Peter Schantz[1]

Verfassungsrechtliche Probleme von »Online-Durchsuchungen«

A. Einführung

Die Freiheit der Bürger ist in den letzten Jahren durch eine Vielzahl neuer Befugnisse der Ermittlungsbehörden eingeschränkt worden. Zur Begründung verweist man zunächst auf die verschärfte Bedrohungslage durch die Organisierte Kriminalität und jetzt durch den internationalen Terrorismus.[2] Ferner, so wird argumentiert, müsse der Staat seine Mittel dem technischen Fortschritt anpassen und dürfe keine »rechtsfreien Räume« entstehen lassen.[3] Zusätzlich führt der Wandel des Sicherheitsrechts vom Recht der punktuellen Gefahrenabwehr zu einer flächendeckenden Risikosteuerung dazu, dass der einzelne Bürger auch durch rechtmäßiges Verhalten nicht mehr verhindern kann, Ziel staatlicher Eingriffe zu werden.[4]

Vor diesem Hintergrund wird auch die aktuelle Diskussion um den heimlichen Fernzugriff auf Computer, die sog. »Online-Durchsuchung«, geführt. Zunächst ist die Befugnis zur »Online-Durchsuchung« auf Landesebene in Nordrhein-Westfalen im Rahmen einer Novelle des Verfassungsschutzgesetzes eingeführt worden (§ 5 Abs. 2 Nr. 11 VSG NRW).[5] Auf Bundesebene erwähnte das Programm zur Stärkung der Inneren Sicherheit (PSIS) vom Oktober 2006 zum ersten Mal Pläne zur Entwicklung der Voraussetzungen, um »entfernte PC auf verfahrensrelevante Inhalte hin durchsuchen zu können, ohne selbst am Standort des Gerätes anwesend zu sein«.[6] Die politische Diskussion um die Schaffung einer entsprechenden Rechtsgrundlage hat jedoch erst mit dem Beschluss des Bundesgerichtshofs vom 31. Januar 2007 begonnen, in dem der BGH feststellt, dass es im Rahmen der Strafprozessordnung keine Eingriffsermächtigung gibt, die eine »Online-Durchsuchung« legitimieren kann.[7] Anfragen an die Bundesregierung ergaben, dass diese meinte, im nachrichtendienstlichen Bereich durch die Generalklausel zur heimlichen Informationserhebung (z. B. § 9 Abs. 1, § 8 Abs. 2 BVerfSchG) über eine ausreichende Eingriffsermächtigung zu verfügen[8] und die »Online-Durchsuchung« über eine Dienstanweisung regeln zu können. In der Bundesregierung wird seitdem intensiv an einer gesetz-

---

1 Der Autor ist Rechtsanwalt in Berlin und wissenschaftlicher Mitarbeiter an der Humboldt-Universität zu Berlin (Lehrstuhl Prof. Dr. Hans-Peter Schwintowski). Er ist Prozessbevollmächtigter und Beschwerdeführer einer der Verfassungsbeschwerden gegen die Befugnis zur Durchführung von «Online-Durchsuchungen« nach § 5 Abs. 2 Nr. 11 VSG NRW.

2 Ähnlich *Schaar/Landwehr*, K&R 2007, 202 (202).

3 *Prantl*, in: Süddeutsche Zeitung vom 17. Februar 2007, S. 4.

4 *Volkmann*, JZ 2006, 918 (918 f.).

5 Landtag Nordrhein-Westfalen, Drucksache 14/2211.

6 Vgl. Programm zur Stärkung der Inneren Sicherheit, Anlage 2b; ausführlich hierzu *Gercke*, CR 2007, 245 (245 f.).

7 BGH vom 31. Januar 2007 – Az.: 18/16.

8 Antwort der Bundesregierung auf die schriftliche Frage des Abgeordneten Wolfgang Wieland vom 12. März 2007 sowie auf die Frage des Abgeordneten Hartfrid Wolf vom 12. März 2007.

lichen Grundlage für die »Online-Durchsuchung« gearbeitet. Unklar ist bisher jedoch, gegen welche Formen der Bedrohung und Kriminalität sie eingesetzt werden soll. Das Spektrum der Vorschläge reicht von der Terrorismusbekämpfung[9] über die Verfolgung von Computerkriminalität[10] bis hin zur Bekämpfung von »Umsatzsteuerkarussellen«.[11]

Im Folgenden soll untersucht werden, ob eine gesetzliche Regelung der »Online-Durchsuchung« mit dem Grundgesetz vereinbar ist. Nicht eingegangen wird dabei auf die Frage, ob eine mögliche Änderung des Grundgesetzes, wie sie Bundesinnenminister Wolfgang Schäuble vorschlägt,[12] mit Art. 79 Abs. 3 GG vereinbar wäre. Zunächst soll jedoch kurz die technische Seite der »Online-Durchsuchung« beleuchtet werden.

B. Technische Durchführung[13]

Es ist unklar, auf welche konkrete Art und Weise »Online-Durchsuchungen« von staatlichen Behörden durchgeführt werden sollen. Allerdings ist es aus den Erfahrungen mit Schadprogrammen und privater Spionagesoftware möglich, den Rahmen der technischen Möglichkeiten abzustecken. Nachrichtendienste und Strafverfolgungsbehörden werden sich derselben Techniken bedienen müssen, die Hacker verwenden. Grundsätzlich gibt es daher folgende Möglichkeiten, auf die Daten, die auf einem Rechner gespeichert sind, über das Internet zuzugreifen:[14]

Zunächst kann derjenige, der sich den Zugang zu Daten auf einem Rechner erschleichen will, auf eigenständige Programme zu diesem Zweck zurückgreifen. Hierbei ist zu unterscheiden zwischen *»Trojanern«* und *»Backdoor-Programmen«*. »Trojaner« sind eigenständige Programme, die sich getarnt als harmlose Programme oder Anwendungen in den Rechner des Benutzers einnisten. Je nach Programmierung speichern sie aufgerufene Dokumente und Emails, aber auch Passwörter, Kreditkartennummern oder bloße Tastatureingaben (sog. *Keylogger*) und leiten diese an eine vorbestimmte E-Mail-Adresse weiter; ferner können sie Telefonate mitschneiden, die über das Internet geführt werden. Treffender wäre es in diesem Zusammenhag daher, von der »Online-Überwachung« eines Rechners zu sprechen. Die Fähigkeiten von »Backdoor-Programmen« reichen noch erheblich weiter. Sie erlauben sogar die Fernsteuerung des Rechners, so dass der Täter durch sie andere Programme auf einem fremden Rechner starten, beliebig Dateien einsehen und auf seinen Rechner kopieren kann. Es ist sogar möglich, die Kamera und das Mikrophon eines Computers fernzusteuern und so den Raum, in dem der Computer steht, auszuspähen.[15]

---

9 Landtag Nordrhein-Westfalen, Drucksache 14/2211, S. 15 und 17.
10 So der Entwurf der bayrischen Landesregierung, BR-Drucksache 275/07.
11 *Kemper*, ZRP 2007, 105 (107).
12 Interview in der Welt am Sonntag vom 15. April 2007.
13 Siehe zu dieser Problematik den umfassenden und instruktiven Überblick von *Buermeyer*, HRRS, 2007, 154 ff. sowie *Gercke*, CR 2007, 245 ff.
14 Vgl. hierzu den instruktiven Überblick von *Graf*, in: Münchener Kommentar zum Strafgesetzbuch (2003), § 202a, Rz. 62 ff.; *Thomas Böckenförde*, Die Ermittlung im Netz (2003), S. 209-213; *Buermeyer*, HRRS 2007, 154 (157 ff.).
15 Eine solche Maßnahme wäre verfassungsrechtlich an den Voraussetzungen der Art. 13 Abs. 3 bzw. Abs. 4 GG zu messen und ist nicht Gegenstand der aktuellen Diskussion.

Eine andere Frage ist, wie diese Programme auf den Rechner der Zielperson gelangen.[16] *»Backdoor-Programme«* und *»Trojaner«* können dem Benutzer getarnt in harmlosen E-Mails zugesandt werden. Es ist aber auch möglich, durch geschicktes Ausnutzen der Gewohnheiten einer Person diese auf eine vorbereite Website zu locken. Dort wird im Hintergrund ein *»Wurm«* auf den Rechner geladen, der die Installation des »Trojaners« auf dem Zielrechner vornimmt. Diese Vorgehensweisen setzen – wenn auch im geringen Maße – eine *»Mithilfe«* der Zielperson voraus, da sie eine entsprechende Email öffnen bzw. die fragliche Website aufrufen muss, damit sich das Schadprogramm installieren kann. Ermittlungstaktisch wird man daher mittels *social engineering* versuchen, die Neugier der Zielperson zu wecken, indem man beispielsweise vorspiegelt, Absender der Email wäre der Arbeitgeber oder ein Bekannter der Zielperson.

Daneben gibt es die Möglichkeit, Programmfehler auszunutzen. Hierbei handelt es sich um Sicherheitslücken in Programmen, die dann den unbemerkten Zugriff auf einen Rechner, der an das Internet angebunden ist, ermöglichen. Problematisch an dieser Methode ist es, dass solche Sicherheitslücken nur für geringe Zeiträume bestehen, da die Softwarefirmen bemüht sind, diese zu schließen. Die Bundesregierung hat die Möglichkeit ausgeschlossen, in Zusammenarbeit mit den Softwarefirmen gezielt Sicherheitslücken vorzusehen, die den Ermittlungsbehörden den Zugriff erleichtern würden.[17] Schließlich könnte man die Schadsoftware im Datenstrom verstecken, der notwendigerweise zwischen dem Zielrechner und dem Internetprovider der Zielperson fließt, wenn sie sich in das Internet einwählt. Regelungstechnisch liegt es nahe, die Provider zu verpflichten, »eine Standardschnittstelle zur Einleitung von Überwachungssoftware«[18] zur Verfügung zu stellen. Gemäß Art. 11 TKÜV i.V.m. der technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation sind die Provider bereits jetzt verpflichtet, Standardschnittstellen für die Telekommunikationsüberwachung einzurichten.[19]

Unklar ist allerdings die Effektivität der »Online-Durchsuchung«, da auch sie ihre technischen Grenzen hat. Zum einen ist die Menge der Daten begrenzt, die über das Internet von einem Rechner kopiert werden kann. So würde es beispielsweise circa sechs Tage dauern, eine fünfzig Gigabyte große Festplatte komplett zu kopieren und über das Internet zu versenden.[20] Zum anderen können und sollten Computeranwender, die das Internet benutzen, ihre Rechner durch Firewalls und Antivirenprogramme schützen. Moderne Antivirenprogramme identifizieren Schadprogramme nicht mehr aufgrund ihrer spezifischen Signatur; sie gehen heuristisch vor und erkennen die Schadprogramme aufgrund ihres typischen Verhaltens.[21] Infolgedessen müssten sie von den Ermittlungsbehörden eingesetzte Schadprogramme ebenfalls erkennen kön-

16 Hierzu *Buermeyer,* HRRS 2007, 154 (163 ff.); *Gercke*, CR 2007, 245 (248 f.).
17 BT-Drucksache 16/4995, S. 2.
18 *Jürgen Schmidt*, heise security vom 11. März 2007, abrufbar unter http://www.heise.de/security/artikel/print/86415.
19 *Buermeyer*, HRRS 2007, 154 (164).
20 *Buermeyer,* HRRS 2007, 154 (164 f.).
21 *Buermeyer,*, HRRS 2007, 154 (158).

nen.[22] Hiergegen wird allerdings eingewandt, dass es möglich sei, mit ausreichend Zeit und Mitteln jedes Sicherheitssystem zu umgehen. Die Diskussion, ob »Online-Durchsuchungen« auch erfolgreich durchgeführt werden können, scheint daher noch nicht abgeschlossen zu sein.

C. Verfassungsrechtliche Zulässigkeit der «Online-Durchsuchung«

Eine gesetzliche Regelung der »Online-Durchsuchung« berührt den Schutzbereich der Unverletzlichkeit der Wohnung, des Fernemeldegeheimnisses, des Rechts auf informationelle Selbstbestimmung sowie des Kernbereichs privater Lebensgestaltung (hierzu I. bis IV.). Ferner stellen sich Fragen der Verhältnismäßigkeit (hierzu V.) und der Vereinbarkeit mit den allgemeinen Regeln des Völkerrechts im Sinne von Art. 25 S. 1 GG (hierzu VI.), die unabhängig von einem konkreten Regelungsentwurf erörtert werden können. Auf Fragen der Bestimmtheit und Normenklarheit[23] werde ich nur am Rande eingehen, da sie nur schwer losgelöst von einem konkreten Regelungsentwurf diskutiert werden können. Dies gilt ebenfalls für die Anforderungen an die Benachrichtigung der Betroffenen[24] und den Umgang mit den gewonnenen Daten.

I. Art. 13 Abs. 1 GG

Die umstrittenste Frage der verfassungsrechtlichen Bewertung von «Online-Durchsuchungen« ist, ob sie einen Eingriff in den Schutzbereich der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) darstellen, wenn sich der Zielrechner in einer Wohnung oder einem Geschäftsraum befindet.

1. Eingriff in die Unverletzlichkeit der Wohnung?

a) Schutzbereich des Art. 13 Abs. 1 GG

Auf einem Rechner gespeicherte Daten fallen in den Schutzbereich des Art. 13 Abs. 1 GG.[25] Dieses Grundrecht schützt die Unverletzlichkeit der Wohnung und gewährleistet dadurch für den Einzelnen einen im Hinblick auf seine Menschenwürde und die Entfaltung seiner Persönlichkeit elementaren Lebensraum. Die Wohnung ist ein Ort räumlicher Privatsphäre, in der er das Recht hat, in Ruhe gelassen zu werden.[26] Geschützt werden durch Art. 13 Abs. 1 GG auch Geschäftsräume.[27]

---

22 *Gercke*, CR 2007, 245 (249).

23 Vgl. zu diesem Punkt die Anforderungen, die das Bundesverfassungsgericht kürzlich in seiner Entscheidung zum NdsSOG aufgestellt hat, BVerfGE 113, 348 (375 ff.).

24 Hierzu umfassend BVerfGE 109, 279 (363 ff.); 100, 313, (364 ff.).

25 So auch *Kutscha*, NJW 2007, 1169 (1170 f.); *Schlegel*, HRRS 2007, 44 (48); *Bär*, MMR 2007, 239 (240); *Jahn/Kudlich*, JR 2007, 57 (59 f.); *Rux,* JZ 2007, 285 (292); *Schaar/Landwehr*, K&R 2007, 202 (204); a.A.: *Gercke*, CR 2007, 245 (250); *Beulke/Meininghaus*, StV 2007, 63 (64); *Hofmann*, NStZ 2005, 121 (124); Thomas *Böckenförde*, Die Ermittlung im Netz (2003), S. 224; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet (2000), S. 540 ff.

26 BVerfGE 115, 166 (196) m.w.N.

27 BVerfGE 32, 54 (68 ff.).

Der Schutz der räumlichen Privatsphäre erstreckt sich dabei nicht nur darauf, was in den Wohnräumen geschieht, sondern auch darauf, welche Informationen aus dem Bereich der Wohnung Dritten zugänglich sind.[28] Wie Art. 13 Abs. 2 GG einerseits sowie Art. 13 Abs. 3 bis Abs. 6 GG andererseits zeigen, schützt Art. 13 Abs. 1 GG vor allen Eingriffen von außen in diesen Raum der Privatsphäre – gleich, ob das Eindringen durch körperliches Betreten oder mittels technischer Vorrichtungen erfolgt:[29]

> *»Im Zeitpunkt der Schaffung des Grundgesetzes diente das Grundrecht des Art. 13 Abs. 1 GG primär dem Schutz des Wohnungsinhabers vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt. Seitdem sind neue Möglichkeiten für Gefährdungen des Grundrechts hinzugekommen. Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes 1 umfasst wäre.«*

Erfasst wird von diesem Schutz auch der Zugriff auf die in der Wohnung aufbewahrten Gegenstände durch besondere technische Mittel – nicht zuletzt besonders dann, wenn diese Gegenstände Informationen über den Wohnungsinhaber enthalten. Dies ergibt sich bereits aus Art. 13 Abs. 2 GG, der Möglichkeit der Durchsuchung. Diese Grundrechtsschranke wäre überflüssig, wenn das Grundrecht nur die Vorgänge innerhalb einer Wohnung, nicht aber auch Gegenstände innerhalb einer Wohnung schützen würde, die Auskunft über den Wohnungsinhaber geben. Eine Durchsuchung ist das ziel- und zweckgerichtete Suchen nach Sachen, die der Wohnungsinhaber von sich aus nicht offen legen will.[30] Der Wohnungsinhaber vertraut daher darauf, dass die Gegenstände, die sich innerhalb seiner Wohnung befinden, verglichen mit allen Gegenständen außerhalb davon, einen besonders hohen Schutz genießen, da sie sich innerhalb der durch Art. 13 Abs. 1 GG gewährleisteten räumlichen Privatsphäre befinden. Diese Erwägungen müssen erst recht für die »Online-Durchsuchung« gelten, weil diese von den Ermittlungsbehörden häufig anstelle einer physischen Durchsuchung durchgeführt werden wird, weil man sich davon ermittlungstaktische Vorteile verspricht.

Viele vertrauliche Informationen, die früher in körperlicher Form in der Wohnung aufbewahrt wurden und damit unstreitig in den räumlichen Schutzbereich der Wohnung fielen, werden heute auf dem heimischen Computer gespeichert und fallen daher ebenfalls in den Schutzbereich des Art. 13 GG.[31] Die fortschreitende technische Entwicklung darf daher nicht zu einer Absenkung des Niveaus des Grundrechtsschutzes führen. Dementsprechend schützt Art. 13 Abs. 1 GG auch Geräte, die innerhalb des

28 *Hermes*, in: Dreier, GG, 2. Auflage (2004), Art. 13, Rdn. 12.
29 BVerfGE 109, 279 (309).
30 Vgl. nur *Papier*, in: Maunz/Dürig, GG, 36. Lfg. (1999), Art. 13, Rz. 33 m.w.N.
31 So auch die Bundesministerin der Justiz *Brigitte Zypries* in ihrer Rede auf dem 10. Europäischen Polizeikongress am 13. Februar 2007, abrufbar unter www.bundesjustizministerium.de.

räumlichen Schutzbereiches der Wohnung installiert sind,[32] und vor der Suche nach gespeicherten Daten.[33] Ebenso entfaltet Art. 13 GG Schutzwirkung auch hinsichtlich der Erhebung, Speicherung und Verarbeitung von Daten im räumlichen Bereich der Wohnung[34] und über das Geschehen in der Wohnung.[35] So hat das Bundesverfassungsgericht in seiner Entscheidung zu den Handyverbindungsdaten vom 02. März 2006 festgestellt, dass der Zugriff auf diese Daten nicht nur am Recht auf informationelle Selbstbestimmung zu messen ist, sondern auch an Art. 13 Abs. 1 GG, wenn sie auf einem Datenträger innerhalb einer Wohnung gespeichert sind.[36]

Eine engere Interpretation würde gerade den Schutz einer räumlichen Privatsphäre durch Art. 13 GG weitgehend seiner Wirkkraft berauben und angesichts der Gewährleistungen der anderen Grundrechte (insbesondere des allgemeinen Persönlichkeitsrechts) funktionslos werden lassen. Art. 13 Abs. 1 GG schützt vielmehr die Beherrschbarkeit dieses Raumes der Privatsphäre durch den Bürger. Denn nur, wenn er selbst entscheiden kann, wer Zutritt zu diesem Bereich hat und welche Informationen über Vorgänge innerhalb der Wohnung und der darin befindlichen Gegenstände nach außen dringen, kann der Bürger sich selbst entfalten und den durch das Grundrecht gewährleisteten Rückzugsraum finden. Eine engere Interpretation stände ferner auch nicht mit der Entstehungsgeschichte der Norm im Einklang, bei deren Formulierung man sich der besonderen Anfälligkeit dieses Lebensbereiches für staatliche Eingriffe nach den geschichtlichen Erfahrungen der NS-Zeit besonders bewusst war.[37]

b) Grundrechtsverzicht durch Anschluss an das Internet?

Nicht überzeugend ist hingegen die Argumentation, durch die Verbindung mit dem Internet würde eine Person die auf ihrem Computer gespeicherten Daten für die Außenwelt öffnen und damit gewissermaßen auf ihren Grundrechtsschutz verzichten.[38] Ein Zugriff auf den Rechner des Bürgers ist nur unter Umgehung besonderer Sicherheitsvorkehrung und mithin missbräuchlich möglich. Allein die technische Möglichkeit des Zugriffs führt noch nicht dazu, dass der Bürger konkludent auf den grundrechtlichen Schutz verzichtet oder sich in die Sozialsphäre begibt. Entscheidend ist vielmehr, ob der Bürger begründetermaßen darauf vertrauen darf, dass die auf seinem Rechner gespeicherten Daten nur ihm zur Verfügung stehen und vertraulich sind. Mit einer Umgehung der Sicherheitsvorkehrungen seines Rechners in missbräuchlicher und straf-

32 BGH NStZ 1997, 247 (248); so auch der Beschluss des BGH vom 31. Januar 2007 – Az.: 18/06 –, Rz. 15. Der Senat setzt dies implizit voraus, wenn er erörtert, ob die Maßnahme als Durchsuchung oder als Wohnraumüberwachung einzuordnen ist.

33 BVerfGE 115, 166 (198 f.).

34 BVerfGE 51, 97 (105); *Papier*, in: Maunz/Dürig, GG, 36. Lfg. (1999), Art. 13, Rz. 148.

35 *Kunig,* in: von Münch/Kunig, GG, 5. Auflage (2000), Art. 13, Rd. 17.

36 BVerfGE 115, 166 (166), erster Leitsatz: »Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten werden nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt.«

37 BVerfGE 32, 54 (71).

38 In diese Richtung argumentiert *Hofmann*, NStZ 2005, 121 (124).

rechtlich relevanter Weise (vgl. nur § 202a StGB[39]) muss er ebenso wenig rechnen, wie der Benutzer eines Telefons mit dem Abhören des Telfongespräches rechnen müsste, ein Bürger des Schutzes des gesprochenen Wortes verlustig ginge, nur weil es möglich ist, dieses aufzuzeichnen, oder ein Bürger auf die Unverletzbarkeit seiner Wohnung verzichtet, nur weil er die Haustür offenlässt.[40] Folgte man dieser Argumentation, wäre der Grundrechtsschutz durch die technische Möglichkeit des Eingriffs in ein Grundrecht definiert und mithin vom Stand der Technik abhängig. Es gilt jedoch das Gegenteil: Wer Daten auf einem Personalcomputer in seiner Wohnung abspeichert, kann gerade davon ausgehen, dass diese Daten dort besonders sicher sind.[41] Seine Vertraulichkeitserwartung bleibt auch angesichts neuer technischer Eingriffsmöglichkeiten, die einen heimlichen Zugriff darauf ermöglichen, aus verfassungsrechtlicher Sicht besonders schützenswert.[42]

Diese Sichtweise steht auch mit den jüngsten Rechtsprechung des Bundesverfassungsgerichts im Einklang: Im Falle der Videoüberwachung eines öffentliches Platzes kann selbst dann nicht von einer Einwilligung des Bürgers in die Beeinträchtigung seiner Grundrechte ausgegangen werden, wenn der Eingriff offensichtlich ist und der Protest ausbleibt.[43] Übertragen auf die »Online-Durchsuchung« muss dies erst recht gelten, zumal die meisten Anwender Sicherheitsvorkehrungen gegen den Zugriff auf ihre Rechner nutzen.[44]

c) Gegenargumente: Zufälligkeit des Standortes des Rechners und fehlende Überwindung einer räumlichen Barriere

Auch andere Gegenargumente vermögen nicht zu überzeugen: So wird argumentiert, dass der Schutz eines Personalcomputers von seinem Standort abhänge, dieser aber aufgrund von tragbaren Computern und W-Lan-Netzen zunehmend zufällig sei.[45] Ferner wird vorgebracht, durch den Online-Zugriff würden gerade nicht die räumlichen Barrieren der Wohnung, die akustische, optische und körperliche Schranken für Beobachtungen von außen sind, überwunden werden.[46] Schließlich würde der Zugriff über das Internet die Stätte des räumlichen Lebens und Wirkens nicht beeinflussen.[47]

---

39 Vgl. *Graf*, in: Münchener Kommentar zum Strafgesetzbuch (2003), § 202a, Rz. 62 ff. Der Bundestag hat ferner am 25. Mai 2007 das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität beschlossen und sich darin den verschiedenen Formen des Hackings entgegengestellt, vgl. BT-Drucksache 16/3565.

40 Vgl. BVerfGE 106, 28 (40) zum Fall der heimlichen Aufzeichnung des gesprochenen Wortes.

41 *Sokol*, Landtag Nordrhein-Westfalen, Stellungnahme 14/0625, S. 10.

42 BVerfGE 65, 1 (42); 113, 29 (45 f.); 115, 320 (342, 350 f.) für das Recht auf informationelle Selbstbestimmung; BVerfGE 109, 279 (309) für Art. 13 GG.

43 BVerfG vom 23. Februar 2007 – Az.: 1 BvR 2368/06 – Rdn. 40.

44 Ähnlich *Kutscha*, NJW 2007, 1169 (1170).

45 *Thomas Böckenförde*, Die Ermittlung im Netz (2003), S. 224; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet (2000), S. 541 f.; *Beulke*/*Meininghaus*, StV 2007, 63 (64).

46 *Thomas Böckenförde*, Die Ermittlung im Netz (2003), S. 224; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet (2000), S. 541; *Gercke*, CR 2007, 245 (250).

47 *Thomas Böckenförde*, Die Ermittlung im Netz (2003), S. 224.

Diese Argumente stellen allein auf die Perspektive der Person ab, die von außen in die Wohnung eindringt. Sie vernachlässigen aber die Sichtweise des Bürgers: Dieser hat die Erwartung einer besonderen Vertraulichkeit, wenn er in seiner Wohnung seinen Computer benutzt. Es kann aus seiner Sicht keinen Unterschied machen, ob er einen Brief oder ein Tagebuch in Papierform aufbewahrt oder sie auf einer Festplatte speichert.[48] Jede andere Argumentation würde die Veränderung der technischen Möglichkeiten und kulturellen Gepflogenheiten nicht berücksichtigen und somit den Grundrechtsschutz verkürzen, nur weil der Bürger die technischen Möglichkeiten unserer Zeit nutzt.[49] Eine Verkürzung des Grundrechtsschutzes darf aber auch nicht durch den technischen Fortschritt auf Seiten der Eingriffsmöglichkeiten geschehen. Nur weil ein Zugriff auf Informationen in einer Wohnung nicht mehr das körperliche Eindringen in die Wohnung erfordert und damit für den Bürger im Verborgenen bleibt, führt dies nicht dazu, dass der Schutzbereich des Art. 13 Abs. 1 GG nicht berührt wird. Wäre dies der Fall, ständen die Grundrechte unter einem »Vorbehalt des technischen Fortschritts«. Darüber hinaus berücksichtigt dieses Argument nicht, dass Art. 13 Abs. 1 GG gerade einen Ort der Privatsphäre und Vertraulichkeit garantieren soll, an dem der Einzelne sich nicht nur mit anderen austauschen kann, sondern auch – unbeobachtet – den vielfältigen Möglichkeiten der Gestaltung des privaten Lebens alleine nachgehen kann. Hierzu gehört auch die Nutzung eines Personalcomputers und des Internets. Die für die Entstehung von Privatsphäre notwendige Vertraulichkeit geht jedoch verloren, wenn der Bürger befürchten muss, dass private Handlungen innerhalb seiner Wohnung von Personen, denen er keinen Zugang dazu gewährt hat, nachvollzogen oder aufgezeichnet werden können. Insoweit hat bereits die Möglichkeit der Datenerhebung von außen einen Einfluss auf die Vorgänge innerhalb der Wohnung und beeinträchtigt die private Lebensgestaltung darin.[50] Wie bereits die verfassungsrechtliche Möglichkeit der Überwachung mit technischen Mitteln (Art. 13 Abs. 3 bis 6 GG) zeigt, ist dieser Schutz umfassend gewährleistet und nicht nur gegenüber dem körperlichen Eindringen oder einer anderen Art der Überwindung einer räumlichen Barriere. Ob die Anschläge auf einer Tastatur von außerhalb einer Wohnung mittels eines Key-Logging-Programms, das diese aufzeichnet, oder aber mittels einer hochauflösenden Kamera beobachtet werden, kann im Ergebnis keinen Unterschied machen.

Die zunehmende Mobilität von Personalcomputern kann nicht zu einer Verkürzung des Grundrechtsschutzes der großen Mehrheit der Bürger führen, die ihren Computer weiterhin innerhalb ihrer Wohnung nutzen und diesem Umfeld eine entsprechend hohe Vertraulichkeitserwartung entgegenbringen.[51] Wenn Bürger ihren Computer auch außerhalb ihrer Wohnung nutzen können und dies Zweifel auf der Seite der Er-

48 Vgl. auch *Bär*, MMR 2007, 23 (240).

49 *Sokol*, Landtag Nordrhein-Westfalen, Stellungnahme 14/0625, S. 10.

50 Vgl. SächsVerfGH, JZ 1996, 957 (967).

51 Sogar für eine Übertragung der Schranken des Art. 13 auf einen Personalcomputer außerhalb der Wohnung plädiert *Rux*, JZ 2007, 285 (294). Hiergegen spricht allerdings, dass die Dogmatik zum Allgemeinen Persönlichkeitsrecht, dessen Ausfluss das Recht auf informationelle Selbstbestimmung ist, mit der Sphärentheorie ein hinreichendes Differenzierungsinstrument bereithält, um inhaltlich hochsensible Daten ausreichend zu schützen.

mittlungsbehörde erregt, wie der Standort eines Rechners eindeutig zu bestimmen ist, dürfen weder das Verhalten einzelner Bürger noch die Zweifel der Ermittlungsbehörden dazu führen, dass auch die Bürger, die ihren Rechner weiterhin in ihrer Wohnung oder ihren Geschäftsräumen nutzen, den Schutz des Art. 13 Abs. 1 GG verlieren.[52]

2. Rechtfertigung des Eingriffs

Folgt man der Ansicht, dass die »Online-Durchsuchung« ein Eingriff in den Schutzbereich der Unverletzlichkeit der Wohnung ist, stellt sich die Frage, ob dieser Eingriff gerechtfertigt sein kann. Dies ist nur dann der Fall, wenn die »Online-Durchsuchung« unter eine der Schrankenregelungen des Art. 13 Abs. 2-7 GG fällt, da der Verfassungsgeber alle Konfliktlagen mit anderen Verfassungsgütern abschließend geregelt hat.[53]

a) Durchsuchung (Art. 13 Abs. 2 GG)

Der heimliche Zugriff auf gespeicherte Daten ist keine Durchsuchung im Sinne des Art. 13 Abs. 2 GG. Eine Durchsuchung ist das »ziel- und zweckgerichtete Suchen staatlicher Organe in einer Wohnung, um dort planmäßig etwas aufzuspüren, was der Inhaber von sich aus nicht offen legen oder herausgeben will«.[54] Eine Durchsuchung erfordert danach das körperliche Betreten der Räume.[55] Eine »Online-Durchsuchung« erlaubt aber gerade einen Zugriff, der sich lediglich heimlicher technischer Mittel bedient und daher schon seinem äußeren Erscheinungsbild nach nicht als Durchsuchung einzuordnen ist, sondern als Einsatz technischer Mittel. Hierfür spricht auch, dass – in Abgrenzung zu den heimlichen Maßnahmen nach Art. 13 Abs. 3 bis 5 GG – Kennzeichen der Durchsuchung die Offenheit staatlichen Handelns ist.[56] Wie selbstverständlich dieses Verständnis des verfassungsrechtlichen Durchsuchungsbegriffs ist, zeigen die Erwägungen der drei abweichenden Richter im ersten G-10-Urteil, die eine heimliche Hausdurchsuchung nur im Wege der Verfassungsänderung für möglich hielten:

> *»So könnte Art. 13 dahin erweitert werden, dass unter bestimmten Voraussetzungen Hausdurchsuchungen ohne Zuziehung des Wohnungsinhabers oder dritter Personen vorgenommen (...) werden dürfen.«*[57]

---

52 Inwieweit auch Rechner außerhalb eines Geschäftsraumes oder einer Wohnung von Schutz des Art. 13 GG erfasst werden können, wäre unter Berücksichtigung des Schutzzwecks des Art. 13 GG eingehend zu diskutieren.

53 *Kunig*, in: von Münch/Kunig, GG, 5. Auflage (2000), Art. 13, Rdn. 23 m.w.N.; *Gusy*, DVBl.1991, 1288 (1292), a.A.: *Gornig*, in: von Mangoldt/Klein/Starck, GG, 5. Auflage (2005), Rdn. 148 und 170, der eine solche Möglichkeit für »außergewöhnliche Konfliktlagen« vorschlägt. Zur Kritik dieser Art von Argumentationsfiguren, die sich letztlich auf dem Gedanken des Staatsnotstandes gründen, siehe *Jahn,* Das Strafrecht des Staatsnotstandes (2004), S. 197 ff.

54 BVerfGE 76, 83 (89).

55 *Jarass*, in: Jarass/Pieroth, GG, 8. Auflage (2006), Art. 13, Rdn. 9; *Herdegen*, in: Bonner Kommentar zum Grundgesetz, 71. Lfg. (1993), Art. 13, Rz. 52; *Papier*, in: Maunz/Dürig, GG, 36. Lfg. (1999), Art. 13, Rz. 47; *Ziekow/Guckelberger*, in: Berliner Kommentar zum GG, 12. Ergänzungslieferung (2005), Art. 13, Rdn. 55 m.w.N sowie SächsVerfGH, JZ 1996, 957 (967) zu Art. 30 Abs. 2 der Sächsischen Verfassung.

56 *Gornig*, in: von Mangoldt/Klein/Starck, 5. Auflage (2005), GG, Art. 13, Rdn. 65.

57 BVerfGE 30, 1 (46 f.) - abweichende Meinung.

Auch die Überlegung, die Definition der Durchsuchung weiterzufassen, um neue technische Möglichkeiten zu berücksichtigen, führt nicht weiter. Dies würde nämlich den Grundrechtsschutz unter den Vorbehalt des technisch Machbaren stellen. Das Bundesverfassungsgericht betont dem gegenüber die gesteigerte Gefährdungslage aufgrund des technischen Fortschritts.[58]

Selbst wenn man einem solchen Interpretationsansatz folgen würde, würde er zu keinem anderen Ergebnis führen. Eine Interpretation der Eingriffsmöglichkeiten des Grundgesetzes im Lichte der technischen Entwicklung kann nicht dazu führen, dass diese qualitativ völlig neue Eingriffe erlauben. Genau dies wäre hier aber der Fall: Die klassische Durchsuchung und die Befugnis zur Durchsetzung einer »Online-Durchsuchung« unterscheiden sich nicht nur graduell voneinander, sondern qualitativ. Während sich der Bürger bei einer Durchsuchung mit einem offenen Eindringen in seine Privatsphäre konfrontiert sieht, lassen ihn die neuen Befugnisse in einer »Situation vermeintlicher Vertraulichkeit«.[59] Dementsprechend hat der Bundesgerichtshof in seinen Beschlüssen vom 25. November 2006 und 31. Januar 2007 im heimlichen Zugriff auf einen Computer keine Durchsuchung gesehen, da diese ein körperlicher und kein elektronischer Vorgang sei, und eine entsprechende Anwendung der §§ 102 ff. StPO abgelehnt.[60] Schon vom zugrunde liegenden Grundrechtsverständnis her nicht nachvollziehbar ist die Argumentation, der Online-Zugriff sei gegenüber der klassischen Durchsuchung sogar der vorzugswürdigere Eingriff, da die Durchsuchung der gesamten Wohnung ein schwererer Eingriff in die Privatsphäre sei.[61] Dieses Argument steht nicht mit der Rechtsprechung des Bundesverfassungsgerichts in Einklang, wonach die Heimlichkeit einer Maßnahme die Intensität des Grundrechtseingriffs erhöht.[62] Infolgedessen scheidet die Rechtfertigung einer »Online-Durchsuchung« als Durchsuchung im Sinne des Art. 13 Abs. 2 GG aus.

b) Akustische Wohnraumüberwachung (Art. 13 Abs. 3 GG) und technische Überwachungsmaßnahmen (Art. 13 Abs. 4 und 5 GG)

aa) Abgesehen von der Möglichkeit, mittels eines Online-Zugriffs das Mikrophon eines Computers zur Überwachung eines Raumes zu nutzen, fällt die «Online-Durchsuchung« nicht unter den Einsatz akustischer Mittel im Sinne des Art. 13 Abs. 3 GG. Ein Einsatz der »Online-Durchsuchung« für Zwecke der Strafverfolgung scheidet infolgedessen auf der Grundlage des geltenden Verfassungsrechts aus.[63]

58 BVerfGE 65, 1 (42); 113, 29 (45 f.); 115, 320 (342) für das Recht auf informationelle Selbstbestimmung; BVerfGE 109, 279 (309) für Art. 13 GG.

59 BVerfGE 107, 299 (321); BVerfGE 34, 238 (247).

60 BGH vom 25. November 2006 – Az. 1 BGs 184/2006; BGH vom 31. Januar 2007 – Az: StB 18/06.

61 So argumentiert *Hofmann*, NStZ 2005, 121 (124).

62 BVerfGE 115, 166 (194); 115, 320 (353).

63 So auch *Kudlich/Jahn*, JR 2007, 57 (60); *Schaar/Landwehr*, K&R 2007, 202 (205); Stellungnahme des Strafrechtsausschusses der Bundesrechtsanwaltskammer vom März 2007, BRAK-Stellungnahme 4/2007, S. 4.

bb) Aufgrund der Nutzung technischer Zugriffsmöglichkeiten auf Datenbestände ließe sich überlegen, »Online-Durchsuchungen« als Einsatz technischer Mittel im Sinne von Art 13 Abs. 4 und 5 GG einzuordnen; dann wäre der Einsatz dieses Instruments zumindest zu Zwecken der Gefahrenabwehr möglich. Wie sich aber bereits aus der Begründung der Verfassungsänderung ergibt, soll der Begriff »technische Mittel« gegenüber der akustischen Wohnraumüberwachung lediglich zusätzlich den Einsatz optischer Überwachungsmittel erlauben.[64] Die »Online-Durchsuchung« ist jedoch weder eine optische, noch eine akustische Überwachungsmaßnahme. Darüber hinaus sollen die technischen Mittel nach dem Wortlaut des Art. 13 Abs. 4 S. 1 GG der Überwachung *von* Wohnungen dienen. Man kann bezweifeln, ob dies auch den Zugriff auf Gegenstände und darauf gespeicherte Daten innerhalb der Wohnung erlaubt und nicht nur die Überwachung der aktuellen Vorgänge innerhalb der Wohnung.[65]

Selbst wenn man den Begriff der »technischen Mittel« entwicklungsoffen für technische Neuerungen ansehen würde, fiele die »Online-Durchsuchung« nicht darunter, denn durch eine »Online-Durchsuchung« werden nicht nur Kenntnisse über die aktuelle Nutzung des Computers gewonnen. Darüber hinaus erhält der Staat Zugriff auf Informationen über bereits abgeschlossene Geschehnisse und kann sich so sehr leicht ein umfassendes Bild über die Interessen, Neigungen und Gewohnheiten des Computernutzers machen, was einem Persönlichkeitsprofil sehr nahe kommen kann. Ein ähnlich umfangreiches Maß an Informationen lässt sich sogar durch eine sehr langfristig angelegte Überwachung einer Wohnung mit technischen Mitteln kaum gewinnen. Die «Online-Durchsuchung« stellt daher gegenüber den Eingriffen, die Art. 13 Abs. 3 bis 6 GG vorsehen, nicht nur eine Anpassung an den technischen Fortschritt dar, sondern einen qualitativ neuen Eingriff.

Neben der Frage, ob die «Online-Durchsuchung« überhaupt ein technisches Mittel im Sinne des Art. 13 Abs. 4 GG ist, ist es zweifelhaft, ob dieses Mittel dann den Verfassungsschutzbehörden zur Verfügung stehen würde, wie dies gerade die Novelle des nordrhein-westfälischen Verfassungsschutzgesetzes in § 5 Abs. 2 Nr. 11 VSG NRW vorsieht. Aus der Gesetzgebungsgeschichte ergibt sich nämlich, dass der verfassungsändernde Gesetzgeber Nachrichtendiensten gerade nicht den Einsatz technischer Mittel gestatten wollte.[66] Während der Entwurf des verfassungsändernden Gesetzes noch eine Sondervorschrift für den Verfassungsschutz vorsah,[67] wurde diese Reglung vom verfassungsändernden Gesetzgeber nicht übernommen.

c) Sonstiger Eingriff gemäß Art. 13 Abs. 7 GG

Eine Rechtfertigung der »Online-Durchsuchung« kommt daher nur unter den engen Voraussetzungen des Art. 13 Abs. 7 GG zur Gefahrenabwehr überhaupt in Betracht.

64 BT-Drucksache 13/8650, S. 5; ebenso *Papier*, in: Maunz/Dürig, GG, 36. Lfg. (1999), Art. 13, Rz. 89; hiervon geht auch *Frank Braun*, NVwZ 2000, 375 (376) wie selbstverständlich aus, a.A.: *Kutscha*, NJW 2007, 1169 (1170).

65 *Jahn/Kudlich,* JR 2007, 57 (60).

66 *Baldus*, NVwZ 2003, 1289 (1292 f.); *Werthebach/Droste*, in: Bonner Kommentar zum Grundgesetz, Art. 73 Nr. 10, Rz. 232; a.A.: *Rux*, JZ 2007, 285 (294).

67 Vgl. BT-Drucksache 13/8650, S. 3.

Es ist jedoch sehr sonderbar, dass die Auffangregelung des Art. 13 Abs. 7 GG einen Eingriff legitimieren können soll, der aufgrund der weitaus engeren Voraussetzungen von Art. 13 Abs. 2 bis 6 GG nicht zulässig wäre. Dabei handelt es sich bei der »Online-Durchsuchung« sogar um einen schwereren Eingriff, als die Maßnahmen, die Art. 13 Abs. 2 bis 6 GG vorsehen. Es ist daher zu überlegen, ob ein Rückgriff auf Art. 13 Abs. 7 GG überhaupt zulässig ist, wenn es sich – wie im Falle der »Online-Durchsuchung« – um eine Maßnahme handelt, die von ihrer Eingriffsintensität her den Maßnahmen entspricht, die Art. 13 Abs. 2 bis 6 GG regeln, oder diesen Maßnahmen bereits von ihrem äußeren Erscheinungsbild her sehr nahe kommt, ohne unter eine dieser Regelungen zu fallen.

3. Zwischenergebnis

Eine »Online-Durchsuchung« greift in den Schutzbereich der Wohnung zumindest dann ein, wenn sich der Zielcomputer in einer Wohnung oder einem Geschäftsraum befindet. Die Schrankenregelungen des Art. 13 GG sind nicht geeignet, eine »Online-Durchsuchung« zum Zwecke der Strafverfolgung zu rechtfertigen. Im Bereich der Gefahrenabwehr erscheint lediglich ein Rückgriff auf Art. 13 Abs. 7 GG möglich. Unabhängig von ihrer sonstigen verfassungsrechtlichen Bewertung kann eine »Online-Durchsuchung« im Rahmen der Strafverfolgung nur durchgeführt werden, wenn Art. 13 GG entsprechend geändert werden würde.[68] Es ist fragwürdig, ob eine solche Änderung des Grundgesetzes mit Art. 79 Abs. 3 i.V.m. Art. 1 Abs. 1 GG vereinbar wäre.[69]

II. Art. 10 GG

Möglicherweise berührt der Zugriff auf die Daten eines Computers über das Internet nicht nur den Schutzbereich des Art. 13 Abs. 1 GG und des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), sondern auch des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG).

1. Auslegung des Schutzbereichs des Fernmeldegeheimnisses durch den Zweiten Senat

Nach der Rechtsprechung des Zweiten Senats des Bundesverfassungsgerichts schützt Art. 10 GG die Vertraulichkeit des Kommunikationsvorganges (»Privatheit auf Distanz«). Dadurch soll der Bürger so gestellt werden, wie er bei der Kommunikation unter Anwesenden stünde, auch wenn er sich im Falle der Kommunikation über Distanz Kommunikationsmittlern anvertrauen muss.[70] Dieses besondere Schutzbedürfnis sei nicht mehr gegeben, sobald der Kommunikationsvorgang abgeschlossen ist, und sich

68 So auch Bundesinnenminister *Schäuble* im Handelsblatt vom 05. April 2007.

69 Vgl. zu den entsprechenden Argumenten in der Diskussion um die Vereinbarkeit von Art. 13 Abs. 3 bis Abs. 6 GG mit Art. 79 Abs. 3 GG *Raum/Palm,* JZ 1994, 447 (451 f.).

70 Auf der Linie dieser Rechtsprechung liegt auch der Beschluss der 1. Kammer des Zweiten Senats des Bundesverfassungsgerichts zum IMSI-Catcher, BVerfG vom 22. August 2006 – Az.: 2 BvR 1345/03 – Rdn. 50 ff.

die Kommunikationsdaten und -inhalte in der beherrschbaren Privatsphäre des Bürgers befinden. Denn dann könne ein unbemerkter Zugriff Dritter in der Regel nicht mehr stattfinden; die Daten unterschieden sich nicht mehr von anderen vom Bürger angelegten Datensätzen.[71] Empfangene Emails würden danach grundsätzlich ebenso wenig in den Schutzbereich des Art. 10 Abs. 1 GG fallen wie Daten, in keinerlei Zusammenhang mit der Kommunikation mit anderen Personen stehen.

Es sind allerdings auch einzelne Fallkonstellationen möglich, in denen der Zugriff auf gespeicherte Daten – auch nach dieser Interpretation – ein Eingriff in das Fernmeldegeheimnis ist. Dies wäre etwa dann der Fall, wenn ein Gespräch über Internettelefonie (Voice-over-IP) mitgehört, eine Email automatisch weitergeleitet oder der Abruf von einem externen Email-Server beobachtet werden würde.[72] Diese Fälle sind vergleichbar mit dem Abhören am Endgerät, eine Maßnahme, die nach der Rechtsprechung des Gerichts ein Eingriff in das Fernmeldegeheimnis ist.[73] Wenn eine solche Konstellation vorliegt, wird sie nicht nur vom Schutzgehalt des Art. 10 Abs. 1 GG, sondern auch des Rechts auf informationelle Selbstbestimmung sowie des Rechts auf Unverletzlichkeit der Wohnung erfasst, denn diesen Grundrechten kommt jeweils ein eigenständiger Schutzgehalt zu.

2. Stellungnahme und Kritik

Die Abgrenzung der Schutzbereiche des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung in der jüngeren Rechtsprechung des Zweiten Senats des Bundesverfassungsgerichts fordert Kritik heraus. Durch Art. 10 Abs. 1 GG sollen nicht nur die konkreten Kommunikationsinhalte und -vorgänge, sondern auch die Bedingungen einer freien Kommunikation aufrechterhalten werden.[74] Zu den Bedingungen freier Kommunikation gehört auch, empfangsbereit für eingehende Kommunikationsvorgänge wie Emails oder Telefonate zu sein;[75] dies ist eine notwendige Voraussetzung für das Zustandekommen jeglicher moderner Fernmeldekommunikation. Muss der Bürger jedoch befürchten, dass Ermittlungsbehörden den durch die Empfangsbereitschaft eröffneten Zugang – etwa die Einwahl in das Internet zum Empfang von Emails – für den Online-Zugriff ausnutzen, wird sich dies auf sein Kommunikationsverhalten negativ auswirken und den freien Meinungs- und Informationsaustausch über das Internet beeinträchtigen.[76] Dementsprechend erschöpft sich ein

71 Vgl. BVerfGE 115, 166 (181 f.).

72 Zu dieser Frage liegt dem Bundesverfassungsgericht ebenfalls eine Verfassungsbeschwerde vor (2 BvR 902/66), vgl. Stellungnahme des Strafrechts- und des Verfassungsrechtsausschusses der Bundesrechtsanwaltskammer, BRAK-Stellungnahme Nr. 1/2007; *Schlegel*, HRRS 2007, 44.

73 BVerfGE 115, 166 (186 f.).

74 BVerfGE 100, 313 (359).

75 Anders die 3. Kammer des Zweiten Senates des Bundesverfassungsgerichts in ihrem Beschluss zum IMSI-Catcher, BVerfG vom 22. August 2006 – Az.: 2 BvR 1345/03 – Rdn. 61.

76 So auch *Nachbaur*, NJW 2007, 335 (337); *Schenke*, AöR 125 (2000), 1 (20 f.); vgl. zum Abschreckungseffekt auch BVerfGE 65, 1 (43); 93, 181 (188).

Fernzugriff auf einen Rechner über das Internet nicht in einem Eingriff in die Schutzbereiche des Art. 13 Abs. 1 und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; vielmehr kommt dem Fernmeldegeheimnis hier eine eigenständige Freiheitsgarantie zu.[77]

III. Kernbereich privater Lebensgestaltung (Art. 1 Abs. 1 GG)

1. Umfang des Kernbereichs privater Lebensgestaltung

Im Rahmen der verdeckten Ausforschung der auf einem Personalcomputer gespeicherten Daten kann der Kernbereich privater Lebensgestaltung in vielfältiger Weise tangiert werden. Diese spezielle Grundrechtsverbürgung wird nicht durch Art. 13 Abs. 1 GG verdrängt.[78] Beispiele hierfür sind auf dem Personalcomputer gespeicherte Tagebuchaufzeichnungen, private Photos, medizinische Unterlagen oder Kommunikation mit engsten Vertrauten[79] (hier spricht eine Vermutung dafür, sie ihrem Inhalt nach zum Kernbereich privater Lebensgestaltung zu zählen). Gleiches gilt für die Korrespondenz mit einem Strafverteidiger.[80]

Zuerst in der Tagebuch-Entscheidung, aber auch im Urteil zum »Großen Lauchangriff« hat das Bundesverfassungsgericht den Kernbereichsschutz jedoch abhängig vom konkreten Inhalt begrenzt: So würden Äußerungen, Emails oder Tagebuchaufzeichnungen mit Bezug zu konkreten Straftaten nicht in den Kernbereich privater Lebensgestaltung fallen, da sie einen Sozialbezug aufwiesen.[81] Sieht man den Kernbereich privater Lebensgestaltung als Teil der Menschenwürde an,[82] kann man an dieser Rechtsprechung zweifeln. Die Menschenwürde ist, sofern man nicht neueren Interpretationsansätzen[83] folgen will, unantastbar und der Abwägung mit anderen Verfassungsrechtsgütern nicht zugänglich.[84] Das Bundesverfassungsgericht führt hier jedoch verdeckt eine Abwägung zwischen der Menschenwürde und dem Verfassungsgut der effektiven Strafrechtspflege durch.[85]

2. Maßnahmen zum Schutz des Kernbereichs privater Lebensgestaltung

Der Kernbereich privater Lebensgestaltung ist Teil der unantastbaren Menschenwürde (Art. 1 Abs. 1 GG); eine Rechtfertigung eines Eingriffs in diesen Bereich scheidet daher von vornherein aus. Der hohe Stellenwert der Menschenwürde verpflichtet den Staat ferner, wie das Bundesverfassungsgericht im Urteil zum sog. »Großen Lau-

77 So im Ergebnis auch *Bär*, MMR 2007, 239 (240); ähnlich für das Verhältnis von Art. 10 und Art. 13 GG *Gusy*, in: von Mangoldt/Klein/Starck, GG, 5. Auflage (2005), Art. 13, Rdn. 101.

78 Vgl. BVerfGE 115, 166 (187 f.).

79 BVerfGE 109, 279 (317, 321 f.).

80 BVerfGE 109, 279 (148).

81 BVerfGE 109, 279 (319); 80, 367 (375).

82 So ausdrücklich BVerfGE 109, 279 (319).

83 *M. Herdegen*, in: Maunz/Dürig, Grundgesetz (42. Lfg., Stand: Februar 2003), Art. 1 Abs. 1, Rdn. 43 ff.; überzeugende Kritik an diesem Ansatz übt *Ernst-Wolfgang Böckenförde*, Blätter für deutsche und internationale Politik 2004, 1216 ff.

84 *Niels Petersen*, KJ 2004, 316 (319) m.w.N.

85 Dies zeigt sich besonders deutlich in den Erwägungen der Tagebuch-Entscheidung, vgl. BVerfGE 80, 367 (373 ff.).

schangriff« und den Folgeentscheidungen festgestellt hat, wirksame Schutzmechanismen zu treffen, um einen Eingriff in den Kernbereich privater Lebensgestaltung zu verhindern. Hierzu gehören mindestens gesetzliche Regelungen, die bereits vor der Durchführung der Maßnahme darauf zielen zu verhindern, dass ein Eingriff in den Kernbereich stattfindet, und die Prognosenentscheidung der Behörde regeln, wann davon auszugehen ist, dass eine Überwachungsmaßnahme den Kernbereich privater Lebensgestaltung berührt.[86] Ferner muss der Gesetzgeber für den Fall, dass dennoch Informationen aus dem Kernbereich privater Lebensgestaltung erfasst werden, gewährleisten, dass diese nicht ausgewertet, sondern unverzüglich gelöscht werden.[87]

Schließlich muss eine gesetzliche Reglung vorsehen, dass die gewonnenen Daten durch eine unabhängige Stelle gesichtet werden, die sicherstellt, dass keine Informationen aus dem unantastbaren Kernbereich privater Lebensgestaltung verwertet werden.[88] Im Widerspruch zu dieser Voraussetzung, die der Erste Senat im Urteil zum »Großen Lauschangriff« aufgestellt hat, scheint der Nichtannahmebeschluss der 3. Kammer des Zweiten Senates vom 11. Mai 2007 zu stehen. Diese vertrat die Ansicht, dass die Regelung des § 107c Abs. 7 S. 1 StPO mit dem Grundgesetz vereinbar sei. Nach dieser Vorschrift hat die Staatsanwaltschaft einen Beurteilungsspielraum, ob sie die Entscheidung eines Gerichts über die Verwertbarkeit der Informationen herbeiführt.[89] Dieser Beschluss übersieht, dass die Überprüfung durch eine unabhängige Stelle nicht vom Willen der Ermittlungsbehörde abhängen darf, wenn sie einen effektiven Kernbereichsschutz durch Löschungspflicht und Verwertungsverbot gewährleisten soll und zugleich ein Ausgleich für die fehlenden Rechtsschutzmöglichkeiten des Betroffenen in diesem Verfahrensstadium sein soll. Ein wirksamer Kernbereichsschutz setzt vielmehr voraus, dass eine unabhängige Stelle die gewonnenen Daten auf ihre Kernbereichsrelevanz untersucht, bevor die Ermittlungsbehörden Zugriff erhalten. Eine solche Regelung lässt sich gerade für die »Online-Durchsuchung« leicht verwirklichen, darf jedoch kein Ersatz für Vorkehrungen dafür sein, dass kernbereichsrelevante Daten gar nicht erst erhoben werden.[90]

IV. Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)

Grundsätzlich verdrängen die speziellen Grundrechtsgewährleistungen der Art. 10 und 13 GG das Recht auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht hat aber betont, dass Art. 10 und Art. 13 GG den Schutz des allgemeinen Persönlichkeitsrechts, dessen Ausprägung das Recht auf informationelle Selbstbestimmung ist, punktuell verstärken können, wenn dem Recht auf informationelle Selbstbestim-

86 Zuletzt BVerfG vom 11. Mai 2007 – 2 BvR 543/06 – Rdn. 39; grundlegend BVerfGE 109, 279 (318 ff.).
87 BVerfGE 109, 279 (331 ff.); 113, 348 (391 f.).
88 so ausdrücklich BVerfGE 109, 279 (334).
89 BVerfG vom 11. Mai 2007 – 2 BvR 543/06 – Rdn. 65 f.
90 Wie *Niels Petersen*, KJ 2004, 316 (326) treffend feststellt, findet die Verletzung der Menschenwürde nicht erst durch die Verwertung, sondern bereits durch die staatliche Kenntnis dieser Informationen statt.

mung eine eigenständige Freiheitsgarantie zukommt, die über die Überwindung der räumlichen Grenzen der Privatsphäre hinausgeht.[91]

Durch die »Online-Durchsuchung« eines Computers erhält der Staat umfassenden Zugang zu den darauf gespeicherten Daten. Diese Daten geben nicht nur Auskunft über Vorgänge im geschützten Bereich der räumlichen Privatsphäre, sondern besitzen auch einen darüber hinausgehenden Aussagegehalt. Der Staat erhält mit dem Datenzugang ein umfassendes Bild etwa darüber, wie der Bürger das Internet nutzt, mit wem er per Email geschäftlich oder privat kommuniziert oder welche Bankgeschäfte er abschließt. Die Informationen geben über die Neigungen, Interessen und Gewohnheiten des Bürgers Auskunft und erlauben dadurch nahezu die Erstellung eines umfassenden Persönlichkeitsprofils.[92] Im Falle eines so schweren Eingriffs in das Recht auf informationelle Selbstbestimmung kommt dieser Grundrechtsgewährleistung gegenüber dem Fernmeldegeheimnis und dem Schutz der Unverletzlichkeit der Wohnung ein eingeständiger Schutz zu, so dass Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nicht von den spezielleren Freiheitsgewährleistungen verdrängt wird.

V. Verhältnismäßigkeit

Unabhängig davon, ob man neben dem Recht auf informationelle Selbstbestimmung noch die speziellen Grundrechtsgarantien der Art. 13 Abs. 1 und Art. 10 Abs. 1 GG für anwendbar hält, muss sich eine gesetzliche Regelung der »Online-Durchsuchung« am Grundsatz der Verhältnismäßigkeit messen lassen.

1. Geeignetheit und Erforderlichkeit

Angesichts der Möglichkeit der Betroffenen, Gegenmaßnahmen gegen »Online-Durchsuchung« zu ergreifen,[93] bestehen bereits Zweifel an der Geeignetheit der Maßnahme, zur Gefahrenabwehr oder der effektiven Strafverfolgung beizutragen.

Fraglich ist aber auch, ob die »Online-Durchsuchung« überhaupt erforderlich ist und dieselben Ziele nicht auch mit den bisherigen Eingriffsbefugnissen, wie der Telekommunikationsüberwachung oder einer physischen Durchsuchung und Beschlagnahme des Rechners erreicht werden können.[94] Soweit lediglich auf die Verlagerung der Kommunikation auf das Internet verwiesen wird,[95] überzeugt dies nicht, da bereits mittels der herkömmlichen Telekommunikationsüberwachung ein staatlicher Zugriff stattfinden kann.[96] Von Seiten der Behörden werden die ermittlungstaktischen Vorteile

91 BVerfGE 115, 166 (187 f.).
92 Vgl. BVerfGE 115, 166 (189 f.). Dort geht das Gericht auch auf die Bedeutung des Personalcomputers ein.
93 Die Erwägungen des Bundesverfassungsgerichts in BVerfGE 109, 279 (337) zeigen, dass dieser Punkt für die Frage der Geeignetheit der Maßnahme relevant sein kann.
94 Zweifel hieran hat auch die Bundesjustizministerin geäußert, vgl. auch ihre Rede auf dem 10. Europäischen Polizeikongress am 13. Februar 2007, abrufbar unter www.bundesjustizministerium.de.
95 So z.B. die Begründung des Verfassungsschutzgesetzes Nordrhein-Westfalen, Landtag Nordrhein-Westfalen, Drucksache 14/2211, S. 15 und 17 f.
96 Vgl. hierzu *Löffelmann*, AnwBl. 2006, 598 (599 f.).

der »Online-Durchsuchung« betont, da sie heimlich stattfindet und den Verdächtigen damit nicht warnt. Ferner wird auf Probleme der Ermittlungsbehörden mit der Verschlüsselung von Daten mittels kryptographischer Verfahren hingewiesen; die »Online-Durchsuchung« soll den Behörden die Möglichkeit geben, die Kommunikation dann »mitzulesen«, wenn der Empfänger sie entschlüsselt hat. Schließlich sei es möglich, die Nutzung eines Rechners kontinuierlich zu überwachen, was auch den Zugriff auf extern gespeicherte Daten ermöglichen würde.[97] Im Rahmen des Gesetzgebungsverfahrens bedarf es einer intensiven Diskussion darüber, ob diese Vorteile in der Realität notwendig und alternativlos sind. Dies ist bisher noch nicht dargelegt worden.

2. Angemessenheit

Zweifelhaft ist vor allem aber die Angemessenheit der »Online-Durchsuchung«. Angemessen ist nämlich nur ein Eingriff, dessen Schwere bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der rechtfertigenden Gründe steht.[98] Wie das Bundesverfassungsgericht zuletzt in der Entscheidung zur Rechtmäßigkeit der Rasterfahndung betont hat, kann dies dazu führen, dass Maßnahmen, die durchaus zum Schutz eines Rechtsgutes geeignet und erforderlich sind, unterbleiben müssen, weil sie zu stark in die Rechte der Bürger eingreifen.[99]

a) Zweck des Eingriffs

Eine effektive Strafverfolgung und Gefahrenabwehr sind Rechtsgüter von hohem verfassungsrechtlichem Gewicht. Es ist unbestritten, dass sich die zuständigen Behörden an den technischen Fortschritt anpassen müssen, um diese Ziele weiterhin gewährleisten zu können.[100]

b) Schwere des Eingriffs

Die »Online-Durchsuchung« ist ein besonders schwerwiegender Eingriff, denn sie wird regelmäßig zu Konflikten mit dem Kernbereich privater Lebensgestaltung (Art. 1 Abs. 1 GG) führen, da sich auf den meisten Computern kernbereichsrelevante Daten befinden werden. Ferner berührt sie Daten, die aufgrund des besonderen Schutzes der Art. 13 und 10 GG unter einer besonderen Vertraulichkeitserwartung des Bürgers stehen.[101]

Es ist auch zu berücksichtigen, dass sich aufgrund des technischen Fortschritts das Gewicht bestimmter Grundrechtseingriffe erhöht. So werden der Personalcomputer und das Internet für viele Tätigkeiten des privaten und beruflichen Lebens genutzt. Eine einzelne Überwachungsmaßnahme an diesem Punkt erlaubt daher unter Umständen die Erfassung aller Neigungen, Interessen und Tätigkeiten eines Bürgers, so dass sich ein nahezu komplettes Persönlichkeitsprofil erstellen lässt.[102] Ist eine Überwachungsmaß-

97 *Buermeyer*, HRRS 2007, 154 (160 ff.).
98 BVerfGE 115, 320 (345 f.) m.w.N.
99 BVerfGE 115, 320 (345 f.).
100 Vgl. BVerfG vom 22.08.2006 – Az: 2 BvR 1345/03 – Rz. 75.
101 Vgl. BVerfGE 115, 320 (348); 108, 279 (313 f.); 113, 348 (364 f., 383, 391).
102 Vgl. BVerfGE 115, 166 (189 f., 193).

nahme so umfassend, verstößt sie nach Ansicht des Bundesverfassungsgerichts sogar gegen die Menschenwürde.[103] Dementsprechend ist es unzulässig, die gesamte Festplatte eines Rechners auszulesen,[104] zumal hierdurch große Mengen von Daten ohne Verfahrensrelevanz erhoben werden würden.[105] Zu beachten ist zusätzlich, dass die »Online-Durchsuchung« häufig in Kombination mit anderen Überwachungsmaßnahmen durchgeführt werden wird. Hier ist der Gesetzgeber verpflichtet, besonders schwerwiegende Belastungen durch »additive Grundrechtseingriffe« zu verhindern.[106]

Die Schwere des Eingriffs wird durch seine Heimlichkeit weiter erhöht. Der Betroffene kann somit sein Verhalten nicht mehr anpassen und der Durchführung der Maßnahme entgegentreten, indem er Rechtsschutz sucht.[107] Hinzu kommt der vom Bundesverfassungsgericht immer wieder zurecht hervorgehobene Abschreckungseffekt, der bereits von der Möglichkeit der Vornahme der »Online-Durchsuchung« ausgeht und die Bürger veranlasst, ihre Freiheit selbst zu beschränken, wenn sie nicht mehr sicher sein können, wer sie beobachtet und wer welche Informationen über sie besitzt.[108]

c) Drittbetroffene

Zu berücksichtigen ist ferner, dass die Maßnahme entgegen der ersten Vermutung eine hohe Streubreite aufweist und zu einer hohen Zahl von Drittbetroffenen führt.[109] Ursache hierfür ist die Benutzung eines Rechners durch mehrere Personen, wie sie unvermeidlich bei der Benutzung eines Internetcafes, eines Computerpools einer Universität oder des Familiencomputers auftritt. Zum anderen ist es sehr schwierig, den Zielrechner allein anhand seiner IP-Adresse zu identifizieren.

d) Zwischenergebnis

Wägt man die Schwere des Eingriffs und den verfolgten Zweck miteinander ab, überwiegen die Argumente, die dafür sprechen, die »Online-Durchsuchung« für nicht verhältnismäßig im engeren Sinne anzusehen. Hält man eine verfassungskonforme Ausgestaltung dennoch für möglich, muss eine gesetzliche Regelung der »Online-Durchsuchung« zumindest die Voraussetzungen erfüllen, die das Bundesverfassungsgericht für die Eingriffsschwellen bei der akustische Wohnraumüberwachung aufgestellt hat; d.h. eine »Online-Durchsuchung« ist nur zulässig zur Bekämpfung schwerer Kriminalität[110] und setzt einen auf Tatsachen gegründeten Verdacht voraus.[111] Ein Einsatz zur Gefahrenabwehr erscheint nur zur Abwehr von Gefahren für Verfassungsrechtsgüter von hoher Bedeutung zulässig.[112]

---

103 BVerfGE 109, 279 (323).
104 BVerfGE 115, 166 (199).
105 Vgl. BVerfGE 113, 29 (53, 54 f.).
106 BVerfG vom 12. April 2005 – Az.: 2 BvR 581/01 – Rz. 60 ff.; zu dieser grundrechtsdogmatisch neuen Figur siehe auch *Gregor Kirchhof*, NJW 2006, 732; *Lücke*, DVBl. 2001, 1469.
107 BVerfGE 115, 166 (194); 115, 320 (353).
108 BVerfGE 65, 1 (43); 100, 313 (381); 113, 29 (46).
109 Vgl. BVerfGE 115, 320 (354); 100, 313 (376, 392); 109, 279 (353); 113, 348 (383).
110 BVerfGE 109, 279 (343 ff.).
111 BVerfGE 109, 279 (350 f.).
112 Vgl. BVerfGE 115, 320 (360 f.).

VI. Art. 25 GG

Eine besondere Herausforderung für den Gesetzgeber wird es sein, eine Regelung zu finden, die mit den allgemeinen Regeln des Völkerrechts (Art. 25 S. 1 GG) im Einklang steht. Eine »Online-Durchsuchung« deutscher Behörden kann nämlich leicht in Konflikt mit der territorialen Souveränität eines anderen Staates geraten. Aufgrund der transnationalen Struktur des Internets ist es weder voraussehbar, wo sich der Zielrechner befindet, mit dem sich die beobachtete Person ins Internet einwählt, noch von wo die Email abgerufen werden wird, die das Schadprogramm auf den Rechner tragen soll. Die Zielperson kann dies von ihrer heimischen Wohnung in Deutschland aus tun, aber auch von einem Internetcafe in Washington aus. Für die deutschen Ermittlungsbehörden ist der Unterschied kaum erkennbar.

Wird jedoch auf einen Rechner zugegriffen, der sich physisch im Ausland befindet, verletzt die Bundesrepublik Deutschland die Souveränität des ausländischen Staates. Ausfluss der territorialen Souveränität eines Staates ist nämlich das Verbot gegenüber anderen Staaten, ohne Zustimmung oder Duldung des betroffenen Staates auf dessen Staatsgebiet Hoheitsakte zu setzen.[113] Dies umfasst insbesondere das Verbot der heimlichen Durchführung von Hoheitsakten.[114] Diese Regeln sind Teil der allgemeinen Regeln des Völkerrechts im Sinne des Art. 25 S. 1 GG[115] und binden unmittelbar den deutschen Gesetzgeber (Art. 25 S. 2 GG). Auch eine «Online-Durchsuchung« von Rechnern im Ausland verstößt dementsprechend gegen diese allgemeine Regel des Völkerrechts.[116]

Unerheblich ist es in diesem Zusammenhang, ob der Zugriff auf einen Rechner, der sich im Ausland befindet, bewusst erfolgt oder die Verletzung der Souveränität des anderen Staates nicht intendiert war.[117] Der Eingriff in die territoriale Unversehrtheit eines anderen Staates ist ein völkerrechtliches Delikt und setzt weder Fahrlässigkeit noch Vorsatz voraus. Auch eine Rechtfertigung ist nur in den engen Grenzen des Völkerrechts möglich; diese finden sich nach dem momentanen Stand des Völkergewohnheitsrechts in der VN-Resolution zur Staatenverantwortlichkeit von 2001[118] (insb. Art. 20 ff. und Art. 49 ff.). In der Literatur wird teilweise vorgeschlagen, es sei zwischen der Souveränität des einen Staates und dem Interesse des ermittelnden Staates an der effektiven Wahrnehmung seiner Hoheitsgewalt abzuwägen. Die Pflicht, die fremde Gebietshoheit zu respektieren, dürfe nicht dazu führen, dass der Staat auf die Ausübung der eigenen Gebietshoheit übermäßig verzichte.[119] Diese These kann sich auf keine der Rechtsquellen des Völkerrechts i.S.d. Art. 38 IGH-Statut stützen und muss daher als rein rechtspolitische Äußerung betrachtet werden. Es gibt keine Anzei-

113 Allgemein hierzu *Epping/Gloria*, in: Ipsen, Völkerrecht, 5. Auflage (2004), § 23, Rz. 69 ff.
114 *Epping/Gloria*, in: Ipsen, Völkerrecht, 5. Auflage (2004), § 23, Rz. 72.
115 Vgl. BVerfGE 63, 343 (361).
116 *Wolfgang Bär*, Der Zugriff auf Computerdaten im Strafverfahren (1992), S. 235 f. mit jeweils weiteren Nachweisen.
117 Vgl. *Christoph Engel*, MMR Beilage 4/2003, S. 8.
118 Anlage der Resolution der VN-Generalversammlung Nr. 56/83 vom 12. Dezember 2001.
119 *Germann*, Gefahrenabwehr und Strafverfolgung im Internet (1999), S. 644 ff.

chen, dass die völkergewohnheitsrechtlichen Zuständigkeitsreglungen im Bereich des Internets von den allgemeinen Regeln der Gebietshoheit abweichen würden. Gerade die schleppende Ratifikation der Cybercrime-Convention, die nur eine geringe Einschränkung territorialer Souveränität erlaubt, zeigt, dass die Staaten auch in diesem Regelungsbereich an der klassischen Auffassung territorialer Souveränität festhalten.

Da der Einsatz der »Online-Durchsuchung« gerade im Zusammenhang mit der Bekämpfung der internationalen Kriminalität und des Terrorismus vorgeschlagen wird, ist der Konflikt mit der Hoheitsgewalt fremder Staaten voraussehbar, und damit die irreparable Verletzung fremder Hoheitsrechte vorprogrammiert. Der nordrhein-westfälische Gesetzgeber hat sogar klargestellt, dass er von einer Anwendung der »Online-Durchsuchung« auf Computer im Ausland ausgeht.[120] Der Grundsatz der Völkerrechtsfreundlichkeit[121] kann sich nicht in einer völkerrechtskonformen Auslegung innerstaatlichen Rechts, lediglich auf Computer mit Standort im Inland zuzugreifen, und der Pflicht zur Korrektur begangener Völkerrechtsverstöße[122] erschöpfen, wenn die Verletzung des Völkerrechts vorprogrammiert ist. Er gebietet vielmehr, von solchen Maßnahmen Abstand zu nehmen oder aber Regelungen für ein Verfahren zu treffen, das solche vorsehbaren Verstöße gegen allgemeine Regeln des Völkerrechts verhindert.

D. Rechtspolitische Bewertung

Der Gesetzgeber würde mit der Einführung der »Online-Durchsuchung« die Belastungsgrenzen der Verfassung überschreiten. In Nordrhein-Westfalen hat er dies bereits getan. Selbst wenn man die »Online-Durchsuchung« für verfassungsrechtlich zulässig halten sollte, bedeutet dies noch nicht, dass sie eine rechtspolitisch angemessene Maßnahme ist, da das Grundgesetz nur die äußersten Grenzen des staatlichen Handelns festlegt.

Es sprechen auch aus rechtspolitischer Sicht überzeugende Argumente dafür, von dieser neuen Ermittlungsmethode Abstand zu nehmen. Die »Online-Durchsuchung« ist ein drastischer Grundrechtseingriff. Der Computer nimmt im Privat- und Berufsleben vieler Bürger eine so zentrale Stellung ein, dass er prägnant als »ausgelagertes Gehirn«[123] des Bürgers bezeichnet werden kann. Ein einzelner Zugriff erlaubt es daher dem Staat, sich Daten in einem Umfang zu sichern, welche nahezu die Erstellung eines Persönlichkeitsprofils erlauben. Muss der Bürger aber mit solchen Eingriffen rechnen, wird dies das Vertrauen der Bürger im Umgang mit von Computern und dem Internet erheblich verringern. Dies gilt umso mehr, als der Staat, der auf der einen Seite

120 Vgl. Landtag von Nordrhein-Westfalen, Drucksache 14/2211, S. 18. Dies zeigt sich auch deutlich durch den Verweis auf BVerfGE 100, 313 (363); an dieser Stelle der G-10-Entscheidung setzte sich das Verfassungsgericht mit der rechtlichen Bewertung von Ferngesprächen ins Ausland auseinander.

121 Hierzu allgemein *Jarass*, in Jarass/Pieroth, GG, Art. 25, Rz. 4 m.w.N.

122 BVerfGE 112, 1 (26).

123 *Burkhard Hirsch*, zitiert nach DER SPIEGEL, 6/2007, S. 18.

IT-Sicherheit und E-Government fördert, sich gerade der Mittel von »Hackern« bedient, die er gleichzeitig kriminalisiert und ächtet.[124] Zu bedenken ist auch das Missbrauchsrisiko, da die »Hintertüren« der Computer der Bürger nicht nur Sicherheitsbehörden, sondern auch Kriminellen offen stehen.[125] Die Folgen eines Vertrauensverlustes der Bürger in die Sicherheit der Informationstechnologien verursachen nicht nur volkswirtschaftliche Schäden, sondern führen auch zu einer Einbuße an Freiheit, denn die Bürger werden bestimmte Nutzungsmöglichkeiten ihrer Computer nicht mehr wahrnehmen. Hierin verwirklicht sich der Abschreckungseffekt, den das Bundesverfassungsgericht seit dem Volkszählungsurteil immer wieder hervorgehoben hat.[126] Dies aber verändert nicht nur schleichend das gesellschaftliche Klima, sondern auch die Funktionsbedingungen einer freiheitlichen demokratischen Gesellschaft.[127]

124 Vgl. Entschließung des 73. Datenschutzkongresses des Bundes und der Länder vom 8./9. März 2007; vgl. hierzu auch das Strafrechtsergänzungsgesetz zur Bekämpfung der Computerkriminalität (BT-Drucksache 16/3656), das der Bundestag am 24. Mai 2007 beschlossen hat.

125 *Schaar/Landwehr*, K&R 2007, 202 (205).

126 BVerfGE 65, 1 (43).

127 Ähnlich auch BVerfGE 65, 1 (43).