Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht)

Ebenso wie das Grundrecht auf informationelle Selbstbestimmung (siehe Volkszählungsurteil) ist das IT-Grundrecht durch ein Urteil des Bundesverfassungsgerichts (BVerfGE vom 27.02.2008, Az.: 1 BvR 370/07) erstmalig festgeschrieben worden und nicht ausdrücklich im Grundrechtskatalog des Grundgesetzes verankert. Es wird auch als Computergrundrecht oder Grundrecht auf digitale Intimsphäre bezeichnet und schützt persönliche Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden.

Ursprung des Urteils zum IT-Grundrecht

Grundlage für das im Jahr 2008 entwickelte Grundrecht waren Verfassungsbeschwerden gegen die Normen des Verfassungsschutzgesetzes des Landes Nordrhein-Westfalen zur Online-Durchsuchung. Die entsprechenden Normen erklärte das Bundesverfassungsgericht in seinem Urteil für verfassungswidrig. Das IT-Grundrecht ist Ausfluss des allgemeinen Persönlichkeitsrechts, welches sich aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes herleitet.

Inhalt des IT-Grundrechts

Das IT-Grundrecht schützt einzelne Personen vor dem Zugriff auf Netzwerke, Computer und andere informationstechnische Systeme, über die er allein oder mit anderen gemeinsam verfügt, wenn ein Zugriff auf diese Systeme einen Einblick in wesentliche Teile der Lebensgestaltung der Person ermöglicht. Gegenüber dem Grundrecht des Telekommunikationsgeheimnisses (Artikel 10 Absatz 1 Grundgesetz), der Unverletzlichkeit der Wohnung (Artikel 13 Absatz 1 Grundgesetz) sowie dem Rechts auf informationelle Selbstbestimmung ist das IT-Grundrecht zwar nachrangig, hilft aber dabei, die durch den technischen Fortschritt entstehenden Rechtsschutzlücken hinsichtlich der Datenverarbeitung und -speicherung zu schließen. Der Schutzbereich ist dann eröffnet, wenn auf ein informationstechnisches System, dergestalt zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.

Einschränkungen dieses Rechts sind nur zulässig wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr für überragend wichtige Rechtsgüter bestehen. Als solche überragend wichtigen Rechtsgüter bezeichnet das Gericht Leib, Leben und Freiheit der Person so wie solche Güter der Allgemeinheit, deren Bedrohung den Bestand des Staates oder die Existenz der Menschen gefährden würde.

Einfluss des Urteils auf die Gesetzgebung

Die im Urteil zum IT-Grundrecht getroffenen Erwägungen sind als Maßstab für künftige Regelungen zur Online-Durchsuchung heranzuziehen, betreffen aber auch mögliche andere staatliche Eingriffe in Computersysteme. Zudem kann sich aus dem Grundrecht eine Schutzpflicht des Staates ergeben. Ähnlich wie etwa das Briefgeheimnis durch Strafnormen oder das Telekommunikationsgeheimnis zusätzlich durch spezielles Telekommunikationsrecht geschützt wird, kann sich eine staatliche Verpflichtung ergeben, die Bürgerinnen und Bürger vor Eingriffen Dritter in informationstechnischen System zu schützen.

Leitsätze

zum Urteil des Ersten Senats vom 27. Februar 2008

- 1 BvR 370/07 -

- 1 BvR 595/07 -

1 Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

2 Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

3 Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

4 Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.

5 Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.

Wortlaut des

Urteils des Ersten Senats vom 27. Februar 2008

BUNDESVERFASSUNGSGERICHT
- 1 BvR 370/07 –
- 1 BvR 595/07 -

Verkündet
am 27. Februar 2008
Kehrwecker
Amtsinspektor
als Urkundsbeamter
der Geschäftsstelle

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerden

1. a) der Frau W...,
b) des Herrn B...,

- Bevollmächtigter:
Rechtsanwalt Dr. Fredrik Roggan,
Müllerstraße 153, 13353 Berlin -

gegen § 5 Abs. 2 Nr. 11 in Verbindung mit § 7 Abs. 1, § 5 Abs. 3, § 5a Abs. 1 und § 13 VSG NRW in der Fassung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW 2006, S. 620)
- 1 BvR 370/07 -,

2. a) des Herrn B...,
b) des Herrn Dr. R...,
c) des Herrn S...

- Bevollmächtigte:
1 Rechtsanwälte Baum, Reiter & Collegen,
Benrather Schlossallee 121, 40597 Düsseldorf,
2 Rechtsanwalt Peter Schantz,
Schaperstraße 10, 10719 Berlin,
Bevollmächtigter der Beschwerdeführer zu 2a und 2b -

gegen § 5 Abs. 2 Nr. 11, § 5 Abs. 3, § 7 Abs. 2, § 8 Abs. 4 Satz 2 in Verbindung mit §§ 10, 11 und
§ 17 Abs. 1 VSG NRW in der Fassung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW 2006, S. 620)
- 1 BvR 595/07 -
hat das Bundesverfassungsgericht - Erster Senat – unter Mitwirkung der Richterin und Richter

Präsident Papier,
Hohmann-Dennhardt,
Hoffmann-Riem,
Bryde,
Gaier,
Eichberger,
Schluckebier,
Kirchhof,

aufgrund der mündlichen Verhandlung vom 10. Oktober 2007 durch

Urteil

für Recht erkannt:

1 § 5 Absatz 2 Nummer 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen in der Fassung des Gesetzes vom 20. Dezember 2006 (Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Seite 620) ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, Artikel 10 Absatz 1 und Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar und nichtig.

2 Damit erledigen sich die von den Beschwerdeführern gegen § 5 Absatz 3 und § 17 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen erhobenen Rügen.

3 Die Verfassungsbeschwerde des Beschwerdeführers zu 1b wird zurückgewiesen, soweit sie gegen § 5a Absatz 1 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen gerichtet ist.

4 Im Übrigen werden die Verfassungsbeschwerden verworfen.

5 Das Land Nordrhein-Westfalen hat den Beschwerdeführern drei Viertel ihrer notwendigen Auslagen zu erstatten.

Gründe:

A.

Gegenstand der Verfassungsbeschwerden sind Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen (im Folgenden: VSG), die zum einen Befugnisse der Verfassungsschutzbehörde zu verschiedenen Datenerhebungen insbesondere aus informationstechnischen Systemen, zum anderen den Umgang mit den erhobenen Daten regeln.

I.

Die angegriffenen Vorschriften wurden überwiegend durch das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW, S. 620) eingefügt oder geändert.

1. Beide Verfassungsbeschwerden rügen die Verfassungswidrigkeit von § 5 Abs. 2 Nr. 11 VSG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde zu zwei Arten von Ermittlungsmaßnahmen: zum einen zum heimlichen Beobachten und sonstigen Aufklären des Internet (Alt. 1), zum anderen zum heimlichen Zugriff auf informationstechnische Systeme (Alt. 2).

a) Das Internet ist ein elektronischer Verbund von Rechnernetzwerken. Es besteht damit aus informationstechnischen Systemen und kann zudem auch selbst als informationstechnisches System angesehen werden. Der Unterschied der beiden in § 5 Abs. 2 Nr. 11 VSG geregelten Maßnahmetypen ist am äußeren Erscheinungsbild des technischen Zugriffs auf das informationstechnische System ausgerichtet. Unter dem heimlichen Aufklären des Internet ist eine Maßnahme zu verstehen, mit der die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer serverorientierten Internetaufklärung.

Unter einem heimlichen Zugriff auf ein informationstechnisches System ist demgegenüber eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer clientorientierten Aufklärung des Internet. Allerdings enthält die angegriffene Vorschrift keinen Hinweis darauf, dass sie ausschließlich Maßnahmen im Rahmen einer am Server-Client-Modell orientierten Netzwerkstruktur ermöglichen soll.

b) Soweit § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG zum heimlichen Aufklären des Internet ermächtigt, regelt die Norm zunächst die Kenntnisnahme allgemein zugänglicher Kommunikationsinhalte durch die Verfassungsschutzbehörde. Beispiel wäre der Aufruf einer nicht zugangsgesicherten Webseite im World Wide Web mittels eines Web-Browsers. Nach der Gesetzesbegründung soll die

Verfassungsschutzbehörde daneben in die Lage versetzt werden, unter einer Legende an Chats, Auktionen oder Tauschbörsen teilzunehmen oder verborgene Webseiten aufzufinden (vgl. LTDrucks 14/2211, S. 17). Denkbar wäre zudem etwa, dass die Verfassungsschutzbehörde ein anderweitig - beispielsweise von einem Informanten oder durch sogenanntes Keylogging - ermitteltes Passwort einsetzt, um auf ein E-Mail-Postfach oder auf eine zugangsgeschützte Webseite zuzugreifen. Auch in einem derartigen Fall würde die Verfassungsschutzbehörde Inhalte der Internetkommunikation äußerlich auf dem dafür vorgesehenen Weg zur Kenntnis nehmen.

c) Der in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG geregelte heimliche Zugriff auf informationstechnische Systeme mittels technischer Infiltration wird in jüngerer Zeit in Politik und Rechtswissenschaft unter dem Schlagwort „Online-Durchsuchung/Online-Überwachung“ intensiv diskutiert (vgl. zur juristischen Auseinandersetzung etwa Buermeyer, HRRS 2007, S. 392; Hofmann, NStZ 2005, S. 121; Hornung, DuD 2007, S. 575; Rux, JZ 2007, S. 285; Schaar/Landwehr, K&R 2007, S. 202; Schlegel, GA 2007, S. 648; Warntjen, Jura 2007, S. 581). Vereinzelt wurden derartige Maßnahmen durch Bundesbehörden bereits ohne besondere gesetzliche Ermächtigung durchgeführt. Über die Art der praktischen Durchführung der bisherigen „Online-Durchsuchungen“ und deren Erfolge ist wenig bekannt. Die von dem Senat im Rahmen der mündlichen Verhandlung angehörten Präsidenten des Bundeskriminalamts und des Bundesamts für Verfassungsschutz haben mangels einer entsprechenden Aussagegenehmigung keine Ausführungen dazu gemacht. Die Durchführung solcher Maßnahmen wurde im Übrigen einstweilen eingestellt, als der Bundesgerichtshof entschied, dass die Strafprozessordnung für derartige Maßnahmen derzeit keine Rechtsgrundlage enthält (vgl. BGHSt 51, 211).

aa) Die hier zu prüfende Landesnorm enthält die erste und bislang einzige ausdrückliche Ermächtigung einer deutschen Behörde zu „Online-Durchsuchungen“. Auf Bundesebene ist derzeit umstritten, welche Behörden unter welchen Voraussetzungen zu „Online-Durchsuchungen“ ermächtigt werden sollen. Insbesondere wird gegenwärtig diskutiert, eine derartige Ermächtigung für das Bundeskriminalamt im Zuge seiner - im Rahmen der sogenannten Föderalismusreform neu in das Grundgesetz aufgenommenen - Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus (Art. 73 Nr. 9a GG) zu schaffen.

bb) „Online-Durchsuchungen“ sollen den Ermittlungsschwierigkeiten Rechnung tragen, die sich ergeben, wenn Straftäter, insbesondere solche aus extremistischen und terroristischen Kreisen, zur Kommunikation sowie zur Planung und Durchführung von Straftaten informationstechnische Mittel und insbesondere das Internet nutzen. Die Präsidenten des Bundeskriminalamts und des Bundesamts für Verfassungsschutz haben in der mündlichen Verhandlung dargelegt, dass informationstechnische Systeme auch genutzt werden, um weltumspannend Kontakte zur Vorbereitung terroristischer Gewalttaten aufzubauen und zu pflegen. Insbesondere wenn Personen, die extre-

mistischen oder terroristischen Kreisen zuzurechnen sind, gespeicherte Dateien und Kommunikationsinhalte verschlüsseln oder verstecken, könnten Ermittlungen mit den klassischen Methoden wie etwa einer Beschlagnahme von informationstechnischen Systemen und Speichermedien oder einer netzbasierten Telekommunikationsüberwachung erheblich erschwert oder sogar ganz unmöglich gemacht werden.

Der heimliche Zugriff auf ein informationstechnisches System kann mit erheblichen Schwierigkeiten verbunden sein (vgl. zum Folgenden etwa Buermeyer, HRRS 2007, S. 154; Hansen/Pfitzmann, DRiZ 2007, S. 225; Pohl, DuD 2007, S. 684). Dies ist insbesondere der Fall, wenn der Nutzer des Zielsystems technische Sicherheitsvorkehrungen getroffen hat und sein Betriebssystem regelmäßig aktualisiert. Nach Auffassung der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann der Betroffene eine Infiltration jedenfalls auf einigen der in Betracht kommenden Zugriffswege derzeit wirkungsvoll verhindern. Zumindest kann eine solche Infiltration je nach Lage des Einzelfalls mit erheblichem Zeitaufwand verbunden sein.

Gelingt die Infiltration, so bietet sie der Ermittlungsbehörde gegenüber herkömmlichen Ermittlungsmethoden mehrere Vorteile. Wegen der Heimlichkeit des Zugriffs ist der Betroffene, anders als etwa bei einer offen durchgeführten Wohnungsdurchsuchung, nicht für die Zukunft vorgewarnt. Soweit der Nutzer eines Rechners Daten nur in verschlüsselter Form ablegt, können solche Daten im Rahmen einer „Online-Durchsuchung“ gegebenenfalls in unverschlüsselter Form erhoben werden. Denn durch die Infiltration des Rechners kann die Behörde in der Weise auf die Daten zugreifen wie der Nutzer sie im fraglichen Zeitpunkt verwendet. Der Vorteil der Umgehung von Verschlüsselungstechnik ist auch bedeutsam für eine Überwachung der laufenden Internetkommunikation. Soweit solche Kommunikation verschlüsselt abläuft - dies ist insbesondere bei der Sprachtelefonie oftmals der Fall -, kann sie nur am Endgerät wirkungsvoll überwacht werden. Durch eine länger andauernde Überwachung der Nutzung des Rechners können eingesetzte Verschlüsselungstechnologien und andere Sicherheitsvorkehrungen weitgehend umgangen werden. Zudem können auch flüchtige Daten wie etwa Passwörter und weitere Informationen über das Nutzungsverhalten des Betroffenen erhoben werden. Solche Erkenntnisse ließen sich mittels klassischer Ermittlungsmethoden kaum gewinnen.

d) § 5 Abs. 2 Nr. 11 VSG ermächtigt die Verfassungsschutzbehörde zu den geregelten Maßnahmen grundsätzlich unter den allgemeinen Voraussetzungen für nachrichtendienstliche Datenerhebungen, die sich aus § 5 Abs. 2 in Verbindung mit § 7 Abs. 1 und § 3 Abs. 1 VSG ergeben. Danach ist grundsätzlich erforderlich, dass auf diese Weise Erkenntnisse über verfassungsschutzrelevante Bestrebungen oder Tätigkeiten oder die zur Erlangung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können. Soweit Maßnahmen nach der angegriffenen Norm einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen beziehungsweise in Art und Schwere

diesem gleichkommen, sind sie jedoch gemäß § 5 Abs. 2 Nr. 11 Satz 2 VSG nur unter den Voraussetzungen des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10; im Folgenden: Gesetz zu Art. 10 Grundgesetz) zulässig.

e) Nur die Beschwerdeführer zu 2 wenden sich im Zusammenhang mit Maßnahmen nach § 5 Abs. 2 Nr. 11 VSG auch gegen § 17 VSG, der die Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörde regelt.

2. Beide Verfassungsbeschwerden richten sich weiter gegen § 5 Abs. 3 VSG. Diese Vorschrift hat die Benachrichtigung des Betroffenen nach einem Einsatz der in § 5 Abs. 2 VSG geregelten nachrichtendienstlichen Mittel zum Gegenstand. Sie enthält in Satz 1 eine grundsätzliche Pflicht zur Benachrichtigung, von der Satz 2 mehrere Ausnahmen vorsieht.

3. Nur die Beschwerdeführer zu 1 wenden sich gegen § 5a Abs. 1 VSG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde dazu, bei Kreditinstituten Auskünfte über Beteiligte am Zahlungsverkehr und über Geldbewegungen und Geldanlagen einzuholen. Voraussetzung ist, dass tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die Schutzgüter des Verfassungsschutzes bestehen.

Eine Ermächtigung zur Erhebung von Kontoinhalten enthielt das Verfassungsschutzgesetz bereits vor dem Änderungsgesetz vom 20. Dezember 2006. Neu an der angegriffenen Fassung der Vorschrift ist, dass Kontoinhalte auch erhoben werden dürfen, um Erkenntnisse über Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG zu erlangen, nämlich solche, die allgemein gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Nach der Gesetzesbegründung soll hiermit ermöglicht werden, die Finanzierungsströme inländischer terroristischer Netzwerke, sogenannter „home-grown-networks“, aufzudecken (vgl. LTDrucks 14/2211, S. 19).

4. Ebenfalls nur die Beschwerdeführer zu 1 rügen die Verfassungswidrigkeit von § 13 VSG. Diese Norm ermächtigt die Verfassungsschutzbehörde, ihre Erkenntnisse in gemeinsamen Dateien mit anderen Sicherheitsbehörden zu verarbeiten. Wegen Anlass, Umfang und weiteren Anforderungen an die Dateiführung verweist die Norm auf sonstiges Bundes- oder Landesrecht. Dieses sonstige Recht haben die Beschwerdeführer zu 1 allerdings nicht zum Gegenstand ihrer Verfassungsbeschwerde gemacht.

5. Ausschließlich die Beschwerdeführer zu 2 wenden sich gegen § 7 Abs. 2 VSG. Diese Vorschrift ermächtigt die Verfassungsschutzbehörde zur akustischen und optischen Überwachung von Wohnungen. Sie stammt aus dem Jahr 1994 und wurde im Rahmen der Novellierung des Verfas-

sungsschutzgesetzes nicht verändert. Eine Überarbeitung oder Streichung der Norm wurde zwar erwogen, letztlich aber zurückgestellt (vgl. LTDrucks 14/2211, S. 16).

6. Schließlich greifen wiederum nur die Beschwerdeführer zu 2 die in § 8 Abs. 4 Satz 2 in Verbindung mit §§ 10, 11 VSG enthaltenen Regelungen über die Führung sogenannter elektronischer Sachakten an. Diese Vorschriften sehen in ihrer Zusammenschau vor, dass personenbezogene Daten, die in solchen Sachakten enthalten sind, auch dann gespeichert bleiben dürfen, wenn an der betroffenen Person selbst kein Ermittlungsinteresse der Verfassungsschutzbehörde mehr besteht. Damit soll die für eine elektronische Dokumentenverwaltung erforderliche Vollständigkeit der elektronisch geführten Sachakte gesichert werden. Die Belange des Datenschutzes werden dadurch berücksichtigt, dass die betroffenen personenbezogenen Daten nicht mehr recherchierbar sein und auch nicht uneingeschränkt verwendet werden dürfen.

7. Das Verfassungsschutzgesetz lautet im Zusammenhang auszugsweise, soweit für die vorliegenden Verfahren von Interesse:

§ 3
Aufgaben

(1) Aufgabe der Verfassungsschutzbehörde ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht,
3. Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,
4. Bestrebungen und Tätigkeiten, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes) oder das friedliche Zusammenleben der Völker (Artikel 26 des Grundgesetzes) gerichtet sind,

im Geltungsbereich des Grundgesetzes, soweit tatsächliche Anhaltspunkte für den Verdacht solcher Bestrebungen und Tätigkeiten vorliegen.

...

§ 5
Befugnisse

(1) ...
(2) Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:

...

11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. Soweit solche Maßnahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu

...

(3) Mit nachrichtendienstlichen Mitteln gewonnene personenbezogene Daten sind zu kennzeichnen und den Personen, zu denen diese Informationen erfasst wurden, nach Beendigung der Maßnahme mitzuteilen. Einer Mitteilung bedarf es nicht, wenn

1. eine Gefährdung der Aufgabenerfüllung durch die Benachrichtigung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Offenlegung des Erkenntnisstandes oder der Arbeitsweise der Verfassungsschutzbehörde zu befürchten ist,
3. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen,
5. eine der unter 1-4 genannten Voraussetzungen auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt und mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegen wird.

...

§ 5a
Besondere Befugnisse

(1) Die Verfassungsschutzbehörde darf im Einzelfall bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen unentgeltlich Auskünfte über Beteiligte am Zahlungsverkehr und über Geldbewegungen und Geldanlagen einholen, wenn dies zur Erfüllung ihrer Aufgaben nach § 3 Abs. 1 erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 3 Abs. 1 genannten Schutzgüter vorliegen.
(2) ...
(3) Auskünfte nach den Absätzen 1 bis 2 dürfen nur auf Antrag eingeholt werden. Der Antrag ist durch den Leiter der Verfassungsschutzabteilung oder seinen Vertreter schriftlich zu stellen und zu begründen. Über den Antrag entscheidet der Innenminister. Die G 10-Kommission (§ 3 Abs. 1 Satz 1 des Gesetzes über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz (AG G 10 NRW)) ist unverzüglich über die beschiedenen Anträge vor deren Vollzug zu unterrichten. Bei Gefahr im Verzuge kann der Innenminister den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen. Die G 10-Kommission prüft von Amts wegen oder auf Grund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 3 Abs. 5 AG G 10 NRW ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach den Absätzen 1 bis 2 erlangten personenbezogenen Daten erstreckt. Entscheidungen über Auskünfte, die die G 10-Kommission für unzulässig oder nicht notwendig erklärt, hat der Innenminister unverzüglich aufzuheben. Für die Verarbeitung der nach den Absätzen 1 bis 2 erhobenen Daten ist § 4 AG G 10 NRW entsprechend anzuwenden. Das Auskunftsersuchen und die übermittelten Daten dürfen dem Betroffenen oder Dritten vom Auskunftsgeber nicht mitgeteilt werden. § 5 AG G 10 NRW findet entsprechende Anwendung.

...

§ 7
Besondere Formen der Datenerhebung
(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben Informationen, insbesondere personenbezogene Daten, durch Befragung von nichtöffentlichen Stellen und mit den Mitteln gemäß § 5 Abs. 2 erheben, wenn Tatsachen die Annahme rechtfertigen, dass

1. auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 oder die zur Erlangung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können oder
2. dies zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen der Verfassungsschutzbehörde gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

(2) Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr (Artikel 13 Abs. 4 des Grundgesetzes) darf das in einer Wohnung

nicht öffentlich gesprochene Wort mit technischen Mitteln heimlich mitgehört oder aufgezeichnet werden. Satz 1 gilt entsprechend für einen verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen. Maßnahmen nach den Sätzen 1 und 2 werden durch den Leiter der Verfassungsschutzabteilung oder seinen Vertreter angeordnet, wenn eine richterliche Entscheidung nicht rechtzeitig herbeigeführt werden kann. Die richterliche Entscheidung ist unverzüglich nachzuholen. Zuständig ist das Amtsgericht, in dessen Bezirk die Verfassungsschutzbehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die erhobenen Informationen dürfen nur nach Maßgabe des § 4 Abs. 4 AG G 10 NRW verwendet werden. Technische Mittel im Sinne der Sätze 1 und 2 dürfen überdies zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen verwendet werden, soweit dies zur Abwehr von Gefahren für deren Leben, Gesundheit oder Freiheit unerlässlich ist (Artikel 13 Abs. 5 des Grundgesetzes). Maßnahmen nach Satz 8 werden durch den Leiter der Verfassungsschutzabteilung oder seinen Vertreter angeordnet. Außer zu dem Zweck nach Satz 8 darf die Verfassungsschutzbehörde die hierbei erhobenen Daten nur zur Gefahrenabwehr im Rahmen ihrer Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 sowie für Übermittlungen nach Maßgabe des § 4 Abs. 4 Nr. 1 und 2 AG G 10 NRW verwenden. Die Verwendung ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzuge ist die richterliche Entscheidung unverzüglich nachzuholen. § 4 Abs. 6 AG G 10 NRW gilt entsprechend. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird insoweit eingeschränkt.

...

§ 8
Verarbeitung personenbezogener Daten

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben personenbezogene Daten in schriftlichen oder elektronischen Akten und in zur Person geführten Dateien verarbeiten, wenn tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen und Tätigkeiten nach § 3 Abs. 1 vorliegen, dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 erforderlich ist oder dies für die Erfüllung ihrer Aufgaben nach § 3 Abs. 2 erforderlich ist.

...

(4) Der Zugriff auf personenbezogene Daten in elektronischen Sachakten ist zu protokollieren. In elektronischen Sachakten gespeicherte personenbezogene Daten dürfen nach Löschung der zur Person geführten Dateien nicht für Aufgaben nach § 3 Abs. 2 verwandt oder an andere Behörden übermittelt werden. Solche Daten dürfen nicht elektronisch recherchierbar sein.

...

§ 10
Berichtigung, Löschung und Sperrung
personenbezogener Daten in zur Person
geführten Dateien

(1) Die Verfassungsschutzbehörde hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind. ...

(2) Die Verfassungsschutzbehörde hat die in Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. ...

...

§ 11
Berichtigung und Sperrung
personenbezogener Daten in schriftlichen oder elektronischen Akten, Aktenvernichtung

(1) Stellt die Verfassungsschutzbehörde fest, dass in schriftlichen oder elektronischen Akten gespeicherte personenbezogene Daten unrichtig sind, sind sie zu berichtigen. ...

(2) Die Verfassungsschutzbehörde hat personenbezogene Daten in schriftlichen oder elektronischen Akten zu sperren, wenn sie im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden und die Daten für ihre künftige Aufgabenerfüllung nicht mehr erforderlich sind. ...

(3) Die Verfassungsschutzbehörde hat zur Person geführte Akten zu vernichten, wenn diese zu ihrer Aufgabenerfüllung nicht mehr erforderlich sind und der Vernichtung schutzwürdige Belange der betroffenen Person nicht entgegenstehen. ...

...
§ 13
Gemeinsame Dateien

Die Verfassungsschutzbehörde ist befugt, personenbezogene Daten in gemeinsamen Dateien mit den Verfassungsschutzbehörden des Bundes und der Länder und anderen Sicherheitsbehörden

zu verarbeiten, wenn besondere bundesrechtliche oder landesrechtliche Vorschriften Anlass, Umfang und sonstige datenschutzrechtliche Anforderungen regeln.

§ 14
Auskunft

(1) Die Verfassungsschutzbehörde erteilt auf schriftlichen Antrag der antragstellenden Person gebührenfrei Auskunft über die zu ihrer Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Speicherung. Ein Recht auf Akteneinsicht besteht nicht.

...

§ 17
Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörde

(1) Die Verfassungsschutzbehörde darf personenbezogene Daten an Gerichte und inländische Behörden übermitteln, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist oder der Empfänger zum Zwecke der Erfüllung seiner Aufgaben die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. ...

(2) Die Verfassungsschutzbehörde darf personenbezogene Daten an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit die Bundesrepublik Deutschland dazu im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. II 1961 S. 1183, 1218) verpflichtet ist.

(3) Die Verfassungsschutzbehörde darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben oder zur Abwehr einer erheblichen Gefahr für den Empfänger erforderlich ist. ...

...

Das Gesetz zu Artikel 10 Grundgesetz, auf das § 5 Abs. 2 Nr. 11 Satz 2 VSG verweist, enthält für Telekommunikationsüberwachungen durch Verfassungsschutzbehörden unter anderem folgende Regelungen:

§ 1

Gegenstand des Gesetzes

(1) Es sind

1. die Verfassungsschutzbehörden des Bundes und der Länder ... zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages,

2. ... berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen. ...

...

§ 3
Voraussetzungen

(1) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80 bis 83 des Strafgesetzbuches),
2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84 bis 86, 87 bis 89 des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),
3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 96, 97a bis 100a des Strafgesetzbuches),
4. Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches),
5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages (§§ 87, 89, 94 bis 96, 98 bis 100, 109e bis 109g des Strafgesetzbuches) in Verbindung mit Artikel 7 des Vierten Strafrechtsänderungsgesetzes vom 11. Juni 1957 (BGBl. I S. 597) in der Fassung des Gesetzes vom 25. Juni 1968 (BGBl. I S. 741),
6. Straftaten nach

a) den §§ 129a bis 130 des Strafgesetzbuches sowie
b) den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder
7. Straftaten nach § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes plant, begeht oder begangen hat. Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied

einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

(2) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind.

Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

§ 4
Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung

(1) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 1 Abs. 1 Nr. 1 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. ...

...

§ 9
Antrag

(1) Beschränkungsmaßnahmen nach diesem Gesetz dürfen nur auf Antrag angeordnet werden.

...

§ 10
Anordnung

(1) Zuständig für die Anordnung von Beschränkungsmaßnahmen ist bei Anträgen der Verfassungsschutzbehörden der Länder die zuständige oberste Landesbehörde, im Übrigen ein vom Bundeskanzler beauftragtes Bundesministerium.

...

Die in § 5a Abs. 3 VSG in Bezug genommenen §§ 4 und 5 des nordrhein-westfälischen Gesetzes über die Ausführung des Gesetzes zu Artikel 10 Grundgesetz (im Folgenden: AG G 10 NRW) lauten auszugsweise:

§ 4
Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung

(1) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. ...

...

§ 5
Kontrolle der Mitteilung
an Betroffene durch die G 10-Kommission

(1) Beschränkungsmaßnahmen sind Betroffenen durch das Innenministerium nach ihrer Einstellung mitzuteilen, wenn eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. ...

...

II.

1. Die Beschwerdeführerin zu 1a ist Journalistin und schreibt vor allem für eine Online-Publikation. Im Rahmen ihrer beruflichen Tätigkeit besucht sie auch Internet-Präsenzen, die von verfassungsfeindlichen Personen und Organisationen betrieben werden. Sie engagiert sich darüber hinaus in datenschutzrechtlichen Angelegenheiten und betreibt zusammen mit anderen die Homepage

www.stop1984.com. Im Zusammenhang mit dieser Homepage besteht die Möglichkeit, an sogenannten Chats teilzunehmen. Diese Möglichkeit wird auch von Rechtsextremisten genutzt. Informationen über diese Personen speichert die Beschwerdeführerin zu 1a auf der Festplatte ihres privat wie beruflich genutzten Computers.

Der Beschwerdeführer zu 1b ist aktives Mitglied des Landesverbandes Nordrhein-Westfalen der Partei DIE LINKE, die vom nordrhein-westfälischen Verfassungsschutz beobachtet wird. Für seine politische Tätigkeit nutzt er auch seinen an das Internet angeschlossenen Computer. Wie die Beschwerdeführerin zu 1a greift er daneben auf das Internet zur privaten Kommunikation sowie zur Abwicklung von Zahlungsvorgängen über sein Girokonto zu.

Die Beschwerdeführer zu 2a und 2b sind Sozien einer Rechtsanwaltskanzlei. Der Beschwerdeführer zu 2a betreut als Rechtsanwalt unter anderem Asylbewerber. Unter ihnen befand sich ein führendes Mitglied der kurdischen Arbeiterpartei PKK, die unter der Beobachtung der nordrhein-westfälischen Verfassungsschutzbehörde steht. Er nutzt sowohl in seiner Wohnung als auch in den Kanzleiräumen Computernetzwerke, die mit dem Internet verbunden sind. Das Kanzleinetzwerk wird auch von dem Beschwerdeführer zu 2b sowie von dem Beschwerdeführer zu 2c, der in der Kanzlei als freier Mitarbeiter beschäftigt ist, genutzt.

2. Soweit die Verfassungsbeschwerden sich gegen § 5 Abs. 2 Nr. 11 VSG richten, rügen die Beschwerdeführer eine Verletzung von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 13 Abs. 1 GG.

Soweit die Norm eine Teilnahme an Kommunikationseinrichtungen des Internet vorsehe, regle sie einen Eingriff in das Fernmeldegeheimnis. In dem von der Norm weiter vorgesehenen heimlichen Zugriff auf informationstechnische Systeme liege ein Eingriff in Art. 13 GG, wenn der Zugriffsrechner sich in einer Wohnung befinde. Maßgeblich sei insoweit, dass persönliche Verhaltensweisen gerade durch ihre Verwirklichung in der räumlich abgeschotteten Wohnung einen besonderen Schutz genössen. Daneben könnten derartige Maßnahmen auch in das allgemeine Persönlichkeitsrecht und in das Fernmeldegeheimnis eingreifen.

Soweit Maßnahmen nach § 5 Abs. 2 Nr. 11 VSG als Eingriff in Art. 13 GG anzusehen seien, sei die Vorschrift bereits deshalb verfassungswidrig, weil sie keinem der besonderen Schrankenvorbehalte von Art. 13 Abs. 2 bis 7 GG genüge. Auch sei das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG nicht gewahrt.

§ 5 Abs. 2 Nr. 11 VSG verstoße zudem gegen das Gebot der Normenklarheit. Die in Satz 2 der Norm enthaltene Verweisung auf das Gesetz zu Artikel 10 des Grundgesetzes sei weder in ihren

Voraussetzungen noch in ihrer Reichweite hinreichend bestimmt. Weiter fehle es an hinreichenden normativen Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Solche Vorkehrungen seien erforderlich, da heutzutage insbesondere privat genutzte Rechner in weitem Umfang dazu dienten, Daten höchstpersönlichen Inhalts zu verarbeiten. Schließlich sei der Verhältnismäßigkeitsgrundsatz nicht gewahrt. Die gesetzliche Eingriffsschwelle sei zu niedrig angesetzt. Zudem fehle es an Verfahrensvorkehrungen zum Schutz des Betroffenen wie etwa einem Richtervorbehalt. Auch könnten die erhobenen Daten in zu weitem Umfang zweckentfremdet oder an andere Behörden übermittelt werden.

3. Die Beschwerdeführer rügen weiter, § 5 Abs. 3 VSG verletze die Rechtsschutzgarantie des Art. 19 Abs. 4 GG sowie die materiellen Grundrechte, in die durch Maßnahmen nach § 5 Abs. 2 VSG eingegriffen werde. Satz 2 der Vorschrift sehe zu weitgehende Ausnahmen von der grundrechtlich gebotenen Benachrichtigungspflicht vor, die diese weitgehend leer laufen ließen.

4. Die Beschwerdeführer zu 1 sind der Auffassung, § 5a Abs. 1 VSG verletze das Recht auf informationelle Selbstbestimmung. Die Vorschrift ermögliche die Erhebung von Kontoinhalten unter zu niedrigen Voraussetzungen und sei daher unverhältnismäßig. § 13 VSG verstoße gegen das Trennungsgebot zwischen Geheimdiensten und Polizeibehörden, das als Ausprägung des Rechtsstaatsgebots in Verbindung mit dem Recht auf informationelle Selbstbestimmung anzusehen sei.

5. Die Beschwerdeführer zu 2 bringen vor, § 7 Abs. 2 VSG verletze Art. 13 Abs. 1 GG. Die Vorschrift entspreche nicht den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zur strafprozessualen akustischen Wohnraumüberwachung aufgestellt habe. § 8 Abs. 4 Satz 2 VSG verletze das Recht auf informationelle Selbstbestimmung, da es an einer Regelung über die Löschung personenbezogener Daten in elektronischen Sachakten fehle. Die Norm ermögliche damit eine unzulässige Datenspeicherung auf Vorrat. Soweit Daten betroffen seien, die durch eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG gewonnen worden seien, sei schließlich auch die in § 17 Abs. 1 VSG enthaltene Übermittlungsregelung verfassungswidrig. Sie verstoße gegen die Gebote der Zweckbindung, der Normenklarheit und der Verhältnismäßigkeit.

III.

Zu den Verfassungsbeschwerden haben schriftlich Stellung genommen: die Bundesregierung, die Landesregierung und der Landtag von Nordrhein-Westfalen, die sächsische Staatsregierung, das Bundesverwaltungsgericht, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Fraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN im nordrhein-westfälischen Landtag haben ein ihnen erstattetes Rechtsgutachten vorgelegt. Der Senat hat zudem sachkundige schriftliche

Stellungnahmen der Herren Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling, Professor Dr. Andreas Pfitzmann und Professor Dr. Ulrich Sieber eingeholt.

1. Die Bundesregierung erörtert ohne direkte Bezugnahme auf die angegriffenen Normen in allgemeiner Form die verfassungsrechtlichen Fragen eines heimlichen Zugriffs auf informationstechnische Systeme mit technischen Mitteln.

Solche Maßnahmen seien von der unter Art. 10 GG fallenden Überwachung der Telekommunikation zu unterscheiden. Bei den in der Vergangenheit von dem Bundesamt für Verfassungsschutz vereinzelt durchgeführten „Online-Durchsuchungen“ sei davon ausgegangen worden, dass grundrechtlicher Maßstab allein Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sei. Zunehmend trete jedoch Art. 13 Abs. 1 GG als möglicherweise einschlägiger Maßstab für „Online-Durchsuchungen“ in den Vordergrund. Die technische Möglichkeit wiederholten Eindringens oder länger andauernden Verweilens in einem Rechner nähere die „Online-Durchsuchung“ einer Überwachung an. Zumindest in der Empfindung der betroffenen Personen könne ein sehr umfassender Teil der Privatsphäre, die sich früher auf die Räume einer Wohnung verteilt habe, im Rechner konzentriert sein.

Der Zugriff bedürfe als qualifiziertes Mittel des Verfassungsschutzes besonderer verfahrensrechtlicher Sicherungen. Der Schutz des Kernbereichs privater Lebensgestaltung sei zu wahren, auch wenn er sich nicht bereits beim Kopieren und Überspielen der von der Software aufgrund bestimmter Suchparameter für relevant gehaltenen Informationen, sondern erst bei der anschließenden Durchsicht der Dateien auf dem Behördenrechner sicherstellen lasse. Angesichts der Nähe zu Maßnahmen der Wohnungsdurchsuchung und Wohnraumüberwachung sei in Erwägung zu ziehen, den Zugriff unter einen Richtervorbehalt zu stellen. Grundsätzlich sei eine Benachrichtigungspflicht vorzusehen. An „Online-Durchsuchungen“ seien zudem hohe Verhältnismäßigkeitsanforderungen zu stellen. Eine solche Maßnahme könne angesichts ihrer Eingriffsintensität für eine Verfassungsschutzbehörde nur ultima ratio sein.

2. Die Landesregierung von Nordrhein-Westfalen hält die Verfassungsbeschwerden für unzulässig, jedenfalls aber für unbegründet.

Die in § 5 Abs. 2 Nr. 11 VSG vorgesehenen Maßnahmen bewirkten keinen Eingriff in Art. 13 GG. Dieses Grundrecht greife nur, wenn eine staatliche Maßnahme einen konkreten Raumbezug aufweise, also räumliche Abgrenzungen überwunden würden. Dies sei hier nicht der Fall. Maßnahmen der Aufklärung des Internet wie die Überwachung des E-Mail-Verkehrs oder der Internet-Telefonie seien allerdings an Art. 10 GG zu messen. Im Übrigen sei das Recht auf informationelle Selbstbestimmung einschlägig.

§ 5 Abs. 2 Nr. 11 VSG genüge dem Gebot der Normenklarheit. Die Norm sei mit Blick auf mögliche technische Neuerungen entwicklungsoffen formuliert worden. Die Norm achte weiter den Kernbereich privater Lebensgestaltung. Der erforderliche Kernbereichsschutz werde durch § 4 Abs. 1 G 10, auf den verwiesen werde, sichergestellt. Die angegriffene Vorschrift sei schließlich auch verhältnismäßig. Der Aktionsraum der Verfassungsschutzbehörde müsse der zunehmenden Verlagerung der Kommunikation gerade auch verfassungsfeindlicher Bestrebungen auf das Internet Rechnung tragen. Der Zugriff auf einzelne Rechner sei erforderlich, weil es technisch möglich sei, Kommunikationsinhalte so zu versenden, dass ein Zugriff während des Versands ausscheide. § 7 Abs. 1 VSG enthalte insoweit eine hinreichende Eingriffsschwelle. Weitere materielle Kriterien und verfahrensrechtliche Vorkehrungen ergäben sich insbesondere aus § 3 G 10. Es sei damit zu rechnen, dass die Zahl der Zugriffe auf informationstechnische Systeme pro Jahr im einstelligen Bereich liegen werde.

Die Regelung der Kennzeichnungs- und Mitteilungspflichten in § 5 Abs. 3 VSG sei gleichfalls verfassungsrechtlich nicht zu beanstanden. Für Maßnahmen der Internetaufklärung nach § 5 Abs. 2 Nr. 11 VSG gelte ohnehin nicht § 5 Abs. 3 VSG, sondern § 12 G 10.

Die in § 5a Abs. 1 VSG enthaltene Befugnis zum Abruf von Kontoinhaltsdaten sei ebenfalls verfassungsgemäß. Das Phänomen sogenannter home-grown-networks, die inländische Anschlagsziele verfolgten, stelle eine neuartige und erhebliche Gefährdungslage dar. Die Befugnis könne zur Aufklärung von personellen Verflechtungen und Finanzflüssen, etwa bei der Waffenbeschaffung, und über die Geldgeber militanter Gruppierungen beitragen.

3. Der nordrhein-westfälische Landtag hält die Verfassungsbeschwerden gleichfalls für unbegründet.

Die Ausweitung des internationalen Terrorismus erzeuge eine neuartige Bedrohungslage, die den Staat im Interesse einer effektiven Terrorabwehr zur Einschränkung von Grundrechten zwinge. Der Rechtsstaat müsse das überkommene rechtliche Instrumentarium behutsam fortentwickeln, um neuen Herausforderungen gerecht zu werden. Insbesondere müsse die informationstechnische Handlungsfähigkeit der Sicherheitsbehörden den aktuellen Rahmenbedingungen angepasst werden. Moderne Kommunikationstechniken würden bei der Begehung und Vorbereitung unterschiedlichster Straftaten eingesetzt und trügen so zur Effektivierung krimineller Handlungen bei.

Zwar seien im klassischen Polizeirecht intensive Grundrechtseingriffe erst ab einer bestimmten Verdachts- beziehungsweise Gefahrenstufe zulässig. Dies beruhe jedoch auf einem behördlichen Aufgabenkreis, der sich grundlegend von der Tätigkeit der Verfassungsschutzbehörden unterscheide. Mit der Gewinnung struktureller Vorfelderkenntnisse zur Aufklärung terroristischer Aktivi-

täten seien in aller Regel keine unmittelbaren Sanktionen und Konsequenzen für die Betroffenen verbunden.

Art. 13 GG werde durch Maßnahmen nach § 5 Abs. 2 Nr. 11 VSG nicht berührt. Der Zugriff auf gespeicherte Daten ziele nicht auf die Überwindung der räumlichen Abgrenzung einer Wohnung ab. Auch sollten keine in der Wohnung stattfindenden Vorgänge überwacht werden. Dagegen könne im Einzelfall ein Eingriff in Art. 10 GG vorliegen. Die Norm genüge jedoch den verfassungsrechtlichen Anforderungen an die Eingriffsrechtfertigung.

Auch die in § 5 Abs. 3 Satz 2 VSG geregelten Ausnahmen von der Benachrichtigungspflicht seien mit dem Grundgesetz vereinbar.

4. Die sächsische Staatsregierung führt aus, die Kommunikation innerhalb islamistischer und islamistisch-terroristischer Gruppierungen erfolge zum großen Teil über das Internet. Auch Autonome benutzten das Internet und Mobiltelefone mit der Möglichkeit geschützter Kommunikation. Mit der vermehrten Nutzung von informationstechnischen Systemen durch beobachtete Personen sei der Zugang über klassische nachrichtendienstliche Mittel teilweise unmöglich geworden.

§ 5 Abs. 2 Nr. 11 VSG ermächtige nicht zu Eingriffen in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG. Die Vorschrift sei im Übrigen hinreichend bestimmt und verhältnismäßig. Der Kernbereich privater Lebensgestaltung sei nicht betroffen, da der Bürger zur höchstpersönlichen Kommunikation nicht auf einen Personalcomputer angewiesen sei. Auch § 5 Abs. 3, § 5a Abs. 1 und § 13 VSG stünden mit dem Grundgesetz in Einklang.

5. Das Bundesverwaltungsgericht äußert verfassungsrechtliche Bedenken gegen die in § 5 Abs. 2 Nr. 11 VSG enthaltene Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme. Sowohl für als auch gegen die Anwendung von Art. 13 GG sprächen gewichtige Argumente. In jedem Fall greife der geregelte Zugriff in das Recht auf informationelle Selbstbestimmung ein. Es erscheine zweifelhaft, ob dieser Eingriff verhältnismäßig sei. Es liege nahe, angesichts des Gewichts des Grundrechtseingriffs eine „Online-Durchsuchung“ von einer konkreten Gefahr für bestimmte Rechtsgüter abhängig zu machen. Das Gesetz enthalte keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

6. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen halten die angegriffenen Normen für verfassungswidrig. Ihre Ausführungen hierzu stimmen in der inhaltlichen Argumentationslinie und im Ergebnis weitgehend mit dem Vorbringen der Beschwerdeführer überein.

7. Die Fraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN im nordrhein-westfälischen Landtag haben ein ihnen erstattetes Rechtsgutachten vorgelegt. Dieses kommt zu dem Schluss, dass die angegriffenen Normen weder mit dem Grundgesetz noch mit der nordrhein-westfälischen Landesverfassung vereinbar sind.

8. Die sachkundigen Auskunftspersonen Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling und Professor Dr. Andreas Pfitzmann haben sich insbesondere zu den technischen Fragen des heimlichen Zugriffs auf informationstechnische Systeme geäußert, Professor Dr. Ulrich Sieber auch zu Fragen der Rechtsvergleichung und zu möglichen Anforderungen an die Rechtmäßigkeit der hier betroffenen Maßnahmen.

IV.

In der mündlichen Verhandlung haben sich geäußert: die Beschwerdeführer, die Bundesregierung, das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, das Bundesamt für Sicherheit in der Informationstechnik, die Landesregierung und der Landtag von Nordrhein-Westfalen, das nordrhein-westfälische Landesamt für Verfassungsschutz, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen sowie als sachkundige Auskunftspersonen die Herren Andreas Bogk, Dirk Fox, Professor Dr. Felix Freiling, Professor Dr. Andreas Pfitzmann und Professor Dr. Ulrich Sieber.

B.

Die Verfassungsbeschwerden sind nur teilweise zulässig.

I.

Soweit die Verfassungsbeschwerden sich gegen § 5 Abs. 2 Nr. 11 VSG richten, bestehen gegen ihre Zulässigkeit keine Bedenken.

II.

Hinsichtlich der von allen Beschwerdeführern erhobenen Rüge der Verfassungswidrigkeit von § 5 Abs. 3 VSG sind die Verfassungsbeschwerden nur insoweit zulässig, als es um die Benachrichtigung im Anschluss an eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG geht. Im Übrigen genügt die Begründung der Verfassungsbeschwerden nicht den Anforderungen von § 23 Abs. 1 Satz 2, § 92 BVerfGG. Danach ist eine Verfassungsbeschwerde hinreichend substantiiert zu begründen. Der Beschwerdeführer hat darzulegen, mit welchen verfassungsrechtlichen Anforderungen die angegriffene Maßnahme kollidiert. Dazu muss er aufzeigen, inwieweit sie die bezeichneten Grundrechte verletzen soll (vgl.BVerfGE 99, 84 <87>; 108, 370 <386>).

Daran fehlt es hier, soweit die Beschwerdeführer allgemein rügen, die Regelung der Benachrichtigung im Anschluss an nachrichtendienstliche Maßnahmen im Sinne des § 5 Abs. 2 VSG genüge nicht den verfassungsrechtlichen Anforderungen. Inwieweit das Grundgesetz eine Benachrichtigung des von einer heimlichen informationellen Maßnahme des Staates Betroffenen verlangt, hängt unter anderem maßgeblich davon ab, ob und mit welcher Intensität diese Maßnahme in Grundrechte des Betroffenen eingreift (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2473>). § 5 Abs. 2 VSG sieht eine Vielzahl unterschiedlicher Maßnahmen vor, die in ihrer Eingriffsqualität und Eingriffsintensität erheblich voneinander abweichen. Angesichts dessen hätten die Beschwerdeführer aufzeigen können und müssen, nach welchen dieser Maßnahmen ihrer Ansicht nach eine Benachrichtigung geboten ist und inwieweit die in § 5 Abs. 3 Satz 2 VSG geregelten Ausnahmen von der Benachrichtigungspflicht angesichts des Gewichts des jeweiligen Grundrechtseingriffs unangemessen sind. Derartige Darlegungen finden sich in den Verfassungsbeschwerden jedoch allein im Hinblick auf Maßnahmen nach § 5 Abs. 2 Nr. 11 VSG in hinreichendem Ausmaß.

III.

Die Verfassungsbeschwerde der Beschwerdeführer zu 2 ist auch zulässig, soweit sie sich gegen § 17 VSG richtet. Insofern ist die Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt. Durch das Inkrafttreten des § 5 Abs. 2 Nr. 11 VSG wurde der Anwendungsbereich der allgemeinen Übermittlungsregelung des § 17 VSG auf die neu geregelten Maßnahmen erstreckt und so teilweise erweitert. Darin liegt eine neue grundrechtliche Beschwer, für welche die Beschwerdefrist neu in Gang gesetzt wird (vgl.BVerfGE 45, 104 <119>; 78, 350 <356>; 100, 313 <356>). Die Rüge der Beschwerdeführer zu 2 beschränkt sich auf diese neue Beschwer.

IV.

Die Verfassungsbeschwerde des Beschwerdeführers zu 1b ist auch insofern zulässig, als sie sich gegen § 5a Abs. 1 VSG richtet. Insbesondere ist die Beschwerdefrist gewahrt. Die Rüge des Beschwerdeführers zu 1b beschränkt sich auf die Erweiterung des Anwendungsbereichs der Norm im Zuge der Novellierung des Verfassungsschutzgesetzes.

Die Verfassungsbeschwerde der Beschwerdeführerin zu 1a ist hingegen in Bezug auf § 5a Abs. 1 VSG unzulässig, da sie ihre eigene und gegenwärtige Betroffenheit durch die angegriffene Norm nicht aufgezeigt hat. Dazu hätte sie darlegen müssen, dass sie mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in ihren Grundrechten berührt wird (vgl.BVerfGE 67, 157 <169 f.>; 100, 313 <354>; 109, 279 <307 f.>). Dies ist hier nicht ersichtlich. Die Beschwerdeführerin zu 1a hat keinerlei Ausführungen gemacht, aus denen sich auch nur die entfernte Wahrscheinlichkeit ergibt, dass ihre Kontoinhaltsdaten für die Verfassungsschutzbehörde von Interesse sein könnten. Nach den Tatbestandsvoraussetzungen von § 5a Abs.

1 VSG und der Natur der geregelten Maßnahmen kann auch nicht für praktisch jedermann von einer möglichen Betroffenheit ausgegangen werden (vgl. zu derartigen FällenBVerfGE 109, 279 <308>; 113, 348 <363>).

V.

Soweit die Verfassungsbeschwerde der Beschwerdeführer zu 2 sich gegen § 7 Abs. 2 VSG richtet, ist die Beschwerdefrist des § 93 Abs. 3 BVerfGG nicht gewahrt. Diese Vorschrift ist bereits 1994 in Kraft getreten. Ohne Belang ist hier, ob der Gesetzgeber der Novelle des Verfassungsschutzgesetzes § 7 Abs. 2 VSG erneut in seinen Willen aufgenommen hat, da hierdurch die Beschwerdefrist nicht neu in Gang gesetzt wird (vgl.BVerfGE 11, 255 <259 f.>; 18, 1 <9>; 43, 108 <116>; 80, 137 <149>).

Den Beschwerdeführern zu 2 wird durch die Unzulässigkeit der Verfassungsbeschwerde in diesem Punkt nicht die Möglichkeit genommen, die Verfassungswidrigkeit der angegriffenen Norm geltend zu machen (vgl. dazu BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 21. November 1996 - 1 BvR 1862/96 -, NJW 1997, S. 650). Falls die Beschwerdeführer zu 2 befürchten, von Maßnahmen nach § 7 Abs. 2 VSG betroffen zu werden, können sie hiergegen Rechtsschutz vor den Verwaltungsgerichten erlangen. Dabei kann grundsätzlich auch vorläufiger sowie vorbeugender Rechtsschutz gewährt werden. Der Umstand, dass dafür ein hinreichendes Rechtsschutzinteresse und die hinreichende Wahrscheinlichkeit einer belastenden Maßnahme dargetan werden müssen, schließt die grundsätzliche Verfügbarkeit fachgerichtlichen Rechtsschutzes nicht aus. Im fachgerichtlichen Verfahren dürfen die Anforderungen an das Rechtsschutzinteresse im Sinne eines effektiven Grundrechtsschutzes nicht überspannt werden (vgl. allgemein dazuBVerfGE 110, 77 <88>).

VI.

Die Verfassungsbeschwerde der Beschwerdeführer zu 2 ist auch insoweit unzulässig, als sie sich gegen die Regelungen von § 8 Abs. 4 Satz 2 in Verbindung mit §§ 10, 11 VSG über den Umgang mit personenbezogenen Daten in elektronischen Sachakten richtet. Hinsichtlich dieser Regelungen ist der Grundsatz der Subsidiarität der Verfassungsbeschwerde nicht gewahrt.

Nach dem Grundsatz der Subsidiarität ist die Verfassungsbeschwerde eines von der angegriffenen Rechtsnorm betroffenen Grundrechtsträgers unzulässig, wenn er in zumutbarer Weise Rechtsschutz durch die Anrufung der Gerichte erlangen kann (vgl.BVerfGE 72, 39 <43 f.>; 90, 128 <136 f.>). Damit soll erreicht werden, dass das Bundesverfassungsgericht nicht auf ungesicherter Tatsachen- und Rechtsgrundlage weitreichende Entscheidungen trifft (vgl.BVerfGE 79, 1 <20>; 97, 157 <165>).

Danach sind die Beschwerdeführer zu 2 zur Erlangung von Rechtsschutz gegen die Regelungen des Verfassungsschutzgesetzes über den Umgang mit personenbezogenen Daten, die in elektronischen Sachakten gespeichert sind, gehalten, sich zunächst an die Fachgerichte zu wenden.

Die Beschwerdeführer zu 2 richten ihre Rüge gegen die von dem Verfassungsschutzgesetz ihrer Ansicht nach vorgesehene Speicherung nicht mehr benötigter personenbezogener Daten. Wie weitgehend das Gesetz die Löschung solcher Daten ausschließt, bedarf jedoch zunächst einfachrechtlich der Klärung durch die Behörden und Fachgerichte. Der Wortlaut des § 10 VSG schließt es jedenfalls nicht aus, die bestehenden Löschungsregeln in dieser Vorschrift auch auf Daten anzuwenden, die in elektronischen Sachakten enthalten sind. Im Übrigen enthält das Gesetz keine ausdrücklichen Regelungen über den Umgang mit nicht mehr benötigten elektronischen Sachakten, so dass die Rechtslage auch insoweit nicht eindeutig ist.

Den Beschwerdeführern zu 2 ist zumutbar, die einfachrechtliche Lage von den dafür zuständigen Fachgerichten klären zu lassen. Insbesondere ist ihnen die Anrufung der Gerichte nicht etwa deshalb faktisch verwehrt, weil sie von den sie betreffenden Datenspeicherungen keine Kenntnis erlangen können. Entgegen der Ansicht der Beschwerdeführer zu 2 ergibt sich aus dem Wortlaut des § 14 Abs. 1 VSG nicht zwingend, dass personenbezogene Daten in elektronischen Sachakten von dem in dieser Norm geregelten Auskunftsanspruch von vornherein nicht erfasst werden, so dass nicht ausgeschlossen ist, dass insoweit Auskunft erteilt werden muss. Zudem geht es den Beschwerdeführern zu 2 mit der gegen § 8 Abs. 4 Satz 2 VSG gerichteten Rüge nicht darum, einen punktuellen Grundrechtseingriff abzuwenden, dem ein nachträglicher Rechtsschutz nur begrenzt abhelfen könnte. Sie wollen vielmehr materiellrechtliche Löschungsansprüche geltend machen, die sie im fachgerichtlichen Verfahren durchsetzen können.

VII.

Soweit die Beschwerdeführer zu 1 die Verfassungswidrigkeit von § 13 VSG rügen, ist ihre Verfassungsbeschwerde mangels unmittelbarer Betroffenheit unzulässig. § 13 VSG erlaubt der Verfassungsschutzbehörde, Daten in gemeinsame Dateien einzustellen, die nach Maßgabe von bundes- oder landesrechtlichen Vorschriften geführt werden. Erst aufgrund dieser anderen Vorschriften können Maßnahmen stattfinden, die als Grundrechtseingriff anzusehen sein könnten. Die Öffnungsnorm des § 13 VSG, die ohne die in Bezug genommenen Dateiführungsregeln leer läuft, ist für sich genommen grundrechtlich irrelevant. Gegen in Bezug genommene Normen, etwa die Vorschriften des Antiterrordateigesetzes vom 22. Dezember 2006 (BGBl I, S. 3409), richtet sich die Verfassungsbeschwerde der Beschwerdeführer zu 1 jedoch nicht.

C.

Die Verfassungsbeschwerden sind, soweit zulässig, weitgehend begründet. § 5 Abs. 2 Nr. 11 VSG ist in der zweiten dort aufgeführten Alternative verfassungswidrig und nichtig (I). Gleiches gilt für die erste Alternative dieser Norm (II). In der Folge der Nichtigkeit erledigen sich die gegen § 5 Abs. 3 und § 17 VSG gerichteten Rügen (III). Gegen § 5a Abs. 1 VSG bestehen hingegen keine verfassungsrechtlichen Bedenken (IV).

I.

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (1). Vorliegend sind die Eingriffe verfassungsrechtlich nicht gerechtfertigt: § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt nicht dem Gebot der Normenklarheit (2 a), die Anforderungen des Verhältnismäßigkeitsgrundsatzes sind nicht gewahrt (2 b) und die Norm enthält keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (2 c). Die angegriffene Norm ist nichtig (2 d). Einer zusätzlichen Prüfung anhand anderer Grundrechte bedarf es nicht (2 e).

1. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; sie tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.

a) Das allgemeine Persönlichkeitsrecht gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen (vgl.BVerfGE 99, 185 <193>; 114, 339 <346>). Einer solchen lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann (vgl.BVerfGE 54, 148 <153>; 65, 1 <41> ; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2465>). Die Zuordnung eines konkreten Rechtsschutzbegehrens zu den verschiedenen Aspekten des Persönlichkeitsrechts richtet sich vor allem nach der Art der Persönlichkeitsgefährdung (vgl.BVerfGE 101, 361 <380>; 106, 28 <39>).

b) Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.

aa) Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.

Dies gilt zunächst für Personalcomputer, über die mittlerweile eine deutliche Mehrheit der Haushalte in der Bundesrepublik verfügt (vgl. Statistisches Bundesamt, Statistisches Jahrbuch 2007, S. 113). Die Leistungsfähigkeit derartiger Rechner ist ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen.

Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind.

bb) Der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Dies wird insbesondere aufgrund der gestiegenen Nutzung des Internet durch große Kreise der Bevölkerung mehr und mehr zum Normalfall.

Eine Vernetzung informationstechnischer Systeme ermöglicht allgemein, Aufgaben auf diese Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen. So können etwa die von einzelnen der vernetzten Systeme gelieferten Daten ausgewertet und die Systeme zu bestimmten Reaktionen veranlasst werden. Auf diese Weise kann zugleich der Funktionsumfang des einzelnen Systems erweitert werden.

Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Rechners nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er aktiv soziale

Verbindungen aufbauen und pflegen kann. Zudem führen technische Konvergenzeffekte dazu, dass auch herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können (vgl. etwa zur Sprachtelefonie Katko, CR 2005, S. 189).

cc) Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.

(1) Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (vgl. zu den aus solchen Folgerungen entstehenden Persönlichkeitsgefährdungen BVerfGE 65, 1 <42>).

(2) Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten der Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.

Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des

geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten - etwa die Verschlüsselung oder die Verschleierung sensibler Daten - werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.

c) Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.

aa) Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl.BVerfGE 67, 157 <172>; 106, 28 <35 f.>), nicht aber auch die Vertraulichkeit und Integrität von informationstechnischen Systemen.

(1) Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden (vgl.BVerfGE 106, 28 <36>; 115, 166 <182>). Der Schutzbereich des Telekommunikationsgeheimnisses erstreckt sich danach auch auf die Kommunikationsdienste des Internet (vgl. zu E-Mails BVerfGE 113, 348 <383>). Zudem sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl.BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 f.>). Das Telekommunikationsgeheimnis begegnet in diesem Rahmen alten sowie neuen Persönlichkeitsgefährdungen, die sich aus der gestiegenen Bedeutung der Informationstechnik für die Entfaltung des Einzelnen ergeben.

Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf

der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt (vgl.BVerfGE 106, 28 <37 f.>; 115, 166 <186 f.>). Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt.

(2) Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich allerdings nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort (vgl.BVerfGE 115, 166 <183 ff.>).

(3) Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist (vgl. Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 497; Rux, JZ 2007, S. 285 <292>).

(4) Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist.

Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung“), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder - soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert - das Verhalten in der eigenen Wohnung.

Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen - anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung - stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden.

Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung“, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.

bb) Auch die durch Art. 13 Abs. 1 GG gewährleistete Garantie der Unverletzlichkeit der Wohnung verbürgt dem Einzelnen mit Blick auf seine Menschenwürde sowie im Interesse der Entfaltung seiner Persönlichkeit einen elementaren Lebensraum, in den nur unter den besonderen Voraussetzungen von Art. 13 Abs. 2 bis 7 GG eingegriffen werden darf, belässt aber Schutzlücken gegenüber Zugriffen auf informationstechnische Systeme.

Das Schutzgut dieses Grundrechts ist die räumliche Sphäre, in der sich das Privatleben entfaltet (vgl. BVerfGE 89, 1 <12>; 103, 142 <150 f.>). Neben Privatwohnungen fallen auch Betriebs- und Geschäftsräume in den Schutzbereich des Art. 13 GG (vgl. BVerfGE 32, 54 <69 ff.>; 44, 353 <371>; 76, 83 <88>; 96, 44 <51>). Dabei erschöpft sich der Grundrechtsschutz nicht in der Abwehr eines körperlichen Eindringens in die Wohnung. Als Eingriff in Art. 13 GG sind auch Maßnahmen anzusehen, durch die staatliche Stellen sich mit besonderen Hilfsmitteln einen Einblick in Vorgänge innerhalb der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind. Dazu gehören nicht nur die akustische oder optische Wohnraumüberwachung (vgl.BVerfGE 109, 279 <309, 327>), sondern ebenfalls etwa die Messung elektromagnetischer Abstrahlungen, mit der die Nutzung eines informationstechnischen Systems in der Wohnung überwacht werden kann. Das kann auch ein System betreffen, das offline arbeitet.

Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen

bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden.

Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet (vgl. etwa Beulke/Meininghaus, StV 2007, S. 63 <64>; Gercke, CR 2007, S. 245 <250>; Schlegel, GA 2007, S. 648 <654 ff.>; a.A. etwa Buermeyer, HRRS 2007, S. 392 <395 ff.>; Rux, JZ 2007, S. 285 <292 ff.>; Schaar/Landwehr, K&R 2007, S. 202 <204>). Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone.

Art. 13 Abs. 1 GG schützt zudem nicht gegen die durch die Infiltration des Systems ermöglichte Erhebung von Daten, die sich im Arbeitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht (vgl. zum gleichläufigen Verhältnis von Wohnungsdurchsuchung und BeschlagnahmeBVerfGE 113, 29 <45>).

cc) Auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts, insbesondere die Gewährleistungen des Schutzes der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, genügen dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems nicht in ausreichendem Maße.

(1) In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll (vgl.BVerfGE 27, 344 <350 ff.>; 44, 353 <372 f.>; 90, 255 <260>; 101, 361 <382 f.>). Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der

Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.

(2) Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl.BVerfGE 65, 1 <43>; 84, 192 <194>). Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann. Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2466>).

Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Oktober 2006 - 1 BvR 2027/02 -, JZ 2007, S. 576) zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können (vgl.BVerfGE 65, 1 <42>; 113, 29 <45 f.>; 115, 320 <342>; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2466>).

Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Per-

sönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.

d) Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

aa) Allerdings bedarf nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält - zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik - , unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können.

bb) Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

(1) Das allgemeine Persönlichkeitsrecht in der hier behandelten Ausprägung schützt insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können. Der Grundrechtsschutz umfasst sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten. Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa bei einem Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur.

(2) Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.

2. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein. Der Einzelne muss dabei nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Hinsichtlich der vorliegend zu überprüfenden Ermächtigung der Verfassungsschutzbehörde, präventive Maßnahmen vorzunehmen, fehlt es daran.

a) Die angegriffene Norm wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht.

aa) Das Bestimmtheitsgebot findet auch im Hinblick auf das allgemeine Persönlichkeitsrecht in seinen verschiedenen Ausprägungen seine Grundlage im Rechtsstaatsprinzip (Art. 20, Art. 28 Abs. 1 GG; vgl.BVerfGE 110, 33 <53, 57, 70>; 112, 284 <301>; 113, 348 <375>; 115, 320 <365>). Es soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann (vgl.BVerfGE 110, 33 <52 ff.>; 113, 348 <375 ff.>). Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen (vgl.BVerfGE 100, 313 <359 f., 372>; 110, 33 <53>; 113, 348 <375>; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2466>).

Je nach der zu erfüllenden Aufgabe findet der Gesetzgeber unterschiedliche Möglichkeiten zur Regelung der Eingriffsvoraussetzungen vor. Die Anforderungen des Bestimmtheitsgrundsatzes richten sich auch nach diesen Regelungsmöglichkeiten (vgl.BVerfGE 110, 33 <55 f.> ; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2467>). Bedient sich der Gesetzgeber unbestimmter Rechtsbegriffe, dürfen verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justitiabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind (vgl.BVerfGE 21, 73 <79 f.>; 31, 255 <264>; 83, 130 <145>; 102, 254 <337>; 110, 33 <56 f.>; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2467>).

bb) Nach diesen Maßstäben genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG dem Gebot der Normenklarheit und Normenbestimmtheit insoweit nicht, als sich die tatbestandlichen Voraussetzungen der geregelten Maßnahmen dem Gesetz nicht hinreichend entnehmen lassen.

(1) Die Voraussetzungen für Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG können über zwei Normverweisungen zu bestimmen sein. Zum einen verweist § 5 Abs. 2 VSG allgemein auf § 7 Abs. 1 VSG, der seinerseits § 3 Abs. 1 VSG in Bezug nimmt. Danach ist ein Einsatz nachrichtendienstlicher Mittel zulässig, wenn auf diese Weise verfassungsschutzrelevante Erkenntnisse gewonnen werden können. Zum anderen verweist § 5 Abs. 2 Nr. 11 Satz 2 VSG für den Fall, dass eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG in das Brief-, Post- oder Fernmeldegeheimnis eingreift oder einem solchen Eingriff nach Art und Schwere gleichkommt, auf die strengeren Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz.

(2) Mit dem Gebot der Normenklarheit und Normenbestimmtheit ist nicht vereinbar, dass § 5 Abs. 2 Nr. 11 Satz 2 VSG für die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz darauf abstellt,

ob eine Maßnahme in Art. 10 GG eingreift. Die Antwort auf die Frage, in welche Grundrechte Ermittlungsmaßnahmen der Verfassungsschutzbehörde eingreifen, kann komplexe Abschätzungen und Bewertungen erfordern. Zu ihnen ist zunächst und vorrangig der Gesetzgeber berufen. Seiner Aufgabe, die einschlägigen Grundrechte durch entsprechende gesetzliche Vorkehrungen zu konkretisieren, kann er sich nicht entziehen, indem er durch eine bloße tatbestandliche Bezugnahme auf ein möglicherweise einschlägiges Grundrecht die Entscheidung darüber, wie dieses Grundrecht auszufüllen und umzusetzen ist, an die normvollziehende Verwaltung weiterreicht. Eine derartige „salvatorische“ Regelungstechnik genügt dem Bestimmtheitsgebot nicht bei einer Norm wie § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, die neuartige Ermittlungsmaßnahmen vorsieht, welche auf neuere technologische Entwicklungen reagieren sollen.

Der Verstoß gegen das Gebot der Normenklarheit wird noch vertieft durch den in § 5 Abs. 2 Nr. 11 Satz 2 VSG enthaltenen Zusatz, die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz greife auch dann, wenn eine Ermittlungsmaßnahme einem Eingriff in Art. 10 GG „in Art und Schwere“ gleichkommt. Damit werden die tatbestandlichen Voraussetzungen des geregelten Zugriffs von einem wertenden Vergleich zwischen diesem Zugriff und einer Maßnahme, die als Eingriff in ein bestimmtes Grundrecht anzusehen wäre, abhängig gemacht. Für diesen Vergleich enthält § 5 Abs. 2 Nr. 11 Satz 2 VSG keinerlei Maßstäbe. Wenn schon durch die bloße Verweisung auf ein bestimmtes Grundrecht die Tatbestandsvoraussetzungen nicht hinreichend bestimmt geregelt werden können, so gilt dies erst recht für eine Norm, die einen derartigen, normativ nicht weiter angeleiteten Vergleich der geregelten Maßnahme mit einem Eingriff in ein bestimmtes Grundrecht Vorsieht.

(3) Die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz in § 5 Abs. 2 Nr. 11 Satz 2 VSG genügt dem Gebot der Normenklarheit und Normenbestimmtheit auch insoweit nicht, als die Reichweite der Verweisung nicht hinreichend bestimmt geregelt ist.

§ 5 Abs. 2 Nr. 11 Satz 2 VSG verweist auf die „Voraussetzungen“ des Gesetzes zu Artikel 10 Grundgesetz. Die Norm lässt damit weitgehend im Unklaren, auf welche Teile des Gesetzes zu Artikel 10 Grundgesetz verwiesen werden soll. Ihr lässt sich nicht entnehmen, ob unter den Voraussetzungen dieses Gesetzes nur die in § 3 G 10 geregelte materielle Eingriffsschwelle zu verstehen ist oder ob auch weitere Vorschriften in Bezug genommen werden sollen. So könnten auch die Verfahrensregelungen der §§ 9 ff. G 10 zu den Voraussetzungen eines Eingriffs nach diesem Gesetz gezählt werden. Zumindest denkbar wäre sogar, die Verweisung noch weitergehend auf sowohl die materiellen Eingriffsschwellen als auch sämtliche Verfahrensvorkehrungen des Gesetzes zu Artikel 10 Grundgesetz zu beziehen, wie dies die nordrhein-westfälische Landesregierung vorschlägt. Danach wären auch die in § 4 G 10 enthaltenen Regelungen über den Umgang mit erhobenen Daten und die Normen der §§ 14 ff. G 10 über die parlamentarische Kontrolle erfasst,

obwohl diese Normen Regelungen enthalten, die erst nach einem Eingriff zu beachten sind und daher sprachlich kaum zu den Eingriffsvoraussetzungen gezählt werden können.

Es ist nicht ersichtlich, dass die unbestimmte Fassung des Gesetzes besonderen Regelungsschwierigkeiten geschuldet wäre. Dem Gesetzgeber wäre ohne weiteres möglich gewesen, in der Verweisungsnorm einzelne Vorschriften des Gesetzes zu Artikel 10 Grundgesetz aufzuzählen, auf die verwiesen werden soll.

b) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt auch nicht den Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl.BVerfGE 109, 279 <335 ff.>; 115, 320 <345>; BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2468>; stRspr).

aa) Die in der angegriffenen Norm vorgesehenen Datenerhebungen dienen der Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben nach § 3 Abs. 1 VSG und damit der im Vorfeld konkreter Gefahren einsetzenden Sicherung der freiheitlichen demokratischen Grundordnung, des Bestandes von Bund und Ländern sowie bestimmter auf das Verhältnis zum Ausland gerichteter Interessen der Bundesrepublik. Dabei wurde mit der Novellierung des Verfassungsschutzgesetzes nach der Gesetzesbegründung insbesondere auch das Ziel verfolgt, eine effektive Terrorismusbekämpfung durch die Verfassungsschutzbehörde angesichts neuer, insbesondere mit der Internetkommunikation verbundener, Gefährdungen sicherzustellen (vgl. LTDrucks 14/2211, S. 1). Allerdings ist der Anwendungsbereich der Neuregelung weder ausdrücklich noch als Folge des systematischen Zusammenhangs auf die Terrorismusbekämpfung begrenzt. Die Norm bedarf einer Rechtfertigung für ihr gesamtes Anwendungsfeld.

Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen (vgl.BVerfGE 49, 24 <56 f.>; 115, 320 <346>). Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG (vgl. BVerfGE 115, 118 <152>). Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschlie-

ßen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen (vgl. zur StrafverfolgungBVerfGE 115, 166 <193>).

bb) Der heimliche Zugriff auf informationstechnische Systeme ist geeignet, diesen Zielen zu dienen. Mit ihm werden die Möglichkeiten der Verfassungsschutzbehörde zur Aufklärung von Bedrohungslagen erweitert. Bei der Beurteilung der Eignung ist dem Gesetzgeber ein beträchtlicher Einschätzungsspielraum eingeräumt (vgl.BVerfGE 77, 84 <106>; 90, 145 <173>; 109, 279 <336>). Es ist nicht ersichtlich, dass dieser Spielraum hier überschritten wurde.

Die in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG enthaltene Befugnis verliert nicht dadurch ihre Eignung, dass der Betroffene nach einer in der Literatur vertretenen (vgl. etwa Buermeyer, HRRS 2007, S. 154 <165 f.>; Gercke, CR 2007, S. 245 <253>; Hornung, DuD 2007, S. 575 <579>) und von den in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen geteilten Einschätzung technische Selbstschutzmöglichkeiten hat, um jedenfalls einen Zugriff wirkungsvoll zu verhindern, bei dem die Infiltration des Zielsystems mit Hilfe einer Zugriffssoftware durchgeführt wird. Im Rahmen der Eignungsprüfung ist nicht zu fordern, dass Maßnahmen, welche die angegriffene Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen. Die gesetzgeberische Prognose, dass Zugriffe der geregelten Art im Einzelfall Erfolg haben können, ist zumindest nicht offensichtlich fehlsam. Es kann nicht als selbstverständlich unterstellt werden, dass jede mögliche Zielperson eines Zugriffs bestehende Schutzmöglichkeiten dagegen nutzt und tatsächlich fehlerfrei implementiert. Im Übrigen erscheint denkbar, dass sich im Zuge der weiteren informationstechnischen Entwicklung für die Verfassungsschutzbehörde Zugriffsmöglichkeiten auftun, die sich technisch nicht mehr oder doch nur mit unverhältnismäßigem Aufwand unterbinden lassen.

Weiter ist die Eignung der geregelten Befugnis auch nicht deshalb zu verneinen, weil möglicherweise der Beweiswert der Erkenntnisse, die mittels des Zugriffs gewonnen werden, begrenzt ist. Insoweit wird vorgebracht, eine technische Echtheitsbestätigung der erhobenen Daten setze grundsätzlich eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus (vgl. Hansen/Pfitzmann, DRiZ 2007, S. 225 <228>). Jedoch bewirken diese Schwierigkeiten der Beweissicherung nicht, dass den erhobenen Daten kein Informationswert zukommt. Zudem dient der Online-Zugriff nach der angegriffenen Norm nicht unmittelbar der Gewinnung revisionsfester Beweise für ein Strafverfahren, sondern soll der Verfassungsschutzbehörde Kenntnisse verschaffen, an deren Zuverlässigkeit wegen der andersartigen Aufgabenstellung des Verfassungsschutzes zur Prävention im Vorfeld konkreter Gefahren geringere Anforderungen zu stellen sind als in einem Strafverfahren.

cc) Der heimliche Zugriff auf informationstechnische Systeme verletzt auch den Grundsatz der Erforderlichkeit nicht. Im Rahmen seiner Einschätzungsprärogative durfte der Gesetzgeber annehmen, dass kein ebenso wirksamer, aber den Betroffenen weniger belastender Weg gegeben ist, die auf solchen Systemen vorhandenen Daten zu erheben.

Grundsätzlich ist zwar eine - im Verfassungsschutzgesetz nicht vorgesehene – offene Durchsuchung des Zielsystems gegenüber dem heimlichen Zugriff als milderes Mittel anzusehen (vgl. Hornung, DuD 2007, S. 575 <580>). Hat die Verfassungsschutzbehörde jedoch im Rahmen ihrer Aufgabenstellung einen hinreichenden Grund, die auf den Speichermedien eines informationstechnischen Systems abgelegten Dateien umfassend - unter Einschluss verschlüsselter Daten - zu sichten, über einen längeren Zeitraum Änderungen zu verfolgen oder die Nutzung des Systems umfassend zu überwachen, so sind mildere Mittel, diese Erkenntnisziele zu erreichen, nicht ersichtlich. Gleiches gilt für den Zugriff auf verschlüsselte Inhalte der Internetkommunikation, soweit ein Zugriff auf der Übertragungsstrecke nicht erfolgversprechend ist.

dd) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG wahrt jedoch nicht das Gebot der Verhältnismäßigkeit im engeren Sinne. Dieses Gebot verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (vgl.BVerfGE 90, 145 <173>; 109, 279 <349 ff.>; 113, 348 <382> ; stRspr). Der Gesetzgeber hat das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann dazu führen, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange (vgl.BVerfGE 115, 320 <345 f.>; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. - , NJW 2007, S. 2464 <2469>).

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt dem nicht. Die in dieser Norm vorgesehenen Maßnahmen bewirken derart intensive Grundrechtseingriffe, dass sie zu dem öffentlichen Ermittlungsinteresse, das sich aus dem geregelten Eingriffsanlass ergibt, außer Verhältnis stehen. Zudem bedarf es ergänzender verfahrensrechtlicher Vorgaben, um den grundrechtlich geschützten Interessen des Betroffenen Rechnung zu tragen; auch an ihnen fehlt es.

(1) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Grundrechtseingriffen von hoher Intensität.

(a) Eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen weist ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen auf. Dies gilt bereits für einmalige und punktuelle Zugriffe wie beispielsweise die Beschlagnahme oder Kopie von

Speichermedien solcher Systeme (vgl. zu solchen Fallgestaltungen etwa BVerfGE 113, 29; 115, 166; 117, 244).

(aa) Ein solcher heimlicher Zugriff auf ein informationstechnisches System öffnet der handelnden staatlichen Stelle den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. Dies liegt an der Vielzahl unterschiedlicher Nutzungsmöglichkeiten, die komplexe informationstechnische Systeme bieten und die mit der Erzeugung, Verarbeitung und Speicherung von personenbezogenen Daten verbunden sind. Insbesondere werden solche Geräte nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt. Der verfügbare Datenbestand kann detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen.

Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.

(bb) Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die - auch im Allgemeinwohl liegende - Möglichkeit der Bürger beschränkt wird, an einer unbeobachteten Fernkommunikation teilzunehmen (vgl. zur Erhebung von VerbindungsdatenBVerfGE 115, 166 <187 ff.>). Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann. Zudem weisen solche Datenerhebungen insoweit eine beträchtliche, das Gewicht des Eingriffs erhöhende Streubreite auf, als mit den Kommunikationspartnern der Zielperson notwendigerweise Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <382 f.>; ferner BVerfGE 34, 238 <247>; 107, 299 <321>).

(b) Das Gewicht des Grundrechtseingriffs ist von besonderer Schwere, wenn - wie dies die angegriffene Norm vorsieht - eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.

(aa) Umfang und Vielfältigkeit des Datenbestands, der durch einen derartigen Zugriff erlangt werden kann, sind noch erheblich größer als bei einer einmaligen und punktuellen Datenerhebung.

Der Zugriff macht auch lediglich im Arbeitsspeicher gehaltene flüchtige oder nur temporär auf den Speichermedien des Zielsystems abgelegte Daten für die Ermittlungsbehörde verfügbar. Er ermöglicht zudem, die gesamte Internetkommunikation des Betroffenen über einen längeren Zeitraum mitzuverfolgen. Im Übrigen kann sich die Streubreite der Ermittlungsmaßnahme erhöhen, wenn das Zielsystem in ein (lokales) Netzwerk eingebunden ist, auf das der Zugriff erstreckt wird.

Flüchtige oder nur temporär gespeicherte Daten können eine besondere Relevanz für die Persönlichkeit des Betroffenen aufweisen oder einen Zugriff auf weitere, besonders sensible Daten ermöglichen. Dies gilt etwa für Cache-Speicher, die von Dienstprogrammen wie etwa Web-Browsern angelegt werden und deren Auswertung Schlüsse über die Nutzung solcher Programme und damit mittelbar über Vorlieben oder Kommunikationsgewohnheiten des Betroffenen ermöglichen kann, oder für Passwörter, mit denen der Betroffene Zugang zu technisch gesicherten Inhalten auf seinem System oder im Netz erlangt. Zudem ist eine längerfristige Überwachung der Internetkommunikation, wie sie die angegriffene Norm ermöglicht, gegenüber einer einmaligen Erhebung von Kommunikationsinhalten und Kommunikationsumständen gleichfalls ein erheblich intensiverer Eingriff. Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs.

Auch das Risiko einer Bildung von Verhaltens- und Kommunikationsprofilen erhöht sich durch die Möglichkeit, über einen längeren Zeitraum die Nutzung des Zielsystems umfassend zu überwachen. Die Behörde kann auf diese Weise die persönlichen Verhältnisse und das Kommunikationsverhalten des Betroffenen weitgehend ausforschen. Eine solche umfassende Erhebung persönlicher Daten ist als Grundrechtseingriff von besonders hoher Intensität anzusehen.

(bb) Die Eingriffsintensität des geregelten Zugriffs wird weiter durch dessen Heimlichkeit bestimmt. In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2469 f.>). Erfährt der Betroffene von einer ihn belastenden staatlichen Maßnahme vor ihrer Durchführung, kann er von vornherein seine Interessen wahrnehmen. Er kann zum einen rechtlich gegen sie vorgehen, etwa gerichtlichen Rechtsschutz in Anspruch nehmen. Zum anderen hat er bei einer offen durchgeführten Datenerhebung faktisch die Möglichkeit, durch sein Verhalten auf den Gang der Ermittlung einzuwirken. Der Ausschluss dieser Einflusschance verstärkt das Gewicht des Grundrechtseingriffs (vgl. zu rechtlichen AbwehrmöglichkeitenBVerfGE 113, 348 <383 f.>; 115, 320 <353>).

(cc) Das Gewicht des Eingriffs wird schließlich dadurch geprägt, dass infolge des Zugriffs Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch Dritter begründet werden.

Die in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen haben ausgeführt, es könne nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht. So könnten Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen (vgl. auch Hansen/Pfitzmann, DRiZ 2007, S. 225 <228>). Zudem ist zu beachten, dass es einen rein lesenden Zugriff infolge der Infiltration nicht gibt. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können aufgrund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen. Dies kann den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen.

Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.

(2) Der Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, entspricht im Rahmen einer präventiven Zielsetzung angesichts seiner Intensität nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.

(a) In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte gehört es zur Aufgabe des Gesetzgebers, in abstrakter Weise einen Ausgleich der widerstreitenden Interes-

sen zu erreichen (vgl.BVerfGE 109, 279 <350>). Dies kann dazu führen, dass bestimmte intensive Grundrechtseingriffe nur zum Schutz bestimmter Rechtsgüter und erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen. In dem Verbot unangemessener Grundrechtseingriffe finden auch die Pflichten des Staates zum Schutz anderer Rechtsgüter ihre Grenze (vgl.BVerfGE 115, 320 <358>). Entsprechende Eingriffsschwellen sind durch eine gesetzliche Regelung zu gewährleisten (vgl. BVerfGE 100, 313 <383 f.>; 109, 279 <350 ff.>; 115, 320 <346>).

(b) Ein Grundrechtseingriff von hoher Intensität kann bereits als solcher unverhältnismäßig sein, wenn der gesetzlich geregelte Eingriffsanlass kein hinreichendes Gewicht aufweist. Soweit das einschlägige Gesetz der Abwehr bestimmter Gefahren dient, wie sich dies für das Verfassungsschutzgesetz aus § 1 VSG ergibt, kommt es für das Gewicht des Eingriffsanlasses maßgeblich auf den Rang und die Art der Gefährdung der Schutzgüter an, die in der jeweiligen Regelung in Bezug genommen werden (vgl.BVerfGE 115, 320 <360 f.>).

Wiegen die Schutzgüter einer Eingriffsermächtigung als solche hinreichend schwer, um Grundrechtseingriffe der geregelten Art zu rechtfertigen, begründet der Verhältnismäßigkeitsgrundsatz verfassungsrechtliche Anforderungen an die tatsächlichen Voraussetzungen des Eingriffs. Der Gesetzgeber hat insoweit die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits zu wahren (vgl.BVerfGE 100, 313 <392 ff.>). Die Anforderungen an den Wahrscheinlichkeitsgrad und die Tatsachenbasis der Prognose müssen in angemessenem Verhältnis zur Art und Schwere der Grundrechtsbeeinträchtigung stehen. Selbst bei höchstem Gewicht der drohenden Rechtsgutsbeeinträchtigung kann auf das Erfordernis einer hinreichenden Eintrittswahrscheinlichkeit nicht verzichtet werden. Auch muss als Voraussetzung eines schweren Grundrechtseingriffs gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen besitzen (vgl.BVerfGE 113, 348 <386>; 115, 320 <360 f.>).

(c) Der Verhältnismäßigkeitsgrundsatz setzt einer gesetzlichen Regelung, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, zunächst insoweit Grenzen, als besondere Anforderungen an den Eingriffsanlass bestehen. Dieser besteht hier in der Gefahrenprävention im Rahmen der Aufgaben der Verfassungsschutzbehörde gemäß § 1 VSG.

(aa) Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu

zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.

Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die - wie hier - die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.

(bb) Die gesetzliche Ermächtigungsgrundlage muss weiter als Voraussetzung des heimlichen Zugriffs vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter der Norm bestehen.

() Das Erfordernis tatsächlicher Anhaltspunkte führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze allein nicht ausreichen, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die eine Gefahrenprognose tragen (vgl.BVerfGE 110, 33 <61>; 113, 348 <378>).

Diese Prognose muss auf die Entstehung einer konkreten Gefahr bezogen sein. Dies ist eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird. Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher. Der hier zu beurteilende Zugriff auf das informationstechnische System kann allerdings schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird. Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur ein durch relativ diffuse Anhaltspunkte für mögliche Gefahren gekennzeichnetes Geschehen bekannt

ist. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet (vgl. zur Straftatenverhütung BVerfGE 110, 33 <59>).

() Die verfassungsrechtlichen Anforderungen an die Regelung des tatsächlichen Eingriffsanlasses sind im Fall des heimlichen Zugriffs auf ein informationstechnisches System für alle Eingriffsermächtigungen mit präventiver Zielsetzung zu beachten. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die Gleiche ist, besteht hinsichtlich seiner Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden. Dass Polizei- und Verfassungsschutzbehörden unterschiedliche Aufgaben und Befugnisse haben und in der Folge Maßnahmen mit unterschiedlicher Eingriffstiefe vornehmen können, ist für die Gewichtung des heimlichen Zugriffs auf das informationstechnische System grundsätzlich ohne Belang.

Zwar können Differenzierungen zwischen den Ermächtigungen der verschiedenen Behörden mit präventiven Aufgaben vor der Verfassung Bestand haben. So rechtfertigen die besonderen Zwecke im Bereich der strategischen Telekommunikationsüberwachung durch den Bundesnachrichtendienst, dass die Eingriffsvoraussetzungen anders bestimmt werden als im Polizei- oder Strafprozessrecht (vgl.BVerfGE 100, 313 <383>). Auch können die Einschreitvoraussetzungen für Ermittlungsmaßnahmen unterschiedlich gestaltet werden, je nachdem welche Behörde mit welcher Zielsetzung handelt. Auf diese Weise kann etwa der besonderen Aufgabenstellung der Verfassungsschutzbehörden zur Aufklärung verfassungsfeindlicher Bestrebungen im Vorfeld konkreter Gefahren Rechnung getragen werden (vgl. allgemein zum Problem adäquater Ermittlungsregelungen im Vorfeldbereich Möstl, DVBl 2007, S. 581; Volkmann, JZ 2006, S. 918). So ist es grundsätzlich verfassungsrechtlich nicht zu beanstanden, dass die Verfassungsschutzbehörden nachrichtendienstliche Mittel auch einsetzen dürfen, um Erkenntnisse über Gruppierungen zu erlangen, die die Schutzgüter des Verfassungsschutzgesetzes - zumindest noch – auf dem Boden der Legalität bekämpfen. Auch ist für den Einsatz solcher Mittel nicht generell zu fordern, dass über die stets erforderlichen tatsächlichen Anhaltspunkte für derartige Bestrebungen (vgl. etwa § 7 Abs. 1 Nr. 1 i.V.m. § 3 Abs. 1 VSG) hinaus konkrete Verdachtsmomente bestehen.

Jedoch ist der Gesetzgeber auch bei der Regelung der einzelnen Befugnisse von Sicherheitsbehörden, deren Aufgabe in der Vorfeldaufklärung besteht, an die verfassungsrechtlichen Vorgaben gebunden, die sich aus dem Verhältnismäßigkeitsgrundsatz ergeben. Dies kann dazu führen, dass auch solche Behörden zu bestimmten intensiven Grundrechtseingriffen nur dann ermächtigt werden dürfen, wenn erhöhte Anforderungen an die Regelung des Eingriffsanlasses gewahrt sind. So liegt es insbesondere bei dem heimlichen Zugriff auf ein informationstechnisches System, der un-

abhängig von der handelnden Behörde das Risiko birgt, dass der Betroffene für eine weitgehende staatliche Ausspähung seiner Persönlichkeit verfügbar gemacht wird. Auch wenn es nicht gelingen sollte, speziell auf im Vorfeld tätige Behörden zugeschnittene gesetzliche Maßgaben für den Eingriffsanlass zu entwickeln, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen wie es der überkommene Gefahrenbegriff etwa im Polizeirecht leistet, wäre dies kein verfassungsrechtlich hinnehmbarer Anlass, die tatsächlichen Voraussetzungen für einen Eingriff der hier vorliegenden Art abzumildern.

(d) Weiter muss eine Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme mit geeigneten gesetzlichen Vorkehrungen verbunden werden, um die Interessen des Betroffenen verfahrensrechtlich abzusichern. 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 (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2471>, m.w.N.). Insbesondere ist der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.

(aa) Ein solcher Vorbehalt ermöglicht die vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz. Eine derartige Kontrolle kann bedeutsames Element eines effektiven Grundrechtsschutzes sein. Sie ist zwar nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden (vgl.BVerfGE 110, 33 <67 f.>). Sie kann aber gewährleisten, dass die Entscheidung über eine heimliche Ermittlungsmaßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn der Betroffene selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann. Die Kontrolle dient insoweit der „kompensatorischen Repräsentation“ der Interessen des Betroffenen im Verwaltungsverfahren (vgl. SächsVerfGH, Urteil vom 14. Mai 1996 - Vf.44-II-94 -, JZ 1996, S. 957 <964>).

(bb) Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, grundsätzlich ein Regelungsspielraum eingeräumt. 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. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Be-

troffenen im Einzelfall am besten und sichersten wahren (vgl.BVerfGE 103, 142 <151>; 107, 299 <325>). Vorausgesetzt ist allerdings, dass sie die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten (zu den Anforderungen an die Anordnung einer akustischen Wohnraumüberwachung vgl. BVerfGE 109, 279 <358 ff.>; zur Kritik an der Praxis der Ausübung des Richtervorbehalts bei Wohnungsdurchsuchungen vgl. BVerfGE 103, 142 <152>, m.w.N.).

Der Gesetzgeber darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter. Auch von ihr muss eine Begründung zur Rechtmäßigkeit gegeben werden.

Von dem Erfordernis einer vorherigen Kontrolle der Maßnahme durch eine dafür geeignete neutrale Stelle darf eine Ausnahme für Eilfälle, etwa bei Gefahr im Verzug, vorgesehen werden, wenn für eine anschließende Überprüfung durch die neutrale Stelle gesorgt ist. Für die tatsächlichen und rechtlichen Voraussetzungen der Annahme eines Eilfalls bestehen dabei indes wiederum verfassungsrechtliche Vorgaben (vgl.BVerfGE 103, 142 <153 ff.> zu Art. 13 Abs. 2 GG).

(3) Nach diesen Maßstäben genügt die angegriffene Norm nicht den verfassungsrechtlichen Anforderungen.

(a) Nach § 5 Abs. 2 in Verbindung mit § 7 Abs. 1 Nr. 1 und § 3 Abs. 1 VSG sind Voraussetzung für den Einsatz nachrichtendienstlicher Mittel durch die Verfassungsschutzbehörde lediglich tatsächliche Anhaltspunkte für die Annahme, dass auf diese Weise Erkenntnisse über verfassungsfeindliche Bestrebungen gewonnen werden können. Dies ist sowohl hinsichtlich der tatsächlichen Voraussetzungen für den Eingriff als auch des Gewichts der zu schützenden Rechtsgüter keine hinreichende materielle Eingriffsschwelle. Auch ist eine vorherige Prüfung durch eine unabhängige Stelle nicht vorgesehen, so dass die verfassungsrechtlich geforderte verfahrensrechtliche Sicherung fehlt.

(b) Diese Mängel entfallen nicht, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG auf die näheren Voraussetzungen nach dem Gesetz zu Artikel 10 Grundgesetz trotz ihrer Unbestimmtheit in die Prüfung einbezogen und in der weiten Interpretation der nordrheinwestfälischen Landesregierung so verstanden wird, dass sie sich auf sämtliche formellen und materiellen Vorkehrungen dieses Gesetzes bezieht. § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG beschränkt den heimlichen Zugriff auf ein informationstechnisches System nicht auf eine Telekommunikationsüberwachung, deren Voraussetzungen § 3 Abs. 1 G 10 regelt, sondern ermöglicht derartige Zugriffe grundsätzlich zur Gewinnung aller verfügbaren Daten.

Weder die Regelung der Eingriffsschwelle noch die verfahrensrechtlichen Vorgaben in den in § 3 Abs. 1 G 10 vorgesehenen Eingriffstatbeständen genügen den verfassungsrechtlichen Anforderungen.

(aa) Nach § 3 Abs. 1 Satz 1 G 10 ist eine Überwachungsmaßnahme zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat aus einem in der Norm geregelten Katalog plant, begeht oder begangen hat. Der Straftatenkatalog lässt zum einen kein Konzept erkennen, nach dem es gerechtfertigt sein könnte, sämtliche dort aufgeführten Straftaten zum Anlass von Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG zu nehmen. So ist nicht bei allen in Bezug genommenen Normen gesichert, dass der Zugriff im konkreten Fall der Abwehr eines der oben (C I 2 b, dd <2> <c> <aa>) aufgeführten überragend wichtigen Rechtsgüter dient. Zum andern stellt die Verweisung auf § 3 Abs. 1 Satz 1 G 10 nicht in jedem Fall sicher, dass der heimliche Zugriff auf ein informationstechnisches System nur erfolgt, wenn solche Rechtsgüter im Einzelfall mit hinreichender Wahrscheinlichkeit (C I 2 b, dd <2> <c> <bb>) in näherer Zukunft gefährdet sind.

Gemäß § 3 Abs. 1 Satz 2 G 10 kann eine Überwachungsmaßnahme auch angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die sich gegen die Schutzgüter des Verfassungsschutzes richten. Die Straftaten werden allerdings nur allgemein umschrieben, so dass das Risiko einer ausweitenden Auslegung naheliegt, die einen Eingriff auch zum Schutz von Rechtsgütern ermöglichen würde, die nicht überragend wichtig sind. Zudem müssten nach dieser Vorschrift nicht in jedem Fall, in dem der Eingriffstatbestand des § 3 Abs. 1 Satz 2 G 10 verwirklicht ist, hinreichende tatsächliche Anhaltspunkte für eine im Einzelfall von dieser Person oder der Vereinigung drohende Gefahr für ein überragend wichtiges Rechtsgut vorliegen.

(bb) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG genügt weiter selbst dann, wenn die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz einbezogen wird, nicht den verfassungsrechtlichen Anforderungen an die vorbeugende Kontrolle eines heimlichen Zugriffs auf ein informationstechnisches System.

§ 10 G 10 sieht eine vorherige Anordnung der Überwachungsmaßnahme vor, die auf Antrag der Verfassungsschutzbehörde von der zuständigen obersten Landesbehörde erteilt wird. Dieses Verfahren reicht nicht aus, um die von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geforderte vorbeugende Kontrolle sicherzustellen. Das Gesetz regelt weder einen Richtervorbehalt noch - da die in § 3 Abs. 6 AG G 10 NRW enthaltene Regelung einer vorbeugenden Kontrolle durch die G 10-Kommission nicht von dem Verweis erfasst ist - einen gleichwertigen Kontrollmechanismus. Die

zuständige oberste Landesbehörde kann, anders als ein Gericht, aufgrund ihres Ressortzuschnitts ein eigenes Interesse an der Durchführung nachrichtendienstlicher Maßnahmen des Verfassungsschutzes haben. Sie bietet keine vergleichbare Gewähr für die Unabhängigkeit und Neutralität einer Kontrolle wie ein Gericht.

c) Schließlich fehlt es an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung durch Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG zu vermeiden.

aa) Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt (vgl.BVerfGE 6, 32 <41>; 27, 1 <6>; 32, 373 <378 f.>; 34, 238 <245>; 80, 367 <373>; 109, 279 <313>; 113, 348 <390>). Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in ihn nicht rechtfertigen (vgl. BVerfGE 34, 238 <245>; 109, 279 <313>). Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen (vgl.BVerfGE 109, 279 <314>).

Im Rahmen eines heimlichen Zugriffs auf ein informationstechnisches System besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind. So kann der Betroffene das System dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente, anzulegen und zu speichern. Derartige Dateien können ebenso wie etwa schriftliche Verkörperungen des höchstpersönlichen Erlebens (dazu vgl.BVerfGE 80, 367 <373 ff.>; 109, 279 <319>) einen absoluten Schutz genießen. Zum anderen kann das System, soweit es telekommunikativen Zwecken dient, zur Übermittlung von Inhalten genutzt werden, die gleichfalls dem Kernbereich unterfallen können. Dies gilt nicht nur für Sprachtelefonate, sondern auch etwa für die Fernkommunikation mittels E-Mails oder anderer Kommunikationsdienste des Internet (vgl.BVerfGE 113, 348 <390>). Die absolut geschützten Daten können bei unterschiedlichen Arten von Zugriffen erhoben werden, etwa bei der Durchsicht von Speichermedien ebenso wie bei der Überwachung der laufenden Internetkommunikation oder gar einer Vollüberwachung der Nutzung des Zielsystems.

bb) Soll heimlich auf das informationstechnische System des Betroffenen zugegriffen werden, bedarf es besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen.

Die Bürger nutzen zur Verwaltung ihrer persönlichen Angelegenheiten und zur Telekommunikation auch mit engen Bezugspersonen zunehmend komplexe informationstechnische Systeme, die ihnen Entfaltungsmöglichkeiten im höchstpersönlichen Bereich bieten. Angesichts dessen schafft eine Ermittlungsmaßnahme wie der Zugriff auf ein informationstechnisches System, mittels dessen die auf dem Zielsystem vorhandenen Daten umfassend erhoben werden können, gegenüber anderen Überwachungsmaßnahmen – etwa der Nutzung des Global Positioning Systems als Instrument technischer Observation (vgl. dazuBVerfGE 112, 304 <318>) - die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden.

Wegen der Heimlichkeit des Zugriffs hat der Betroffene keine Möglichkeit, selbst vor oder während der Ermittlungsmaßnahme darauf hinzuwirken, dass die ermittelnde staatliche Stelle den Kernbereich seiner privaten Lebensgestaltung achtet. Diesem vollständigen Kontrollverlust ist durch besondere Regelungen zu begegnen, welche die Gefahr einer Kernbereichsverletzung durch geeignete Verfahrensvorkehrungen abschirmen.

cc) Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes können je nach der Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein.

Eine gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, hat so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Ist es - wie bei dem heimlichen Zugriff auf ein informationstechnisches System - praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden (vgl.BVerfGE 109, 279 <318>; 113, 348 <391 f.>).

(1) Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhebung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.

Selbst wenn der Datenzugriff unmittelbar durch Personen ohne vorherige technische Aufzeichnung erfolgt, etwa bei einer persönlichen Überwachung der über das Internet geführten Sprachtelefonie, stößt ein Kernbereichsschutz schon bei der Datenerhebung auf praktische Schwierigkeiten. Bei der Durchführung einer derartigen Maßnahme ist in der Regel nicht sicher vorhersehbar, welchen Inhalt die erhobenen Daten haben werden (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <392>). Auch kann es Schwierigkeiten geben, die Daten inhaltlich während der Erhebung zu analysieren. So liegt es etwa bei fremdsprachlichen Textdokumenten oder Gesprächen. Auch in derartigen Fällen kann die Kernbereichsrelevanz der überwachten Vorgänge nicht stets vor oder bei der Datenerhebung abgeschätzt werden. In solchen Fällen ist es verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen, da Grundlage des Zugriffs auf das informationstechnische System tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Schutzgut sind.

(2) Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten.

(a) Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt (vgl. zur Telekommunikationsüberwachung BVerfGE 113, 348 <391 f.>; zur akustischen Wohnraumüberwachung BVerfGE 109, 279 <318, 324>). Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben. Anders liegt es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.

(b) In vielen Fällen wird sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären lassen. Der Gesetzgeber hat durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben.

Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt. Ergibt die Durchsicht, dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen (vgl.BVerfGE 109, 279 <324>; 113, 348 <392>).

dd) Das Verfassungsschutzgesetz enthält die erforderlichen kernbereichsschützenden Vorschriften nicht. Nichts anderes ergibt sich, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG auf das Gesetz zu Artikel 10 Grundgesetz trotz ihrer Unbestimmtheit einbezogen wird. Dieses Gesetz enthält gleichfalls keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Entgegen der Auffassung der nordrhein-westfälischen Landesregierung kann insoweit selbst dann nicht § 4 Abs. 1 G 10 herangezogen werden, wenn die Verweisung des § 5 Abs. 2 Nr. 11 Satz 2 VSG in weiter Interpretation so verstanden wird, dass sie sich auf diese Vorschrift erstreckt. § 4 Abs. 1 G 10 regelt lediglich, dass erhobene Daten, die nicht oder nicht mehr benötigt werden, zu löschen sind, und normiert damit das allgemeine Gebot der Erforderlichkeit. Die Vorschrift enthält demgegenüber keinerlei besondere Maßgaben für die Erhebung, Durchsicht und Löschung von Daten, die einen Kernbereichsbezug aufweisen können. Das Gebot der Erforderlichkeit kann mit der verfassungsrechtlich gebotenen Achtung des Kernbereichs privater Lebensgestaltung nicht gleichgesetzt werden. Der Kernbereich ist vielmehr einer Relativierung durch gegenläufige Ermittlungsinteressen, wie sie durch eine Anwendung des Erforderlichkeitsgebots implizit eingeführt würde, gerade nicht zugänglich (vgl.BVerfGE 109, 279 <314>).

d) Der Verstoß gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) führt zur Nichtigkeit von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG.

e) Angesichts dessen bedarf es keiner Prüfung mehr, wie weit Maßnahmen, zu denen die Norm ermächtigt, auch gegen andere Grundrechte oder das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG verstoßen.

II.

Die Ermächtigung zum heimlichen Aufklären des Internet in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG verletzt das durch Art. 10 Abs. 1 GG gewährleistete Telekommunikationsgeheimnis. Maßnahmen nach dieser Norm können sich in bestimmten Fällen als Eingriff in dieses Grundrecht darstellen, der verfassungsrechtlich nicht gerechtfertigt ist (1); auch ist Art. 19 Abs. 1 Satz 2 GG verletzt (2). Die Verfassungswidrigkeit führt zur Nichtigkeit der Norm (3). Die Verfassungsschutzbehörde darf allerdings weiterhin Maßnahmen der Internetaufklärung treffen, soweit diese nicht als Grundrechtseingriffe anzusehen sind (4).

1. Das in § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG geregelte heimliche Aufklären des Internet umfasst Maßnahmen, mit der die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt, also zum Beispiel durch Aufruf einer Webseite im World Wide Web mittels eines Web-Browsers (s.o. A I 1 a). Dies kann in bestimmten

Fällen in das Telekommunikationsgeheimnis eingreifen. Ein solcher Eingriff wird durch die angegriffene Norm verfassungsrechtlich nicht gerechtfertigt.

a) Der Schutzbereich von Art. 10 Abs. 1 GG umfasst die mit einem an das Internet angeschlossenen informationstechnischen System geführte laufende Fernkommunikation (vgl. oben I 1 c, aa <1>). Allerdings schützt dieses Grundrecht lediglich das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird. Dagegen ist das Vertrauen der Kommunikationspartner zueinander nicht Gegenstand des Grundrechtsschutzes. Steht im Vordergrund einer staatlichen Ermittlungsmaßnahme nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liegt darin kein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 106, 28 <37 f.>). Die staatliche Wahrnehmung von Inhalten der Telekommunikation ist daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein. Das Grundrecht schützt dagegen nicht davor, dass eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt.

Erlangt eine staatliche Stelle Kenntnis von den Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle hierzu nicht durch Kommunikationsbeteiligte autorisiert ist. Da das Telekommunikationsgeheimnis das personengebundene Vertrauen der Kommunikationsbeteiligten zueinander nicht schützt, erfasst die staatliche Stelle die Kommunikationsinhalte bereits dann autorisiert, wenn nur einer von mehreren Beteiligten ihr diesen Zugriff freiwillig ermöglicht hat.

Das heimliche Aufklären des Internet greift danach dann in Art. 10 Abs. 1 GG ein, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. So liegt es etwa, wenn ein mittels Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen. Dagegen ist ein Eingriff in Art. 10 Abs. 1 GG zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt. Erst recht scheidet ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht.

b) Die von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG ermöglichten Eingriffe in Art. 10 Abs. 1 GG sind verfassungsrechtlich nicht gerechtfertigt. Die angegriffene Norm genügt nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu solchen Eingriffen.

aa) § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht, da aufgrund der Unbestimmtheit von Satz 2 dieser Vorschrift die Eingriffsvoraussetzungen nicht hinreichend präzise geregelt sind (vgl. oben C I 2 a, bb).

bb) Die angegriffene Norm steht weiter, soweit sie an Art. 10 Abs. 1 GG zu messen ist, mit dem Gebot der Verhältnismäßigkeit im engeren Sinne nicht in Einklang.

Der Eingriff in das Telekommunikationsgeheimnis wiegt schwer. Auf der Grundlage der angegriffenen Norm kann die Verfassungsschutzbehörde auf Kommunikationsinhalte zugreifen, die sensibler Art sein und Einblicke in die persönlichen Angelegenheiten und Gewohnheiten des Betroffenen zulassen können. Betroffen ist nicht nur derjenige, der den Anlass für die Überwachungsmaßnahme gegeben hat. Der Eingriff kann vielmehr eine gewisse Streubreite aufweisen, wenn Erkenntnisse nicht nur über das Kommunikationsverhalten desjenigen, gegen den sich die Maßnahme richtet, sondern auch über seine Kommunikationspartner gewonnen werden. Die Heimlichkeit des Zugriffs erhöht die Eingriffsintensität. Zudem können wegen der weiten Fassung der Eingriffsvoraussetzungen in § 7 Abs. 1 Nr. 1 in Verbindung mit § 3 Abs. 1 VSG auch Personen überwacht werden, die für den Eingriffsanlass nicht verantwortlich sind.

Ein derart schwerwiegender Grundrechtseingriff setzt auch unter Berücksichtigung des Gewichts der Ziele des Verfassungsschutzes grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus (vgl. zu strafrechtlichen ErmittlungenBVerfGE 107, 299 <321>). Daran fehlt es hier. Vielmehr lässt § 7 Abs. 1 Nr. 1 in Verbindung mit § 3 Abs. 1 VSG nachrichtendienstliche Maßnahmen in weitem Umfang im Vorfeld konkreter Gefährdungen zu, ohne Rücksicht auf das Gewicht der möglichen Rechtsgutsverletzung und auch gegenüber Dritten. Eine derart weitreichende Eingriffsermächtigung ist mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar.

cc) Das Verfassungsschutzgesetz enthält im Zusammenhang mit Eingriffen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Solche Regelungen sind jedoch erforderlich, soweit eine staatliche Stelle zur Erhebung von Inhalten der Telekommunikation unter Eingriff in Art. 10 Abs. 1 GG ermächtigt wird (vgl. BVerfGE 113, 348 <390 ff.>).

2. Schließlich genügt § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG, soweit die Norm zu Eingriffen in Art. 10 Abs. 1 GG ermächtigt, nicht dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG.

Nach Art. 19 Abs. 1 Satz 2 GG muss ein Gesetz dasjenige Grundrecht unter Angabe seines Artikels benennen, das durch dieses Gesetz oder aufgrund dieses Gesetzes eingeschränkt wird. Das Zitiergebot erfüllt eine Warn- und Besinnungsfunktion (vgl. BVerfGE 64, 72 <79 f.>). Durch die Benennung des Eingriffs im Gesetzeswortlaut soll gesichert werden, dass der Gesetzgeber nur Eingriffe vorsieht, die ihm als solche bewusst sind und über deren Auswirkungen auf die betroffenen Grundrechte er sich Rechenschaft ablegt (vgl. BVerfGE 5, 13 <16>; 85, 386 <404>). Die ausdrückliche Benennung erleichtert es auch, die Notwendigkeit und das Ausmaß des beabsichtigten Grundrechtseingriffs in öffentlicher Debatte zu klären. Nicht ausreichend ist hingegen, dass der Gesetzgeber sich des Grundrechtseingriffs bewusst war, wenn sich dies im Gesetzestext nicht niedergeschlagen hat (vgl. BVerfGE 113, 348 <366 f.>).

Die angegriffene Norm wahrt das Zitiergebot im Hinblick auf Art. 10 Abs. 1 GG nicht. Entgegen der Ansicht der nordrhein-westfälischen Landesregierung genügt die angegriffene Norm den Anforderungen nicht schon deshalb, weil § 5 Abs. 2 Nr. 11 Satz 2 VSG durch die Verweisung auf das Gesetz zu Artikel 10 Grundgesetz darauf hindeuten mag, dass der Gesetzgeber einen Eingriff in das Telekommunikationsgeheimnis für möglich gehalten hat. Dem Zitiergebot ist nur Rechnung getragen, wenn das Grundrecht im Gesetzestext ausdrücklich als eingeschränkt benannt wird. Im Übrigen ergibt sich angesichts des Umstands, dass § 5 Abs. 2 Nr. 11 VSG zwei unterschiedliche Eingriffsermächtigungen enthält, aus dem Gesetz keineswegs mit hinreichender Deutlichkeit, für welche von ihnen der Gesetzgeber zumindest mit der Möglichkeit eines Eingriffs in Art. 10 GG gerechnet hat.

3. Der Verstoß von § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG gegen Art. 10 Abs. 1 und Art. 19 Abs. 1 Satz 2 GG bewirkt die Nichtigkeit der Vorschrift.

4. Die Nichtigkeit der Ermächtigung führt allerdings nicht dazu, dass der Behörde Maßnahmen der Internetaufklärung grundsätzlich verwehrt sind, soweit diese nicht in Grundrechte eingreifen.

Das heimliche Aufklären des Internet greift, soweit es nicht unter Art. 10 Abs. 1 GG fällt, insbesondere nicht stets in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht ein.

a) Die von dem allgemeinen Persönlichkeitsrecht gewährleistete Vertraulichkeit und Integrität informationstechnischer Systeme wird durch Maßnahmen der Internetaufklärung nicht berührt, da Maßnahmen nach § 5 Abs. 2 Nr. 11 Satz 1 Alt. 1 VSG sich darauf beschränken, Daten, die der Inhaber des Systems - beispielsweise der Betreiber eines Webservers – für die Internetkommunikation vorgesehen hat, auf dem technisch dafür vorgesehenen Weg zu erheben. Für solche Da-

tenerhebungen hat der Betroffene selbst sein System technisch geöffnet. Er kann nicht darauf vertrauen, dass es nicht zu ihnen kommt.

b) Zumindest in der Regel ist auch ein Eingriff in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in der Ausprägung als Recht auf informationelle Selbstbestimmung zu verneinen.

aa) Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können (vgl. etwa Böckenförde, Die Ermittlung im Netz, 2003, S. 196 f.; Zöller, GA 2000, S. 563 <569>). Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. So liegt es etwa, wenn die Behörde eine allgemein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offen stehende Mailingliste abonniert oder einen offenen Chat beobachtet.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann allerdings gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Hierfür bedarf es einer Ermächtigungsgrundlage.

bb) Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde (vgl. zu Ermittlungen durch verdeckte Ermittler BVerwG, Urteil vom 29. April 1997 - 1 C 2/95 -, NJW 1997, S. 2534; Di Fabio, in: Maunz/Dürig, GG, Art. 2 Abs. 1 Rn. 176; Duttge, JZ 1996, S. 556 <562 f.>; Murswiek, in: Sachs, GG, 4. Aufl., 2007, Art. 2 Rn. 88 b; Warntjen, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 2007, S. 163; speziell zu Ermittlungen im Netz Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 519 ff.).

Danach wird die reine Internetaufklärung in aller Regel keinen Grundrechtseingriff bewirken. Die Kommunikationsdienste des Internet ermöglichen in weitem Umfang den Aufbau von Kommunikationsbeziehungen, in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen bereitstehen. Dies gilt selbst dann, wenn bestimmte Personen - etwa im Rahmen eines Diskussionsforums - über einen längeren Zeitraum an der Kommunikation teil-

nehmen und sich auf diese Weise eine Art „elektronische Gemeinschaft“ gebildet hat. Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig.

III.

Da § 5 Abs. 2 Nr. 11 VSG insgesamt nichtig ist, erledigen sich die gegen § 5 Abs. 3 und § 17 VSG vorgebrachten Rügen. Soweit die Rügen der Beschwerdeführer zulässig sind, ist die Verfassungswidrigkeit der angegriffenen Normen lediglich in Bezug auf Maßnahmen nach der nichtigen Vorschrift geltend gemacht.

IV.

§ 5a Abs. 1 VSG steht mit dem Grundgesetz in Einklang, soweit sein Anwendungsbereich auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG ausgedehnt wurde. Insbesondere verletzt diese Vorschrift nicht Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

1. Die in § 5a Abs. 1 VSG vorgesehene Erhebung von Kontoinhalten und Kontobewegungen greift in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein.

Derartige Kontoinformationen können für den Persönlichkeitsschutz des Betroffenen bedeutsam sein und werden vom Grundrecht geschützt. Nach den gegenwärtigen Gepflogenheiten werden die meisten Zahlungsvorgänge, die über Bargeschäfte des täglichen Lebens hinausgehen, über Konten abgewickelt. Werden Informationen über die Inhalte der Konten einer bestimmten Person gezielt zusammengetragen, ermöglicht dies einen Einblick in die Vermögensverhältnisse und die sozialen Kontakte des Betroffenen, soweit diese - etwa durch Mitgliedsbeiträge oder Unterhaltsleistungen - eine finanzielle Dimension aufweisen. Manche Konteninhaltsdaten, etwa die Höhe von Zahlungen im Rahmen verbrauchsabhängiger Dauerschuldverhältnisse, können auch weitere Rückschlüsse auf das Verhalten des Betroffenen ermöglichen (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2466>).

Die in § 5a Abs. 1 VSG vorgesehenen Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein. Dabei kommt es nicht darauf an, ob sich der Regelungsgehalt der angegriffenen Norm in einer Befugnis der Verfassungsschutzbehörde erschöpft, ein Auskunftsersuchen an ein Kreditinstitut zu richten, oder ob sie implizit eine Auskunftspflicht des jeweiligen Kreditinstituts enthält. In jedem Fall ermächtigt die Vorschrift die Behörde zu Datenerhebungen, die bereits als solche einen Grundrechtseingriff bewirken.

2. Die in § 5a Abs. 1 VSG vorgesehenen Grundrechtseingriffe sind jedoch zur Ermittlung im Hinblick auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG verfassungsrechtlich gerechtfertigt. Insbesondere genügt die angegriffene Norm insoweit dem Verhältnismäßigkeitsgrundsatz.

a) Die in § 5a Abs. 1 VSG geregelten Maßnahmen dienen aufgrund der Erweiterung des Anwendungsbereichs der Norm auch zur Aufklärung der Finanzierungswege und der finanziellen Verhältnisse und Verflechtungen im Zusammenhang mit Bestrebungen im Sinne von § 3 Abs. 1 Nr. 1 VSG. Dies ist ein legitimes Ziel des Verfassungsschutzes.

Die Norm ist in ihrer erweiterten Fassung geeignet, dieses Ziel zu erreichen. Sie ist hierzu auch erforderlich. Ein den Betroffenen weniger belastendes, aber ebenso wirksames Mittel zur Aufklärung von Bankgeschäften mit Blick auf Bestrebungen im Sinne des § 3 Abs. 1 Nr. 1 VSG ist nicht ersichtlich.

b) § 5a Abs. 1 VSG wahrt auch das Gebot der Verhältnismäßigkeit im engeren Sinne.

aa) Allerdings ermächtigt die Norm die Verfassungsschutzbehörde zu Grundrechtseingriffen. Bei Informationen über Kontoinhalte und Kontobewegungen kann es sich um sensible Daten handeln, deren Kenntnisnahme die grundrechtlich geschützten Interessen des Betroffenen erheblich beeinträchtigt. Die Erhebung solcher Informationen hat daher in der Regel ein erhöhtes grundrechtliches Gewicht (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2470>). Die Intensität des Eingriffs wird zudem durch seine Heimlichkeit verstärkt. Nach § 5a Abs. 3 Satz 11 VSG darf auch das auskunftgebende Kreditinstitut dem Betroffenen das Auskunftsersuchen und die übermittelten Daten nicht mitteilen. Schließlich können dem Betroffenen Nachteile daraus entstehen, dass das kontoführende Kreditinstitut selbst zwangsläufig von der Datenerhebung erfährt und daraus ungünstige Schlüsse über den Betroffenen ziehen kann (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2469>).

bb) Die mit § 5a Abs. 1 VSG verfolgten öffentlichen Interessen weisen jedoch solches Gewicht auf, dass sie zu den in der Norm geregelten Grundrechtseingriffen nicht außer Verhältnis stehen.

(1) Das Gesetz knüpft die Kenntnisnahme der Kontoinhalte und Kontobewegungen an tatbestandliche Voraussetzungen, die der Bedeutung des Grundrechtseingriffs für den Betroffenen hinreichend Rechnung tragen.

§ 5a Abs. 1 VSG macht die Erhebung von einem sowohl hinsichtlich der betroffenen Rechtsgüter als auch hinsichtlich der tatsächlichen Grundlage des Eingriffs qualifizierten Gefährdungstatbestand abhängig. Es müssen tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in §

3 Abs. 1 VSG genannten Schutzgüter vorliegen. Der Begriff der schwerwiegenden Gefahr verweist - ebenso wie in dem insoweit gleichlautenden § 8a Abs. 2 BVerfSchG (vgl. dazu BTDrucks 16/2921, S. 14) - auf eine erhöhte Intensität der Rechtsgutsbedrohung. Durch das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr wird zudem die tatsächliche Grundlage des Eingriffs qualifiziert. Es reicht nicht aus, dass die geregelte Datenerhebung allgemein für die Aufgabenerfüllung der Verfassungsschutzbehörde nützlich ist. Vielmehr müssen Anhaltspunkte für einen Zustand bestehen, in dem das Schutzgut konkret bedroht ist.

Diese in zweifacher Hinsicht qualifizierte Eingriffsschwelle genügt den Anforderungen des allgemeinen Persönlichkeitsrechts. Weitere Eingrenzungen der tatbestandlichen Voraussetzungen des Eingriffs sind von Verfassungs wegen nicht zu fordern. Zurückzuweisen ist insbesondere die Auffassung des Beschwerdeführers zu 1b, die materielle Eingriffsschwelle müsse hinsichtlich der in § 3 Abs. 1 Nr. 1 VSG genannten Bestrebungen so heraufgesetzt werden, dass § 5a Abs. 1 VSG nur militante und volksverhetzende Bestrebungen erfasst. Durch das Erfordernis tatsächlicher Anhaltspunkte für eine schwerwiegende Gefahr ist hinreichend sichergestellt, dass nicht jeder vage Verdacht, bestimmte Gruppierungen könnten sich gegen die freiheitliche demokratische Grundordnung richten, zu einer Erhebung von Kontoinhalten und Kontobewegungen ausreicht. Der damit verbundene Eingriff wiegt andererseits nicht so schwer, dass er lediglich zur Bekämpfung gewalttätiger oder solcher Gruppierungen verhältnismäßig sein könnte, die volksverhetzend tätig werden.

Keine durchgreifenden verfassungsrechtlichen Bedenken ergeben sich auch daraus, dass § 5a Abs. 1 VSG keine besonderen Anforderungen an die Auswahl des von einer Datenerhebung Betroffenen regelt. Aufgrund dessen kann es zwar geschehen, dass Kontoinhaltsdaten einer Person erhoben werden, die nicht im Verdacht steht, für die Gefahr rechtlich verantwortlich zu sein. In Betracht kommt insbesondere, dass jemand als undoloses Werkzeug in Vermögenstransaktionen der betroffenen Bestrebung eingeschaltet worden ist. Jedoch ist es verfassungsrechtlich zulässig, eine Maßnahme nach § 5a Abs. 1 VSG auch gegen eine solche Person zu treffen, wenn sich Finanzierungsmechanismen ansonsten nicht aufklären lassen. Die Auswahl zwischen mehreren denkbaren Betroffenen kann durch den auch im Rahmen von § 5a Abs. 1 VSG geltenden Verhältnismäßigkeitsgrundsatz hinreichend angeleitet werden. Dagegen werden Auskünfte über die Kontoinhalte von Personen, die nicht im Verdacht stehen, an den Vermögenstransaktionen der betroffenen Bestrebung bewusst oder unbewusst beteiligt zu sein, kaum je dem gesetzlichen Ziel dienen können, einer schwerwiegenden Gefahr durch die Aufklärung von Finanzierungsmechanismen zu begegnen.

(2) Die angegriffene Norm trägt dem Gewicht des geregelten Grundrechtseingriffs zudem durch geeignete Verfahrensvorkehrungen Rechnung.

So bedarf die Datenerhebung nach § 5a Abs. 3 Satz 3 VSG einer Anordnung des Innenministers, die vom Leiter der Verfassungsschutzabteilung oder seinem Vertreter zu beantragen ist. Der in der Erhebung von Kontoinhalten und Kontobewegungen liegende Grundrechtseingriff wiegt zwar nicht so schwer, dass eine ex-ante-Kontrolle durch eine neutrale Stelle verfassungsrechtlich schlechthin geboten wäre. Die vorgesehene behördeninterne Kontrolle dient jedoch der Sicherung der Interessen des Betroffenen bereits im Vorfeld der Datenerhebung und trägt so zur Verhältnismäßigkeit des Eingriffs bei. Zudem ist eine zusätzliche ex-post-Kontrolle durch die G 10-Kommission gemäß § 5a Abs. 3 Satz 4 bis 8 VSG vorgesehen, die gleichfalls dem Schutz der grundrechtlich geschützten Interessen des Betroffenen dient.

Für die Verarbeitung und Übermittlung der erhobenen Daten enthält § 5a Abs. 3 Satz 9 VSG in Verbindung mit § 4 AG G 10 NRW Maßgaben, die insbesondere den Geboten der Erforderlichkeit und der Zweckbindung genügen.

§ 5a Abs. 3 Satz 11 VSG in Verbindung mit § 5 AG G 10 NRW sieht schließlich eine Benachrichtigung des Betroffenen vor, sobald eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Auf diese Weise wird dem Betroffenen weitgehend ermöglicht, seine Interessen zumindest im Nachhinein zu verfolgen.

V.

Die Kostenentscheidung beruht auf § 34a Abs. 2 BVerfGG.

Papier, Hohmann-Dennhardt, Hoffmann-Riem, Bryde, Gaier, Eichberger, Schluckebier, Kirchhof