Überwachung

Wir veröffentlichen den Gesetzentwurf: Seehofer will Staatstrojaner für den Verfassungsschutz

Der Verfassungsschutz soll neue Befugnisse bekommen und unter anderem Staatstrojaner einsetzen dürfen. Das steht in einem Gesetzentwurf des Innenministeriums, den wir veröffentlichen. Justizministerin Barley lehnt den Entwurf komplett ab und verlangt einen neuen Vorschlag von Innenminister Seehofer.

28.03.2019 um 08:09 Uhr - Andre Meister, Anna Biselli - 2 Ergänzungen

Innenminister Seehofer will nicht nur Feature-Phones hacken.— Gemeinfrei Wilfried Pohnke

IT-Geräte hacken und mit Trojanern infizieren: Das ist die intensivste Überwachungsmethode im Arsenal von Polizei und Geheimdiensten. Eingeführt wurde das staatliche Hacken, um internationalen Terrorismus zu verhindern. Seit zwei Jahren darf die Polizei damit Alltagskriminalität verfolgen.

Noch während Verfassungsbeschwerden gegen diese Ausweitung laufen, legt Innenminister Seehofer nach und will auch den Geheimdiensten Verfassungsschutz und BND Staatstrojaner erlauben. Wir veröffentlichen den vollständigen Gesetzentwurf des Innenministeriums.

Staatlicher Eingriff in IT-Systeme

Demnach soll In- und Auslandsgeheimdienst der „Eingriff in informationstechnische Systeme“ erlaubt werden. Dadurch dürften die Geheimdienste Geräte wie Computer und Smartphones hacken, aber auch andere IT-Systeme im „Internet der Dinge“ – sogar Autos.

Sven Herpig von der Stiftung Neue Verantwortung beschäftigt sich intensiv mit dem Zusammenhang von staatlichem Hacking und IT-Sicherheit. Gegenüber netzpolitik.org sagt er:

> Durch die neuen Befugnisse dürften BfV und BND zukünftig Quellen-Telekommunikationsüberwachung und Online-Durchsuchung auch gegen Heimautomatisierung wie Alexa und Co einsetzen. Das kommt einer massiven Ausweitung invasiver Überwachungsmaßnahmen gleich.

Kein Unterschied zwischen zwei Trojanern

Für die Polizei wurde ein rechtlicher Unterschied zwischen zwei Trojaner-Arten erfunden: eine „Online-Durchsuchung“ infiziert ein Gerät und wertet dann sämtliche Daten und Sensoren aus, während eine „Quellen-Telekommunikationsüberwachung“ nach einer Infektion versucht, nur Kommunikation abzuhören. Technisch gibt es diesen Unterschied nicht, das neue Gesetz versucht diese Trennung gar nicht mehr.

Der Verfassungsschutz soll nicht nur Geräte von Gefährdern hacken dürfen, sondern auch IT-Systeme, die Informationen von Gefährdern verarbeiten. Das gilt auch, wenn andere Personen als die Zielpersonen „unvermeidlich“ mitbetroffen sind. Das könnte Anbieter von Internet-Diensten treffen, die nicht mit dem Geheimdienst kooperieren oder davon nichts erfahren sollen.

Für den BND ist das Ausland vogelfrei

Im Gegensatz zum Verfassungsschutz darf der BND schon hacken. Seit vielen Jahren gibt es in Pullach eine geheime Hacker-Einheit. Der BND und seine Hacker betrachten Ausländer im Ausland als „vogelfrei“, die sie jederzeit überwachen und mit Schadsoftware infizieren können. Das neue Gesetz will die Praxis rechtssicher machen.

Der BND soll im Ausland so ziemlich alles hacken dürfen, so lange es „Erkenntnisse von außen- und sicherheitspolitischer Bedeutung“ verspricht. Dieser Satz aus dem BND-Gesetz erlaubt laut Verfassungsrechtlern „die Überwachung von annähernd beliebigen Zielen“.

Als der BND 2007 einen afghanischen Minister hackte, war auch eine deutsche Journalistin davon betroffen. Damals war das ein Skandal. In Zukunft soll der Auslandsgeheimdienst ganz legal deutsche Bürger, Firmen oder Vereine hacken dürfen, wenn er sie auch sonst mit anderen Methoden überwachen darf.

Staatstrojaner für alle Sicherheitsbehörden

Der BND soll Staatstrojaner nicht nur für sich selbst einsetzen, sondern auch für andere. In Zukunft sollen alle deutsche Behörden den BND für sich hacken lassen können, wenn sie das auch selbst dürfen. Das Gesetz bezeichnet diese Amtshilfe als „ressourcenschonende Zusammenarbeit“.

Damit nicht jede Behörde eigene Trojaner entwickeln muss, wurde vor zwei Jahren eine Hacker-Behörde zur Forschung und Entwicklung gegründet: die Zentrale Stelle für Informationstechnik im Sicherheitsbereich. Die „Kunden“ der ZITiS sind Bundeskriminalamt, Bundespolizei und Bundesverfassungsschutz. Der BND ist im Beirat nur Gast, er teilt seine Sicherheitslücken nicht gerne mit anderen.

In der Umsetzung könnte das so aussehen: Eine Polizeibehörde sagt dem BND, wen er hacken soll. Der Geheimdienst infiltriert das Ziel, leitet die Daten aus und gibt der Polizei eine Kopie. Wie genau der BND das macht, kann er für sich behalten. Damit umgeht der Auslandsgeheimdienst nicht nur seinen Interessenkonflikt, er untergräbt auch demokratische Kontrolle und das Trennungsgebot von Polizei und Geheimdiensten.

SPD geht auf die Barrikaden

Der Gesetzentwurf wurde vom Innenministerium erarbeitet und Anfang März zur Ressortabstimmung an die anderen Ministerien übermittelt. Seit letzter Woche kursiert das Papier unter Journalisten.

Der Koalitionspartner SPD „geht auf die Barrikaden“. Der innenpolitische Sprecher der SPD-Fraktion im Bundestag Burkhard Lischka sagte der taz: „Mit der SPD ist das nicht zu machen“. Gegenüber netzpolitik.org bestätigt er: „Da die SPD den Gesetzentwurf in der vorliegenden Form in Gänze ablehnt, bitte ich um Verständnis dafür, dass wir nicht auf weitere Detailfragen eingehen wollen.“

Gestern berichtete die Funke Mediengruppe, dass auch Justizministerin Katarina Barley eine Prüfung des Entwurfs ablehnt und nicht über Einzelmaßnahmen diskutieren will. Stattdessen soll Innenminister Seehofer nacharbeiten und einen neuen Vorschlag vorlegen.

Justizministerin oder Spitzenkandidatin?

Das Innenministerium gibt sich gelassen: „Natürlich nehmen wir den Entwurf nicht zurück, nur weil irgendjemand meint, Anmerkungen zu haben“, so ein Sprecher gegenüber netzpolitik.org. Damit hat die Bundesregierung mit dem Verfassungsschutz-Gesetz einen weiteren Streitpunkt, der vielleicht nur mit einem Machtwort der Kanzlerin geklärt werden kann.

Es könnte natürlich sein, dass Katarina Barley ihr Veto nicht als Justizministerin einlegt, sondern als Spitzenkandidatin für die Europawahl. Vor der Wahl Ende Mai dürfte die Regierung das Gesetz jedenfalls nicht beschließen. Danach kommt es dann auf die SPD an – und Barleys Nachfolger:in.

Hier der Gesetzentwurf in Volltext:

Referentenentwurf des Bundesministeriums des Innern, für Bau

und Heimat

Entwurf eines Gesetzes zur Harmonisierung des Verfassungsschutzrechts

A. Problem und Ziel

Die föderal arbeitsteilige Organisation des Verfassungsschutzes erfordert angesichts gesamtstaatlicher Rechtsgüter und länderübergreifender Bedrohungen zur effektiven Zusammenarbeit der Verfassungsschutzbehörden des Bundes und der Länder einen harmonisierten Rechtsrahmen mit wirksamen Befugnissen. Diese Befugnisse sollten sich nach der Evaluierung von bislang befristeten Regelungen des Bundesverfassungsschutzgesetzes zugleich wertungskonsistenter in das Bundesrecht einfügen.

B. Lösung

Zu diesen Harmonisierungszwecken wird das Bundesverfassungsschutzgesetz auf der Grundlage der betreffenden Empfehlungen der Innenministerkonferenz zur Rechtsvereinheitlichung novelliert. Gleichzeitig wird der Anwendungsbereich von Regelungen zu Unternehmensauskünften konsequenter auf Anfragen der Landesverfassungsschutzbehörden erstreckt, um die intendierte Rechtsvereinheitlichung insoweit bereits bundesgesetzlich zu erreichen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht durch die Wiedereinführung der Regelung zu Auskunftsersuchen über Postdienstleistungen lediglich ein marginaler Erfüllungsaufwand, da die erwartbare Fallzahl gering ist. Die Erstreckung der bundesrechtlichen Mitwirkungspflichten auch auf den Landesvollzug lässt angesichts bisheriger Fallzahlen und derzeitiger landesgesetzlicher Parallelregelungen keine nennenswerten Mehraufwände erwarten, die im Übrigen durch Erstattungspflichten abgegolten werden. Möglicherweise ergeben sich hier auch Einsparungen durch erleichterte Durchführung auf einheitlicher Grundlage.

E.3 Erfüllungsaufwand der Verwaltung

Durch die Änderung des Bundesverfassungsschutzgesetzes kann sowohl dem Bund als auch den Ländern Erfüllungsaufwand entstehen.

Bund:

Dem Bund entsteht ein Erfüllungsaufwand in nicht bezifferbarer Höhe mit der Durchführung neuer Befugnisse (einschließlich Mitteilungsvorschriften, parlamentarischer und Datenschutzkontrolle). Gleichzeitig ergeben sich nicht bezifferbare Einsparungen durch Bürokratieabbau bei der wertungskonsistenten Anpassung von Prozessen. Ebenfalls nicht abschätzbar ist, inwiefern durch die neuen Regelungen aufwändigere Ermittlungen mit anderen Methoden entfallen können und dadurch Aufwände eingespart werden.

Entstehender Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Länder:

Die vorstehenden Erwägungen gelten grundsätzlich ebenso für die Länder, soweit Regelungen neu auf sie erstreckt werden. Allerdings bestanden bislang bereits entsprechende landesgesetzliche Befugnisse.

Kommunen:

Für die Kommunen fällt kein Erfüllungsaufwand an.

F. Weitere Kosten

Keine.

Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat

Entwurf eines Gesetzes zur Harmonisierung des Verfassungsschutzrechts

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1 – Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S.2954, 2970), das zuletzt durch [...] geändert worden ist, wird wie folgt geändert:

1. Dem § 5 Absatz 3 werden folgende Sätze angefügt:

„Kommt ein Einvernehmen zu allgemeinen Regelungen nicht zustande, kann das Bundesamt für Verfassungsschutz entscheiden. Die Entscheidung tritt außer Kraft, wenn die Mehrheit der Landesbehörden für Verfassungsschutz widerspricht."

2. § 6 Absatz 2 Sätze 1 bis 3 werden durch folgende Sätze ersetzt:

„Die Verfassungsschutzbehörden verarbeiten zur Erfüllung ihrer Unterrichtungspflichten nach Absatz 1 Informationen im gemeinsamen nachrichtendienstlichen Informationssystem. Der Militärische Abschirmdienst kann zur Erfüllung der Unterrichtungspflichten nach § 3 Absatz 3 des MAD-Gesetzes am nachrichtendienstlichen Informationssystem teilnehmen. Der

Abruf von Daten aus dem nachrichtendienstlichen Informationssystem im automatisierten Verfahren ist im Übrigen nur entsprechend §§ 22a, 22b zulässig. Für die Verarbeitung personenbezogener Daten im nachrichtendienstlichen Informationssystem gelten §§ 10 und 11."

3. § 8 Absatz 2 wird aufgehoben.

4. Die §§ 8a bis 9b werden ersetzt durch die folgenden §§ 8a bis 9e:

"

§ 8a – Übermittlungs- und Mitwirkungspflicht nicht-öffentlicher Stellen

(1) Geschäftsmäßige Dienstleister der Branchen

1. Personenverkehr,
2. [Kredit- und] Finanzwesen,
3. Post-, Telekommunikations- und Telemediendienste,

die in Deutschland eine Niederlassung haben oder Leistungen erbringen oder hieran mitwirken, haben den Verfassungsschutzbehörden des Bundes und der Länder auf Verlangen die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses mit den Nutzern der angebotenen Dienste (Bestandsdaten) gespeicherten Daten zu übermitteln, soweit die Auskunft zur Erfüllung ihrer Aufgaben nach § 3 Absatz 1 erforderlich ist. Besondere Vorschriften, insbesondere über die jeweils mitzuteilenden Datenarten, bleiben unberührt. Eine Auskunft nach Satz1 Nummer 3 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). Dient eine Auskunft ausschließlich der Vorbereitung von Folgemaßnahmen, darf sie nur nach Maßgabe der dafür geltenden Regelungen verlangt werden. Die Verfassungsschutzbehörden können die zur Erfüllung ihrer Aufgaben erforderlichen Bestandsdaten auch durch Ersuchen um Abruf an das Bundeszentralamt für Steuern nach § 93b der Abgabenordnung und die Bundesnetzagentur nach § 112 des Telekommunikationsgesetzes erheben.

(2) Absatz 1 Satz 1, auch in Verbindung mit Satz 2, gilt für die dort Verpflichteten ebenso zu den Umständen und Inhalten der von ihnen erbrachten Leistungen, wenn die Auskunft zur Aufklärung von Tätigkeiten nach § 3 Absatz 1 Nummer 2, Bestrebungen nach § 3 Absatz 1 Nummer 3 oder Bestrebungen von erheblicher Bedeutung nach § 3 Absatz 1 Nummer 1 und 4 (Bedrohungen von erheblicher Bedeutung) erforderlich und die Verfassungsschutzbehörde zur Erhebung der Daten befugt ist. Wenn Leistungsgegenstand der Transport oder die Verwahrung von Sachen ist, erfolgt die Auskunft durch Gewährung vorübergehenden Besitzes zur Augenscheinnahme und Untersuchung.

(3) Die Betreiber einer Videoüberwachung nach § 4 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes sind verpflichtet, einer Verfassungsschutzbehörde die Überwachung auszuleiten und Aufzeichnungen zu übermitteln, wenn dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung erforderlich ist. Die Maßnahme darf nur unter den Voraussetzungen des § 9 Absatz 4 Satz 1 gegen eine Person gerichtet werden.

(4) Die Verpflichteten und ihre mit der Durchführung betrauten oder hieran beteiligten Beschäftigten haben über das Mitwirkungsverlangen und die Mitwirkung gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren. § 2 Absatz 2 Satz 2 des Artikel 10-Gesetzes gilt entsprechend für die Mitwirkung an Maßnahmen nach § 9d. Das Mitwirkungsverlangen ist mit dem Hinweis zu verbinden, dass die Erhebung keinen Verdacht auf ein rechtswidriges Verhalten des Betroffenen begründet. Der Verpflichtete darf an die Datenerhebung in Geschäftsverbindungen oder im Rechtsverkehr keine dem Betroffenen nachteiligen Folgen knüpfen.

(5) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Justiz und für Verbraucherschutz und dem Bundesministerium der Verteidigung ohne Zustimmung des Bundesrates zu bestimmen, dass die Verpflichteten

1. an angeordneten Maßnahmen nach dem Artikel 10-Gesetz und § 9d im Rahmen ihres Geschäftsbetriebs mitwirken, insbesondere durch
   a. Zugangsgewährung zu ihren Einrichtungen,
   b. Einbringen von technischen Mitteln zur Durchführung von § 11 Absatz 1a des Artikel 10-Gesetzes oder § 9d,

2. Informationen, soweit dazu keine Regelungen auf Grund des § 110 des Telekommunikationsgesetzes getroffen werden, ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermitteln müssen. Dabei können insbesondere geregelt werden
   a. die Voraussetzungen für die Anwendung des Verfahrens,
   b. das Nähere über Form, Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten,
   c. die Art und Weise der Übermittlung der Daten,
   d. die Zuständigkeit für die Entgegennahme der zu übermittelnden Daten,
   e. der Umfang und die Form der für dieses Verfahren erforderlichen besonderen Erklärungspflichten des Auskunftspflichtigen und
   f. Tatbestände und Bemessung einer auf Grund der Auskunftserteilung nach Absatz 2 an Verpflichtete zu leistenden Aufwandsentschädigung.

Zur Regelung der Datenübermittlung kann in der Rechtsverordnung auf Veröffentlichungen sachverständiger Stellen verwiesen werden; hierbei sind das Datum der Veröffentlichung, die Bezugsquelle und eine Stelle zu bezeichnen, bei der die Veröffentlichung archivmäßig gesichert niedergelegt ist.

§ 9 – Einsatz nachrichtendienstlicher Mittel

(1) Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) einsetzen. Nachrichtendienstliche Mittel sind insbesondere

1. Legenden, insbesondere fingierte biographische, berufliche oder gewerbliche Angaben, und Beschaffung, Erstellung und

Verwendung von Tarnpapieren und Tarnkennzeichen,

2. Personen, die der Verfassungsschutzbehörde logistische oder sonstige Hilfe leisten,
3. Personen, die in Einzelfällen oder gelegentlich wegen ihrer Kontakte zu einem Beobachtungsfeld Hinweise geben,
4. Informationserhebung im Internet unter Ausnutzung schutzwürdigen Vertrauens Betroffener,
5. Ermittlungen durch planmäßig und dauerhaft zur Informationsbeschaffung eingesetzte Personen,
   a. deren Einsatz für das Bundesamt für Verfassungsschutz Dritten nicht bekannt ist (Vertrauensleute),
   b. die als eigene Mitarbeiter unter einer auf Dauer angelegten Legende eingesetzt werden (Verdeckte Mitarbeiter)

   ohne deren tatsächlichen Zweck anzugeben (verdeckte Ermittlungen),

6. Observationen,
7. technische Mittel, insbesondere zur heimlichen
   a. optischen oder akustischen Überwachung von Personen, Gegenständen oder Vorgängen und
   b. Aufklärung technischer Signale, insbesondere zur Gewinnung von Erkenntnissen über gesendete Inhalte, nähere Umstände oder abstrahlende Geräte,

8. vorübergehende heimliche Inbesitznahme von Sachen.

Das Bundesamt für Verfassungsschutz hat die nachrichtendienstlichen Mittel in einer Dienstvorschrift abschließend zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat, das das Parlamentarische Kontrollgremium unterrichtet.

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten mit nachrichtendienstlichen Mitteln nur erheben bei tatsächlichen Anhaltspunkten dafür, dass

1. auf diese Weise Erkenntnisse über
   a. Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 oder

b. die zu deren Erforschung erforderlichen Quellen

gewonnen werden können oder

2. dies erforderlich ist zum Schutz
   a. der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten oder
   b. überwiegender Interessen des Betroffenen, indem der Zweck der Ermittlungen Dritten nicht bekannt wird (Absatz 2 Nummer 5).

(3) Es darf

1. verdeckte Ermittlungen (Absatz 1 Satz2 Nummer 5) zur Aufklärung von Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 und 4 nur nach Maßgabe des § 9b durchführen,
2. Personen durchgehend länger als 48 Stunden ohne Eingriff in Artikel 13 des Grundgesetzes observieren (Absatz 1 Satz2 Nummer 6 und 7) nur zur Aufklärung von Bedrohungen von erheblicher Bedeutung,
3. nachrichtendienstliche Mittel unter Eingriff in Artikel 10, 13 des Grundgesetzes oder die Vertraulichkeit und Integrität informationstechnischer Systeme nur nach Maßgabe der §§ 9c bis 9e einsetzen.

(4) Nachrichtendienstliche Mittel dürfen sich nach Absatz 2 Nummer 1 Buchstabe a und Nummer 2 Buchstabe a systematisch nur gegen Personen richten, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. an den Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 oder an einer Gefährdung nach Absatz 2 Nummer 2 Buchstabe a durch ihr Verhalten oder Sachen in ihrem Besitz, die für die Bestrebungen, Tätigkeiten oder Gefährdungen genutzt werden, beteiligt sind oder
2. im Zusammenhang mit einer Person nach Nummer 1 stehen und durch die Maßnahme Erkenntnisse für die Aufklärung der Bestrebungen, Tätigkeiten oder Gefährdungen gewonnen werden können, die nicht gleichermaßen nach Nummer 1 zu

gewinnen sind.

Die besonderen Regelungen zur Maßnahmerichtung in §§ 9c bis 9e bleiben unberührt. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidlich betroffen werden.

(5) Beim Einsatz nachrichtendienstlicher Mittel nach Absatz1 Satz2 Nummern 6 bis 9 und Absatz 3 Nummer 1 gegen Personen ist die Durchführung zu protokollieren, insbesondere

1. die Person, gegen die sich die Maßnahme richtet,
2. Art, Umfang und Dauer der Maßnahme,
3. in den dort geregelten Fällen die Angaben nach § 11 Absatz 1a des Artikel 10-Gesetzes sowie nach § 9d Absatz 6 Satz 4 und § 9e Absatz 3 Satz 1 Nummer 1.

§ 9a – Schranken nachrichtendienstlicher Mittel

(1) Beim Einsatz nachrichtendienstlicher Mittel sind Schutznormen der Rechtspflege und der parlamentarischen Kontrolle zu beachten. In Individualrechte darf durch nachrichtendienstliche Mittel nur nach Maßgabe besonderer Befugnisse eingegriffen werden. Der Einsatz nachrichtendienstlicher Mittel ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen oder ein rechtlich geschütztes öffentliches Interesse weniger beeinträchtigende Weise möglich ist. Eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch Ersuchen nach § 18 Absatz 3 gewonnen werden kann.

(2) Eine Maßnahme ist unzulässig, soweit

1. tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Informationen aus dem Kernbereich privater Lebensgestaltung gewonnen werden würden, oder
2. Informationen
   a. bei einer in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder 4 der Strafprozessordnung genannten Person, im Falle dessen Nummer 3 beschränkt auf
      - Rechtsanwälte oder
      - Kammerrechtsbeistände,

b. oder deren Berufshelfer (§ 53a der Strafprozessordnung)

nicht zur Aufklärung von Beteiligungen dieser Personen an Bedrohungen erhoben werden und die Maßnahme voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte.

Werden solche Informationen bei einer Maßnahme gewonnen, dürfen sie nicht genutzt werden. Aufzeichnungen sind zu löschen. Die Tatsache der Erlangung und Löschung dieser Informationen ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist

1. in den Fällen der §§ 9c bis 9e sechs Monate nach der Mitteilung an den Betroffenen oder dem abschließenden Absehen von der Mitteilung,
2. im Übrigen nach Mitteilung an den Bundesbeauftragten oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am Ende des übernächsten Kalenderjahres, das der Protokollierung folgt,

zu löschen.

(3) Ergeben sich bei der Maßnahme während der Durchführung tatsächliche Anhaltspunkte dafür, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst werden, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung eingesetzter Personen möglich ist und solange die Anhaltspunkte bestehen. Beim Einsatz technischer Mittel nach § 9 Absatz 2 Satz1 Nummer7 und § 9 Absatz 3 Nummer 3 dürfen automatische Aufzeichnungen fortgesetzt werden, wenn Zweifel am Vorliegen solcher Inhalte bestehen.

(4) Auf Aufzeichnungen nach

1. Absatz 3 Satz 2 und
2. §§ 9d, 9e Absatz 1, soweit bei deren Auswertung tatsächliche Anhaltspunkte dafür bekannt werden, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst wurden, ohne dass bereits das Bundesamt für Verfassungsschutz dabei solche Inhalte feststellt,

ist § 3a Absatz 1 Satz 4 bis 6 und Absatz 2 des Artikel 10-Gesetzes entsprechend anzuwenden. Ist die weitere Verarbeitung danach unzulässig, gilt Absatz 2 Satz 2 bis 6.

(5) Die Beeinträchtigung rechtlich geschützter Interessen durch Anwendung eines nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Näheres ist in der Dienstvorschrift nach §9 Absatz 2 Satz 3 zu regeln. Erfolgen Maßnahmen bei einer in § 53 Absatz 1 Satz1 Nummer 3 bis 3b oder Nummer 5 der Strafprozessordnung genannten Person oder deren Berufshelfer (§ 53a der Strafprozessordnung) nicht zur Aufklärung von Beteiligungen dieser Personen an Bedrohungen, sind das öffentliche Interesse an den von dieser Person wahrgenommenen Aufgaben und das Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Für Rechtsanwälte oder Kammerrechtsbeistände bleiben die Absätze 2 bis 4 unberührt.

(6) Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich ergibt, dass er nicht oder nicht auf diese Weise erreicht werden kann.

§ 9b – Vertrauensleute, Verdeckte Mitarbeiter

(1) Das Bundesamt für Verfassungsschutz darf Privatpersonen als Vertrauensleute (§ 9 Absatz 3 Nummer 1 Buchstabe a) zur Aufklärung von Bestrebungen unter den Voraussetzungen des § 9 Absatz 1 einsetzen. Ein dauerhafter Einsatz zur Aufklärung von Bestrebungen nach § 3 Absatz 1 Nummer 1 und 4 ist nur bei Bestrebungen von erheblicher Bedeutung zulässig, insbesondere wenn sie darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten.

(2) Über die Verpflichtung von Vertrauensleuten entscheidet die Amtsleitung oder eine dazu ermächtigte Abteilungsleitung. Als Vertrauensleute zur Aufklärung von Bestrebungen dürfen Personen nicht angeworben und eingesetzt werden, die

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,
2. von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,

3. an einem Aussteigerprogramm teilnehmen,
4. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Mitarbeiter eines solchen Mitglieds oder einer Fraktion dieser Parlamente sind oder
5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Der Präsident oder die Präsidentin des Bundesamtes kann eine Ausnahme von Satz1 Nummer 5 zulassen, wenn die Verurteilung nicht als Täter eines Totschlags (§§212, 213 des Strafgesetzbuches) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Bestrebungen, die auf die Begehung von in § 3 Absatz 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, unerlässlich ist. Im Falle einer Ausnahme nach Satz 3 ist der Einsatz nach höchstens sechs Monaten zu beenden, wenn er zur Erforschung der in Satz 3 genannten Bestrebungen nicht zureichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten.

(3) Vertrauensleute dürfen weder zur Gründung von Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 oder 4 noch zur steuernden Einflussnahme auf diese eingesetzt werden. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbaren Vereinigungen, tätig werden, um deren Bestrebungen aufzuklären. Im Übrigen ist im Einsatz eine Beteiligung an Bestrebungen zulässig, wenn sie

1. nicht in Individualrechte eingreift,
2. von den an den Bestrebungen Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und
3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.

Sofern zureichende Anhaltspunkte dafür bestehen, dass Vertrauensleute rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht haben, soll der Einsatz

unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen von Satz 4 entscheidet die Amtsleitung.

(4) Die Staatsanwaltschaft kann von der Verfolgung von Vergehen, die Vertrauensleute der Verfassungsschutzbehörden im Einsatz begangen haben, absehen oder eine bereits erhobene Klage in jeder Lage des Verfahrens zurücknehmen und das Verfahren einstellen, wenn

1. der Einsatz zur Aufklärung von Bestrebungen erfolgte, die auf die Begehung von in § 3 Absatz 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, und
2. die Tat von den übrigen Beteiligten derart erwartet wurde, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich war.

Dabei ist das Verhältnis der Bedeutung der Aufklärung des Sachverhalts zur Schwere der begangenen Straftat und Schuld des Täters zu berücksichtigen. Ein Absehen von der Verfolgung ist ausgeschlossen, wenn eine höhere Strafe als ein Jahr Freiheitsstrafe zu erwarten ist. Ein Absehen von der Verfolgung ist darüber hinaus stets ausgeschlossen, wenn zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt werden würde. Dritten kann ein anderer Einstellungsgrund angegeben werden, wenn dies zum Schutz des Betroffenen oder seines Einsatzes erforderlich ist. Die Sätze 1 bis 5 gelten auch bei der Aufklärung von Tätigkeiten nach § 3 Absatz 1 Nummer 2 und in Fällen der Landesbehörden für Verfassungsschutz.

(5) Die Eigenschaft als Vertrauensperson ist geheim. Liegt in einem amtlichen Verfahren ausnahmsweise ein hohes Interesse an einer Aufklärung der Eigenschaft als Vertrauensperson vor, kann das Bundesamt für Verfassungsschutz auf Anfrage der verfahrensführenden Stelle vor Anhörung des Zeugen eine Genehmigung zur Aussage erteilen, wenn

1. der Sachverhalt offenkundig von Bedeutung für das Verfahren ist,
2. aufgrund besonderer Umstände auszuschließen ist, dass dadurch
   a. das Wohl des Bundes oder

b. überwiegende schutzwürdige Interessen des Betroffenen oder Dritter gefährdet würden.

Die Frage nach der Eigenschaft als Vertrauensperson ist nur zulässig, wenn die Genehmigung nach Satz 2 erteilt wurde. Die Sätze 1 bis 3 gelten auch in Fällen der Landesbehörden für Verfassungsschutz.

(6) Die Bundesregierung trägt dem Parlamentarischen Kontrollgremium mindestens einmal im Jahr einen Lagebericht zum Einsatz von Vertrauensleuten vor.

(7) Die Absätze 1, 3, 4 und 5 sind entsprechend auf den Einsatz von Verdeckten Mitarbeitern (§ 9 Absatz 3 Nummer 1 Buchstabe b) anzuwenden.

§ 9c – Eingriff in Brief-, Post- und Fernmeldegeheimnis

(1) Die Verfassungsschutzbehörden des Bundes und der Länder dürfen nach Maßgabe des Artikel 10-Gesetzes Telekommunikation überwachen und aufzeichnen sowie dem Brief- oder Postgeheimnis unterliegende Sendungen öffnen und einsehen.

(2) Die Verfassungsschutzbehörden des Bundes und der Länder dürfen Umstände der Verkehre bei Unternehmen, die Telekommunikations- oder Postdienste erbringen oder daran mitwirken, erheben, wenn dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung (§ 8a Absatz 2 Satz 1) erforderlich ist. Die auf Grund des § 113b des Telekommunikationsgesetzes gespeicherten Daten dürfen nur nach Maßgabe des Absatzes 1 erhoben werden.

(3) Für Maßnahmen nach Absatz 2 gelten zum Verfahren und zur Kontrolle sowie zur Weiterverarbeitung der erhobenen personenbezogenen Daten §§ 4 und 9 bis 16 des Artikel 10-Gesetzes, soweit sie auf Maßnahmen nach § 3 des Artikel 10-Gesetzes anzuwenden sind, entsprechend mit folgenden Maßgaben:

1. Abweichend von § 10 Absatz 3 des Artikel 10-Gesetzes genügt für die Erhebung von Umständen von Telekommunikation deren räumlich und zeitlich hinreichende Bezeichnung, sofern

anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

2. Abweichend von § 10 Absatz 5 des Artikel 10-Gesetzes ist die Anordnung einer Auskunft über künftig anfallende Daten oder deren Verlängerung auf höchstens sechs Monate zu befristen.

§ 9d – Eingriff in informationstechnische Systeme

(1) Das Bundesamt für Verfassungsschutz darf bei besonders schweren Bedrohungen durch Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 ohne Wissen des Betroffenen unter Eingriff in ein informationstechnisches System die dort verarbeiteten Daten erheben. Bedrohungen sind besonders schwer, wenn hinreichende Anhaltspunkte vorliegen für eine dringende Gefahr für

1. Bestand oder die Sicherheit des Bundes oder eines Landes,
2. die Funktionsfähigkeit lebenswichtiger Einrichtungen (§ 1 Absatz 5 Satz 1 des Sicherheitsüberprüfungsgesetzes) oder
3. Leib, Leben oder Freiheit einer Person.

Ein Fall des Satzes 2 Nummer 1 liegt insbesondere vor, wenn hinreichende Anhaltspunkte bestehen, dass jemand eine Straftat nach

1. §§ 81, 82, 94, 95 Absatz 3, § 96 Absatz 1, § 98 Absatz 1 Satz 2, § 99 Absatz2, § 100a Absatz 4 des Strafgesetzbuches oder § 13 des Völkerstrafgesetzbuches oder
2. §§ 202a, 202b, 303a, 303b, 308 Absatz 1 bis 3 des Strafgesetzbuches, soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet,

   plant oder begeht oder

3. §§ 89a, 89c Absatz 1 bis 4, § 100, § 129 Absatz 1 in Verbindung mit Absatz 5, wenn der Zweck oder die Tätigkeit der kriminellen Vereinigung auf politisch motivierte Gewalttaten gerichtet ist, § 129a Absatz 1, 2, 4, 5 Satz 1 Alternative1, jeweils auch in Verbindung mit § 129b Absatz 1 des Strafgesetzbuches, begangen hat und sein auf Gewaltanwendung gerichtetes

Verhalten fortsetzt.

(2) Maßnahmen nach Absatz 1 sind in der Regel nach § 9a Absatz 1 Satz 3 nur zulässig, wenn die Erforschung des Sachverhalts mit anderen Mitteln aussichtslos oder wesentlich erschwert wäre.

(3) Die Maßnahme darf sich nur gegen Personen richten, zu denen hinreichende Anhaltspunkte bestehen, dass

1. sie die Straftat planen oder begangen haben oder an den bezeichneten Bedrohungen beteiligt sind,
2. in ihrem informationstechnischen System Personen nach Nummer 1 Informationen verarbeiten und die Erforschung des Sachverhalts nicht ebenso durch eine Maßnahme nach Nummer 1 möglich ist.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidlich betroffen werden. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(4) Für das Verfahren und die Kontrolle gelten §§ 9 bis 12, § 14 Absatz 1 und § 15 Absatz 5 bis 7 des Artikel 10-Gesetzes, soweit sie auf Maßnahmen nach § 3 des Artikel 10-Gesetzes anzuwenden sind, entsprechend. In Antrag und Anordnung ist auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, anzugeben. Erfolgt der Vollzug nach § 15 Absatz 6 Satz 2 des Artikel 10-Gesetzes bereits vor Unterrichtung der G 10-Kommission, gelten § 15 Absatz 6 Satz 7 und 8 des Artikel 10-Gesetzes entsprechend.

(5) Das Bundesamt für Verfassungsschutz darf

1. die nach Absatz 1 erhobenen personenbezogenen Daten zur Aufklärung eines dort bezeichneten Verdachts weiterverarbeiten, einschließlich einer Übermittlung an Verfassungsschutzbehörden, und
2. Erkenntnisse aus der Verarbeitung nach Nummer 1 übermitteln, wenn hinreichende Anhaltspunkte bestehen, dass dies
   a. zur Abwehr einer in Absatz 1 bezeichneten dringenden Gefahr oder

b. zur Verfolgung einer in § 100b Absatz 1 der Strafprozessordnung genannten Straftat

erforderlich ist. § 4 Absatz 1, Absatz 2 Satz 1 und 2, Absatz 3 und 6 des Artikel 10-Gesetzes gelten entsprechend.

(6) An dem informationstechnischen System dürfen nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Sie sind bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig zu machen. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Bei jedem Einsatz sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

(7) Ein Systemabbild darf auch erhoben werden, wenn lediglich tatsächliche Anhaltspunkte für eine Gefahr für die in Absatz 1 Satz 1 benannten Rechtsgüter, insbesondere für einen Verdacht nach Absatz 1 Satz 2 vorliegen. Absatz 4 in Verbindung mit § 10 Absatz 2 Satz 2 G 10 ist mit der Maßgabe anzuwenden, dass die Bestimmung der Dauer der Beschränkungsmaßnahme entfällt. Absatz 5 ist mit der Maßgabe anzuwenden, dass ebenfalls tatsächliche Anhaltspunkte genügen.

§ 9e – Technische Datenerhebung aus Wohnungen

(1) Das Bundesamt für Verfassungsschutz darf ohne Wissen des Betroffenen unter Einsatz technischer Mittel personenbezogene Daten aus einer Wohnung entsprechend § 9d Absatz 1 und 2 erheben, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die

dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Auf die erhobenen Daten ist § 9d Absatz 5 mit der Maßgabe entsprechend anzuwenden, dass nach Nummer 2 Buchstabe b keine laufenden Bildaufzeichnungen übermittelt werden, wenn sie nicht unmittelbar die Begehung der Straftat dokumentieren.

(2) Die Maßnahme darf sich nur gegen Personen richten, zu denen hinreichende Anhaltspunkte bestehen, dass sie die Straftat planen oder begangen haben oder an den bezeichneten Bedrohungen beteiligt sind. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn hinreichende Anhaltspunkte bestehen, dass sich eine in Satz 1 genannte Person in ihr aufhält und der Zweck der Maßnahme nicht unter Beschränkung auf deren Wohnung zu erreichen ist.

(3) Für das Verfahren und die Kontrolle gelten §§ 9, 10 Absatz 1 bis 3 und 5 bis 7, § 12, § 14 Absatz 1 und § 15 Absatz 5 Sätze 2 bis 4 des Artikel 10-Gesetzes entsprechend mit folgenden Maßgaben:

1. In Antrag und Anordnung sind auch die zu überwachende Wohnung oder die zu überwachenden Wohnräume anzugeben.
2. Die Kontrollbefugnis der Kommission erstreckt sich auf die Anordnungskonformität der Erhebung und die gesamte Weiterverarbeitung der erlangten personenbezogenen Daten.

Die Maßnahme darf erst vollzogen werden, wenn das Bundesverwaltungsgericht die Zulässigkeit festgestellt hat. Satz 2 gilt nicht bei Gefahr im Verzug. Wird die Anordnung bei Gefahr im Verzug bereits vor der Zulässigkeitsfeststellung vollzogen, tritt sie außer Kraft, wenn die Feststellung nach Satz 2 nicht binnen drei Werktagen erfolgt. Tritt die Anordnung nach Satz 4 außer Kraft, ist die Verarbeitung erhobener personenbezogener Daten einzuschränken. Bis zur Feststellung nach Satz 2 ist die Weiterverarbeitung unzulässig. Stellt das Bundesverwaltungsgericht die Unzulässigkeit der Maßnahme fest, sind die Daten zu löschen. § 9a Absatz 2 Sätze 4 bis 6 gelten entsprechend.

(4) Beteiligte des Feststellungsverfahrens nach Absatz 3 sind die antragstellende und die anordnende Behörde. Die anordnende Behörde legt dem Bundesverwaltungsgericht mit dem

Feststellungsantrag die Anordnung vor. Macht die anordnende Behörde geltend, dass besondere Gründe des Geheimschutzes der Vorlage an das Gericht entgegenstehen, wird sie dadurch bewirkt, dass die Anordnung dem Gericht in von der anordnenden Behörde bestimmten Räumlichkeiten zur Verfügung gestellt wird. Das Gericht kann den Sachverhalt durch Anhörung der Beteiligten erforschen. Im Einverständnis der anordnenden Behörde kann der Vorsitzende oder Berichterstatter anstelle des Senats entscheiden. Gegen die Entscheidung nach Satz 5 kann die anordnende Behörde innerhalb von zwei Wochen nach Bekanntgabe Entscheidung des Senats beantragen. Das Verfahren unterliegt den Vorschriften des materiellen Geheimschutzes. Die Mitglieder des Gerichts sind zur Geheimhaltung verpflichtet. Für das nichtrichterliche Personal gelten die Regelungen des personellen Geheimschutzes.

(5) Im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz von Personen in einer Wohnung für das Bundesamt für Verfassungsschutz darf es in oder aus der Wohnung Daten mit technischen Mitteln erheben, wenn dies zur Abwehr von Gefahren für deren Leib, Leben oder Freiheit unerlässlich ist. Die erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eigensicherung nach Satz 1, sonstiger Gefahrenabwehr oder der Strafverfolgung verarbeitet werden. Die Verarbeitung zur sonstigen Gefahrenabwehr oder der Strafverfolgung setzt die Feststellung der Rechtmäßigkeit der Maßnahme durch das Bundesverwaltungsgericht voraus; bei Gefahr im Verzug ist die gerichtliche Entscheidung unverzüglich nachzuholen.

(6) Das Bundesamt für Verfassungsschutz darf Wohnungen auch betreten, um Maßnahmen nach den Absätzen 1 und 5, nach § 11 Absatz 1a des Artikel 10-Gesetzes oder § 9d vorzubereiten. Dies muss in der Anordnung oder einer Ergänzungsanordnung erlaubt sein. Heimlich betreten werden darf nur die Wohnung dessen, gegen den sich die Überwachungsanordnung richtet."

5. § 11 Absatz 1 wird aufgehoben.

6. In § 12 Absatz 3 Satz 2 wird das Wort „zehn" durch das Wort „fünfzehn" ersetzt.

7. In § 13 Absatz 4 Satz 3 wird die Angabe „§ 10 Absatz 1 Nummer 1

und 2 oder § 11 Absatz 1 Satz 3“ durch die Angabe „§ 10 Absatz 1 Nummer 1 oder 2“ ersetzt.

8. § 17 Absatz 2 und 3 werden durch folgenden Absatz ersetzt:

„(2) Soweit dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung (§ 8a Absatz 2) erforderlich ist, können auf Ersuchen einer Verfassungsschutzbehörde

1. an den Bestrebungen oder Tätigkeiten beteiligte Personen und
2. Personen und Sachen, die im Zusammenhang mit Personen nach Nummer 1 stehen, wenn dadurch Erkenntnisse über die Bestrebungen oder Tätigkeiten gewonnen werden können, die nicht nach Nummer 1 zu gewinnen sind,

zur polizeilichen Beobachtung ausgeschrieben werden. Den Verfassungsschutzbehörden darf die Eingabe der Ausschreibung in polizeiliche Informationssysteme ermöglicht werden. Dies gilt für das Bundesamt für Verfassungsschutz nach Maßgabe der unionsrechtlichen Bestimmungen auch für Datenverarbeitungssysteme der Europäischen Union. Ausschreibungen des Bundesamtes für Verfassungsschutz ordnet die Amtsleitung, eine dazu ermächtigte Abteilungsleitung oder ein dazu besonders beauftragter Bediensteter, der die Befähigung zum Richteramt hat, an. Die Ausschreibung ist auf höchstens ein Jahr zu befristen und kann wiederholt angeordnet werden. Liegen die Voraussetzungen für die Ausschreibung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen. Ausschreibungsersuchen und Eingaben nach Satz 2 und 3 hat die ausschreibende Verfassungsschutzbehörde zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.“

9. § 18 wird wie folgt geändert:

a) Absatz 1a Satz 3 wird aufgehoben.

b) In Absatz 1b werden vor dem Wort „unterrichten“ die Wörter „und das Bundesamt für Sicherheit in der Informationstechnik“

eingefügt.

c) In Absatz 5 sind nach Satz 1 folgende Sätze einzufügen:

„Ein Datenabruf im automatisierten Verfahren ist entsprechend § 6 Absatz 3 zu protokollieren. Protokollierungsregelungen für Abrufe anderer Stellen sind auf Abrufe der Verfassungsschutzbehörden nicht anzuwenden."

d) Absatz 6 wird wie folgt gefasst:

„(6) Personenbezogene Daten aus Maßnahmen, die §§ 9c bis 9e entsprechen, dürfen jeweils nur für Zwecke übermittelt werden, die in diesen Vorschriften zur Weiterverarbeitung durch das Bundesamt für Verfassungsschutz zugelassen sind. Werden personenbezogene Daten mit einer Kennzeichnung übermittelt, dass sie mit Maßnahmen, die §§ 9c bis 9e entsprechen, erhoben worden sind, ist diese Kennzeichnung aufrechtzuerhalten. Sie dürfen nur entsprechend diesen Vorschriften verarbeitet werden."

10. § 19 wird wie folgt geändert:

a) In Absatz 3 wird nach Satz 2 folgender Satz eingefügt:

„Personenbezogene Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres dürfen nur übermittelt werden, wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass die Übermittlung zur Abwehr einer erheblichen Gefahr für Leib oder Leben einer Person erforderlich ist oder tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zur Verfolgung einer der in § 3 Absatz 1 des Artikel 10-Gesetzes genannten Straftaten erforderlich ist."

b) Folgender Absatz 6 wird angefügt:

„(6) Eine Übermittlung ist auch zulässig, wenn offensichtlich ist, dass sie im Interesse des Betroffenen liegt, bei Minderjährigen insbesondere für Zwecke der Jugendhilfe."

11. § 22a wird wie folgt geändert:

a) In der Überschrift wird das Wort „Projektbezogene" gestrichen und das Wort „gemeinsame" durch das Wort „Gemeinsame"

ersetzt.

b) Absatz 1 wird durch folgende Absätze ersetzt:

„(1) Das Bundesamt für Verfassungsschutz kann mit dem Bundesnachrichtendienst und dem Bundesamt für Sicherheit in der Informationstechnik eine gemeinsame Datei zur Aufklärung von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 einrichten, an der auch Landesbehörden für Verfassungsschutz und der Militärische Abschirmdienst teilnehmen können.

(1a) Polizeibehörden des Bundes oder der Länder oder das Zollkriminalamt dürfen an einer gemeinsamen Datei teilnehmen, wenn die Teilnahme

1. zur projektbezogenen Zusammenarbeit bei der Aufklärung von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 erfolgt, im Falle der Nummern 1 und 4 nur wenn sie darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten und
2. auf höchstens zwei Jahre befristet ist. Die Frist kann um zwei Jahre und danach um ein weiteres Jahr, bei Aufklärung von Strukturen in den Fällen der §§ 129 bis 129b des Strafgesetzbuchs um jeweils ein weiteres Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist.“

c) Dem Absatz 2 werden folgende Sätze angefügt:

„Bei der Weiterverarbeitung personenbezogener Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verarbeitung personenbezogener Daten Anwendung. Zweckbindungen für eine Weiterverarbeitung, auch durch den Empfänger nach Übermittlung, bleiben unberührt.“

d) Absatz 3 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „projektbezogenen“ gestrichen.

bb) Folgende Sätze werden angefügt:

„Scheidet ein Teilnehmer aus, geht zu den von ihm eingegebenen

Daten die Verantwortung einer speichernden Stelle auf das Bundesamt für Verfassungsschutz über. Der ausgeschiedene Teilnehmer bleibt nach § 26 nachberichtspflichtig."

e) Absatz 4 wird aufgehoben.

12. § 22b wird wie folgt geändert:

a) Dem Absatz 1 wird folgender Satz angefügt:

„Der Militärische Abschirmdienst und der Bundesnachrichtendienst können zur Erfüllung ihrer Aufgaben an der Datei teilnehmen."

b) Absatz 6 wird wie folgt gefasst:

„(6) Für die Verarbeitung personenbezogener Daten sind anzuwenden durch

1. das Bundesamt für Verfassungsschutz § 10 Absatz 1 und 3 und §§ 11 und 12 Absatz 1 bis 3
2. den Militärischen Abschirmdienst § 6 Absatz 1 und 2 des MAD-Gesetzes in Verbindung mit § 10 Absatz 1 und 3 und § 12 Absatz 1 bis 3 sowie § 7 des MAD-Gesetzes,
3. den Bundesnachrichtendienst §§ 19 und 20 des BND-Gesetzes.

Die Speicherung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Soweit die Übermittlung von Daten einer besonderen Zweckbindung unterliegt, ist die Speicherung nur zulässig, wenn die gemeinsame Datenhaltung einem solchen Zweck dient und die Verarbeitung durch die anderen Teilnehmer entsprechend eingeschränkt ist. Für die Verantwortung des teilnehmenden Nachrichtendienstes gilt §6 Absatz 2 Satz 4 und 5 entsprechend."

13. § 24 wird aufgehoben.

14. In § 26a Absatz 2 werden dem Satz 1 die Wörter „auch unabhängig von Beschwerden nach Absatz 1 mindestens alle zwei Jahre unter Einschluss der Datenschutzvorschriften zum Einsatz nachrichtendienstlicher Mittel und der Weiterverarbeitung der

damit erhobenen Daten“ angefügt.

15. Nach § 27 wird folgender § 28 angefügt:

„

§ 28 – Einschränkung von Grundrechten

Die Grundrechte der Versammlungsfreiheit (Artikel 8 des Grundgesetzes), des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.“

Artikel 2 – Änderung des MAD-Gesetzes

Das MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

[Folgeänderungen – werden zum Ende der Abstimmung eingearbeitet]

Artikel 3 – Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 2 Absatz 1 Nummer 4 BNDG wird wie folgt gefasst:

„4. über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, wenn sie nur auf diese Weise zu erlangen sind.“

2. § 3 BNDG wird wie folgt gefasst:

„

§ 3 – Auskunftsverlangen gegenüber nicht-öffentlichen Stellen

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben nach § 1 Absatz 2 sowie zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände oder Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten

Auskunft über Bestandsdaten verlangen von

1. geschäftsmäßigen Dienstleistern im Personen- und Güterverkehr,
2. Verpflichteten nach § 2 Absatz1 des Geldwäschegesetzes, soweit sie nicht durch Rechtsverordnung nach § 2 Absatz 2 des Geldwäschegesetzes vom Anwendungsbereich des Geldwäschegesetzes ausgenommen sind.
3. geschäftsmäßigen Post-, Telekommunikations- und Telemediendienstleistern,

die in Deutschland eine Niederlassung haben oder Leistungen erbringen oder hieran mitwirken (Verpflichtete). Die Verpflichteten nach Satz 1 haben die Auskünfte, die der Bundesnachrichtendienst verlangt, zu erteilen. Eine Auskunft nach Satz1 Nummer 3 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). Dient eine Auskunft ausschließlich der Vorbereitung von Folgemaßnahmen, darf sie nur nach Maßgabe der dafür geltenden Regelungen verlangt werden. Der Bundesnachrichtendienst darf die zur Erfüllung seiner Aufgaben oder zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände oder Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlichen Bestandsdaten auch durch Ersuchen um Abruf an das Bundeszentralamt für Steuern nach § 93b Absatz 1 der Abgabenordnung und die Bundesnetzagentur nach § 112 Absatz 2 des Telekommunikationsgesetzes erheben.

(2) Der Bundesnachrichtendienst darf Auskünfte von Verpflichteten nach Absatz 1 Satz 1 über die Umstände und Inhalte der von ihnen erbrachten Leistungen nur verlangen, soweit dies erforderlich ist, um Bedrohungen von erheblicher Bedeutung aufzuklären. Auskünfte von Verpflichteten nach Absatz 1 Satz 1 Nummer 3 über Inhalte der von ihnen erbrachten Leistungen, die dem Brief-, Post- und Fernmeldegeheimnis unterliegen, darf der BND nur nach Maßgabe des Artikel 10-Gesetzes verlangen. Absatz 1 Satz 2 gilt entsprechend. Wenn Leistungsgegenstand der Transport oder die Verwahrung von Sachen ist, umfasst das Auskunftsverlangen auch die Gewährung vorübergehenden Besitzes zur Augenscheinnahme und Untersuchung der Sachen.

Die auf Grund des § 113b des Telekommunikationsgesetzes gespeicherten Daten dürfen nur nach Maßgabe des Artikel 10-Gesetzes erhoben werden. Hinsichtlich des Verfahrens, der Kontrolle sowie der Weiterverarbeitung der nach diesem Absatz erhobenen personenbezogenen Daten gelten §§ 4 und 9 bis 16 des Artikel 10-Gesetzes, soweit sie auf Maßnahmen nach § 3 des Artikel 10-Gesetzes anzuwenden sind, entsprechend mit folgenden Maßgaben: Abweichend von § 10 Absatz 1 des Artikel 10-Gesetzes ist anordnende Behörde das Bundeskanzleramt. Abweichend von § 10 Absatz 3 des Artikel 10-Gesetzes genügt für die Erhebung von Umständen von Telekommunikation deren räumlich und zeitlich hinreichende Bezeichnung, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre. Abweichend von § 10 Absatz 5 des Artikel 10-Gesetzes ist die Anordnung einer Auskunft über künftig anfallende Daten oder deren Verlängerung auf höchstens sechs Monate zu befristen.

(3) Die Betreiber einer Videoüberwachung nach § 4 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes sind verpflichtet, dem Bundesnachrichtendienst die Überwachung auszuleiten und Aufzeichnungen zu übermitteln, wenn dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung erforderlich ist. Die Maßnahme darf nur unter den Voraussetzungen des § 5 Absatz 4 gegen eine Person gerichtet werden.

(4) Die Verpflichteten und ihre mit der Durchführung betrauten oder hieran beteiligten Beschäftigten haben über das Auskunftsverlangen und die Mitwirkung gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren. § 2 Absatz 2 Satz 2 des Artikel 10-Gesetzes gilt entsprechend für die Mitwirkung an Maßnahmen nach § 5b. Das Auskunftsverlangen ist mit dem Hinweis zu verbinden, dass die Erhebung keinen Verdacht auf ein rechtswidriges Verhalten des Betroffenen begründe und dass der Verpflichtete an die Datenerhebung in Geschäftsverbindungen oder im Rechtsverkehr keine dem Betroffenen nachteiligen Folgen knüpfen darf.

(5) Eine unter den Voraussetzungen des § 8a Absatz 5 Bundesverfassungsschutzgesetz erlassene Rechtsverordnung kann die Vorgaben zur Mitwirkung der Verpflichteten nach dieser Norm ergänzen."

3. § 4 BNDG entfällt.

4. § 5 BNDG wird wie folgt gefasst:

„

§ 5 – Einsatz nachrichtendienstlicher Mittel

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben und zum Eigenschutz Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) einsetzen. Nachrichtendienstliche Mittel sind insbesondere

1. das Gewinnen und Führen von Personen, die nicht Mitarbeiter des Bundesnachrichtendienstes sind, zu Zwecken der heimlichen Informationsbeschaffung (Anbahnung und Einsatzführung),
2. Legenden, insbesondere fingierte biographische, berufliche oder gewerbliche Angaben, und Beschaffung, Erstellung und Verwendung von Tarnpapieren und Tarnkennzeichen,
3. Personen, die bei der Informationsbeschaffung oder bei Anbahnungshandlungen unterstützen.
4. Informationserhebung im Internet unter Ausnutzung schutzwürdigen Vertrauens Betroffener,
5. Observationen,
6. technische Mittel, insbesondere zur heimlichen
   a. optischen oder akustischen Überwachung von Personen, Gegenständen oder Vorgängen und
   b. Aufklärung technischer Signale, insbesondere zur Gewinnung von Erkenntnissen über gesendete Inhalte, nähere Umstände oder abstrahlende Geräte,

   und

7. vorübergehende heimliche Inbesitznahme von Sachen.

Der Bundesnachrichtendienst hat die nachrichtendienstlichen Mittel in einer Dienstvorschrift abschließend zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes, das das Parlamentarische

Kontrollgremium unterrichtet.

(2) Personenbezogene Daten darf der Bundesnachrichtendienst mit nachrichtendienstlichen Mitteln nur erheben bei tatsächlichen Anhaltspunkten dafür, dass

1. auf diese Weise Erkenntnisse über
   a. Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, oder
   b. die für die Aufgabenerfüllung notwendigen Nachrichtenzugänge einschließlich deren Vorbereitung und begleitenden Absicherung sowie aller sonstigen Unterstützungshandlungen

   gewonnen werden können, oder

2. dies erforderlich ist zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesnachrichtendienstes gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten

(3) Observationen von Personen, die durchgehend länger als 48 Stunden durchgeführt werden, dürfen nur eingesetzt werden

1. wenn dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung erforderlich ist oder
2. in unmittelbarem zeitlichen und örtlichen Zusammenhang mit dem Einsatz von Personen für den Bundesnachrichtendienst, wenn dies zur Sicherung des Einsatzes erforderlich ist.

(4) Nachrichtendienstliche Mittel dürfen sich nach Absatz 2 Nummer 1 Buchstabe a und Nummer 2 nur gegen Personen richten, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie über die für die Aufgabenerfüllung des BND notwendigen Nachrichtenzugänge verfügen,
2. von ihnen Erkenntnisse über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, gewonnen werden können und sie nur auf diese Weise zu erlangen sind oder wenn
3. von ihnen eine Gefährdung der Mitarbeiter, Einrichtungen,

Gegenstände und Quellen des Bundesnachrichtendienstes im Sinne des § 2 Absatz 1 Nummer 1 ausgeht.

Die Mittel dürfen auch angewandt werden, wenn andere Personen unvermeidlich betroffen werden.

(5) Setzen Mitarbeiter des Bundesnachrichtendienstes nachrichtendienstliche Mittel im Rahmen der gesetzlichen Vorgaben ein, so ist ihr Handeln nicht rechtswidrig.

(6) Beim Einsatz nachrichtendienstlicher Mittel nach Absatz1 gegen Personen sind folgende Angaben zu protokollieren:

1. die Person, gegen die sich die Maßnahme richtet,
2. Art, Umfang und Dauer der Maßnahme,
3. bei Maßnahmen nach § 5b
   - die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,
   - die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
   - die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und die Organisationseinheit, die die Maßnahme durchführt."

5. Nach § 5 werden folgende §§ 5a bis 5e angefügt:

"

§ 5a – Anbahnung und Einsatzführung

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben Personen, die nicht Mitarbeiter des Bundesnachrichtendienstes sind, zu Zwecken der heimlichen Informationsbeschaffung anbahnen und führen (§ 5 Absatz 1 Satz 1 Nummer 1 und 2).

(2) Angebahnt werden dürfen keine Personen, die

1. noch nicht das 16. Lebensjahr vollendet haben oder aus einem anderen Grund als Minderjährigkeit noch nicht voll geschäftsfähig sind,

2. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Mitarbeiter eines solchen Mitglieds oder einer Fraktion dieser Parlamente sind oder
3. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Die Behördenleiterin oder der Behördenleiter des Bundesnachrichtendienstes oder eine Vertreterin oder ein Vertreter kann Ausnahmen von Absatz 2 Satz1 Nummer 3 zulassen, wenn die Verurteilung nicht als Täter eines Totschlags (§§212, 213 des Strafgesetzbuches) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Gefahren nach § 3 Absatz 2 unerlässlich ist. Im Falle einer Ausnahme nach Satz 4 ist der Einsatz nach höchstens zwölf Monaten zu beenden, wenn er zur Erforschung der in Satz 4 genannten Gefahren nicht zureichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten.

(3) Angebahnte oder geführte Personen dürfen weder zur Gründung noch zur steuernden Einflussnahme auf Gruppierungen oder Netzwerke eingesetzt werden, deren Aufklärung zu den Aufgaben des Bundesnachrichtendienstes gehört. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbaren Vereinigungen, tätig werden, um Erkenntnisse über das Ausland zu gewinnen. Handlungen, die Personen im Sinne des Satzes 1 bei ihrer Tätigkeit nach Satz 2 vornehmen sind zulässig, wenn sie

1. nicht in Individualrechte eingreifen,
2. von den an den Gruppierungen oder Netzwerken Beteiligten derart erwartet werden, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich sind, und
3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen.

(4) Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass angebahnte oder geführte Personen im Inland rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht

haben, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen von Satz 1 entscheidet die Amtsleitung.

(5) Die Staatsanwaltschaft soll von der Verfolgung von Vergehen, die angebahnte und geführte Personen des Bundesnachrichtendienstes im Einsatz begangen haben, absehen oder eine bereits erhobene Klage in jeder Lage des Verfahrens zurücknehmen und das Verfahren einstellen, wenn

1. der Einsatz zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, erfolgte und
2. die Tat von den übrigen Beteiligten derart erwartet wurde, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich war.

Ein Absehen von der Verfolgung ist ausgeschlossen, wenn eine höhere Strafe als ein Jahr Freiheitsstrafe zu erwarten ist. Ein Absehen von der Verfolgung ist darüber hinaus stets ausgeschlossen, wenn zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt werden würde. Dritten kann ein anderer Einstellungsgrund angegeben werden, wenn dies zum Schutz des Betroffenen oder seines Einsatzes erforderlich ist.

(6) Die Eigenschaft als angebahnte und geführte Person ist geheim. Liegt in einem amtlichen Verfahren ausnahmsweise ein hohes Interesse an einer Aufklärung dieser Eigenschaft vor, kann der Bundesnachrichtendienst auf Anfrage der verfahrensführenden Stelle vor Anhörung des Zeugen eine Genehmigung zur Aussage erteilen, wenn

1. der Sachverhalt offenkundig von Bedeutung für das Verfahren ist,
2. aufgrund besonderer Umstände auszuschließen ist, dass dadurch
   a. das Wohl des Bundes oder
   b. überwiegende schutzwürdige Interessen des Betroffenen oder Dritter gefährdet würden.

Die Frage nach der Eigenschaft als angebahnte und geführte Person ist nur zulässig, wenn die Genehmigung nach Satz 2 erteilt

wurde.

§ 5b – Eingriff in informationstechnische Systeme

(1) Der Bundesnachrichtendienst darf ohne Wissen des Betroffenen unter Eingriff in ein informationstechnisches System von deutschen Staatsangehörigen, von inländischen juristischen Person oder von sich im Bundesgebiet aufhaltenden Personen mit technischen Mitteln die dort verarbeiteten Daten erheben, wenn die Maßnahme der Erkennung und Begegnung von

1. Gefahren nach § 5 Absatz 1 Satz 3 des Artikel 10-Gesetzes oder
2. Straftaten im Sinne § 3 Absatz 1 des Artikel 10-Gesetzes

dient.

(2) Für das Verfahren und die Kontrolle gelten §§ 9 bis 12, § 14 Absatz 1 und § 15 Absatz 5 bis 7 des Artikel 10-Gesetzes, soweit sie auf Maßnahmen nach § 3 des Artikel 10-Gesetzes anzuwenden sind, entsprechend und mit der Maßgabe, dass an die Stelle des Bundesministerium des Innern das Bundeskanzleramt tritt. In Antrag und Anordnung ist auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, anzugeben. Erfolgt der Vollzug nach § 15 Absatz 6 Satz 2 des Artikel 10-Gesetzes bereits vor Unterrichtung der G 10-Kommission gelten § 15 Absatz 6 Satz 7 und 8 des Artikel 10-Gesetzes entsprechend.

(3) Der Bundesnachrichtendienst darf die nach Absatz 1 erhobenen Daten zu den dort genannten Zwecken weiterverarbeiten, § 4 Absatz 1, Absatz 2 Satz 1 und 2 und Absatz 3 des Artikel 10-Gesetzes gelten entsprechend. Für die Übermittlung an inländische und ausländische öffentliche Stellen gelten § 4 Absatz 1, Absatz 2 Satz 1 und 2, Absatz 3, 4 und 6 des Artikel 10-Gesetzes entsprechend.

(4) An dem informationstechnischen System dürfen nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Sie sind bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig zu machen. Das eingesetzte Mittel ist nach dem Stand der Technik gegen

unbefugte Nutzung zu schützen.

(5) Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

§ 5c – Erhebung von Daten aus informationstechnischen Systemen von Ausländern im Ausland

(1) Der Bundesnachrichtendienst darf ohne Wissen des Betroffenen aus einem informationstechnischen System von Ausländern im Ausland vom Inland aus mit technischen Mitteln die dort verarbeiteten Daten erheben, wenn diese Daten erforderlich sind, um

1. frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland erkennen und diesen begegnen zu können,
2. die Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren oder
3. sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung über Vorgänge zu gewinnen, die in Bezug auf Art und Umfang durch das Bundeskanzleramt im Einvernehmen mit dem Auswärtigen Amt, dem Bundesministerium des Innern, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung bestimmt werden.

(2) Erhebungen nach Absatz 1 aus einem informationstechnischen System von Unionsbürgerinnen und Unionsbürgern sind nur zulässig, wenn dies erforderlich ist, um

1. Gefahren nach § 5 Absatz 1 Satz 3 des Artikel 10-Gesetzes oder Straftaten im Sinne des § 3 Absatz 1 des Artikel 10-Gesetzes zu erkennen und zu begegnen oder
2. Informationen im Sinne des Absatzes 1 Satz 1 Nummer 1 bis 3 zu gewinnen, soweit ausschließlich Daten über Vorgänge in Drittstaaten gesammelt werden sollen, die von besonderer Relevanz für die Sicherheit der Bundesrepublik Deutschland sind.

(3) Erhebungen aus informationstechnischen Systemen von Einrichtungen der Europäischen Union oder von öffentlichen Stellen ihrer Mitgliedstaaten sind unzulässig.

(4) Die technische und organisatorische Umsetzung von Maßnahmen nach Absatz 1 sowie die Kontrollzuständigkeiten innerhalb des Bundesnachrichtendienstes sind in einer Dienstvorschrift festzulegen, die auch ein Anordnungsverfahren regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes. Das Bundeskanzleramt unterrichtet das Parlamentarische Kontrollgremium.

§ 5d – Technische Datenerhebung aus Wohnungen

(1) Der Bundesnachrichtendienst darf ohne Wissen des Betroffenen unter Einsatz technischer Mittel personenbezogene Daten aus einer Wohnung entsprechend § 5b Absatz 1 erheben, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Auf die erhobenen Daten ist § 5b Absatz 3 entsprechend anzuwenden.

(2) Die Maßnahme darf sich nur gegen Personen richten, zu denen hinreichende Anhaltspunkte für den Verdacht bestehen, dass sie eine Straftat nach § 3 Absatz 1 Artikel10-Gesetz planen, begehen oder begangen haben oder an einer in § 5 Absatz 1 des Artikel 10-Gesetzes bezeichneten Gefahr beteiligt sind. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn hinreichende Anhaltspunkte bestehen, dass sich eine in Satz 1 genannte Person in ihr aufhält und der Zweck der Maßnahme nicht unter Beschränkung auf deren Wohnung zu erreichen ist.

(3) Für das Verfahren und die Kontrolle gelten §§ 9, 10 Absatz 1 bis 3 und 5 bis 6, § 12, § 14 Absatz 1 und § 15 Absatz 5 Sätze 2 bis 4 des Artikel 10-Gesetzes entsprechend mit folgenden Maßgaben:

1. In Antrag und Anordnung sind auch die zu überwachende Wohnung oder die zu überwachenden Wohnräume anzugeben.

2. Die Kontrollbefugnis der G10-Kommission erstreckt sich auf die Anordnungskonformität der Erhebung und die gesamte Weiterverarbeitung der erlangten personenbezogenen Daten.
3. An die Stelle des Bundesministeriums des Innern tritt das Bundeskanzleramt.

Die Maßnahme darf erst vollzogen werden, wenn das Bundesverwaltungsgericht die Zulässigkeit festgestellt hat. Satz 2 gilt nicht bei Gefahr im Verzug. Wird die Anordnung bei Gefahr im Verzug bereits vor der Zulässigkeitsfeststellung vollzogen, tritt sie außer Kraft, wenn die Feststellung nach Satz 2 nicht binnen drei Werktagen erfolgt. Tritt die Anordnung nach Satz 4 außer Kraft, ist die Verarbeitung erhobener personenbezogener Daten einzuschränken. Bis zur Feststellung nach Satz 2 ist die Weiterverarbeitung unzulässig. Stellt das Bundesverwaltungsgericht die Unzulässigkeit der Maßnahme fest, sind die Daten zu löschen. § 5e Absatz 2 Sätze 4 bis 7 gelten entsprechend.

(4) Beteiligte des Feststellungsverfahrens nach Absatz 3 sind der Bundesnachrichtendienst und das Bundeskanzleramt. Das Bundeskanzleramt legt dem Bundesverwaltungsgericht mit dem Feststellungsantrag die Anordnung vor. Macht das Bundeskanzleramt geltend, dass besondere Gründe der Geheimhaltung oder des Geheimschutzes der Vorlage mittels Übergabe oder Übermittlung an das Gericht entgegenstehen, kann die Vorlage nach Satz 1 dadurch bewirkt werden, dass die Dokumente dem Gericht in vom Bundeskanzleramt bestimmten Räumlichkeiten zur Verfügung gestellt werden.. Das Gericht kann den Sachverhalt durch Anhörung der Beteiligten erforschen. Im Einverständnis mit dem Bundeskanzleramt kann der Vorsitzende oder Berichterstatter anstelle des Senats entscheiden. Gegen die Entscheidung nach Satz 5 kann das Bundeskanzleramt innerhalb von zwei Wochen nach Bekanntgabe eine Entscheidung des Senats beantragen. Das Verfahren unterliegt den Vorschriften des materiellen Geheimschutzes. Die Mitglieder des Gerichts sind zur Geheimhaltung verpflichtet. Für das nichtrichterliche Personal gelten die Regelungen des personellen Geheimschutzes.

(5) Im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz von Personen für den Bundesnachrichtendienst in einer Wohnung darf er in oder aus dieser Wohnung Daten mit technischen Mitteln

erheben, wenn dies zur Abwehr von Gefahren für deren Leib, Leben oder Freiheit unerlässlich ist. Die erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eigensicherung nach Satz 1, sonstiger Gefahrenabwehr oder der Strafverfolgung verarbeitet werden. Die Verarbeitung zur sonstigen Gefahrenabwehr oder der Strafverfolgung setzt die Feststellung der Rechtmäßigkeit der Maßnahme durch das Bundesverwaltungsgericht voraus; bei Gefahr im Verzug ist die gerichtliche Entscheidung unverzüglich nachzuholen.

(6) Der Bundesnachrichtendienst darf Wohnungen auch betreten, um Maßnahmen nach den Absätzen 1 und 5, nach § 11 Absatz 1a des Artikel 10-Gesetz oder § 5b vorzubereiten. Dies muss in der Anordnung oder einer Ergänzungsanordnung enthalten sein. Heimlich betreten werden darf nur die Wohnung dessen, gegen den sich die Überwachungsanordnung richtet.

§ 5e – Schranken nachrichtendienstlicher Mittel

(1) Beim Einsatz nachrichtendienstlicher Mittel sind Schutznormen der Rechtspflege und der parlamentarischen Kontrolle zu beachten. Der Einsatz nachrichtendienstlicher Mittel ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger oder ein rechtlich geschütztes Interesse weniger beeinträchtigende Weise möglich ist. Eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch Ersuchen nach § 23 Absatz 3 gewonnen werden kann.

(2) Eine Maßnahme ist unzulässig, soweit

1. tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Informationen aus dem Kernbereich privater Lebensgestaltung gewonnen werden würden, oder
2. Informationen
   a. bei einer in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder 4 der Strafprozessordnung genannten Person, im Falle der Nummer 3 beschränkt auf
      - Rechtsanwälte oder
      - Kammerrechtsbeistände,

   b. oder deren Berufshelfer (§ 53a der Strafprozessordnung)

nicht zur Aufklärung von Beteiligungen dieser Personen an Bedrohungen erhoben werden und die Maßnahme voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte.

Werden solche Informationen bei einer Maßnahme gewonnen, dürfen sie nicht genutzt werden. Aufzeichnungen sind zu löschen. Die Tatsache der Erlangung und Löschung dieser Informationen ist zu protokollieren. Die Protokollierung darf nicht die erhobenen Informationen umfassen und keine Daten enthalten, die schutzwürdige Details des Einsatzes des nachrichtendienstlichen Mittels offenbaren würden. Die Protokollierung darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist

1. in den Fällen der §§ 3 Absatz 2, 5b und 5d sechs Monate nach der Mitteilung an den Betroffenen oder dem abschließenden Absehen von der Mitteilung,
2. im Übrigen nach Mitteilung an den Bundesbeauftragten oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am Ende des übernächsten Kalenderjahres, das der Protokollierung folgt,

zu löschen.

(3) Ergeben sich bei der Maßnahme während der Durchführung tatsächliche Anhaltspunkte dafür, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst werden, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung eingesetzter Personen möglich ist und solange die Anhaltspunkte bestehen. Bei dem Einsatz technischer Mittel (§ 5 Absatz 1 Satz2 Nummer7) dürfen automatische Aufzeichnungen fortgesetzt werden, wenn Zweifel am Vorliegen solcher Inhalte bestehen.

(4) Auf Aufzeichnungen nach

1. Absatz 3 Satz 2 und

2. §§ 5b Absatz 1, 5d Absatz 1, soweit bei deren Auswertung tatsächliche Anhaltspunkte dafür bekannt werden, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst wurden, ohne dass bereits der Bundesnachrichtendienst dabei solche Inhalte feststellt,

ist § 3a Absatz 1 Satz 4 bis 6 und Absatz 2 des Artikel 10-Gesetzes entsprechend anzuwenden. Ist die weitere Verarbeitung danach unzulässig, gilt Absatz 2 Satz 2 bis 6.

(5) Die Beeinträchtigung rechtlich geschützter Interessen durch Anwendung eines nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Näheres ist in der Dienstvorschrift nach §5 Absatz 1 Satz 3 zu regeln. Erfolgen Maßnahmen bei einer in § 53 Absatz 1 Satz1 Nummer 3 bis 3b oder Nummer 5 der Strafprozessordnung genannten Person oder deren Berufshelfer (§ 53a der Strafprozessordnung) nicht zur Aufklärung von Beteiligungen dieser Personen an Bedrohungen, sind das öffentliche Interesse an den von dieser Person wahrgenommenen Aufgaben und das Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Für Rechtsanwälte oder Kammerrechtsbeistände bleiben die Absätze 2 bis 4 unberührt.

(6) Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich ergibt, dass er nicht oder nicht auf diese Weise erreicht werden kann."

6. Nach § 20 Absatz 1 Satz 1 wird folgender Satz 2 angefügt:

„§ 12 Abs. 3 Satz 2 Bundesverfassungsschutzgesetz findet keine Anwendung."

7. Nach § 23 wird folgender § 23a eingefügt:

"

§ 23a – Ausschreibungen

Soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, können auf Ersuchen des Bundesnachrichtendienstes

1. Personen, die
   a. über die für die Aufgabenerfüllung des Bundesnachrichtendienstes notwendigen Nachrichtenzugänge verfügen
   b. von denen Erkenntnisse über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die

Bundesrepublik Deutschland sind, gewonnen werden können und sie nur auf diese Weise zu erlangen sind, oder

c. von denen eine Gefährdung der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesnachrichtendienstes im Sinne des § 2 Absatz 1 Nummer 1 ausgeht,

2. Personen und Sachen, die im Zusammenhang mit Personen nach Nummer 1 stehen, wenn dadurch Erkenntnisse gewonnen werden können, die nicht nach Nummer 1 zu gewinnen sind,

zur polizeilichen Beobachtung ausgeschrieben werden. Dies gilt nach Maßgabe der unionsrechtlichen Bestimmungen auch für Datenverarbeitungssysteme der Europäischen Union. Ausschreibungen des Bundesnachrichtendienstes ordnet die Amtsleitung, eine dazu ermächtigte Abteilungsleitung oder ein dazu besonders beauftragter Bediensteter, der die Befähigung zum Richteramt hat, an. Die Ausschreibung ist auf höchstens ein Jahr zu befristen und kann wiederholt angeordnet werden. Liegen die Voraussetzungen für die Ausschreibung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen."

8. Nach § 24 wird folgender § 24a BNDG eingefügt:

"

§ 24a – Datenverarbeitung auf Ersuchen inländischer öffentlicher Stellen

(1) Der Bundesnachrichtendienst darf auf Ersuchen einer inländischen Behörde, welche die Befugnis zur Fernmeldeaufklärung hat, zu deren entsprechender Aufgabenerfüllung Informationen einschließlich personenbezogener Daten mit technischen Mitteln der Fernmeldeaufklärung verarbeiten. Hiervon erfasst wird insbesondere die Erhebung der Daten und deren automatisierte Übermittlung an die ersuchende Behörde, einschließlich der Daten, die unter den Voraussetzungen des § 12 Absatz 1 BNDG

erhoben wurden. § 24 findet insoweit keine Anwendung.

(2) Die Zulässigkeit der Datenverarbeitung nach Absatz 1 richtet sich nach dem für die ersuchende Behörde geltenden Recht, die Durchführung durch den Bundesnachrichtendienst nach § 6 Absatz 1 Satz 2, § 12 Absatz 2. Die ersuchende Behörde trägt gegenüber dem Bundesnachrichtendienst die Verantwortung für die Rechtmäßigkeit der durchzuführenden Maßnahme. Der Bundesnachrichtendienst ist für die Durchführung verantwortlich. Die Einzelheiten sind in einer Verwaltungsvereinbarung zu regeln.

(3) Der Bundesnachrichtendienst darf die nach Absatz 1 erhobenen Daten gemäß den für ihn geltenden Vorschriften für eigene Zwecke weiterverarbeiten, soweit ihre Erhebung zu diesen Zwecken auch nach den Vorschriften des Abschnitts 2 zulässig gewesen wäre.

(4) Die Absätze 1 bis 2 gelten entsprechend für Datenerhebungen aus informationstechnischen Systemen mit technischen Mitteln ohne Wissen des Betroffenen unter der Maßgabe, dass § 6 und 12 keine Anwendung finden. Die ersuchende Behörde muss die Befugnis zu Datenerhebungen aus informationstechnischen Systemen haben. Der Bundesnachrichtendienst darf die nach Satz 1 erhobenen Daten gemäß den für ihn geltenden Vorschriften für eigene Zwecke weiterverarbeiten, soweit ihre Erhebung zu diesen Zwecken auch nach den Vorschriften des Abschnitts 1 zulässig gewesen wäre.“

9. § 25 BNDG wird wie folgt geändert:

a) In der Überschrift wird das Wort „Projektbezogene“ gestrichen und das Wort „gemeinsame“ durch das Wort „Gemeinsame“ ersetzt.“

b) Absatz 1 wird durch folgende Absätze ersetzt:

(1) Der Bundesnachrichtendienst darf mit dem Bundesamt für Verfassungsschutz und dem Bundesamt für Sicherheit in der Informationstechnik eine gemeinsame Datei zum Erkennen und Begegnen von Gefahren im Sinne § 5 Absatz 1 des Artikel 10-Gesetzes einrichten, an der auch Landesbehörden für Verfassungsschutz und das Bundesamt für den Militärischen

Abschirmdienst teilnehmen können.

(1a) Polizeibehörden des Bundes und der Länder oder das Zollkriminalamt dürfen an einer gemeinsamen Datei teilnehmen, wenn die Teilnahme

1. zur projektbezogenen Zusammenarbeit bei der Auswertung von Informationen
   a. zu den in § 5 Absatz 1 Satz 3 Nummer 1 bis 3 Artikel 10-Gesetz genannten Gefahrenbereichen erfolgt oder
   b. zu den in § 5 Absatz 1 Satz 3 Nummer 4 bis 8 Artikel 10-Gesetz genannten Gefahrenbereichen erfolgt, soweit deren Aufklärung Bezüge zum internationalen Terrorismus aufweist und

2. auf höchstens zwei Jahre befristet ist. Die Frist kann um zwei Jahre und danach um ein weiteres Jahr, bei Aufklärung von Strukturen in den Fällen der §§ 129 bis 129b des Strafgesetzbuchs um jeweils ein weiteres Jahr verlängert werden, wenn das Ziel der projektbezogenen Zusammenarbeit bei Projektende noch nicht erreicht worden ist und die Datei weiterhin für die Erreichung des Ziels erforderlich ist."

c) Dem Absatz 2 werden folgende Sätze angefügt:

„Bei der Weiterverarbeitung personenbezogener Daten finden für die beteiligten Behörden die jeweils für sie geltenden Vorschriften über die Verarbeitung personenbezogener Daten Anwendung. Zweckbindungen für eine Weiterverarbeitung, auch durch den Empfänger nach Übermittlung, bleiben unberührt."

d) Absatz 3 wird wie folgt geändert:

aa) In Absatz 3 Satz 1 wird das Wort „projektbezogenen" gestrichen.

bb) Folgende Sätze werden angefügt:

„Scheidet ein Teilnehmer aus, geht zu den von ihm eingegebenen Daten die Verantwortung einer speichernden Stelle auf den Bundesnachrichtendienst über. Der ausgeschiedene Teilnehmer bleibt nach § 31 i.V.m. § 26 des Bundesverfassungsschutzgesetzes nachberichtspflichtig."

e) Absatz 4 wird aufgehoben.

f) Absatz 5 wird Absatz 4.

g) Absatz 6 wird Absatz 5 und in Satz 1 Nummer 5 wird das Wort „projektbezogen“ gestrichen.

10. In § 26 wird nach Absatz 1 folgender Satz angefügt:

„Der Militärische Abschirmdienst und das Bundesamt für Verfassungsschutz können zur Erfüllung ihrer Aufgaben an der Datei teilnehmen.“

11. § 36 wird wie folgt gefasst:

„

§ 36 – Einschränkung von Grundrechten

Die Grundrechte der Versammlungsfreiheit (Artikel 8 des Grundgesetzes), des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) und der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) werden nach Maßgabe dieses Gesetzes eingeschränkt.“

Artikel 4 – Änderung des Sicherheitsüberprüfungsgesetzes

Das Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

a) In Absatz 1 wird Satz 3 aufgehoben.

b) In Absatz 2 wird Satz 4 aufgehoben.

2. In § 12 Absatz 4 wird in Satz 1 nach den Wörtern „Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der“ das Wort „ehemaligen“ eingefügt.

3. § 13 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 8 wird das Wort „oder“ durch das Wort „und“ ersetzt.

bb) In Nummer 18 wird das Wort „oder“ durch das Wort „und“ ersetzt.

cc) Satz 1 werden folgende Sätze 2 und 3 angefügt:

„Der Sicherheitserklärung sind zwei aktuelle Lichtbilder der betroffenen Person mit der Angabe des Jahres der Aufnahme beizufügen. Das Lichtbild kann in elektronischer Form verlangt werden.“

b) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 Nummer 6 wird das Wort „oder“ durch das Wort „und“ ersetzt.

bb) In Satz 1 Nummer 7 wird das Wort „oder“ durch das Wort „und“ ersetzt.

cc) Satz 2 wird aufgehoben.

4. § 20 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Die Angabe „§ 13 Abs. 1 Nr. 1 bis 6“ wird durch die Angabe „§ 13 Absatz 1 Nummer 1 bis 6 und Absatz 4 Satz 1 Nummer 1“ ersetzt.

bb) Nach dem Wort „Daten“ werden die Wörter „der betroffenen Person und der mitbetroffenen Person“ eingefügt.

b) In Absatz 2 Satz 1 Nummer 1 wird die Angabe „§ 13 Abs. 1 Nr. 1 bis 6“ durch die Angabe „§ 13 Absatz 1 Nummer 1 bis 6 und Absatz 4 Satz 1 Nummer 1“ ersetzt.

c) In Absatz 2 Satz 2 wird die Angabe „Nummer 1“ durch die Wörter „Satz 1 Nummer 1“ ersetzt.

Artikel 5 – Änderung des Artikel 10-Gesetzes

Das Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. § 2 Absatz 2 Satz 3 wird wie folgt gefasst:

„Der Behördenleiter der berechtigten Stelle oder dessen Stellvertreter kann die nach Absatz 1 Satz 1 oder 3 Verpflichteten schriftlich auffordern, die Beschränkungsmaßnahme bereits vor Abschluss der Sicherheitsüberprüfung durchzuführen."

2. § 3a wird wie folgt geändert:

a) Sätze 1 bis 12 werden Absatz 1.

b) Absatz 1 Satz 12 wird wie folgt gefasst:

„Sie ist sechs Monate nach der Mitteilung nach § 12 Absatz 1 Satz 1 oder der Feststellung nach § 12 Absatz 1 Satz 5 zu löschen."

c) Folgender Absatz 2 wird angefügt:

„(2) Bei Gefahr im Verzug können Aufzeichnungen nach Absatz 1 Satz 3 unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, gesichtet werden. Der Bedienstete entscheidet im Benehmen mit dem oder der Beauftragten für den Datenschutz (§ 5 des Bundesdatenschutzgesetzes) oder einem von diesem beauftragten Beschäftigten, für den § 6 Absatz 3 des Bundesdatenschutzgesetzes insoweit entsprechend gilt, über eine vorläufige Nutzung."

3. § 3b wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „einer in § 53 Absatz 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozessordnung genannten Person" durch die Angabe „einer in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder 4 der Strafprozessordnung genannten Person, im Falle dessen Nummer 3 beschränkt auf Rechtsanwälte oder Kammerrechtsbeistände," ersetzt.

b) In Absatz 1 Satz 5 wird die Angabe „§ 53 Absatz 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozessordnung" durch die Angabe „Satz 1" ersetzt.

c) In Absatz 2 Satz 1 wird nach der Angabe „einer in § 53 Absatz 1

Satz 1 Nr. 3 bis 3b oder 5 der Strafprozessordnung genannten Person“ ein Komma und der Halbsatz “ im Falle dessen Nummer 3 mit Ausnahme von Rechtsanwälten oder Kammerrechtsbeiständen,“ ersetzt.

4. § 4 wird wie folgt geändert:

a) In Absatz 1 Satz 1 werden die Wörter „und sodann in Abständen von höchstens sechs Monaten“ gestrichen.

b) In Absatz 4 Satz 1 wird folgende Nummer 4 eingefügt

„4. zur Sicherheitsüberprüfung von Personen nach § 3 Absatz 2 Satz 1 Nummer 1 des Bundesverfassungsschutzgesetzes, § 1 Absatz 3 Nummer 1 des MAD-Gesetzes, § 2 Absatz 1 Nummer 2 des BND-Gesetzes oder sonstigen gesetzlich bestimmten Personenüberprüfungen, wenn sie auch dem vorbeugenden Schutz vor drohenden Gefahren nach § 1 Absatz 1 Nummer 1 dienen,“

c) In Absatz 6 Satz 2 werden die Wörter „und sodann in Abständen von höchstens sechs Monaten“ gestrichen.

5. § 8 Absatz 3 Satz 4 wird wie folgt gefasst:

„Ist die Überwachungsmaßnahme erforderlich, um einer im Einzelfall bestehenden Gefahr für Leib oder Leben einer Person zu begegnen, dürfen die Suchbegriffe auch Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung der Rufnummer oder einer anderen Kennung des Telekommunikationsanschlusses dieser Person im Ausland oder einer anderen Person mit deren Zustimmung führen.“

6. In § 9 Absatz 3 Satz 2 wird ein Komma und folgender Halbsatz angefügt:

„im Falle der Durchführung nach § 11 Absatz 1a auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll“

7. In § 11 werden nach Absatz 1 folgende Absätze eingefügt:

„(1a) Inhalte und Umstände von Telekommunikation, die nach der Anordnung übertragen worden ist oder wird, dürfen auch aus

einem von dem Betroffenen genutzten informationstechnischen System erhoben werden, wenn der Eingriff notwendig ist, um die Informationen insbesondere auch in unverschlüsselter Form zu gewinnen. An dem informationstechnischen System dürfen nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Sie sind bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig zu machen. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Bei jedem Einsatz sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

(1b) Werden nach der Anordnung weitere Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung als Verdächtiger oder Nachrichtenmittler (§ 3 Absatz 2 Satz 2, Fälle 1 und 2) richtet, durch eindeutige Auskunft nach § 112 des Telekommunikationsgesetzes, elektronische Aufklärung nach § 9 Absatz 1 Satz 2 Nummer 7 des Bundesverfassungsschutzgesetzes, technische Mittel nach § 5 Absatz 1 Satz 2 Nummer 6 des Bundesnachrichtendienstgesetzes oder durch Informationsübermittlungen ausländischer öffentlicher Stellen bekannt, darf die Durchführung auch auf diese Kennungen erstreckt werden. Das zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über durchgeführte Erstreckungen."

8. § 12 Absatz 1 Satz 2 wird wie folgt gefasst:

„Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist, oder solange dies zum Schutz des Betroffenen vor Gefahren für Leib, Leben oder Freiheit erforderlich

ist.“

9. In § 14 Absatz 2 Satz 3 wird das Wort „Tagen“ durch das Wort „Werktagen“ ersetzt.

10. § 15 wird wie folgt geändert:

a) Absatz 1 Satz 4 wird wie folgt gefasst:

„Sie nehmen ein öffentliches Ehrenamt wahr und werden von dem Parlamentarischen Kontrollgremium nach Anhörung der Bundesregierung für die Dauer einer Wahlperiode des Deutschen Bundestages mit der Maßgabe bestellt, dass ihre Amtszeit erst einen Monat nach Neubestimmung der Mitglieder der Kommission endet.“

b) In Absatz 6 Satz 7 wird das Wort „Tagen“ durch das Wort „Werktagen“ ersetzt.

Artikel 6 – Änderung des Vereinsgesetzes

Dem § 4 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), das zuletzt durch [...] geändert worden ist, wird folgender Absatz 6 angefügt:

„(6) Liegen tatsächliche Anhaltspunkte dafür vor, dass ein Verein

1. sich gegen die verfassungsmäßige Ordnung oder den Gedanken der Völkerverständigung richtet oder
2. als Ausländerverein oder als ausländischer Verein in Deutschland Zwecke oder Tätigkeiten nach § 14 Absatz 2, auch in Verbindung mit § 15 Absatz 1, verfolgt,

können die Landesbehörden für Verfassungsschutz zur Aufklärung des Verdachts im Rahmen ihrer Zuständigkeit nach § 3 Absatz 1 Nummer 1 des Bundesverfassungsschutzgesetzes die Befugnisse des Bundesverfassungsschutzgesetzes anwenden. Weitergehende landesgesetzliche Befugnisse bleiben unberührt.“

Artikel 7 – Änderung des Bundeskriminalamtgesetzes

§ 76 Absatz 4 des Bundeskriminalamtgesetzes vom 1. Juni 2017

(BGBl. I S. 1354), das zuletzt durch … geändert worden ist, wird wie folgt gefasst:

„(4) Im Falle einer Ausschreibung nach § 17 Absatz 2 des Bundesverfassungsschutzgesetzes erfolgt keine Benachrichtigung durch das Bundeskriminalamt. Das Bundesamt für Verfassungsschutz teilt der betroffenen Person im Rahmen einer Auskunft nach Maßgabe des § 15 des Bundesverfassungsschutzgesetzes auch die Ausschreibung mit."

Artikel 8 – Änderung der Verwaltungsgerichtsordnung

Die Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), die zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In § 48 wird folgender Absatz 3 angefügt:

„(3) Das Oberverwaltungsgericht entscheidet im ersten Rechtszug ferner über Klagen, denen Vorgänge im Geschäftsbereich der Verfassungsschutzbehörden des Bundes und der Länder nach § 3 Absatz 1 des Bundesverfassungsschutzgesetz oder des Militärischen Abschirmdienstes nach § 1 Absatz1 des MAD-Gesetzes zugrunde liegen."

2. In § 50 wird nach Nummer 4 folgende Nummer 4a eingefügt:

„4a. über Feststellungsanträge nach § 9e Absatz 3 Satz 2 des Bundesverfassungsschutzgesetzes,"

Artikel 9 – Änderung der Abgabenordnung

§ 93 der Abgabenordnung in der Fassung der Bekanntmachung vom 1.Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. Absatz 8 Satz 1 wird wie folgt geändert:

a) Die Wörter „über die in § 93b Absatz 1 bezeichneten Daten" werden durch die Wörter „durch automatisierten Abruf nach § 93b" ersetzt.

b) Nummer 3 wird wie folgt gefasst:

„3. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, soweit dies für ihre Aufgabenerfüllung erforderlich ist."

2. In Absatz 9 Satz 1 wird nach der Angabe „Absatz 8" die Angabe „Satz 1 Nummer 1 und Sätze 2 und 3" eingefügt.

Artikel 10 – Änderung des Telekommunikationsgesetzes

§ 113c Absatz 1 Nummer 2 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch ... geändert worden ist, wird wie folgt gefasst:

„2. an eine Gefahrenabwehrbehörde, eine Verfassungsschutzbehörde, den Militärischen Abschirmdienst und den Bundesnachrichtendienst übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zum Schutz vor einer gemeinen Gefahr oder einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes erlaubt, verlangt;"

Artikel 11 – Änderung des Straßenverkehrsgesetzes

Das Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. § 30 Absatz 1 wird wie folgt gefasst:

„(1) Die Eintragungen im Fahreignungsregister dürfen übermittelt werden an

1. die Stellen, die zuständig sind für
   a. die Verfolgung von Straftaten, zur Vollstreckung oder zum Vollzug von Strafen,
   b. die Verfolgung von Ordnungswidrigkeiten und die Vollstreckung von Bußgeldbescheiden und ihren Nebenfolgen nach diesem Gesetz und dem Gesetz über das

Fahrpersonal im Straßenverkehr oder

c. Verwaltungsmaßnahmen auf Grund dieses Gesetzes oder der auf ihm beruhenden Rechtsvorschriften,

2. die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst sowie den Bundesnachrichtendienst,

soweit dies für die Erfüllung der diesen Stellen obliegenden Aufgaben zu den in § 28 Absatz 2 genannten Zwecken jeweils erforderlich ist."

2. Dem § 30a Absatz 3 wird folgender Satz angefügt:

„Die Abrufe durch die in § 30 Absatz 1 Nummer 2 genannten Behörden werden nur von der abrufenden Behörde protokolliert."

3. § 52 Absatz 1 wird wie folgt gefasst:

„(1) Die in den Fahrerlaubnisregistern gespeicherten Daten dürfen übermittelt werden an

1. die Stellen, die zuständig sind für
   a. die Verfolgung von Straftaten, zur Vollstreckung oder zum Vollzug von Strafen,
   b. die Verfolgung von Ordnungswidrigkeiten und die Vollstreckung von Bußgeldbescheiden und ihren Nebenfolgen nach diesem Gesetz oder
   c. Verwaltungsmaßnahmen auf Grund dieses Gesetzes oder der auf ihm beruhenden Rechtsvorschriften, soweit es um Fahrerlaubnisse, Führerscheine oder sonstige Berechtigungen, ein Fahrzeug zu führen, geht,

2. die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst sowie den Bundesnachrichtendienst,

soweit dies für die Erfüllung der diesen Stellen obliegenden Aufgaben zu den in § 49 genannten Zwecken jeweils erforderlich ist."

4. In § 53 Absatz 3 wird folgender Satz angefügt:

„Die Abrufe der in § 52 Absatz 1 Nummer 2 genannten Behörden werden nur von der abrufenden Behörde protokolliert."

Artikel 12 – Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

(2) Artikel 10 und 13 Absatz 2 des Terrorismusbekämpfungsergänzungsgesetzes vom 5. Januar 2007 (BGBl. I S. 2), das zuletzt durch ... geändert worden ist, und § 13 der Sicherheitsüberprüfungsfeststellungsverordnung in der Fassung der Bekanntmachung vom 12. September 2007 (BGBl. I S. 2294), die zuletzt durch ... geändert worden ist, werden aufgehoben.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Verfassungsschutz ist in hohem Maße auf Zusammenarbeit angelegt. Schutzgut sind vornehmlich gesamtstaatliche Rechtsgüter, Aufklärungsobjekte dabei vornehmlich überregionale Bedrohungen. Nach der bundesstaatlichen Ordnung ist diese Aufgabe Bund und Ländern gemeinsam anvertraut, die mithin arbeitsteilig gemeinsame Ergebnisse erzielen müssen. Hieraus erwächst im Bereich der Gesetzgebung ein spezifischer Bedarf für harmonisierte, gemeinsame Grundlagen, um ein einheitliches Schutzniveau der zusammenwirkenden Teilbeiträge zu ermöglichen. Ebenso ist auf Ebene untergesetzlicher Regelungen in weiten Bereichen Standardisierung geboten, was effektive Verfahren zum Erlass bindender Vorschriften erfordert.

Die Innenministerkonferenz (IMK) hat in ihrer 206. Sitzung am 14. Juni 2017 die Notwendigkeit eines harmonisierten Rechtsrahmens mit wirksamen Befugnissen festgestellt (TOP 34) und dazu in ihrer 207. Sitzung am 8. Dezember 2017 Musterregelungen beschlossen (TOP 29). In ihrem Koalitionsvertrag für die 19. Wahlperiode haben die Koalitionsparteien vereinbart, das Bundesverfassungsschutzgesetz auf der Grundlage eines einheitlichen Rechtsrahmens der IMK zu novellieren.

Diese Harmonisierung schließt auch die bislang im Bundesverfassungsschutzgesetz befristeten, ursprünglich mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361, 3142) eingeführten, zuletzt mit dem Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen vom 3. Dezember 2015 (BGBl. I S. 2161) fortgeschriebenen Regelungen der bisherigen §§ 8a, 8b BVerfSchG ein. Die Harmonisierung führt insoweit zugleich zu einer Konsolidierung und Verstetigung des Normbestandes. Inhaltlich deckt sich dies mit den Ergebnissen der nunmehr vierten Evaluierung, die wiederum die grundsätzliche Angemessenheit der Regelungen bestätigt, gleichzeitig aber gewisse Wertungsbrüche aufgezeigt hat, die mit der neuen Regelung beseitigt werden.

Im Bereich der Verwaltung besitzt der Bund neben seiner originären Verfassungsschutzaufgabe die besondere Zentralstellenkompetenz (Artikel 87 Absatz1 Satz 2 GG), die spezifisch auch koordinativen Gehalt hat. Die Innenministerkonferenz hatte bereits in ihrer 196. Sitzung am 7. Dezember 2012 zur Neuausrichtung des Verfassungsschutzes die Stärkung der Zentralstellenfunktion des Bundesamtes für Verfassungsschutz (BfV) beschlossen. Dessen Koordinierungskompetenz wurde infolge dessen mit dem Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) mit dem neuen § 5 Absatz 3 BVerfSchG erstmals gesetzlich geregelt. Die seitherige Praxis hat bestätigt, dass eine konsensmoderierende Koordinierung weitgehend zusammenarbeitsadäquat ist, gleichzeitig aber auch aufgezeigt, dass für Ausnahmesachverhalte, in denen das Konsensziel nicht erreicht wird, die Koordinierungsverantwortung noch mit effektiven Instrumenten und Mechanismen unterlegt werden muss. Der Zielsetzung dieses Gesetzes folgend, erhält das BfV eine gestärkte Standardisierungskompetenz, wobei allerdings Länderbelange verfahrensmäßig gesichert bleiben.

Zudem entkoppelt das vorliegende Gesetz die beiden nachrichtendienstlichen Fachgesetze für das BfV und den Bundesnachrichtendienst (BND). Die bisherige Regelungstechnik sah das Bundesverfassungsschutzgesetz als Stammgesetz vor, das alle wesentlichen nachrichtendienstlichen Eingriffsbefugnisse normierte. Das BND-Gesetz hing insoweit quasi-akzessorisch an

diesem Stammgesetz, so dass für Eingriffsbefugnisse wie z.B. diejenigen zum Einsatz nachrichtendienstlicher Mittel (§ 5 BNDG) lediglich die entsprechende Geltung der korrespondieren Befugnisse für das BfV angeordnet wurde. Ihre Rechtfertigung fand diese Befugnisharmonisierung in dem Gedanken, dass für alle Nachrichtendienste des Bundes bei Tätigwerden im Inland dieselben Befugnisgrenzen gelten sollten. Es hat sich jedoch gezeigt, dass dies den unterschiedlichen Aufgaben nicht genügend Rechnung trägt.

Der Auftrag des BND aus § 1 Absatz 2 Satz 1 BNDG richtet sich auf die Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, und umfasst neben der Aufklärung von Bedrohungen und Gefahrenlagen (wie z.B. des internationalen Terrorismus) auch Entwicklungen im Ausland, die ohne eine aktuell bedrohliche Entwicklung zu nehmen für die Außen- und Sicherheitspolitik der Bundesregierung wichtig sind. Auslandsaufklärung ist damit nicht bloß ein Instrument der Gefahrenabwehr, sondern dient generell dazu, die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesregierung umfassend zu gewährleisten.

Thematisch folgt die Auslandsaufklärung Entwicklungen im Ausland, die nicht der souveränen Gestaltung der deutschen Staatsgewalt unterliegen. Zudem ergibt sich häufig die Notwendigkeit, kurzfristig auf neue Entwicklungen im Ausland zu reagieren, diese im Idealfall sogar zu antizipieren. Sofern der BND zur Aufgabenerfüllung Mitarbeiter und Quellen im Ausland zur geheimen Informationsgewinnung einsetzt, erfordert der Schutz von deren Freiheit, Leib und ggf. Leben besonderen Vorkehrungen. So kann z.B. der BND – anders als Sicherheitsbehörden im Inland – seine Aufklärungsbemühungen im Ausland nötigenfalls nicht unmittelbar mit polizeilichen oder anderen hoheitlichen Rettungsmaßnahmen schützen. Auch können sich Mitarbeiter oder Quellen des BND im Ausland nicht ohne weiteres an einen sicheren Ort unter die Obhut deutscher staatlicher Stellen flüchten.

Dabei bedeutet die bisherige normative Verweisungstechnik für die Auftragserfüllung des BND in denjenigen Fallkonstellationen ein ernsthaftes Hindernis, bei denen die Aufklärungstätigkeit im

Ausland durch Maßnahmenverbote im Inland empfindlich eingeschränkt oder Quellen und Mitarbeiter des BND hierdurch gefährdet worden wären. Der Gesetzentwurf führt auch das mit der am 31.12.2016 in Kraft getretenen BNDG-Novellierung damals insbesondere für die Ausland-Ausland-Fernmeldeaufklärung (§§ 6 ff. BNDG) verfolgte Vorhaben fort, die nachrichtendienstlichen Rechtsgrundlagen für die Arbeit der Nachrichtendienste des Bundes aufgabenadäquat auszudifferenzieren

II. Wesentlicher Inhalt des Entwurfs

Wesentliche inhaltliche Änderungen sind:

- Die nachrichtendienstlichen Befugnisse werden auf der Grundlage der IMK-Musterregelungen – unter Einbezug einer erstmaligen Befugnis zur „Online-Durchsuchung“ – neu geregelt, dies unter Einschluss der grundrechtsschützenden Maßgaben, speziell durch umfassenden Schutz des Kernbereichs privater Lebensgestaltung, gesetzliche Beschränkung nachrichtendienstlicher Zielpersonen, Verfahrenssicherungen mit besonderen Anordnungs- und Kontrollverfahren und spezifischen Zweckbindungen.
- Die zur Aufklärung extremistischer Operationen bestehenden Mitwirkungspflichten bestimmter Branchen (Personenverkehr, Finanzen, Kommunikation) werden klarer als Annex der Erhebungsbefugnis geregelt, um die mehrpolige Eingriffsdimension (Informationelle Selbstbestimmung des Betroffenen beschränkt durch die Erhebungsbefugnis / Handlungsfreiheit des Unternehmens beschränkt durch die Mitwirkungspflicht) systematischer zu ordnen. Gleichzeitig werden die Mitwirkungspflichten der Unternehmen umfassend (bisher nur nach § 2 G 10) auch zugunsten der Landesverfassungsschutzbehörden begründet, um das Harmonisierungsziel insoweit bereits bundesgesetzlich zu erreichen.
- Die Regelung zur Speicherung Minderjähriger wird für die nachrichtendienstliche Gefahrenaufklärung an das polizeiliche System angepasst, wonach Sachverhalte aufgabenadäquat unabhängig von Schuld- und Verantwortungsfähigkeit erfasst werden (wobei bei jungen Menschen der spezifischen Entwicklungsdynamik durch verkürzte Aussonderungsprüffristen Rechnung getragen wird). Auch dies

entspricht dem IMK-Bericht zur Rechtsharmonisierung und trägt dazu aktuellen Anforderungen Rechnung.

- Der Militärische Abschirmdienst (MAD) ist geschäftsbereichsbezogene Sonderbehörde des Verfassungsschutzes (Aufgaben nach § 1 Absatz 1 und 3 Satz 1 Nummer 1 MADG). Um dem Verwaltungszweig Verfassungsschutz entsprechend dem Zweck des Nachrichtendienstlichen Informationssystems eine einheitliche Informationsgrundlage zu verschaffen, wird der MAD optional vollwertig einbezogen (bisher lediglich begrenzter Lesezugriff). Die aufzuklärenden Lebenssachverhalte folgen nicht der behördlichen Gliederung des Verwaltungszweigs, so dass dazu nicht nur die Informationen von Bundes- und Landesbehörden, sondern ebenso die Informationen im und außerhalb des Geschäftsbereichs des BMVg zusammenzuführen sind.
- Die Koordinierungskompetenz des BfV als Zentralstelle im Verfassungsschutzverbund wird aufbauend auf der bisherigen Regelung um wirksame Mechanismen zur Standardisierung im Bereich von Dienstvorschriften – auch zum Vollzug durch die Landesverfassungsschutzbehörden – ergänzt.
- Der Einsatz nachrichtendienstlicher Mittel im BND-Gesetz wird umfassend neu geregelt (§§ 5 ff. BNDG). Insbesondere werden viele Detailregelungen, die bisher in BND-internen Dienstvorschriften festgelegt waren, nunmehr unmittelbar im Gesetz kodifiziert. Das stärkt Transparenz und Klarheit dieser Befugnisregelungen. Dem dient auch eine konsequentere Zuordnung der Befugnisse zu den einzelnen Dienstegesetzen, wonach Ausschreibungsbefugnisse des BND (§ 17 Absatz 3 BVerfSchG a.F.) nunmehr systemgerecht im BND-Gesetz (§ 23a BNDG) integriert sind.
- Auf die spezielle Aufgabenzuweisung des BND zugeschnitten wird zudem eine Vorschrift zu Datenerhebungen aus informationstechnischen Systemen von Ausländern im Ausland (§ 5c BNDG) eingefügt.

III. Alternativen

Umfassende Rechtsharmonisierung durch Bundesgesetz mit Geltung eines einheitlichen Verfassungsschutzgesetzes auch für den Landesvollzug. Dies begegnet indes kompetenziellen Einwänden zur Gesetzgebungszuständigkeit des Bundes. Daher

erscheint der Weg zielführender, den einheitlichen Rechtsrahmen der IMK je gesondert durch Bundes- und Landesgesetze umzusetzen.

Hinsichtlich der Änderungen im BNDG wäre die Alternative die Beibehaltung der bisherigen Verweisungstechnik auf das BVerfSchG. Diese Regelungstechnik entspricht jedoch nicht mehr den aktuellen Herausforderungen für die Auftragserfüllung des BND. Die Arbeit des BND findet unter anderen tatsächlichen Bedingungen als die Arbeit eines Inlandsnachrichtendienstes statt.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes zur Änderung des Bundesverfassungsschutzgesetzes (BVerfSchG) und des Artikel 10-Gesetzes folgt aus Artikel 73 Absatz 1 Nummer 10 Buchstabe b und c GG, wobei ergänzend die Auskunfts- und Mitwirkungspflichten von Unternehmen auf Artikel 73 Absatz 1 Nummer 6 und 7 und Artikel 74 Absatz 1 Nummer 11 GG zu stützen sind und die Verfahrensregelungen in § 9b Absatz 5 BVerfSchG auf Artikel 74 Absatz 1 Nummer 1 GG, zur Änderung des MAD-Gesetzes (MADG) aus Artikel 73 Absatz 1 Nummer 1 und Nummer 10 Buchstabe b GG, für Änderungen des BND-Gesetzes (BNDG) aus Artikel 73 Absatz 1 Nummer 1 GG, für die Änderung des Sicherheitsüberprüfungsgesetzes (SÜG) aus der Natur der Sache, der Verwaltungsgerichtsordnung (VwGO) und für die Regelung des Strafverfahrens in § 9b Absatz 4 BVerfSchG aus Artikel 74 Absatz 1 Nummer 1 GG, des BKA-Gesetzes aus Artikel 73 Absatz 1 Nummer 10 GG, des Vereinsgesetzes aus Artikel 74 Absatz 1 Nummer 3 GG, und des Straßenverkehrsgesetzes Artikel 74 Absatz 1 Nummer 22 GG. Die Änderung des Straßenverkehrsgesetzes hat die Nutzung von Einrichtungen des Bundes (Register) zum Gegenstand, die der Natur der Sache nach nur bundesgesetzlich zu regeln sind. Die Auskunftspflichten der Finanzbranche und im Personenverkehr sind einheitlich auch gegenüber den Landesverfassungsschutzbehörden im gesamtstaatlichen Interesse erforderlich, da der Verfassungsschutz gesamtstaatlichen Rechtsgütern dient und dabei durch arbeitsteiliges Zusammenwirken Landesbehörden Teile zu einem einheitlichen Bundeslagebild und Informationen zum Erkennen und zur Analyse länderübergreifender Bedrohungen beitragen müssen.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

VI. Gesetzesfolgen

Die Regelungen tragen zur besseren Gefahrerforschung und Aufklärung von Gefahren des Extremismus und Terrorismus sowie der Spionage und Proliferation in Deutschland bei und bewirken dabei einen abgewogenen Ausgleich zwischen den damit verfolgten Gemeinwohlbelangen und den Interessen einzelner durch Datenverarbeitung in ihren Persönlichkeitsrechten betroffenen Personen.

Die Neuregelungen ermöglichen dem BND, gerade im HUMINT-Bereich, eine nachrichtendienstliche Aufklärung, die ihren gesetzlich weit gespannten Auftrag auch unter den heutigen Rahmenbedingungen einer eng vernetzten und dadurch grenzüberschreitend transparenten Lebensrealität erfüllen muss. Gleichzeitig werden die Interessen der infolge des Einsatzes heimlicher nachrichtendienstlicher Mittel betroffenen Grundrechtsträger durch umfangreiche Detailregelungen, beispielsweise zum Kernbereichsschutz, und rechtsklarer gefassten Normen besser geschützt.

1. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie, speziell Indikator 16.1 „Kriminalität Persönliche Sicherheit weiter erhöhen“. Die Bezüge sind dabei allerdings in mehrfacher Hinsicht mittelbar. Schutzgut des Verfassungsschutzes sind nicht Individualrechtsgüter, sondern die Universalrechtsgüter nach Artikel 73 Absatz 1 Nummer 10 Buchstabe b GG. Diese bilden aber den strukturellen Rahmen, in dem sich individuelle Sicherheit realisiert. Die Wirkungen sind auch insofern mittelbar, als der Verfassungsschutz eine Frühwarnfunktion hat und ausdrücklich nicht über intervenierende Befugnisse verfügt, so dass sich diese Aufgabenwahrnehmung

unter Umständen erst in vielstufigen Wirkungsketten in konkreten Sicherheitseffekten abbildet. Eine Operationalisierung statistischer Messbarkeit der Wirkungen des Gesetzes in Bezug auf den Nachhaltigkeits-Indikator ist danach nicht möglich, mithin sind auch entsprechende prognostische Einschätzungen gegenständlich nicht eröffnet. Gleichwohl ist generell davon auszugehen, dass die effektive Aufgabenwahrnehmung des Verfassungsschutzes sich auch im Indikator 16.1 positiv niederschlägt.

Der Gesetzentwurf dient mit den Änderungen zum BND-Gesetz auch dazu, die Bundesregierung mit denjenigen Informationen zu versorgen, die sie zur Verfolgung insbesondere der Unterziele 16.1 (deutliche Verringerung aller Formen der Gewalt), 16.4 (Bekämpfung illegaler Finanz- und Waffenströme und der organisierten Kriminalität) und 16.5 (Reduzierung von Korruption und Bestechung) aus der Deutschen Nachhaltigkeitsstrategie benötigt. Darüber hinaus sind die vom BND gemäß § 1 Absatz 2 Satz 1 BNDG geforderten Erkenntnisse über das Ausland eine wichtige Informationsquelle für eine Vielzahl von Aspekten der deutschen Außen- und Sicherheitspolitik, die auch andere Ziele im Sinne dieser Nachhaltigkeitsstrategie betreffen, z.B. der Ziele 1 und 2 (Armut- und Hungerbekämpfung) oder der Ziele 6 und 7 (Wasser- und Energieversorgung). Die Bundesregierung begreift Sicherheitspolitik jedoch nicht nur in Kategorien traditioneller staatlicher Sicherheitsinstrumente (Streitkräfte, Polizei), sondern als Ineinander-Greifen vieler für die Stabilität und Sicherheit einer Region verantwortlicher Faktoren. Dazu zählen auch Entwicklungszusammenarbeit, Bildung, Zugang zu Ressourcen oder gesellschaftlichen Partizipation aller Bevölkerungsteile. Daher schlagen sich letztlich die meisten der vom BND über die Situation in auftragsrelevanten Ländern gesammelten Erkenntnisse in einer Politik nieder, die die vorstehend genannten Ziele für nachhaltige Entwicklung verfolgt.

2. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

3. Erfüllungsaufwand

a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht durch zwei Regelungen ein geringfügiger Erfüllungsaufwand.

§8a BVerfSchG enthält eine Mitwirkungspflicht für privatwirtschaftliche Unternehmen, die allerdings im Kern den bisherigen Regelungen in § 8a BVerfSchG (und § 2 G10) entsprechen. Die regelmäßige parlamentarische Berichterstattung zeigt geringe Fallzahlen auf (zuletzt: BT-Drs. 19/1280), zu der auch künftig keine erheblichen Änderungen zu erwarten sind. Wesentliche Änderungen im Erfüllungsaufwand der Wirtschaft sind danach nicht zu erwarten.

Auch durch die Regelung des § 3 BNDG entsteht geringfügiger Erfüllungsaufwand, weil unter den dort genannten Voraussetzungen von bestimmten Unternehmen Auskunft zu bei ihnen vorhandenen Informationen verlangt werden kann.

Der BND hat wie das BfV von den vergleichbaren, niederschwelligen Auskunftsbefugnissen der Vorgängerregelung (§§ 3, 4 BNDG a.F.) seit deren erstmaliger Einführung durch die Terrorismusbekämpfungsgesetze 2002 stets nur in geringem Umfang Gebrauch gemacht (vgl. BT-Drs. 19/1280). Trotz jetzt erfolgter Erweiterungen des Kreises der zur Auskunftserteilung verpflichteten Unternehmen (§ 3 BNDG n.F.) ist daher auch zukünftig kein signifikanter Anstieg des Aufwands zur Erfüllung dieser Auskunftsverlangen zu erwarten.

c) Erfüllungsaufwand für die Verwaltung

Bund:

Für den Bund entsteht ein Erfüllungsaufwand bei der Ausübung der neuen Befugnisse, speziell zur Online-Durchsuchung, sowie wegen erweiterter Pflichten zur Protokollierung und Mitteilung von Grundrechtseingriffen. Da ein künftiges Mengengerüst ebenso wie die Aufwände einer einzelnen Maßnahme durch nicht absehbare operative Anforderungen, Voraussetzungen und Umstände geprägt sind, lässt sich dieser Aufwand nicht näher beziffern. Er ist zudem nicht gesetzlich induziert, sondern beruht

auf dem behördlichen Einsatzermessen, das seinerseits Wirtschaftlichkeitserwägungen mit einbezieht. Dem Aufwand stehen in einem gewissen Umfang Einsparungen durch Entbürokratisierung von Verfahren und voraussichtlich effizientere Ermittlungsmöglichkeiten gegenüber. Eine nähere Bezifferung ist dabei auch insoweit nicht möglich, da sie von nicht aussagekräftig prognostizierbaren künftigen Einsatzlagen abhängt.

Die Zuständigkeit der G10-Kommission wird auf weitere Maßnahmen erstreckt, verbunden auch mit zusätzlichen Aufgaben beim Schutz des Kernbereichs privater Lebensgestaltung. Dies erfordert einen Aufwuchs in der Personal- und Sachausstattung, die ihr zur Erfüllung ihrer Aufgaben zur Verfügung zu stellen ist.
[...]

Länder:

Soweit sie das Bundesverfassungsschutzgesetz anwenden wie der Bund.

4. Weitere Kosten

Weitere Kosten sind nicht zu erwarten.

5. Weitere Gesetzesfolgen

Auswirkungen auf demographierelevante Belange sind nicht zu erwarten.

6. Evaluierung

Gesetzesbegleitend erfolgt eine laufende Evaluierung zur Praxisbewährung der Regelungen sowohl unter Gesichtspunkten der Wirksamkeit wie der Wirtschaftlichkeit.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BVerfSchG)

Zu Nummer 1 (§ 5 Absatz 3 Sätze 3 und 4)

Die Koordinierungskompetenz der Zentralstelle wird mit den neuen Sätzen 3 und 4 für den Bereich allgemeiner Regelungen verstärkt. Die mit dem Gesetz bezweckte Harmonisierung der Arbeitsgrundlagen der Verfassungsschutzbehörden in Bund und

Ländern betrifft nicht allein Rechtsvorschriften, sondern ebenso untergesetzliche Regelungen wie Dienstvorschriften. Auch insoweit ist eine Vereinheitlichung im Interesse homogener Teilbeiträge, die zu einem Gesamtbild zusammenzufügen sind, oder auch effektiver Zusammenarbeit auf Grundlage standardisierter Methoden geboten. So sind beispielsweise Standardisierungsvorgaben bei der einheitlichen Bewertung zur Erfassung im Nachrichtendienstlichen Informationssystem grundlegend für aussagekräftige Erkenntnisse zur überregionalen Gesamtlage.

Auch insoweit bleibt es beim Vorrang konsensualer Koordinierung. Bei Standardisierungsbedarf müssen jedoch im Interesse des Gesamtverbundes unter Umständen Minderheitenpositionen zurücktreten. Hierzu wird für Standardisierungsvorhaben im Verfassungsschutzverbund ein effektiverer Entscheidungsmechanismus für den Fall, dass ein Konsens nicht herzustellen ist, eingeführt. Die Zentralstelle erhält hierzu ein Bestimmungsrecht, die föderale Balance bleibt gleichwohl dadurch gewahrt, dass der Bund keine Letztentscheidung bei mehrheitlicher Gegenposition der Länder treffen kann. Dies bleibt hinter der allgemeinen Weisungsbefugnis des Bundes im ursprünglichen § 5 Absatz 2 BVerfSchG 1950 (BGBl. I S. 682) zurück, stellt aber eine dem Stand der föderalen Kooperation angemessene Lösung dar.

Zu Nummer 2 (§6 Absatz 2 Sätze 1 bis 4)

Wesentlicher Inhalt der in § 6 Absatz 2 neu eingefügten Sätze 1 bis 4 ist die in Satz 2 eröffnete Möglichkeit, den MAD hinsichtlich seiner Verfassungsschutzaufgaben vollständig in den Informationsverbund zu integrieren. Das nachrichtendienstliche Informationssystem dient gerade dazu, die Informationen der Verfassungsschutzbehörden zusammenzuführen und allen Behörden für ihre jeweilige Aufgabe verfügbar zu machen. Dies hat nicht nur die föderale Komponente der Gliederung des Verwaltungszweigs in Landesbehörden und das Bundesamt. Der MAD ist – mit spezieller Zuständigkeit im Geschäftsbereich des Bundesministeriums der Verteidigung – die zweite Bundesverfassungsschutzbehörde mit kongruenten Aufgaben (§ 3 Absatz 1 und 2 Nummer1 und 2 BVerfSchG a.F. / § 1 Absatz 1 und 3 Nummer 1 MADG a.F.). Konsequenterweise bestehen auch

kongruente Zusammenarbeits-, einschließlich Übermittlungspflichten (§ 1 Absatz 2 und 3 und § 6 Absatz 1 Satz 1 BVerfSchG a.F. / § 3 Absatz 1 und 3 Satz 1 MADG). Lediglich das technische Mittel dieses informationellen Verbundes ist noch unterschiedlich, indem nur begrenzt Rechte zu den verschiedenen Datenbanken eingeräumt werden können (§ 3 Absatz 3 Satz 2 ff. MADG a.F.). Dies ist unzeitgemäß und birgt vermeidbare Risiken für die gemeinsame Aufklärungsaufgabe und die herausragenden Schutzgüter, denen sie dient.

Der automatisierte Abruf aus der Verbunddatenbank bleibt im Übrigen aufgabengeprägt restriktiv geregelt, wird dabei aber mit den Regelungen zu gemeinsamen Dateien synchronisiert. Dies dient der technikneutralen Klarstellung, dass solche Dateien durch ihre speziellen Verarbeitungsregelungen eine logische Struktur bilden, die jedoch nicht notwendig auf physisch gesonderter Basis realisiert werden muss.

Im Übrigen werden die bisherigen Regelungen redaktionell überarbeitet: Mit Satz 1 wird der bereits in § 5 Absatz 4 Nummer 1 eingeführte Begriff des „nachrichtendienstlichen Informationssystems“ nunmehr auch für § 6 Absatz 2 aufgegriffen. Er bezeichnet den Informationsverbund. Die technische Plattform kann unbeschadet ihrer originären Funktion auch zur flexiblen Rechtegestaltung und damit auch dazu genutzt werden, eigene Amtsdateien zu führen, die nicht der Erfüllung der Unterrichtungspflicht nach § 6 Absatz 1 dienen (s. BT-Drs. 18/4654, 21). Satz 3 stellt klar, dass die speziellen gesetzlichen Regelungen für eine gemeinsame Datenhaltung zur Zusammenarbeit im nachrichtendienstlichen Bereich unberührt bleiben. Eine gemeinsame Datenhaltung kann technisch auch durch die Einräumung entsprechender Zugriffsrechte auf das nachrichtendienstliche Informationssystem umgesetzt werden. Satz 4 enthält einen Verweis auf die Regelungen zur Verarbeitung personenbezogener Daten im nachrichtendienstlichen Informationssystem.

Zu Nummer 3 (§ 8 Absatz 2)

Die Aufhebung des bisherigen § 8 Absatz 2 ist Folge der künftig umfassenderen Regelung in §§ 9, 9a, in die u.a. auch die bisherigen Bestimmungen aus § 8 Absatz 2 eingehen.

Zu Nummer 4 (§§8a bis 9e)

Die Nummer enthält mit der Übernahme des einheitlichen Rechtsrahmens der Innenministerkonferenz den Kern des Harmonisierungsvorhabens.

Nachrichtendienstliche Frühaufklärung ist Ausdruck der Grundentscheidung des Grundgesetzes für eine wehrhafte Demokratie und des Selbstbehauptungswillens des Rechtsstaates (BVerfGE 143, 101 – Rn. 126 und BVerfGE 146, 1 – Rn. 110). Bedrohungen für die herausragenden Schutzgüter des § 1 Absatz 1 mit der spezifischen Potenzialität der Gefährdungslagen nach § 3 Absatz 1 (zweckgerichtete Personenzusammenschlüsse und Wirkungsmacht fremder Staaten) bedingen effektive Frühaufklärung bereits mit niedriger Risikoschwelle. „Vorfeld"-Charakteristik nachrichtendienstlicher Aufklärung ist ein bereits risikobasierter Aufgabenansatz, der grundsätzlich nicht erst bei konkreten bzw. konkretisierten Gefahren einsetzt, sondern deren Entstehen frühzeitig erkennt (und diese Erkenntnis dann zunächst verdichtet, bevor staatliche Intervention darauf gestützt wird).

Die föderale Arbeitsteilung in dieser gemeinsamen Aufklärungsaufgabe benötigt angesichts des gesamtstaatlichen Rechtsguts bei überregionalen Bedrohungen einen harmonisierten Rechtsrahmen mit wirksamen Befugnissen (so bereits die Innenministerkonferenz in ihrer 206. Sitzung am 14. Juni 2017, TOP 34). In ihrer 207. Sitzung am 8. Dezember 2017 hat die Innenministerkonferenz dazu Musterregelungen (TOP 29) beschlossen. In ihrem Koalitionsvertrag für die 19. Wahlperiode haben die Koalitionsparteien als Harmonisierungsbeitrag des Bundes vereinbart, das Bundesverfassungsschutzgesetz auf der Grundlage der IMK-Musterregelungen zu novellieren.

Zu § 8a

Der neue § 8a integriert bisher in §§ 8a, 8b Absatz 8 und § 8d BVerfSchG a.F. getroffene Regelungen. Er enthält dabei verschiedene Neuerungen.

Der Anwendungsbereich erstreckt sich künftig auch auf die Unterstützung von Landesverfassungsschutzbehörden. Solche bundesrechtlichen Unternehmenspflichten bestanden bislang nur

punktuell, insbesondere im Telekommunikationssektor (§§ 112 f. TKG und § 2 G 10). Dieser Ansatz wird gemäß dem Harmonisierungsziel des Gesetzentwurfs nunmehr verbreitert und im neuen § 8a allgemein zugrunde gelegt. Geregelt sind hier lediglich die Unternehmenspflichten, wohingegen die Erhebung der Verfassungsschutzbehörden gesondert geregelt ist, sich mithin für die Landesverfassungsschutzbehörden nach Landesrecht richtet. Erhebungsgrundlage des BfV ist allgemein § 8 Absatz 1 BVerfSchG, soweit nicht spezielle Regelungen zu besonderen Datenerhebungen gelten. Dies ist wegen der Beschränkung des Post- und Fernmeldegeheimisses in § 9c der Fall.

Die sektorale Ausgestaltung der Mitwirkungspflichten erfolgt wertungshomogen nach den der Sektorauswahl zugrunde liegenden Erwägungen und zukunftsfest durch deren allgemeine Fassung, entsprechend der Gesetzgebungsfunktion, das Wesentliche abstrakt-generell zu regeln.Tragend ist dabei, dass die Strukturaufklärung der Verfassungsschutzbehörden zentral auf Interaktion Beteiligter gerichtet ist und dazu deren personale Mobilität sowie Finanz- und Kommunikationsbeziehungen wesentliche Aufklärungsansätze bilden.

- Mit der neuen Nummer 1 werden nun allgemein entgeltliche oder geschäftsmäßige Anbieter von Leistungen zum Transport von Personen (Personenverkehr) erfasst. Hierzu zählen insbesondere Eisenbahnverkehrsunternehmen im Sinne des § 2 Absatz 3 des Allgemeinen Eisenbahngesetzes, Unternehmen für den Linienverkehr mit Kraftomnibussen im Sinne des § 42a Satz 1 des Personenbeförderungsgesetzes sowie Unternehmen, die entgeltlich oder geschäftsmäßig Mittel für den öffentlichen Personenverkehr bereitstellen wie gewerbliche Anbieter von Mietfahrzeugen für Selbstfahrer im Sinne des § 6 Absatz 1 Nummer 12 des Straßenverkehrsgesetzes und Carsharinganbieter im Sinne des § 2 Nummer 2 des Gesetzes zur Bevorrechtigung des Carsharing. Mit der Regelung wird der zunehmenden Bedeutung alternativer Verkehrsträger Rechnung getragen.
- Nummer 2 erfasst ebenso den gesamten Wirtschaftssektor mit Finanzaufgaben (Zahlungsverkehre, Kapitalbeschaffung/-verwendung), dessen Auskünfte für Finanzermittlungen benötigt werden.

- Mit der neuen Nummer 3 werden neben Telekommunikationsdiensten gemäß der fachrechtlichen Terminologie Telemedien miterfasst (der bisherige Begriff der „Teledienste“ – und der diesbetreffend differenzierende Ansatz – ist im Telemediengesetzes gegenstandsadäquat aufgegeben worden). Zukünftig werden zudem auch geschäftsmäßig erbrachte Postdienste wieder einbezogen. Es ist nicht sachgerecht, diese Mitwirkung, für die objektiv Bedarf besteht, gesetzlich restriktiver als bei den in der Lebenswirklichkeit wesentlich weitergehenden Eingriffen in das Fernmeldegeheimnis auszugestalten. Den objektiven Bedarf hat zuletzt auch die neuerliche Evaluierung des bisherigen § 8a BVerfSchG durch wissenschaftliche Sachverständige bestätigt. In der extremistischen Praxis sind Umgehungsgestaltungen zur Vermeidung der gegebenen Überwachungsmöglichkeiten festzustellen, beispielsweise durch Ersetzung von Überweisungen durch Bargeldbriefsendungen an dafür eingerichtete Postfächer. Das geltende Recht war bislang insoweit auch widersprüchlich, als in § 2 Absatz 1 G10 eine Mitwirkungspflicht von Postdienstleistern – auch hinsichtlich der Umstände des Postverkehrs – enthalten war, in § 8a Absatz 2 BVerfSchG a.F. hingegen nicht.

Zur Auskunft über Bestandsdaten nach Absatz 1 Satz1 Nummern 1 bis 3 sind auch diejenigen Dienstleister verpflichtet, die geschäftsmäßig an der Erbringung von Leistungen in den genannten Branchen mitwirken, wie Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen. Die Verpflichtung ist nicht auf Unternehmen mit einer (Zweig-)Niederlassung im Inland beschränkt, sondern bezieht nach dem Marktortprinzip auch die inländische Leistungserbringung ein (kraft deren die deutsche Jurisdiktion für die gesetzliche Auskunftspflicht gegeben ist).

Zum Eingriffsgehalt unterscheidet die neue Regelung klarer zwischen den berührten Grundrechtsverhältnissen, einerseits der Personen, deren Daten erhoben werden, und andererseits der Unternehmen, die an dieser Erhebung durch Übermittlung mitwirken müssen. Der Eingriff in die informationelle Selbstbestimmung bemisst sich dabei grundsätzlich nach den jeweiligen Erhebungsbefugnissen, die nach § 8a Absatz 2 Satz 1 gesondert vorliegen müssen und insoweit nicht durch § 8a

erweitert werden. Dieser Eingriff ist für den Vorgang maßgeblich und damit auch für die Begründung der annexen Mitwirkungspflichten der Unternehmen führend. Die isolierten Unternehmensbelastungen sind von vergleichsweise untergeordneter Bedeutung, so dass die jeweiligen materiellen Schwellen bzw. Verfahrens- oder Transparenzanforderungen bei der Beschränkung der Betroffenenrechte erst Recht für die Belastung der Unternehmen angemessen sind. Im Ergebnis stärkt die neue Regelung zugleich die Wertungskonsistenz im Bundesrecht, zu der die neuerliche Evaluierung des bisherigen § 8a BVerfSchG a.F. verschiedene Brüche aufgezeigt hat (vgl. im Evaluierungsbericht Abschnitt 5).

Zur Erhebung bloßer Bestandsdaten sind die Verfassungsschutzbehörden nach der allgemeinen Erhebungsbefugnis (des BfV in § 8 Absatz 1) berechtigt, folglich sind auch die Übermittlungsregelungen in § 8a Absatz 1 insoweit allgemein auf die Aufgabenerforderlichkeit bezogen, die ausschließlich herausragenden öffentlichen Interessen dient. Dies entspricht auch § 112 Absatz 2 Nummer 4 TKG. Besondere Übermittlungsvorschriften bleiben nach Absatz 1 Satz 3 unberührt, also beispielsweise § 113 Absatz 1 Satz 1 TKG zu den im manuellen Verfahren zu übermittelnden Datenarten. Unternehmensbelange sind vornehmlich mit der wirtschaftlichen Belastung durch die verbundenen Aufwände berührt. Angesichts der bestehenden Automatisierung von Standardabfragen zu Bestandsdaten (§ 112 TKG, § 93b AO) bleiben diese Aufwände auch künftig auf niedrigem Niveau. Im Übrigen bleibt es bei der Verordnungsregelung zur Aufwandsentschädigung (Absatz 5 Satz 1 Nummer 2 Buchstabe f), von der im Interesse rechtssystematischer Vereinheitlichung der Telekommunikationssektor (bisher Sonderregelung in § 8b Absatz 9 BVerfSchG a.F.) nicht weiter ausgenommen wird. Mit Absatz 1 Satz 5 wird zudem klargestellt, dass die materiellen Voraussetzungen für Folgemaßnahmen vorliegen müssen, soweit ein Auskunftsverlangen allein deren Vorbereitung dient. Hiermit wird die bisher nur als Spezialfall in § 8d Absatz 1 Satz 2 (a.F.) ausdrücklich normierte Regelung als allgemeine Regelung auf alle Fälle des Satzes 1 Nummer 3 ausgeweitet.

Die Regelungen werden im Übrigen gemäß der Gesetzgebungsfunktion auf die wesentlichen Entscheidungen konzentriert. So entfällt beispielsweise die spezielle gesetzliche

Regelung des bisherigen § 8b Absatz 6 BVerfSchG a.F., dass Auskünfte „unverzüglich, vollständig, richtig“ zu erteilen sind, da dies auch ohne besondere Regelung für die Umsetzung öffentlich-rechtlicher Pflichten gilt.

Zur Vertragsdurchführung sind nach Absatz 2 sowohl Umstände als auch Inhalte der Leistungserbringung zu beauskunften. Die Mitwirkungspflicht ist annex zur Erhebungsbefugnis, setzt also beispielsweise zur Erhebung der in § 9c Absatz 2 geregelten Telekommunikationsverkehrsdaten die dort geregelte Schwelle sowie das dafür nach § 9c Absatz 3 geregelte Anordnungs- und Kontrollverfahren voraus. Mindestschwelle der Mitwirkungspflicht ist nach Absatz 2 allerdings generell (auch unabhängig von besonderen Erhebungsschwellen), dass Bedrohungen von erheblicher Bedeutung aufzuklären sind. Diese Schwelle qualifiziert den Gefahrengrad, dem die Schutzgüter des § 3 Absatz 1 durch die jeweilige Bedrohung ausgesetzt sind, wobei gleichermaßen Vorgehensweise (insbesondere klandestin oder gewalttätig), Wirkungsweise (etwa bei elektronischen Angriffen), Wirkungen (wie Diskursrelevanz in der extremistischen Subkultur und darüber hinaus) und Handlungspotenzial (bei fremden Staaten, aber auch größeren Personenzusammenschlüssen, ggf. auch Finanzkraft) risikobestimmend sind. Folglich haben Tätigkeiten nach § 3 Absatz 1 Nummer 2 und – per se gewaltorientierte – Bestrebungen nach § 3 Absatz 1 Nummer 3 generell erhebliche Bedeutung (vgl. bereits § 9a Absatz 1 Satz 2 BVerfSchG a.F.).

Zu den Umständen und Inhalten der Leistungserbringung gehören insbesondere die bisher in § 8a Absatz 2 BVerfSchG a.F. aufgeführten Datenarten. Im Interesse besserer Flexibilität im Gesetzesvollzug auch unter Berücksichtigung etwaiger künftiger Entwicklungen wird der Erhebungsumfang abstrakter normiert, wobei Konkretisierungen zu den Inhalten der übermittlungspflichtigen Datenarten durch Verordnung erfolgen können (Absatz 5 Satz 1 Nummer 2 Buchstabe b). Beispielsweise hat die Praxis gezeigt, dass zur verwechslungsfreien Personenzuordnung, die auch im Datenschutzinteresse liegt, beim Identifizierungsdatensatz des bisherigen § 8a Absatz 2 Satz 1 Nummer 1 BVerfSchG a.F. auch das Geburtsdatum nötig ist, das indes im Gesetz nicht aufgeführt ist, was in der Praxis erhebliche Rechtsunsicherheit veranlasst. Weiteres Beispiel für Umstände der

Leistungserbringung ist die Einbuchung eines aktiv geschalteten Mobiltelefons in eine Funkzelle, die die Erreichbarkeit für Verkehre schafft. Zu den Inhalten gehört beispielsweise auch die Verwahrung bestimmter Sachen in Bankschließfächern. Absatz 2 Satz 2 stellt dazu klar, dass die Information der berechtigten Verfassungsschutzbehörde hier durch Herausgabe erfolgt.

Eine neue Mitwirkungspflicht begründet Absatz 3 für Betreiber einer Videoüberwachung, wenn sie nach § 4 Absatz 1 Satz 2 BDSG bereits spezifischen Sicherheitsinteressen der Allgemeinheit dient. Die Mitwirkungspflicht ist dabei zudem auf qualifiziert gefährdende Sachverhalte (Tätigkeiten fremder Mächte und Bestrebungen von erheblicher Bedeutung) beschränkt (Satz 2).

Die Formulierung von Absatz 4 Satz 1 ist angelehnt an § 113 Absatz 4 Satz 2 TKG und greift inhaltlich die bisherige Regelung aus § 8b Absatz 4 Satz 2 BVerfSchG a.F. auf. Die weiteren Regelungen des Absatzes entsprechen dem bisherigen § 8b Absatz 5 BVerfSchG a.F. Das Benachteiligungsverbot des Satzes 4 ist lex specialis insbesondere auch gegenüber anderen gesetzlichen Verdachtsmeldepflichten, etwa nach § 43 GWG. Die Anfrage der Verfassungsschutzbehörde begründet keinen meldepflichtigen Verdacht (auf unzureichender Informationsgrundlage) des Unternehmens, vielmehr wäre es Sache der Verfassungsschutzbehörde (in Kenntnis aller ihr verfügbaren Informationen), ihrerseits andere Bedarfsträger – nach Maßgabe der dafür einschlägigen Übermittlungsregelungen – zu informieren.

Die Verordnungsermächtigung des Absatzes 5 baut auf dem bisherigen § 8b Absatz 8 BVerfSchG a.F. auf. Neu ist die Ermächtigung nach Nummer 1, auch Mitwirkungspflichten, die die Vorbereitung von Datenerhebungen betreffen, zu regeln.

Zu §§ 9 ff.

Die Regelungen zum Einsatz nachrichtendienstlicher Mittel sind in Übernahme der IMK-Musterregelungen wertungskonsistenter ausgeformt, dabei mit umfassenderen rechtsstaatlichen Eingrenzungen, speziell zum Schutz des Kernbereichs privater Lebensgestaltung und zur Maßnahmerichtung, versehen und auch regelungsdichter gefasst.

§ 9 bleibt die allgemeine Befugnisnorm, die mit § 9a um allgemeine Befugnisschranken und mit §§ 9b ff. um spezielle Befugnisse ergänzt wird.

Wie in den meisten Landesverfassungsschutzgesetzen werden Mittel der heimlichen Informationsbeschaffung nunmehr auch im Bundesverfassungsschutzgesetz als nachrichtendienstliche Mittel bezeichnet. Dies dient einerseits der terminologischen Harmonisierung der Verfassungsschutzgesetze. Zum anderen wird damit aber auch in bewusster Abgrenzung zu besonderen Mitteln der Datenerhebung der Polizei der spezifische Aufgabenkontext, in dem diese Mittel durch Verfassungsschutzbehörden eingesetzt werden, begrifflich einbezogen. Die Befugnisse sind nicht isoliert nach einer Maßnahmetypik zu würdigen (die auch einer Polizeibehörde verfügbar ist), sondern unter Einbezug der Folgen (vgl. BVerfGE 120, 378 – Rn. 80), somit im Anwendungsrahmen des Bundesverfassungsschutzgesetzes, also als nachrichtendienstliche Maßnahme getrennt von polizeilichen Zwangsbefugnissen.

Diese organisatorische Trennung von nachrichtendienstlicher Erforschung und exekutiver Intervention ist international nicht singulär, allerdings kein allgemeiner Standard. Beispielsweise in Österreich (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung), Schweden (Säkerhetspolisen) oder den USA (Federal Bureau of Investigation) erfolgt die nachrichtendienstliche Vorfeldaufklärung – auch – im Staatsschutz durch die Kriminalpolizei (Mischbehörden). Die Trennung hat indes den Vorteil, dass Informationen aus einer naturgemäß bei der Informationsgewinnung erheblich streuenden Lageaufklärung nicht als Rohinformation für die Ausübung von Zwangsgewalt verfügbar sind, sondern erst nach einem behördlich gesonderten Auswertungsprozess, der Informationen nach Relevanz filtert, validiert und verdichtet, hierdurch Privatsphäre von Informationen mit Sozialbezug abschichtet und Verantwortlichkeiten herausarbeitet, die Grundlage zielgerichteter Folgemaßnahmen sind. Das Trennungsprinzip ist danach eine organisatorische Sicherung der Erkenntnisqualität, die Risiken der informationellen Fehlsteuerung von Zwangsgewalt reduziert. Zugleich ist es Grundlage, die spezifischen Anforderungen an Arbeitsweise und resultierende Erfordernisse der Funktionsfähigkeit der Nachrichtendienste (allg. BVerfGE 146, 1 – Rn. 110 ff.) möglichst weitgehend zu gewährleisten.

Die Systematik der nachrichtendienstlichen Befugnisse trägt dem nicht nur bei den materiellen Einsatzschwellen Rechnung, sondern ebenso bei der aufgaben- und risikoadäquaten Gestaltung der Verfahrenssicherungen. Dabei wird im Wesentlichen – abstufend – unterschieden zwischen Maßnahmen,

- die in die informationelle Selbstbestimmung eingreifen,
- die in die besonderen Privatheitsrechte der Artikel 10 und 13 GG – und dazu parallel in die Vertraulichkeit und Integrität informationstechnischer Systeme – eingreifen.

Der Schutzansatz informationeller Selbstbestimmung beruht darauf, dass der Betroffene Interaktionen seiner sozialen Umwelt in seinen Verhaltensentscheidungen antizipiert (BVerfGE 65, 1 [Absatz 172]). Information, über die diese Umwelt verfügt, ist dabei deren Aktionsgrundlage. Hiernach vermag bereits der fremde Informationsbesitz (und auch bereits die Unsicherheit darüber) die eigene Betätigung von Handlungsfreiheit zu hemmen. Informationellen Eingriffen wird hiernach Eingriffsqualität zugemessen, weil die Informationen Grundlage für aktionelle Entscheidungen der öffentlichen Gewalt sein können und die vorgelagerte Datenverarbeitung dafür die Voraussetzungen schafft. Informationelle Selbstbestimmung erweitert den grundrechtlichen Schutz von Verhaltensfreiheit, indem sie bereits Gefährdungstatbestände als eingriffsgleich qualifiziert (BVerfGE 120, 378 – Rn. 63). Die Eingriffsbedeutung des informationellen Akts erschließt sich mithin nicht isoliert aus dem Realakt der Erhebung, vielmehr ist dafür das Risiko potenzieller – aktioneller – Verwendung der gewonnenen Information mit bestimmend (BVerfGE 120, 378 – Rn. 80).

Nachrichtendienste besitzen selbst keine aktionellen (Interventions-)Befugnisse. Mit dem nachrichtendienstlichen Informationsbesitz selbst gehen mithin noch keine unmittelbaren Risiken dafür aus, dass der Staat einem Betroffenen bei Ausübung von dessen Handlungsfreiheit beschränkend begegnet. Allerdings erfüllt sich die Nachrichtendienstaufgabe nicht in der Informationssammlung, sie intendiert vielmehr einen Schutz, der erst aufgrund Informationsweitergabe durch intervenierende Aufgabenträger realisiert wird. Dieses Ziel ist nicht nur bestimmend für die Gewichtung der Gemeinwohlbedeutung der (Schutz-)Aufgabe, sondern ebenso der verbundenen Risiken für

individuelle Freiheitsbetätigung.

Der Informationsfluss zu exekutiven Aufgabenträgern hat jedoch nicht die Rohinformation des ursprünglichen Erforschungseingriffs zum Gegenstand, vielmehr ist es gerade nachrichtendienstliche Aufgabe, aus diesem Ursprungsaufkommen bloße Privatheit ohne Sozialbezug auszufiltern und die relevanten Informationen im Weiteren zu verifizieren und zu verdichten (BT-Drs. 18/4654, S. 33). Zudem erfolgt mit den Übermittlungsschwellen der informationellen Trennung zugleich eine rechtsgutbezogene Filterung, beschränkt auf herausragende Interessen der Allgemeinheit. Der staatlichen Interventionsmacht verfügbar werden also erst gehärtete Informationen mit herausragendem Sozialbezug. Hiernach haben nachrichtendienstliche Eingriffsakte nicht die gleichen Wirkungen im Schutzbereich informationeller Selbstbestimmung und bedürfen danach auch nicht derselben Anforderungen. Dies deckt sich mit der generellen Linie der Verfassungsrechtsprechung (BVerfGE 120, 274, Rn. 255; s.a. BVerfGE 130, 151, Rn. 177 und BVerfGE 133, 277, Rn. 117; anders jedoch BVerfGE 125, 260, Rn. 233, wo indes die Schutzaufgabe des Verfassungsschutzes außer Betracht bleibt).

Auf der Grundlage der Sacherwägungen informationeller Selbstbestimmung, bereits chilling effects als freiheitsbeschränkend zu qualifizieren, wird diese normative Würdigung rechtstatsächlich dadurch bestätigt, dass in der jahrzehntelangen Geltungs- und Vollzugspraxis der bisherigen § 8 Absatz 2, § 9 Absatz 1 BVerfSchG a.F eine übermäßige oder auch nur grundrechtlich relevante Verunsicherung der Bevölkerung nicht erkennbar geworden ist, auch in Ansehung des Umstandes, dass nachrichtendienstliche Maßnahmen, die nicht in Artikel 10 oder 13 GG eingreifen, keiner richterlichen – oder sonst unabhängigen – Anordnung unterliegen. Bloße Mutmaßungen, die von jahrzehntelanger Anwendungspraxis nicht bestätigt werden, vermögen indes die gesetzgeberische Einschätzung und Gestaltung nicht zu beschränken (vgl. etwa BVerfGE 110, 141 – Rn. 95; BVerfG 128, 1 – Rn. 140; intuitive Spekulationen sind keine tragfähige Grundlage für rationales Staatshandeln, BVerfGE 141, 220 – Rn. 104).

Wo hingegen nicht erst hemmende Folgewirkungen auf eine künftige Betätigung allgemeiner Handlungsfreiheit die

Eingriffsqualifikation begründen, sondern der grundrechtsspezifische Eingriffsgehalt sich unmittelbar mit dem Eingriff in einen speziell geschützten Privatheitsbereich realisiert, sind differenzierende Würdigungen der Verfahrensanforderungen durch das Trennungsprinzip nicht gleichermaßen veranlasst. Für die Eingriffsbedeutung sind hier potenzielle aktionelle Folgen nicht ebenso tragend, vielmehr realisiert sich der spezifische Eingriffsgehalt unmittelbar im speziellen Privatheitsbruch. Dies betrifft Eingriffe in Artikel 10 und 13 GG und parallel dazu in die Vertraulichkeit und Integrität informationstechnischer Systeme. Demzufolge halten auch die neuen Regelungen an dieser dem Grundgesetz folgenden Differenzierung fest und sehen ein besonderes Anordnungsverfahren mit unabhängiger Kontrolle (durch Richter bzw. G 10-Kommission) nur bei solchen Eingriffen vor. Dies ist für die wirksame Aufgabenwahrnehmung der Nachrichtendienste essentiell. Speziell die Kooperation mit menschlichen Quellen könnte mit einer Verfahrensgestaltung, die nach Wahrnehmung der Betroffenen unübersehbare Zusatzrisiken des Bekanntwerdens einschlösse, weitgehend zum Erliegen kommen.

Zu § 9

§ 9 wird zur Grundnorm für den Einsatz nachrichtendienstlicher Mittel, der § 9a als allgemeine Schrankenregelung korrespondiert. Entsprechend wird die bisher in § 8 Absatz 2 Satz 1 enthaltene Erlaubnis zum Einsatz nachrichtendienstlicher Mittel nunmehr in § 9 Absatz 1 übernommen. Dessen Satz 2 schafft höhere Transparenz zu den einsetzbaren nachrichtendienstlichen Mitteln, indem die Aufzählung breiter gefasst wird und damit die gesamte Typik nachrichtendienstlicher Maßnahmen abbildet, ohne dabei einen abschließenden Katalog zu formulieren, der auch dem nachrichtendienstlichen Gegenüber eine abschließende Grundlage bieten würde, sich darauf einzustellen. Das Maß gesetzlicher Detailschärfe trägt mithin der geregelten Sachmaterie Rechnung (BVerfGE 133, 277 – Rn. 117). Die abschließende Benennung bleibt gleichwohl unter besonderer parlamentarischer Kontrolle durch das Parlamentarische Kontrollgremium (Absatz 2 Satz 2).

Absatz 1 Satz 2 Nummer 4 knüpft bei Internetrecherchen die Qualifikation als nachrichtendienstliches Mittel an die Ausnutzung

schutzwürdigen Vertrauens und folgt damit der Verfassungsrechtsprechung (BVerfGE 120, 274 – Rn. 310). Damit bleibt die im Internet weithin anonyme und flüchtige Kommunikation auch unter einem Benutzernamen („nickname“) grundsätzlich eine Datenerhebung aus offenen Quellen. Werden hingegen gezielt Vertrauensbeziehungen zu Extremisten aufgebaut und zur Informationsbeschaffung ausgenutzt, ist dies als nachrichtendienstliches Mittel zu qualifizieren. Auch unterhalb dieser Schwelle gilt – a fortiori – die Erlaubnis zur behördlichen Aufgabenwahrnehmung, die ihre Schranke ebenso entsprechend § 9a Absatz 1 und 5 findet.

Absatz 1 Satz 2 Nummer 7 schließt zur Feststellung des Aufenthaltsorts nicht nur eigene technische Maßnahmen (wie einen GPS-Sender), sondern auch wirkungsgleiche mittelbare Maßnahmen wie sogenannte „stille SMS“ („Ping-Verfahren“) ein, die eine technische Ortung ermöglichen (bei der „stillen SMS“ liegt kein Kommunikationsvorgang vor, jedenfalls wäre die Behörde selbst Teilnehmer, so dass die Maßnahme nicht in Artikel 10 GG eingreift). Buchstabe b) schließt auch die so genannte „Signals Intelligence (SIGINT)“ ein, wobei die hierunter auch zu subsumierende Fernmeldeaufklärung speziell in § 9c geregelt wird. Die Aufklärung technischer Signale bezieht auch den bisher in § 9 Absatz 4 BVerfSchG a.F. geregelten Einsatz eines „IMSI-Catchers“ zur Kennungsermittlung ein, für den künftig die allgemeine Befugnisnorm des neuen § 9 gilt, nachdem verfassungsgerichtlich geklärt ist, dass hierdurch nicht in Artikel 10 GG eingegriffen wird (BVerfG, Beschluss vom 22. August 2006 – 2BvR 1345/03 – Rn. 57 ff.). Nummer 7 b ist dabei nicht auf die Erfassung gesendeter elektronischer Signale beschränkt, sondern schließt ebenso das verdeckte Auslesen elektronischer Speicherungen ein, wobei der qualifizierte Sachverhalt des heimlichen Eingriffs in ein informationstechnisches System in § 9d speziell geregelt ist. Nummer 8 befugt zum Eingriff in das Individualrecht Besitz, beispielsweise um Gegenstände zur Untersuchung oder Dokumente zum Kopieren vorübergehend in Besitz zu nehmen.

Absatz 2 greift in einer differenzierteren Gliederung den bisherigen § 9 Absatz 1 Satz 1 BVerfSchG a.F. auf. Neu ist dabei in Nummer 2 Buchstabe b eine Schutzregelung zugunsten Betroffener, die entsprechend bereits im Polizeirecht etabliert ist

(z.B. in § 21 Absatz 3 Satz 3 BPolG). So ist u.U. eine verdeckte Ermittlung (also ohne den Zweck anzugeben) möglicherweise zwar nicht aus operativen Interessen des BfV notwendig, gleichwohl aber zum Schutz des Betroffenen angezeigt, da sich mit offenen Ermittlungen bei befragten Personen eine Negativ-Etikettierung der Zielperson verbinden kann.

Im Übrigen werden die Erkenntnisanforderungen nachrichtendienstlicher Frühaufklärung künftig auf „tatsächliche Anhaltspunkte“ bezogen. Dies entspricht der Einsatzschwelle der intensiveren Eingriffe nach § 3 Absatz 1 G 10 und vermeidet insoweit Wertungswidersprüche. Bei Gefahrerforschungsmaßnahmen ist generell unter Verhältnismäßigkeitserwägungen eine Gesamtschau angezeigt, die neben der Erkenntnisdichte u.a. auch die Risikodichte und andererseits ebenso den konkreten Eingriff und seine Wirkungen einbeziehen muss. Bei der Befugnisanwendung stehen folglich die jeweiligen Anforderungen an die prognostische Tatsachengrundlage in Abhängigkeit zur bezeichneten einzelfallbezogenen Gesamtschau.

Absatz 3 verdeutlicht einerseits mit den Nummern 1 und 3 den spezialgesetzlichen Gehalt der §§ 9c ff. Wie die bisherigen Regelungen in §§ 9a und b BVerfSchG a.F. sind spezielle Maßgaben zum Einsatz von Vertrauensleuten und Verdeckten Mitarbeitern dabei jedoch beschränkt auf die Aufklärung von Bestrebungen, da zur Spionageabwehr der staatliche Gegner andere Anforderungen an das Einsatzmittel stellt (BT-Drs. 18/4654, S. 26). In Nummer 1 werden von Buchstabe a) als Vertrauensleute weiterhin Privatpersonen (siehe § 9b Absatz 1 Satz 1) erfasst, die heimlich im Einsatz des BfV tätig sind, wohingegen Mitarbeiter – bei auf Dauer angelegter Legende – unter die Definition des Buchstabens b) fallen. Beide Legaldefinitionen entsprechenden dem geltenden Recht (in § 9a, § 9b)

Mit Nummer 2 wird eine spezielle Einsatzschwelle für die durchgehend längerfristige Observation von Personen neu eingeführt. Der Personenbezug grenzt die Maßnahme insbesondere von lokal-objektbezogenen, stationären Überwachungen ab, etwa zum Zugang zu bestimmten Örtlichkeiten. Das Erfordernis der durchgehenden Observation über mehr als 48 Stunden grenzt gegenüber kurzfristigeren

punktuell-temporären Maßnahmen ab, die mit der Begrenzung gezielter erfolgen und damit nicht gleichermaßen breit in Bereiche der Privatsphäre ohne Sozialbezug eingreifen. Eine durchgehende Personenobservation hat dagegen das – auch nicht öffentliche – Verhalten des Betroffenen über einen längeren geschlossenen Zeitraum zum Gegenstand und damit besonderes Eingriffsgewicht. Zugleich erfordert es hohen Ressourceneinsatz, da nicht lediglich eine punktuelle Verbleibsklärung oder eine stationäre Aufklärung an einem bestimmten Ort erfolgt, sondern der Person durchgehend, hier über 48 Stunden, zu folgen ist. Auch zur wirtschaftlichen Ressourcensteuerung wird dieser Aufwand auf Aufklärungsgegenstände von erheblicher Bedeutung beschränkt (Legaldefinition bereits in § 8a Absatz 2), wobei dieser Zweck auch die Erforschung der dazu erforderlichen Quellen, also etwa die Verlässlichkeit von Vertrauenspersonen, mit umfasst.

Absatz 4 trifft erstmals eine allgemeine gesetzliche Regelung zur Maßnahmerichtung einer Personenaufklärung mit nachrichtendienstlichen Mitteln. Geregelt ist dabei nicht die allgemeine Lageaufklärung, etwa der Beobachtung einer extremistischen Szene, die gemäß dem nachrichtendienstlichen Aufgabenprofil zunächst auch einen verdachtsgewinnenden Ansatz verfolgt, insoweit aber auch noch nicht gezielt personengerichtet ist. Werden Maßnahmen aber zur systematischen Sammlung von Informationen speziell zu einer Zielperson eingesetzt, erhält die Aufklärung einerseits personenbezogen eine neue Qualität und andererseits einen auf diese Person bezogenen Rechtfertigungsbedarf. Eine entsprechende Beschränkung auf gerechtfertigte Personenerforschung enthält Absatz 4 mit Tatbeständen einer spezifischen individuellen Nähe zur aufzuklärenden Gefahr. Satz 1 Nummer 2 regelt die Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel gegen Personen, die lediglich im Zusammenhang mit einer Person stehen, die selbst an Bestrebungen, Tätigkeiten oder Gefährdungen im Sinne der Nummer 1 beteiligt sind. Es muss sich dabei um einen sachlich qualifizierten Zusammenhang handeln, der eine individuelle Nähe zum Aufklärungsziel begründet, der eine aufklärungsgeeignete Maßnahmeanknüpfung eröffnet. Mit der Anforderung, dass durch die Maßnahme Erkenntnisse über die Bestrebungen, Tätigkeiten oder Gefährdungen gewonnen werden können, werden

insbesondere auch lediglich flüchtige und zufallsmäßige Kontakte ausgeschlossen. Die Erkenntnisgewinnung zu Quellen steht per se im Aufklärungszusammenhang des jeweiligen Phänomenbereichs.

Rechtsstaatliche Verwaltung erfordert generell zureichende Dokumentation wesentlicher Akte ihrer Aufgabenwahrnehmung, um die Nachvollziehbarkeit des Verwaltungshandelns für Kontrollzwecke zu gewährleisten. Absatz 5 bekräftigt dies gesetzlich durch spezielle Protokollierungspflichten für gewichtige nachrichtendienstliche Maßnahmen, die zur systematischen Aufklärung bestimmter Personen – direkt personenbezogen – eingesetzt werden. Als Ergänzungsnorm zur Einsatzbefugnis sind die Anwendungsbereiche von Befugnis und Verfahrensregelung jeweils kongruent, d.h. im Falle des Landesvollzugs (§ 9c bzw. Artikel 10-Gesetz) gilt die Protokollierungspflicht auch für die durchführende Landesverfassungsschutzbehörde.

Zweckbindungen für die Weiterverarbeitung der nachrichtendienstlich gewonnenen Daten erfolgen spezifisch konkretisiert im systematischen Zusammenhang der betreffenden Erhebungsbefugnisse in §§ 9c bis 9e. Für die verfassungsschutzinterne Sekundärnutzung von Informationen aus anderen, weniger intensiv eingreifenden nachrichtendienstlichen Mitteln bestehen hingegen keine speziellen Regelungen. Sekundärnutzungen sind im Aufgabenrahmen der Verfassungsschutzbehörden, der auf Aufklärung beschränkt ist und sich allein auf die herausragenden Schutzgüter des Verfassungsschutzes bezieht, immer schutzgutbezogen gleichwertig und auf weiter zu verfolgende Spurenansätze beschränkt. Nicht notwendig – unterhalb der Schwelle der speziell geregelten Intensiveingriffe – ist hingegen eine gleiche Qualifikation der Gefahrenlage über die Schutzgutgleichwertigkeit hinaus auch im Gefahrengrad, wie er Erhebungsvoraussetzung war (BVerfGE 141, 220, Rn. 289), etwa im Sinne einer Bedrohung von erheblicher Bedeutung (die in Absatz 3 Nummer 2 und § 9b Absatz 1 vorausgesetzt wird).

Die zweckändernde Übermittlung ist ebenfalls in §§ 9c bis 9e speziell geregelt und im Übrigen in § 19 allgemein auf Rechtsgüter beschränkt, die bei Anwendung des § 9 bereits der Erhebung zugrunde lagen oder die Erhebung der übermittelten Daten

ebenso rechtfertigen würden. Dies folgt aus der nachrichtendienstlichen Aufgabentypik, die nicht auf Beschaffung und Weitergabe von Rohdaten, sondern auf Gewinnung analytischer Erkenntnisse und Weitergabe von Analyseprodukten bezogen ist. Wenn im Einzelfall tatsächlich nicht analytische Erkenntnisse, sondern Informationen unmittelbar aus nachrichtendienstlichen Maßnahmen übermittelt werden, bleibt beispielsweise faktisch ausgeschlossen, dass dann das gesamte Rohdatenaufkommen einer durchgängig über mindestens 48 Stunden gegen eine Person durchgeführten Observation einer aufgabenfremden Behörde übermittelt wird. Der hypothetische Vergleichsfall ist insoweit die punktuelle Observation zur gezielten und hierauf bereits in der Erhebung begrenzten Gewinnung der übermittelten Daten (keine längerfristige Observation). Dabei handelt es sich um einen eher geringen Eingriff (BVerfGE 141, 220 – Rn. 151). Für außergewöhnliche – nicht vorhersehbare und auch nicht praxisrelevant konkreter typisierbare – Sonderfälle enthält § 23 Nummer 1 eine besondere, individualschützende Übermittlungsschranke.

Zu § 9a

Der neue §9a systematisiert die bisher verstreut im Bundesverfassungsschutzgesetz und teils auch nur dem Artikel 10-Gesetz (G10) geregelten sowie verfassungsgerichtlich entwickelten Schranken zum Einsatz nachrichtendienstlicher Mittel.

Soweit die besondere Erlaubnis zum Einsatz nachrichtendienstlicher Mittel nach § 9 mit allgemeinen Rechtsvorschriften kollidiert, klären insbesondere Absatz 1 und 5 in Übernahme der bisherigen Regelungen (bisheriger § 8 Absatz 2 Sätze 2 und 3) den jeweiligen Anwendungsvorrang. Der Rechtfertigungsgehalt der allgemeinen Befugnis des § 9 Absatz 1 Satz 1 findet danach folgende Schranken:

- Schutznormen von Individualrechten gehen der allgemeinen Einsatzerlaubnis generell vor (Absatz 1 Satz 2; bisher § 8 Absatz 2 Satz 2 und § 9a Absatz 2 Satz 3 Nummer 1 BVerfSchG a.F.), soweit keine besonderen Eingriffsbefugnisse bestehen. Solche Befugnisse bestehen etwa für Schutznormen des persönlichen Lebens- und Geheimbereichs nach Maßgabe von § 9 Absatz 1

Satz 2 und §§ 9b bis 9e, zum Besitzrecht nach Maßgabe des § 9 Absatz 2 Satz 1 Nummer 9.

- Bei Kollision mit anderen rechtlich geschützten öffentlichen Interessen besteht ein absoluter Vorrang der Schutznormen der Rechtspflege und der parlamentarischen Kontrolle, die unbedingt zu beachten sind, was der neue § 9a Absatz 1 Satz 1 nunmehr ausdrücklich klarstellt. Neu ist zudem die Klarstellung in Satz 3, dass der Rechtfertigungsgehalt der Erlaubnis zum Einsatz nachrichtendienstlicher Mittel nicht nur als Eingriffsbefugnis gegenüber dem Betroffenen, sondern ebenso gegenüber anderen rechtlich geschützten öffentlichen Interessen bereits durch das Erfordernis der Erforderlichkeit begrenzt ist. Im Übrigen bleibt es beim Abwägungserfordernis, das bisher in § 8 Absatz 2 Satz 3, § 9a Absatz 2 Satz 3 Nummer 3 BVerfSchG a.F. geregelt war und nunmehr in § 9a Absatz 5 Satz 1 aufgenommen ist, wo ergänzend in Sätzen 3 und 4 besondere Maßgaben zur Aufklärung bei Berufsgeheimnisträgern, soweit sie nicht bereits unter den weitergehenden Schutz nach Absatz 2 Satz 1 Nummer 2 fallen, getroffen werden.

Wesentliche inhaltliche Neuerung ist, dass der Schutz des Kernbereichs privater Lebensgestaltung sowie von bestimmten Berufsgeheimnisträgern, der bislang nur für Maßnahmen nach dem Artikel 10-Gesetz galt (§§ 3a, 3b G10), künftig nach Absatz 2 bis 4 umfassend gilt. Absatz 3 Satz 1 stellt klar, dass die Durchführung einer Maßnahme – sobald dies ohne Gefährdung eingesetzter Personen möglich ist – solange zu unterbrechen ist, wie Anhaltspunkte dafür bestehen, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst werden. Fallen diese Anhaltspunkte weg, entfällt damit lediglich der Unterbrechungsgrund. Ob die Wiederaufnahme der Maßnahme zulässig ist, hängt davon ob, ob deren jeweiligen Voraussetzungen weiter vorliegen. Die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung entzieht höchstpersönliche Vorgänge pauschal der Ausforschung durch die Nachrichtendienste. Dementgegen ist die Kommunikation unmittelbar über Sachverhalte mit Sozialbezug, wie Straftaten oder extremistische Bestrebungen, hiervon nicht geschützt, selbst wenn sie zugleich Höchstpersönliches zum Gegenstand hat (BVerfGE 141, 220 – Rn. 119 ff.).

Für heimliche Eingriffe in informationstechnische Systeme nach § 9d und Maßnahmen der Wohnraumüberwachung nach § 9e Absatz 1 kommt als besondere Verfahrenssicherung entsprechend dem Artikel 10-Gesetz hinzu, dass die Kontrolle durch die G 10-Kommission unabhängig von einer Vorlage durch das BfV nach § 9a Absatz 4 Satz 1 ist, da sie auch eigeninitiativ von Amts wegen erfolgt. Sie dient somit nicht lediglich zum Herausfiltern der vom BfV erkannten Zweifelsfälle, sondern zur umfassenden Rechtmäßigkeitskontrolle (vgl. BVerfG a.a.O. Rn.200 und 204). Dies gewährleistet sogar weitergehend als die strafprozessuale Vorlagepflicht nach § 100d Absatz 4 Satz 5 StPO, dass die Konkretisierung des – als Rechtsbegriff unbestimmten – Kernbereichs privater Lebensgestaltung im Wechselspiel von Anwendungspraxis und gerichtsentsprechender Kontrolle erfolgt (hierzu BVerfG a.a.O. Rn.94) und damit die Heimlichkeit der Maßnahme nicht etwa verdeckt bleibenden Fehlentwicklungen bei der Norminterpretation in der Verwaltung Vorschub leistet. Diese Gewährleistungsfunktion wird mit der Kompetenz der G 10-Kommission zu einzelfallunabhängigen Strukturkontrollen in der Zusammenschau der Verwaltungspraxis sogar effektiver erreicht als mit einer Vorabentscheidung der isolierten Einzelfälle. Unbeschadet dessen ist eine § 100d Absatz 4 Satz 5 StPO entsprechende Vorlagepflicht (erweitert auch auf die Auswertung von Informationen aus einer Online-Durchsuchung) in § 9 Absatz 4 Satz 1 Nummer 2 aufgenommen, die die unabhängige Klärung von Zweifelsfällen auch auf der Verwertungsebene sicherstellt. Handelt es sich nicht lediglich um einen Zweifelsfall, sondern gelangt bereits das BfV zur Qualifikation als Kernbereichsverletzung, sind die Daten unverzüglich zu löschen, ohne dass dazu noch eine unabhängige Prüfung weiterer Verarbeitung erfolgen muss (vgl. auch § 100d Absatz 3 Satz 2 StPO).

Der Anwendungsbereich der Schrankenregelung ist als Gegennorm komplementär zu den Befugnisnormen des Bundesverfassungsschutzgesetzes, erstreckt sich bei § 9c Absatz 2 also auch auf den Landesvollzug. Praktische Bedeutung hat dies für die Anwendung des § 9a Absatz 6. Für die Durchführung des Artikel 10-Gesetzes – durch die Verfassungsschutzbehörden des Bundes und der Länder – gelten die dort getroffenen speziellen Regelungen, insbesondere §§ 3a, 3b G 10, die materiell den neuen

Regelungen des Bundesverfassungsschutzgesetzes entsprechen.

Absatz 6 regelt die notwendige Maßnahmeeinstellung, wenn die Fortsetzung nach dem erreichten Erkenntnisstand nicht geeignet ist, weiter zur bezweckten Aufklärung beizutragen. Besteht insoweit Ungewissheit, handelt es sich um die typische Ausgangslage nachrichtendienstlicher Aufklärung, d.h. die Fortsetzung liegt im Verwaltungsermessen, das einerseits Erkenntniserwartung und andererseits Aufwände und Eingriffsgewicht in einen abwägenden Ausgleich bringen muss.

Zu § 9b

Die Regelung übernimmt die erst in 2015 in das Bundesverfassungsschutzgesetz eingefügten §§ 9a, b vollinhaltlich. Die wiederum beibehaltene Beschränkung des Anwendungsbereichs auf die dauerhafte Aufklärung von Bestrebungen folgt dabei bereits aus § 9 Absatz 3 Nummer 1. Eine spezielle Verarbeitungsregelung erübrigt sich aus den bereits zu § 9 (siehe dortige Begründung am Ende) ausgeführten Erwägungen.

Im Übrigen werden die Regelungen zu Vertrauensleuten sowie Verdeckten Ermittlern dem systematisierenden Konzept des Entwurfs folgend in einem Paragraphen integriert, da sie weitgehend inhaltsgleich sind. Selbstverständlich besteht zwischen den Vertrauensleuten als Szeneangehörigen und den Verdeckten Mitarbeitern als verfassungstreuen Beschäftigten des Bundes im Hinblick auf die Glaub- und Vertrauenswürdigkeit ein erhebliches Gefälle. Dem trägt auch § 9b Absatz 2 Rechnung. Die Absätze 3 und 4 betreffen dagegen Folgen, die sich aus dem Zurechnungszusammenhang der Handlung zu den Schutzzwecken der Aufklärungsaufgabe ergeben, der seinerseits – gleichermaßen für Vertrauensleute wie für Verdeckte Ermittler – aus dem Einsatz resultiert.

§ 9b Absatz 2 Satz 1 BVerfSchG a.F. sah für die Verpflichtung von Vertrauensleuten eine Entscheidung auch durch einen Vertreter vor. Damit war nicht eine Abwesenheitsvertretung gemeint (die auch bei persönlicher Entscheidungszuständigkeit des Behördenleiters gegeben wäre, vgl. BT-Drs. 18/5415, S. 11), sondern Entscheidungsdelegation. Nach dem Normzweck ist dabei allerdings in jedem Fall eine hohe Funktionsebene zu wahren, der eine Delegation auf einen Gruppenleiter/Unterabteilungsleiter

nicht mehr genügt. Im Interesse der Normenklarheit wird die Delegation nunmehr im neuen § 9b Absatz 2 gesetzlich ausdrücklich auf der Abteilungsleiterebene abgeriegelt.

In Absatz 3 Satz 4 wird an der bisherigen Verdachtsschwelle der „zureichenden" Anhaltspunkte festgehalten, da es hier speziell um einen Straftatenverdacht geht und die Regelung sich dabei an die Strafprozessordnung (insbes. § 152 Absatz 2 StPO) anlehnt. In Absatz 4 ist mit Satz 5 eine neue Regelung zum Schutz des Betroffenen oder seines Einsatzes bei Einstellungssachen aufgenommen worden.

Absatz 5 Satz 1 trägt der besonderen Geheimhaltungsbedürftigkeit der Verbindung des Betroffenen zum BfV Rechnung. Diese Geheimhaltung ist grundlegend für den Schutz des Betroffenen – insbesondere vor Racheakten aus der Szene, in der er zur Aufklärung tätig war oder ist – wie auch für die Funktionsfähigkeit nachrichtendienstlicher Aufklärung beim Schutz der herausragenden Rechtsgüter nach § 1 Absatz 1 BVerfSchG (vgl. BVerfGE 146, 1 – Rn. 112 ff.). Die üblichen Verfahren der Aussagegenehmigung sind ungeeignet, diesem speziellen Geheimhaltungsbedürfnis Rechnung zu tragen, da mit dem Hinweis auf die Erforderlichkeit einer Aussagegenehmigung bereits die Vertraulichkeit gebrochen wäre. Deshalb enthält Absatz 5 Satz 1 insoweit ein Beweisthemaverbot. Satz 2 führt eine korrespondierende Prüfpflicht des BfV ein, wenn im konkreten Fall die Risiken, die in der Regel Geheimhaltung erfordern, auszuschließen sind. Hierdurch wird ein angemessener Interessenausgleich zur Wahrung der Rechte anderer Verfahrensbeteiligter, insbesondere auch des Anspruchs auf ein faires und rechtsstaatliches Strafverfahren und des parlamentarischen Informationsinteresses im Sinne des o.g. Urteils (BVerfGE 146, 1 – Rn. 124), gewährleistet. Eine entsprechende Prüfung kann von der verfahrensführenden Stelle angestoßen werden. Das BfV hat dem Betroffenen eine Aussagegenehmigung zu erteilen, wenn eine Stellung als Vertrauensperson besteht und die Voraussetzungen von Satz 2 vorliegen. Aus der Ablehnung einer Genehmigung kann im Umkehrschluss nicht gefolgert werden, dass der Betroffene eine Vertrauensperson ist oder gewesen ist. Nach Satz 4 erfolgt das Prüfverfahren zur Erteilung einer Aussagegenehmigung auf Anfrage auch in Fällen der Landesbehörden für den Verfassungsschutz über das BfV als

Zentralstelle. Hiermit wird sichergestellt, dass das Prüfverfahren unabhängig davon, welche Verfassungsschutzbehörde des Bundes oder der Länder eine Vertrauensperson möglicherweise eingesetzt hat, durchgeführt werden kann.

Zu §9c

Die Regelung enthält die Erhebungsbefugnisse, die das Post- und Fernmeldegeheimnis beschränken. Im Interesse der Normenklarheit nimmt dazu Absatz 1 eine Verweisung auf das Artikel 10-Gesetz in das Bundesverfassungsschutzgesetz auf. Ergänzend zu Absatz 2, der die Befugnis zum Eingriff in die Grundrechte des Betroffenen enthält, enthält § 8a Absatz 2 eine komplementäre Mitwirkungspflicht der an das Post- bzw. Fernmeldegeheimnis gebundenen Unternehmen.

Entsprechend der gestuften Eingriffsintensität und der betreffenden Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 141, 220 – Rn. 107) wird in den materiellen Einsatzschwellen weiterhin zwischen der Erhebung von einerseits Inhalten (Absatz 1) und andererseits Umständen (Absatz 2) der Verkehre unterschieden, dabei jedoch in Absatz 2 Satz 2 die Nutzung vorsorglich gespeicherter Daten der Inhaltsüberwachung gleichgestellt. Im Übrigen beschränkt Absatz 2 die Verkehrsdatenerhebung auf Bedrohungen von erheblicher Bedeutung. Das Fernmeldegeheimnis wird hierdurch beschränkt, die Datenerhebung komplementär erlaubt. Die Mitwirkungspflicht der Unternehmen folgt aus der ergänzenden Regelung in § 8a Absatz 2 Satz 1.

Für das Anordnungs- und Kontrollverfahren gilt nach Absatz 3 – wie bisher auch gem. § 8b BVerfSchG a.F. – einheitlich das Artikel 10-Gesetz. Neu ist in Nummer 1 eine ausdrückliche Regelung zur Funkzellenabfrage, die neuerer Gesetzgebungspraxis zur speziellen Regelung folgt (vgl. etwa § 52 Absatz 3 Satz 2 BKAG oder § 100g Absatz 3 StPO). Mit Nummer 2 wird die Höchstfrist der Anordnung bei Verkehrsdaten entsprechend dem längerfristigen Strukturaufklärungsansatz der Verfassungsschutzbehörden auf 6 Monate verlängert. Für die Durchführung der Anordnung setzt § 9 Absatz 6 die einzelfallbezogene Schranke.

Zu § 9d

Die Befugnis erlaubt Eingriffe in die Vertraulichkeit und Integrität informationstechnischer Systeme. Deren Schutz ist besondere Ausprägung des allgemeinen Persönlichkeitsrechts, die einerseits der rechtstatsächlichen Bedeutung einer Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und andererseits der Eingriffsbreite eines Zugriffs nicht lediglich auf einzelne Kommunikationsvorgänge oder gespeicherte Daten, sondern auf das informationstechnische System insgesamt Rechnung trägt (BVerfGE 120, 274, Rn. 201). Ein Zugriff auf eine derart umfassende Datenverarbeitung ermöglicht potenziell, in wesentliche Teile der Lebensgestaltung einer Person Einblick zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (a.a.O. Rn. 203, 232) und geht dadurch über Datenerhebungen mit punktuellem Bezug zu einem bestimmten Lebensbereich, vor denen das Recht auf informationelle Selbstbestimmung schützt, hinaus (Rn. 202). Dem korrespondieren besonders enge Eingriffsvoraussetzungen. Die Befugnisausgestaltung folgt der jüngeren Verfassungsrechtsprechung, in der der Schutz der Unverletzlichkeit der Wohnung und der Vertraulichkeit informationstechnischer Systeme normativ synchronisiert werden (BVerfGE 141, 220 – Rn. 192, 210 a.E.; ferner 105, 115, 238; das Gericht nutzt das Urteil erklärtermaßen auch, um seine vorangegangene Rechtsprechung fortzuentwickeln, Rn. 292). Dem war der Bundesgesetzgeber zuletzt bereits mit den kongruenten Voraussetzungen in §§ 100b, c StPO gefolgt.

Die materielle Befugnisschwelle orientiert sich hier somit an Artikel 13 Absatz 4 GG. Demgemäß wird zur Gefahrenqualifikation zusätzlich das Kriterium der „dringenden“ Gefahr aufgenommen. Hieraus resultieren qualifizierte Rechtsgutsanforderungen und erhöhte Anforderungen an die Erkenntnisdichte (und resultierende Prognosewahrscheinlichkeit). Diese Qualifikationsmerkmale werden im Tatbestand der Befugnis konkretisierend umgesetzt, einerseits mit dem Katalog qualifizierter Schutzgüter, andererseits mit den qualifizierten Erkenntnisanforderungen „hinreichender“ Anhaltspunkte. Die Qualifikation als „hinreichend“ schließt zugleich eine einzelfallbezogene Relation zwischen der Erkenntnislage (die die Gefahrenprognose trägt) und dem Maßnahmegewicht ein, das auch je nach Maßnahmegestaltung differieren kann (vgl. Absatz 7).

Unter dem in Absatz 1 Satz 1 ausdrücklich aufgenommenen Aufgabenrahmen, handelt es sich bei Satz 2 Nummern 2 und auch 3 im Ergebnis um Spezialfälle der Nummer 1. Diese Ergänzung um die Nummern 2 und 3 erscheint gleichwohl im Interesse einer Gesamtkonsistenz der Norm sinnvoll, speziell um Rechtsunsicherheit für den Fall zu vermeiden, dass die Universalrechtsgüter der Nummer 1 in einer Tatmodalität angegriffen werden, die sich unmittelbar gegen ein Schutzgut der Nummer 3 richtet, hierbei aber mit der Zweckrichtung der Tat (im funktionalen Handlungskontext von Bedrohungen nach § 3 Absatz 1) zugleich ein Schutzgut nach Nummer 1 gefährdet. Auch dieser Sachverhalt ist tatbestandlich, was ohne Nummer 3 (ähnlich auch bei Nummer 2) unklar sein könnte. Dabei gewährleistet der Bezug auf § 3 Absatz 1, dass die Aufklärungsrichtung die verfassungsschutzrelevante Bedrohung ist, nicht isoliert die Gefährdung von Individualrechten (deren Schutz polizeiliche Aufgabe ist).

Der in Absatz 1 Satz 2 Nummer 2 verwendete Begriff der lebenswichtigen Einrichtungen ist mit § 1 Absatz 5 Satz 1 SÜG in die Rechtsordnung eingeführt. Spezielle Sektoren sind dazu in der Sicherheitsüberprüfungsfeststellungsverordnung aufgeführt, die den Bereich zwar nicht abschließend beschreiben (die Aufnahme in die SÜFV folgt Erfordernissen des personellen Sabotageschutzes vor „Innentätern“), aber ein konkretisierendes Leitbild zum Bereich auch für die Anwendung des § 9d vermitteln.

Die Regelung kombiniert die allgemeine, auf Gefahren für Rechtsgüter bezogene Verdachtsklärung (Absatz 1 Satz 2) mit einer konkretisierenden Anknüpfung an bestimmte Straftatbestände (Absatz 1 Satz 3), was nach der Praxiserfahrung der Durchführung des § 3 Absatz 1 G 10 zusätzliche Rechtssicherheit für spezielle – praxisrelevante – Sachverhalte herstellt. Die Konkretisierung beschränkt sich dabei auf Satz 2 Nummer 1, da bei den dort bezeichneten Universalrechtsgütern die Gefährdungsqualifikation grundsätzlich schwieriger ist als insbesondere bei den Individualgefährdungen nach Satz 2 Nummer 3.

Zu den Rechtsgütern des Satzes 2 Nummer 1 enthält § 4 Absatz 1 Satz 1 Buchstaben a) und b) eine Definition. Weitergehende Konkretisierungen hat die Rechtsprechung zu entsprechenden

Normen geleistet. So schließt der Schutz der Funktionsfähigkeit der staatlichen Einrichtungen vor erheblichen Beeinträchtigungen den Schutz vor Einwirkungen durch Gewalt und Drohungen mit Gewalt auf die Wahrnehmung staatlicher Funktionen ein, wobei z.B. bereits die Anwesenheit möglicher Helfer terroristischer Gewalttäter die Fähigkeit des Staates, sich nach innen und nach außen gegen Angriffe und Störungen zur Wehr zu setzen, beeinträchtigt und somit seine Sicherheit gefährdet (BVerwGE 123, 114/120 – Rn. 21). Umfasst ist ebenso der Fall, dass die Bestrebungen geeignet sind, das Vertrauen der Bevölkerung zu erschüttern, vor gewaltsamen Einwirkungen in ihrem Staat geschützt zu sein (BGH, Beschluss vom 6.4.2017 – 3 StR 326/16 -, Rn. 22; Gesetzesbegründung zu § 89a StGB, BT-Drs. 16/12428, S. 14). Im Ergebnis ist die Innere Sicherheit auch ein Zustand des friedlichen und gewaltfreien Zusammenlebens der Bevölkerung (Roth, in: Schenke/Graulich Ruthig, §§ 3, 4 BVerfSchG Rn. 59).

Staatsschutzdelikte sind besonders geeignet, Gefährdungstatbestände dieser Rechtsgüter zu bezeichnen. Deshalb enthält Absatz 1 Satz 3 eine Auswahl spezifisch praxisrelevanter Delikte, um insoweit eine besonders klare Handlungsgrundlage zu schaffen. Hätte der Staat nicht die Mittel, solche Sachverhalte aufzuklären, um schwere Staatsschutzdelikte zu verhindern, wären die Grundlagen staatlicher Funktionsfähigkeit gefährdet und insbesondere das Vertrauen der Bürger erschüttert, dass sie in Deutschland individuell vor Terrorakten und ihr Staat – als demokratische Organisation grundlegender Kollektivanliegen – vor Ausforschung und Angriffen fremder Mächte geschützt sind. Der Katalog geht insofern über § 100b StPO hinaus, als § 129 Absatz 5 StGB ohne Beschränkung auf dessen Satz 3 aufgenommen ist (stattdessen mit der bereichsspezifischen Qualifikation der Ausrichtung auf politisch motivierte Gewalttaten). Anders als im Bereich der Strafverfolgung können hier für Zwecke des Rechtsgüterschutzes über den Strafrahmen hinaus weitere Gesichtspunkte zur Qualifikation eines besonderen Gewichts der Gefahr herangezogen werden (so bereits zu § 3 Absatz 1 Satz 1 Nummer 8 G 10: BT-Drs. 18/4654, S. 40). Vorliegend ist maßgeblich, dass bei besonders schweren Fällen organisiert betriebener politisch motivierter Kriminalität ebenfalls eine dringende Gefahr für die Sicherheit des Staates besteht. Dies ist generell bei organisiert betriebenen, politisch

motivierten Gewalttaten anzunehmen, weil hierin zugleich ein massiver Angriff auf Grundlagen der Demokratie liegt, die auf friedlicher Teilhabe beruht und nur in diesem Friedensrahmen auch funktionsfähig ist.

Zugleich bieten die Katalogtaten einen wertenden Anhalt zur wertenden Ausfüllung der Anforderung der „dringenden" Gefahr (Artikel 13 Absatz 4 GG). Unter Berücksichtigung von Satz 3 Nummer 1 ist beispielsweise auch bei Proliferationsaktivitäten oder elektronischen Sabotageangriffen fremder Mächte von einer „dringenden Gefahr" nach Satz 2 Nummer 1 auszugehen. Gleiches gilt unter Berücksichtigung von Satz 3 Nummer 3 bei besonders schweren Fällen politisch motivierter Kriminalität unabhängig davon, ob hinreichende Anhaltspunkte für ein Vorgehen einer Vereinigung bestehen. Solche besonders schweren Fälle können beispielsweise vorliegen, wenn die Taten im Besonderen als Angriff auf die grundgesetzliche Werteordnung typisiert sind, so etwa, wenn sie mit rassistischem Ansatz das friedliche Zusammenleben der unterschiedlichen Bevölkerungsgruppen in Frage stellen, weil sie einem Teil der Bevölkerung das Recht absprechen, gleichberechtigt am gesellschaftlichen Leben teilzunehmen, und damit geeignet sind, den öffentlichen Frieden qualifiziert zu stören.

Angesichts der hohen Einsatzschwelle für Eingriffe in die Vertraulichkeit und Integrität informationstechnischer Systeme ist bei Delikten, die eher Vorbereitungscharakter besitzen, nicht bereits das Planungsstadium als eingriffsrechtfertigend erfasst, weshalb solche Delikte gesondert in Nummer 3 aufgenommen sind.

Der Anwendungsbereich dieser besonderen Befugnis mit besonders engen Voraussetzungen ist kongruent zum besonderen Schutzbereich der Vertraulichkeit und Integrität informationstechnischer Systeme, der eröffnet ist, soweit die anderen Freiheitsgewährleistungen, wie insbesondere der Schutz des Telekommunikationsgeheimnisses aus Artikel10 Absatz1 GG, der Schutz der Unverletzlichkeit der Wohnung gemäß Art.13 Absatz1 GG sowie das Recht auf informationelle Selbstbestimmung keinen oder keinen hinreichenden Schutz gewähren. So ist zum Beispiel Artikel10 Absatz1 GG alleiniger grundrechtlicher Maßstab für die Beurteilung einer Ermächtigung

zu einer „Quellen-TKÜ“, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt (BVerfG vom 06.09.2016 – 2 BvR 1454/13 – Rn.41). Dieser Eingriff wird mithin nicht in § 9d geregelt, sondern im Artikel 10-Gesetz (spezielle Regelung nun nach Artikel 5 Nummer 6 in § 11 Absatz 1a G 10), so dass hierfür nicht der engere Deliktskatalog des neuen § 9d Absatz 1 Satz 3 gilt, sondern der weitergefasste Deliktskatlog des § 3 Absatz 1 G 10.

Absatz 2 und 3 enthalten Maßgaben zur Erforderlichkeit und Maßnahmerichtung.

Nach Absatz 4 kommen die Verfahrenssicherungen für Anordnung und Kontrolle des Artikel 10-Gesetzes zur Anwendung, insbesondere also die Kontrolle durch die unabhängige G 10-Kommission, die gerichtlichem Rechtsschutz gleichwertigen Schutz bietet (BVerfGE 143, 1 – Rn. 46), insbesondere auch rechtlich bindend entscheidet, dabei aber zugleich – weitergehend als ein Gericht – Kontrolle von Amts wegen auch selbst initiiert, also auch systematische Strukturkontrollen durchführt. Im Falle einer Eilanordnung muss nach Absatz 4 Satz 3 die Bestätigung durch den Vorsitzenden der G 10-Kommission oder seinen Stellvertreter binnen dreier Tage erfolgen (und die Bestätigung durch die Kommission insgesamt unverzüglich nachgeholt werden). Dies entspricht der Regelung für das gerichtliche Verfahren nach § 9e Absatz 3 Satz 4 und trägt der vergleichbaren Eingriffsbedeutung auch in entsprechenden zeitlichen Begrenzungen von Eilanordnungen Rechnung.

Die Zweckänderungsregelung in Absatz 5 beachtet die Rechtsgutsgleichwertigkeit und verweist für die Strafverfolgung in Nummer 2 Buchstabe b auf den Katalog der entsprechenden strafprozessualen Befugnis. Den qualifizierten Erkenntnisanforderungen der Sekundärnutzung von personenbezogenen Daten aus Eingriffen in Artikel 13 GG oder in die Vertraulichkeit informationstechnischer Systeme (BVerfGE 141, 220 – Rn. 283, 291) wird durch Parallelisierung mit den Verdachtsanforderungen des Erhebungseingriffs Rechnung getragen. Nummer 1 regelt die Verarbeitung (nach neuer Datenschutzterminologie also auch die Nutzung) in sachlicher Zuständigkeit der Verfassungsschutzbehörden, einschließlich der

Übermittlung entsprechend ihrer örtlichen Zuständigkeit. Eine Übermittlung an Stellen außerhalb des Verfassungsschutzverbundes ist dagegen in Nummer 2 geregelt. Die Regelung enthält eine doppelte Beschränkung. Zum einen erweitert sie die Zweckbindung über die erhobenen Informationen hinaus auch auf Erkenntnisse, die aus deren Verarbeitung gewonnen werden (allerdings nicht auf Folgeermittlungen oder hybride Erkenntnisse unter Einbezug weiterer Quellen). Zum anderen ermöglicht sie zugleich allein die Übermittlung solcher Erkenntnisse, also schließt eine Übermittlung von noch nicht ausgewerteten bzw. bewerteten Rohdaten aus. Demgemäß muss der Übermittlung eine konkrete Erforderlichkeitsprüfung vorausgehen, die Erforderlichkeit kann nicht bereits dem Erhebungsgegenstand entnommen werden.

Während Absätze 1 bis 5 Ausprägungen der Vertraulichkeit informationstechnischer Systeme sind, schützt Absatz 6 die Integrität des Systems. Die Regelung kommt folglich entsprechend zur Anwendung, wenn ein technischer Eingriff zwar nicht das System als solches überwacht, sondern die Erhebung wie bei der Quellen-TKÜ auf eng umgrenzte Daten beschränkt bleibt, dazu aber in die Integrität des Systems eingreifen muss (§ 11 Absatz 1a Satz 2 ff. G 10).

Absatz 7 trifft eine spezielle Regelung für den Fall, dass keine laufende Überwachung durchgeführt wird, sondern lediglich eine einmalige Momentaufnahme in Form eines Systemabbildes (Image) erfolgt. Der begrenzten Eingriffswirkung (BVerfGE 120, 274, Rn. 234 ff.) wird mit dazu adäquaten Erkenntnisanforderungen Rechnung getragen. Die in Absatz 1 aufgenommene Qualifikation vorliegender Erkenntnis als „hinreichend“ schließt eine einzelfallbezogene Relation zwischen der Erkenntnislage (die die Gefahrenprognose trägt) und dem Maßnahmegewicht ein. Dem minderen Maßnahmegewicht folgend (das spezifische Informationspotenzial aus der laufenden Überwachung der Systemnutzung wird hier nicht eröffnet), soll hier bereits der nachrichtendienstliche Anfangsverdacht „tatsächlicher Anhaltspunkte“ hinreichen. Bei den rechtsgutsqualifizierenden und verfahrensbezogenen Anforderungen bleibt es indes auch für das Systemabbild bei den Voraussetzungen der Überwachungsbefugnis.

Der praktische Bedarf für eine spezielle Regelung ergibt sich besonders für die Aufklärung von Cyber-Angriffen fremder Mächte. Das BfV ist nicht zuständig für die allgemeine Aufklärung von Cyberangriffen, vielmehr ist seine Aufgabe auf die Aufklärung von Bestrebungen und Tätigkeiten nach § 3 Absatz 1 BVerfSchG beschränkt, wobei bei Cyberangriffen Tätigkeiten fremder Mächte nach Nummer 2 im Vordergrund stehen. Die Attribution des Angriffs steht dabei am Ende der Aufklärung, regelmäßig nicht an deren Anfang. Zureichende Anhaltspunkte für die Arbeitshypothese der Tätigkeit eines fremden Nachrichtendienstes sind typischerweise den konkret festgestellten Umständen oder Zielen des Schadsoftwareeinsatzes oder auch der eingesetzten Software zu entnehmen (die unter Einbezug allgemeiner nachrichtendienstlicher Erkenntnisse analysiert werden). Gerade in Fällen neuer Vorgehensmuster und Tatmittel können diese Ableitungen zunächst jedoch vage bleiben. Für eine Aufklärung muss hier bereits eine womöglich entferntere Möglichkeit genügen, dass der Cyber-Angriff von einem fremden Nachrichtendienst ausgeht. Ein Aufklärungsansatz wäre hier, von einem erkannten Angriffs-Server ein Systemabbild zu gewinnen, um durch dessen Auswertung Rückschlüsse z.B. auf Angriffsstruktur und -ziele zu ziehen, was nach dem konturierten Tatprofil gegebenenfalls zur Verdichtung der Annahme führen kann, dass ein ausländischer Nachrichtendienst tätig ist.

Als Angriffs-Server können auch Server genutzt werden, die im Übrigen in keinem Zusammenhang mit fremden Nachrichtendiensten stehen, z.B. Einrichtungen kommerzieller Betreiber. In diesem Fall kann das Systemabbild auch ohne systeminvasive Maßnahme gewonnen werden, indem das Unternehmen nach § 8a Absatz 2 (i.V.m. § 9d Absatz 7) zur Übermittlung des Systemabbildes verpflichtet wird. Hiervon unberührt bleibt die Befugnis nach § 8a Absatz 2 BVerfSchG in Verbindung mit § 15 Absatz 5 Satz 4 TMG, sofern die danach zu übermittelnden Nutzungsdaten für den Aufklärungszweck reichen.

Zu § 9e

Die Befugnis deckt sich in der Einsatzschwelle des Absatzes 1 mit § 9d, der seinerseits – jüngerer Verfassungsrechtsprechung folgend – bereits am Maßstab des Artikels 13 Absatz 4 GG entwickelt ist (s.o.). Zusätzlich enthalten ist der spezifisch zu Wohnungen

gebotene Schutz des Kernbereichs privater Lebensgestaltung bereits bei der situativen Würdigung des Eingriffssachverhalts.

Für die Übermittlung zur Strafverfolgung erfolgt in Absatz 1 Satz 2 ein Ausschluss von Videorohdaten angesichts der in Artikel 13 Absatz 3 GG enthaltenen Beschränkung von Strafermittlungen auf eine akustische Wohnraumüberwachung. Die Verwendungsbeschränkung betrifft nicht Erkenntnisse aus der Videoüberwachung. Sie steht auch nicht einer Weitergabe einzelner Bilder entgegen, die bei Auswertung von Videoaufzeichnungen Sachverhalte besonderen Sozialbezugs punktuell festhalten und belegen, etwa die Anwesenheit weiterer Personen, die im Verdacht stehen, gemeinschaftlich mit dem Hauptbetroffenen Taten zu begehen. Zudem ist die Übermittlung möglich, soweit unmittelbar eine Tatbegehung aufgezeichnet ist. Die Beschränkung technischer Mittel in Artikel 13 Absatz 3 GG bezweckt, privatheitsschonend die Sacherforschung zu begrenzen, aber nicht Beweismittel auszuschließen. Dazu trifft der letzte Halbsatz eine Rückausnahme von der Maßgaberegelung zu Bildaufzeichnungen, wonach auch solche Aufzeichnungen, wenn sie die Straftatenbegehung selbst dokumentieren, nach § 9d Absatz 5 – also in den Fällen von Straftaten nach § 100b Absatz 1 StPO – übermittelt werden können.

Absatz 2 regelt die Maßnahmerichtung.

Absatz 3 verweist zum Anordnungs- und Kontrollverfahren weitgehend auf das Artikel 10-Gesetz. Eine Modifikation ergibt sich daraus, dass Artikel 13 Absatz 4 GG ausdrücklich eine „richterliche“ Entscheidung verlangt. Die G 10-Kommission bietet zwar gerichtlicher Kontrolle gleichwertigen Rechtsschutz, ist jedoch kein Gericht (BVerfGE 143, 1 – Rn. 41, 46). In Angleichung an § 50 Absatz 1 Nummer 4 VwGO wird deshalb hier die Zuständigkeit des Bundesverwaltungsgerichts bestimmt (und § 50 VwGO komplementär angepasst, Artikel 8). Angesichts der gegenständlichen Besonderheit dieses Feststellungsverfahrens wird es in Absatz 4 besonders geregelt, dies orientiert an der bewährten Verfahrenspraxis der G 10-Kommission unter Anlehnung auch an Geheimschutzregelungen des § 99 Absatz 2 VwGO. Dabei steht es im Ermessen des Gerichts, die Verfahrensbeteiligten vor einer Entscheidung über den Feststellungsantrag anzuhören oder ausschließlich auf Grundlage

der eingereichten Unterlagen zu entscheiden. Wie in vergleichbaren Verfahren, etwa zu richterlichen Anordnungen im Ermittlungsverfahren nach der Strafprozessordnung, wird auch vorliegend die Entscheidung durch einen einzelnen Richter adäquat, bei Eilanordnungen eventuell auch verfahrenspraktisch geboten sein. Hiergegen kann allerdings die Entscheidung des Senats beantragt werden, auch um gegebenenfalls zu grundsätzlichen Fragen eine vom gesamten Senat getragene Linie herzustellen.

Es bleibt gleichwohl bei dem umfassenderen Schutzkonzept, dass sich die unabhängige Kontrolle nicht auf die Erhebungsebene beschränkt, sondern vollumfänglich die Verwertungsebene einbezieht. Insoweit bleibt es nach Absatz 3 bei der Anwendung des § 15 Absatz 5 Satz 2 G 10 (mit dem in Absatz 3 Satz 1 Nummer 2 getroffenen Ausschluss einer inzidenten Anordnungsprüfung, da diese bindend beim Bundesverwaltungsgericht liegt). Hierzu besteht eine ergänzende Zuständigkeit der G 10-Kommission, da eine solche aufsichtliche Prüfung – unter Einschluss anlassfreier Strukturprüfungen – nicht dem Profil gerichtlicher Aufgaben entspricht. Trotz der grundsätzlichen Synchronisierung des Schwellen- und Verfahrensrahmens zwischen Wohnraumüberwachung und Online-Durchsuchung wird für letztere in § 9d allerdings auch zur Anordnungsprüfung an der Zuständigkeit der G 10-Kommission festgehalten, da dies angesichts der funktionalen Äquivalenz des unabhängigen Schutzstandards – mangels entgegenstehender ausdrücklicher Grundgesetzregelung – vertretbar erscheint und dies gerade aus der Schutzperspektive sogar die effektivere Lösung ist, weil die G 10-Kommission aufgrund laufender Befassung spezifische Fachkunde in nachrichtendienstlichen Angelegenheiten aufbaut und zudem einen besseren Gesamtüberblick zu den gegen einen Betroffenen gerichteten Intensivmaßnahmen hat.

Der Einsatz von Personen unter Legende bedarf auch bei Kenntnis des Wohnungsinhabers einer besonderen Befugnis, wenn er – ohne Wissen des Wohnungsinhabers – durch technische Überwachung abgesichert erfolgt. Absatz 4 trägt den dazu in Artikel 13 Absatz 5 GG getroffenen Vorgaben Rechnung.

Absatz 6 stellt klar, dass für die bezeichneten Vorbereitungshandlungen ebenso die Wohnung – auch ohne

Zustimmung des Wohnungsinhabers – betreten werden darf.

Zu Nummer 5 (§ 11 Absatz 1)

Die besonderen Voraussetzungen zur Speicherung personenbezogener Daten Minderjähriger nach dem bisherigen § 11 Absatz 1 entfallen. Verantwortungsfähigkeit von Personen ist für eine strafrechtliche Schuldfähigkeit bedeutsam, für objektiv von ihnen ausgehende Gefahren hingegen nicht konstitutiv. Das Polizeirecht enthält demgemäß keine altersbezogene Speicherschwellen (vgl. § 29 BPolG), sondern bewertet ein junges Lebensalter als eine dynamische Entwicklungsphase, der durch angemessene Regelprüfungs/-aussonderungsfristen Rechnung zu tragen ist (vgl. § 35 Absatz 3 BPolG). Letzteres ist – und bleibt – bereits in § 11 Absatz 2 geregelt.

Dieser neue Ansatz trägt auch den praktischen Anforderungen Rechnung. So sind nicht nur auch sehr junge Menschen in die Krisenregionen in Syrien/Irak zur Beteiligung an terroristischen Bestrebungen ausgereist (vgl. bereits BT-Drs. 18/8917, S. 6), auch in Deutschland selbst hat im November/Dezember 2016 ein Zwölfjähriger einen Sprengstoffanschlag unternommen. Die Problemlage verschärft sich durch den Zusammenbruch der Herrschaftsgebiete der terroristischen Aufständischen in der nahöstlichen Krisenregion und die erwartbare Rückkehr weiterer dort Beteiligter, darunter auch Familien mit Kindern (dreistellige Anzahl von Minderjährigen erwartbar: BT-Drs. 19/387, S. 6). Insofern besteht auch ein staatlicher Schutzauftrag zugunsten dieser Kinder mit Aufgaben der Jugendhilfe, die komplementär zur nachrichtendienstlichen Aufklärung von Rückkehrer-Sachverhalten informiert werden muss. Dies bedingt, dass die Verfassungsschutzbehörden solche Sachverhalte nicht einfach ignorieren dürfen, folglich dann aber auch zur Informationsverarbeitung bei Durchführung ihrer Aufgaben befugt sein müssen. Der Sachverhalt unterstreicht zugleich den ganzheitlichen Schutzansatz des Verfassungsschutzes, der – anders als schuldgegründete Strafverfolgung – nicht „gegen“ Personen ausgerichtet ist, sondern „für“ die Schutzgüter des § 1 Absatz 1 und insoweit auf das Gesamtspektrum präventiver Gestaltung zielt, u.a. auch darauf, einem situativ angelegten Radikalisierungsrisiko (als Kind in einer Jihadi-Familie) durch Jugendhilfe zuvorzukommen oder ggf. individuell

deradikalisierend die gesellschaftliche Integration zu fördern.

Zu Nummer 6 (§ 12 Absatz 3 Satz 2)

Typischer Aufklärungsgegenstand der Verfassungsschutzbehörden sind längerfristige Phänomene, nicht individuelle Einzelvorfälle. Diese Aufklärungsperspektive erfordert eine risikosensible Einschätzung zur künftigen Aufgabenerforderlichkeit, die den endgültigen Verlust bei Ungewissheit künftiger Erforderlichkeit vermeidet. Die Annahme, dass der Ablauf von 10 Jahren ohne weitere relevante Informationen regelmäßig indiziert, dass eine weitere Speicherung nicht mehr erforderlich ist (die weitere Speicherung dann mithin durch erkannte Ausnahmegründe zu legitimieren ist), wird rechtstatsächlich nicht bestätigt. Auch im Rahmen der letzten Evaluierung der Regelung haben sich Praktiker für die Fristverlängerung auf 15 Jahre ausgesprochen (Evaluierungsbericht Abschnitt 4.4.2). In der Vergangenheit sind wiederholt auch länger zurück liegende Vorgänge – trotz Fehlens zwischenzeitlich hinzutretender Erkenntnisse – bedeutsam geworden. So konnte bei Aufklärung des NSU-Komplexes eine Aufarbeitung lediglich anhand von Sachakten rekonstruiert werden. Gleiches gilt auch für die strafrechtlichen Ermittlungen des GBA in Bezug auf das Oktoberfestattentat von 1980, welche 2015 wieder aufgenommen worden waren. Bei Würdigung einerseits der Strukturaufklärungsaufgabe des BfV und andererseits der informationellen Trennung seiner Datenverarbeitung von staatlicher Intervention, erscheint der angemessenere Ausgleich zwischen Betroffenen- und Gemeinwohlbelangen in einer Heraufsetzung der Regelfrist von 10 auf 15 Jahre, zumal bei der Aufklärung von Tätigkeiten nach § 3 Absatz 1 Nummer 2 seit jeher auf eine Regelfrist ganz verzichtet wird.

Zu Nummer 7 (§ 13 Absatz 4 Satz 3)

Es handelt sich um eine Folgeänderung zu Nummer 6.

Zu Nummer 8 (§ 17 Absatz 2)

Absatz 2 regelt Ausschreibungen zur polizeilichen Beobachtung – also zur Mitteilung des Antreffens – unter Einbezug der bisherigen Absätze 2 und 3. Erkenntnisziel sind gemäß dem Aufklärungsbedarf nicht allein grenzüberschreitende

Bewegungen. Datenschutzfreundlich erfolgt künftig bereits gesetzlich in Satz 1 Nummer 1 und 2 eine spezielle Regelung zu dem Personenkreis, zu dem Ausschreibungen möglich sind. Diese ist enger gefasst als die allgemeine Befugnis zu Übermittlungsersuchen nach § 18 Absatz 3, um dem Umstand Rechnung zu tragen, dass die Ausschreibungen bereits im polizeilichen Bereich auf qualifizierte Bedarfe beschränkt sind (vgl. etwa § 31 Absatz 2 BPolG, Art. 40 BY PAG, § 37 NI SOG). Zur homogenen Regelung gilt dies künftig ebenso für die Ausschreibung im Grenzfahndungsbestand (bisheriger § 17 Absatz 2 ohne solche Schwelle).

Die Ausschreibung erfolgt im vom BKA betriebenen polizeilichen Informationsverbund, im geschützten Grenzfahndungsbestand der Bundespolizei oder auch in Datenbanken der EU, aktuell dem Schengener Informationssystem. Für Ausschreibungen in EU-Systemen sind die unionsrechtlichen Voraussetzungen maßgeblich. Die EU besitzt keine Regelungskompetenz im Bereich der nationalen Sicherheit ihrer Mitgliedstaaten (Artikel 4 Absatz 2 Satz 3 EUV). Sie legt jedoch die Zwecksetzung ihrer Einrichtungen fest und kann den Zugang zu diesen durch nationale Behörden unionsrechtlich regulieren, muss ihn also zunächst ihrerseits für Zwecke der nationalen Sicherheit öffnen. Dies ist zum SIS derzeit mit Artikel 36 Absatz 3 des SIS-II-Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 erfolgt. Die gesetzliche Regelung verweist künftig nicht mehr auf bestimmte unionsrechtliche Bestimmungen (wie noch im bisherigen § 17 Absatz 3 BVerfSchG a.F. mit einer allerdings bereits veralteten Verweisung), sondern angemessener allgemein und dynamisch auf das jeweils anzuwendende Unionsrecht.

Zum Zweck der Rechtsvereinheitlichung erfolgt die Regelung – wie im bisherigen Absatz 2 – grundsätzlich auch für die Landesverfassungsschutzbehörden. Wie im bisherigen Absatz 3 bleiben Ausschreibungen in EU-Systemen in Übereinstimmung mit § 5 Absatz 5 dem BfV vorbehalten. Ausschreibungen von MAD und BND werden abweichend vom bisherigen Absatz 2 nicht mehr im Bundesverfassungsschutzgesetz, sondern systematisch näherliegender in MAD- bzw. BND-Gesetz geregelt.

Im Interesse wirtschaftlicher und datenschutzgerechter Verwaltung wird im Übrigen gesetzlich ausdrücklich ermöglicht,

dass die ausschreibenden Stellen ihre Ausschreibung unmittelbar eingeben, um unnötigen weiteren Bearbeitungsaufwand und verbundene Fehlerrisiken zu vermeiden. Da Ausschreibungen nach der evaluierten Praxis ganz überwiegend verlängert werden (was dem längerfristig angelegten, strukturellen Aufklärungsprofil der Verfassungsschutzbehörden entspricht), wird nunmehr im Interesse wirtschaftlicher Verwaltung die Höchstdauer der jeweiligen Ausschreibungsanordnung auf ein Jahr verlängert. Sie ist weiterhin unverzüglich zu löschen, sobald ihre Voraussetzungen nicht mehr vorliegen oder der Maßnahmezweck erreicht ist oder nicht mehr erreicht werden kann (Satz 6).

Zu Nummer 9 (§ 18)

Zu Buchstabe a

Als Folge der in den letzten Jahren massiv erhöhten Asylverfahren unter Einschluss besonders sicherheitsrelevanter Herkunftsregionen sind auch die Mitteilungen des BAMF entsprechend gestiegen. Komplementär sind ebenso die Erfordernisse zu internationaler sicherheitsbehördlicher Zusammenarbeit gewachsen. Dies ist nicht auf die angegebenen Herkunftsstaaten fokussiert, betrifft ggf. aber regionale Partner oder auch wichtige westliche Partner, speziell in Europa (CTG). Die bisher in § 18 Absatz 1a Satz 3 vorgesehene Vorabbeteiligung des BAMF ist dabei nicht sinnvoll, da insoweit keine zusätzliche Expertise zur Würdigung der anzuwendenden Übermittlungsvorschriften beizubringen ist. Sie schafft umgekehrt jedoch Verzögerungen, die gerade in Gefährdungssachverhalten sowohl für Deutschland wie auch möglicherweise zu beteiligende Partner Risiken begründen kann. Zudem führt sie entgegen zentralen Geheimschutzgrundsätzen zu einer sachlich nicht begründeten Ausweitung des Kenntnisträgerkreises zur nachrichtendienstlichen Befassung, womit komplementär – vermeidbare – Indiskretionsrisiken einhergehen. Daher wird die unnötige aber kontraproduktive Regelung gestrichen. Das BfV würdigt allgemein bei Auslandsübermittlungen nach § 19 Absatz 3 BVerfSchG von sich aus etwaige Betroffenenbelange sorgfältig, dies gilt auch und im Besonderen für Informationen aus Asylverfahren.

Zu Buchstabe b

Die Ergänzung des Absatzes 5 um Protokollierungsregelungen zu automatisierten Abrufverfahren trägt Geheimschutz- und Datenschutzbelangen Rechnung. Für automatisierte Abrufe wird eine Vollprotokollierung – nur – im Nachrichtendienstlichen Informationssystem vorgesehen. Dies dient insbesondere der Datenschutzkontrolle, die notwendig aus der Aufgabenperspektive der erhebenden Stelle erfolgen muss, also vorzugswürdig durch Dokumentation im erhebenden System zu gewährleisten ist. Gleichzeitig trägt dies Belangen des Geheimschutzes Rechnung, die typischerweise in der abgefragten Datenbank nur mit unwirtschaftlichen Zusatzaufwänden zu gewährleisten sind. Schließlich dient dies zugleich dem Datenschutzinteresse, eine etikettierende Außenwirkung einer Verfassungsschutzanfrage bereits technisch zu vermeiden (Datenschutz durch Technikgestaltung).

Zu Buchstabe c

Die bisher in Absatz 6 für die Telekommunikation getroffene Beschränkung der Übermittlungsbefugnisse wird erweitert auf Eingriffe in die besonderen Privatheitsrechte nach Artikel 10 und 13 sowie die Vertraulichkeit und Integrität Informationstechnischer Systeme. Dabei wird eine wertungskonsistente Synchronisierung mit den Weiterverarbeitungszwecken bei entsprechenden Eigenerhebungen des BfV hergestellt.

Zu Nummer 10 (§ 19)

Zu Buchstabe a

Die Ergänzung übernimmt die Regelung des bisherigen § 24 Absatz 2 und integriert sie als Konkretisierung von Sachverhalten, in denen überwiegende schutzwürdige Betroffeneninteressen der Übermittlung entgegenstehen, in die Grundnorm des § 19 Absatz 3. Von einem generellen Ausschluss der Übermittlung von Daten vor Vollendung des 14. Lebensjahres wird dabei abgesehen, da nach den Praxiserfahrungen (oben zu Nummer 6) unter den Voraussetzungen des neuen Satzes 3 auch eine solche Übermittlung in Betracht kommen muss. Ob sie im Einzelfall zulässig ist, bleibt ergänzend anhand einer einzelfallbezogenen Schutzwürdigkeitsabwägung nach Satz 2 zu prüfen.

Zu Buchstabe b

Die neue Regelung soll dem Schutz Betroffener auch in atypischen – insofern von den vorausgegangenen Übermittlungsvorschriften noch nicht zureichend abgedeckten – Fällen verbessert Rechnung tragen. Eingeschlossen ist eine rechtsklare Übermittlungsgrundlage zur Information der Jugendhilfe, etwa in den aktuellen Fällen der Rückkehr von Personen, die in den nahöstlichen Krisenregionen in terroristische Strukturen eingebunden waren. Dabei handelt es sich teilweise um Familien mit Kindern, die dort geboren worden sind, bei Rückkehr nach Deutschland angesichts der besonderen familiären Zusammenhänge aber womöglich besonderer staatlicher Fürsorge bedürfen.

Zu Nummer 11 (§ 22a)

Zu Buchstabe a

Es handelt sich um eine begriffliche Folgeanpassung zu Buchstabe b) im Hinblick auf den neuen § 22a Absatz 1.

Zu Buchstabe b

Der neue Absatz 1 erleichtert die Zusammenarbeit im nachrichtendienstlichen Bereich über § 6 (LfV/MAD) hinaus unter Einbezug des BND. Ferner einbezogen ist das BSI, insbesondere um elektronischer Angriffe fremder Mächte gemeinsam aufklären zu können. Das BSI ist kein Nachrichtendienst, besitzt aber keine vollzugspolizeilichen Zwangsbefugnisse und ist danach aus der Datenschutzperspektive der Risikobewertung für schutzwürdige Betroffeneninteressen systematisch dem neuen Absatz 1 zuzuordnen, nicht der Zusammenarbeit zwischen Nachrichtendiensten und Polizeien, die künftig in Absatz 1a geregelt ist. Die informationelle Zusammenarbeit ist danach ebenso wie im Falle des BND nicht spezifischen Einschränkungen einer grundsätzlichen informationellen Trennung unterworfen. Der Bezug auf die Aufgaben nach § 3 Absatz 1 gewährleistet auch für diese Zusammenarbeit eine Beschränkung auf besondere Bedrohungen herausragender Rechtsgüter, im Falle des BSI geht es vornehmlich um elektronische Angriffe fremder Mächte/Staaten.

Absatz 1b entspricht dem bisherigen Absatz 1, wobei jedoch Satz 2

die Spionageabwehr nicht auf gewaltorientierte Tätigkeiten beschränkt und Satz 3 eine erweiterte Verlängerungsmöglichkeit bei der projekthaften Aufklärung (politisch-) krimineller/terroristischer Vereinigungen eröffnet. Diese bestehen teils länger als der bisherige Zeitrahmen (Al Qaida etwa mittlerweile seit Jahrzehnten), weshalb dieser insofern nicht aufgabenadäquat ist. Es bleibt auch insofern aber beim Projektansatz, d.h. die gemeinsame Datenhaltung kann nicht zur Aufklärung eines gesamten – etwa terroristischen – Phänomenbereichs betrieben werden.

Zu Buchstabe c

Die Sätze 3 und 4 des bisherigen Absatzes 1 werden systematisch stimmiger in die Verarbeitungsregelungen des Absatzes 2 integriert. Die neuen Absätze 1 und 1a beschränken sich infolge auf die zulässigen Zwecke und Teilnehmer gemeinsamer Dateien.

Zu Buchstabe d

Die Änderung bei aa entspricht der Änderung nach Buchstabe a.

Mit bb werden klarstellende Folgeregelungen für den Fall des Ausscheidens eines Teilnehmers ergänzt, die dem Grundmodell folgen, das die Eingabe als Übermittlung an alle Teilnehmer qualifiziert. Zur klaren Zuordnung liegt die Verantwortung der speichernden Stelle zu den übermittelten Datensätzen nach Ausscheiden der eingebenden Stelle bei der dateiführenden Stelle, dem BfV. Die eingebende Stelle bleibt als funktionaler Datenübermittler nachberichtspflichtig nach § 26.

Zu Buchstabe e

Die Regelungen des bisherigen Absatzes 4 sind in den neuen Absatz 1a integriert worden.

Zu Nummer 12 (§ 22b)

Mit der Änderung wird die sachlich gebotene Teilnahme von BND und MAD an gemeinsamen Projektdateien des BfV mit ausländischen Nachrichtendiensten eröffnet. Gleichzeitig wird die Verarbeitungsregelung in Absatz 6 normenklarer als selbständige Regelung gefasst.

Zu Nummer 13 (§ 24)

Die Aufhebung steht im Zusammenhang mit Nummern 5 und 10 und dient einem insgesamt abgewogeneren Umgang mit personenbezogener Daten Minderjähriger, der deren individuellen Schutz weiter wahrt, dabei aber zwingende Belange des Gemeinwohls besser berücksichtigt.

Zu Nummer 14 (§ 26a)

Die Regelung ergänzt gesetzliche Minimalanforderungen unabhängiger Datenschutzkontrolle. Die Kontrollpraxis der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ist seit jeher wesentlich dichter und intensiver und verbleibt jenseits des gesetzlichen Mindeststandards, der speziell auf Datenschutz im Zusammenhang nachrichtendienstlicher Maßnahmen bezogen wird, auch künftig in ihrem flexiblen Auswahlermessen zu Anlässen und Gegenständen einzelner Prüfungen, um den jeweils aktuell im Vordergrund stehenden Datenschutzbelangen jeweils angemessen Rechnung zu tragen.

Zu Nummer 15 (§ 28)

Entsprechend üblicher Gesetzestechnik werden die Einschränkungszitate nunmehr in einem gesonderten Paragraphen zusammengefasst. Neu aufgenommen wird Artikel 8 GG, da die sicherheitsbehördliche Beobachtung von Versammlungen, speziell beim Einsatz technischer Mittel, als Eingriff in dieses Grundrecht qualifiziert werden könnte. Die Zitierung stellt mithin klar, dass auch Versammlungen – wie etwa extremistische Aufzüge – unter den gesetzlichen Voraussetzungen beobachtet werden dürfen.

Zu Artikel 2 (Änderung MADG)

...

Zu Artikel 3 (Änderung des BNDG)

Zu Nummer 1 (§ 2 Absatz 1 Nr. 4)

Die Subsidiaritätsklausel in der bisherigen Fassung der Nr. 4 ist angesichts der inzwischen vielfältigen Schnittmengen v.a. mit der Arbeit des BfV, z.B. in der Terrorismusaufklärung, sachlich überholt

und angesichts der anderweitigen Zuständigkeitsregeln auch nicht mehr erforderlich.

Zu Nummer 2 (§ 3)

Der vollständig neu gefasste § 3 ersetzt den bisherigen umfangreichen Verweis auf die Parallelvorschrift des § 8a BVerfSchG mit einer eigens auf die Auftragserfüllung des BND zugeschnittenen Regelung. § 4 BNDG wird durch die Neufassung obsolet. Mit der Befugnis des BND zum Verlangen einer Auskunft von den privaten Verpflichteten geht denknotwendig eine Verpflichtung derselben einher.

Absatz 1 regelt Auskunftsverlangen des BND zu Bestandsdaten. Zur Erhebung bloßer Bestandsdaten ist der BND zur Erfüllung seiner Aufgaben nach § 1 Absatz 2 sowie zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände oder Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten berechtigt. Der Kreis der Verpflichteten besteht aus Unternehmen jener Branchen, die nach bisheriger Erfahrung in besonderem Ausmaß über Daten zu Auslandssachverhalten in den für die Auftragserfüllung des BND relevanten Gebieten und Themen verfügen. Systematisch wird dies u.a. durch den Verweis auf das Geldwäschegesetz abgebildet. Insbesondere soweit die dort (§ 2 Absatz 1 GwG) aufgeführten Unternehmen und Personen im Immobiliensektor und im Handel mit hochwertigen Gütern tätig sind, besteht ein besonders ausgeprägtes Geldwäscherisiko. Illegal erwirtschaftete Gelder können hier wertstabil angelegt und – gerade bei Luxusgütern – mit Bargeld leichter erworben sowie grenzüberschreitend transportiert werden.

Mit Absatz 1 Nummer 3 werden neben Telekommunikationsdiensten gemäß der bestehenden gesetzlichen Terminologie Telemedien miterfasst (wie auch in § 8a Absatz 1 Satz 1 Nummer 3 BVerfSchG n.F.).

Die Neuregelung stellt dabei auf das Marktortprinzip ab, so dass eine inländische Leistungserbringung für die Begründung der Auskunftspflicht ausreicht. Ergänzend daneben steht, wie in der Vorgängerregelung, die Befugnis, Bestandsdaten auch beim Bundeszentralamt für Steuern sowie insoweit deklaratorisch, weil bereits in § 112 TKG vorgesehen bei der Bundesnetzagentur zu

erheben. Andere gesetzliche Vorschriften, die Auskunftsverlangen des BND gegenüber nationalen Behörden regeln (z.B. § 32 Absatz 2, 3 GwG), bleiben unberührt.

Die in Absatz 1 zum Auskunftsgegenstand gemachten Bestandsdaten umfassen, den Legaldefinitionen in § 3 Nr. 3 TKG und in § 8a Absatz 1 BVerfSchG folgend, alle für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses mit den in Absatz 1 genannten Dienstleistern bei diesen gespeicherten Daten.

Die mit der Befugnis des BND, um Auskunft zu ersuchen, einhergehende Verpflichtung der genannten Unternehmen wird explizit in Satz 2 benannt.

Mit Absatz 1 Satz 4 wird klargestellt, dass die materiellen Voraussetzungen für Folgemaßnahmen vorliegen müssen, soweit ein Auskunftsverlangen allein deren Vorbereitung dient. Hiermit wird die bisher nur als Spezialfall in § 4 BNDG i.V.m. § 8d Absatz 1 Satz 2 BVerfSchG (a.F.) ausdrücklich normierte Regelung als allgemeine Regelung auf alle Fälle des Absatz 1 Satz 1 Nummer 3 ausgeweitet.

Auskünfte über die Umstände und Inhalte der erbrachten Leistungen dürfen lediglich unter den qualifizierenden Voraussetzungen des Absatzes 2 verlangt werden. Umstände der erbrachten Leistungen dürfen verlangt werden, sofern dies zur Aufklärung von Bedrohungen von erheblicher Bedeutung erforderlich ist. Gleiches gilt für Inhalte der nach Absatz 1 Satz 1 Verpflichteten erbrachten Leistungen, sofern diese nicht dem Brief-, Post- und Fernmeldegeheimnis unterliegen. Für Auskunftsverlangen zu Inhalten einer Leistung eines nach Absatz 1 Satz 1 Nummer 3 Verpflichteten, die dem Brief-, Post- und Fernmeldegeheimnis unterliegen, verbleibt es bei den Maßgaben des Artikel 10-Gesetzes. Dadurch besteht ein klares inhaltliches Gefälle zwischen den Voraussetzungen für Auskunftsverlangen zu Bestandsdaten (Absatz 1, Aufgabenerfüllung sowie Schutz von Mitarbeitern, Einrichtungen etc.) und Auskunftsverlangen zu Umständen bzw. Inhalten einer Leistung, hinsichtlich der Inhalte differenziert nach der Art des Verpflichteten (Abs. 2, Bedrohungen von erheblicher Bedeutung bzw. Maßgaben des Artikel 10-Gesetzes).

Die inhaltlich neue Regelung des Absatz 2 Satz 2 erstreckt das Auskunftsverlangen gegenüber Unternehmen, deren Leistungsgegenstand der Transport oder die Verwahrung von Sachen ist, auch auf die Gewährung vorübergehenden Besitzes zur Augenscheinnahme und zur Untersuchung dieser Sachen. Diese Befugnis ist insbesondere für die Aufklärung proliferationsrelevanter Sachverhalte erforderlich und bewegt sich systematisch im Rahmen zulässiger klassischer Eingriffe in das Postgeheimnis. Folgerichtig gelten dafür gemäß Absatz 2 Satz 4 weitgehend Verfahrensvorschriften aus dem Artikel 10-Gesetz.

Die Erhebung von Informationen nach der gleichfalls neuen Vorschrift des Absatzes 3 ist zweifach beschränkt. Informationen aus Videoüberwachungen dürfen gemäß Satz 1 nur ausgeleitet bzw. übermittelt werden, wenn die damit beabsichtigte Aufklärung Bedrohungen von erheblicher Bedeutung gilt. Eine bloße Auftragsrelevanz ist also nicht ausreichend. Vielmehr muss es sich um Bedrohungen von erheblicher Bedeutung handeln. Hierunter fallen jedenfalls die in den §§ 3 und 5 Artikel 10-Gesetz-Gefahren definierten Gefahren. Aber auch andere als die dort explizit aufgezählten Gefahren können Bedrohungen von erheblicher Bedeutung sein. Zusätzlich sind Informationserhebungen, die gezielt zur Überwachung bestimmter Personen eingesetzt werden, gemäß Satz 2 auf Fälle beschränkt, in denen diese nach § 5 Absatz 4 zulässige Adressaten nachrichtendienstlicher Mittel sind.

Zu Nummer 3 (§§ 5 ff.)

Mit den Neuregelungen in den §§ 5 bis 5e werden sehr viel detailliertere Regelungen zum Einsatz nachrichtendienstlicher Mittel v.a. beim Einsatz von Human Sources Intelligence (HUMINT) als die alte Regelung in § 5 BNDG i.V.m. §§ 8 ff. BVerfSchG geschaffen.

§ 5 ist dabei die allgemeine Befugnisnorm für den Einsatz nachrichtendienstlicher Mittel, die in §§ 5a bis 5d mit ergänzenden Spezialregelungen für einzelne solcher Mittel ergänzt und in § 5e mit einer Schrankenregelung abgeschlossen wird, die für alle diese Mittel gilt.

Zu § 5

Absatz 1 greift inhaltlich die alte Befugnisregel aus § 5 BNDG a.F.

i.V.m. § 8 Absatz 2 BVerfSchG a.F. auf, formuliert sie aber als eigenständige, vom BVerfSchG entkoppelte Eingriffsnorm. Die beispielhafte und insofern nicht abschließende Aufzählung der einzelnen nachrichtendienstlichen Mittel in Satz 2 enthält – anders als die Vorgängernorm – zugleich Legaldefinitionen dieser Mittel. Hierdurch wird dem Bestimmtheitsgrundsatz genüge getan, ohne jedoch zugleich durch Formulierung eines abschließenden Katalogs sämtlicher nachrichtendienstlicher Mittel etwaigen Gegenspielern hinreichende Details für Gegenmaßnahmen oder Anpassung ihrer Handlungsweisen zu bieten. Die exemplarische Aufzählung in Satz 2 orientiert sich an den vom BND typischerweise eingesetzten Methoden und den dort eingeführten Begrifflichkeiten. Gleichzeitig gibt sie damit innerdienstlichen Verwaltungsvorschriften (Satz 3) einen verbindlichen materiellen Rahmen, der wie schon die Vorgängerregelung formell um das Erfordernis einer Zustimmung des Bundeskanzleramtes und einer zwingenden Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) ergänzt wird.

Ferner enthält Absatz 1 nunmehr den klarstellenden Hinweis, dass die genannten nachrichtendienstlichen Mittel auch zu Zwecken des Eigenschutzes eingesetzt werden dürfen. Der BND und seine Mitarbeiter, vor allem diejenigen in operativ-beschaffenden Einsätzen, sind ein Hochziel der nachrichtendienstlichen Aufklärungsanstrengungen anderer Staaten. Hierfür kann erforderlich sein, bereits die Zugehörigkeit eines Mitarbeiters zum BND durch den Einsatz entsprechender Legenden, d.h. eines nachrichtendienstlichen Mittels, zu vertarnen. Dabei verbietet schon der verfassungsrechtlich vorgegebene Verhältnismäßigkeitsgrundsatz eine ausufernde Anwendung nachrichtendienstlicher Mittel zu Eigenschutzzwecken. Zudem trägt die Eigenschutzklausel ihre Anwendungsbeschränkung auf defensive Maßnahmen begrifflich in sich: Eigenschutz setzt notwendigerweise eine Zweckbestimmung voraus, die ein offensives Ausspähen von Nicht-Auslandssachverhalten auch mit Blick auf die überwölbende Aufgabenzuweisung in § 1 Absatz 2 Satz 1 verbietet.

Nicht hiervon erfasst sind Maßnahmen im Rahmen von Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz (SÜG), das insoweit abschließende lex specialis bleibt.

Satz 1 Nr.6 greift zwar die frühere Bestimmung des § 5 BNDG i.V.m. § 9 Absatz 4 BVerfSchG auf, öffnet sich aber mit seiner neuen Formulierung („technische Mittel, insbesondere …“) allgemein für die Nutzung von Geräten und Geräteentwicklungen, die auftragsrelevante Informationen bieten können. Von der alten Gesetzesformulierung („technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer“) umfasste Erhebungen sind also gleichfalls inbegriffen.

Personen i.S.d. Absatzes 1 behalten ihre Eigenschaft als nachrichtendienstliches Mittel auch nach Beendigung ihrer eigentlichen nachrichtendienstlichen Tätigkeit, soweit der BND weiter gezielten Kontakt zu ihnen unterhält, etwa für Zwecke der operativen Nachsorge.

Absatz 2 bildet im Normgefüge des vom BVerfSchG entkoppelten Gesetzentwurfs die notwendige (bisher in § 9 Absatz 1 BVerfSchG a.F. enthaltene) Ergänzung der Befugnis aus Absatz 1 um BND-spezifische Zweckbestimmungen für die Erhebung personenbezogener Daten.

Absatz 3 unterwirft Observationen, die ununterbrochen länger als 48 Stunden dauern, besonderen Voraussetzungen. Observationen haben dann ein besonderes Eingriffsgewicht. Durch die Festschreibung einer speziellen Einsatzschwelle für längerfristige Observationen wird von vornherein die Verhältnismäßigkeit des Einsatzes solcher nachrichtendienstlicher Mittel wesentlich gesichert, indem in Abgrenzung zu lediglich kurzfristigen bzw. lokal-objektbezogenen Observationen der Einsatz von Observationen über einen längeren Zeitraum einer qualifizierten Einsatzschwelle (Bedrohungen von erheblicher Bedeutung) unterworfen wird.

Absatz 4 präzisiert in Satz 1 zunächst, gegen wen sich nachrichtendienstliche Mittel nach Absatz 2 Nummer 1 und 3 richten dürfen und knüpft dabei inhaltlich an die Befugnisgrundnorm des § 2 an. Bereits bei nachrichtendienstlichen Operationsansätzen im Geltungsbereich des BNDG (§ 1 Absatz 2 Satz 2) können besondere Risiken für Freiheit, Leib und ggf. Leben von Quellen und Mitarbeiter des BND begründet werden. Die Tarnwirkung nachrichtendienstlicher Mittel sollen daher nicht nur

gegenüber Informationsquellen im engeren Sinne (Nr. 2) oder Gefährdungsquellen für den Dienst (Nr. 3) genutzt werden dürfen, sondern auch gegenüber Personen, die nicht selbst Träger der erhofften Informationen zu ausländischen Sachverhalte sind, aber im Zuge von HUMINT-Operationen dem BND Zugang zu auftragsrelevanten Personen vermitteln (Nr. 1). Eine effektive Tarnwirkung ist dabei in der operativen Praxis oft nur zu erzielen, wenn beispielsweise Legenden umfassend genutzt und dabei auch andere als die eigentlich für operative Zwecke genutzten Personen unvermeidlich mit betroffen sind (Satz 2). Satz 3 schließlich stellt klar, dass die Überprüfung der für die Aufgabenerfüllung des BND notwendigen Zugänge (vgl. § 2 Absatz 1 Nr. 3) von den Vorgaben des Absatz 4 unberührt bleibt, also sich auch an Personen richten darf, die nicht zu dem in Satz 1 aufgezählten Kreis gehören.

Zudem wird in Absatz 5 ergänzt, dass Mitarbeiter des BND, die nachrichtendienstliche Mittel gemäß den gesetzlichen Vorgaben einsetzen, sich nicht rechtswidrig verhalten können.

Die Protokollierungspflichten des Absatzes 6 dienen der Sicherstellung hinreichender (Ex-post-) Rechtmäßigkeitskontrollen.

Zu § 5a

Der neue § 5a regelt die beiden in der HUMINT-Aufklärung des BND praktisch bedeutsamsten nachrichtendienstlichen Mittel, Anbahnung (§ 5 Absatz 1 Nr. 1) und Einsatzführung (§ 5 Absatz 1 Nr. 2). § 5a ist insoweit lex specialis zu § 5 und stellt deshalb für den Einsatz dieser Mittel die eigentliche Befugnisnorm dar. Da eine Anbahnung oder Einsatzführung denknotwendig die Anleitung durch hauptamtliche BND-Mitarbeiter voraussetzt, erstreckt sich die Befugnis nicht nur auf das Handeln der angebahnten bzw. geführten Personen, sondern ebenso auf das dem zugrunde liegende Agieren der hauptamtlichen Mitarbeiter.

Begrifflich spricht das BNDG in diesem Zusammenhang nicht von Vertrauensleuten, sondern neutral von (angebahnten und geführten) Personen. Dies entspricht dem Sprachgebrauch im BND. Der Begriff der Vertrauensleute wird im BND nicht verwendet.

Die für den BND in Absatz 2 niedergelegten Anbahnungseinschränkungen bzw. -verbote nehmen auf Besonderheiten der Auslandsaufklärung Rücksicht. So spiegelt die in Nr. 1 angepasste Altersgrenze eine in vielen Zielregionen der Aufklärung des BND gelebte Tradition und Wirklichkeit wider, wonach Personen bereits ab Vollendung des 16. Lebensjahres vollwertige Akteure z.B. in militärischen Auseinandersetzungen sind und in den Strukturen, in denen sie leben und agieren, umfassende Verantwortung tragen.

Mit ihrem nachrichtendienstlichen Einsatz im Ausland setzen sich Quellen des BND oft einem enormen persönlichen Sicherheitsrisiko aus, das sich ggf. sogar auf ihre Familienangehörigen erstreckt. Dieses Risiko kann in derartigen Fällen oft nur adäquat entlohnt und eine Person als Quelle für den BND erfolgreich angebahnt werden, wenn die finanziellen Zuwendungen des BND entsprechend hoch sind, um eine den Umständen entsprechende Sicherung der Lebensgrundlage ggf. auch nach Beendigung der Arbeit für den BND in ausreichendem Maße gewährleisten zu können. Ferner stellen Zahlungen an Quellen in wirtschaftlich ärmeren Krisenländern auch mit Blick auf die vergleichsweise niedrige absolute Höhe des Einkommens vor Ort – viel häufiger die alleinige finanzielle Lebensgrundlage dar, als dies in Deutschland der Fall wäre. Die Anwerbungseinschränkung des § 9b Absatz 2 Nr. 2 BVerfSchG n.F. passt daher regelmäßig nicht für die Auftragserfüllung des BND als Auslandsnachrichtendienst.

Gleiches gilt für das Verbot, Teilnehmer eines Aussteigerprogrammes anzuwerben (§ 9b Absatz 2 Nr. 3 BVerfSchG n.F.). Die Zielrichtung eines staatlichen Aussteigerprogrammes im Ausland kann weder formell noch nach seinem Sinn und Zweck deutsche Sicherheitsbehörden in die Pflicht nehmen, Programmteilnehmer nicht anzubahnen.

Die Regelungen der Absätze 3 bis 5 folgen den Parallelvorschriften der §§ 9b Absatz 3 und Absatz 4 BVerfSchG. Sie werden jedoch an die besondere Aufgabenzuweisung an den BND angepasst. Die Aufklärungsarbeit des BND ist nicht auf bestimmte Bestrebungen oder Organisationen beschränkt, sondern allgemein auf Themen von außen- und sicherheitspolitischer Bedeutung ausgerichtet. Dabei bestehen in den Zielländern der

BND-Aufklärung nicht selten regionaltypisch enge Verbindungen zwischen Regierungskreisen und außerhalb der Regierung organisierten Gruppierungen oder Netzwerken, so dass die Abgrenzung zwischen beiden Sphären und eine daran anknüpfende rechtliche Differenzierung bei den Anbahnungsverboten in der konkreten Sachverhaltsbeurteilung oftmals nicht möglich ist.

Das Verbot der Fortführung einer laufenden Operation gemäß Absatz 4, in der erstmals die Verwirklichung von Straftatbeständen von erheblicher Bedeutung erkennbar wird, dient wie § 9b Absatz 3 Satz 3 BVerfSchG der Wahrung rechtsstaatlicher Prinzipien. Da nur die rechtswidrige Tatbestandsverwirklichung erfasst wird, fallen nach Absatz 3 erlaubte Handlungen nicht hierunter.

Ungeachtet der bereits jetzt nach §§ 54, 96 StPO (teilweise in analoger Anwendung) bestehenden Möglichkeiten, vom BND geführte Personen für die Zeugenvernehmung in einem Strafverfahren zu sperren bzw. ihre Aussage von einer vorherigen Genehmigung abhängig zu machen, stellt Absatz 6 solche Personen unabhängig von einer förmlichen Verpflichtung (nach dem Verpflichtungsgesetz) wie die Parallelvorschrift in § 9b Absatz 5 BVerfSchG unter eine gesetzliche Verschwiegenheitspflicht. Über die Erteilung einer Aussagegenehmigung hat der BND nach pflichtgemäßem Ermessen zu entscheiden.

Zu § 5b

Die Befugnis erlaubt Eingriffe in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Dessen Schutz ist besondere Ausprägung des allgemeinen Persönlichkeitsrechts, die einerseits der rechtstatsächlichen Bedeutung einer Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und andererseits der Eingriffsbreite eines Zugriffs nicht lediglich auf einzelne Kommunikationsvorgänge oder gespeicherte Daten, sondern auf das informationstechnische System insgesamt Rechnung trägt (BVerfGE 120, 274, Rn. 201).

Für die Auftragserfüllung des BND ist die Nutzung informationstechnischer Systeme in bestimmten Fällen unverzichtbar, z.B. wenn sich für die Sicherheitspolitik der Bundesrepublik bedeutsame Informationen besonders zuverlässig,

authentisch und konzentriert gerade auf Datenträgern in solchen Systemen finden. Der besonderen Intensität derartiger Eingriffe in informationstechnische Systeme von Personen mit Inlandsbezug, d.h. von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, wird BND-spezifisch mit der Anknüpfung an die materiellen Zulässigkeitsvoraussetzungen von Maßnahmen nach §§ 3, 5 Artikel 10-Gesetz, also Fälle bestimmter gravierender Straftaten bzw. Sachverhalte mit besonderen Gefahren für die Bundesrepublik oder ihre Bevölkerung, Rechnung getragen.

Unter „technischen Mitteln" im Sinne des Absatzes 1 sind informationstechnisch basierte nachrichtendienstliche Mittel (IT-basierte ND-Mittel), zu verstehen, die dem heimlichen Aufklären von und/oder der Teilhabe an informationstechnisch erzeugten, verarbeiteten und gespeicherten Daten ohne oder gegen den Willen der Zielperson oder des Dateninhabers auf einem Zielsystem bzw. Zielbereich dienen. Die möglichen IT-basierten ND-Mittel können nicht abschließend dargestellt werden, sie unterliegen einer ständigen Weiterentwicklung.

Folgerichtig zu den an §§ 3, 5 Artikel 10-Gesetz orientierten materiellen Eingriffsvoraussetzungen in Absatz 1 ist die formell-verfahrensseitige Absicherung der Maßnahmen ebenfalls in enger Anlehnung an die Regelungen des Artikel 10-Gesetzes ausgestaltet. So kommen nach Absatz 2 die Verfahrenssicherungen für Anordnung und Kontrolle die §§ 9 bis 12, § 14 Absatz 1 und § 15 Absatz 5 bis 7 Artikel 10-Gesetz zur Anwendung, insbesondere also die Kontrolle durch die unabhängige G10-Kommission. Insgesamt tritt hierbei nach Absatz 2 Satz 1 an die Stelle des Bundesministerium des Innern das Bundeskanzleramt. In Absatz 2 Satz 3 ist die Möglichkeit der Eilanordnung geregelt.

Diesem Regelungskonzept folgt auch Absatz 3, der für die Weiterverarbeitung der Daten inklusive Übermittlung an andere öffentliche Stellen auf die jeweiligen Vorschriften des Artikel 10-Gesetz verweist. Der Begriff der Verarbeitung folgt der neuen Datenschutzterminologie und umfasst damit auch die Nutzung.

Für Datenerhebungen aus informationstechnischen Systemen, die nicht unter Absatz 1 fallen, ist § 5 c einschlägig.

Während Absätze 1 bis 3 Ausprägungen der Vertraulichkeit informationstechnischer Systeme sind, schützt Absatz 4 die Integrität des Systems.

Absatz 5 berücksichtigt systematisch ähnlich wie § 5 Absatz 4 Satz 2 die Tatsache, dass ein Eingriff in ein informationstechnisches System angesichts der vielfachen Sozialbezogenheit dort gespeicherter Daten andere Personen betreffen kann, beschränkt diese Drittbetroffenheit aber auf unvermeidbare und damit sachlich zwingend notwendige Fälle.

Der Anwendungsbereich von § 9d bezieht sich auf den besonderen Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme, der eröffnet ist, soweit andere Freiheitsgewährleistungen, keinen oder keinen hinreichenden Schutz gewähren. Daraus folgt, dass § 9d zum Beispiel keine Anwendung findet, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dann ist Artikel10 Absatz1 GG alleiniger grundrechtlicher Maßstab und die Rechtmäßigkeit der eingreifenden Maßnahme an den Vorschriften des Artikel 10-Gesetzes zu messen.

Zu § 5c

Wie zu § 5b ausgeführt, ist für die Auftragserfüllung des BND die Nutzung informationstechnischer Systeme in bestimmten Fällen unverzichtbar, z.B. wenn sich für die Sicherheitspolitik der Bundesrepublik kritische Informationen besonders zuverlässig, authentisch und konzentriert gerade auf Datenträgern in solchen Systemen finden. Dies gilt auch und insbesondere hinsichtlich informationstechnischer Systeme von Ausländern im Ausland, da naturgemäß im Hinblick auf den auslandsbezogenen gesetzlichen Auftrag des Bundesnachrichtendienstes die Aufklärung von Sachverhalten und diesbezüglich relevanter Akteure im Ausland grundsätzlich von besonderer Bedeutung ist.

Der besonderen Intensität von Eingriffen in informationstechnische Systeme von Personen mit Inlandsbezug, d.h. von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen, wird BND-spezifisch in §5b mit der Anknüpfung an die materiellen Zulässigkeitsvoraussetzungen von Maßnahmen nach

§§ 3, 5 Artikel 10-Gesetz, also Fälle gravierender Straftaten bzw. Sachverhalte mit besonderen Gefahren für die Bundesrepublik oder ihre Bevölkerung, Rechnung getragen. Daneben soll mit dem neuen § 5c eine klarstellende Regelung für die vom Inland aus durchgeführte Datenerhebung aus informationstechnischen Systemen von Ausländern im Ausland geschaffen werden. Die Datenerhebung aus informationstechnischen Systemen von Ausländern im Ausland knüpft hierbei an dieselben Voraussetzungen an, unter denen auch die Erhebung von Informationen einschließlich personenbezogener Daten betreffend die Telekommunikation von Ausländern im Ausland nach § 6 Absatz 1 zulässig ist. Absatz 1 trifft hierzu die entsprechenden Regelungen. Grundlage für Datenerhebungen aus informationstechnischen Systemen von Ausländern im Ausland, die vom Ausland aus durchgeführt werden, ist weiterhin § 1 Absatz 2.

Absatz 2 regelt besondere Voraussetzungen für die Erhebung von Daten aus informationstechnischen Systemen von Unionsbürgerinnen und Unionsbürgern, die sich an der parallelen Regelung für die Ausland-Ausland-Fernmeldeaufklärung in § 6 Absatz 3 und 4 orientieren und damit nur in eng umgrenzten Ausnahmefällen zulässig sind. Ebenso wie in § 6 Absatz 3 ist zur Erfüllung der in Absatz 2 Nummer 1 genannten Voraussetzung der Aufklärung von Gefahren im Sinne des § 5 Artikel10-Gesetz kein Inlandsbezug notwendig.

Nach Absatz 3 sind Erhebungen aus informationstechnischen Systemen von Einrichtungen der Europäischen Union und von öffentlichen Stellen ihrer Mitgliedstaaten unzulässig.

Absatz 4 bestimmt, dass die Einzelheiten der Umsetzung der Erhebung von Daten aus informationstechnischen Systemen von Ausländern im Ausland, u.a. die BND-internen Abläufe und Zuständigkeiten, Prüf- und Unterrichtungsvorgaben sowie technische Details der Maßnahmen, in einer Dienstvorschrift zu regeln sind. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes, das das Parlamentarische Kontrollgremium unterrichtet.

Zu § 5d

In § 5d erfährt die bereits bisher eröffnete Möglichkeit zur

heimlichen Informationserhebung aus Wohnungen (§ 5 BNDG i.V.m. § 9 Absatz 2 BVerfSchG a.F.) eine umfassende Neuregelung. Schon aus Verhältnismäßigkeitserwägungen darf der BND dieses nachrichtendienstliche Mittel nicht als gängiges Instrument der Informationsbeschaffung einsetzen. Die verfahrensrechtlichen und materiellen besonderen Vorgaben für den Einsatz in dieser Vorschrift, auch mit ihren Verweisen in das Artikel 10-Gesetz, sichern dies zusätzlich ab. Die Befugnis deckt sich in der Einsatzschwelle grundsätzlich mit § 5b, wobei zusätzlich der spezifisch zu Wohnungen gebotene Schutz des Kernbereichs privater Lebensgestaltung bereits im Rahmen des Eingriffssachverhalts gewürdigt wird.

Prognosemaßstab für die Frage, in welchen Fällen eine Erfassung von Äußerungen aus dem Kernbereich privater Lebensführung anzunehmen ist, ist gemäß der verfassungsgerichtlichen Rechtsprechung eine Wahrscheinlichkeitsbetrachtung (BVerfGE 141, 220 [300]). Demnach ist zwar nicht erforderlich, dass derartige Erfassungen von vornherein kategorisch ausgeschlossen werden können; besteht jedoch die Wahrscheinlichkeit, dass die Überwachungsmaßnahme in den Kernbereich eindringt, also bei entsprechender positiver Prognose, ist sie unzulässig.

Auch hinsichtlich der Weiterverarbeitung, einschließlich der Übermittlung, wird auf die Vorschriften aus § 5b, hier Absatz 3, verwiesen.

Absatz 2 regelt die Maßnahmenrichtung verschärfend zu den allgemeinen Vorgaben nach §5 Abs. 4. Er beschränkt die Erhebungsmethodik für den BND mit der Anknüpfung an §§ 3, 5 Artikel 10-Gesetz auf Fälle gravierender Straftaten bzw. Sachverhalte mit besonderen Gefahren für die Bundesrepublik oder ihre Bevölkerung. Die Eingriffsbefugnis ist damit auch insofern materiell an die gleichen Gefahrenlagen geknüpft wie Eingriffe nach § 5b. Das entspricht der bundesverfassungsgerichtlichen Rechtsprechung zur Schwere dieser beiden Eingriffsarten (vgl. BVerfGE 141, 220 [304]).

Für die Auftragserfüllung des BND können solche Datenerhebungen aus Wohnungen beispielsweise eine Rolle spielen, wenn aus behördlichem Vorwissen bekannt ist, dass bei einem Treffen in einer Wohnung, einem Hotelzimmer oder

anderen unter den verfassungsrechtlichen Wohnungsbegriff fallenden Räumlichkeiten Anschlagsplanungen, Proliferationssachverhalte oder Schleusungsvorgänge von erheblicher Bedeutung besprochen werden sollen (§ 5c Absatz 2 Satz1 i.V.m. § 3 Absatz 1 Nr. 6 bzw. § 5 Absatz 1 Satz 1 Nr. 2, 3 oder 7 Artikel 10-Gesetz).

Absatz 3 verweist zum Anordnungs- und Kontrollverfahren weitgehend auf das Artikel 10-Gesetz mit entsprechenden Anpassung in Absatz 2 Satz 1 Nummer 1 bis 3. Da Artikel 13 Absatz 4 GG jedoch ausdrücklich eine „richterliche Entscheidung" verlangt, wird in Absatz 3 Satz 2 zusätzlich für die Entscheidung über die Zulässigkeit der Maßnahme – die Zuständigkeit des Bundesverwaltungsgerichts (vgl. § 50 Absatz 1 Nummer 4 VwGO) bestimmt. Die Maßnahme darf grundsätzlich erst vollzogen werden, wenn das Bundesverwaltungsgericht die Zulässigkeit festgestellt hat. Nach Satz 3 besteht die Möglichkeit eines Eilverfahrens.

Das Verfahren dieses neu eingeführten Feststellungsverfahrens wird in Absatz 4 besonders geregelt. Es orientiert sich an der bewährten Verfahrenspraxis der G 10-Kommission unter Anlehnung an Geheimschutzregelungen des § 99 Absatz 2 VwGO. U.a. steht es dabei im Ermessen des Gerichts, die Verfahrensbeteiligten vor einer Entscheidung anzuhören oder ausschließlich auf Grundlage der eingereichten Unterlagen zu entscheiden.

Aufgrund den Vorgaben in Artikel 13 Absatz 5 GG bedarf der Einsatz von BND Mitarbeitern oder Quellen auch bei eingeweihtem Wohnungsinhabers einer besonderen Befugnis, wenn er – ohne Wissen des Wohnungsinhabers – durch technische Überwachung abgesichert erfolgt. Absatz 5 stellt eine solche Befugnis dar. Praktischer Anwendungsfall hierfür sind etwa Situationen, in denen der BND Anhaltspunkte dafür hat, dass seinen Mitarbeitern oder Quellen bei einem Treffen durch die anderen Treffteilnehmer, z.B. aus einem gewaltbereiten Milieu, Gefahren für Leib oder Leben drohen könnten.

Das zudem in Absatz 6 vorgesehene Betretungsrecht ist die fachlich notwendige Ergänzungsbefugnis, um Maßnahmen nach Absatz 1 und 5 durchführen zu können. Satz 3 komplettiert dies

mit der Klarstellung, dass auch Vorbereitungsmaßnahmen nur in der Wohnung des Adressaten der Überwachungsanordnung nach Absatz 2 zulässig sind. Heimlich betreten erfasst hierbei das Betreten ohne Kenntnis des Wohnungsinhabers.

Zu § 5e

§ 5e greift die Zulässigkeitsschranken der §§ 5 BNDG, 9 Absatz 1 BVerfSchG a.F. auf (Absätze 1, 6), ergänzt sie aber sehr detailliert und trägt damit dem Erfordernis rechtsklar definierter gesetzlicher Eingriffsschranken Rechnung.

Dabei wird eingangs (Absatz 1 Satz 1) klargestellt, dass Schutznormen der Rechtspflege (also insbesondere §§ 153 ff. StPO) und der parlamentarischen Kontrolle (z.B. § 5 Absatz 2 PKGrG) durch den Einsatz nachrichtendienstlicher Mittel generell nicht beeinträchtigt werden dürfen.

Die Subsidiaritätsregel aus Satz 2 und 3 besagt nicht, dass das Vorfinden einer Information in allgemein zugänglichen Quellen deren Verifizierung oder Falsifizierung mit nachrichtendienstlichen Mitteln verbietet. Nachrichtendienstliche Aufklärung kann auch dazu dienen, aus anderem Aufkommen erhältliche Informationen auf ihre inhaltliche Belastbarkeit zu prüfen und so Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu erhalten.

Die Absätze 2 bis 5 enthalten neue Bestimmungen zum Kernbereichsschutz und zum Schutz der dort genannten Träger von Berufsgeheimnissen. Dabei werden die schutzwürdigen Interessen der Betroffenen und bestehende Kontrollerfordernisse gegenüber dem besonderen Geheimhaltungsbedürfnis des BND bei operativ hochsensiblen und daher besonders schutzwürdigen Informationen ausbalanciert.

Im Umkehrschluss sich bereits aus der jeweiligen Befugnisnorm ergebend, wird in Absatz 6 noch einmal ausdrücklich festgestellt, dass eine Maßnahme unverzüglich zu beenden ist, wenn ihr Zweck erreicht ist oder feststeht, dass er nicht (mehr) erreichbar ist.

Zu Nummer 4 (§ 20)

Die Einfügung des neuen Satzes 2 in Absatz 1 stellt klar, dass der

pauschale Verweis des Satzes 1 auf § 12 BVerfSchG keine Vorgabe einer Höchstspeicherfrist, wie in § 12 Absatz 3 Satz 2 BVerfSchG geregelt, umfasst. Zum Auftrag des BND gehört es, außen- und sicherheitspolitisch relevante Informationen über das Ausland zu beschaffen, auszuwerten und der Bundesregierung Bericht zu erstatten. Hierfür müssen z.B. länderbezogene Analysen über einen langen Zeitraum in detailintensiver Arbeit aufgebaut und auch mit früheren Analysen verglichen werden. Diesem Umstand hat der Gesetzgeber mit der Regelung in §20 Rechnung getragen, als er für den BND eine regelmäßige Prüffrist nach spätestens zehn Jahren festschreibt, ohne eine Höchstspeicherfrist vorzugeben. Diese gesetzgeberische Intention wird mit dem neuen Satz 2 im Sinne der Rechtsklarheit normativ bestätigt.

Zu Nummer 5 (§ 23a)

§ 23a BNDG überführt eine zuvor in § 17 Absatz 3 BVerfSchG normierte Befugnis des BND systemgerecht in das BNDG. Erkenntnisziel des BND sind Reisebewegungen, insbesondere von Personen, die als Quellen für den BND in Betracht kommen oder bereits geführt werden.

Auch hier ist wie in der Parallelvorschrift des § 17 BVerfSchG n.F. – die Konkretisierung des fraglichen Personenkreises enger gefasst als die allgemeine Befugnis zu Übermittlungsersuchen nach § 23 Absatz 3 BNDG i.V.m. § 18 Absatz 3 BVerfSchG. Die Ausschreibung erfolgt im vom BKA betriebenen polizeilichen Informationsverbund, im geschützten Grenzfahndungsbestand der Bundespolizei oder auch in Datenbanken der EU, aktuell dem Schengener Informationssystem. Soweit es um EU-Datenbanken geht, sind die dafür bestehenden unionsrechtlichen Regulierungen zu beachten.

Zu Nummer 6 (§ 24a)

Durch die Neuschaffung des § 24a wird neben einer Verbesserung der Zusammenarbeit zwischen dem BND und anderen inländischen öffentlichen Stellen der Schaffung von Redundanzen in Form paralleler Ressourcen vorgebeugt. Absatz 1 regelt die Zusammenarbeit des BND mit anderen zur Fernmeldeaufklärung befugten inländischen öffentlichen Stellen, insbesondere der Bundeswehr. Für diese anderen öffentlichen Stellen ist das Vorhalten von Erfassungssystemen, die bei entsprechendem

Bedarf eine Vielzahl von Gebieten weltweit abzudecken vermögen, weder rechtlich geboten noch wirtschaftlich vertretbar. Vielmehr handelt es sich dabei um eine Aufgabe im Zuständigkeitsbereich des BND nach §1 Absatz 2.

Die Datenverarbeitung und -übermittlung nach Absatz 1 durch den BND wird jeweils auf ein konkretes Ersuchen bewilligt, sofern der BND über entsprechende Technik und Personal verfügt. Sie umfasst insbesondere die Erhebung der Daten, eine eventuelle weitere Bearbeitung und Speicherung sowie die (automatisierte) Übermittlung an die ersuchende Behörde. Auch unselektierte, unbearbeitete Informationen einschließlich personenbezogener Daten können Gegenstand der Übermittlung sein; für die (weitere) Selektion und Verarbeitung ist die ersuchende Behörde nach eigenem Recht zuständig (Absatz 2). Die Datenverarbeitung nach § 24a umfasst vom Inland aus erhobene Daten; die Verarbeitung und Übermittlung vom Ausland aus stützt sich weiterhin auf § 1 Absatz 2 BNDG.

Die Möglichkeit einer automatisierten Übermittlung der Daten ist erforderlich, um auch zeitkritischen Bedarf der ersuchenden Behörde decken zu können. Ein solcher besteht beispielsweise bei der Bundeswehr betreffend Informationen zur aktuellen Sicherheitslage in deren Einsatzgebieten im Ausland zum Schutz des Bundeswehrpersonals. Um etwa Versorgungsrouten und Patrouillen sicher planen und durchführen zu können, sind für die Bundeswehr auch kurzfristige, mitunter stündliche Lageveränderungen von essentiellem Interesse. § 24 ist insoweit nicht anzuwenden, zumal sich sowohl das Ersuchen an den BND als auch die Verarbeitung der Informationen durch die ersuchende Behörde zu eigenen Zwecken nach den für diese geltenden Vorschriften richten. Damit ist die Gesetzmäßigkeit der Gesamtmaßnahme sichergestellt.

Absatz 2 nimmt eine Abgrenzung der Zuständigkeitsbereiche vor: Die Prüfung der sachlichen Zuständigkeit und rechtlichen Befugnis zur Verarbeitung der Informationen zu eigenen Zwecken obliegt der ersuchenden Behörde, während der BND für die technische Durchführung der Maßnahme verantwortlich ist. Dabei verarbeitet der BND nur Informationen aus Telekommunikationsnetzen, die zuvor durch Anordnung nach §§ 6 Absatz 1 Satz 2, 9, 12 Absatz 2 zur Datenerhebung oder zur Eignungsprüfung bestimmt worden

sind.

Die Datenverarbeitung nach Absatz 1 kann sich mit Handlungen, die dem BND als eigene Aufgabe obliegen, überschneiden. So umfasst etwa im Falle der Zusammenarbeit mit der Bundeswehr der Aufgabenbereich des BND im Rahmen seines Gesamtauftrages mit strategischer Zielsetzung auch die Sicherheit der Bundeswehr in deren Einsatzgebieten.

Daher ist eine Verwendung der nach Absatz 1 erhobenen Daten durch den BND im Rahmen seiner eigenen Aufgabenerfüllung angezeigt, um parallele Datenerhebungen und damit eine Vergeudung von Ressourcen zu vermeiden. Die Verarbeitung der Daten zu eigenen Zwecken erfolgt nach den Vorschriften dieses Gesetzes, insbesondere §§ 6 ff. (Ausland-Ausland-Fernmeldeaufklärung, hier speziell unter Beachtung von §6 Absatz 2 und § 7 Absatz 1) und § 12 (Eignungsprüfung im Rahmen der Ausland-Ausland-Fernmeldeaufklärung, hier speziell unter Beachtung von § 12 Absatz 3).

Nach Absatz 4 wird die Möglichkeit der ressourcenschonenden Zusammenarbeit auch auf Datenerhebungen aus informationstechnischen Systemen mit technischen Mitteln ohne Wissen des Betroffenen ausgeweitet, sofern die ersuchende Behörde eine entsprechende Erhebungsbefugnis besitzt. § 6 und § 12, die sich auf Telekommunikationsnetze beziehen, finden insofern keine Anwendung.

Zu Nummer 7 (§ 25)

Die Änderung des § 25 dient einer effektiveren Zusammenarbeit der dort genannten Gefahrenabwehrbehörden sowie gleichzeitig einer stärker nach den jeweils beteiligten Behörden differenzierten Ausgestaltung der einzelnen Kooperationsbeziehungen. Hierzu wird die Möglichkeit gemeinsamer Dateien des BND mit dem BfV und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) neu – ohne Projektbezug oder Befristung – geregelt (Absatz 1) und die bisherigen Vorgaben für die Zusammenarbeit in gemeinsamen Dateien mit Polizeibehörden oder dem Zollkriminalamt – unter Beibehaltung des Projektbezugs bzw. Befristung beibehalten (Absatz 2).

Absatz 1 ermöglicht gemeinsame Dateien mit den Verfassungsschutzbehörden und dem Militärischen Abschirmdienst, nimmt aber das Bundesamt für Sicherheit in der Informationstechnik (BSI) in dessen zentraler Funktion bei der Bekämpfung von Gefahren aus dem Cyber-Raum als zulässigen Beteiligten auf. Zulässig sind solche Dateien sowohl mit einer als auch mit mehreren der aufgezählten Behörden. Das bisherige Befristungserfordernis entfällt, da eine effektive Aufgabenerfüllung zum Schutz vor den in der Vorschrift genannten Gefahren (Anknüpfung an § 5 Absatz 1 Artikel 10 Gesetz) längerfristige Kooperationen verlangt.

Der neue Absatz 1a hingegen zieht vor dem Hintergrund des Trennungsgebotes für gemeinsame Dateien des BND mit Polizeibehörden oder dem Zollkriminalamt engere Grenzen und belässt auch die Erfordernisse von Befristung und Projektbezogenheit.

Die Sätze 3 und 4 des bisherigen Absatzes 1 werden aus systematischen Gründen zu den Verarbeitungsregelungen in Absatz 2 verschoben, während die zulässigen Zwecke und Teilnehmer gemeinsamer Dateien nun in den neuen Absätzen 1 und 1a geregelt werden.

Durch die Ergänzung des Absatzes 3 neu eingeführt wird die Klarstellung, dass im Falle des Ausscheidens eines Teilnehmers die Verantwortung der speichernden Stelle zu den eingegebenen und damit rechtlich an alle Teilnehmer übermittelten Datensätze auf den BND als dateiführende Stelle übergeht. Die eingebende Stelle bleibt als funktionaler Datenübermittler nachberichtspflichtig nach § 26 BVerfSchG

Zu Nummer 8 (§ 26)

Mit der Beteiligungsmöglichkeit von MAD und BfV an gemeinsamen Dateien mit ausländischen öffentlichen Stellen wird Gleichlauf zur ebenfalls neuen Vorschrift des § 22b Absatz 1 Satz 2 BVerfSchG [+ ggf. Verweis auf entsprechende neue Passage im MADG] hergestellt.

Zu Nummer 9 (§ 36)

Mit Ablauf des 31. Dezember 2017 ist die in § 36 durch das Gesetz

zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes aufgenommene Übergangsregelung obsolet geworden.

An dessen Stelle tritt nunmehr eine zentrale Norm um dem Zitiergebot Rechnung zu tragen.

Zu Artikel 4 (Änderung des SÜG)

Zu Nummer 1 (§ 2)

Die Streichung des Schriftformerfordernisses für die Zustimmung zur Sicherheitsüberprüfung ist Voraussetzung für eine weitere Modernisierung und möglichst medienbruchfreie Durchführung des Sicherheitsüberprüfungsverfahrens. Bereits heute werden die von einer Sicherheitsüberprüfung betroffenen oder mitbetroffenen Personen angehalten, ihre Sicherheitserklärungen möglichst über ein elektronisches Formular abzugeben. Einer elektronischen Übermittlung der so ausgefüllten Formulare zur Sicherheitserklärung steht derzeit jedoch das Schriftformerfordernis entgegen. Somit müssen bisher betroffene und mitbetroffene Personen die elektronisch ausgefüllten Sicherheitserklärungen ausdrucken, unterschreiben und den zuständigen Stellen persönlich oder auf dem Postweg zuleiten. Dies verursacht zum einen vermeidbare Kosten und Aufwände. Zum anderen verlängert sich das Sicherheitsüberprüfungsverfahren um die entsprechenden Postlaufzeiten, was insbesondere in Eilfällen zu vermeiden ist.

Die Warnfunktion, die einer schriftlichen Zustimmung zukommen soll, ist im Falle der Zustimmung zur Sicherheitsüberprüfung bereits dadurch sichergestellt, dass die betroffenen und mitbetroffenen Personen eine mehrere Seiten lange Sicherheitserklärung mit persönlichen Angaben befüllen müssen. Dies erfordert eine intensive Auseinandersetzung mit dem eigenen Lebensweg zumindest der letzten fünf Jahre. Ein unbedachtes Ausfüllen und Absenden der Sicherheitserklärung ist somit auch ohne Schriftformerfordernis ausgeschlossen. Hinzu kommt, dass eine einmal erteilte Zustimmung zur Sicherheitsüberprüfung jederzeit widerrufen werden kann. Folge ist, dass die weitere Durchführung einer Sicherheitsüberprüfung unzulässig und diese wegen des daraus resultierenden Verfahrenshindernisses einzustellen ist.

Zu Nummer 2 (§ 12)

Es handelt sich bei der Änderung um eine redaktionelle Klarstellung, die die amtliche Bezeichnung des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik in das Gesetz aufnimmt.

Zu Nummer 3 (§ 13)

Die Möglichkeit zur alternativen Angabe von telefonischer oder elektronischer Erreichbarkeit der betroffenen Personen sowie der Referenz- und Auskunftspersonen hat sich in der Praxis nicht bewährt. Die Angabe der Erreichbarkeiten ist erforderlich für mögliche Rückfragen zur Sicherheitserklärung; insbesondere aber für Terminabsprachen zu Befragungen der betroffenen Personen oder der Referenz- und Auskunftspersonen. Festzustellen ist, dass zu vielen Personen lediglich die elektronischen Erreichbarkeiten angegeben werden. Terminabsprachen auf allein elektronischem Weg gestalten sich in der Praxis in vielen Fällen schwierig. Teilweise erfolgt keine oder aber eine verzögerte Reaktion auf eine elektronische Kontaktaufnahme; teilweise bedarf es mehrerer Kontaktaufnahmen, bis erfolgreich ein Gesprächstermin vereinbart werden kann. Dies führt immer wieder dazu, dass sich notwendige Befragungen durch Sicherheitsermittler verzögern und dadurch die Dauer von Sicherheitsüberprüfungen ansteigt. Weitere Unannehmlichkeiten für die betroffenen Personen oder die Referenzpersonen können entstehen, wenn Termine seitens der Sicherheitsermittler kurzfristig verschoben oder gar abgesagt werden müssen. In solchen Fällen ist nicht sichergestellt, dass den Betroffenen die notwendigen Informationen zeitgerecht erreichen. Vor diesem Hintergrund erscheint die gleichzeitige Angabe sowohl der telefonischen als auch der elektronischen Erreichbarkeit angezeigt.

Der Bedarf, der Sicherheitserklärung zwei aktuelle Lichtbilder beizufügen, besteht aufgrund der durch das erste Gesetz zur Änderung des Sicherheitsüberprüfungsgesetzes eingeführten Maßnahme der Internetrecherche im Rahmen von Sicherheitsüberprüfungen. Bei der Durchführung dieser Maßnahme stehen die mitwirkenden Behörden immer wieder vor der Frage, ob Inhalte im Internet den betroffenen Personen

zugeordnet werden können. Aufgrund von Namensidentitäten kann es ohne die Möglichkeit eines (automatisierten) Lichtbildabgleichs zunächst zu einer Vermutung für eine Zuordnung zur betroffenen Person kommen. Ob diese Zuordnung tatsächlich zutrifft kann in solchen Fällen oftmals nur durch eine verwaltungsaufwändige Eigenbefragung der betroffenen Person erfolgen. So muss mit der betroffen Person ein Gesprächstermin vereinbart werden und ein Sicherheitsermittler im Rahmen einer Dienstreise diesen Gesprächstermin wahrnehmen. Häufig könnte in diesen Fällen eine Zuordnung bereits durch einen einfachen Lichtbildabgleich bestätigt oder ausgeschlossen werden. Das Beifügen von (elektronischen) Lichtbildern entlastet somit den Verwaltungsaufwand bei den mitwirkenden Behörden. Die bislang erforderlichen Eigenbefragungen durch Sicherheitsermittler entfallen in vielen Fällen künftig. Dadurch werden auch die betroffenen Personen entlastet. Auch für diese ist es künftig in einer Vielzahl von Fällen nicht mehr erforderlich, Terminabsprachen mit Sicherheitsermittlern zu treffen, um mögliche Fehlzuordnungen auszuräumen.

Zu Nummer 4 (§ 20)

Zu Buchstaben a) und b)

In beiden Absätzen wird durch die Benennung der einschlägigen Normen konkretisierend dargestellt, welche personenbezogenen Daten seitens der zuständigen Stelle sowie der mitwirkenden Behörde zur Erfüllung ihrer Aufgaben in Dateien gespeichert, verändert und genutzt werden dürfen. Die Ergänzung in beiden Absätzen dient der Klarstellung, dass die Speicherbefugnis alle in § 13 Absatz 1 Nummer 1 bis 6 genannten Datenkategorien unabhängig von der Rechtsgrundlage der Erhebung umfasst. So enthält § 13 Absatz 1 Nummer 5 eine zeitliche Begrenzung der anzugebenen Wohnsitze, die jedoch die Befugnis zur Speicherung weiterer, rechtmäßig erhobener Wohnsitzdaten (vgl. § 13 Absatz 4 Satz 1 Nummer 1) unberührt lässt. In Absatz 1 wird ferner die Speicherbefugnis der zuständigen Stelle um Daten der mitbetroffenen Person erweitert. Die Speicherung ist notwendig, um Daten aus elektronisch eingehenden Sicherheitserklärungen für die Nutzung durch die mitwirkende Behörde weiterverarbeiten zu können.

Zu Buchstabe c)

Es handelt sich bei der Einfügung um eine Präzisierung der Verweisung.

Zu Artikel 5 (Änderung G 10)

Zu Nummer 1 (§ 2 Absatz 2 Satz 3)

Die vorgesehene Änderung dient der Verwaltungsvereinfachung. Mit der Vorschrift sollen verfahrensbedingte Verzögerungen notwendiger Beschränkungsmaßnahmen vermieden werden. Insofern ist es sachgerecht, die Entscheidung über die Durchführung einer Beschränkungsmaßnahme auch für den Ausnahmefall, dass eine Sicherheitsüberprüfung noch nicht abgeschlossen werden konnte, unmittelbar der berechtigten Stelle als sachlich vollziehende Verwaltungsbehörde zu übertragen.

Zu Nummer 2 (§ 3a)

Die Änderung nach Buchstabe a) ist eine Folgeänderung zur Änderung nach Buchstabe c).

Die Änderung nach Buchstabe b) passt die Löschungsregelung des Artikel 10-Gesetzes – in Übereinstimmung mit dem neuen § 9a Absatz 2 Satz 5 Nummer 1 BVerfSchG – an Vorgaben des Bundesverfassungsgerichtes an (BVerfGE 141, 220 – Rn. 205).

Buchstabe c) ergänzt – in Anlehnung an § 51 Absatz 8 BKAG – eine Eilfallregelung, um den Behörden für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen (BVerfGE 141, 220 – Rn. 129).

Zu Nummer 3 (§ 3b)

Die Änderung erweitert den geschützten Personenkreis im Anschluss an jüngere Verfassungsrechtsprechung (BVerfGE 141, 220 – Rn. 257).

Zu Nummer 4 (§ 4)

Zu Buchstaben a) und c)

Die Streichung dient wirtschaftlicher Verwaltung durch Bürokratieentlastung. Eine halbjährliche Sonderprüfung von TKÜ-Aufkommen ist nicht einmal im polizeilichen Verwendungskontext – also bei Zwangsbefugnissen – nach der

Strafprozessordnung oder den Polizeigesetzen vorgesehen und ebenso bei der nachrichtendienstlichen Aufklärung funktionslos, aber aufwändig. Angesichts der gesetzlichen Voraussetzungen sind G 10-Maßnahmen auf besonders aktiv und intensiv betriebene Aufklärungssachverhalte beschränkt. In diesen Vorgängen erfolgt bereits aus operativen Erfordernissen zielführender Aufklärung eine permanente Qualitätssicherung auch durch laufende Relevanzabschätzung der vorliegenden Informationen. Werden danach G 10-Erkenntnisse als relevant erkannt, ist angesichts der spezifischen Verlässlichkeit des technischen Informationsaufkommens dessen Weiterverarbeitung typischerweise besonders bedeutsam für die bezweckte Aufklärung von Bedrohungen. Die speziellen gesetzlichen Prüfroutinen laufen demgemäß erwartbar und zugleich sachangemessen in der Praxis leer. Die Regelung ist nicht geeignet, den verfolgten Zwecken zu dienen, produziert aber erhebliche Bürokratielasten. Sie wird daher gestrichen. Qualitätssicherung und Datenschutz bleiben auch insoweit angemessen nach § 12 BVerfSchG gewährleistet, abgestützt zusätzlich durch die besonderen jährlichen Prüfungen nach § 12 G 10 bis zur Mitteilung an den Betroffenen.

Die Änderung in Absatz 6 vollzieht die Änderung des Absatzes 1 komplementär nach.

Zu Buchstabe b)

Die neue Nummer 4 befugt nunmehr ausdrücklich auch zur Mitwirkung an Sicherheitsüberprüfungen und entsprechenden Personenüberprüfungen zum vorbeugenden personellen Staatsschutz. Dies bleibt konsistent zur verfassungsschutzinternen Verwendung nach Absatz 2 Satz 3, denn solche Personenüberprüfungen sind speziell darauf gerichtet, diese Schutzgüter vorbeugend zu schützen. Werden bei der Überwachung von Angehörigen ausländischer Nachrichtendienste qualifizierte Kontakte zu einer Person mit Verschlusssachenzugriff bekannt, muss dies auch für Zwecke des Geheimschutzes verwertbar und müssen entsprechende Risiken an den Geheimschutzbeauftragten übermittelbar sein.

Zu Nummer 5 (§ 8 Absatz 3 Satz 4 G10):

In § 8 Absatz 3 Satz 4 wird die Zulässigkeit von

Überwachungsmaßnahmen um die Alternative erweitert, dass, die Suchbegriffe auch Identifizierungsmerkmale enthalten dürfen, die zu einer gezielten Erfassung der Rufnummer oder einer anderen Kennung des Telekommunikationsanschlusses einer anderen Personen als derjenigen führen, bei der die Gefahr für Leib und Leben vorliegt. Voraussetzung ist, dass diese dritte Person der Maßnahme zustimmt.

Anwendungsfall des § 8 sind typischerweise Entführungsfälle im Ausland. Anwendungsfall für die Erweiterung sind beispielsweise Personen aus dem familiären oder beruflichen Umfeld der entführten Person, bei denen damit gerechnet werden kann, dass sie durch die Entführer oder sonstige in dem Vorgang involvierte Personen aus dem Lager bzw. Umfeld der Entführer kontaktiert werden.

Die Maßnahme ist nur mit Zustimmung der dritten Person zulässig. Dadurch wird dem Umstand Rechnung getragen, dass die Telekommunikation dieser Person überwacht wird, obwohl sie selbst an der Verursachung der Gefahrensituation nicht beteiligt ist und damit trotz der Erweiterung der Schutz ihres Telekommunikationsgeheimnisses gewährleistet.

Zu Nummer 6 (§ 9 Absatz 3 Satz 2)

Es handelt sich um eine Folgeänderung zu Nummer 6.

Zu Nummer 7 (§ 11)

Da sich in der Gesetzgebungspraxis spezielle Regelungen zur sogenannten Quellen-TKÜ etabliert haben, wird auch das Artikel 10-Gesetz mit dem in § 11 eingefügten Absatz 1a um eine solche Regelung zu dieser besonderen Form der Durchführung der Überwachungsmaßnahme ergänzt. Wie bereits in § 100a Absatz 1 Satz 3 in Verbindung mit Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO erstreckt sich die Regelung auf alle Inhalte und Umstände von Telekommunikation, die nach der Anordnung übertragen worden ist. Insoweit schließt sie „ruhende“ Kommunikation ein und geht über die Ausleitung laufender Kommunikation hinaus, bleibt dabei aber punktuell begrenzt auf Kommunikationssachverhalte, die aufgrund der Anordnung auch als laufende Kommunikation überwachbar waren.

Der neue Absatz 1b regelt den speziellen Fall einer technischen Erweiterung der gegen eine Person laufenden Maßnahme aufgrund eindeutiger Erkenntnisse über weitere Kennungen von Telekommunikationsanschlüssen dieser von der Maßnahme betroffenen Person. Voraussetzung ist, dass die Kennung durch eindeutige Auskunft nach § 112 des Telekommunikationsgesetzes, elektronische Aufklärung nach § 9 Absatz 1 Satz 2 Nummer 7 des Bundesverfassungsschutzgesetzes oder technische Mittel nach § 5 Absatz 1 Satz 2 Nummer 6 Bundesnachrichtendienstgesetz oder Hinweise ausländischer öffentlicher Stellen bekannt werden.

Dieser Sachverhalt füllt lediglich die mit der Anordnung getroffene Beschränkung aus, die auf dem begründenden Gefährdungssachverhalt beruht. Insofern reicht es aus, dass die G10-Kommission hierüber im Regelprozess nach § 15 Absatz 6 unterrichtet wird (sie also die Gesamtkontrolle behält), ohne dass dazu das Sonderverfahren einer zusätzlichen Eilanordnung nötig ist.

Zu Nummer 8 (§ 12)

Durch die Erweiterung wird die Möglichkeit eröffnet, von einer Mitteilung an den Betroffenen auch dann abzusehen, solange dies zu dessen Schutz vor Gefahren für Leib, Leben oder Freiheit erforderlich ist.

Die Ergänzung des § 12 Absatz 1 Satz 2 betrifft Betroffene, bei denen zu befürchten ist, dass durch die Vornahme der Mitteilung die Tatsache der Überwachung durch einen Nachrichtendienst Dritten bekannt wird. Insbesondere in Fallgestaltungen, in denen sich der Betroffene im Ausland aufhält, kann es vorkommen, dass die Mitteilung Sicherheitsdiensten des ausländischen Staates zur Kenntnis gelangt und diese gerade aufgrund dieser Kenntnis Maßnahmen mit Gefahren für Leib, Leben oder Freiheit des Betroffenen ergreifen.

Eine entsprechende Zurückstellung der Mitteilung bedarf einer auf tatsächlichen Anhaltspunkten beruhenden Begründung, bei der das aus dem Telekommunikationsgeheimnis abzuleitende Interesse des Betroffenen an einer Mitteilung über die erfolgte Beschränkungsmaßnahme einerseits und das Interesse des Betroffenen an Schutz vor Gefahren für Leib, Leben oder Freiheit

abzuwägen sind.

Zu Nummer 9 (§ 14)

Die Fristbemessung wird – orientiert an justiziellen Regelungen, etwa in § 100e Absatz 1 Satz 2 StPO – auf Werktage bezogen.

Zu Nummer 10 (§ 15)

Die Änderung von Absatz 1 Satz 4 dient dazu, eine kontinuierliche Handlungsfähigkeit der G 10-Kommission zu gewährleisten, indem die Amtsdauer der Kommissionsmitglieder mit der Bestimmung der nachfolgenden Mitglieder verknüpft wird.

Die Änderung in Absatz 6 entspricht der Änderung in § 14.

Zu Artikel 6 (VereinsG)

Dem Ansatz der Rechtsvereinheitlichung folgend, schafft die Ergänzung des § 4 einen gemeinsamen Befugnismindeststandard speziell zu vereinsrechtlichen Ermittlungen auch der Landesverfassungsschutzbehörden.

Zu Artikel 7 (BKAG)

Die Änderung dient der Wertungskonsistenz zu anderen nachrichtendienstlichen Maßnahmen der Aufenthaltsfeststellung, über die eine Zielperson nicht benachrichtigt wird. Nachrichtendienste sammeln Daten grundsätzlich geheim. Sie sind materiespezifisch von Transparenz- und Berichtspflichten gegenüber den Betroffenen weithin freigestellt (BVerfGE 133, 277 – Rn. 117). Sie betreiben Strukturaufklärung, nicht isoliert individualbezogene Sachverhalte. Individuelle Benachrichtigungen begründen damit regelmäßig Risiken für die strukturellen Aufklärungsansätze. Demzufolge sind Mitteilungspflichten auf spezielle Eingriffe in besondere grundrechtliche Privatheitsbereiche (Artikel 10, 13 GG, Vertraulichkeit informationstechnischer Systeme) beschränkt.

Zu Artikel 8 (VwGO)

Mit Nummer 1 wird die erstinstanzliche Zuständigkeit des Oberverwaltungsgerichts in Verfassungsschutz-Sachen begründet. Dies folgt der Zuständigkeitsentscheidung in § 99 Absatz 2 Satz 1

und bündelt damit auch gerichtliche Fachkompetenz, da im nachrichtendienstlichen Geschäftsbereich der Verfassungsschutzbehörden nach § 3 Absatz 1 BVerfSchG sowie des MAD nach § 1 Absatz 1 MADG naturgemäß Geheimschutzbelange regelmäßig berührt werden und dies nicht erst im Zwischenverfahren zu berücksichtigen ist. Eine spezielle gerichtliche Eingangszuständigkeit besteht mit § 50 Absatz 1 Nr. 4 bereits zum BND. Beim stärker im Inland tätigen BfV ist allerdings von einem Verfahrensaufkommen auszugehen, das eine erstinstanzliche Befassung des Bundesverwaltungsgerichts nicht gleichermaßen adäquat erscheinen lässt, so dass im Ergebnis die OVG-Ebene insgesamt sachgerecht ist.

Nummer 2 ist eine Folgeänderung zu der mit Artikel 1 Nummer 4 aufgenommenen Zuständigkeitsregelung in § 9e Absatz 3 Satz 2 BVerfSchG.

Zu Artikel 9 (Änderung der AO)

Nummer 1 führt zu einer klareren Fassung. Mit Buchstabe a) wird transparenter, dass es sich um ein automatisiertes Abrufverfahren handelt, das im Übrigen nicht nur die Daten nach § 93b Absatz 1 AO, sondern ebenso nach dessen Absatz 1a zum Gegenstand hat. Buchstabe b) führt zu einer klareren Fassung, indem nunmehr BfV, MAD und BND bereits in der AO als abrufberechtigte Stellen aufgeführt werden (nicht erst gemäß § 93 Absatz 8 Satz 3 in Verbindung mit den Fachgesetzen). Zudem entfällt der Bezug auf Landesrecht, weil im Interesse der Rechtsharmonisierung die Abrufberechtigung auch der Landesverfassungsschutzbehörden im neuen § 8a Absatz 1 Satz 6 BVerfSchG mit geregelt ist.

Nummer 2 greift die Regelung des bisherigen § 8a Absatz 2a Satz 2 BVerfSchG auf. Da zwischenzeitlich das Abrufverfahren auch für die polizeiliche Gefahrenabwehr eröffnet (in § 93 Absatz 8 Satz 1 Nummer 2 AO) und das Verfahren nach Absatz 9 auch insoweit aufgabeninadäquat ist, erfolgt eine Regelung nunmehr unmittelbar in der Abgabenordnung, was zugleich zu einer systematisch übersichtlicheren Gesamtregelung führt.

Zu Artikel 10 (Änderung TKG)

Die Regelung ergänzt die Verfassungsschutzbehörden sowie MAD und BND als erhebungsbefugte Stellen, so dass sich nicht mehr die

zuvor im Hinblick auf Artikel 15 Absatz 3 BayVSG umstrittene Frage stellt, ob Verfassungsschutzbehörden bereits als Gefahrenabwehrbehörden im Sinne der Norm zu verstehen waren. Gleichzeitig wird die Norm an die Rechtsprechung des Bundesverfassungsgerichts angepasst, indem als Schutzgut auch die Sicherheit des Bundes oder eines Landes sowie die gemeine Gefahr aufgenommen wird (BVerfGE 125, 260 – Ls. 5). Für die Verfassungsschutzbehörden ist dabei eine spezielle Erhebungsbefugnis im neuen § 9c Absatz 2 Satz 2 BVerfSchG vorgesehen, der der aktuellen Verfassungsrechtsprechung folgend (BVerfGE 141, 220 – Rn. 107) die Eingriffsvoraussetzungen mit der Inhaltsüberwachung synchronisiert.

Zu Artikel 11 (Änderung des StVG)

Mit den Änderungen werden die Abrufrechte der Verfassungsschutzbehörden (wie auch des MAD und BND) über das Fahrzeugregister hinaus auch auf das Fahreignungs- und Fahrerlaubnisregister erstreckt. In Zeiten, in denen Kraftfahrzeuge als Mittel für Terroranschläge missbraucht werden, ist es für eine zielführende Aufklärung unerlässlich zu erfahren, über welche Fahrberechtigungen Gefährder verfügen, bzw. ob eine Entziehung droht. Auch jenseits der Terrorismusaufklärung müssen die Nachrichtendienste die Mobilität ihrer Zielpersonen einschätzen können, so z.B. bei der Frage, inwieweit die Person in der Lage ist, im Rahmen von Bestrebungen und Aktionen fremde Kraftfahrzeuge, wie z.B. Mietwagen, nutzen zu können.

Zu Artikel 12 (Inkrafttreten/Außerkrafttreten)

Die Vorschrift regelt in Absatz 1 das Inkrafttreten der Änderungen. Mit der Aufhebung des Artikels 10 des Terrorismusbekämpfungsergänzungsgesetzes, der speziellen Inkrafttretensvorschrift dazu in Artikel 13 Absatz 2 sowie der komplementären Befristungsregelung in der Sicherheitsüberprüfungsfeststellungsverordnung wird der Regelungsstand auch in Ansehung der zuvor – seit 2001 – befristeten Bestimmungen, die zwischenzeitlich vier Mal evaluiert worden sind, konsolidiert.

Über den Autor/ die Autorin

andre

Andre ist seit 2008 bei netzpolitik.org, seit 2012 festangestellt. Er beschäftigt sich vor allem mit investigativer Recherche. Andre hat Sozialwissenschaften an der Humboldt-Universität zu Berlin studiert und Abschlüsse in Bachelor und Master zu netzpolitischen Themen gemacht. Er ist Gründungsmitglied der Vereine Digitale Gesellschaft, Gesellschaft für Freiheitsrechte und netzpolitik.org, Mitglied im Chaos Computer Club sowie Beobachter bei European Digital Rights. Außerdem arbeitet Andre als System-Administrator, er hat z.B. den ersten Mail-Server von Frag Den Staat aufgesetzt und nutzt ihn gerne. Und irgendwas mit Landesverrat. **Kontakt:** E-Mail, OpenPGP, Telefon, CryptoPhone, Twitter, Flattr, Bitcoin.

anna

Auf einem Zettel steht, dass sie eigentlich Informatikerin ist. Anna ist seit 2013 bei netzpolitik.org dabei. Sie interessiert sich vor allem für staatliche Überwachung und Dinge rund ums BAMF. Du erreichst sie unter anna@netzpolitik.org - am besten verschlüsselt [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]

Veröffentlicht
28.03.2019 um 08:09

Kategorie
Überwachung

Schlagworte
BfV, BMI, BND, Burkhard Lischka, Gesetzentwurf, Horst Seehofer, Innenministerium, Katarina Barley, Onlinedurchsuchung, quellen-telekommunikationsüberwachung, SPD, Staatstrojaner, Verfassungsschutz, ZITiS

2 Ergänzungen

Jane Bond sagt:
28. März 2019 um 08:31 Uhr

Verfassungsschutz bitte immer in Anführungszeichen setzen. Zur Erinnerung: es handelt sich um die spärlich kontrollierte Institution, die im Bund von einem rechten Verschwörungstheoretiker geleitet wurde, die Neonazis als V-Leute beschäftigt(e) und einen Mitarbeiter anstellte, der in einem rechtsextremen Netzwerk mit Mitgliedern aus Sicherheitsbehörden aktiv war.

https://www.heise.de/tp/features/Der-NSU-und-die-V-Leute-des-Verfassungsschutzes-3614870.html?seite=all

https://machtelite.wordpress.com/2018/10/03/social-media-ueberwachung-bfv-praesident-maassen-instrumentalisierte-vor-dem-innenausschuss-den-mutmasslich-linksextremistischen-twitter-account-hamburger-linie/

http://www.taz.de/!5577527/

Titus von Unhold sagt:
29. Mai 2019 um 19:30 Uhr

V-Leute werden nicht beschäftigt und sind auch sonst rechtlich nicht mit dem sogenannten Verfassungsschutz verbunden.