



---

**Ausarbeitung**

---

**Zu einer künftigen Regelung des heimlichen Betretens von Wohnungen zur Vorbereitung technischer Überwachung**

**Zu einer künftigen Regelung des heimlichen Betretens von Wohnungen zur Vorbereitung technischer Überwachung**

Aktenzeichen: WD 3 - 3000 - 214/19  
Abschluss der Arbeit: 25. September 2019  
Fachbereich: WD 3: Verwaltung und Verfassung

---

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

---

<b>1.</b>	<b>Fragestellung</b>	<b>4</b>
<b>2.</b>	<b>Art. 13 GG (Unverletzlichkeit der Wohnung)</b>	<b>4</b>
2.1.	Schutzbereich	4
2.2.	Eingriff	5
2.3.	Rechtfertigung	6
2.3.1.	Ermächtigungsgrundlage	6
2.3.2.	Richtervorbehalt	6
2.3.2.1.	Vorbereitung zur Gefahrenabwehr	6
2.3.2.2.	Vorbereitung der Sicherung von Einsatzpersonal	7
2.3.2.3.	Vorbereitung von G-10-Maßnahmen	8
2.3.2.4.	Übergreifende Aspekte	8
2.3.3.	Verhältnismäßigkeit	9
2.3.3.1.	Legitimes Ziel	9
2.3.3.2.	Geeignetheit	10
2.3.3.3.	Erforderlich	10
2.3.3.4.	Angemessenheit	11
<b>3.</b>	<b>Trennungsprinzip</b>	<b>11</b>
<b>4.</b>	<b>Rechtsstaatsprinzip (Normenklarheit)</b>	<b>13</b>
<b>5.</b>	<b>Anhang: Auszüge Entwurf BVerfSchG</b>	<b>15</b>
	§ 9d BVerfSchG – Eingriff in informationstechnische Systeme	15
	§ 9e BVerfSchG – Technische Datenerhebung aus Wohnungen	17
	§ 11 G-10-Gesetz – neue Absätze 1a und 1b	18

## 1. Fragestellung

Ein im Netz veröffentlichter umfangreicher<sup>1</sup> „Entwurf eines Gesetzes zur Harmonisierung des Verfassungsschutzrechts“<sup>2</sup> (im Folgenden: „Entwurf BVerfSchG“) sieht folgende neue Bestimmung für das Bundesverfassungsschutzgesetz (BVerfSchG) vor (vollständiger Wortlaut im Anhang, Hervorhebung durch Autor):

„§ 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 [...].

(3) [...] Die Maßnahme darf erst vollzogen werden, wenn das **Bundesverwaltungsgericht** die Zulässigkeit festgestellt hat. Satz 2 gilt nicht bei Gefahr im Verzug. [...]

(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.

(6) Das Bundesamt für Verfassungsschutz darf **Wohnungen** auch **betreten**, um **Maßnahmen** nach den Absätzen 1 [„technische Überwachung zur Gefahrenabwehr“] und 5 [„technische Überwachung zur Eigensicherung“], nach § 11 Absatz 1a des Artikel 10-Gesetzes [„Quellentelekommunikationsüberwachung“] oder § 9d [„Eingriff in IT-Systeme“] **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.“

Es stellt sich die Frage, wie die Befugnis des § 9e Abs. 6 Entwurf BVerfSchG zum Betreten der Wohnung verfassungsrechtlich zu beurteilen ist, auch im Hinblick auf das informationelle Trennungsprinzip.

## 2. Art. 13 GG (Unverletzlichkeit der Wohnung)

### 2.1. Schutzbereich

Der Schutzbereich des Art. 13 Abs. 1 Grundgesetz (GG) ist eröffnet, da die Ermächtigungsgrundlage bereits dem Wortlaut nach an das Betreten einer „Wohnung“ anknüpft.

---

1 Rund 33.000 Wörter, entsprechend rund hundert Druckseiten im HTML-Format.

2 <https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/#Referentenentwurf-Bundesverfassungsschutzgesetz>.

## 2.2. Eingriff

Das Betreten der Wohnung stellt einen Eingriff in den Schutzbereich des Art. 13 GG dar.<sup>3</sup> Art. 13 GG unterscheidet die folgenden Eingriffe:<sup>4</sup>

- Abs. 2 (Durchsuchung),
- Abs. 4 bzw. 5 (Einsatz technischer Mittel),
- Abs. 7 (sonstiger Eingriff).

Das heimliche Betreten nach § 9e Abs. 6 Entwurf BVerfSchG lässt sich nicht als Eingriff nach Art. 13 Abs. 2 GG „**Durchsuchung**“ werten. Durchsuchungen gehen grundsätzlich mit der Kenntnis des Betroffenen einher.<sup>5</sup> Ferner ist eine Durchsuchung nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) „das ziel- und zweckgerichtete Suchen staatlicher Organe nach Personen oder Sachen[, die] der Inhaber der Wohnung von sich aus nicht offenlegen oder herausgeben will [...]“.<sup>6</sup> Die Zielrichtung des § 9e Abs. 6 Entwurf BVerfSchG ist aber eine andere.

Art. 13 Abs. 4 und 5 GG ermöglichen ihrem Wortlaut nach nur den **Einsatz** „technischer Mittel zur Überwachung von Wohnungen“ z. B. durch Kameras oder Mikrofone,<sup>7</sup> nicht aber das Betreten der Wohnung.<sup>8</sup> Gleichwohl zieht die überwiegende Kommentierung sie als Grundlage für das heimliche Betreten einer Wohnung heran.<sup>9</sup>

Hierfür lässt sich insbesondere der **sachliche Zusammenhang** zwischen dem Einsatz technischer Mittel und dem Betreten der betreffenden Wohnung anführen. Im Strafprozess- und Polizeirecht besteht auf einfachgesetzlicher Ebene eine ähnliche Auslegungsproblematik u. a. bezüglich § 100c Strafprozessordnung. Kommentierung und Rechtsprechung gehen überwiegend davon aus, dass

---

3 Kluckert/Fink, in: BeckOK GG, 41. Edition Stand: 15.5.2019, Art. 13 Rn. 6; Roggan, DÖV 2019, 425 (428).

4 Hermes, in: Dreier, GG, 3. Auflage 2013, Art. 13 Rn. 29: „Art. 13 GG enthält in seinen Absätzen 2 bis 7 eine differenzierte Schrankensystematik, die an verschiedene Eingriffe unterschiedliche Rechtfertigungsanforderungen stellt. [...] Sie steuern das Auffinden der richtigen Schranke.“

5 Derin/Golla, NJW 2019, 1111 (1113): „Für offene Maßnahmen wie die Durchsuchung ist charakteristisch, dass der Betroffene von ihrem Grund und ihrer Durchführung Kenntnis erlangt. Eine gezielte Verknüpfung mit heimlichen Grundrechtseingriffen liefe dieser Maßgabe zuwider.“

6 BVerfGE 76, 83 (89).

7 Kluckert/Fink, in: BeckOK GG, 41. Edition Stand: 15.5.2019, Art. 13 Rn. 8.

8 Vgl. Roggan, DÖV 2019, 425 (428), der betont, dass Art. 13 Abs. 4 GG lediglich den Einsatz der Mittel erfasst.

9 Hermes, in: Dreier, GG, 3. Auflage 2013, Art. 13 Rn. 63; Gornig, in: von Mangoldt/Klein/Starck, GG, 7. Auflage 2018, Art. 13 Rn. 96 m.w.N.

insoweit eine „Annexkompetenz“<sup>10</sup> besteht (Betreten als Annex zum technischen Überwachen).<sup>11</sup> Eine direkte Aussage des BVerfG zu dieser nicht unumstrittenen<sup>12</sup> Frage steht jedoch noch aus.

Kaum naheliegend erscheint es, den **Auffangtatbestand**<sup>13</sup> des Art. 13 Abs. 7 GG anzuwenden. Dieser erfasst „Eingriffe und Beschränkungen [...] im übrigen [...] zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen“. Eingriffe nach Abs. 7 stehen nicht unter Richtervorbehalt. Es wäre widersprüchlich, das heimliche Betreten nach § 9e Abs. 6 des Entwurfs BVerfSchG auf Abs. 7 zu stützen: Die Eingriffsintensität des heimlichen (physischen) Betretens einer Wohnung entspricht mindestens dem heimlichen technischen Überwachen.

### 2.3. Rechtfertigung

#### 2.3.1. Ermächtigungsgrundlage

Mit § 9e Abs. 6 des Gesetzentwurfs bestünde eine **ausdrückliche** gesetzliche **Ermächtigungsgrundlage**. Dies würde Bedenken kritischer Stimmen Rechnung tragen, die sich dagegen wenden, das heimliche Betreten der Wohnung als Annexkompetenz zu der gesetzlich vorgesehenen technischen Überwachung anzusehen.<sup>14</sup>

#### 2.3.2. Richtervorbehalt

##### 2.3.2.1. Vorbereitung zur Gefahrenabwehr

Art. 13 Abs. 4 GG stellt den Einsatz technischer Mittel zur Gefahrenabwehr unter Richtervorbehalt. § 9e Abs. 3 Entwurf BVerfSchG sieht vor, dass die Maßnahme „erst vollzogen werden [darf], wenn

---

10 Siehe z.B. Lottkus, in: BeckOK PolR NRW, 12. Edition Stand: 10.7.2019, § 20c Rn. 41.

11 WD 3 - 3000 - 213/19, Heimliches Betreten von Wohnungen zum Zwecke der technischen Überwachung: Rechtsgrundlagen für Sicherheitsbehörden des Bundes und der Länder, S. 5 ff.

12 So insbesondere Roggan, DÖV 2019, 425 (428): „Die physische Anwesenheit von Geheimdienstmitarbeitern ist [...] als verfassungsrechtlich nicht zu rechtfertigender Eingriff in das Wohnungsgrundrecht anzusehen.“

13 Kluckert/Fink, in: BeckOK GG, 41. Edition Stand: 15.5.2019, Art. 13 Rn. 24.

14 Roggan, DÖV 2019, 425 (428): „[D]ie auf bundesrechtlicher Grundlage agierenden Geheimdienste [sind] entgegen der genannten Auffassung, die von einer Annexkompetenz zum heimlichen Betreten von Wohnungen ausgeht, de lege lata nicht befugt, Datenerhebungen in Wohnungen vorzunehmen“; Schwabenbauer, Heimliche Grundrechtseingriffe, S. 190: Aus der Befugnisnorm für die „eigentliche Ausforschungsmaßnahme lässt sich eine Erlaubnis zur heimlichen Vorbereitung nur dann ableiten, wenn sie kraft Evidenz *conditio sine qua non* [=notwendige Voraussetzung] für die Anwendung der Befugnis ist. Grundsätzlich bedarf es daher für entsprechende Vorbereitungsmaßnahmen gesonderter Regelungen.“

das Bundesverwaltungsgericht die Zulässigkeit festgestellt hat.“ In **verfassungskonformer Auslegung** dürfte dies auch das heimliche Betreten der Wohnung gem. § 9e Abs. 6 Entwurf BVerfSchG erfassen.<sup>15</sup>

Hierfür spricht auch, dass nach § 9e Abs. 6 S. 2 Entwurf BVerfSchG das Betreten der Wohnung „in der Anordnung oder einer Ergänzungsanordnung erlaubt sein“ muss. Beide Anordnungen dürften jedenfalls bei verfassungskonformer Auslegung Gegenstand der vorherigen **richterlichen Prüfung** sein.

#### 2.3.2.2. Vorbereitung der Sicherung von Einsatzpersonal

Dient der Einsatz technischer Mittel ausschließlich dem Schutz von Einsatzpersonal, ist ein Richtervorbehalt verfassungsrechtlich nicht vorgesehen (vgl. Art. 13 Abs. 5 GG). Dies betrifft zum Beispiel folgenden Fall: Ein verdeckter Ermittler ist in die Wohnung des Verdächtigen eingeladen. Es besteht die **Gefahr**, dass die wahre Identität des verdeckten Ermittlers bekannt wird und die Situation **gewalttätig eskaliert**. Insoweit kann der verdeckte Ermittler zum Beispiel technische Mittel am Körper führen, oder Mitarbeiter überwachen die Wohnung von außen mit Kameras und Lasermikrofonen. Hierzu heißt es im Gesetzentwurf zur Änderung des Art. 13 GG:

„[Den Einsatz technischer Mittel kann nach Art. 13 Abs. 5 GG] anstelle des Richters auch eine andere gesetzlich bestimmte Stelle anordnen, denn Ziel der Maßnahme ist in diesem Fall ausschließlich die Eigensicherung der verdeckt ermittelnden Personen.“<sup>16</sup>

Für den Wegfall des Richtervorbehalts in Art. 13 Abs. 5 GG lassen sich insbesondere folgende Gründe anführen: Die Überwachung fokussiert sich auf den **verdeckten Ermittler** und dient nicht der Gewinnung von Information über die verdächtige Person. Ferner befindet sich ein verdeckter Ermittler in dieser Situation auf **Einladung** des Wohnungsinhabers in dessen Wohnung (auch wenn der Wohnungsinhaber über die wahre Identität des Ermittlers irrt). Der zusätzliche Eingriff durch Mikrofone oder Kameras während des Einsatzes des Ermittlers erscheint vergleichsweise eher gering.

Demgegenüber stellt sich das heimliche Betreten der Wohnung ohne Zustimmung des Wohnungsinhabers wohl als gewichtiger zusätzlicher **physischer Eingriff** in Art. 13 GG dar. Es bestehen Zweifel, ob der Verfassungsgesetzgeber mit der Ausnahme des Art. 13 Abs. 5 GG auch Fälle des heimlichen Betretens der Wohnung erfassen wollte. Nach der durchgehenden Logik des Art. 13 GG steht jedes Betreten (und Ausforschen) einer Wohnung, das **heimlich** oder **gegen den Willen** des Wohnungsinhabers erfolgt, unter Richtervorbehalt. Zwar dient das Betreten bei Art. 13 Abs. 5 GG letztlich nur der „Absicherung“ des verdeckten Ermittlers und nicht der Ausforschung der Wohnung. Aus Sicht des Grundrechtsträgers hingegen ist das heimliche Betreten der Wohnung ein

---

15 Siehe auch Hermes, in: Dreier, GG, 3. Auflage 2013, Art. 13 Rn. 32: „In Fällen, in denen das Gesetz unter Verstoß gegen Art. 13 II GG weder einen Richtervorbehalt noch ein für die richterliche Entscheidung vorgesehenes Verfahren normiert, haben die Gerichte aufgefordert durch das Bundesverfassungsgericht die Lücke durch eine problematische verfassungskonforme Auslegung mittels einer ‚unmittelbaren‘ Anwendung des Richtervorbehalts in Art. 13 II GG und einer analogen Anwendung passender Verfahrensvorschriften geschlossen“ (Fußnoten ausgelassen).

16 Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG), BT-Drs. 13/8650, S. 5.

zusätzlicher physischer Eingriff. Dies spricht dafür, den **Richtervorbehalt** nach Art. 13 Abs. 4 GG direkt oder analog auf das heimliche Betreten einer Wohnung anzuwenden,<sup>17</sup> auch wenn dieses „nur“ der Eigensicherung im Sinne des Art. 13 Abs. 5 GG dient. Eine Klarstellung in § 9e Abs. 6 Entwurf BVerfSchG würde diesbezügliche verfassungsrechtliche Zweifel ausräumen.

#### 2.3.2.3. Vorbereitung von G-10-Maßnahmen

Das Recht zum heimlichen Betreten der Wohnung erfasst auch die Quellen-Telekommunikationsüberwachung (§ 11 Abs. 1a des Artikel 10-Gesetzes, § 9e Abs. 6 Entwurf BVerfSchG). **Telekommunikationsüberwachung** fällt unter den Schutzbereich des Art. 10 GG. Nach Art. 10 Abs. 2 S. 2 GG kann „die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane“ erfolgen. Dies bezieht sich jedoch nur auf die Überwachung selbst. Das heimliche Betreten der **Wohnung** selbst fällt unter den Schutzbereich des Art. 13 GG. Insoweit dürften Art. 13 Abs. 4 GG und der entsprechende Richtervorbehalt Anwendung finden.<sup>18</sup> § 9e Abs. 6 Entwurf BVerfSchG ist daher so auszulegen, dass der **Richtervorbehalt** nach § 9e Abs. 3 S. 2 Entwurf BVerfSchG auch für Maßnahmen nach § 11 Abs. 1a des Artikel 10-Gesetzes gilt. Vorzuziehen wäre wohl eine **ausdrückliche Formulierung** (siehe zur Normenklarheit unten Abschnitt 4).

#### 2.3.2.4. Übergreifende Aspekte

Das Grundrecht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG) begründet **kein Recht auf mehrere Instanzen**.<sup>19</sup> Insoweit bestehen keine Bedenken gegen die alleinige Zuständigkeit des Bundesverwaltungsgerichts. Entsprechendes gilt für die Entscheidung durch den **Einzelrichter** (§ 9e Abs. 4 S. 5 Entwurf BVerfSchG).<sup>20</sup>

Die Ausnahme vom Richtervorbehalt bei **Gefahr im Verzug** ist in Art. 13 Abs. 4 S. 2 GG bereits angelegt: In diesem Fall ist „eine richterliche Entscheidung [...] unverzüglich nachzuholen“. § 9e Abs. 3 S. 3 Entwurf BVerfSchG sieht hierzu folgende Bestimmung vor:

„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

---

17 Siehe auch Hermes, in: Dreier, GG, 3. Auflage 2013, Art. 13 Rn. 32 (Zitat oben Fn. 15).

18 Vgl. auch BVerfGE 120, 274 (331 ff.): „Sieht eine Norm heimliche Ermittlungstätigkeiten des Staates vor, die – wie hier – besonders geschützte Zonen der Privatheit berühren oder eine besonders hohe Eingriffsintensität aufweisen, ist dem Gewicht des Grundrechtseingriffs durch geeignete Verfahrensvorkehrungen Rechnung zu tragen [...]. Bei einem Grundrechtseingriff von besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist.“

19 BVerfGE 42, 243 (248); 107, 395 (401 ff.); 108, 341 (345 ff.).

20 BVerfG, Beschluss vom 22.9.1983 - 2 BvR 1475/83: „Aus Art. 19 IV 1 GG läßt sich kein Gebot herleiten, daß der dort gewährleistete Rechtsschutz grundsätzlich von gerichtlichen Spruchkörpern gewährt werden müsse, die von mehreren Richtern gebildet werden“; Umkehrschluss aus Art. 13 Abs. 3 S. 3 GG: Ein mit mehreren Richtern besetzter Spruchkörper ist nur in Art. 13 Abs. 3 S. 3 GG betreffend Strafverfolgung vorgesehen, nicht aber in den anderen Absätzen betreffend Gefahrenabwehr.



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.“

Die Frist von **drei Tagen** findet sich z. B. auch in § 100e Strafprozessordnung: „Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft.“ Verfassungsrechtliche Bedenken hiergegen finden sich in der Kommentierung soweit ersichtlich nicht.<sup>21</sup>

### 2.3.3. Verhältnismäßigkeit

Weiterhin muss das Gesetz dem Grundsatz der Verhältnismäßigkeit gerecht werden. Dies setzt voraus, dass ein legitimes Ziel in geeigneter, erforderlicher und angemessener Weise verfolgt wird.<sup>22</sup> Dabei gelten die besonderen Anforderungen der Abs. 4 und 5 des Art. 13 GG, die nach überwiegender Auffassung anwendbar sind (siehe oben 2.2).

#### 2.3.3.1. Legitimes Ziel

Art. 13 Abs. 4 GG beschränkt den Einsatz technischer Mittel zur Gefahrenabwehr auf Fälle der „Abwehr **dringender Gefahren** für die **öffentliche Sicherheit**, insbesondere einer gemeinen Gefahr oder einer **Lebensgefahr**“ (Hervorhebung durch Autor).

Die tatbestandlichen Voraussetzungen der §§ 9e, 9d Entwurf BVerfSchG greifen diese Formulierungen auf (Hervorhebung durch Autor):

§ 9e Abs. 1: „Das Bundesamt für Verfassungsschutz darf ohne Wissen des Betroffenen unter Einsatz technischer Mittel personenbezogene Daten aus einer Wohnung entsprechend § 9d Abs. 1 und 2 erheben [...]“

§ 9d Abs. 1: „Das Bundesamt für Verfassungsschutz darf bei besonders schweren Bedrohungen [...] 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** [...] oder
3. Leib, **Leben** oder Freiheit einer Person.“

„Leib“ und „Freiheit“ einer Person sind der Kommentierung zufolge grundsätzlich taugliche Schutzgüter des Art. 13 Abs. 4 GG.<sup>23</sup>

---

21 Graf, in: BeckOK StPO, 34. Edition Stand: 1.7.2019, § 100e StPO Rn. 15.

22 Grzeszick, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 107.

23 Kluckert/Fink, in: BeckOK GG, 41. Edition Stand: 15.5.2019, Art. 13 Rn. 6: „Schützenswert sind vergleichbar Art. 13 Abs. 3 die Schutzgüter des Art. 2 Abs. 2, also Leben, körperliche Unversehrtheit und Freiheit der Person, wobei die Gefahr einfacher Körperverletzungen nicht ausreicht.“

---

Art. 13 Abs. 5 GG ermöglicht den Einsatz technischer Mittel darüber hinaus zum **Schutz von Einsatzpersonal**. Auch dies greift § 9e des Entwurfs in Abs. 5 auf.

„Im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz von Personen in einer Wohnung [...] darf [das Bundesamt für Verfassungsschutz] in oder aus der Wohnung Daten mit technischen Mitteln erheben, wenn dies zur Abwehr von Gefahren für deren **Leib, Leben oder Freiheit unerlässlich** ist.“

Entsprechendes gilt für Maßnahmen nach § 11 Abs. 1a des Artikel 10-Gesetzes.

#### 2.3.3.2. Geeignetheit

Das heimliche Betreten der Wohnung zum Anbringen technischer Überwachungsmittel kann geeignet sein, die vorgenannten Gefahren abzuwehren.

#### 2.3.3.3. Erforderlich

Das heimliche Betreten muss das mildeste unter gleich effektiven Mitteln sein:

„Maßnahmen [greifen] weniger stark in das Wohnungsgrundrecht ein [...], sofern die Datenerhebungen ausschließlich von außen stattfinden können und vorherige Wohnungsbetretungen sich damit erübrigen. [...] **Betretungsrechte** [sind deshalb] **nur subsidiär** [zu gewähren.]“<sup>24</sup>

In **verfassungskonformer Anwendung** dürfte das Bundesamt für Verfassungsschutz die Wohnung daher nur heimlich betreten, wenn die technische Überwachung nicht anderweitig gleich effektiv möglich wäre.

Auch bei der **Auswahl** der **Adressaten** gilt das Gebot der Erforderlichkeit: „Der Verhältnismäßigkeitsgrundsatz setzt insb. der Überwachung unbeteiligter Dritter enge Grenzen.“<sup>25</sup> Insoweit begrenzt § 9e Abs. 6 S. 3 Entwurf BVerfSchG das Recht zum heimlichen Betreten auf die Wohnung desjenigen, gegen den sich die Überwachungsanordnung richtet.

Nach § 9d Abs. 3 Nr. 2 Entwurf BVerfSchG dürfen sich Überwachungsmaßnahmen auch gegen **Dritte** richten, in deren „informationstechnischem System [verdächtige Personen<sup>26</sup>] Informationen verarbeiten“ und die Erforschung des Sachverhalts **nicht ebenso** durch eine Maßnahme“ gegen den Verdächtigen möglich ist. Damit sieht der Entwurf BVerfSchG das Prinzip der Erforderlichkeit insoweit ausdrücklich vor.

---

24 Roggan, DÖV 2019, 425 (432) – Hervorhebung nur hier, nicht im Original.

25 Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 92.

26 Personen, „die Straftat planen oder begangen haben oder an den bezeichneten Bedrohungen beteiligt sind“.

#### 2.3.3.4. Angemessenheit

Bei der Angemessenheit ist das wichtige Rechtsgut der Unverletzlichkeit der Wohnung mit den Rechtsgütern abzuwägen, denen der Eingriff dient. Entscheidend ist dabei, dass § 9e Entwurf BVerfSchG dem Schutz **höchster Rechtsgüter** dient, die das Grundgesetz als Rechtfertigungsgründe für Eingriffe bestimmt (Art. 13 Abs. 4 GG, siehe schon oben unter 2.3.3.1).

Bei der **Anwendung** der Norm können sich Fragen der Angemessenheit stellen. Zu solchen Angemessenheitsaspekten gehört nach der Rechtsprechung des BVerfG insbesondere ein unantastbarer „Kernbereich persönlicher Lebensgestaltung“:

„Der **Schutz** des Kernbereichs privater Lebensgestaltung ist **strikt** und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden.“<sup>27</sup>

Das heimliche Betreten der Wohnung könnte im Ausnahmefall dazu führen, dass die heimlich handelnden Mitarbeiter mit Sachverhalten aus dem Kernbereich privater Lebensgestaltung konfrontiert sind. In diesem Fall müssten die heimlich handelnden Mitarbeiter ihre **Maßnahmen** in der Wohnung entsprechend zurückhaltend **anpassen**.

Davon abgesehen ist es nur angemessen, eine Wohnung zu betreten, wenn die vorzubereitende **Überwachung** selbst **verhältnismäßig**, und dabei insbesondere angemessen ist. Dies richtet sich nach einer Vielzahl weiterer Vorschriften und deren verhältnismäßiger Anwendung. Je eher z. B. Wohnungen von Dritten betroffen sind (also nicht verdächtigen Personen), desto höher sind die Anforderungen an die Angemessenheit der Maßnahme.<sup>28</sup>

### 3. Trennungsprinzip

Im Grundsatz sollen Polizei und Nachrichtendienste getrennt voneinander arbeiten (Trennungsprinzip):

„Besondere Anforderungen an die Behördenstruktur ergeben sich aus dem Trennungsprinzip. Dieses verlangt eine grundsätzliche Trennung zwischen polizeilichen und nachrichtendienstlichen Befugnissen. Anders ausgedrückt geht es um das Gebot einer **organisatorischen Trennung** von Polizei und Verfassungsschutz, oder das Verbot der Vereinigung von Polizei und Nachrichtendienst in einer Behörde. Nur der Polizei obliegt die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung. Diese ist von der Informationsbeschaffung und der

---

27 BVerfGE 141, 220 (278) (Hervorhebung durch Autor).

28 Siehe nur Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 92: „Der Verhältnismäßigkeitsgrundsatz setzt insb. der Überwachung unbeteiligter Dritter enge Grenzen.“

Beratung im Sinne der politischen Vorfeldaufklärung durch die Nachrichtendienste strikt zu trennen.“<sup>29</sup>

Vor diesem Hintergrund erscheint die neue Ermächtigungsgrundlage des § 9e Abs. 6 Entwurf BVerfSchG **unproblematisch**. Sie befugt ausschließlich das Bundesamt für Verfassungsschutz. Über das Verhältnis zu Strafverfolgungsbehörden trifft § 9e Entwurf BVerfSchG keine Aussage.

Das Trennungsprinzip wirkt sich darüber hinaus auch auf den **Informationsaustausch** zwischen Nachrichtendiensten und Strafverfolgungsbehörden aus:

„Das Bundesverfassungsgericht hat [...] im Urteil zum Antiterrordateigesetz ein aus dem Grundrecht auf informationelle Selbstbestimmung folgendes informationelles Trennungsprinzip bejaht. Hiernach unterliegt der Austausch von Daten der Nachrichtendienste und der Polizeibehörden engen verfassungsrechtlichen Grenzen. Er sei nur ausnahmsweise zulässig, soweit er einem herausragenden öffentlichen Interesse diene und auf der Grundlage normenklarer **gesetzlicher Regelungen** erfolge, die ihrerseits hinreichend konkrete und qualifizierte Eingriffsschwellen vorsehen müssten.“<sup>30</sup>

Die Schutzwirkung des **Art. 13 GG** soll sich „auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme dieser Ereignisse anschließt, und den Gebrauch, der von den erlangten Kenntnissen gemacht wird“, erstrecken. Dabei „ist die Verwendung erlangter Daten [grundsätzlich] an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat (Grundsatz der **Zweckbindung**)“.<sup>31</sup> In der Praxis allerdings werden die Daten „oft von vornherein sowohl zu präventiven als auch zu repressiven Zwecken erhoben“, sodass „es keiner gesetzlichen Grundlage für die (Weiter-)Verwendung zu einem der Zwecke bedarf“.<sup>32</sup> In dieser Hinsicht, aber auch in Bezug auf andere praktische Aspekte (wie z. B. den Austausch von Daten in Kooperationsplattformen)<sup>33</sup> ergeben sich Fragen in Bezug auf das informationelle Trennungsprinzip vielfach nur aus den Umständen des **Einzelfalls**.

Im Übrigen schafft § 9e Abs. 6 Entwurf BVerfSchG keine neue Befugnis, sondern stellt diese lediglich auf eine **ausdrückliche Gesetzesgrundlage** (folgt man der überwiegenden Kommentarmedeutung zur bisherigen Praxis). Insoweit ergibt sich durch § 9e Abs. 6 Entwurf BVerfSchG keine neue Befugnis zur Datenerhebung, die zu einer neuen Ausnahme vom informationellen Trennungsprinzip führen würde. Die ausdrückliche Regelung sorgt vielmehr dafür, dass für den gesamten Eingriff,

---

29 WD 3 - 3000 - 406/18, Gemeinsames Terrorismusabwehrzentrum (GTAZ), S. 15, <https://www.bundestag.de/resource/blob/594538/8aff4300410fcac3f2e414d67922d5a9/WD-3-406-18-pdf-data.pdf> (Hervorhebung durch Autor).

30 WD 3 - 3000 - 406/18, Gemeinsames Terrorismusabwehrzentrum (GTAZ), S. 16, <https://www.bundestag.de/resource/blob/594538/8aff4300410fcac3f2e414d67922d5a9/WD-3-406-18-pdf-data.pdf> (Hervorhebung durch Autor).

31 Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 99 (Hervorhebung durch Autor).

32 Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 99.

33 Hierzu ausführlich WD 3 - 3000 - 406/18, Gemeinsames Terrorismusabwehrzentrum (GTAZ), <https://www.bundestag.de/resource/blob/594538/8aff4300410fcac3f2e414d67922d5a9/WD-3-406-18-pdf-data.pdf>.

und damit mittelbar auch für den nachfolgenden Datenaustausch eine ausdrückliche Gesetzesgrundlage besteht.<sup>34</sup>

#### 4. Rechtsstaatsprinzip (Normenklarheit)

Normenklarheit ist ein Grundsatz des Rechtsstaatsprinzips (Art. 20 Abs. 3 GG) und bedeutet: „Die Normadressaten müssen zumindest im Wesentlichen erkennen können, mit welchen Rechtswirkungen sie zu rechnen haben.“<sup>35</sup> In diesem Zusammenhang sind die langen Normen des Entwurfs BVerfSchG und die auch für Juristen mitunter nur schwer zugänglichen Verweisungsketten nicht unproblematisch. Ein Teil der Kommentierung führt hierzu in anderem Zusammenhang aus:

„Die Ausweitung der Möglichkeiten für staatliche Informationszugriffe auf Finanzdaten ist mit seinen zahlreichen Regelungsorten im Polizeirecht, Strafrechtsverfahrensrecht, im Recht der Nachrichtendienste, im Steuer- und Wirtschaftsverwaltungsrecht und aufgrund einer **kafkaesken Verweisungstechnik** nur noch schwer überschaubar. Ob sich in diesem Geflecht aus Zuständigkeiten und Befugnissen Wege der Erlangung von Informationen über die finanzielle Privatsphäre von Bürgerinnen und Bürgern noch rekonstruieren, geschweige dann effektiv kontrollieren lassen werden, erscheint fraglich.“<sup>36</sup>

Das BVerfG hat sich im Kontext der Brief- und Telefonüberwachung durch das Zollkriminalamt im Jahr 2004 ebenfalls kritisch geäußert:

„Dieser **Mangel an Normenklarheit** bewirkt bei **Überwachungsmaßnahmen** im Planungsstadium und dort insbesondere beim Handeln unter Zeitdruck ein **hohes Risiko**, dass sich die Handelnden keine Rechenschaft mehr darüber geben, ob sich die beobachteten Indizien auf konkrete Straftatbestände beziehen lassen. [...] Verweisungsketten können als solche in komplexen Regelungszusammenhängen gegenüber der als Alternative in Betracht kommenden Umschreibung aller Eingriffsvoraussetzungen in der Eingriffsnorm selbst durchaus vorzuzugswürdig sein. An Klarheit wird durch die Zusammenfassung in einer einzigen Norm nicht notwendig etwas gewonnen. Allerdings ist leichter zu erkennen, welche Tatbestandsmerkmale erheblich sind. Erreicht der Gesetzgeber die Festlegung des Normeninhalts aber – wie hier – nur mit Hilfe zum Teil langer, über **mehrere Ebenen gestaffelter**, unterschiedlich **variabler Verweisungsketten**, die bei gleichzeitiger **Verzweigung** in die Breite den Charakter von **Kaskaden** annehmen, leidet die praktische Erkennbarkeit der maßgebenden

---

34 Vgl. Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 13 Rn. 100: Zweckänderungen bei der Datenübermittlung „bedürfen jedoch ihrerseits einer gesetzlichen Grundlage“; die Diskussion um die Verfassungsmäßigkeit von Vorschriften wie § 20 BVerfSchG ist nicht Gegenstand dieser Ausarbeitung. Siehe zum Streitstand nur: Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 20 Rn. 12: „Auch wenn hinsichtlich der Datenübermittlungen zur Verfolgung von Staatsschutzdelikten eine rechtlich offene Überprüfung von § 20 auf seine Grundrechtskonformität gefordert worden ist, ergibt sich aus der Tatsache einer mehrfachen Novellierung des BVerfSchG seit 2015, dass der Gesetzgeber insofern keinen besonderen Regelungsbedarf sieht.“

35 Herdegen, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 87. EL März 2019, Art. 79 Rn. 154.

36 Herzog/Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, Einleitung Rn. 160 (Hervorhebung durch Autor); zustimmend Wonka, NJW 2017, 3334; in Bezug auf nachrichtendienstliche Gesetzgebung der Länder: Baldus, NVwZ 2003, 1289 (1290): „mühsam zu entwirrende Verweisungsketten“.

Rechtsgrundlage. Der Prüfungsvorgang wird dadurch fehleranfällig. Gerade in Eilfällen besteht eine gesteigerte Gefahr von Fehlentscheidungen der Verwaltung und der eingeschalteten Gerichte.“<sup>37</sup>

Eine entsprechende Aussage des BVerfG zu den vielfach komplexen Vorschriften der **geltenden Fassung des BVerfSchG** liegt soweit ersichtlich jedoch nicht vor.<sup>38</sup>

Im Hinblick auf den Entwurf BVerfSchG könnten sich Bedenken insbesondere in folgender Hinsicht ergeben: Die Vorbereitung von technischen Maßnahmen nach **§ 1a G-10-Gesetz** (künftige Fassung) soll sich hinsichtlich des heimlichen Betretens von Wohnungen nach § 9e Abs. 6 Entwurf BVerfSchG richten. Unklar ist, ob sich das Verfahren für diese Maßnahme, einschließlich Richtervorbehalt, nunmehr nach § 9e Abs. 3 Entwurf BVerfSchG richtet, oder nach G-10-Gesetz (ohne Richtervorbehalt). In ersterem Fall dürften sich unklare Überlagerungen mit den Verfahrensvorschriften des G-10-Gesetzes ergeben. In letzterem Fall wäre problematisch, dass ein Leser des G-10-Gesetzes keine Kenntnis darüber erlangte, dass ein Recht zum Betreten der Wohnung auch bei G-10-Maßnahmen besteht.<sup>39</sup> Ferner wäre unklar, ob der Richtervorbehalt des § 9e Abs. 3 S. 2 Entwurf BVerfSchG für die G-10-Maßnahme gilt, oder nicht.

\* \* \*

---

37 Beschluss vom 3.3.2004 - 1 BvF 3/92, Rn. 133 ff. – Hervorhebung durch Autor.

38 Beschwerde der fehlenden Normenklarheit des BVerfSchG nicht aufgegriffen in: BVerfG, Beschluss vom 17.9.2013 - 2 BvR 2436/10, Rn. 127: „Die notwendige Bestimmtheit fehlt aber nicht schon deshalb, weil eine Norm auslegungsbedürftig ist“; siehe auch BVerfG, Urteil vom 27.2.2008 - 1 BvR 370, 595/07, Rn. 208 ff. zur fehlenden Normenklarheit des Verfassungsschutzgesetzes Nordrhein-Westfalen aufgrund unbestimmter Begriffe.

39 Vgl. BVerfG, Beschluss vom 3.3.2004 - 1 BvF 3/92, Rn. 158, wonach das Gebot der Normenklarheit nicht nur aus Sicht der anwendenden Gerichte gilt, sondern auch aus Sicht der potentiell überwachten Personen: „Letztlich muss der Betroffene in der Lage sein, die Auswirkungen einer Datenerhebung zu überblicken“.

## 5. Anhang: Auszüge Entwurf BVerfSchG

### § 9d BVerfSchG – 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 Absatz 2, § 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 Alternative 1, 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 BVerfSchG – 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.

### **§ 11 G-10-Gesetz – neue Absätze 1a und 1b**

(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.