Bundesverfassungsgericht:

Verfassungsmäßigkeit der Regelungen zur Internetaufklärung bzw. Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz – Urteil vom 27.2.2008, 1 BvR 370/07 – Teil 2

von Dr. Rolf Meier
Ministerialrat, Vertreter der Parlamentarischen Geschäftsführerin und Justitiar der SPD-Landtagsfraktion Rheinland-Pfalz

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.>).

Dr. Rolf Meier, Ministerialrat

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>).
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.
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> [BVerfG 26.05.1993 - 1 BvR 208/93]; 103, 142 <150 [BVerfG 08.02.2001 - 2 BvF 1/00] f.>). Neben Privatwohnungen fallen auch Betriebs- und Geschäftsräume in den Schutzbereich des
Art. 13 GG (vgl. BVerfGE 32, 54 <69 [BVerfG 13.10.1971 –
1 BvR 280/66] 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 Beschlagnahme BVerfGE 113, 29 <45>).

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.

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 [BVerfG 15.01.1970 - 1 BvR 13/68] 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.

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> [BVerfG 11.06.1991 - 1 BvR 239/90]). 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 Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.

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.

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.

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.
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.
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.
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.
Die angegriffene Norm wird dem Gebot der Normenklarheit und Normenbestimmtheit nicht gerecht.
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> [BVerfG 03.03.2004 - 1 BvF 3/92]; 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 [BVerfG 03.03.2004 - 1 BvF 3/92] 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> [BVerfG 14.01.2004 - 2 BvR 564/95]; 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 [BVerfG 03.03.2004 - 1 BvF 3/92] 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 [BVerfG 12.01.1967 - 1 BvR 169/63] 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>).
211 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.
...(wird ausgeführt)
§ 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).
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. LT Drucks 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 erschließen, 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 Strafverfolgung BVerfGE 115, 166 <193>).
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> [BVerfG 09.03.1994 - 1 BvR 1369/90]; 109, 279 <336> [BVerfG 26.02.2004 - 2 BvH 1/04]). 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.

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.
§ 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 [BVerfG 26.02.2004 - 2 BvH 1/04] 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.
§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Grundrechtseingriffen von hoher Intensität. 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).
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.
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 Verbindungsdaten BVerfGE 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> [BVerfG 31.01.1973 - 2 BvR 454/71]; 107, 299 <321>).
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.
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.
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 Abwehrmöglichkeiten BVerfGE 113, 348 <383 f.>; 115, 320 <353>).
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.
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.
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 Interessen 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. [BVerfG 26.02.2004 - 2 BvH 1/04]>; 115, 320 <346>).
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.>).
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. 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.
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> [BVerfG 03.03.2004 - 1 BvF 3/92]; 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.
Fortsetzung folgt.

253 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> [BVerfG 03.03.2004 - 1 BvF 3/92]).
254 () 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.
255 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 [BVerfG 04.04.2006 - 1 BvR 518/02]). 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.

256
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 unabhängig 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.
257
(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.
258
(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 [BVerfG 03.03.2004 - 1 BvF 3/92] 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> [LVerfG Sachsen 14.05.1996 - Vf II 44/94]).
259
(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 Betroffenen im Einzelfall am besten und sichersten wahren (vgl. BVerfGE 103, 142 <151> [BVerfG 20.02.2001 - 2 BvR 1444/00]; 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> [BVerfG 20.02.2001 - 2 BvR 1444/00], m.w.N.).
260
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.

261
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 [BVerfG 20.02.2001 - 2 BvR 1444/00] ff.> zu Art. 13 Abs. 2 GG).
262
(3)
Nach diesen Maßstäben genügt die angegriffene Norm nicht den verfassungsrechtlichen Anforderungen.... (wird ausgeführt)
.

270
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.
271
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> [BVerfG 16.01.1957 - 1 BvR 253/56]; 27, 1 <6> [BVerfG 16.07.1969 - 1 BvL 19/63]; 32, 373 <378 [BVerfG 08.03.1972 - 1 BvR 674/70] 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> [BVerfG 31.01.1973 - 2 BvR 454/71]; 109, 279 <313> [BVerfG 26.02.2004 - 2 BvH 1/04]). 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>).
272
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 [BVerfG 14.09.1989 - 2 BvR 1062/87] 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.273
bb)
Soll heimlich auf das informationstechnische System des Betroffenen zugegriffen werden, bedarf es besonderer gesetzlicher Vorkehrungen, die den Kernbereich der privaten Lebensgestaltung schützen.
274
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. dazu BVerfGE 112, 304 <318>) - die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden.
275

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.

276

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.

277

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.>).

278

(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.

279

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.

280

(2)

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

281

(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.

282

(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.

283

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>).

284

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...(wird ausgeführt)

286

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.

287

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.

288

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).

289

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.

290

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.

291
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.
292
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.
293Dagegen 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.
294
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.
295
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).
296
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.
297
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.
298
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 Ermittlungen BVerfGE 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.
299
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.>).

300
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...(wird ausgeführt)
303
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.
304
4.
Die Nichtigkeit der Ermächtigung führt allerdings nicht dazu, dass der Behörde Maßnahmen der Internetaufklärung grundsätzlich verwehrt sind, soweit diese nicht in Grundrechte eingreifen.
305
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.
306
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 Datenerhebungen hat der Betroffene selbst sein System technisch geöffnet. Er kann nicht darauf vertrauen, dass es nicht zu ihnen kommt.
307
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.
308
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.
309
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.
310
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 [BVerwG 29.04.1997 - 1 C 2/95]; 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.).
311
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 teilnehmen 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.
312
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.
313
§ 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… (wird ausgeführt)

IV. Anmerkungen

Auf dem Gebiet der inneren Sicherheit war das Jahr 2008 erneut gekennzeichnet durch intensive Diskussionen über die Zulässigkeit staatlicher Eingriffe in das Recht auf informationelle Selbstbestimmung bzw. das allgemeine Persönlichkeitsrecht. Vor allem die Möglichkeiten der modernen Kommunikationstechnik, die Bedrohung durch den internationalen Terrorismus und die Frage des Verhältnisses von Sicherheit und Freiheit bestimmen diese Diskussionen . Das Bundesverfassungsgericht hat durch seine Entscheidung hier manche Klarheit geschaffen und eine neue Ausprägung des allgemeinen Persönlichkeitsrechts in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt.

1. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Mit der Entwicklung dieser Ausprägung des Allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs.1 GG trägt das BVerfG dem Umstand Rechnung, dass durch die Möglichkeiten neuer, vernetzter Kommunikations- und Informationstechnologien und ihre intensive Nutzung neue Entwicklungsmöglichkeiten, aber auch neue Gefährdungen der Persönlichkeit entstehen, das daraus erwachsende Schutzbedürfnis aber durch die in Art. 10, Art. 13 und in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleisteten Grundrechte nicht hinreichend abgedeckt werden kann. Der Schutzbereich dieses Grundrechts ist betroffen, 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 . Für die Abgrenzung zu anderen Grundrechten gibt das Urteil wertvolle Hinweise.

2. Der Kernbereichsschutz

Der Kernbereich privater Lebensgestaltung, der durch Art. 1 Abs. 1 GG in besonderer Weise geschützt wird , steht auch bei dieser Entscheidung im Mittelpunkt. Das BVerfG entwickelt hier vor dem Hintergrund, dass bei einer Online-Durchsuchung beim Beginn der Maßnahme kaum feststellbar ist, welche Daten diesem Kernbereich zuzurechnen sind, einen gestuften Schutz: eine gesetzliche Ermächtigung muss, so weitgehend wie möglich sicherstellen, 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 .

3.
Das Urteil steht in der Tradition der neueren Rechtsprechung des BVerfG. Kutscha ist beizupflichten, wenn er die Rechtsprechung des BVerfG auf die Formel bringt, dass nicht alles, was technisch machbar ist und besonders effizient erscheint, mit den Freiheitsgewährleistungen des GG vereinbar ist . Eine intensivere Beachtung dieser Formel schon im Vorfeld der Gesetzgebung scheint dringend geboten. Darüber hinaus sollten die Ausführungen des BVerfG zu den einzelnen Formulierungen des Gesetzes und hinsichtlich z.B. des Zitiergebotes von den gesetzgebenden Organen gründlich analysiert werden.

V. Fundstellen und Literatur

Urteil: NJW 2008, 822-837; DÖV 2008, 459-466; www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
Literatur: Kutscha, Martin: Mehr Schutz durch Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042-1044