Bundesverfassungsgericht:

Dr. Rolf Meier, Ministerialrat

Verfassungsmäßigkeit der Regelungen zur Internetaufklärung bzw. Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz – Urteil vom 27.2.2008, 1 BvR 370/07 – Teil 3
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.
293 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.
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;
http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
Literatur: Kutscha, Martin: Mehr Schutz durch Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042-1044