Bundesverfassungsgericht:

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

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

I. Amtliche Leitsätze

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.

II. Sachverhalt

Die Verfassungsbeschwerden einer Journalistin, eines Mitglieds des Landesverbandes Nordrhein-Westfalen der Partei
DIE LINKE und dreier Rechtsanwälte richteten sich gegen das am 30. Dezember 2006 in Kraft getretene Änderungsgesetz zum nordrhein-westfälischen Verfassungsschutzgesetz, welches dem Verfassungsschutz unter anderem die Befugnis gibt, heimlich auf an das Internet angeschlossene Computersysteme zuzugreifen (sog.„Online-Durchsuchung„). Im Einzelnen wurden folgende Vorschriften angegriffen:

Die Norm ermächtigt die Verfassungsschutzbehörde zu zwei verschiedenen Arten von Maßnahmen: Zum einen erlaubt sie das Beobachten und Aufklären des Internets; hierunter fallen in erster Linie die Sichtung und Teilnahme an der Internet-Kommunikation (z.B. E-Mails, Newsgroups, Chats, Webseiten). Zum anderen ermächtigt die Norm die Verfassungsschutzbehörde zum heimlichen Zugriff auf informationstechnische Systeme, auch mittels technischer Mittel. Derartige Zugriffe werden in jüngerer Zeit unter dem Schlagwort „Online-Durchsuchung„ diskutiert. Die Norm spezifiziert nicht näher, welche Arten von Zugriffen auf informationstechnische Systeme gesetzlich erlaubt sein sollen. Technisch denkbar und unter Ermittlungsgesichtspunkten möglicherweise zielführend könnten eventuell die folgenden Arten von Zugriffen sein: Der einmalige Zugriff auf die auf der Festplatte des betroffenen Computers gespeicherten Daten; eine kontinuierliche Überwachung der gespeicherten Daten, bei der jede Änderung des Datenbestands mitgeschnitten wird; der Zugriff auf weitere Funktionen des betroffenen Rechners (etwa Mitverfolgung der Tastatureingaben, Zugriff auf über das Internet geführte Telefonate).
Danach sind mit nachrichtendienstlichen Mitteln gewonnene personenbezogene Daten zu kennzeichnen und den Personen, zu denen diese Informationen erfasst wurden, nach Beendigung der Maßnahme mitzuteilen. Unter bestimmten Voraussetzungen kann eine

Benachrichtigung des Betroffenen unterbleiben.
Unter bestimmten Voraussetzungen darf die Verfassungsschutzbehörde bei Kreditinstituten, Finanzdienstleistungsunternehmen und Finanzunternehmen Auskünfte über Beteiligte am Zahlungsverkehr und über Geldbewegungen und Geldanlagen einholen. Auf diese Weise soll ermöglicht werden, die Finanzierungsströme terroristischer Netzwerke zu ermitteln.
Die Norm regelt die Befugnis des Verfassungsschutzes zur akustischen Wohnraumüberwachung.
Das Gesetz unterscheidet zwischen Akten der Verfassungsschutzbehörde, die zu bestimmten Personen geführt werden, und Sachakten über verfassungsfeindliche Bestrebungen, in die allerdings auch personenbezogene Informationen aufgenommen werden können. § 8 Abs. 4 VSG regelt den Zugriff auf personenbezogene Daten, die in Sachakten enthalten sind. Der angegriffenen Satz 2 bestimmt, dass personenbezogene Daten in Sachakten bestehen bleiben dürfen, auch wenn die zu der betreffenden Person geführten Dateien gelöscht worden sind.
Die Norm ermächtigt die Verfassungsschutzbehörde, ihre Erkenntnisse in gemeinsamen Dateien nicht nur – wie bereits bisher – mit anderen Verfassungsschutzbehörden, sondern auch mit weiteren Sicherheitsbehörden zu verarbeiten.
Nach Auffassung der Beschwerdeführer verletzt die „Online-Durchsuchung„ (§ 5 Abs. 2 Nr. 11 VSG) das Recht auf Unverletzlichkeit der Wohnung. Viele vertrauliche Informationen, die früher in körperlicher Form in der Wohnung aufbewahrt wurden und damit in den räumlichen Schutzbereich der Wohnung fielen, würden heute auf dem heimischen Computer gespeichert und fielen daher ebenfalls in den Schutzbereich des Art. 13 GG. Die Unverletzlichkeit der Wohnung könne nur unter den Vo-
raussetzungen des Art. 13 Abs. 2 bis 7 GG eingeschränkt werden. Die Online-Durchsuchung werde aber von keiner der dort vorgesehenen Einschränkungsmöglichkeiten erfasst. Darüber hinaus rügen die Beschwerdeführer eine Verletzung des Rechts auf informationelle Selbstbestimmung. Die Regelung über die Online-Durchsuchung wahre weder das Gebot der Normenklarheit noch den Grundsatz der Verhältnismäßigkeit. Soweit § 5 Abs. 2 Nr. 11 VSG das Beobachten des Internets vorsehe, verletze die Norm auch das Fernmeldegeheimnis. Soweit es um die Benachrichtigung des Betroffenen im Anschluss an eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG geht, sehe § 5 Abs. 3 VSG zu weit reichende Ausnahmen von der Benachrichtigungspflicht vor und sei daher mit der Rechtsschutzgarantie des Art. 19 Abs. 4 GG nicht vereinbar. § 5 a Abs. 1 VSG, der die Erhebung von Konteninhalten regelt, verstoße gegen das Recht auf informationelle Selbstbestimmung.
entspreche nicht den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zur strafprozessualen akustischen Wohnraumüberwachung aufgestellt habe. Es fehle an kernbereichsschützenden Regelungen und Vorschriften zur Kennzeichnung der gewonnenen Daten.
verletze das Recht auf informationelle Selbstbestimmung, da es an einer Regelung über die Löschung personenbezogener Daten in den Sachakten fehle.
schließlich verstoße gegen das Trennungsgebot zwischen Geheimdiensten und Polizeibehörden und damit gegen das Rechtsstaatsprinzip.

III. Aus den Gründen

Die Verfassungsbeschwerden sind, soweit zulässig, weitgehend begründet. § 5 Abs. 2 Nr. 11 VSG ist in der zweiten dort aufgeführten Alternative verfassungswidrig und nichtig (I). Gleiches gilt für die erste Alternative dieser Norm (II). In der Folge der Nichtigkeit erledigen sich die gegen § 5 Abs. 3 und § 17 VSG gerichteten Rügen (III). Gegen § 5a Abs. 1 VSG bestehen hingegen keine verfassungsrechtlichen Bedenken (IV).
§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG, der den heimlichen Zugriff auf informationstechnische Systeme regelt, verletzt das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.
Diese Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist (1). Vorliegend sind die Eingriffe verfassungsrechtlich nicht gerechtfertigt: § 5 Abs. 2
Nr. 11 Satz 1 Alt. 2 VSG genügt nicht dem Gebot der Normenklarheit (2 a), die Anforderungen des Verhältnismäßigkeitsgrundsatzes sind nicht gewahrt (2 b) und die Norm enthält keine hinreichenden Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (2 c). Die angegriffene Norm ist nichtig (2 d). Einer zusätzlichen Prüfung anhand anderer Grundrechte bedarf es nicht (2 e).

§ 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG ermächtigt zu Eingriffen in das allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; sie tritt zu den anderen Konkretisierungen dieses Grundrechts, wie dem Recht auf informationelle Selbstbestimmung, sowie zu den Freiheitsgewährleistungen der Art. 10 und Art. 13 GG hinzu, soweit diese keinen oder keinen hinreichenden Schutz gewähren.
Das allgemeine Persönlichkeitsrecht gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen (vgl. BVerfGE 99, 185 <193> [BVerfG 10.11.1998 - 1 BvR 1531/96]; 114, 339 <346> [BVerfG 25.10.2005 - 1 BvR 1696/98]). Einer solchen lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann (vgl. BVerfGE 54, 148 <153> [BVerfG 03.06.1980 - 1 BvR 185/77]; 65, 1 <41>; BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2465>). Die Zuordnung eines konkreten Rechtsschutzbegehrens zu den verschiedenen Aspekten des Persönlichkeitsrechts richtet sich vor allem nach der Art der Persönlichkeitsgefährdung (vgl. BVerfGE 101, 361 <380> [BVerfG 15.12.1999 - 1 BvR 653/96]; 106, 28 <39> [BVerfG 27.06.2002 - 2 BvF 4/98]).Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.
Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.
Dies gilt zunächst für Personalcomputer, über die mittlerweile eine deutliche Mehrheit der Haushalte in der Bundesrepublik verfügt (vgl. Statistisches Bundesamt, Statistisches Jahrbuch 2007, S. 113). Die Leistungsfähigkeit derartiger Rechner ist ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen.
Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind.
Der Leistungsumfang informationstechnischer Systeme und ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Dies wird insbesondere aufgrund der gestiegenen Nutzung des Internet durch große Kreise der Bevölkerung mehr und mehr zum Normalfall.
Eine Vernetzung informationstechnischer Systeme ermöglicht allgemein, Aufgaben auf diese Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen. So können etwa die von einzelnen der vernetzten Systeme gelieferten Daten ausgewertet und die Systeme zu bestimmten Reaktionen veranlasst werden. Auf diese Weise kann zugleich der Funktionsumfang des einzelnen Systems erweitert werden.
Insbesondere das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Rechners nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er aktiv soziale Verbindungen aufbauen und pflegen kann. Zudem führen technische Konvergenzeffekte dazu, dass auch herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können (vgl. etwa zur Sprachtelefonie Katko, CR 2005, S. 189).
Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.
Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt

oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (vgl. zu den aus solchen Folgerungen entstehenden Persönlichkeitsgefährdungen BVerfGE 65, 1 <42>).
Bei einem vernetzten, insbesondere einem an das Internet angeschlossenen System werden diese Gefährdungen in verschiedener Hinsicht vertieft. Zum einen führt die mit der Vernetzung verbundene Erweiterung der Nutzungsmöglichkeiten dazu, dass gegenüber einem alleinstehenden System eine noch größere Vielzahl und Vielfalt von Daten erzeugt, verarbeitet und gespeichert werden. Dabei handelt es sich um Kommunikationsinhalte sowie um Daten mit Bezug zu der Netzkommunikation. Durch die Speicherung und Auswertung solcher Daten über das Verhalten der Nutzer im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden.
Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.
Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.
Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 <172> [BVerfG 20.06.1984 - 1 BvR 1494/78]; 106, 28 <35 [BVerfG 27.06.2002 - 2 BvF 4/98] f.>), nicht aber auch die Vertraulichkeit und Integrität von informationstechnischen Systemen.
Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden (vgl. BVerfGE 106, 28 <36>; 115, 166 <182>). Der Schutzbereich des Telekommunikationsgeheimnisses erstreckt sich danach auch auf die Kommunikationsdienste des Internet (vgl. zu E-Mails BVerfGE 113, 348 <383>). Zudem sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172> [BVerfG 20.06.1984 - 1 BvR 1494/78]; 85, 386 <396> [BVerfG 25.03.1992 - 1 BvR 1430/88]; 100, 313 <358> [BVerfG 27.04.1999 - 1 BvR 1613/94]; 107, 299 <312 f.>). Das Telekommunikationsgeheimnis begegnet in diesem Rahmen alten sowie neuen Persönlichkeitsgefährdungen, die sich aus der gestiegenen Bedeutung der Informationstechnik für die Entfaltung des Einzelnen ergeben. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme

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

© Verlag Deutsche Polizeiliteratur