R e d a k t i o n e l l e U r t e i l s a n m e r k u n g

1. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.
2. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.
3. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.
4. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen.
5. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein (amtliche Leitsätze).

GG Art. 2 Abs. 1 i.V.m. 1 Abs. 1, 10; VSG § 5 Abs. 2 Nr. 11

BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07 und 1 BvR 595/07

I. Problemstellung

Die Kriminalstrafe ist das äußerste Mittel, das ein freiheitlich verfasster Staat gegen seine Bürger einzusetzen befugt ist. Sie darf – richtigerweise – nur zur Verteidigung der für das friedliche Zusammenleben unabdingbaren Normen eingesetzt werden, deren gesellschaftliche Akzeptanz bereits durch den Verdacht eines strafbaren Verhaltens Schaden zu nehmen droht. Soweit im Strafverfahren das Legalitätsprinzip (§ 152 Abs. 2 StPO) gilt, sind Staatsanwaltschaft und Polizei deshalb schon bei Vorliegen eines Anfangsverdachts verpflichtet, den Sachverhalt zu erforschen. Die Mittel, derer sie sich zu diesem Zweck bedienen dürfen, müssen – ebenso wie die Verhängung der Strafe bei rechtskräftig festgestellter Schuld – aus zweierlei Gründen in einem angemessenen Verhältnis zum mutmaßlichen Normbruch stehen:

Zunächst muss dem Staat um der Funktionalität des Strafrechts willen daran gelegen sein, Übertreibungen zu vermeiden. Wird schon bei dem Verdacht einer nur verhältnismäßig geringfügigen Straftat das praktisch zur Verfügung stehende Ermittlungsarsenal vollständig ausgeschöpft, kann dies dem – schon mit der Verdachtsklärung verfolgten – Ziel der Bestätigung der Normgeltung abträglich sein. Wer im sprichwörtlichen Sinne mit Kanonen auf Spatzen schießt, macht sich bestenfalls lächerlich. Schlimmstenfalls erweckt er den falschen Eindruck, sich nicht nur Spatzen erwehren zu müssen; die Beeinträchtigung der gesellschaftlichen Normanerkennung kann dann durch die staatliche Reaktion auf den Verdacht sogar verstärkt statt kompensiert werden.

Darüber hinaus müssen die bei der Strafverfolgung eingesetzten Mittel auch in Ansehung verfassungsrechtlich verbürgter Freiheitsgewährungen angemessen sein. Das Strafverfahrensrecht gilt als Seismograph der Staatsverfassung. In einem Rechtsstaat kann es deshalb keine Strafverfolgung um jeden Preis geben – selbst wenn diese im Einzelfall funktional wäre. In Zeiten terroristischer Bedrohung ist die damit vom Strafverfahrensrecht zu gewährleistende Balance zwischen individueller Freiheit und kollektiver Sicherheit besonders gefährdet. Die Versuchung, alle technisch möglichen Eingriffsbefugnisse in den Dienst der Strafverfolgung zu stellen, ist angesichts der Herausforderungen, vor die sich die Gesellschaft gestellt sieht, verführerisch. Die sog. Online-Durchsuchung gilt angesichts der Bedrohungen durch den islamistischen Terrorismus in der Praxis als unverzichtbares Instrument nicht nur der präventiven Abwehr terroristischer Straftaten, sondern auch der repressiven Strafverfolgung in diesem Bereich.

Der Ermittlungsrichter des Bundesgerichtshofs sah sich in der Vergangenheit mehrfach mit Anträgen des Generalbundesanwalts konfrontiert, die heimliche Durchsuchung des Computers eines Beschuldigten anzuordnen. Dabei sollte dem Beschuldigten ein hierfür eigens konzipiertes Computerprogramm zugespielt werden, das die auf den Speichermedien des Computers abgelegten Dateien ohne Wissen kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden übertragen sollte.[1] Die heimliche Durchsuchung des Computers ist vom Ermittlungsrichter des BGH in der Vergangenheit mindestens in einem Fall – allerdings mit der Auflage des einmaligen Zugriffs auf den Computer – genehmigt worden.[2] In einem anderen Fall wurde ein entsprechender Antrag unter Hinweis auf eine fehlende Ermächtigungsgrundlage abgelehnt.[3] Die hiergegen eingelegte Beschwerde des Generalbundesanwalts blieb erfolglos. Der *3. Strafsenat* hat in seinem auf die Beschwerde hin ergangenen Beschluss vom 31. Januar 2007

[1] BGHSt 51, 211.
[2] BGH – Ermittlungsrichter – StV 2007, 60, mit ablehnender Anmerkung *Beulke/Meininghaus*.
[3] Vgl. BGHSt 51, 211.

klargestellt, dass eine verdeckte Online-Durchsuchung nicht auf § 102 i.V.m. § 110 StPO gestützt werden kann. Wie sich insbesondere aus den Regelungen der §§ 105 Abs. 2 S. 1, 106 Abs. 1 und § 107 Abs. 1 StPO ergebe,[4] ermächtige die Strafprozessordnung nur zu einer offen durchgeführten Durchsuchung.[5]

Für die Rechtspraxis ist auf der Grundlage des geltenden Rechts damit davon auszugehen, dass ein heimlicher Zugriff auf Computersysteme zum Zwecke der Strafverfolgung mangels gesetzlicher Befugnisnorm unzulässig ist. Die am 27. Februar 2008 ergangene Entscheidung des *Ersten Senats* des BVerfG betrifft die Frage, ob und ggf. in welchen Grenzen der Gesetzgeber von Verfassung wegen zu entsprechenden Maßnahmen ermächtigen *darf*. Sie war mit Spannung erwartet worden, weil Bundesinnenminister *Schäuble* den Beschluss des *3. Strafsenats* zum Anlass genommen hatte, eine in der Großen Koalition umstrittene Rechtsgrundlage für den verdeckten Zugriff auf informationstechnische Systeme einzufordern.[6] Die Entscheidung des *Ersten Senats* steckt insoweit den gesetzgeberischen Handlungsspielraum ab. Sie setzt sich – bedingt durch den Gegenstand der Entscheidung – allerdings primär mit der Frage auseinander, unter welchen Voraussetzungen der Staat zur Verhütung künftiger Straftaten, also zum Zwecke der Gefahrenabwehr, heimlich auf informationstechnische Systeme zugreifen darf.

II. Kernaussagen

Der Entscheidung lagen zwei Verfassungsbeschwerden gegen 2006 eingefügte oder geänderte Vorschriften des Verfassungsschutzgesetzes NRW[7] (im Folgenden: VSG) zugrunde.[8] Sie enthielten Ermächtigungen zum heimlichen Beobachten und sonstigen Aufklären des Internet (§ 5 Abs. 2 Nr. 11 S. 1 Alt. 1 VSG) sowie zum heimlichen Zugriff auf informationstechnische Systeme (Alt. 2). Unter einem heimlichen Aufklären im Sinne der 1. Alt. ist die Kenntnisnahme der Internetkommunikation auf dem technisch vorgesehenen Wege zu verstehen.[9] Die Vorschrift ermächtigte folglich dazu, allgemein zugängliche Kommunikationsinhalte, z.B. von Internetseiten, Chats, Auktionen und Tauschbörsen, zu erlangen. Darüber hinaus rechtfertigte sie die Kenntnisnahme zugangsgeschützter Informationen, soweit diese – technisch ordnungsgemäß – unter Verwendung des jeweils gültigen Passwortes erfolgt.[10] Der heimliche Zugriff auf ein informationstechnisches System im Sinne der 2. Alt. bezeichnet dagegen die technische Infiltration des Systems, mit der es möglich ist, dessen Nutzung zu überwachen, Speichermedien durchzusehen und das System fernzusteuern.[11]

Der *Erste Senat* prüft in seiner Entscheidung zunächst die Verfassungsmäßigkeit der durch § 5 Abs. 2 Nr. 11 S. 1 Alt. 2 VSG eröffneten Befugnis zum heimlichen Zugriff auf ein informationstechnisches System. Die Vorschrift verletzt nach seiner Ansicht das Allgemeine Persönlichkeitsrecht (im Folgenden: APR), Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, in der durch die Entscheidung – erstmals – ausformulierten Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (unten 1.).[12] Im Anschluss daran erörtert er die Verfassungsmäßigkeit des heimlichen Aufklärens des Internet, § 5 Abs. 2 Nr. 11 S. 1 Alt. 1 VSG, und stellt eine Verletzung des Telekommunikationsgeheimnisses aus Art. 10 GG und des Zitiergebots, Art. 19 Abs. 1 S. 2 GG, fest (unten 2.).[13]

1. Der heimliche Zugriff auf informationstechnische Systeme

Das vom *Ersten Senat* als neue Ausprägung des APR entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist betroffen, wenn eine Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, aufgrund derer im Fall eines staatlichen Zugriffs ein Einblick in wesentliche Teile der Lebensgestaltung einer Person oder gar ein aussagekräftiges Bild der Persönlichkeit gewonnen werden können. Vom Schutzbereich dieses Grundrechts sind laut Entscheidung des BVerfG insbesondere (privat oder beruflich genutzte) Personalcomputer,[14] aber auch Mobiltelefone oder elektronische Terminkalender erfasst, soweit sie über einen entsprechenden Funktionsumfang verfügen und die Speicherung personenbezogener Daten vielfältiger Art zulassen.[15]

a) Abgrenzung zu anderen Grundrechten

Andere grundrechtliche Gewährleistungen, insbesondere das Fernmeldegeheimnis, Art. 10 GG, das Grundrecht auf Unverletzlichkeit der Wohnung, Art. 13 GG, sowie die als Ausprägungen des APR bereits bekannten Rechte auf Privatheit und informationelle Selbstbestimmung sind nach Einschätzung des *Senats* nicht geeignet, den mit der Informationstechnik entstandenen neuartigen Gefährdungen der Persönlichkeit[16]

[4] BGHSt 51, 211 (213).
[5] BGHSt 51, 211 (216).
[6] Vgl. den Artikel „Heimliche Online-Durchsuchung unzulässig“, F.A.Z. vom 6.2.2008, S. 1.
[7] Die Änderungen gehen auf das Gesetz über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl. NW, S. 620) zurück.
[8] Die Darstellung beschränkt sich auf die Vorschriften zur „Online-Durchsuchung“; nicht eingegangen wird auf die sonstigen angegriffenen Vorschriften, bezüglich derer die Beschwerden entweder als unzulässig verworfen wurden, sich mit der Feststellung der Verfassungswidrigkeit des § 5 Abs. 1 Nr. 11 erledigten oder als unbegründet abgewiesen wurden.
[9] BVerfG, Urt. v. 27.2.2008, Rn. 4, abrufbar unter http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (27.5.2008).
[10] BVerfG, Urt. v. 27.2.2008, Rn. 6.
[11] BVerfG, Urt. v. 27.2.2008, Rn. 5.
[12] BVerfG, Urt. v. 27.2.2008, Rn. 166.
[13] BVerfG, Urt. v. 27.2.2008, Rn. 288.
[14] BVerfG, Urt. v. 27.2.2008, Rn. 203.
[15] BVerfG, Urt. v. 27.2.2008, Rn. 203.
[16] BVerfG, Urt. v. 27.2.2008, Rn. 170.

hinreichend Rechnung zu tragen. Sie beträfen jeweils nur Teilaspekte des Umgangs mit informationstechnischen Systemen und würden deshalb der gestiegenen Bedeutung der Nutzung solcher Systeme für die Persönlichkeitsentfaltung[17] nicht gerecht. So ermögliche das Internet nicht nur den Zugriff auf eine Fülle von Informationen, sondern stelle überdies verschiedene Kommunikationsdienste zum Aufbau und zur Pflege sozialer Kontakte bereit, die herkömmliche Formen der Fernkommunikation in zunehmendem Maße verdrängten.[18] Diese seien mit der teils bewussten, teils durch die Systeme selbsttätig vorgenommenen Erzeugung, Verarbeitung und Speicherung von Daten verbunden, die allesamt im Hinblick auf Verhalten und Eigenschaften des Nutzers ausgewertet werden könnten.[19] Die Erhebung und Auswertung der in Arbeitsspeicher und auf Speichermedien enthaltenen Vielzahl von Daten mit Bezug zu persönlichen Verhältnissen, sozialen Kontakten und ausgeübten Tätigkeiten des Nutzers ermöglichten weitreichende Rückschlüsse auf seine Persönlichkeit bis hin zu einer Profilbildung.[20] Dies verlange nach einem umfassenden Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme.

Das vom BVerfG zu diesem Zweck entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt zunächst das Interesse des Nutzers daran, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[21] Sein Schutzbereich ist nach Ansicht des *Ersten Senats* aber auch betroffen, wenn die Leistungen, Funktionen und Speicherinhalte infolge eines manipulativen Zugriffs auf das System durch Dritte genutzt werden können.[22] Dies gelte auch für Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. Damit kann auch der Einsatz sog. Hardware-Keylogger oder die Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur einen Eingriff darstellen.[23]

b) Schranken

Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird als Ausprägung des APR allerdings nicht schrankenlos gewährt. Eingriffe können nach der Entscheidung des *Ersten Senats* sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.[24] Sie bedürfen allerdings – wie auch jeder sonstige Eingriff in Grundrechte – einerseits einer dem Gebot der Normenklarheit und Normenbestimmtheit entsprechenden Ermächtigungsgrundlage und sind wegen der besonderen Bedeutung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme andererseits unter Beachtung des Verhältnismäßigkeitsgrundsatzes nur in engen Grenzen zulässig. Die in § 5 Abs. 2 Nr. 11 S. 1 Alt. 2 VSG enthaltene Ermächtigung zum heimlichen Zugriff auf informationstechnische Systeme wird nach Einschätzung des *Ersten Senats* beiden Anforderungen nicht gerecht.[25] Von besonderer Bedeutung sind insoweit die aus dem Verhältnismäßigkeitsgrundsatz folgenden inhaltlichen Grenzen einer möglichen gesetzlichen Befugnis zum heimlichen Zugriff auf informationstechnische Systeme.

aa) Besondere Gefährdungslage

Bei der Entwicklung dieser Grenzen hat sich der *Senat* insbesondere davon leiten lassen, dass eine staatliche Datenerhebung aus komplexen informationstechnischen Systemen ein beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen aufweist[26], weil der Staat Zugang zu einem Datenbestand erhalte, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffe.[27] Dies gelte angesichts der gegenwärtigen Nutzungsgepflogenheiten solcher Geräte gerade auch für persönliche Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien.[28] Der verfügbare Datenbestand könne 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.[29]

Soweit Daten erhoben würden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, werde die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die – auch im Allgemeinwohl liegende – Möglichkeit der Bürger beschränkt werde, an einer unbeobachteten Fernkommunikation teilzunehmen.[30] Die Zulässigkeit der Erhebung solcher Daten beeinträchtige infolge der durch sie bedingten Furcht vor Überwachung mittelbar die Freiheit der Bürger, indem sie eine unbefangene Individualkommunikation verhindern könne.[31] Zudem wiesen solche Datenerhebungen eine das Gewicht des Eingriffs erhöhende – und im Fall der Einbindung in ein Netzwerk sogar nochmals gesteigerte[32] – Streubreite auf, weil von ihnen notwendigerweise auch unbeteiligte Dritte erfasst würden.[33] Zugleich könnten die Betroffenen infolge der Heimlichkeit des Eingriffs ihre Interessen nicht wirkungsvoll wahrnehmen.[34]

Das Gewicht des Eingriffs werde ferner auch dadurch geprägt, dass der Zugriff Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch

[17] BVerfG, Urt. v. 27.2.2008, Rn. 174.
[18] BVerfG, Urt. v. 27.2.2008, Rn. 176.
[19] BVerfG, Urt. v. 27.2.2008, Rn. 178.
[20] BVerfG, Urt. v. 27.2.2008, Rn. 178.
[21] BVerfG, Urt. v. 27.2.2008, Rn. 204.
[22] BVerfG, Urt. v. 27.2.2008, Rn. 204.
[23] BVerfG, Urt. v. 27.2.2008, Rn. 205.
[24] BVerfG, Urt. v. 27.2.2008, Rn. 207.
[25] BVerfG, Urt. v. 27.2.2008, Rn. 208, 218.
[26] BVerfG, Urt. v. 27.2.2008, Rn. 230.
[27] BVerfG, Urt. v. 27.2.2008, Rn. 231.
[28] BVerfG, Urt. v. 27.2.2008, Rn. 231.
[29] BVerfG, Urt. v. 27.2.2008, Rn. 231.
[30] BVerfG, Urt. v. 27.2.2008, Rn. 233.
[31] BVerfG, Urt. v. 27.2.2008, Rn. 233.
[32] BVerfG, Urt. v. 27.2.2008, Rn. 235.
[33] BVerfG, Urt. v. 27.2.2008, Rn. 233.
[34] BVerfG, Urt. v. 27.2.2008, Rn. 238.

Dritter begründe, da durch ihn – unbeabsichtigt oder auch gezielt – Schäden wie Datenverlust verursacht werden könnten.[35] Schließlich könne durch die Nutzung unbekannter Sicherheitslücken ein Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme entstehen.[36] In der Folge bestehe die Gefahr, dass die Ermittlungsbehörde es unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben.[37]

bb) Konsequenzen für die Zulässigkeit

Der heimliche Zugriff auf informationstechnische Systeme kann vor dem Hintergrund dieser Erwägungen nach der Entscheidung des *Ersten Senats* nur unter folgenden Voraussetzungen verhältnismäßig sein: Er müsse erstens zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut notwendig sein, die Rechte des Betroffenen bedürften zweitens des Schutzes durch Verfahrensvorkehrungen und der Gesetzgeber habe drittens Regelungen zu schaffen, die nach Möglichkeit einen Eingriff in den unantastbaren Kernbereich der Persönlichkeit verhinderten.

(1) Konkrete Gefahr für ein überragend wichtiges Rechtsgut

Die erforderliche konkrete Gefahr für ein überragend wichtiges Rechtsgut könne zunächst in einer Bedrohung der Individualrechtsgüter Leib, Leben und Freiheit der Person bestehen. Sie sei aber auch bei einer Gefährdung von Gütern der Allgemeinheit gegeben, wenn dadurch die Grundlagen oder der Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt würden, wie etwa bei einer Gefährdung der Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.[38] Nicht erforderlich sei, dass die Gefahr schon in näherer Zukunft eintrete.[39] Nach Ansicht des *Ersten Senats* reicht es aus, wenn konkrete Tatsachen „den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen“ und über die Identität der beteiligten Personen zumindest so viel bekannt sei, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden könne.[40]

(2) Grundrechtsschutz durch Verfahren

Ergänzend sieht der *Erste Senat* die Notwendigkeit, dass ein zum Eingriff ermächtigendes Gesetz Grundrechtsschutz durch Verfahrensvorschriften gewährleiste, indem die Rücksichtnahme auf die Interessen des Betroffenen durch die vorbeugende Kontrolle einer neutralen Instanz gesichert werde.[41] Die Maßnahme müsse deshalb unter den Vorbehalt der Anordnung eines Richters oder einer anderen unabhängigen und neutralen Stelle gestellt werden.[42] Für Eilfälle reiche eine nachträgliche Überprüfung,[43] wie sie auch ansonsten bei präventiven oder strafprozessualen Eingriffsmaßnahmen üblich ist.

(3) Schutz des absoluten Kernbereichs

Schließlich betont der *Erste Senat* – wie schon in seiner Entscheidung zur akustischen Wohnraumüberwachung[44] –, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung auch durch überwiegende Interessen der Allgemeinheit nicht gerechtfertigt werden können.[45] Eine Regelung, die die Befugnis zum heimlichen Zugriff auf informationstechnische Systeme enthalte, müsse deshalb zugleich Sicherungen vorsehen, die etwa einen Zugriff auf tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente verhindern.[46]

Zur Wahrung des absolut geschützten Kernbereichs der Persönlichkeit hält der *Erste Senat* ein zweistufiges Schutzkonzept für erforderlich[47]: Die gesetzliche Regelung habe erstens sicherzustellen, dass die Erhebung kernbereichsrelevanter Daten nach Möglichkeit unterbleibt.[48] Bei konkreten Anhaltspunkten dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, dürfe der Zugriff deshalb grundsätzlich nicht vorgenommen werden – es sei denn, bestimmte Tatsachen deuteten zugleich darauf hin, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.[49] Soweit entsprechende konkrete Anhaltspunkte nicht bestünden, sei es verfassungsrechtlich allerdings nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen.[50] Wenn sich die Kernbereichsrelevanz daher nicht vor oder bei Datenerhebung klären lasse, müsse der Gesetzgeber zweitens für einen hinreichenden Schutz in der Auswertungsphase sorgen.[51] Die Daten seien nach Erhebung auf kernbereichsrelevante Informationen durchzusehen und bei Kernbereichsrelevanz unverzüglich zu löschen. Zusätzlich müsse ihre Weitergabe und Verwertung ausgeschlossen werden.[52]

[35] BVerfG, Urt. v. 27.2.2008, Rn. 239.
[36] BVerfG, Urt. v. 27.2.2008, Rn. 241.
[37] BVerfG, Urt. v. 27.2.2008, Rn. 241.
[38] BVerfG, Urt. v. 27.2.2008, Rn. 242 ff.
[39] BVerfG, Urt. v. 27.2.2008, Rn. 242.
[40] BVerfG, Urt. v. 27.2.2008, Rn. 251.
[41] BVerfG, Urt. v. 27.2.2008, Rn. 242, 257 ff.
[42] BVerfG, Urt. v. 27.2.2008, Rn. 259 f.
[43] BVerfG, Urt. v. 27.2.2008, Rn. 261.
[44] BVerfGE 109, 279 (314 ff.).
[45] BVerfG, Urt. v. 27.2.2008, Rn. 270 f.
[46] BVerfG, Urt. v. 27.2.2008, Rn. 272.
[47] BVerfG, Urt. v. 27.2.2008, Rn. 276, 280.
[48] BVerfG, Urt. v. 27.2.2008, Rn 277, 281.
[49] BVerfG, Urt. v. 27.2.2008, Rn. 281.
[50] BVerfG, Urt. v. 27.2.2008, Rn. 279.
[51] BVerfG, Urt. v. 27.2.2008, Rn. 277, 282 f.
[52] BVerfG, Urt. v. 27.2.2008, Rn. 277, 283.

2. Die heimliche Aufklärung des Internet

Anders als den heimlichen Zugriff auf informationstechnische Systeme betrifft die in § 5 Abs. 2 Nr. 11 S. 1 Alt. 1 VSG enthaltene Befugnis zum heimlichen Aufklären des Internet nicht das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Der *Erste Senat* misst diese Befugnis deshalb nicht an dieser Ausprägung des APR,[53] sondern vor allem an der Gewährleistung des Telekommunikationsgeheimnisses, Art. 10 Abs. 1 GG, und des Grundrechts auf informationelle Selbstbestimmung[54]. Im Ergebnis genügt die Regelung nach Ansicht des Gerichts weder dem Zitiergebot des Art. 19 Abs. 1 S. 2 GG[55] noch den inhaltlichen Anforderungen des grundrechtlich geschützten Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG.

a) Schutzbereich und Eingriff

Der Schutzbereich von Art. 10 Abs. 1 GG umfasse in Bezug auf die mit einem an das Internet angeschlossenen informationstechnischen System geführte laufende Fernkommunikation das Vertrauen des Einzelnen in die Nichtkenntnisnahme durch Dritte, nicht jedoch das Vertrauen der Kommunikationspartner zueinander.[56] Die staatliche Wahrnehmung von Inhalten der Telekommunikation sei daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein, nicht jedoch, wenn eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt.[57]

Ein Eingriff in Art. 10 Abs. 1 GG scheide daher aus, wenn eine staatliche Stelle Kenntnis von den Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür technisch vorgesehenen Weg mit der Autorisation zumindest eines Kommunikationsbeteiligten oder unter Nutzung eines freiwillig zur Verfügung gestellten Zugangs erhalte. Das gelte erst recht bei der Erhebung allgemein zugänglicher Inhalte, etwa aus öffentlichen Diskussionsforen oder nicht zugangsgesicherten Webseiten.[58] Zumindest in der Regel sei insoweit auch ein Eingriff in das Recht auf informationelle Selbstbestimmung zu verneinen.[59] Bei allgemein zugänglichen Websites, Mailinglisten oder Chats handele es sich um öffentlich zugängliche Informationen, die sich an einen nicht weiter abgegrenzten Personenkreis richteten, selbst wenn es sich um im Einzelfall personenbezogene Daten handele.[60] Ein Eingriff in das Recht auf informationelle Selbstbestimmung könne deshalb nur vorliegen, wenn Informationen aus allgemein zugänglichen Inhalten gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergebe.[61] Von diesem Fall abgesehen, weise das heimliche Aufklären des Internet nur bei der Überwachung zugangsgesicherter Kommunikationsinhalte ohne oder gegen den Willen der Kommunikationsbeteiligten Grundrechtsrelevanz auf.[62] Insoweit sei ein Eingriff in das grundrechtlich geschützte Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG, zu bejahen.

b) Verfassungsrechtliche Vorgaben

Eine gesetzliche Ermächtigung zur Vornahme entsprechender Maßnahmen müsse damit zunächst dem Gebot der Normenklarheit und Normenbestimmtheit genügen[63] und unterliege darüber hinaus inhaltlichen, sich aus dem Grundsatz der Verhältnismäßigkeit ergebenden Grenzen.[64] Nach Ansicht des *Ersten Senats* ist hier insbesondere zu berücksichtigen, dass entsprechende Befugnisse den Zugriff auf sensible Daten erlaubten, und zwar sowohl bei demjenigen, der Anlass für die Überwachungsmaßnahme gegeben hat, als auch bei seinen Kommunikationspartnern.[65] Eine solche Befugnis dürfe nur unter der Voraussetzung einer qualifizierten Eingriffsschwelle gewährt werden. Darüber hinaus sei der Gesetzgeber verfassungsrechtlich gehalten, die zum Schutz des Kernbereichs privater Lebensgestaltung erforderlichen Regelungen zu schaffen.[66]

III. Würdigung

Die Entscheidung des *Ersten Senats* betont im Hinblick auf den heimlichen Zugriff auf informationstechnische Systeme mit Recht die Schwere eines entsprechenden staatlichen Eingriffs. Sie verdient auch Zustimmung, soweit sich das Gericht angesichts der erheblichen Bedeutung der Nutzung solcher Systeme und der Fülle der von ihnen vorgehaltenen sensiblen Daten um eine neuerliche Ausdifferenzierung des grundrechtlichen Schutzes der Persönlichkeitsentfaltung bemüht. Das als Ausprägung des APR vom *Ersten Senat* im Volkszählungsurteil vom 15. Dezember 1983[67] aus der Taufe gehobene Recht auf informationelle Selbstbestimmung ist – wegen seines weit abgesteckten Schrankenvorbehalts – nicht in der Lage, der in der Entscheidung zutreffend beschriebenen neuen Gefahrenlage für die Persönlichkeitsentfaltung wirksam zu begegnen. Das (neue) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kann infolgedessen als sachgerechte Beschreibung eines

[53] BVerfG, Urt. v. 27.2.2008, Rn. 305 f.
[54] BVerfG, Urt. v. 27.2.2008, Rn. 289 ff., 307 ff.
[55] BVerfG, Urt. v. 27.2.2008, Rn. 288, 300 ff.
[56] BVerfG, Urt. v. 27.2.2008, Rn. 290.
[57] BVerfG, Urt. v. 27.2.2008, Rn. 290.
[58] BVerfG, Urt. v. 27.2.2008, Rn 291 ff.
[59] Ein Eingriff in das Recht auf informationelle Selbstbestimmung liege nicht schon darin, dass eine staatliche Stelle verdeckt eine Kommunikationsbeziehung zu einem Grundrechtsträger aufbaue. Das Vertrauen in die Identität und Wahrhaftigkeit des Kommunikationspartners sei mangels Überprüfungsmechanismen nicht schutzwürdig (dazu BVerfG, Urt. v. 27.2.2008, Rn. 310 f.).
[60] BVerfG, Urt. v. 27.2.2008, Rn. 308.
[61] BVerfG, Urt. v. 27.2.2008, Rn. 309.
[62] BVerfG, Urt. v. 27.2.2008, Rn. 292 f.
[63] BVerfG, Urt. v. 27.2.2008, Rn. 295.
[64] BVerfG, Urt. v. 27.2.2008, Rn. 296.
[65] BVerfG, Urt. v. 27.2.2008, Rn. 297.
[66] BVerfG, Urt. v. 27.2.2008, Rn. 299.
[67] BVerfGE 65, 1.

besonders schutzwürdigen Kernbereichs des Rechts auf informationelle Selbstbestimmung angesehen werden.

Trotz seiner restriktiven Schrankenbeschreibung, die der des Grundrechts auf Unverletzlichkeit der Wohnung, Art. 13 GG, vergleichbar ist, hat das BVerfG der Online-Durchsuchung im Kontext der Terrorismusbekämpfung allerdings ohne praktisch bedeutsame Einschränkungen den Weg geebnet. Weisen bestimmte Tatsachen darauf hin, dass konkrete Personen einen terroristischen Anschlag planen, so ist ein – nach Möglichkeit, aber nicht notwendigerweise auf diese Personen begrenzter – heimlicher Zugriff auf informationstechnische Systeme unter dem Vorbehalt richterlicher Anordnung ohne Weiteres zulässig. Zur präventiven Verhütung terroristischer Anschläge darf der Staat damit die im vorliegenden Zusammenhang technisch realisierbaren Überwachungsmaßnahmen vollumfänglich einsetzen.

Der Vorbehalt des absoluten Schutzes des Kernbereichs privater Lebensgestaltung ändert daran nichts. Der *Erste Senat* geht davon aus, dass Inhalte, die dem Ermittlungsziel unterfallen (etwa weil sie Angaben über Anschlagspläne enthalten), wegen ihres Sozialbezugs nicht zugleich dem Kernbereich privater Lebensgestaltung zuzuordnen sind. Soweit konkrete Anhaltspunkte dafür bestehen, dass zwecks Vermeidung der Überwachung kernbereichsbezogene Kommunikationsinhalte mit dem Ermittlungsziel unterfallenden Inhalten verknüpft werden, hält er die Überwachung deshalb trotz zugleich bestehender Kernbereichsrelevanz für zulässig.[68]

Der Schutz des Kernbereichs privater Lebensgestaltung setzt der Terrorismusbekämpfung damit allenfalls scheinbare Grenzen. Dies gilt nach der Entscheidung des *Ersten Senats* auch deshalb, weil es danach – in Abkehr zu den ebenfalls vom *Ersten Senat* für die akustische Wohnraumüberwachung[69] entwickelten Grundsätzen – nicht notwendig sein soll, Ermittlungsmaßnahmen abzubrechen, wenn die erhobenen Informationen dem Kernbereich der Persönlichkeitsentfaltung angehören. Jedenfalls beim heimlichen Zugriff auf informationstechnische Systeme reicht, dass Daten mit Kernbereichsbezug bei der Auswertung der erlangten Informationen gelöscht und nicht verwertet werden.[70]

Ist der heimliche Zugriff auf informationstechnische Systeme damit zum Zwecke der präventiven Terrorismusbekämpfung vollumfänglich möglich, so bleibt die Frage zu beantworten, ob Entsprechendes auch für den Einsatz derartiger Eingriffsbefugnisse zum Zwecke der Terrorismusbekämpfung durch Strafverfolgung gilt. Die Entscheidung behandelt diese Problematik nicht näher. Lediglich am Rande wird erwähnt, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität auch zum Zwecke der Strafverfolgung eingeschränkt werden darf. Die insoweit zu beachtenden – mangels akuter Gefahrensituation möglicherweise engeren – Schranken werden nicht thematisiert.

Auch im politischen Raum sind gegenwärtig in erster Linie das Recht der Gefahrenabwehr betreffende Änderungen des BKA-Gesetzes (im Folgenden: BKAG-E) geplant. § 20k des aktuellen Entwurfes eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 16. April 2008[71] enthält eine an den Vorgaben des *Ersten Senats* orientierte Ermächtigung zum verdeckten Zugriff auf informationstechnische Systeme. Die Maßnahme darf danach nur auf Antrag des Präsidenten des BKA oder seines Vertreters richterlich angeordnet werden (§ 20k Abs. 5 S. 1 BKAG-E). Bei Gefahr im Verzug soll sie auch ohne richterliche Genehmigung angeordnet werden können (§ 20k Abs. 5 S. 2 und 3 BKAG-E).

Konkrete Pläne für eine strafprozessuale Rechtsgrundlage liegen derzeit noch nicht vor. Informationen, die infolge einer präventiv begründeten Maßnahme erlangt wurden, sind aber auch in Strafverfahren von Bedeutung und nach der in der Praxis vorherrschenden Sichtweise jedenfalls als Spurenansatz nutzbar. § 20v Abs. 5 S. 1 Nr. 3 BKAG-E sieht insoweit ausdrücklich die Übermittlung der gewonnenen Daten zur Verfolgung von Straftaten vor, wenn diese im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind. § 161 Abs. 2 StPO stünde nur einer strafprozessualen Verwendung der Daten „zu Beweiszwecken“ entgegen. Die Vorschrift sperrt damit weder die Übermittlung noch die Auswertung solcher Daten zur Gewinnung neuer Ermittlungsansätze.

Im Kontext der Terrorismusbekämpfung ist der maßgebliche Seismograph der Staatsverfassung bei In-Kraft-Treten der gegenwärtigen Pläne zur Reform des BKAG damit nicht mehr die Strafprozessordnung, sondern das Recht der Gefahrenabwehr. Angesichts dieser Sachlage wäre den Freiheitsrechten des Einzelnen möglicherweise mehr mit einer ergänzenden – auf besonders schwerwiegende terroristische Straftaten beschränkten – strafprozessualen Ermächtigung als mit dem Verzicht auf eine solche Regelung gedient. Der Gesetzgeber müsste allerdings durch eine spezielle Verwendungsregelung zugleich klarstellen, dass durch eine präventive Online-Durchsuchung gewonnene Erkenntnisse im Strafverfahren auch in Bezug auf etwaige Spurenansätze nur bei Vorliegen der Voraussetzungen der strafprozessualen Ermächtigung genutzt werden dürfen.[72]

Prof. Dr. Mark Deiters, Wiss. Mitarbeiterin Anna Helena Albrecht, Münster

[68] BVerfG, Urt. v. 27.2.2008, Rn. 281.
[69] BVerfGE 109, 279 (318 f.).
[70] BVerfG, Urt. v. 27.2.2008, Rn. 277, 283.

[71] BKAG-Entwurf S. 16 ff.; abrufbar unter http://netzpolitik.org/2008/der-entwurf-des-bka-gesetzes-zum-download/ (Stand: 14.5.2008).
[72] Nach ihrem Wortlaut ist es naheliegend, die Verwendungsregelung des § 100d Abs. 5 Nr. 3 StPO entsprechend zu deuten; ihr Gehalt ist aber nicht unumstritten, siehe dazu *Wolter*, in: Rudolphi u.a. (Hrsg.), Systematischer Kommentar zur Strafprozeßordnung und zum Gerichtsverfassungsgesetz, 56. Lieferung, Stand: Februar 2008, § 100d Rn. 67, 35 ff.