden die Begriffe der Zielperson, der Kontaktperson und des Nachrichtenmittlers bestimmt. Die Legaldefinitionen dienen der Begrenzung des Adressatenkreises von erheblichen Grundrechtseingriffen, um deren Streubreite so gering wie möglich zu halten. Zu denken ist hier z. B. an die Anwendung nachrichtendienstlicher Mittel nach § 8 Abs. 2 Satz 3.

**Nr. 1**

Die Begriffsbestimmung der Zielperson orientiert sich an § 4 Abs. 1 BVerfSchG. Zielperson ist danach eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie

- in einem oder
- für einen

Personenzusammenschluss handelt, der Bestrebungen oder Tätigkeiten im Sinne von § 5 Abs. 1 verfolgt.

In einem Personenzusammenschluss handeln dessen Mitglieder (Buchst. a). Mitglied ist, wer

- seinen Willen dem Personenzusammenschluss mit dessen Einverständnis unterordnet und
- in fortdauernder Weise für seine Zwecke tätig wird.

Es gilt hier der strafrechtliche Begriff der Mitgliedschaft, den die Rechtsprechung im Hinblick auf kriminelle bzw. terroristische Vereinigungen hinreichend konkretisiert hat (§§ 129, 129 a und 129 b StGB; BGH, Beschluss vom 22. Oktober 1979 - 1 StE 3/79-2 StB 52/79 - NJW 1980, 462, 463).

Für einen Personenzusammenschluss handelt, wer diesen nachdrücklich unterstützt (Buchst. d). Insoweit wird § 4 Abs. 1 Satz 2 BVerfSchG gefolgt. Der Begriff des Unterstützens ist im Strafrecht (§ 129 a Abs. 5 Satz 1 StGB) hinreichend bestimmt (BGH, Urteil vom 25. Januar 1984 - 3 StR 526/83 - NJW 1984, 1049, 1049; BGH, Urteil vom 3. Oktober 1979 - 3 StR 264/79 - NJW 1980, 64, 64; BGH, Urteil vom 30. Oktober 1964 - 3 StR 45/64 - NJW 1965, 260, 261) und findet auch im Aufenthaltsrecht (§ 47 Abs. 2 Nr. 2 und 3, § 54 Nr. 5 AufenthG) sowie im Staatsangehörig-

keitsrecht (§ 11 Satz 1 Nr. 2 StAG) Anwendung (BVerwG, Urteil vom 15. März 2005 - 1 C 26/03 - NVwZ 2005, 1091, 1092; OVG Hamburg, Urteil vom 6. Dezember 2005 - 3 Bf 172/04 - zit. n. Juris, dort Rn. 64; VGH Mannheim, Urteil vom 10. November 2005 - 12 S 1696/05 - zit. n. Juris, dort Rn. 26; BT-Drs. 16/2950, S. 15). Danach ist Unterstützer, wer als Nichtmitglied

- den Fortbestand des Personenzusammenschlusses oder
- die Verwirklichung seiner Ziele

fördert. Auf einen beweisbaren oder messbaren Nutzen für den Personenzusammenschluss kommt es dabei ebenso wenig an wie auf eine subjektive Vorwerfbarkeit der Unterstützungshandlung.

Zielperson ist ein Unterstützer allerdings nur dann, wenn die Unterstützung nachdrücklich ist. Dies ist der Fall, wenn sie wiederholt oder einmalig im erheblichen Ausmaß erfolgt, z. B. in Form einer größeren Spende (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 169).

Soweit tatsächliche Anhaltspunkte dafür vorliegen, dass eine Einzelperson außerhalb eines Personenzusammenschlusses Verhaltensweisen zeigt, die gemäß Abs. 1 Satz 2 als Bestrebungen im Sinne dieses Gesetzes gelten, ist diese ebenfalls Zielperson (Buchst. c). Zielperson ist weiterhin eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine solche Einzelperson nachdrücklich unterstützt (Buchst. d). Auch insoweit wird der Systematik des § 4 Abs. 1 BVerfSchG gefolgt.

Bei sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht fehlt es definitionsgemäß an einer Bestrebung. Gleichwohl sind Personen, die diese Tätigkeit verfolgen, gemäß dem verfassungsschutzbehördlichen Beobachtungsauftrag des § 5 Abs. 1 Nr. 2 Zielpersonen (Buchst. b). Gleiches gilt für deren nachdrückliche Unterstützer (Buchst. d).

**Nr. 2**

Von der Zielperson wird die Kontaktperson unterschieden. Kontaktperson ist eine Person, bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie

- zu der Zielperson in näherer persönlicher oder geschäftlicher Beziehung steht,
- den Kontakt über einen längeren Zeitraum unterhält oder
- den Kontakt unter konspirativen Umständen hergestellt hat oder pflegt.

Auf diese Weise wird deutlich gemacht, dass eine qualifizierte Verbindung zur Zielperson bestehen muss und nicht schon äußerlich flüchtige oder zufällige Alltagskontakte oder Beziehungen ausreichen. Die Legaldefinition entspricht im Ergebnis der des § 2 Satz 1 Nr. 3 des Antiterrordateigesetzes (BT-Drs. 16/2950, S. 16), konkretisiert jene jedoch im Lichte der Rechtsprechung zur verdeckten polizeilichen Gefahrerforschung (SächsVerfGH, Urteil vom 14. Mai 1996 - Vf. 44-II/94 - LKV 1996, 273, 284).

Von dem Kreis der Kontaktpersonen ausgenommen sind Personen, die ein gesetzlich geschütztes Vertrauensverhältnis zur Zielperson unterhalten. Ein solches Verhältnis besteht zwischen

- beratenden Berufen und ihren Mandanten (Rechtsanwälte, Notare, Wirtschaftsprüfer, Steuerberater, Buchprüfer),
- Heilberufen und ihren Patienten (Ärzte, Krankenschwestern, Hebammen, Heilpraktiker, Drogenberater, Psychologen)

sowie ferner im Falle

- des Redaktionsgeheimnisses von Presse und Rundfunk,
- des Beichtgeheimnisses und
- des Abgeordnetengeheimnisses,

kurzum bei den verschiedenen Amtsgeheimnissen (§ 53 Abs. 1 Nr. 1 bis 4, § 53 a StPO, § 383 Abs. 1 Nr. 4 bis 6 der Zivilprozessordnung, § 102 der Abgabenordnung, § 43 a Abs. 2 der Bundesrechtsanwaltsordnung, § 18 der Bundesnotarordnung, § 43 Abs. 1, § 50 der Wirtschaftsprüferordnung, § 35 des Sozialgesetzbuches I, § 43 des Deutschen Richtergesetzes, § 203 StGB, Art. 47 GG, Art. 24 Abs. 3 der Landesverfassung). Auf diese Weise wird dem Vertrauen in die Integrität der verfassungsrechtlich geschützten Beziehungen und deren Bedeutung sowohl für die Ausübung der Grundfreiheiten wie auch für die Funktionsfähigkeit der freiheitlich-demokratischen Rechtsordnung Rechnung getragen (SächsVerfGH, Urteil vom 14. Mai 1996 - Vf. 44-II/94 - LKV 1996, 273, 285; auch Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 231).

**Nr. 3**

Die Person des Nachrichtenmittlers (BVerfG, Urteil vom 12. März 2003 - 1 BvR 330/96 und 1 BvR 348/99 - NJW 2003, 1787, 1791 ff.) wird in Anlehnung an § 3 Abs. 2 Satz 2 G 10-Gesetz legaldefiniert.

**Zu Nr. 4 (§ 8)**

**Abs. 2**

Abs. 2 beinhaltet die Befugnis, nachrichtendienstliche Mittel anzuwenden, welche zunächst legaldefiniert werden. Danach handelt es sich um Methoden und Gegenstände einschließlich technischer Mittel zur heimlichen Datenerhebung. Es wird insoweit am geltenden § 8 Abs. 2 Satz 1 festgehalten.

In der Neufassung der Vorschrift wird die exemplarische Aufzählung nachrichtendienstlicher Mittel des geltenden § 8 Abs. 2 Satz 2 (Einsatz geheimer Mitarbeiterinnen und Mitarbeiter, Observationen, Bild- und Tonaufzeichnungen sowie Tarnpapiere und Tarnkennzeichen) zu einem Katalog ausgeweitet. Der Katalog nachrichtendienstlicher Mittel trägt dem Bestimmtheitsgebot Rechnung. Das Bestimmtheitsgebot verlangt, dass die Eingriffsinstrumente genau bezeichnet werden, damit der Inhalt der Befugnis vom Pflichtigen erkannt werden kann. Die gesetzlichen Formulierungen müssen aber nicht jede Einbeziehung technischer Neuerungen ausschließen (BVerfG, Urteil vom 12. April 2005 - 2 BvR 581/01 - NJW 2005, 1338, 1340).

Die Anforderungen an die Bestimmtheit der Eingriffsinstrumente sind umso höher, je stärker damit in die Grundrechte eingegriffen wird (BVerfG, Beschluss vom 1. Januar 1981 - 2 BvL 3, 9/77 - NJW 1981, 1311, 1311). Diesem Grundsatz folgend werden in

Satz 3 nachrichtendienstliche Mittel, die mit erheblichen Eingriffen in die Grundrechte verbunden sind, abschließend aufgeführt. Erheblich sind

- Eingriffe in die Brief-, Post und Fernmeldefreiheit (Art. 10 GG), so beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (Satz 3 Nr. 6) oder bei der Post- und Fernmeldeüberwachung nach dem Artikel 10-Gesetz (Satz 3 Nr. 7),
- Eingriffe, die ihrer Art und Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleichkommen, hier der Einsatz technischer Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes (Satz 3 Nr. 4),
- Eingriffe, die zumindest ihrer Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleichkommen: die langandauernde Observation (Satz 3 Nr. 3) und der Einsatz technischer Mittel zu Observationszwecken (Satz 3 Nr. 5; geltender § 8 Abs. 4 Satz 1 und Abs. 5; LT-Drs. 12/807, S. 30; siehe auch § 9 Abs. 3 BVerfSchG; Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 322 f.) sowie
- Eingriffe in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG), wenn jene schwerwiegend sind, so beim Einsatz von verdeckten Ermittlerinnen und Ermittlern, Vertrauensleuten, Gewährspersonen und sonstigen geheimen Informantinnen und Informanten sowie von zum Zwecke der Spionageabwehr überworbenen Agentinnen und Agenten (Satz 3 Nr. 1) und bei der Anfertigung verdeckter Bildaufnahmen und -aufzeichnungen (Satz 3 Nr. 4).

Maßnahmen, die diese Schwelle nicht erreichen, führt Satz 2 lediglich exemplarisch auf. Angesichts der geringen Eingriffsintensität dieser „einfachen“ nachrichtendienstlichen Mittel genügt es, die Arbeitweise der Verfassungsschutzbehörde insoweit in ihren Grundzügen darzustellen. Weitere Beispiele für „einfache“ nachrichtendienstliche Mittel ergeben sich im Erstrechtschluss aus Satz 3. Zu denken ist hier an verwandte Maßnahmen, welche die dort vorgesehene Eingriffsintensität nicht erreichen, z. B. die kurzandauernde Observation.

Ferner wird klargestellt, dass das heimliche Beobachten und die verdeckte Nutzung des Internets ebenfalls zu den nachrichtendienstlichen Mitteln gehören (Satz 2 Nr. 4), d. h. die Überwachung von Webseiten mit verfassungsfeindlichen Inhalten oder die legendierte Teilnahme an so genannten Chats. Die Maßnahmen finden ihre Grenze an der Brief-, Post- und Fernmeldefreiheit (Art. 10 GG). Wird z. B. der E-Mail-Verkehr überwacht, stellt dies eine Beschränkungsmaßnahme nach dem Artikel 10-Gesetz dar (Satz 3 Nr. 7), die nur unter den dort vorgesehenen Voraussetzungen zulässig ist. Die so genannte Online-Durchsuchung, d. h. der Einsatz technischer Mittel zur Ausforschung des heimischen PC oder sonstiger Kommunikationsanlagen (§ 5 Abs. 2 Nr. 11 Verfassungsschutzgesetz Nordrhein-Westfalen (VSG NRW) vom 20. Dezember 1994 (GV. NW. 1995 S. 28), geändert durch Gesetz vom 20. Dezember 2006 (GV. NRW. S. 620)), ist als nachrichtendienstliches Mittel nicht vorgesehen.

Der Katalog des Abs. 2 macht das bisher vorgesehene gesetzliche Erfordernis einer die nachrichtendienstlichen Mittel bezeichnenden Dienstvorschrift (geltender § 8 Abs. 2 Satz 3) entbehrlich. Gleichwohl bleibt der Verfassungsschutzbehörde die Möglichkeit einer internen Regelung unbenommen.

Für die nachrichtendienstlichen Mittel gilt im Einzelnen:

**Satz 2 Nr. 1**

Die Verwendung von Legenden dient dazu, dass ein verfassungsschutzbehördliches Tätigwerden nicht als solches erkannt wird. Sie soll überdies die Personen schützen, die für die Verfassungsschutzbehörde tätig werden.

**Satz 2 Nr. 2**

Die Legendierung (Satz 2 Nr. 1) wird durch die Beschaffung, Erstellung und Verwendung von Tarnpapieren und Tarnkennzeichen flankiert. Tarnpapiere sind „echte“, aber eine andere Identität des Inhabers vermittelnde Dienst- und Personalausweise sowie Führerscheine. Bei Tarnkennzeichen handelt es sich um Kfz-Kennzeichen, die einer besonderen Sperrung unterliegen (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 283).

**Satz 2 Nr. 3**

Das Abhören des Funkverkehrs ist jedermann möglich, der über geeignete technischen Einrichtungen verfügt. Das Fernmeldegeheimnis (Art. 10 GG) erstreckt sich im Funkverkehr nur auf den öffentlichen Fernmeldeverkehr und auf die dafür vorgesehenen Kanäle und Frequenzen. Die Verfassungsschutzbehörde ist befugt, andere Kanäle als nachrichtendienstliches Mittel zu beobachten. Ein Eingriff in das Fernmeldegeheimnis ist hingegen nur unter den strengen Voraussetzungen des Artikel 10-Gesetzes zulässig (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 285).

**Satz 2 Nr. 4**

Das heimliche Aufklären des Internets beschränkt sich auf Maßnahmen, mit denen die Verfassungsschutzbehörde Inhalte der Internet-Kommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt, also z. B. durch Abruf einer Webseite im World Wide Web mittels eines so genannten Webbrowsers. Es erstreckt sich weder

- auf den heimlichen Zugriff auf informationstechnische Systeme (so genannte Online-Durchsuchung) noch
- auf die Telekommunikationsüberwachung z. B. des E-Mail-Verkehrs; jene unterliegt den strengen Anforderungen des Artikel 10-Gesetzes.

Abgrenzend zu einer Telekommunikationsüberwachung nach dem Artikel 10-Gesetz ist die Verfassungsschutzbehörde beim heimlichen Aufklären des Internets nicht befugt, zugangsgesicherte Kommunikationsinhalte zu überwachen, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsteilnehmer erhoben hat. Hierin ist ein Eingriff in das Telekommunikationsgeheimnis zu sehen, der von dem nachrichtendienstlichen Mittel der Nr. 4 nicht abgedeckt ist. So liegt es etwa, wenn ein mittels so genanntem Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder einem geschlossenen Chat zu erlangen.

Anders verhält es sich, wenn etwa ein Teilnehmer eines geschlossenen Chats, der für die Verfassungsschutzbehörde handelnden Personen seinen Zugang freiwillig zur

Verfügung gestellt hat, und die Behörde in der Folge diesen Zugang nutzt. Auf diese Weise kann das Internet ohne einen Eingriff in das Telekommunikationsgeheimnis heimlich beobachtet und verdeckt genutzt werden (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 595/07 - zit. n. Juris, Rn. 289 ff.).

Ein heimliches Aufklären des Internets liegt allerdings nicht schon dann vor, wenn die Verfassungsschutzbehörde öffentlich zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht. Dies gilt auch für den Fall, in dem die Verfassungsschutzbehörde sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt und dabei das Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie sonst nicht erhalten würde (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 595/07 - zit. n. Juris, Rn. 304 ff.). In einer solchen schlichten Internet-Aufklärung ist kein nachrichtendienstliches Mittel zu sehen. Es handelt sich vielmehr um ein allgemeines Beobachten der Verfassungsschutzbehörde, das seine Rechtsgrundlage bereits in der Generalklausel findet (§§ 7, 8 Abs. 1).

**Satz 3 Nr. 1**

Die Verfassungsschutzbehörde bedient sich bei ihren verdeckten Ermittlungen

- Vertrauensleuten,
- Gewährspersonen,
- verdeckten Ermittlern,
- sonstigen geheimen Informanten und
- zum Zwecke der Spionageabwehr überworbenen Agenten.

Vertrauensleute (V-Leute) sind geheime, der Verfassungsschutzbehörde nicht angehörende (freie) Mitarbeiter, die aus einem Beobachtungsobjekt, z. B. einer gefahrträchtigen Bestrebung – in der Regel aufgrund eigener Zugehörigkeit – berichten. Charakteristisch ist die gezielte, auf Dauer angelegte geheime Anleitung der V-Leute durch die Verfassungsschutzbehörde (Borgs/Ebert, Das Recht der Geheimdienste, 1986, Rn. 157 zu A § 3).

Sonstige geheime Informanten sind Personen, die Kontakte zu einem Beobachtungsfeld haben und im Einzelfall oder gelegentlich einen konkreten Hinweis geben. Im Unterschied zu den V-Leuten werden Informanten durch die Verfassungsschutzbehörde nicht angeleitet. Die Verfassungsschutzbehörde beschränkt sich auf die Informationsabschöpfung.

Eine dem V-Mann vergleichbare Rolle spielt im Bereich der Spionageabwehr der überworbene Agent (Counterman – CM), da er auch als freier Mitarbeiter der Verfassungsschutzbehörde tätig wird. Im Unterschied zum V-Mann ist der CM Mitarbeiter eines fremden Nachrichtendienstes, der zur Mitarbeit im eigenen Dienst überworben wurde, also in der Funktion eines „Doppelagenten“ zum Nachteil seines früheren „Arbeitgebers“ tätig wird.

Gewährspersonen sind Personen, die der Verfassungsschutzbehörde logistische oder sonstige Hilfe leisten, ohne V-Mann, CM oder Informant zu sein. Ihre Zugänge sind häufig beruflich oder privat begründet. Sie üben ihre Tätigkeit für den Verfas-

sungsschutz nicht über einen längeren Zeitraum aus, sondern nur von Fall zu Fall. Regelmäßig unterliegen sie bei der Informationsbeschaffung keiner Steuerung durch die Verfassungsschutzbehörde.

Verdeckte Ermittler sind längerfristig verdeckt arbeitende Bedienstete der Verfassungsschutzbehörde, so genannte Under Cover Agents (UCA). Sie werden unter falscher Identität in das Beobachtungsobjekt eingeschleust (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 275 ff.).

**Satz 3 Nr. 2**

Die Anfertigung verdeckter Bildaufnahmen und -aufzeichnungen umfasst das heimliche Fotografieren, Videografieren, Filmen oder sonstiges Abbilden von Personen, Objekten und Ereignissen zur Anfertigung ganzheitlicher Bilder (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 285). Die Maßnahme kann im Einzelfall das Recht am eigenen Bild verletzen.

Das Recht am eigenen Bild stellt eine spezielle Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) dar. Es gewährleistet dem Einzelnen Einfluss- und Entscheidungsmöglichkeiten, soweit es um die Anfertigung und Verwendung von Fotografien oder Aufzeichnungen seiner Person durch andere geht (BVerfG, Beschluss vom 18. November 2004 - 1 BvR 2252/04 - NJW 2005, 883, 883).

Allerdings besteht das Recht am eigenen Bild nicht uneingeschränkt: In kollektiven Situationen öffentlicher Veranstaltungen und zeitgeschichtlicher Ereignisse, bei Demonstrationen und Aktionen kann es grundsätzlich nicht geltend gemacht werden (Schlink, Das nachrichtendienstliche Mittel, NJW 1980, 552, 556). Dem trägt § 23 Kunsturhebergesetz (KUG) Rechnung, wenngleich im Falle von Versammlungen der Schutz des Grundrechts aus Art. 8 GG im Einzelfall bei der Verhältnismäßigkeitsprüfung besonders zu berücksichtigen ist.

Anders verhält es sich, wenn das fotografische Interesse ausnahmsweise nicht einer kollektiven Situation, sondern einer Einzelperson gilt, z. B. bei der Observation (Meyer-Goßner, Rn. 1 zu § 100 f StPO). In diesem Fall ist die Anfertigung verdeckter Bildaufnahmen und -aufzeichnungen aus überwiegenden Interessen der Allgemeinheit gestattet (BGH, Urteil vom 16. September 1966 - VI ZR 268/64 (KG) - NJW 1966, 2353, 2354), so zur Aufrechterhaltung der öffentlichen Sicherheit (§ 24 KUG). Die Verfassungsschutzbehörde ist somit berechtigt, sich dieses nachrichtendienstlichen Mittels zu bedienen.

**Satz 3 Nr. 3**

Eine Observation ist die in der Regel unauffällige planmäßige – gegebenenfalls unter Einsatz technischer Mittel erfolgende – Beobachtung einer Person oder eines Objekts mit dem Ziel der Erhebung diesbezüglicher Erkenntnisse. Sie stellt einen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) dar (BVerwG, Urteil vom 21. März 1986 - 7 C 71/83 - NJW 1986, 2329, 2330).

Dauern Observationen nur kurz an, ist die Eingriffsintensität gering. Kurzandauernde Observationen sind daher bereits unter den Voraussetzungen des § 8 Abs. 2 Satz 1 Abs. 3 zulässig. Anders verhält es sich bei Observationen, die länger andauern, d. h., wenn die Beobachtung

- innerhalb einer Woche länger als 24 Stunden oder
- über den Zeitraum einer Woche hinaus

vorgesehen ist oder tatsächlich durchgeführt wird. Die in die Vorschrift aufgenommene Legaldefinition der langandauernden Observation entspricht der des hiesigen Polizeirechts (§ 185 Abs. 1 Nr. 1 Landesverwaltungsgesetz – LVwG).

Der mit einer Observation einhergehende Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) kann auf Dauer der Art und Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleichkommen (§ 8 Abs. 4 und 5; LT-Drs. 12/807, S. 30). Dies ist dann der Fall, wenn die Maßnahme länger als drei Monate andauert. Eine Observation ist unzulässig, wenn sie zu einer „Rundumüberwachung“ führt, mit der ein umfassendes Persönlichkeitsprofil der oder des Betroffenen erstellt werden könnte (BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209/83 - NJW 1984, 419, 424; BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/99 - NJW 2004, 999, 1004).

**Satz 3 Nr. 4**

Technische Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes sind z. B. so genannte Wanzen, versteckte Mikrofone und Aufzeichnungsgeräte (Meyer-Goßner, Rn. 7 zu § 100 f StPO). Der Einsatz solcher technischer Mittel kommt in seiner Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleich (§ 9 Abs. 3 BVerfSchG).

Im Unterschied dazu stellt das bloße Belauschen fremder Gespräche, z. B. durch einfaches Mithören eines etwa in einem Lokal geführten Gesprächs keinen Grundrechtseingriff dar. Jedermann hat die Möglichkeit, sich gegen eine solche Maßnahme ohne weiteres zu schützen, indem leiser gesprochen oder ein anderer Platz aufgesucht wird (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 328). An einem Grundrechtseingriff fehlt es ferner, wenn die Verfassungsschutzbehörde Beiträge oder Reden auf öffentlichen Veranstaltungen mithört oder aufzeichnet (Schlink, Das nachrichtendienstliche Mittel, NJW 1980, 552, 556), wobei im Falle von Versammlungen das Grundrecht aus Art. 8 GG in besonderer Weise zu berücksichtigen ist. Es handelt sich bei diesen Formen der Datenerhebung jedenfalls nicht um nachrichtendienstliche Mittel. Die betreffenden Maßnahmen können bereits auf der Grundlage der verfassungsschutzrechtlichen Generalklausel (§§ 7, 8 Abs. 1) ergriffen werden.

**Satz 3 Nr. 5**

Sonstige besondere technische Mittel für Observationszwecke sind solche, die weder der Anfertigung verdeckter Bildaufnahmen oder -aufzeichnungen noch dem Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes dienen (Meyer-Goßner, Rn. 2 zu § 100 f StPO). Zu denken ist hier an Nachtsichtgeräte, Alarmkoffer, Bewegungsmelder und Peilsender, auch unter Verwendung eines satellitengestützten Ortungssystems („Global Positioning System“ - GPS; BVerfG, Urteil vom 12. April 2005 - 2 BvR 581/01 - NJW 2005, 1338, 1340). Keine besonderen Observationsmittel sind Dienstwagen, Telefon, Sprechfunkgeräte usw. Sie gehören zur gebräuchlichen Ausstattung (Hilger, Neues Strafverfahrensrecht durch das OrgKG, NStZ 1992, 457, 461 f., dort Fn. 89).

Der Einsatz besonderer technischer Mittel für Observationszwecke stellt einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) dar und kann ebenso wie die Observation auf Dauer der Art und Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleichkommen (§ 8 Abs. 4 und 5; LT-Drs. 12/807, S. 30).

**Satz 3 Nr. 6**

Vgl. Begründung zu Abs. 8.

**Satz 3 Nr. 7**

Die Post- und Fernmeldeüberwachung umfasst

- die Überwachung und Aufzeichnung der Telekommunikation sowie
- das Öffnen und Einsehen von Sendungen, die dem Brief- und Postgeheimnis unterliegen.

Der damit einhergehende Eingriff in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) ist im Artikel 10-Gesetz geregelt, wobei die dortigen Befugnisse in Abs. 9 landesrechtlich ausgestaltet werden.

**Abs. 4**

Die Vorschrift bezweckt den Schutz des Kernbereichs privater Lebensgestaltung bei der Anwendung nachrichtendienstlicher Mittel. Sie trägt damit der Menschenwürdegarantie des Art. 1 Abs. 1 GG und der Rechtsprechung des Bundesverfassungsgerichts Rechnung. Zum Schutz des Kernbereichs hat das Bundesverfassungsgericht ein gestuftes Vorgehen vorgezeichnet (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - NJW 2008, 822, 834; BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/99 - NJW 2004, 999, 1006).

Vor der Anwendung nachrichtendienstlicher Mittel ist auf der ersten Stufe eine Prognoseentscheidung zu treffen, ob durch die Ermittlungsmaßnahme der Bereich des Höchstpersönlichen betroffen wird. Sofern ein Betroffensein des Kernbereichs bejaht wird, besteht ein Erhebungsverbot. Wird ein Kernbereichsbezug nur vorgetäuscht, z. B. um den Erfolg der Maßnahme zu vereiteln, ist nach objektiver Betrachtung der Kernbereich nicht berührt.

Erscheint angesichts der Prognoseentscheidung die Überwachungsmaßnahme möglich, dann ist auf der zweiten Stufe zu kontrollieren, ob eine Kernbereichsverletzung vorliegt. Schließlich sind Löschungspflichten und Verwertungsverbote zu beachten, sofern es versehentlich zu einer Erhebung von Informationen gekommen ist, die dem Kernbereich zuzuordnen sind.

**Abs. 5**

Die Vorschrift bestimmt die Anforderungen, die an die Anwendung nachrichtendienstlicher Mittel nach Abs. 2 Satz 3 zu stellen sind. Sie werden durch die besonderen Maßgaben der Abs. 6 bis 8 ergänzt. Die Anforderungen beschränken die Befugnis

des § 8 a Abs. 2 Satz 1, Abs. 3 in Abhängigkeit von der Intensität der mit der Anwendung der einzelnen nachrichtendienstlichen Mittel verbundenen Grundrechtseingriffe.

In Anlehnung an das Strafprozessrecht stellt Satz 1 die Anwendung nachrichtendienstlicher Mittel zunächst unter den Vorbehalt der Subsidiaritätsklausel des § 163 f Abs. 1 Satz 2 StPO. Danach muss das Ermittlungsergebnis auf andere Weise weniger Erfolg versprechend oder erschwert zu erreichen sein.

Die Subsidiaritätsklausel des Satzes 1 stellt eine im Vergleich zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) niedrigere Hürde dar. So muss als Voraussetzung für eine Post- und Fernmeldeüberwachung die Ermittlung auf andere Weise aussichtslos oder wesentlich erschwert sein (§ 3 Abs. 2 Satz 1 Artikel 10-Gesetz). Nichts anderes kann

- für das Ausfindigmachen eines Mobilfunkendgerätes (Satz 3 Nr. 6) gelten, wodurch ebenfalls in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) eingegriffen wird (so auch § 9 Abs. 4 Satz 2 BVerfSchG), aber auch
- für den Einsatz technischer Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes (Satz 3 Nr. 4), der nach seiner Art und Schwere einem solchen Eingriff gleichkommt (siehe auch § 100 f Abs. 1 StPO).

Dem Rechnung tragend findet sich die Subsidiaritätsklausel des Satzes 1 in den Abs. 8 Satz 1 Nr. 2 und Abs. 7 Satz 1 Nr. 2 verschärft.

Satz 2 beschränkt die Streubreite der Anwendung nachrichtendienstlicher Mittel auf das erforderliche Maß. Sie dürfen sich grundsätzlich nur gegen Zielpersonen und Kontaktpersonen richten. Im Falle des Einsatzes technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes tritt an die Stelle der Kontaktperson der Nachrichtenmittler. Dies ergibt sich aus der Natur der Maßnahme und wird in Abs. 8 Satz 2 klargestellt.

Im Übrigen kann auf die Anwendung nachrichtendienstlicher Mittel nicht deswegen verzichtet werden, weil Dritte, gegen die sich die Maßnahme nicht richtet, unvermeidbar betroffen werden. Erfolgt z. B. eine Observation auf einer Straße oder an allgemein zugänglichen Orten, werden regelmäßig auch andere Personen von den ermittelnden Beamten wahrgenommen und damit betroffen. Hierauf weist Satz 3 hin.

**Abs. 6**

Die Vorschrift enthält Maßgaben für die Anordnung

- des Einsatzes von verdeckten Ermittlerinnen und Ermittlern, Vertrauensleuten, Gewährspersonen und sonstigen geheimen Informantinnen und Informanten sowie von zum Zwecke der Spionageabwehr überworbenen Agentinnen und Agenten (Abs. 2 Satz 3 Nr. 1) und
- der langandauernden Observation (Abs. 2 Satz 3 Nr. 3).

Sie ergänzen die allgemeinen Voraussetzungen zur Anwendung nachrichtendienstlicher Mittel.

Mit den Maßnahmen kann ein erheblicher Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) verbunden sein. Dem Rechnung tragend sieht Satz 1 vor, dass die Maßnahme durch die Leitung der Verfassungsschutzabteilung

anzuordnen ist. Auf eine explizite Regelung des Vertretungsfalls wird verzichtet, da sich jene aus den Bestimmungen des Geschäftsverteilungsplans ergibt.

Im Falle der Observation hängt die Eingriffsintensität insbesondere von deren Dauer ab. Um einer unzulässigen „Rundumüberwachung“, mit der ein umfassendes Persönlichkeitsprofil der oder des Betroffenen erstellt werden könnte (BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209/83 - NJW 1984, 419, 424; BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/99 - NJW 2004, 999, 1004), vorzubeugen, ist die Anordnung auf höchstens drei Monate zu befristen. Satz 2 folgt insoweit dem Strafprozessrecht (§ 163 f Abs. 3 Satz 3, § 100 b Abs. 1 Satz 4 und 5 StPO).

Dauert die Observation länger als drei Monate an, kann die Maßnahme ihrer Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleichkommen. Ihre Verlängerung unterliegt daher dem Ministervorbehalt. Gemäß § 8 b Abs. 1 Satz 3 ist die Verlängerung auf höchstens drei Monate zu befristen. Eine weitere Verlängerung um nochmals drei Monate ist nicht möglich. § 8 b Abs. 1 Satz 4 ist von dem Verweis des Satzes 3 ausgenommen. Aufgrund der gesteigerten Eingriffsintensität der Verlängerungsanordnung ist jene dem Betroffenen gemäß § 8 b Abs. 3 mitzuteilen. Ferner ist das Parlamentarische Kontrollgremium über die verlängerte Observation nach Maßgabe des § 8 b Abs. 4 zu unterrichten.

Sofern bei der Observation technische Mittel (Satz 3 Nr. 5) zum Einsatz kommen, kann hierin ein Annex gesehen werden, an den keine gesonderten Anforderungen zu stellen sind.

**Abs. 7**

Die Vorschrift sieht ergänzende Anforderungen für den Einsatz technischer Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes (Abs. 2 Satz 3 Nr. 4) vor. Sie orientiert sich an § 100 f StPO, wobei klargestellt wird, dass die Maßnahme innerhalb von Wohnungen („Großer Lauschangriff“) unzulässig ist (Satz 2).

Die Maßnahme kommt ihrer Art und Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleich (§ 9 Abs. 3 BVerfSchG). Dem Rechnung tragend verlangt die Vorschrift das Vorliegen einer schwerwiegenden Gefahr für die verfassungsschutzrechtlichen Schutzgüter im Sinne von § 8 a Abs. 2. Es gilt hier nichts anderes als bei Eingriffen in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG), sei es im Falle der Auskunft zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten über Telemedien, sei es beim Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes (Abs. 8 Satz 1 Nr. 1). Ferner wird das Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter den Vorbehalt einer im Vergleich zu Abs. 5 Satz 1 verschärften Subsidiaritätsklausel gestellt (Satz 1 Nr. 2). Auch hier gibt die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) die Messlatte für den Eingriff vor (§ 3 Abs. 2 Satz 1 Artikel 10-Gesetz). Die Eingriffsvoraussetzungen des Satzes 1 entsprechen im Wesentlichen denen vergleichbarer Maßnahmen aufgrund des Strafprozessrechts (§ 100 f Abs. 1 StPO).

Die gesteigerte Eingriffsintensität findet sich überdies im Verfahrensrecht berücksichtigt. So ist der Einsatz technischer Mittel zum Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes durch die Innenministerin oder den Innenminister

anzuordnen. Satz 3 verweist dazu auf § 8 b Abs. 1. Das dort geregelte Verfahren ist dem des Strafprozessrechts (§ 100 f Abs. 4, § 100 b Abs. 1 StPO) gleichwertig. Ferner ist die Maßnahme der betroffenen Person mitzuteilen und das Parlamentarische Kontrollgremium zu unterrichten (Sätze 4 und 5).

Bei der Verarbeitung von Daten, die beim Mithören und Aufzeichnen gewonnen worden sind, müssen die Prüf-, Kennzeichnungs- und Löschungspflichten des § 4 Artikel 10-Gesetz sowie die dortigen Regelungen zur Übermittlung und Zweckbindung der Daten befolgt werden (Satz 6). Das Datenschutzniveau entspricht somit dem, welches bei Post- und Fernmeldeüberwachungen zur Anwendung kommt.

**Abs. 8**

Abs. 8 regelt den Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes. Dazu wird die bundesgesetzliche Regelung des § 9 Abs. 4 BVerfSchG übernommen.

Zur Vorbereitung einer Telekommunikationsüberwachung nach dem Artikel 10-Gesetz ist die Kenntnis der

- Gerätenummer („International Mobile Equipment Identity“ - IMEI) des Mobilfunkendgerätes, sprich des Mobiltelefons oder
- Kartennummer („International Mobile Subscriber Identity“ - IMSI) einer SIM-Karte („Subscriber Identity Module“)

erforderlich (Abs. 2 Satz 3 Nr. 6 Buchst. a). Die Kennungen können mithilfe eines so genannten IMSI-Catchers ermittelt werden. Technische Voraussetzung für den Einsatz des IMSI-Catchers ist die ungefähre Kenntnis des Standortes des Mobiltelefons. Anhand der Kennungen können dann die beim Netzbetreiber gespeicherten Bestandsdaten abgefragt werden. Die Bestandsdaten spezifizieren den Telefonanschluss hinreichend für eine Telekommunikationsüberwachung. Aus ihnen geht unter anderem der Besitzer des Mobiltelefons hervor (BVerfG, Beschluss vom 22. August 2006 - 2 BvR 1345/03 - NJW 2007, 351, 351).

Von der Ermittlung der Kennungen ist die Lokalisierung eines aktiv geschalteten Mobilfunkendgerätes zu unterscheiden (Abs. 2 Satz 3 Nr. 6 Buchst. b). Dazu werden verdeckte SMS an das Gerät versandt, um mithilfe der dadurch anfallenden Verkehrsdaten die Funkzelle zu ermitteln, in der sich der Anschluss befindet. Auf diese Weise kann der Standort des Gerätes fast „in Echtzeit“ nachvollzogen werden, wobei die Genauigkeit der Ortung von der Größe der Funkzelle (100 Meter bis 30 Kilometer) abhängt. Die Lokalisierung des Mobiltelefons ist geeignet, eine Observation zu erleichtern (BT-Drs. 15/4725, S. 22; Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 328 f., dort Fn. 1079; Eisenberg/Singelnstein, Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS“, NStZ 2005, 62, 62, Fn. 2).

Sowohl die Ermittlung der Kennungen als auch die des Standortes eines aktiv geschalteten Mobiltelefons unterfallen dem Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG; Nachbaur, Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers“, NJW 2007, 335, 337). Der Eingriff ist der Erhebung von Telekommunikationsverkehrsdaten (§ 8 a Abs. 2 Nr. 4) vergleichbar. Die Verkehrsdatenauskunft kann allerdings nur zu Mobiltelefonen eingeholt werden, mit denen gerade telefoniert wird. Die Ermittlung des Standortes eines lediglich

aktiv geschalteten Mobiltelefons bedarf der weitergehenden Befugnis. Diese wird durch Abs. 8 geschaffen.

Der Grundrechtseingriff beim Einsatz eines IMSI-Catchers nimmt sich im Vergleich zur Telekommunikationsüberwachung nach dem Artikel 10-Gesetz gering aus. So erfolgt keine Überwachung der Kommunikationsinhalte. Die im Sendebereich aktiv geschalteten, jedoch nicht telefonierenden Mobiltelefone werden lediglich für maximal acht Sekunden erfasst. Nur während dieser Sekunden ist ein Verbindungsaufbau des erfassten Mobiltelefons nicht möglich. Hierauf beschränkt sich die Beeinträchtigung, insbesondere werden laufende Gespräche in keinem Fall gestört. Die Streubreite ist zudem begrenzt: Von einem Messvorgang betroffen ist für gewöhnlich eine Zahl von Mobiltelefonen im unteren zweistelligen Bereich. Da zur IMSI-Ermittlung unter Umständen Messvorgänge in mehreren Netzen und jeweils mehrere Messvorgänge zur Feststellung von Übereinstimmungen nötig sind, können bei einer Maßnahme je nach Sachverhalt insgesamt durchaus auch 1.000 Mobiltelefone in dieser Weise betroffen sein. D. h. jene können für maximal acht Sekunden keine – andere – Verbindung aufbauen (BT-Drs. 16/2921, S. 16).

Aufgrund der Betroffenheit des Grundrechts aus Art. 10 setzt der Einsatz technischer Mittel zum Ausfindigmachen eines Mobilfunkendgerätes eine schwerwiegende Gefahr für die verfassungsschutzrechtlichen Schutzgüter im Sinne von § 8 a Abs. 2 voraus (Satz 1 Nr. 1). Ferner steht die Maßnahme unter dem Vorbehalt einer im Vergleich zu Abs. 5 Satz 1 verschärften Subsidiaritätsklausel (Satz 1 Nr. 2). Abweichend von Abs. 2 Satz 2 darf sich die Maßnahme nur gegen Zielpersonen und deren Nachrichtenmittler richten (Satz 2). Das nach Satz 3 bis 7 vorgesehene Verfahren entspricht dem der Anordnung von Auskunftspflichten zu Post- und Telekommunikationsverkehrsdaten sowie zu Nutzungsdaten über Telemedien nach § 8 a Abs. 2 Nr. 3 bis 5, Abs. 7.

Bei der Verarbeitung der Daten gelten die strengen Prüfungs- und Löschungspflichten des § 4 Artikel 10-Gesetz. Nachdem durch Abgleich mehrerer Messvorgänge die IMSI der Zielperson eindeutig ermittelt ist, werden die übrigen, zu diesem Zweck lediglich technisch zwischengespeicherten übrigen IMSI gelöscht; ihre Nutzung – etwa zur Einholung der Rufnummer oder zur sonstigen Herstellung eines Personenbezuges – ist verboten (Abs. 8 Satz 8). Bei den unbeteiligten Dritten wird danach nicht die Schwelle eines Grundrechtseingriffs erreicht (BT-Drs. 16/2921, S. 16).

Nach Art. 19 Abs. 1 GG ist die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) als eingeschränktes Grundrecht zu zitieren. Dem Zitiergebot wird Satz 9 gerecht.

**Abs. 9**

Abs. 9 gestaltet die Befugnisse zur Post- und Fernmeldeüberwachung nach dem Artikel 10-Gesetz landesrechtlich aus. Die dazu erforderliche Zuständigkeitszuweisung folgt der Systematik des Artikel 10-Gesetzes.

**Zu Nr. 5 (§§ 8 a und 8 b)**

**§ 8 a**

§ 8 a setzt die besonderen Auskunftsverlangen des § 8 a BVerfSchG landesrechtlich um. Danach ist die Verfassungsschutzbehörde befugt, gegenüber privaten Unternehmen Auskunftspflichten zur Erbringung von Finanz-, Post-, Telekommunikations-,

Telemedien- und Luftverkehrsdienstleistungen anzuordnen. Bei der Anordnung wird zwischen

- Bestandsdaten (Abs. 1) und
- Verkehrsdaten (Abs. 2)

unterschieden.

Auskünfte zu Verkehrsdaten stellen für die Betroffenen einen gewichtigen Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) dar. Im Falle der Post- und Telekommunikationsverkehrsdaten sowie der Nutzungsdaten zu Telemedien ist überdies die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) berührt. An die Anordnungen der betreffenden Auskunftspflichten werden daher besondere Anforderungen gestellt. Die Auskünfte dürfen

- nur im Falle einer schwerwiegenden Gefahr für die in § 5 Abs. 1 genannten Schutzgüter – wobei § 8 a Abs. 2 Satz 2 im Hinblick auf den „einfachen“ Extremismus weitergehende Einschränkungen vorsieht – und
- nur zu dem in Abs. 4 bestimmten Personenkreis

verlangt werden. Ferner sind die Verfahrensmaßgaben der Abs. 5 bis 8 in Verbindung mit der allgemeinen Verfahrensvorschrift des § 8 b zu beachten. Die Verfahrensmaßgaben tragen § 8 a Abs. 8 BVerfSchG Rechnung, wonach die landesrechtliche Einführung einer Befugnis zur Anordnung von Auskunftspflichten zu Verkehrsdaten unter dem Vorbehalt steht, dass das Landesrecht vergleichbare Verfahrens- und Kontrollmechanismen vorsieht.

**Abs. 1**

Abs. 1 befugt die Verfassungsschutzbehörde, Auskünfte über Bestandsdaten zu Postdienstleistungen, Telekommunikationsdiensten und zu Telemedien zu verlangen. Der Begriff der Bestandsdaten entspricht hinsichtlich der Telemedien dem des § 14 Abs. 1 Telemediengesetz (TMG).

<u>Postdienstleistungen</u>

Postdienstleistungen sind Brief-, Paket- und Büchersendungen im Sinne von § 4 Nr. 1 des Postgesetzes (PostG). Bestandsdaten zu Postdienstleistungen sind insbesondere

- der Name,
- die Hausanschrift und
- die Postfachadresse

derjenigen, die Postdienstleistungen in Anspruch nehmen. Anhand der Bestandsdaten kann noch nicht auf die näheren Umstände des Postverkehrs geschlossen werden. Sie unterfallen somit nicht dem Postgeheimnis (§ 39 Abs. 1 PostG; auch Lackner/Kühl, Rn. 13 zu § 206 StGB).

Die Kenntnis der Bestandsdaten ist für die Verfassungsschutzbehörde erforderlich, um insbesondere den Vertrieb volksverhetzender Propaganda aufzuklären. So werden in rechtsextremistischen Publikationen mitunter Postfächer als Kontaktadressen

benannt. Postfächer spielen auch bei der Bestellung und dem Vertrieb rechtsextremistischer Skinhead-Musik eine Rolle (BT-Drs. 16/2921, S. 14). Die Verfassungsschutzbehörde benötigt die Bestandsdaten ferner zur Aufklärung der Kommunikationswege terroristischer Gruppen, um die Überwachung der Kommunikationsinhalte im Wege der Post- und Fernmeldeüberwachung nach dem Artikel 10-Gesetz vorzubereiten (BT-Drs. 16/5982, S. 9).

Telekommunikationsdienste

Telekommunikationsdienste sind in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich der Übertragungsdienste in Rundfunknetzen (§ 3 Nr. 24 des Telekommunikationsgesetzes – TKG). Diese Definition umfasst insbesondere

- das (klassische) Fernmeldewesen, aber auch
- den E-Mail-Dienst und
- den Internet-Zugang

(Geppert/Piepenbrock/Schütz/Schuster, Rn. 49 zu § 3 TKG). Zur Auskunft verpflichtet sind diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen. Das geschäftsmäßige Erbringen von Telekommunikationsdiensten ist in einem nachhaltigen Angebot von Telekommunikation (§ 3 Nr. 22 TKG) für Dritte mit oder ohne Gewinnerzielungsabsicht zu sehen (§ 3 Nr. 10 TKG).

Bestandsdaten zu Telekommunikationsdiensten sind üblicherweise

- der Name und die Anschrift des Teilnehmers sowie
- die Anschlussnummer,
- die Art des Anschlusses (z. B. ISDN, anlog),
- die Art der Endeinrichtung,
- rechnungsrelevante Daten wie die Rechnungsanschrift, Bankverbindung, Lastschriftermächtigung sowie
- besondere Tarifmerkmale und
- die in Anspruch genommene Dienstleistung

(Geppert/Piepenbrock/Schütz/Schuster, Rn. 3 zu § 95 TKG). Im Hinblick auf eine Internet-Nutzung sind Bestandsdaten ferner statische und dynamisch vergebene IP-Adressen (BT-Drs. 16/5846, S. 61). Die Bestandsdaten haben keinen Bezug zu einem konkreten Telekommunikationsvorgang und unterfallen deshalb nicht dem Fernmeldegeheimnis nach Art. 10 GG, § 88 TKG (Bär, Anm. zu LG Stuttgart, Beschluss vom 4. Januar 2005, MMR 2005, 626, 626). Es ist lediglich das Recht auf informationelle Selbstbestimmung berührt.

Die Zulässigkeit des Auskunftsersuchens ist in § 112 Abs. 2 Nr. 4 und § 113 Abs. 1 Satz 1 TKG geregelt. Die telekommunikationsrechtlichen Vorschriften stellen allerdings noch keine Befugnisse dar. Bislang sind die Auskunftsersuchen auf die verfassungsschutzrechtliche Generalklausel gestützt worden. Zwar ist dies rechtlich nicht zu beanstanden (Geppert/Piepenbrock/Schütz/Schuster, Rn. 9 ff. zu § 113 TKG).

Gleichwohl bietet es sich aus Gründen der Rechtsklarheit an, im Zuge der Einführung einer spezialgesetzlichen Befugnis zur Anordnung von Auskunftspflichten auch die Auskünfte nach § 112 Abs. 2 Nr. 4 und § 113 Abs. 1 Satz 1 TKG gesetzlich auszugestalten (BT-Drs. 15/2316, S. 97, 13/3609, S. 55 f.). Es wird insoweit von § 8 a Abs. 1 BVerfSchG abgewichen.

Telemedien

Abs. 1 befugt die Verfassungsschutzbehörde ferner, Auskünfte über Bestandsdaten zur Nutzung von Telemedien einzuholen. Zur Auskunft verpflichtet sind Dienstanbieter im Sinne des Telemediengesetzes, d. h. jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (§ 2 Nr. 1 TMG).

Abweichend von § 8 a Abs. 1 BVerfSchG wird in Abs. 1 und auch in Abs. 2 Satz 1 Nr. 5 die durch Art. 1 des Elektronischen-Geschäfsverkehr-Vereinheitlichungsgesetzes veränderte Rechtslage berücksichtigt, wonach Teledienste und Mediendienste unter dem Begriff Telemedien zusammengefasst worden sind. Telemedien ist ein aus

- Teledienste (§ 2 Abs. 2 des vormaligen Teledienstegesetzes) und
- Mediendienste (§ 2 Abs. 2 des vormaligen Mediendienste-Staatsvertrages)

gebildeter Oberbegriff für elektronische Informations- und Kommunikationsdienste. Während sich Teledienste an den individuellen Nutzer richten, dienen Mediendienste der Meinungsbildung und zielen auf die Allgemeinheit ab.

Danach gehören zu den Telemedien beispielsweise

- der Internet-Zugang und der E-Mail-Dienst,
- Diskussionsforen, Newsgroups, Chatrooms und Blogs,
- Telebanking, Webshops und Online-Auktionshäuser,
- abrufbare Telespiele und Videos,
- Webportale und Suchmaschinen,
- Informationsdienste (Verkehrs-, Wetter-, Umwelt- und Börsendaten) sowie
- Webseiten.

Keine Telemedien sind der herkömmliche Rundfunk sowie Live-Streamings oder Webradios. Ausgenommen sind ferner

- telekommunikationsgestützte Dienste im Sinne des § 3 Nr. 25 TKG, z. B. Mehrwertdienste, die über Nummerngassen wie 0900 oder 0800 erbracht werden, sowie
- Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, z. B.
    - das (klassische) Fernmeldewesen, aber auch
    - die Internet-Telefonie (Voice over Internet Protocol – VoIP),

  wohingegen Telekommunikationsdienste, die lediglich überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen (z. B. der Inter-

net-Zugang und der E-Mail-Dienst) sowohl dem Telemediengesetz als auch dem Telekommunikationsgesetz unterfallen,

so die Abgrenzung in § 1 Abs. 1 TMG (BR-Drs. 556/06, S. 17 f.).

Die Erweiterung des verfassungsschutzbehördlichen Auskunftsanspruchs auf Telemedien, die sich an die Allgemeinheit richten (vormals Mediendienste), trägt nicht nur der veränderten Rechtslage Rechnung. Sie ist auch fachlich geboten: Volksverhetzende Propaganda wird unter anderem auf an die Allgemeinheit gerichteten Webseiten verbreitet. Es handelt sich dabei um Mediendienste, deren Bestandsdaten nicht dem auf Teledienste beschränkten Auskunftsanspruch des § 8 a Abs. 1 BVerfSchG unterfallen. Gleichwohl ist die Kenntnis der betreffenden Bestandsdaten zur Aufklärung von Bestrebungen und Tätigkeiten im Sinne von § 5 Abs. 1 erforderlich.

Bestandsdaten im Sinne des Telemediengesetzes (§ 14 Abs. 1 TMG) sind üblicherweise

- der Name und die Anschrift des Nutzers sowie
- rechnungsrelevante Daten (Rechnungsanschrift, Bankverbindung, Lastschriftermächtigung).

Zu den Bestandsdaten sind auch die Informationen zu rechnen, welche ständig für die technische Möglichkeit der Diensterbringung („inhaltliche Ausgestaltung“) Voraussetzung sind. Hierzu können etwa

- eine zugewiesene Benutzerkennung,
- ein Passwort,
- die Art des Zugangsprotokolls und
- Informationen über die verwendete Hardware (Modem, ISDN-Karte o. ä.)

gehören (Spindler/Schmitz/Geis, Rn. 8 zu § 5 TDDSG), ferner sowohl statisch als auch dynamisch vergebene IP-Adressen (LG Stuttgart, Beschluss vom 4. Januar 2005 - 13 Qs 89/04 - NJW 2005, 614, 614 f.; Sankol, Die Qual der Wahl: § 113 TKG oder §§ 100 g, 100 h StPO? – Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, MMR 2006, 361, 362 ff. m. w. N.).

Die Zulässigkeit der Auskunft zu den Bestandsdaten ist in § 14 Abs. 2 TMG geregelt. Danach darf der Dienstanbieter unter anderem auf Anordnung der Verfassungsschutzbehörde im Einzelfall Auskunft über Bestandsdaten zur Nutzung von Telemedien erteilen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Die Vorschrift stellt allerdings noch keine Befugnis für die Verfassungsschutzbehörde dar, so dass es der Regelung in Abs. 1 bedarf (BR-Drs. 556/06, S. 22 f.).

Die Kenntnis der Bestandsdaten zu Telemedien, insbesondere zu Telebanking, Webshops und Online-Auktionshäusern ist für die Verfassungsschutzbehörde erforderlich, um z. B. den Vertrieb volksverhetzender Propaganda oder die Finanzierung von Bestrebungen im Sinne von § 6 Abs. 1 aufzuklären. Ferner kann sie bei der Spionageabwehr von Bedeutung sein (BT-Drs. 16/2921, S. 14).

**Abs. 2**

Ergänzend zu den Auskünften zu Bestandsdaten nach Abs. 1 kann die Verfassungsschutzbehörde Auskünfte zu

- Passagierdaten,
- Kontostamm- und -verbindungsdaten,
- Postverkehrsdaten,
- Telekommunikationsverkehrsdaten und
- Nutzungsdaten zu Telemedien

verlangen.

**Nr. 1**

Luftfahrtunternehmen sind Unternehmen, die Fluggäste, Post und/oder Fracht im gewerblichen Luftverkehr befördern. Es gilt das dem Luftfahrtsrecht der Europäischen Gemeinschaft zugrunde liegende Begriffsverständnis (Art. 2 Buchst. b und c der Verordnung (EWG) Nr. 2407/92 des Rates über die Erteilung von Betriebsgenehmigungen an Luftfahrtunternehmen vom 23. Juli 1992, ABl. Nr. L 240, S. 1, ber. ABl. Nr. 45, S. 30).

Die Datenverarbeitung der Luftfahrtunternehmen unterliegt dem allgemeinen Datenschutzrecht (§ 27 Abs. 1, § 28 BDSG). Danach ist die Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke grundsätzlich zulässig, wobei im grenzüberschreitenden Verkehr immer mehr Staaten dazu übergehen, von Luftfahrtunternehmen die Vorabübermittlung von Passagierdaten an Grenzschutz- und Zollbehörden zu verlangen (BR-Drs. 16/07, S. 44). Nach § 28 Abs. 3 Nr. 2 BDSG ist die Übermittlung oder Nutzung der Passagierdaten ferner zulässig, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit erforderlich ist.

Passagierdaten sind

- der Name und die Anschrift des Kunden sowie
- Daten zur Inanspruchnahme und zu den Umständen der Transportleistung, insbesondere
    - zum Zeitpunkt von Abfertigung und Abflug und
    - zum Buchungsweg.

Die frühzeitige und umfassende Verfügbarkeit dieser Daten dient insbesondere der Aufklärung des internationalen Terrorismus. Sie ermöglicht eine Analyse der Ruhe- und Vorbereitungsräume sowie der Zielgebiete terroristischer Vereinigungen (BT-Drs. 14/7386, S. 40; BT-Drs. 16/5982, S. 10).

**Nr. 2**

Kontostamm- und -verbindungsdaten sind

- Daten zu Konten, Kontoinhabern und sonstigen Berechtigten, d. h.

- o die Kontonummer,
- o der Tag der Errichtung und ggf. Auflösung des Kontos,
- o die Namen und das Geburtsdatum des Kontoinhabers oder eines Verfügungsberechtigten sowie
- o die Namen und die Anschrift eines abweichend wirtschaftlich Berechtigten (§ 24c Kreditwesengesetz – KWG),

– Daten zu Geldbewegungen und -anlagen, d. h.

- o zu den Zahlungsein- und -ausgängen und
- o zu den am Zahlungsweg Beteiligten sowie zum

– Kontostand.

Zur Auskunft verpflichtet sind Kreditinstitute, Finanzdienstleistungsinstitute und Finanzunternehmen im Sinne von § 1 Abs. 1, 1 a und 3 KWG.

Informationen zu Kontostamm- und -verbindungsdaten sind zunächst durch das Bankgeheimnis geschützt. Das Bankgeheimnis findet sich in Nr. 2 Abs. 1 der Allgemeinen Geschäftsbedingungen der privaten Banken und der Genossenschaftsbanken (AGB-Banken) i. d. F. vom April 2002 umrissen. Darin wird klargestellt, dass das Bankgeheimnis unter dem Vorbehalt einer gesetzlichen Durchbrechung steht, so z. B. im Steuer- und Strafrecht (Ebenroth/Boujong/Joost, HGB, Rn. 156 ff.).

Ferner unterliegt die Datenverarbeitung der Kreditinstitute, Finanzdienstleistungsinstitute und Finanzunternehmen dem allgemeinen Datenschutzrecht (§§ 27 Abs. 1, 28 BDSG). Danach ist den Unternehmen die Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke gestattet. Darüber hinaus ist die Übermittlung oder Nutzung der Daten zulässig, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit erforderlich ist (§ 28 Abs. 3 Nr. 2 BDSG).

Die Kenntnis der Kontostamm- und -verbindungsdaten ist erforderlich, um die finanziellen Ressourcen und damit die Gefährlichkeit vor allem terroristischer Gruppen frühestmöglich einschätzen zu können. Es gilt Transaktionen im Zahlungsverkehr zu ermitteln, die der Logistik des Terrorismus dienen. Die Verbesserung der Erkenntnismöglichkeiten der Verfassungsschutzbehörde bezweckt die vom VN-Sicherheitsrat mit Resolution 1373 (2001) nachdrücklich geforderte Unterbindung der Finanzströme terroristischer Organisationen (Ziffer 1 Buchst. a der Resolution; auch BT-Drs. 14/7386, S. 39).

**Nr. 3**

Postverkehrsdaten unterfallen als Umstände des Postverkehrs dem Postgeheimnis (§ 39 Abs. 1 PostG). Das Postgeheimnis schützt insoweit vor der Offenbarung, wer mit wem durch die Post Briefe und Sendungen wechselt (BVerfG, Beschluss vom 20. Juni 1984 - 1 BvR 1494/78 - NJW 1985, 121, 122; auch Lackner/Kühl, Rn. 13 zu § 206 StGB). Von den Umständen des Postverkehrs ist der Inhalt der Postsendung zu unterscheiden. Jener kann von der Verfassungsschutzbehörde nur nach den strengen Anforderungen des Artikel 10-Gesetzes eingesehen werden.

Mit der verfassungsschutzbehördlichen Befugnis, Auskunftspflichten zu den Umständen des Postverkehrs anordnen zu können, wird in zulässiger Weise in das Postge-

heimnis eingegriffen (§ 39 Abs. 3 Satz 3 PostG). Die Regelung entspricht § 8 a Abs. 2 Satz 1 Nr. 3 BVerfSchG. Die Kenntnis der Umstände des Postverkehrs ist für die Verfassungsschutzbehörde erforderlich, um insbesondere den Vertrieb volksverhetzender Propaganda (§ 130 StGB) aufzuklären.

**Nr. 4**

Telekommunikationsverkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 TKG). Abweichend von § 8 a BVerfSchG wird in Abs. 2 Satz 1 Nr. 4 ein Rückgriff auf so genannte Vorratsdaten nach § 113 a TKG vorgesehen. Dazu wird dem Zitiergebot des § 113 b TKG Rechung getragen. Auf diese Weise wird das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) landesrechtlich umgesetzt. So kann hinsichtlich der Verkehrsdaten unterschieden werden zwischen denjenigen,

- die alle Anbieter nach § 96 Abs. 1 TKG zum Zwecke der Erbringung des Telekommunikationsdienstes speichern dürfen, und solchen,
- die lediglich die Anbieter öffentlich zugänglicher Telekommunikationsdienste nach § 113 a TKG auf Vorrat speichern müssen (so genannte Vorratsdatenspeicherung).

Bei den Verkehrsdaten nach § 96 Abs. 1 TKG handelt es sich zunächst um

- die Nummer oder die Kennung der beteiligten Anschlüsse oder der Endeinrichtung,
- personenbezogene Berechtigungskennungen,
- die Kartennummer (bei Verwendung von Kundenkarten) sowie
- die Standortdaten (bei mobilen Anschlüssen).

Verkehrsdaten sind ferner

- der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
- der vom Nutzer in Anspruch genommene Telekommunikationsdienst (z. B. Sprachtelefonie oder Datenübertragung) und
- die Endpunkte von festgeschalteten Verbindungen (z. B. im Falle von Standverbindungen zwischen Rechenzentren), ihr Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen.

Nach dem Auffangtatbestand des § 96 Abs. 1 Nr. 5 TKG sind Verkehrsdaten im Übrigen sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Soweit die Verkehrsdaten ausschließlich der Entgeltabrechnung dienen, sind sie von dem verfassungsschutzbehördlichen Auskunftsverlangen ausgenommen. § 8 a Abs. 2 Satz 1 Nr. 4 BVerfSchG folgend wird damit dem datenschutzrechtlichen Erforderlichkeitsgrundsatz Rechnung getragen (BT-Drs. 16/2921, S. 15). Dies gilt auch für die nach § 113 a TKG zu bevorratenden Verkehrsdaten.

Die in § 113 a Abs. 2 bis 4 TKG im Zusammenhang mit der Vorratsdatenspeicherung aufgeführten Verkehrsdaten entsprechen im Wesentlichen denen des § 96 Abs. 1 TKG. Es wird insoweit auf die Gesetzesbegründung dazu (BT-Drs. 16/5846, S. 174 ff.) verwiesen.

Bei den Verkehrsdaten handelt es sich um sensible Daten, die dem Fernmeldegeheimnis unterfallen (Ohlenburg, Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, 431, 434). Ihre Übermittlung ist nach § 96 Abs. 2 Satz 1 TKG (BT-Drs. 15/5213, S. 23 f.) und nach § 113 b Nr. 3 TKG zulässig. Ergänzend dazu bedarf es einer verfassungsschutzbehördlichen Befugnis zur Anordnung der Auskunftspflicht, wobei diese im Hinblick auf den Abruf von Vorratsdaten auf § 113 a TKG verweisen muss. Dem wird die Befugnis des Abs. 2 Satz 1 Nr. 4 gerecht.

Die Kenntnis der Verkehrsdaten zu Telekommunikationsdiensten ist für die Verfassungsschutzbehörde erforderlich, um insbesondere das Umfeld der Zielperson aufzuklären, z. B. terroristische Netzwerke. Auf diese Weise können zusätzliche Ermittlungsansätze gewonnen werden (BT-Drs. 16/5982, S. 11, 16/5846, S. 183; Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 246).

**Nr. 5**

Nutzungsdaten im Sinne des Telemediengesetzes sind in § 15 Abs. 1 TMG aufgeführt. Danach sind Nutzungsdaten insbesondere

- Merkmale zur Identifikation des Nutzers,
- Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

Bei der Einordnung der Daten muss allerdings jeweils geprüft werden, inwieweit es sich nicht (zumindest auch) um Bestandsdaten handelt, die Abs. 1 unterfallen, so z. B. im Falle von IP-Adressen, Nutzernamen und Passworten (Spindler/Schmitz/Geis, Rn. 9 zu § 6 TDDSG).

Dem datenschutzrechtlichen Erforderlichkeitsgrundsatz Rechnung tragend sind Nutzungsdaten, die ausschließlich der Entgeltabrechnung dienen, von dem verfassungsschutzbehördlichen Auskunftsersuchen ausgenommen. Es gilt hier nichts anderes als für die Telekommunikationsverkehrsdaten (BT-Drs. 16/2921, S. 15).

Die Zulässigkeit der Übermittlung der Nutzungsdaten an die Verfassungsschutzbehörde richtet sich nach § 14 Abs. 2 TMG (§ 15 Abs. 5 Satz 4 TMG), die Befugnis dafür hält Abs. 2 Satz 2 Nr. 5 vor. Die Kenntnis der Nutzungsdaten ist für die Verfassungsschutzbehörde erforderlich, um z. B. den Vertrieb volksverhetzender Propaganda oder die Finanzierung von Bestrebungen im Sinne des § 2 Abs. 1, insbesondere terroristischer Netzwerke aufzuklären.

<u>Schwerwiegende Gefahr</u>

Die Befugnis des Abs. 2 steht unter dem Vorbehalt, dass über die Voraussetzungen der verfassungsschutzrechtlichen Generalklausel hinausgehend eine schwerwiegende Gefahr für die Schutzgüter des § 5 Abs. 1 bestehen muss. Die Vorschrift folgt insoweit § 8 a Abs. 2 Satz 1 BVerfSchG.

Die Voraussetzung der schwerwiegenden Gefahr enthält eine schutzgutbezogene Qualifizierung. Es müssen tatsächliche Anhaltspunkte für solche Bestrebungen oder Tätigkeiten vorliegen, die geeignet sind, die in § 5 Abs. 1 genannten Schutzgüter erheblich zu beschädigen. Dies ist unter den Voraussetzungen der Post- und Telekommunikationsüberwachung (§ 3 Abs. 1 Artikel 10-Gesetz) der Fall, geht aber darüber hinaus, indem keine Anhaltspunkte für die Planung von dort bezeichneten Straftaten vorliegen müssen. Beispiele sind hier organisierte, erhebliche Geldsammlungen zur Unterstützung militanter Organisationen oder proliferationsrelevante Sachverhalte. Schwerwiegende Gefahren gehen insbesondere von Bestrebungen aus, die die qualifizierenden Voraussetzungen des Abs. 2 Satz 2 erfüllen. Abs. 2 Satz 2 beschränkt die Befugnisse bei der Beobachtung des „einfachen“ Extremismus“ (§ 5 Abs. 1 Nr. 1) auf volksverhetzende und militante Bestrebungen.

Abs. 2 Satz 2 Nr. 1 orientiert sich dabei an der durch das Zuwanderungsgesetz in § 55 Abs. 2 Nr. 8 Buchst. b des Aufenthaltsgesetzes getroffenen Regelung zu „Hasspredigern“, die sich wiederum auf § 130 Abs. 1 des Strafgesetzbuches bezieht. Korrespondierend zu § 5 Abs. 1 Nr. 4 werden danach neben völkerverständigungswidrigen Bestrebungen auch solche Bestrebungen, die das friedliche Zusammenleben in Deutschland besonders gefährden, einbezogen. Dies wird allerdings auf Bestrebungen beschränkt, die bezwecken oder geeignet sind, die Bereitschaft zur Anwendung von Gewalt zu fördern.

Abs. 2 Satz 2 Nr. 2 bezieht militante Bestrebungen ein. Dies betrifft nicht nur Bestrebungen, die selbst Gewalt anwenden, sondern auch solche, die sie vorbereiten, etwa in der in § 14 Abs. 2 Nr. 4 und 5 des Vereinsgesetzes bezeichneten Weise (BT-Drs. 16/2921, S. 14).

**Abs. 3**

Auskunftsverlangen nach Abs. 1 und 2 bedürfen einer schriftlichen Anordnung (Satz 1). Die zur Auskunft Verpflichteten müssen über die Anordnung Verschwiegenheit gegenüber den Betroffenen und Dritten wahren (Satz 2). Die Regelung folgt § 8 a Abs. 7 BVerfSchG. Sie ist erforderlich, um effektive Ermittlungen der Verfassungsschutzbehörde sicherzustellen (BT-Drs. 14/7386, S. 39).

**Abs. 4**

In Abs. 4 wird der Personenkreis, zu dem Auskünfte nach Abs. 2 eingeholt werden können, eingeschränkt. Dabei wird zur Rechtsklarheit und zur besseren Lesbarkeit des Gesetzes auf die Legaldefinitionen der Zielperson (§ 6 Abs. 3 Satz 2 Nr. 1) und des Nachrichtenmittlers (§ 6 Abs. 3 Satz 2 Nr. 3) zurückgegriffen.

Nach Satz 1 ist die Anordnung einer Auskunftspflicht nach Abs. 2 zunächst zur Zielperson zulässig. Gegen andere Personen als die Zielperson dürfen sich die Auskunftsverlangen nur richten, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie Leistungen von

- Luftfahrtunternehmen (Abs. 2 Nr. 1),
- Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen (Abs. 2 Nr. 2) sowie
- Telemedienanbietern (Abs. 2 Nr. 5)

für die Zielperson in Anspruch nehmen (Satz 1 Nr. 1). Zu denken ist hier an den Fall, dass ein Terrorist einen bestimmten Flug genutzt hat und somit tatsächliche Anhaltspunkte zu den Passagieren des Fluges vorliegen, die die Verfassungsschutzbehörde dazu berechtigen, die Übermittlung der Passagierdaten zu verlangen, wenn dies zur weiteren Klärung erforderlich ist, weil zunächst unbekannt ist, welchen Namen der Terrorist bei seiner Flugreise verwendet hat (BT-Drs. 16/2921, S. 15).

Ähnlich verhält es sich im Hinblick auf Post- und Telekommunikationsdienstleistungen bei der Person des Nachrichtenmittlers, sprich wenn im Falle des Satzes 1 Nr. 2 tatsächliche Anhaltspunkte dafür vorliegen, dass

- sie für die Zielperson bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt oder
- die Zielperson ihre Adresse oder ihren Anschluss benutzt.

Angesichts der durch das Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz geänderten Rechtslage, wonach auch der Internet-Zugang und der E-Mail-Dienst den Telemedien zuzurechnen sind, muss die Verfassungsschutzbehörde Auskünfte zum Nachrichtenmittler ferner bei der Inanspruchnahme von Telemedien verlangen können. Die in § 8 a Abs. 3 Nr. 2 Buchst. b BVerfSchG vorgesehene Beschränkung auf Post- und Telekommunikationsdienstleistungen greift vor diesem Hintergrund zu kurz.

Personen im Sinne von Satz 1 sind zunächst natürliche Personen. Ergänzend dazu stellt Satz 2 klar, dass auch juristische Personen Gegenstand eines Auskunftsverlangens nach Abs. 2 sein können, so z. B. wenn zur Aufklärung einer schwerwiegenden Gefahr für ein Schutzgut des § 5 Abs. 1 Informationen zu dem Konto einer extremistischen Organisation erforderlich sind (BT-Drs. 16/2921, S. 15).

**Abs. 5 bis 8**

Bei der landesrechtlichen Einführung einer Befugnis zur Anordnung von Auskunftspflichten zu Verbindungs-, Verkehrs- bzw. Nutzungsdaten im Sinne des § 8 a Abs. 2 BVerfSchG müssen dem Bundesrecht vergleichbare Verfahrens- und Kontrollmechanismen vorgesehen werden (§ 8 a Abs. 8 BVerfSchG). Die betreffenden Regelungen finden sich in den Abs. 5 bis 8.

Die Anforderungen an die Verfahrens- und Kontrollmechanismen hängen von der Intensität der mit den betreffenden Maßnahmen verbundenen Grundrechtseingriffe ab. So kommt es darauf an, ob

- ein Auskunftsersuchen in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) eingreift,
- die Maßnahme ihrer Schwere nach einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommt oder
- das Ersuchen (lediglich) in erheblicher Weise in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) eingreift.

Dieser Systematik folgend werden die Verfahrens- und Kontrollmechanismen – abweichend vom zugrunde liegenden Bundesrecht – nach der Intensität der betreffenden Grundrechtseingriffe geordnet (Abs. 5 bis 7), wobei die Parlamentarischen Kon-

trollgremien des Landes und des Bundes nach Abs. 8 in jedem Fall über die Maßnahmen zu unterrichten sind.

Ferner werden im Unterschied zum Bundesrecht die einzelnen Verfahrensschritte lediglich aufgeführt, nicht aber in den Abs. 5 bis 7 ausgestaltet. Hierzu wird auf die allgemeine Verfahrensvorschrift des § 8 b verwiesen. Diese Regelungstechnik dient der besseren Lesbarkeit des Gesetzes.

Die genannten Abweichungen lassen die bundesrechtlich geforderten Verfahrens- und Kontrollmechanismen inhaltlich unberührt. Die Vorschriften erfüllen die Anforderungen des § 8 a Abs. 8 BVerfSchG vollumfänglich.

**Abs. 5**

Auskunftsverlangen zu Passagierdaten (Abs. 2 Nr. 1) greifen in erheblicher Weise in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) ein, zumal die Auskünfte heimlich eingeholt werden (Abs. 3). Derart erhebliche Eingriffe müssen nach einem Verfahren erfolgen, welches den infolge der Heimlichkeit der Maßnahme erschwerten Rechtsschutz kompensiert.

Anders als bei Eingriffen in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) muss das Verfahren zur Anordnung der Auskunftspflicht zu Passagierdaten aber nicht den hohen Anforderungen des Artikel 10-Gesetzes gerecht werden. Ein ministerieller Anordnungsvorbehalt, wie ihn § 10 Abs. 1 Artikel 10-Gesetz vorsieht, ist nicht erforderlich. Vielmehr kann die Anordnung auf administrativer Ebene erfolgen. Gleichwohl verlangt das Bundesrecht, dass die Zuständigkeit für die Anordnung von Auskunftspflichten zu Passagierdaten zu regeln ist. Nach § 8 a Abs. 4 Satz 1 BVerfSchG soll dies in einer Dienstvorschrift geschehen.

Die Regelung der Anordnungsbefugnis in einer Dienstvorschrift ist für die Betroffenen schwer nachvollziehbar. Im Einklang mit den bundesrechtlichen Anforderungen des § 8 a Abs. 4 Satz 1 BVerfSchG kann ein Mehr an Transparenz und Rechtsklarheit dadurch erreicht werden, dass die Anordnungsbefugnis gesetzlich bestimmt wird. Dazu sieht Abs. 5 vor, dass Auskunftsverlangen zu Passagierdaten durch die Leitung der Verfassungsschutzabteilung anzuordnen sind. Auf eine explizite Regelung des Vertretungsfalls wird verzichtet, da sich jene aus den Bestimmungen des Geschäftsverteilungsplans ergibt. Im Übrigen sind die Parlamentarischen Kontrollgremien des Landes und des Bundes gemäß Abs. 8 über die angeordneten Auskunftspflichten zu Passagierdaten zu unterrichten (§ 8 a Abs. 6 und 8 Satz 2 BVerfSchG).

**Abs. 6**

Auskunftsverlangen zu Kontoverbindungsdaten (Abs. 2 Nr. 2) berühren das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG). Der Eingriff ist erheblicher als im Falle der Passagierdaten (Abs. 2 Nr. 1). In den Kontobewegungen kann nämlich eine Art von Kommunikation gesehen werden. So sind Auskünfte darüber, wer wem zu welchem Zeitpunkt welchen Betrag überweist, Auskünften zu den Umständen des Postverkehrs vergleichbar. Letztere unterfallen dem Postgeheimnis, Kontoverbindungsdaten dem Bankgeheimnis.

Vor diesem Hintergrund kommen Auskunftsverlangen zu Kontoverbindungsdaten, wenn auch nicht unbedingt in ihrer Art (Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 322 f.), so doch zumindest in ihrer Schwere einer Beschränkung des

Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) gleich. Daraus folgt, dass gesteigerte Anforderungen an den Rechtsschutz durch das Verfahren zu stellen sind.

Dem Rechnung tragend sieht Satz 1 vor, dass Auskunftsverlangen zu Kontoverbindungsdaten auf Antrag der Leitung der Verfassungsschutzabteilung durch die Innenministerin oder den Innenminister angeordnet werden (siehe auch geltender § 8 Abs. 4 Satz 1). Das ministerielle Anordnungsverfahren findet sich in § 8 b Abs. 1 entsprechend den Maßgaben des § 8 a Abs. 4 Satz 2, 4 bis 6 BVerfSchG ausgestaltet. Aus Gründen der Rechtsklarheit verzichtet die Vorschrift auf die durch das Bundesrecht eingeräumte Sonderregelung, wonach die ministerielle Anordnung auch durch eine Bedienstete oder einen Bediensteten der Verfassungsschutzbehörde erwirkt werden kann, der die Befähigung zum Richteramt hat (§ 8 a Abs. 4 Satz 3 BVerfSchG).

Ferner verlangt Satz 2, dass die Anordnung der betroffenen Person gemäß § 8 b Abs. 3 mitzuteilen ist (siehe auch geltender § 8 Abs. 4 Satz 1 und Abs. 5 bzw. § 9 Abs. 3 BVerfSchG). Die Vorschrift folgt den bundesrechtlichen Anforderungen des § 8 a Abs. 4 Satz 7 BVerfSchG. Im Übrigen sind die Parlamentarischen Kontrollgremien des Landes und des Bundes gemäß Abs. 8 über die angeordneten Auskunftspflichten zu Kontoverbindungsdaten zu unterrichten (§ 8 a Abs. 6 und 8 Satz 2 BVerfSchG).

**Abs. 7**

Die Auskunftsverlangen zu Post- und Telekommunikationsverkehrsdaten und zu Nutzungsdaten über Telemedien (Abs. 2 Nr. 3 bis 5) greifen in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) ein (BT-Drs. 16/2921, S. 15). Vor diesem Hintergrund ist ein Rechtsschutz durch ein Verfahren vorzusehen, welches den Anforderungen des Artikel 10-Gesetzes entspricht.

Danach sind Auskunftsverlangen nach Abs. 2 Nr. 3 bis 5 durch die Innenministerin oder den Innenminister anzuordnen. Satz 1 verweist insoweit auf das in § 8 b Abs. 1 ausgestaltete Anordnungsverfahren. Die Vorschrift trägt § 10 Abs. 1 Artikel 10-Gesetz Rechnung und folgt damit den bundesrechtlichen Maßgaben des § 8 a Abs. 4 Satz 2, 4 bis 6 und Abs. 8 Satz 1 BVerfSchG.

Nach Satz 2 ist die G 10-Kommission über die Auskunftsverlangen zu unterrichten. Das Verfahren zur Unterrichtung und die Prüfungsbefugnis der G 10-Kommission sind in § 8 b Abs. 2 ausgestaltet, worauf die Vorschrift verweist. Es wird auf diese Weise § 15 Artikel 10-Gesetz berücksichtigt und § 8 a Abs. 5 Satz 1 bis 6 BVerfSchG gemäß § 8 a Abs. 8 Satz 1 BVerfSchG landesrechtlich umgesetzt.

Die Personen, zu denen die Auskünfte nach Abs. 2 Nr. 3 bis 5 verlangt werden, sind von der Verfassungsschutzbehörde über die zugrunde liegende Anordnung zu unterrichten. Nach Satz 3 ist dabei das Mitteilungsverfahren nach § 12 Abs. 1 und 3 Artikel 10-Gesetz entsprechend anzuwenden. Auf diese Weise findet § 8 a Abs. 5 Satz 8 und Abs. 8 Satz 1 BVerfSchG Berücksichtigung. Zur Rechtsklarheit wird in Satz 4 darauf hingewiesen, dass der betroffenen Person nach der Mitteilung der Rechtsweg offen steht. Es gilt hier nichts anderes als im Falle einer Mitteilung nach § 8 b Abs. 3, dort Satz 3.

Die Verarbeitung von Daten, die aufgrund eines Eingriffs in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) gewonnen worden sind, bedarf einer besonderen Re-

gelung, um Missbrauch vorzubeugen. Satz 5 verweist dazu auf die Prüf-, Kennzeichnungs- und Löschungspflichten des § 4 Artikel 10-Gesetz sowie auf die dortigen Regelungen zur Übermittlung und Zweckbindung der Daten. Damit folgt die Vorschrift § 8 a Abs. 5 Satz 7 und Abs. 8 Satz 1 BVerfSchG.

Nach Art. 19 Abs. 1 GG ist die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) als eingeschränktes Grundrecht zu zitieren. Dem Zitiergebot wird Satz 6 gerecht.

Im Übrigen sind die Parlamentarischen Kontrollgremien des Landes und des Bundes gemäß Abs. 8 über die Maßnahmen zu unterrichten. § 8 a Abs. 6 und 8 Satz 1 BVerfSchG findet sich insoweit berücksichtigt.

**Abs. 8**

Die Tätigkeit der Verfassungsschutzbehörde unterliegt der Kontrolle des Parlamentarischen Kontrollgremiums (§ 26 Abs. 1). Grundsätzlich ist für die parlamentarische Kontrolle kein besonderes Verfahren vorgesehen. Da die verfassungsschutzbehördlichen Auskunftsverlangen zu Verbindungs-, Verkehrs- bzw. Nutzungsdaten nach Abs. 2 in nicht unerheblicher Weise in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) bzw. im Falle des Abs. 2 Nr. 3 bis 5 in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) eingreifen, bedarf es insoweit einer Straffung der Kontrolle. Diese wird durch die in § 8 b Abs. 4 ausgestalteten Berichtspflichten der Verfassungsschutzbehörde gewährleistet. Satz 1 folgt insoweit § 8 a Abs. 6 Satz 1 BVerfSchG und kommt damit der Forderung des § 8 a Abs. 8 BVerfSchG nach Einführung gleichwertiger Kontrollmechanismen nach.

Ferner verlangt § 8 a Abs. 8 BVerfSchG eine Unterrichtung des Parlamentarischen Kontrollgremiums des Bundes. An den Bericht werden wiederum die gleichen Anforderungen gestellt wie an den Bericht der Verfassungsschutzbehörde gegenüber dem hiesigen Parlamentarischen Kontrollgremium (§ 8 b Abs. 4). Die Maßgabe wird in Satz 2 landesrechtlich umgesetzt.

**§ 8 b**

Die Vorschrift gestaltet das Verfahren

- der Anordnung von Maßnahmen durch die Innenministerin oder den Innenminister (Abs. 1),
- zur Unterrichtung der G 10-Kommission (Abs. 2),
- zur Mitteilung der Betroffenen (Abs. 3) und
- zur Unterrichtung des Parlamentarischen Kontrollgremiums (Abs. 4)

aus, soweit diese Verfahrensschritte im Gesetz vorgesehen sind und auf § 8 b verwiesen wird. Die Ausgestaltung des Verfahrens orientiert sich an den bundesrechtlichen Verfahrensmaßgaben zu den besonderen Auskunftsverlangen (§ 8 a Abs. 4 bis 6 BVerfSchG).

Die Anknüpfung an das Bundesrecht ist zur landesrechtlichen Umsetzung der besonderen Auskunftsverlangen des § 8 a BVerfSchG in § 8 a erforderlich. Jene steht nämlich unter dem Vorbehalt, dass das Landesrecht ein gleichwertiges Verfahren und eine gleichwertige parlamentarische Kontrolle vorsehen muss (§ 8 a Abs. 8 BVerfSchG).

Der danach zu gewährleistende Rechtsschutz durch Verfahren ist überdies geeignet, die Anwendung nachrichtendienstlicher Mittel (§ 8 Abs. 2 ff.), mit der vergleichbare Grundrechtseingriffe verbunden sein können, rechtsstaatlich auszugestalten. Die Ausgestaltung der einzelnen Verfahrensschritte wird daher von der Befugnis des § 8 a losgelöst und in § 8 b als einheitlicher Standard vorgegeben. Auf diese Weise werden die Verfahren harmonisiert.

**Abs. 1**

Die Vorschrift regelt den Ministervorbehalt bei der Anordnung von Maßnahmen und deren Verlängerung. Die Vorschrift folgt § 8 a Abs. 4 Satz 2 und 4 bis 6 BVerfSchG, wobei

- die Antragsbefugnis der Leitung der Verfassungsschutzabteilung und
- die Anordnungsbefugnis der Innenministerin oder dem Innenminister

zugewiesen werden. Im Falle der Verhinderung der Innenministerin oder des Innenministers ist die Vertretung anordnungsbefugt. Was die Antragsbefugnis der Leitung der Verfassungsschutzabteilung angeht, richtet sich diese im Vertretungsfall nach der internen Geschäftsverteilung.

**Abs. 2**

Maßnahmen, die in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) eingreifen, sind der G 10-Kommission (§ 26 a) zur Entscheidung vorzulegen. Zuständig für die Unterrichtung ist das Innenministerium als Verfassungsschutzbehörde. Das dabei anzuwendende Verfahren regelt Abs. 2 in Anlehnung an die betreffenden Bestimmungen zu den besonderen Auskunftsersuchen (§ 8 a Abs. 5 Satz 1 bis 6 BVerfSchG), die sich wiederum an § 15 Abs. 5 und 6 Artikel 10-Gesetz orientieren.

**Abs. 3**

Ist mit einer Maßnahme der Verfassungsschutzbehörde ein Grundrechtseingriff verbunden, muss die betroffene Person davon grundsätzlich Kenntnis erlangen können. Andernfalls ist ein effektiver Grundrechtsschutz (Art. 19 Abs. 4 GG) nicht gewährleistet. Erfolgt die Maßnahme heimlich und tragen die Auskunftsansprüche des § 25 den Rechten der betroffenen Person nicht angemessen Rechnung, muss sie benachrichtigt werden (BVerfG, Urteil vom 14. Juli 1999 - 1 BvR 2226/94, 2420/95 und 2437/95 - NJW 2000, 55, 57; Urteil vom 15. Dezember 1970 - 2 BvF 1/69, 2 BvR 629/68, 308/69 - NJW 1971, 275, 277 ff.). Einer Benachrichtigung der betroffenen Person bedarf es regelmäßig dann, wenn mit der Maßnahme erhebliche Grundrechtseingriffe verbunden sind. Dies sieht bereits der geltende § 8 Abs. 5 vor. Das dort geregelte Mitteilungsverfahren wird in Abs. 3 unter Berücksichtigung des § 9 Abs. 3 Nr. 1 BVerfSchG vereinfacht.

Die Mitteilungspflicht der Verfassungsschutzbehörde erschöpft sich nicht in einer Benachrichtigung der Zielperson. Grundsätzlich sind auch unbeteiligte Dritte über die sie mitbetreffenden Eingriffe zu unterrichten (§ 8 Abs. 5 Satz 3). Dabei ist Folgendes zu beachten: Werden mitbetroffene Dritte benachrichtigt, kann dies den Grundrechtseingriff bei der Zielperson noch vertiefen. Andererseits wird zusätzlich in die Rechte der Dritten eingegriffen, wenn deren Identität als Voraussetzung für die Mit-

teilung zunächst zu ermitteln ist (BVerfG, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/99 - NJW 2004, 999, 1015 f.). Vor diesem Hintergrund bedarf es der Ausnahmeregelung des Satzes 3, wonach auf eine Mitteilung zur Vermeidung von Härten verzichtet werden kann. Die Vorschrift orientiert sich am Polizeirecht (§ 186 Abs. 4 Satz 1 und 2 LVwG; siehe auch § 101 Abs. 4 StPO).

**Abs. 4**

Für den Fall, dass Maßnahmen der Verfassungsschutzbehörde mit einem Eingriff in das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) verbunden sind bzw. der Eingriff dem nach Art und Schwere gleichkommt, werden in Anlehnung an die bundesrechtlichen Verfahrensmaßgaben zu den besonderen Auskunftsverlangen (§ 8 a Abs. 6 Satz 1 BVerfSchG) gesteigerte Anforderungen an die parlamentarische Kontrolle gestellt. Nach den gesteigerten Anforderungen muss das Innenministerium das Parlamentarische Kontrollgremium (§ 26) im Abstand von höchstens sechs Monaten über die genannten Eingriffe informieren, wobei insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben ist. Auf diese Weise wird die generelle Informationspflicht des § 26 Abs. 5 bezüglich schwerwiegender Grundrechtseingriffe konkretisiert und damit die parlamentarische Kontrolle gestärkt.

**Zu Nr. 6 (§ 10)**

Redaktionelle Anpassung an die Änderung in Nr. 2.

**Zu Nr. 7 (§ 11)**

§ 11 wird um eine Befugnis zur Erfassung von Protokolldaten erweitert (Abs. 4). Die Daten werden zum Zwecke der Datenschutzkontrolle erhoben, können aber auch zur Aufklärung eines Verdachts auf Datenmissbrauch verwendet werden. Es wird insoweit an der datenschutzrechtlichen Zweckbestimmung des § 14 Abs. 3 festgehalten, die infolge der Neuregelung in § 11 Abs. 4 entfallen kann.

**Zu Nr. 8 (§ 12)**

Durch die Änderung in Satz 1 Nr. 2 erfolgt eine redaktionelle Anpassung an die Änderung in Nr. 2.

Der hinzugefügte Satz 2 erlaubt die Speicherung personenbezogener Daten zu Minderjährigen, die das 14. Lebensjahr vollendet haben, wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Straftat nach § 3 Abs. 1 Artikel 10-Gesetz, sprich eine politische Straftat geplant oder begangen wird. Die betreffenden Daten dürfen in Akten, nicht aber in Dateien gespeichert werden (Satz 3).

Mit der Öffnung der Altersgrenze für die Speicherung von Daten zu Minderjährigen wird § 11 BVerfSchG gefolgt, wobei eine absolute Altersuntergrenze dort nicht vorgesehen ist. Die Angleichung an das Bundesrecht trägt der zunehmenden politischen Delinquenz Jugendlicher Rechnung. Dies gilt insbesondere für den Rechts- und Linksextremismus.

**Zu Nr. 9 (§ 13)**

Durch die Änderung in Satz 3 erfolgt eine redaktionelle Anpassung an die Änderung in Nr. 2.

**Zu Nr. 10 (§ 14)**

Folgeänderung zu Nr. 7.

**Zu Nr. 11 (§ 15)**

Es wird die Behördenbezeichnung des ehemaligen Landesbeauftragten für Datenschutz fortgeschrieben.

**Zu Nr. 12 (§ 20)**

Die Vorschrift erweitert § 20 um die Möglichkeit des nachrichtendienstlichen Informationsaustausches im „kleinen Grenzverkehr“. Nachrichtendiensten von Mitgliedstaaten der EU, die an Schleswig-Holstein grenzen oder zu denen Fährverbindungen bestehen (derzeit Dänemark, Schweden, Litauen, Lettland und Finnland), können danach personenbezogene Daten bereits dann zugänglich gemacht werden, wenn die Übermittlung

- zur Erfüllung der Aufgaben der Verfassungsschutzbehörde oder
- zur Wahrung erheblicher Sicherheitsinteressen des Empfängers

erforderlich ist. Auf diese Weise wird die Zusammenarbeit mit den betreffenden Nachrichtendiensten erleichtert. Gleiches gilt für die norwegischen Nachrichtendienste.

Der internationale islamistische Terrorismus ist unter anderem durch erhebliche Reisebewegungen mutmaßlicher Angehöriger und Unterstützer von Terrororganisationen gekennzeichnet. Kurzfristig bekannt gewordene Erkenntnisse von relevanten Personen über aktuelle Reisebewegungen in angrenzende EU-Staaten und nach Norwegen, z. B. bei der möglichen Ausreise über die Fährverbindungen von Schleswig-Holstein nach Skandinavien, sollten möglichst zeitnah an die befreundeten Dienste der betreffenden Staaten weitergegeben werden können. Dies ist erforderlich, damit von den dortigen Behörden ggf. noch entsprechende operative Maßnahmen, wie z. B. Observationen durchgeführt werden können. Genauso verhält es sich bei Erkenntnissen, deren Weitergabe keinen zeitlichen Verzug dulden, wie z. B. konkrete, akute Terrorwarnungen.

Nach geltendem Recht ist eine Übermittlung an ausländische Behörden nur zulässig, wenn es zum Schutz vor Bestrebungen gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes unverzichtbar ist (§ 20 Satz 2, § 19 Abs. 2 Satz 1 Nr. 5). Erkenntnisse über grenzüberschreitende Bewegungen, die dem internationalen Terrorismus zuzurechnen sind, dürfen danach in aller Regel nicht bzw. nur über den Umweg über das Bundesamt für Verfassungsschutz übermittelt werden. Dies kann zu Verzögerungen führen, die unter Berücksichtigung der verkehrsbedingten Nähe der betreffenden Staaten mit der Aufgabe der Verfassungsschutzbehörde nicht vereinbar sind. Andererseits können durch den „Kleinen Grenzverkehr“ auch die Sicherheitsinteressen der Empfänger-

staaten effektiver gewahrt werden, insbesondere dann, wenn gemeinsame Grundwerte betroffen sind.

In diesem Zusammenhang ist anzumerken, dass im Polizeirecht bereits eine länderübergreifende Zusammenarbeit im Rahmen des Schengener Durchführungsübereinkommens vorgesehen ist (§ 192 LVwG). Das Verfassungsschutzrecht folgt dieser Entwicklung im Einklang mit einem Beschluss der Innenministerkonferenz vom 26. November 1993.

**Zu Nr. 13 (§ 23)**

Zur Angleichung an das Bundesrecht wird in Abs. 1 der Änderung der Kreis der auskunftspflichtigen Behörden auf die aufgeführten Bundesbehörden und die Polizeien anderer Länder erweitert (§ 18 Abs. 3 Satz 2 BVerfSchG). Eine Verpflichtung der betreffenden Stellen zur Spontanübermittlung (Abs. 3) ist damit nicht verbunden, steht diese doch nicht zur landesrechtlichen Disposition.

Durch die Änderung in Abs. 3 Satz 3 erfolgt eine redaktionelle Anpassung an die Änderung in Nr. 2.

In Abs. 3 Satz 5 wird der inzwischen veraltete Verweis auf das Artikel 10-Gesetz fortgeschrieben. Das Artikel 10-Gesetz ist 2001 grundlegend überarbeitet worden. Mit der Neufassung werden strengere Anforderungen an die Datenverarbeitung gestellt. Jene sind auch im Rahmen der Übermittlung nach § 23 zu berücksichtigen. Die Gesetzesänderung stellt dies klar.

**Zu Nr. 14 (§ 25)**

Der Auskunftsanspruch wird auf Anregung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein an § 19 Bundesdatenschutzgesetz (BDSG) angepasst. Dabei wird in Abs. 1 gemäß § 19 Abs. 1 Satz 2 und 3 BDSG klargestellt, dass

- der Antrag auf Auskunft spezifiziert werden sollte (Satz 2) und
- insbesondere eine Auskunft aus (nicht automatisierten) Sachakten unterbleiben kann, wenn diese nicht durch Einträge in Dateien erschlossen werden können und infolgedessen die Erteilung der Auskunft außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht (Satz 3).

In Abs. 2 werden die Auskunftsverweigerungsgründe des § 19 Abs. 4 BDSG übernommen, wobei in Nr. 1 klargestellt wird, das die verfassungsschutzbehördliche Aufgabenerfüllung insbesondere dann gefährdet ist, wenn eine Ausforschung der nachrichtendienstlichen Arbeitsmethoden und Mittel zu befürchten steht. Es wird insoweit am geltenden § 25 Abs. 2 festgehalten. Im Übrigen wird in Abs. 4 die Behördenbezeichnung des ehemaligen Landesbeauftragten für Datenschutz fortgeschrieben.

**Zu Nr. 15 (§ 26)**

Die parlamentarische Kontrolle

- über die Angelegenheiten des Verfassungsschutzes und
- über die Durchführung von Maßnahmen zur Post- und Fernmeldeüberwachung (§ 14 Artikel 10-Gesetz, geltender § 2 AG-Artikel 10-Gesetz)

wird organisatorisch in einem Parlamentarischen Kontrollgremium zusammengefasst. Dadurch soll den Parlamentariern ein besserer Überblick über die Tätigkeit der Verfassungsschutzbehörde verschafft werden. Die Zusammenlegung der Gremien dient überdies der Verwaltungsvereinfachung. Es wird damit dem Beispiel des Bundes und Nordrhein-Westfalens gefolgt. Die Vorab-Kontrolle von Maßnahmen zur Post- und Fernmeldeüberwachung durch die G 10-Kommission (§ 15 Artikel 10-Gesetz, § 26 a) bleibt von der Zusammenlegung der Gremien unberührt.

**Zu Nr. 16 (§ 26 a)**

Der G 10-Kommission obliegt die parlamentarische Vorab-Kontrolle verfassungsschutzbehördlicher Maßnahmen zur Post- und Fernmeldeüberwachung nach § 15 Artikel 10-Gesetz (Abs. 1 Satz 1). Ferner ist sie zu beteiligen, wenn durch die in Abs. 1 Satz 2 genannten Maßnahmen der Verfassungsschutzbehörde in anderer Weise in die Brief-, Post- und Fernmeldefreiheit (Art. 10 GG) eingegriffen wird.

Die G 10-Kommission fußt nach geltendem Recht auf § 3 des Ausführungsgesetzes zum Artikel 10-Gesetz (AG-Artikel 10-Gesetz). Das Ausführungsgesetz ist nach der Neufassung des Artikel 10-Gesetzes veraltet. Die dortigen Regelungen werden fortgeschrieben und gehen im Sachzusammenhang der verfassungsschutzbehördlichen Befugnisse (§ 8 Abs. 9) in das Landesverfassungsschutzgesetz ein. Dies erleichtert die Rechtsanwendung und macht eine weitere Rechtsvorschrift entbehrlich.

Abs. 2 regelt unter Rückgriff auf § 3 Abs. 3 AG-Artikel 10-Gesetz die Einrichtung der G 10-Kommission. Die Vorschrift wird um die Maßgaben

- zu den Befugnissen der Vertreter nach § 15 Abs. 1 Satz 1 Artikel 10-Gesetz (Abs. 2 Satz 3) und
- zur Geheimhaltung der Beratungen nach § 15 Abs. 2 Artikel 10-Gesetz ergänzt, wobei insoweit auf die betreffenden Vorschriften zum Parlamentarischen Kontrollgremium verwiesen wird (Abs. 2 Satz 5).

**Zu Nr. 17 (§ 27)**

Folgeänderung zu Nr. 15.

**Zu Artikel 2 (Inkrafttreten, Außerkrafttreten, Übergangsregelung)**

Artikel 2 regelt das Inkrafttreten des Gesetzes und hebt gleichzeitig das Ausführungsgesetz zum Artikel 10-Gesetz auf (Abs. 1). Hinsichtlich der parlamentarischen Kontrolle des Verfassungsschutzes ist folgende Übergangsregelung vorgesehen (Abs. 2 und 3):

Die G 10-Kommission bleibt unverändert bestehen und findet in § 26 a lediglich eine neue Rechtsgrundlage. Das aufgrund des aufgehobenen Ausführungsgesetzes gebildete G 10-Gremium bleibt zunächst bestehen und nimmt seine bisherigen Aufgaben, d. h. die Kontrolle der verfassungsschutzbehördlichen Post- und Fernmeldeüberwachung bis zum Ablauf der Wahlperiode wahr. Die Parlamentarische Kontrollkommission erhält die Bezeichnung Parlamentarisches Kontrollgremium. Es nimmt die nach der Gesetzesänderung erweiterten Aufgaben wahr, zunächst aber nicht die des fortbestehenden G 10-Gremiums (§ 26 Abs. 1 Satz 2 und 3). Die Aufgaben des

G 10-Gremiums gehen erst mit Ablauf der Wahlperiode auf das dann neu zu konstituierende Parlamentarische Kontrollgremium über.