

Dr. Thomas Böckenförde, Köln*

Auf dem Weg zur elektronischen Privatsphäre

Zugleich Besprechung von BVerfG, Urteil v. 27. 2. 2008 – „Online-Durchsuchung“¹

Der Beitrag analysiert das Urteil des BVerfG zur sogenannten Online-Durchsuchung. Außer der dogmatischen Aufarbeitung werden auch Folgefragen für die Rechtsanwendung sowie für die aktuellen Gesetzgebungsvorhaben beleuchtet.

I. Worum es geht

Online-Durchsuchung. Dies war wahrscheinlich eines der am meisten öffentlich diskutierten Worte des Jahres 2007, auch wenn es bei der Wahl „Wort des Jahres“ nur auf dem 8. Platz landete, und das auch nur indirekt.² Die Entscheidung des *BGH* vom Januar 2007,³ der die dort in Rede stehende Online-Durchsuchung mangels Rechtsgrundlage für rechtswidrig erklärte, und die Ankündigung des Bundesinnenministers, dann werde man jetzt eben zügig eine Rechtsgrundlage schaffen,⁴ waren Startschuss für die heftige öffentliche Diskussion. Diese gewann dadurch an Dynamik, dass stets etwas unklar blieb, welche technischen Maßnahmen sich hinter der geplanten Online-Durchsuchung genau verbergen, was also der Staat damit vorhabe und warum dies überhaupt notwendig sei. Diese Unklarheit hielt eine, teils notgedrungen spekulative, Diskussion über das technisch Mögliche und Machbare am Laufen. Der politische Diskurs wurde angetrieben durch ein Tauziehen zwischen Innen- und Justizministerium über das rechtlich Zulässige und Gebotene, er gipfelte August 2007 darin, dass beide Häuser nicht mehr am Kabinetttisch oder in Gremien, sondern über einen formellen Fragenkatalog kommunizierten.⁵

In diesem Umfeld richteten sich im Oktober 2007 die Augen wieder auf den Karlsruher Aeropag, diesmal hin zum *BVerfG* und der dort anberaumten mündlichen Verhandlung. Nun war es nicht die vom Generalbundesanwalt beantragte Maßnahme der Online-Durchsuchung, die es juristisch anhand der StPO zu bewerten galt, sondern es ging um das zur Online-Durchsuchung ermächtigende neue nordrhein-westfälische Verfassungsschutzgesetz, welches auf seine Vereinbarkeit mit der Verfassung hin zu überprüfen war. Damit hatten zum erstenmal originäre Sachverhalte des „Cyberspace“ direkt und unmittelbar das Verfassungsgericht erreicht.

Fragen des im anglo-amerikanischen Rechtskreis so benannten Cyberlaw, hier einmal frei mit Netzrecht übersetzt,

begannen in Deutschland in der zweiten Hälfte der 1990er Jahre langsam an Raum zu gewinnen. Es waren zunächst Gesichtspunkte der insbesondere strafrechtlichen und urheberrechtlichen Verantwortung und Haftung im Netz, die den Ausgangspunkt der Querschnittsmaterie Netzrecht⁶ bildeten. Schnell kamen Markenrecht, Zivilrecht, Datenschutzrecht, internationales Privat-, Straf- und Urheberrecht sowie Strafprozessrecht hinzu. Inzwischen kennt fast jedes Rechtsgebiet Bezugspunkte zu Netzsachverhalten. Es ist nun jedoch der „Ermittlung im Netz“,⁷ und nicht der „Verantwortlichkeit im Netz“ vorbehalten, den Topos für erste grundlegende verfassungsrichterliche Überlegungen zu Cyberlaw und Cyberspace zu bilden.

Im Februar 2008 kam es zur mit großer Spannung erwarteten Verkündung der Entscheidung. Heraus kam ein umfänglich begründetes Urteil, das nicht nur zum Streitgegenständlichen Verfassungsschutzgesetz Stellung bezog, sondern dieses als Ausgangspunkt zur Entwicklung normativer Maßstäbe für ein, von der Presse nahezu euphorisch gefeiertes,⁸ neues Grundrecht⁹ verwendete. Inzwischen haben sich die Wogen geglättet, der mühsame politische Prozess der legislativen Umsetzung hat begonnen.

Man mag manches an dem Urteil kritisieren: In der Begründung bleibt einiges ungereimt und unausgeführt, rechtlich wie technisch. Viele im Vorfeld gestellte Fragen wurden beantwortet, dafür jedoch mindestens ebenso viele neue aufgeworfen. Dies per se als Kritik zu formulieren, hieße die Dialektik des juristischen Erkenntnisprozesses zu verkenne. Allerdings ist dieser Prozess auch noch notwendig, um dem neuen Grundrecht stärkere Konturen zu verleihen und es etwas praxistauglicher zu machen. Zu begrüßen ist, dass in das Dickicht des öffentlichen Diskurses nun verfassungsrechtliche Schneisen geschlagen sind, die die Diskussion anhand bestimmender Begriffe und Leitsätze kanalisieren und schon dadurch voranbringen. In einem hat das *BVerfG* bereits jetzt Maßstäbe gesetzt: Durch die Art und Weise, wie es sich mutig, in einer für deutsche Gerichte nicht immer selbstverständlichen Aufgeschlossenheit, dem Dialog mit der (Informations-)Technik gestellt hat. Wahrscheinlich hat das Gericht seit seinem Bestehen in keinem Verfahren so viele technische Auskunftspersonen einbezogen. Es ist zu

* Der Autor ist Rechtsanwalt in Köln. Für weiterführende Hinweise dankt er herzlich Herrn Richter *Ulf Buermeyer*, Berlin.

¹ Abrufbar unter: www.bundesverfassungsgericht.de; Az. 1 BvR 370/07, 1 BvR 595/07.

² Als Teil der Definition der dort platzierten Wortschöpfung „Bundestrojaner“. Die Pressemitteilung vom 7.12.2007 der die Auszeichnung „Wort des Jahres“ verleihenden Gesellschaft für deutsche Sprache (GfdS) liest sich zum Wort Nr. 8 Bundestrojaner so: „Bundestrojaner ist die kritische Bezeichnung für die Absicht der Behörden, durch ein Computerprogramm die elektronische Kommunikation zu überwachen (Online-Durchsuchung)“. Bundestrojaner als Bezeichnung einer Absicht?

³ *BGH*, Beschluss v. 31.1.2007 – StB 18/06 = JZ 2007, 796 mit Anm. *Cornelius*.

⁴ Am Tag der Verkündung des Beschlusses, vgl. hierzu etwa *FAZ* v. 6.2.2007, S. 1 „Heimliche Online-Durchsuchung unzulässig“.

⁵ Vgl. Fragenkatalog des BMJ an das BMI v. 22.8.2007.

⁶ Unter Netzrecht wird hier kein eigenständiges Rechtsgebiet, sondern eine Bündelung der rechtlichen Fragen verstanden, die ihren rechtsstatsächlichen Ausgangspunkt in der technischen Vernetzung von Computersystemen und den darüber interagierenden Anwendungsdiensten (WWW, News-, Mail-, Chat-Dienste etc.) nehmen. Netzrecht kann nach deutsch-rechtlicher Nomenklatur als Teil des Informationsrechts begriffen werden, das seinerseits als Querschnittsmaterie seinen rechtsstatsächlichen Ausgangspunkt in der Digitalisierung von Information und den damit verbundenen Rechtsfragen findet. Vgl. grundlegend zum Informationsrecht bereits vor fast 20 Jahren: *Sieber* NJW 1989, 2569 ff.

⁷ So *T. Böckenförde*, „Die Ermittlung im Netz“, 2003; vgl. auch Rn. 310 des Urteils.

⁸ Vgl. z. B. „Schritt von historischer Dimension“ (*Der Spiegel*, 3.3.2008, S. 42), „Meilenstein in der juristischen Bewältigung der Herausforderungen der technisch-wissenschaftlichen Moderne“ (*FAZNet* v. 27.2.2008); „Juristische und gesellschaftspolitische Sensation“ (*sueddeutsche.de* v. 27.2.2008).

⁹ „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.

hoffen, dass dieses Bemühen um technisches Verständnis nicht nur die weitere Diskussion, sondern auch Wissenschaft, Rechtsprechung, Gesetzgebung und Praxis beeinflussen wird.

II. Raum und Räumlichkeit

1. Die Firewall ist keine Wohnungswand

Die in der Literatur nach dem *BGH*-Urteil zur Online-Durchsuchung aufgekommene Diskussion hatte ihren verfassungsrechtlichen Schwerpunkt schnell gefunden: Art. 13 GG und der Schutz der räumlichen Privatsphäre. Im Kern ging es um folgende Frage: Greift eine Online-Durchsuchung, hier zunächst einmal verstanden als Infiltration und Ausspähung der Speichermedien eines Computers über Netzverbindungen, dann in die Unverletzlichkeit der Wohnung ein, wenn sich der durchsuchte Computer in einer Wohnung befindet? Die Diskussion war vielstimmig und relativ ausgeglichen, eine herrschende Meinung hatte sich noch nicht herausgebildet.¹⁰

Blickt man zunächst unbefangen auf den Computer in einer Wohnung, kann man sich in der Tat fragen: Wenn sich ein Computer in der Wohnung befindet, warum ist er dann nicht vom Schutzbereich der Wohnung umfasst, wenn über das Netz auf ihn zugegriffen wird? Hat denn nicht, worauf sich die Anwendbarkeit des Art. 13 GG bejahenden Stimmen berufen,¹¹ das *BVerfG* in seinem Verdikt zum großen Lauschangriff festgestellt, dass es für ein Eindringen in die Wohnung nicht darauf ankommt, ob diese körperlich betreten wird oder Ermittlungsbeamte in der Wohnung körperlich anwesend sind,¹² und ist nicht gerade deshalb auch die unkörperliche Online-Durchsuchung des Computers in der Wohnung am Maßstab des Art. 13 GG zu messen? Folgender, vom Verfasser vor einer halben Dekade entwickelter Begründungsansatz mag deutlich machen, warum dies abzulehnen ist: In den Schutzbereich der Wohnung wird nur dann eingedrungen, wenn die eine Wohnung umgebenden räumlichen Barrieren (Wände, Decken, ggf. Boden) auf die Art und Weise überwunden werden, in der sie den Schutzbereich der Wohnung als Ort des unbeobachteten Rückzugs konstituieren:¹³ Als physisches, optisches, akustisches, ggf. auch olfaktorisches Wahrnehmungshindernis, das den Bewohner von der Außenwelt abschirmt.

Es ist die Abschirmungsfunktion der Wohnungswände vor äußeren Einblicken, anhand derer sich der Schutzbereich der Wohnung als Hort des Rückzugs überhaupt erst bestimmen lässt. Diese „Abschirmung der Privatsphäre in räumlicher Hinsicht“ entspricht der ständigen Rechtsprechung des *BVerfG*,¹⁴ sie wurde jüngst in der Entscheidung zum großen Lauschangriff noch einmal ähnlich wie hier begründet.¹⁵ Der

unkörperliche Zugriff über physikalische (drahtgebundene oder drahtlose) Netze auf den Computer, überwindet, anders als die unkörperliche optische oder akustische Wohnraumüberwachung, keine durch Wände, Decken oder Boden geschaffenen Wahrnehmungshindernisse. Zudem: Die Online-Durchsuchung nimmt weder Einfluss auf, noch observiert sie das durch die räumliche Privatsphäre geschützte, vertrauliche Geschehen (Gespräche, Handlungen etc.) in der Wohnung.¹⁶ Die „im“ Computer abgespeicherten Informationen sind nicht durch räumlichen Barrieren gegen den Netzzugriff von außen geschützt. Sondern es ist die auf dem Computer installierte Software, wie etwa eine Firewall,¹⁷ die Hindernisse für die Online-Infiltration des Computersystems darstellt. Indes: Die Firewall ist keine Wohnungswand.

2. Die Entscheidung des *BVerfG*

Das *BVerfG* hat entschieden. Eher am Rande, in insgesamt nur 5 von 167 Absätzen der Begründung, hat es sich Art. 13 GG angenommen und damit den vielfältigen Bemühungen in der Literatur, Netzermittlungen als in Räume eindringend anzusehen, eine Absage erteilt. Kurz und bündig hat das Gericht, in der Struktur seiner Begründung wie hier, auf den Eingriffsvorgang („Zugriffsmodalität“) abgestellt: „Art. 13 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet“ (Rn. 154).¹⁸ Festgestellt wurde weiterhin, dass es die Abgrenzung der Wohnung ist, also ihre Wände, Boden, Decke, welche die räumliche Privatsphäre vermittelt. „Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt“ (Rn. 154). Damit bleibt festzuhalten: Der Cyberspace, wiewohl er – den Raum im Namen tragend – einen Raum sui generis bildet, unterteilt und gliedert sich selbst nicht mehr anhand räumlicher Kategorien der hier verstandenen Art. Die Ermittlung im Netz dringt nicht in Räume ein.

Was wäre die Konsequenz gewesen, hätte sich die verfassungsrechtliche Rechtsprechung an der Auflösung des räumlichen Schutzbereiches beteiligt? Der Kern des Schutzbereiches von Art. 13 GG wäre korrodiert. Das in diese Richtung zielende Bemühen der Literatur war kreativ: So wurde zum Beispiel mit Hilfe einer dem deutschen Verfassungsrecht systemfremden analogen Auslegung der Schutzbereich des Art. 13 GG vom „dreidimensionalen“ Raum auf „virtuelle“ Räume und damit einen Bereich außerhalb der Wohnung erweitert;¹⁹ oder es wurde entlang des Verhältnismäßigkeitsgrundsatzes der Schutzbereich des Art. 13 GG auf außerhalb der Wohnung befindliche Computer ausgedehnt.²⁰ Diese und all die anderen, den Schutzbereich Wohnung ver-

¹⁰ Vgl. hierzu nur, ohne Anspruch auf Vollständigkeit: Für die Anwendbarkeit des Art. 13 GG auf die Online-Durchsuchung: *Beukelmann* StraFo 2008, 1 ff.; *Buermeyer* RDV 2008, 8 ff.; *Hornung* DuD 2007, 575 ff.; *Jahn/Kudlich* JR 2007, 57 ff.; *Rux* JZ 2007; *Schaar/Landwehr* K&R 2007, 202, 204; *Schantz* KritV 2007, 343 ff. Gegen die Anwendbarkeit: *Beulke/Meininghaus* StV 2007, 63 ff.; *Cornelius* JZ 2007, 798 ff.; *Gercke* CR 2007, 245 ff.; *Hoffmann* NSz 2005, 121 ff.; *Schlegel* GA 2007, 648 ff. Vor dieser Diskussion schon: *T. Böckenförde* (Fn. 7), S. 219, 223 f. Diese Frage offen lassend etwa *Kutscha* NJW 2007, 1169 ff.; *Warntjen* JURA 2007, 581 ff.

¹¹ Siehe hierzu vorige Fn.

¹² So *BVerfGE* 109, 279, 309.

¹³ *T. Böckenförde* (Fn. 7), S. 219, 223 f.; mit dieser Begründung auch *Gercke* CR 2007, 245, 250.

¹⁴ Vgl. nur *BVerfGE* 32, 54/72; 65, 1, 40.

¹⁵ Indem dort festgestellt wurde, dass eine Wohnraumüberwachung nur dann einen Eingriff darstelle, soweit sie „solche innerhalb der Wohnung

stattfindenden Vorgänge erfasst, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind“ *BVerfGE* 109, 279, 309.

¹⁶ Anders verhält es sich, wenn der Computer zu einer Observationsplattform für daran angeschlossene Peripheriegeräte (Webcam, Mikrofone) umfunktioniert wird. In diesem Fall ist, ähnlich wie bei der akustischen und optischen Wohnraumüberwachung, Art. 13 GG anwendbar.

¹⁷ Eine Firewall ist eine Software, die den durch einen Computer laufenden Datenverkehr überwacht und anhand vorher festgelegter Regeln entscheidet, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht.

¹⁸ Alle in Klammern angegebenen Randnummern im Text beziehen sich auf die Absätze der amtlichen Textfassung des Urteils (Fn. 1).

¹⁹ *Rux* JZ 2007, 285, 294. Die von *Rux* dargelegten Argumente zur Begründung der Analogie werden in der Erweiterung von *Hornung* JZ 2007, 828, 829 f. überzeugend widerlegt.

²⁰ *Hornung* JZ 2007, 828, 830 f. entwickelt dann in seiner Erwiderung eine eigene Lösung für das von ihm konstatierte Problem, dass die Ermittlungsbehörden beim Online-Zugriff nicht erkennen können, ob sich der

lassenden Begründungen hatten im Wesentlichen eine Stoßrichtung: Den hohen Schutzstandard²¹ des Art. 13 GG auf nach jeweiliger Ansicht vergleichbar schutzbedürftige Sachverhalte zu erstrecken.

Es mag gute Gründe geben, die Online-Durchsuchung des Computers innerhalb der Wohnung als einen ähnlich schutzbedürftigen Eingriff zu empfinden wie etwa die akustische oder optische Wohnraumüberwachung, und, darauf aufbauend, den Zugriff auf den Computer innerhalb der Wohnung als ähnlich schutzbedürftig zu empfinden wie den Zugriff auf den Computer außerhalb der Wohnung. Jedoch, soweit die Diskussion auf dieser Ebene der vergleichbaren Schutzbedürftigkeit verharret, ohne die Wände der Wohnung als schutzbereichsbegründend zu begreifen, bricht das letzte belastbare Kriterium der Abgrenzung von Art. 13 GG zu Art. 2 Abs. 1 GG weg. Damit wäre auch die Frage, ob bei Sachverhalten ähnlicher Art der verfassungsändernde Gesetzgeber, wie bei Art. 13 GG, oder das *BVerfG*, wie bei Art. 2 Abs. 1 GG, für die an Gesetzesvorbehalte zu stellenden Maßstäbe zuständig wäre, allein anhand des schwer rationalisierbaren Kriteriums des „zur Wohnung vergleichbar Schutzbedürftigen“ zu entscheiden. Dies hätte ohne Not dem verfassungsrichterlichen Dezisionismus ein weiteres Anwendungsfeld eröffnet.

III. Online-Durchsuchung

1. Schutzbereich des neuen Grundrechts

a) Grundrecht von Anfang an

Unklar bleibt, warum am Anfang der Begründung das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ (GViiS) zum einen als Ausprägung eines anderen Grundrechts, nämlich des Allgemeinen Persönlichkeitsrechts (APKR), bestimmt, dann aber gleich im nächsten Atemzug selbst zum eigenständigen Grundrecht emporgehoben wird (Rn. 166). Den Titel „Grundrecht“ hat etwa das „Recht auf informationelle Selbstbestimmung“, ein als Konkretisierung des APKR entwickeltes Recht, nicht schon in seiner „Geburtsurkunde“, dem Urteil zur Volkszählung,²² sondern erst 22 Jahre später verliehen bekommen.²³ Andere Ausprägungen des APKR, wie etwa das Recht am eigenen Bild oder das Recht am gesprochenen Wort,²⁴ wiewohl bedeutend älter, wurden die Grundrechtsweihen bisher noch nicht verliehen. Mangels entgegenstehender Anhaltspunkte im Urteil ist davon auszugehen, dass die Verleihung des Grundrechtstitels nicht mit besonderen Rechtsfolgen verbunden ist.²⁵

Computer in der Wohnung befindet oder nicht, entlang des Verhältnismäßigkeitsgrundsatzes. Er kommt zu dem Ergebnis, dass beim Online-Zugriff im Zweifel auch außerhalb der Wohnung stehende Computer vom Schutz des Art. 13 GG umfasst sind.

21 Gemeint ist damit der aus der Unverletzlichkeitsformel abgeleitete Maßstab, dass Eingriffe in die Wohnung nur unter den strengen geschriebenen Voraussetzungen der Absätze 2–7 des Art. 13 GG möglich sind.

22 *BVerfGE* 65, 1 ff.

23 Soweit ersichtlich in *BVerfGE* 115, 166, 188.

24 Recht am eigenen Bild: *BVerfGE* 97, 228, 268; Recht am gesprochenen Wort: *BVerfGE* 34, 238, 246 f.

25 Die Bezeichnung „neues Grundrecht“ ist zutreffend und mehr als ein Schlagwort. So wurde mit dem GViiS eine neue Ausprägung des APKR kreiert, mit eigenem Schutzbereich und eigenen qualifizierten Eingriffsvoraussetzungen ausgestattet und als Grundrecht bezeichnet. Soweit eingewandt wird, dass nicht das Gericht, sondern nur der Gesetzgeber neue Grundrechte schaffen kann, so ist dies nur bedingt richtig. Denn das *BVerfG* bestimmt im Rahmen seiner letztverbindlichen Interpretationskompetenz selbst die – ohnehin fließenden – Grenzen zwischen den Kompetenzen des Normsetzers (verfassungsändernder Gesetzgeber) und denen des Norminterpreten (*BVerfG*) und ist im Rahmen der Norminterpretation schon vielfach als Normsetzer tätig geworden, wie etwa bei allen Ausprägungen des APKR oder in Bezug auf grundrechtsimmanente Schranken. Besser ist es daher, das Wirken des Gerichts nicht entlang der Unterscheidung Normsetzer/Norminterpret, sondern entlang der Unterscheidung geschriebene/ungeschriebene Verfassung zu beschreiben. Denn das Gericht

b) Herleitung des Schutzbereichs

Die Herleitung des neuen Grundrechts erfolgt in Abgrenzung und Auseinandersetzung mit den Schutzbereichen von Art. 10 GG²⁶, Art. 13 GG²⁷ und zwei Ausprägungen des aus Art. 2 Abs. 1 GG hergeleiteten Persönlichkeitsrechts: dem Schutz der Privatsphäre²⁸ und dem Recht auf informationelle Selbstbestimmung (RiS). Es ist die Abgrenzung zum RiS, die einen Schwerpunkt bei der bisherigen Rezeption des Urteils in der Literatur darstellte und dort meist kritisches Echo auslöste.²⁹ Der Fokus dieser Kritik lag auf der Art und Weise der Herleitung der Schutzlücke des RiS: Da dieses Recht nur vor einzelnen Datenerhebungen schütze, der Zugriff auf ein informationstechnisches System jedoch gleich einen potenziell äußerst großen und aussagekräftigen Datenbestand erfasse, bedürfe es einer neuen grundrechtlichen Gewährleistung (Rn. 200).

Für sich genommen – soweit ist der Kritik zuzustimmen – kann diese Begründung nicht überzeugen, da dem RiS für einen viel gewichtigeren Eingriff als eine einzelne Datenerhebung ohne nähere Begründung die Schutzfähigkeit abgesprochen wird. Jedoch, wer nur diese nicht ganz glückliche Herleitung sieht, verliert leicht den Blick für die gänzlich anderen Gefährdungen, die den Ausgangspunkt für eine ganz andere Ausstrahlung des Schutzbereiches bilden: War es seinerzeit der Schutz vor der automatischen Datenverarbeitung der bei einer Volkszählung vom Staat erhobenen Daten, so ist es jetzt der Schutz vor dem heimlichen Zugriff auf einen durch den eigenen Computer als technischem Vehikel aggregierten Gesamtbestand an persönlichen Informationen, der einen vielfach tieferen Einblick in die Persönlichkeit des Betroffenen bietet, als es der Blick auf einzeln erhobene und dann zusammengeführte Daten je zu leisten vermag. Wiewohl wegen des Subsidiaritätscharakters des Art. 2 Abs. 1 GG zunächst nahe liegend, ist die Herleitung und Legitimation eines neuen Rechtes aus den Schutzlücken anderer geschriebener Grundrechte nicht zwingend, und im vorliegenden Fall auch deshalb nicht, weil es nur um die Binnenabgrenzung innerhalb des Art. 2 Abs. 1 GG ging.³⁰ Das RiS, seinerzeit ähnlich neu wie jetzt das GViiS, wurde ohne Abgrenzung zu anderen Grundrechten und deren Schutzlücken aus dem APKR ausgeprägt.³¹ Andere Persön-

hat im Laufe seines Wirkens durch Interpretation der vom Gesetzgeber geschriebenen Verfassung eine diese ergänzende ungeschriebene Verfassung geschaffen, zu der nun ein weiteres ungeschriebenes Grundrecht gehört.

26 Siehe hierzu unten IV.

27 Siehe hierzu unten II.

28 Siehe hierzu unten V.

29 Vgl. hierzu etwa die Erörterungen von *Britz* DÖV 2008, 411, 413 f.; *Eifert* NVwZ 2008, 521 f.; *Hoeren* MMR 2008, 365 f.; *Hornung* CR 2008, 299, 301 f.; *Jäger* jurisPR-ITR 12/2008, Anm. 2, Nr. 3; *Kutscha* NJW 2008, 1042 f.; *Lepsius*, in: *Roggan* (Hrsg.) Online-Durchsuchungen, 2008, S. 21, 28 ff.; *Sachs/Krings* JuS 2008, 481, 483 ff.; *Volkemann* DVBl. 2008, 590 ff. Siehe zur Rezeption des Urteils auch die Entscheidungsanmerkungen von *Bär* MMR 2008, 325 ff. und *Hirsch* NJOZ 2008, 2902 ff., und die anderen Beiträge in *Roggan* (a. a. O.): *Dix*, S. 71 ff.; *Hansen/Pfitzmann*, S. 131 ff.; *Hirsch*, S. 9 ff.; *Kühne*, S. 85 ff.; *Kutscha*, S. 157 ff.; *Roggan*, S. 97 ff.; und *Wartjen*, S. 57 ff.

30 Insbesondere bei der Abgrenzung der Ausprägungen des APKR untereinander hat die im Urteil proklamierte Subsidiarität des RiS gegenüber dem GViiS (Rn. 167) keinen inhaltlichen Gehalt. Sie stellt lediglich das Scharnier für die (Neu-)Interpretation der Schutzbereiche im sich überdeckenden Bereich dar. Wird in dieser Schnittmenge der Schutzbereich des subsidiären RiS eingegrenzt, erhöht dies den Anwendungsbereich des spezielleren GViiS, wird das RiS erweitert, verringert sich entsprechend der Schutzbereich des neuen Grundrechts.

31 So hieß es in *BVerfGE* 65, 1, 41 schlicht: „Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend. Es umfasst, wie bereits in der Entscheidung... angedeutet worden ist, auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des einzelnen, grundsätzlich selbst zu

lichkeitsgefährdungen bedingen andere Schutzrichtungen, die zu unterschiedlichen Ausstrahlungen führen. Soweit sich die Lichtkegel unterschiedlicher Schutzausstrahlungen überdecken, bedarf es dann der Abgrenzung beider Schutzbereiche im Rahmen der für die Grundrechtskonkurrenz aufgestellten Maßstäbe,³² aber nicht schon bei Herleitung der Schutzrichtung.³³

Die Anforderungen an einen Eingriff sind beim GVIIS weitaus höher als beim RiS.³⁴ Soweit angeführt wird,³⁵ diese anderen Eingriffsanforderungen hätten sich gut in den Verhältnismäßigkeitsmaßstab des RiS integrieren lassen, darf dies bezweifelt werden. Wenn einmal davon ausgegangen wird, dass bislang für alle unterschiedlichen Arten von „Informationseingriffen“ im Prinzip einheitliche Grundsätze bei der Prüfung von Grundrechtsbeschränkungen zur Anwendung kommen,³⁶ so sind die Anforderungen an den neuen Informationseingriff „Online-Durchsuchung“ doch so anders, dass sie die Einheitlichkeit der Prüfung sprengen und zu einer unübersichtlichen Zersplitterung innerhalb des Verhältnismäßigkeitsgrundsatzes führen würden. Rechtstechnisch betrachtet legitimiert sich die Erforderlichkeit einer neuen Ausprägung des allgemeinen Persönlichkeitsrechtes doch genau dadurch, dass das neue Recht erstmalige oder spezifisch andere Anforderungen an die Eingriffsvoraussetzungen stellt als die bisher ausgeprägten Rechte. Schon insofern war ein neues (Grund-)recht erforderlich.

In der Tat ist zuzugeben, dass die aufgrund unterschiedlicher Eingriffsvoraussetzungen notwendige Abgrenzung auf der Schutzbereichsebene zwischen GVIIS und RiS noch nicht ausgereift ist, dies gilt übrigens viel mehr noch für die Abgrenzung des GVIIS zu Art. 10 GG.³⁷ Jedoch, das Urteil war erst die Geburtsstunde eines neuen Rechtes, etwas Zeit zur Reife sollte man ihm mithin noch zugestehen.

c) Inhalt des Schutzbereichs

Die positive Definition des *zweigigliedrigen* Schutzbereichs setzt bei drei Schlüsselbegriffen an: „informationstechnisches System“, „Vertraulichkeit“, „Integrität“.³⁸ Was genau ist ein

entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Diese Befugnis bedarf unter den heutigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes.“

³² Vgl. hierzu statt aller *Jarass*, in: *Jarass/Pieroth*, GG, 9. Aufl. 2007, Vorb. vor Art. 1 Rn. 17f.

³³ Im Rahmen der hier verwendeten Metapher des Lichtkegels wäre dies der Standort des in eine bestimmte Schutzrichtung geschwenkten Scheinwerfers.

³⁴ Geht es beim RiS um das überwiegende Allgemeininteresse und um organisatorische Verfahren zur Zweckbindung erhobener Daten, so geht es beim GVIIS um die konkrete Gefahr für ein überragend wichtiges Rechtsgut, richterliche Anordnungen und Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

³⁵ Vgl. etwa *Britz* DÖV 2008, 411, 413; *Eifert* NVwZ 2008, 521, 522; *Hornung* CR 299, 301; *Sachs/Krings* JuS 2008, 481f.; *Volkmann* DVBl. 2008, 590, 592.

³⁶ So *Murswiek*, in: *Sachs* (Hrsg.), GG, 4. Aufl. 2007, Art. 2 Rn. 73.

³⁷ Vgl. hierzu die Ausführungen in Abschnitt IV. und V.

³⁸ Wiewohl „Gewährleistung“ als Begriff ebenfalls im Titel des neuen Grundrechts erscheint, wird eine Gewährleistungsverantwortung des Staates im Urteil selbst nicht weiter herausgearbeitet. Hier dem Staat große Schutzpflichten aufzubürden, ist verfrüht. Im Rahmen der diesbezüglich ohnehin sehr weit gefassten Einschätzungsprärogative des Gesetzgebers (vgl. hierzu nur *Dreier*, in: *Dreier* [Hrsg.], GG, 2. Aufl. 2004, Vorb. Rn. 103) sind ihm durch das Urteil erst einmal keine zwingenden Handlungspflichten zum Schutze des Bürgers vor privaten Akteuren oder etwa zur Etablierung einer sicherheitstechnischen Infrastruktur auferlegt. Allerdings gibt es, neben dem objektiv-rechtlich ausgestalteten Integritätsschutz eines Computersystems, auch andere Anklänge im Urteil an einen objekt-rechtlichen Gehalt des Grundrechts (Rn. 206, 222, 233, 241), die diesem entwicklungs-offenen Recht eine hohe Potentialität des Gewährleistungsschutzes zuwei-

informationstechnisches System? Das Urteil definiert nicht, es exemplifiziert: Ein Personalcomputer (Rn. 172), Laptops, Personal Digital Assisants (PDAs), Mobiltelefone (Rn. 194), letztere beide nur, soweit sie über einen großen Funktionsumfang verfügen und personenbezogene Daten in vielfältiger Weise erfassen und speichern können (Rn. 203). Das System kann auch ein Rechnernetzwerk selbst oder ein Verbund von Rechnernetzwerken sein (Rn. 4). Es hat die Erzeugung, Verarbeitung und Speicherung von Daten zu ermöglichen (Rn. 178). „Nicht vernetzte elektronische Steuerungsanlagen der Haustechnik“ sind ein Beispiel für nicht dem Schutzbereich des neuen Grundrechts unterfallende Systeme (Rn. 202), sie enthalten nur Daten mit punktuelltem Bezug zu einem bestimmten Lebensbereich (ebd.).

Was den ersten Teil des zweigliedrigen Schutzbereichs, den Schutz der *Vertraulichkeit*³⁹ des informationstechnischen Systems anbelangt, geht es tatsächlich um das Vertrauen auf den Schutz des „im“ System gespeicherten von ihm erzeugten Datenbestandes vor (heimlicher) staatlicher Ausspähung und Überwachung. Denn darauf zielt das Ermittlungs- und Schutzinteresse ab. Es ist die Vermittlungsleistung des informationstechnischen Systems, das einzelne personenbezogene Daten zu einer *auf einmal und immer wieder* zugänglichen, dynamischen Gesamtheit aggregiert, und daher bei unberechtigtem Zugang den Betroffenen in seiner persönlichen Lebensführung entblößen kann. Dabei bleibt in Bezug auf den Vertrauensschutz das informationstechnische System stets nur Vehikel der subjektiven wie individuellen Persönlichkeitsentfaltung des Grundrechtsträgers, der den Datenbestand unmittelbar erzeugt bzw. veranlasst.

Etwas anders stellt es sich dar, betrachtet man das zweite Glied des Schutzbereichs: Die *Integrität* des informationstechnischen Systems. Der besondere Schutz rechtfertigt sich aus der herausgehobenen Rolle, die dem System für die durch Art. 2 Abs. 1 GG geschützte Persönlichkeitsentfaltung zugesichert wird (Rn. 174). Anhand des vom *BVerfG* nur knapp und indirekt umrissenen Begriffs der Integrität⁴⁰ lässt sich diese bestimmen als die Unversehrtheit des Systems vor Ausspähung, Überwachung und Manipulation durch Dritte. Damit wird das Stadium des Eingriffs vorverlagert auf die in diese Unversehrtheit eingreifende Infiltration des Systems; unerheblich ist, ob es tatsächlich zum Ausspähen von persönlichen Daten kommt oder ob solche im System enthalten sind. Hier liegt der Akzent nicht auf dem Schutz subjektiver Abwehrrechte, sondern auf der Begründung eines objektiv-rechtlichen Schutzes informationstechnischer Systeme, der allerdings noch der Ausgestaltung durch weitere Entscheidungen bedarf.

sen, welche allerdings erst konkreter Aktualisierungen durch das Gericht bedarf. Ähnlich verhält es sich mit der (potentiell hohen) Drittwirkung des neuen Grundrechts. In der Literatur werden zum Teil schon Programme für Schutzpflichten des Staates entworfen, vgl. etwa *Dix*, in: *Roggan* (Fn. 29), S. 71, 73ff.; *Heckmann* jurisPR-ITR 5/2008, Anm. 1; *Kutscha*, in: *Roggan* (Fn. 29), S. 157, 169ff. Jenseits des Urteils bewegt sich *Lepsius*, in: *Roggan* (Fn. 29), S. 21, 42ff. bei seinen Überlegungen zum „Denken in Gewährleistungsbereichen“, bei denen er u.a. dem neuen Grundrecht seine (in erster Linie) subjektiv-abwehrrechtliche Funktion absprechen will (ebd. S. 41).

³⁹ Siehe zum Stellenwert des Vertraulichkeitsbegriffs in der Entscheidung *Britz* DÖV 2008, 211; differenzierend zwischen Vertraulichkeitserwartung und Interesse an Vertraulichkeit *Sachs/Krings* JuS 2008, 481, 484.

⁴⁰ Im Urteil wird die Integrität indirekt, anhand des Eingriffsvorgangs umschrieben: „Die Integrität eines informationstechnischen Systems wird angetastet, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen“ (Rn. 204).

Vom adaptiven Begriff des informationstechnischen Systems sind nicht nur permanente, sondern auch temporäre Systeme, wie etwa ein „Wirts-Computer“ im Zusammenspiel mit dem darin eingesteckten USB-Stick erfasst.⁴¹ Da ein informationstechnisches System auch ein Netzwerk sein kann (Rn. 4, 235), können auch ausgelagerte Speichermedien auf externen Servern, soweit sie vom eigenen informationstechnischen System für den Grundrechtsträger über ein Intranet, Extranet oder über das Internet zugänglich sind, zum Teil des eigenen informationstechnischen Systems, und damit zum Schutz- und Eingriffsobjekt des neuen Grundrechts werden.

Die Zuordnung eines Systems zum Grundrechtsträger erfolgt nach den knappen Bemerkungen des Urteils dadurch, dass der Betroffene das System „als eigenes nutzt“ und darüber, ggf. auch mit anderen zur Nutzung berechtigten Personen, selbstbestimmt verfügt (Rn. 206). Damit erfolgt die personale Zuordnung, auch wenn der Verfügungsbegriff insoweit etwas missverständlich ist,⁴² nicht über sachenrechtliche Kategorien,⁴³ sondern über eine tatsächliche Nutzungsberechtigung. So kann das eigene System zum Beispiel das im Internet-Cafe genutzte genauso wie das von einem Freund geliehene sein. Wenn man überhaupt zivilrechtliche Kategorien anwenden wollte, wären es eher solche des Schuldrechts. Jedoch – insofern besteht hier eine Parallele zu Art. 13 GG⁴⁴ – ein gekündigter Nutzungsvertrag zerschneidet noch nicht das Band der Zuordnung zwischen Grundrechtsträger und „seinem“ System. Zum eigenen informationstechnischen System kann temporär das als Terminal-Computer fungierende System eines anderen werden, soweit darüber etwa eine Fernzugriffsverbindung aufgebaut und auf den eigenen Computer zu Hause zugegriffen wird (Remote Access; vgl. Rn. 206; oben II.1.).

2. Eingriff und verfassungsrechtliche Rechtfertigung

a) Eingriffsmaßnahme Online-Durchsuchung

aa) Begriff

Was ist eine „Online-Durchsuchung“? Das BMI definiert den Vorgang so: „Die technische Fähigkeit, entfernte PC auf verfahrensrelevante Inhalte hin durchsuchen zu können, ohne selbst am Standort des Gerätes anwesend zu sein“;⁴⁵ der *BGH* wie folgt: „Die Zuspielung eines hierfür konzipierten Computerprogramms an den Beschuldigten, um die auf den Speichermedien des Computers abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen“;⁴⁶ und das *BVerfG* definiert: „Heimlicher Zugriff auf informationstechnische Systeme mittels technischer Infiltration“ (Rn. 7). Vor etwa einer halben Dekade war mit „Online-Durchsuchung“ noch ungefähr das gemeint, was heute vom neuen § 110 Abs. 3 StPO erfasst werden soll: Der Fernzugriff auf die Speichermedien eines Computersystems über das Netz von einem Computer aus, auf den die staatlichen Behörden im Rahmen der Wohnungsdurchsuchung

Zugriff haben.⁴⁷ Was heute vom *BVerfG* als Online-Durchsuchung verstanden wird, hat der Verfasser seinerzeit als „Einschleusen eines technischen Werkzeugs in ein Client-Computersystem“ typisiert,⁴⁸ und dann nicht die Durchsuchung (§ 102 StPO), sondern die damals in § 100c StPO geregelten „Geheimen Ermittlungen unter Einsatz technischer Mittel“ als zunächst einschlägigen Prüfungsmaßstab erachtet.⁴⁹

Wie sich das Kompositum „Online-Durchsuchung“ etwa Mitte/Ende der 1990er Jahre herausbildete, ist nicht mehr genau zu rekonstruieren. Die Nähe zur „Durchsuchung“ und nicht zu anderen Zwangsmaßnahmen ist kein Zufall. Zum einen setzte der (Offline-)Zugriff auf den Raum meist das physische Eindringen in einen Raum voraus, und dazu bedurfte es einer „Durchsuchung“ als Voraussetzung. Zum anderen hat diese Zwangsmaßnahme die niedrigsten Eingriffshürden in der StPO. Angesichts der zunehmenden technischen Möglichkeiten des Netzzugriffs auf einen Computer von außerhalb der Wohnung lag es nahe, sich begrifflich durch Voranstellen des Morphems „Online-“ an die Zwangsmaßnahme Durchsuchung anzudocken, um auch bei der Netzinfiltration eines Computers von deren geringen Eingriffshürden profitieren zu können. Der neue Begriff Online-Durchsuchung hatte allerdings auch zur Folge, dass der Online-Zugriff auf einen Computer stark mit dem Vorstellungsbild des Eindringens in einen Raum behaftet blieb. Sich davon wieder durch Abstraktion zu lösen fällt schwer, wie es die Diskussion zur Anwendbarkeit des Art. 13 GG auf die Online-Durchsuchung unterstreicht.

bb) Ermittlungssachverhalt

Wie wichtig ein genaues technisches Verständnis des jeweils mit „Online-Durchsuchung“ etikettierten Ermittlungssachverhalts ist,⁵⁰ zeigt ein Beispiel aus dem Jahr 2005. Damals hatte, nach Darstellungen in der Presse,⁵¹ ein amtierender Staatssekretär aus dem BMI von seinem Minister eine vom Bundesamt für Verfassungsschutz angeregte Änderung einer Dienstvorschrift unterzeichnen lassen, die dem Amt gemäß § 8 BVerfSchG die Befugnis zur Ausspähung privater Computer gab. Er selber und sein damaliger Minister dachten jedoch, es handele sich dabei nur um die Beobachtung geschlossener Internet-Foren.

Im letzten Jahr sind mögliche Ermittlungssachverhalte einer Online-Durchsuchung auch in technischer Hinsicht gut aufbereitet worden.⁵² Für die rechtliche Bewertung ist es nun angebracht, den auch hier verwendeten Sammelbegriff Online-Durchsuchung zu verlassen und in einzelne Ermittlungsvorgänge aufzugliedern. Bereits die Infiltration stellt einen eigenen, rechtlich getrennt zu bewertenden Vorgang dar. Denn bereits darin liegt ein Eingriff in die Integrität des Systems, unabhängig davon, ob es zur Durchsicht oder Überwachung von persönlichen Daten kommt. Je nachdem,

41 Vgl. hierzu auch *Hornung* CR 2008, 299, 303. Externe Speichermedien (wie z. B. DVD, USB-Sticks oder Speicherkarten) sind für sich kein informationstechnisches System, da sie zwar hohe Speicherkapazitäten, jedoch keine Datenverarbeitungsfunktion besitzen. Wenn jedoch etwa ein USB-Stick, der auch ein Abbild des eigenen personenbezogenen Datenbestandes enthalten kann, an einen fremden Wirtscomputer angeschlossen wird, der sich auch im öffentlichen Raum befinden kann (Internet-Cafe), entsteht ein temporäres informationstechnisches System zwischen eigenem Datenspeicher und einem fremden, Daten verarbeitenden System (Computer). Moderne Software- und Hardware-Standards, wie etwa U3, ermöglichen es, dass vom USB-Stick, wie von einer Festplatte im Computer aus, Programme gestartet oder Anwendungs-Dienste (Mail-Clients, Browser etc.) genutzt werden können, die auf dem Wirtscomputer gar nicht vorhanden sind.

42 Vgl. hierzu *Hoeren* MMR 2008, 365, 366.

43 Vgl. *Hornung* CR 2008, 299, 302 f.

44 Ähnlich wie bei Art. 13 GG geht es auch beim Schutz des GVII nicht um den Schutz des Eigentums oder Besitzes an der Wohnung/dem System, sondern um den Schutz der Privatsphäre. Daher bleibt zum Beispiel in Bezug auf Art. 13 GG der Mieter der Wohnung trotz abgelaufener Kündigungsfrist Grundrechtsträger (h. M., vgl. *Jarass*, in: *Jarass/Pieroth* [Fn. 32], Art. 13 Rn. 6.).

45 So die Formulierung im „Programm zur Stärkung der Inneren Sicherheit“ (PSIS), Anlage 2b, Maßnahme 3, vorgelegt am 10. 10. 2006.

46 *BGH* JZ 2007, 796.

47 *T. Böckenförde* (Fn. 7), S. 220 ff.

48 *T. Böckenförde* (Fn. 7), S. 211 f.

49 Die Prüfung konnte allerdings schnell abgeschlossen werden, da der Tatbestand dieser Zwangsmaßnahme bei näherem Hinsehen wenig Gemeinsames aufweisen konnte mit der Ermittlungstätigkeit des „Einschleusens eines technischen Werkzeugs in ein Client-Computersystem“.

50 Zur Unschärfe des Begriffs „Online-Durchsuchung“ für die mannigfaltigen Formen staatlichen Fernzugriffs auf EDV-Systeme vgl. auch *Buermeyer* HRRS 2007, 154 ff.

51 Siehe hierzu FAZ vom 5. 5. 2007, S. 1 „Schily wollte keine Online-Durchsuchung“ und taz vom 2. 5. 2007, S. 11 „Online-Schnüffeln ohne Freibrief“.

52 Durch besondere technische Kenntnis zeichnen sich aus: *Buermeyer* HRRS 2007, 154 ff.; *Hansen/Pfitzmann* DRiZ 2007, 225 ff.; *Fox* DuD 2007, 827 ff.; *Pohl* DuD 684 ff.; *Schmidt*, in: *heise Security* vom 11. 3. 2007: „Bundestrojaner: Geht was – was geht“ (www.heise.de).

ob das System online, also über das Netz, oder offline, also physisch am Computer infiltriert wird, entscheidet sich, ob nur ein Eingriff in das GVIIS oder, bei Infiltration in der Wohnung, auch ein solcher in Art. 13 GG vorliegt.⁵³ Schon aufgrund ganz unterschiedlicher Eingriffstiefen (Rn. 234) ist es geboten,⁵⁴ bei der Datensuche rechtlich zwischen dem Vorgang des einmaligen Ausspähsens des Zielsystems und der kontinuierlichen Überwachung der Systemnutzung zu unterscheiden. Dies erleichtert auch die Gegenüberstellung von Online-Überwachung und Quellen-Telekommunikations-Überwachung, beides Überwachungsvorgänge, die am informationstechnischen System ansetzen. Der Überwachung des Systems muss nicht immer seine Infiltration vorausgehen, sie kann auch offline erfolgen, beides unterstreicht die Methode der Messung elektromagnetischer Abstrahlungen des Bildschirms (Fn. 192). Von der Suche ist die Sicherung der Daten zu unterscheiden, die meist durch automatisierte Übertragung erhobener Daten an die Computersysteme der staatlichen Behörden über das Netz erfolgt.

Infiltration, Ausspähen, Überwachung, Sicherung – soweit diese Vorgänge über das Netz erfolgen, ist es angebracht, dies durch Voranstellen des Morphems „Online-“ deutlich zu machen. BMJ und BMI haben Mitte letzten Jahres in einer Arbeitsgruppe für die beiden mittleren Vorgänge die Ausdrücke Online-Durchsicht und Online-Überwachung entwickelt.⁵⁵ Um eine Einheitlichkeit der Terminologie zu wahren, schließt sich der Verfasser diesen Begriffen an. Somit ist zu unterscheiden zwischen Online-Infiltration, Online-Durchsicht, Online-Überwachung und Online-Sicherung.

b) Maßstäbe für Eingriffe

aa) Geeignetheit und Erforderlichkeit

Am Anfang von Teil 2 des Abschnitts II. wird im Urteil festgestellt, dass die angegriffene Norm des Verfassungsschutzgesetzes nicht dem rechtsstaatlichen Gebot der Normenklarheit und Normenbestimmtheit genügt (Rn. 211). Sie entspricht zudem nicht dem Grundsatz der Verhältnismäßigkeit (Rn. 218), da sie zwar geeignet und erforderlich, jedoch nicht verhältnismäßig im engeren Sinne ist. Im Rahmen der Geeignetheitsprüfung werden zwei von den technischen Auskunftspersonen aufgeworfene Fragen zur Ungeeignetheit der neuen Ermittlungstätigkeiten behandelt, dann aber jeweils kurz verneint.⁵⁶ Die Erforderlichkeit der in Rede

stehenden Ermittlungsmaßnahmen wird ohne viel Aufhebens ebenfalls bejaht.

Die Erörterung der Geeignetheit und Erforderlichkeit der neuen Ermittlungstätigkeiten wäre unvollständig, würde sie nicht noch auf eine Äußerung des Berichterstatters des Verfahrens eingehen. Dieser verwies im Rahmen seiner Verabschiedung aus dem Karlsruher Amt am 18. 7. diesen Jahres auf die restriktiven Aussageermächtigungen der Präsidenten der Sicherheitsbehörden, die dazu führten, dass nicht über die bisher mit der Online-Durchsicht gemachten Erfahrungen berichtet wurde. Keinerlei Erkenntnisse über Eignung und Angemessenheit der Maßnahmen „wurden dem Gericht offen gelegt“. Die den Präsidenten auferlegten „Maulkörbe“ könnten die Deutung provozieren, es gehe vielleicht darum, „eine Bloßstellung zu vermeiden, vielleicht auch den Befund der relativen Erfolglosigkeit zu überspielen“.⁵⁷

In der Tat wird dem Gericht, soweit ihm solche Erfahrungen vorenthalten werden, eine wesentliche Beurteilungsgrundlage entzogen. Gleiches gilt, soweit dem Parlament bei Erörterung der Maßstäbe für ein neues Eingriffsgesetz diese Erfahrungen vorenthalten werden. Kann die Aussageverweigerung der Sicherheitsbehörden bzw. der Regierung, sprich der Exekutive, gegenüber der Judikative oder Legislative das letzte Wort sein? Wohl nicht. Zwar steht der Exekutive für die Rechtfertigung ihrer Aussageverweigerung eine Einschätzungsprärogative zu, jedoch kann diese in einem Rechtsstaat nicht gänzlich der richterlichen Überprüfung, womöglich durch das *BVerfG*, entzogen werden. Im Rahmen seines eigenen Verfahrens jedenfalls ist das *BVerfG* solchen Aussageverweigerungen nicht wehrlos ausgesetzt. Denn es kann sich aus der Verfassung, wie etwa aus dem Rechtsstaats- und Gewaltenteilungsprinzipien des Art. 20 GG, eigene Abwehrmittel herleiten. Es verwundert in diesem Zusammenhang, dass die Gesichtspunkte der vorenthaltenen Beurteilungsgrundlage der Verhältnismäßigkeitsprüfung nicht innerhalb der Geeignetheits- und Erforderlichkeitsüberprüfung des Urteils angesprochen wurden, denn genau dort wären sie zu verorten gewesen.

bb) Abstufungen

In der folgenden Angemessenheitsprüfung werden verschiedene, teilweise in einem abgestuften Verhältnis zueinander stehende Merkmale für die Intensität des Eingriffs in das GVIIS aufgeführt.⁵⁸ Schon bei der die grundrechtliche Schutzbedürftigkeit begründenden Persönlichkeitsgefährdung nimmt das Urteil Abstufungen vor.⁵⁹ Mit Blick auf

⁵³ Methoden der Online-Infiltration können unter Ausnutzen von Sicherheitslücken in das System eindringen (klassisches Hacking), wie etwa durch Ausnutzen noch nicht allgemein bekannter Sicherheitslücken, sogenannter Zero-Day- oder Less-Than-Zero-Day-Exploits, instruktiv hierzu *Pohl DuD*, 684, 685 ff. Sie können auch eine unbewusste Mitwirkung des Nutzers erfordern, wie etwa das Herunterladen eines als E-Mail Anhang getarnten Schadprogramms (Trojaner). Weitere Methoden dieser Art sind z. B. das Herunterladen eines als Software- oder Sicherheits-Update getarnten Schadprogramms von einer Web-Site, oder schon der Aufruf einer infizierten Web-Site, der die unbemerkte Installation von Schad-Software auf dem eigenen System auslöst. Methoden der Offline-Infiltration lassen sich ebenfalls danach unterscheiden, ob keine oder eine unbewusste Mitwirkung des Nutzers erforderlich ist, welche die Installation von Schadprogrammen auslöst, wie etwa das Einlegen einer geschenkten CD oder das Einstecken eines geschenkten USB-Sticks in den Computer.

⁵⁴ Vgl. hierzu auch das zur mündlichen Verhandlung angefertigte Gutachten von *Sieber*, Stellungnahme im Verfahren 1 BvR 370/07, Version 1.0, S. 2; siehe hierzu auch *Buermeyer HRRS* 2007, 154, 160 ff.

⁵⁵ Siehe hierzu Fragenkatalog des BMJ an das BMI vom 22. 8. 2008, S. 1.

⁵⁶ Zum einen handelte es sich um die Frage, ob realistische technische Selbstschutzmöglichkeiten nicht die Geeignetheit der Maßnahme ausschließen. Zum anderen ging es darum, ob die Eignung der geregelten Befugnisse nicht deshalb zu verneinen sei, weil der Beweiswert der durch die Online-Sicherung gewonnen Erkenntnisse, insbesondere hinsichtlich der technischen Echtheit, Zweifel, nicht zuletzt auch an der strafverfahrensrecht-

lichen Revisionsfestigkeit, lasse. Dazu ist anzumerken, dass die Frage, ob digitale Dateien als Beweismittel im Strafverfahren eingesetzt werden können, mit ihrem Beweiswert in keinem Zusammenhang steht, vgl. hierzu *T. Böckenförde* (Fn. 7), S. 305. Auch die bei einer Online-Sicherung gewonnenen Erkenntnisse unterliegen der freien Beweiswürdigung des erkennenden Strafgerichts gemäß § 261 StPO. Vgl. zur Beweisbedeutung von elektronischen Beweismitteln im Strafprozess ausführlich *T. Böckenförde* (Fn. 7), S. 304 ff.

⁵⁷ Siehe etwa DDP-Meldung v. 18. 8. 2008: Ex Verfassungsrichter: „Regierung ‚mauert‘ bei Online-Durchsicht“. FAZ v. 19. 7. 2008: „Die Politik hat eine Bringschuld“.

⁵⁸ Bereits die einmalige körperliche Beschlagnahme und Durchsicht von Speichermedien stellt einen Eingriff von hoher Intensität dar (Rn. 229 f.). Diese wird durch die Sicherung von Daten der Fernkommunikation erhöht (Rn. 233). Das Gewicht des Grundrechtseingriffs ist besonders schwer bei der längerfristigen Online-Überwachung des Systems (Rn. 234). Intensität und Gewicht des Eingriffs werden durch Heimlichkeit (Rn. 238) und Gefahren für die Integrität des Rechners, für Rechtsgüter des Betroffenen und für Dritte (Rn. 239, 241) geprägt.

⁵⁹ Enorme Verarbeitungs- und Speicherressourcen des Systems schaffen Persönlichkeitsgefährdungen (Rn. 178), diese werden vertieft durch Einbindung in ein Computernetz (Rn. 180 f.).

die noch nicht ganz klar konturierten, dennoch schon gut sichtbaren Abstufungen bei Schutzbereich und Eingriff stellt sich die Frage, ob nicht durch die Entwicklung des neuen Grundrechts auch an wenig intensivere Eingriffsmaßnahmen⁶⁰ weniger intensive, aber dennoch höhere Voraussetzungen als bisher zu stellen sind. Angesprochen sind damit insbesondere Ermittlungsmaßnahmen des Strafprozessrechtes wie etwa die offene Offline-Durchsicht und Offline-Sicherung von Speichermedien eines Computers bei der Wohnungsdurchsuchung oder die durch den neuen § 110 Abs. 3 StPO ausdrücklich ermöglichte offene Online-Durchsicht der Speichermedien externer Computersysteme über das Netz. Auch wenn die geschilderten Maßnahmen nicht heimlich und zum Teil auch nicht online erfolgen, so ist doch das Zielobjekt das gleiche: Der grundrechtlich nunmehr als außerordentlich schutzwürdig erachtete persönliche Datenbestand eines Computersystems. Daher liegt es nahe zu fragen, ob etwa der neue, auch als „Online-Durchsuchung light“ bezeichnete § 110 StPO,⁶¹ der noch kurz vor dem Urteil in Kraft getreten ist,⁶² nicht durch Erhöhen der Eingriffsvoraussetzungen an die Anforderungen des nunmehr geltenden Grundrechtsschutzes angepasst werden muss.

cc) Gefahr sui generis

Die heimliche Online-Infiltration und die darauf aufbauende Online-Durchsicht oder Online-Überwachung des Systems wird vom Gericht als ein Eingriff von so hoher Intensität verstanden, dass damit nur die Gefahr für ein überragend wichtiges Rechtsgut ins Verhältnis gesetzt werden kann, um die Waage wieder ins Gleichgewicht zu bringen: „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 berühren“ (Rn. 247). In dieser Zusammenstellung hat das Gericht, soweit ersichtlich, die bislang hochrangigen Rechtsgüter des deutschen Gefahrenabwehrrechts definiert, und die Anforderungen noch einmal höher geschraubt als bei dem Urteil zur polizeilichen Rasterfahndung vor 2 Jahren.⁶³ Ging es seinerzeit um Freiheit *einer* Person, so geht es nun um Freiheit *der* Person. Die Gefahr für Grundlagen und Bestand des Staates wird nun an die Seite der Gefahr für die Grundlagen der *Existenz der Menschen* gestellt und damit auf ein noch höheres Tableau gehoben. Insgesamt handelt es sich nun um überragend wichtige, und nicht „nur“ um hochrangige Rechtsgüter wie bei der Rasterfahndung.⁶⁴

Hinsichtlich des Gefahrengrades führt das Gericht eine konkrete Gefahr sui generis ein. Der neue Gefahrbegriff, der offenbar den Besonderheiten terroristischer Gefahren Rechnung tragen soll, ist weder begrifflich noch in der praktischen Anwendung einfach zu handhaben. Sein Kennzeichen

ist erst einmal, dass die hinreichende Wahrscheinlichkeit des Schadenseintritts, anders als etwa bei der dringenden Gefahr des Art. 13 Abs. 4 GG⁶⁵ oder der konkreten Gefahr des Polizeirechts⁶⁶ nicht mehr unbedingte Voraussetzung für das Vorliegen einer konkreten Gefahr ist: „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“ (Rn. 251). Es reicht also schon aus, dass der Gefahr eintritt droht, allerdings muss diese Drohung von individualisierbaren Personen ausgehen. Durch dieses ausdrückliche Abstellen auf die Personverursachung, was den neuen ebenfalls vom klassischen⁶⁷ Gefahrbegriff des Polizeirechts⁶⁸ unterscheidet, werden Fälle der Zustandsverantwortlichkeit nicht mehr erfasst.⁶⁹

Für das Vorliegen einer Gefahr müssen weiterhin die beteiligten Personen soweit identifiziert werden, dass die Maßnahmen gezielt gegen sie eingesetzt werden können und Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen (Rn. 251). Was bedeutet ein *seiner Art nach* konkretisiertes Geschehen? Der Rechtsanwender, der vor der Aufgabe steht, die neuen Gefahrmerkmale umzusetzen, nimmt am besten die bekannt gewordenen Einzelheiten des Geschehens rund um die Dschihad-Bombenbauer aus Oberschlehdorn⁷⁰ zusammen und analogisiert diese für seinen Fall. Damit hat er zugleich einen abstrakt bleibenden konkreten Gefahrbegriff dekompliziert, für den mit hinreichender Wahrscheinlichkeit dieses Geschehen die Blaupause war.

Es ist nicht zu übersehen, dass der neue Gefahrbegriff die Tür einen Spalt weit für Vorfeldtätigkeiten öffnet, allerdings nicht so weit aufsperrt, dass nun von der Integration eines informationellen Vorfeldrechts in das klassische Gefahrenabwehrrecht⁷¹ gesprochen werden kann. Es müssen schon tatsächliche Anhaltspunkte für eine drohende Gefahr, für individuell bestimmbare Gefährder sowie ein typischerweise zu einer Gefahr führendes Geschehen vorliegen. Im Vorfeld liegende Maßnahmen der Aufklärung und Vorbeugung einer möglichen Gefahr sind davon nicht erfasst. Die daraus abgeleitete Konsequenz für den Verfassungsschutz findet sich – etwas verklausuliert, aber im Ergebnis eindeutig – im letzten Absatz (Rn. 256) der Ausführungen zur „Gefahr“. Für Sicherheitsbehörden, welche den erhöhten Anforderungen an den Gefahrbegriff beim heimlichen Zugriff auf informationstechnische Systeme nicht genügen können, weil sie per definitionem nur im (weiteren) Vorfeld tätig sind, besteht keine Grundlage, das Erfordernis der konkreten Gefahr weiter abzumildern. Im Klartext: Der heimliche Zugriff auf informationstechnische Systeme bleibt der Polizei und den Strafverfolgungsbehörden (Rn. 207) vorbehalten, der im Vor-

⁶⁰ Wie etwa die *offene Online-Durchsicht* wie *Online-Sicherung* oder die *offene Offline-Durchsicht* und *Offline-Sicherung* des informationstechnischen Systems.

⁶¹ Vgl. zu diesem Begriff und dieser Maßnahme den instruktiven Aufsatz von *Schlegel* HRRS 2008, 23 ff.

⁶² Am 1. 1. 2008 im Rahmen des „Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“. Dieses Gesetz enthielt auch die zur Zeit auf dem verfassungsgerichtlichen Prüfstand stehenden Regelungen zur „Vorratsdatenspeicherung“ von Telekommunikationsverbindungsdaten.

⁶³ *BVerfGE* 115, 320 ff.

⁶⁴ Schwer vorstellbar, dass sich hier noch Steigerungsmöglichkeiten für Güter ergeben, welche die überragend wichtigen Rechtsgüter noch einmal überragen. Es müsste sich dann wohl schon um eine konkrete Gefahr handeln, die Bestand und Sicherheit des Planeten bzw. die Existenz der Weltbevölkerung berührt.

⁶⁵ Die dringende Gefahr des Art. 13 GG setzt die hinreichende Wahrscheinlichkeit des Schadenseintritts an einem wichtigen Rechtsgut voraus, vgl. nur *Jarass*, in: *Jarass/Pieroth* (Fn. 32), Art. 13, Rn. 37; nach anderer Ansicht kommt es auf den engen zeitlichen Zusammenhang des Schadenseintritts an, vgl. nur *Papier*, in: *Maunz/Dürig* (Hrsg.), GG, Bd. 1, Art. 13 Rn. 132, 134.

⁶⁶ Vgl. hierzu etwa *Denninger*, in: *Lisken/Denninger*, Handbuch des Polizeirechts, 4. Aufl. 2007, Kap. E Rdnr. 39 ff.

⁶⁷ *Denninger*, in: *Lisken/Denninger* (Fn. 66).

⁶⁸ Siehe hierzu *Baum* ZRP 2008, 137, 139.

⁶⁹ So auch *Baum* ZRP 2008, 137, 139.

⁷⁰ Siehe hierzu etwa *Rammelsberger*, *Der deutsche Dschihad*, 2008, S. 18–44.

⁷¹ Aufschlussreich hierzu *Möstl* DVBl. 2007, 581 ff.

feld tätige Verfassungsschutz muss sich „auf andere Ermittlungsbefugnisse beschränken.“⁷²

dd) Vorkehrungen

Sodann stellt das Gericht in zweierlei Hinsicht prozedurale Anforderungen für Eingriffe in das GVIIS auf: Die vorbeugende Kontrolle durch eine neutrale und unabhängige Instanz (Rn. 258) und Vorkehrungen, um Eingriffe in den Kernbereich privater Lebensgestaltung zu vermeiden (Rn. 270). Als ideale Besetzung für die neutrale Instanz wird grundsätzlich der Richter erachtet. Einen intensiven Eingriff unter einen Richtervorbehalt zu stellen ist nicht neu, ein Novum stellt es allerdings, soweit ersichtlich, dar, dass auch eine „andere Stelle“ damit betraut werden kann, soweit diese die gleiche Gewähr für Unabhängigkeit und Neutralität bietet wie ein Richter (Rn. 259). Unklar bleibt, wer dies sein könnte (z. B. auch ein Nichthoheitsträger?). Neben der Unabhängigkeit ist entscheidend, dass die Kontroll-Instanz technische Kompetenz und Vertrautheit mit der Bewertung von Gefahrenlagen mitbringt,⁷³ um die Rechtmäßigkeit der Maßnahme zutreffend beurteilen zu können. Diese hohen Anforderungen hätten es sachgerechter erscheinen lassen, wie beim „Großen Lauschangriff“ die Beurteilung einem Richtergremium⁷⁴ und nicht nur dem womöglich schnell überforderten Einzelrichter anzuvertrauen.

Die Ausführungen zum Kernbereichsschutz beeindrucken durch technischen Sachverstand und pragmatisches Verständnis. Praktisch, so das Gericht, ist es unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsschutz bewertet werden kann (Rn. 277); technische Such- und Ausschlussmechanismen sind nicht zuverlässig genug zur Bestimmung der Kernbereichsrelevanz persönlicher Daten (Rn. 278). Mit Letzterem wurde eine technische Erkenntnis ausgesprochen, die nachzuvollziehen manchem immer noch schwer fällt: Die automatische Filterung inhaltlicher Daten nach semantischen Kriterien ist vielfach unzureichend, um rechtlichen Schutz zu verwirklichen. Anders als bei der erstinstanzlichen Entscheidung im Compuserve-Fall⁷⁵ hat nun ein Jahrzehnt später ein anderes deutsches Gericht in Bezug auf das Thema „automatische Filterung“ auch deshalb eine zutreffende Entscheidung getroffen, weil es richtig machte, was seinerzeit nicht beherzigt wurde: Technischen Experten zuhören und sie ernst nehmen. Es ist zu wünschen, dass auch andere staatliche Institutionen⁷⁶ in dieser Hinsicht zum höchsten deutschen Gericht aufschließen.

Weiter ist zu begrüßen, dass empirischen Fakten und nicht axiomatische Voranstellungen des Gerichts nun die Fortentwicklung des Kernbereichsschutzes veranlassen. Das Ergebnis⁷⁷ ist ein zweistufiges Schutzkonzept: Auf der ers-

ten Stufe hat die gesetzliche Regelung auf das Unterbleiben der Erhebung kernbereichsrelevanter Daten hinzuwirken (Rn. 281). Sollte die Erhebung kernbereichsrelevanter Daten praktisch unvermeidbar sein, so muss auf der zweiten Stufe für hinreichenden Schutz in der Auswertungsphase gesorgt werden (Rn. 283)⁷⁸ Eine wichtige Antwort bleibt das Gericht allerdings schuldig: Anhand welcher Kriterien die Kernbereichsrelevanz persönlicher Daten auf einem Computer beurteilt werden soll.⁷⁹

3. De lege ferenda

a) Umsetzung in Bayern

Am 1. 4. 2008, einen Monat nach Urteilsverkündung, hat die bayerische Staatsregierung einen Novellierungsentwurf zum Verfassungsschutzgesetz inklusive der Ermächtigung zur „Verdeckten Online-Datenerhebung“ (Art. 6e BayVSG) auf den Weg gebracht. Einen Tag später folgte aus der Mitte des Landtags ein die Ermächtigung zum „Verdeckten Zugriff auf informationstechnische Systeme“ (Art. 34d PAG) enthaltender Änderungsantrag zum vormaligen Entwurf zum Polizeiaufgabengesetz (PAG). Am 3. 7. 2008 wurden beide Gesetze verabschiedet, am 1. 8. 2008 traten sie in Kraft.⁸⁰

aa) Befugnis ohne Kompetenz

Die Anforderungen an den Gesetzgeber zur Aufnahme der Online-Durchsuchung in ein Verfassungsschutzgesetz sind hoch.⁸¹ Wiewohl der neue Gefahrbegriff des Gerichts in geringem Ausmaß polizeiliche Vorfeldtätigkeiten zulässt, bleiben die Anforderungen an die Konkretetheit der Gefahr doch so hoch, dass für die klassischen, sich weit im Vorfeld einer Gefahr bewegenden Kompetenzen des Verfassungsschutzes kein Raum mehr vorhanden ist. Das Gericht war sich dieser originären Vorfeldkompetenz des Verfassungsschutzes bewusst, als es sinngemäß ausführte, dass diese Kompetenz kein hinreichender Grund sei, die Anforderungen an den konkreten Gefahrbegriff abzumildern, und sei es um den Preis, dass Vorfeldbehörden damit die Vornahme der eingriffsintensiven Online-Durchsuchung verwehrt bliebe (Rn. 256).

Was hat der bayerische Gesetzgeber unternommen, um dennoch dem Verfassungsschutz die Online-Durchsuchung nicht vorenthalten zu müssen? Er hat nicht etwa die Anforderungen an den konkreten Gefahrbegriff abgemildert,⁸² sondern den bayerischen Verfassungsschutz zu einer partikularen Gefahrenabwehrbehörde gemacht.⁸³ In Umkehrung eines elementaren sicherheitsrechtlichen Grundsatzes wurde so von der Befugnis auf die Aufgabe geschlossen. In der Begründung wird dies so kaschiert: „Auch wenn bei den genannten Voraussetzun-

⁷² So die dort in einem anderen Zusammenhang gebrauchte Formulierung des Urteils in Rn. 248.

⁷³ Um etwa beurteilen zu können, ob die betreffende Anordnung das Zielsystem und die personale Zuordnung des Zielsystems zum Grundrechtsträger hinreichend bestimmt identifiziert und um den neuen Gefahrbegriff *sui generis* zutreffend anwenden zu können.

⁷⁴ Vgl. hierzu auch Sieber (Fn. 54), S. 20.

⁷⁵ Vgl. AG München MMR 1998, 429 ff. m. Anm. Sieber MMR 1998, 438 ff.

⁷⁶ So war etwa das BMI zusammen mit dem BKA bis vor kurzem noch der Auffassung, dass bei der Online-Durchsicht einer Festplatte anhand von Suchkriterien wie: Dateiname, -endung, -typ, Schlüsselwörter, Verzeichnis, die kernbereichsrelevanten Daten einer Festplatte erkannt und herausgefiltert werden können. Vgl. hierzu die Antwort auf Frage Nr. 7 im Fragenkatalog der SPD-Bundestagsfraktion an das BMI vom 22. 8. 2007.

⁷⁷ Vgl. hierzu auch die Erörterung von Warmtjen, in: Roggan (Fn. 29), S. 57, 59 ff.

⁷⁸ Zu diesen Schutzmaßnahmen kann etwa gehören, dass aufgefundene kernbereichsrelevante Daten unverzüglich gelöscht werden und ihre Verwertung ausgeschlossen wird.

⁷⁹ Zwar wurden vor allem in der Entscheidung zum großen Lauschangriff Kriterien zur näheren Bestimmung des Kernbereichs aufgestellt, diese sind allerdings sehr auf den Kontext Wohnung und persönliche Gespräche bezogen und bieten für die Kernbereichsrelevanz von Computerdaten nur wenig Orientierung: Nach *BVerfGE* 109, 279, 320 ff. bestimmt sich der Kernbereich privater Lebensgestaltung etwa nach Art der zu überwachenden Räumlichkeiten, ob beim Gespräch Personen des höchstpersönlichen Vertrauens anwesend sind, zu denen etwa Ehegatten, engste Familienangehörige und Verwandte gerader Linie gehören.

⁸⁰ Zum BayVSG: BayLT-Drs. 15/10345; zum PAG: BayLT-Drs. 15/10313.

⁸¹ Vgl. hierzu auch Roggan, in: *ders.* (Fn. 29), S. 97, 113 ff.

⁸² Die konkrete Gefahr wurde explizit als Eingriffsgrundlage in den Tatbestand der verdeckten Online-Datenerhebung aufgenommen und in der Begründung des Gesetzesentwurfs noch einmal genau entlang der Vorgaben des Verfassungsgerichts konkretisiert. Vgl. BayLT-Drs. 15/10313, S. 23.

⁸³ Indem er den Verfassungsschutz bei Vorliegen einer konkreten Gefahr durch Art. 6e BayVSG zur verdeckten Online-Datenerhebung ermächtigte.

gen“, nämlich denen, die an die konkrete Gefahr zu stellen sind, „vom Grundsatz her stets auch eine polizeiliche Maßnahme in Betracht käme, bedarf es zur Wahrnehmung der gesetzlich zugewiesenen Aufgaben des Landesamtes für Verfassungsschutz gleichwohl auch einer eigenständigen Befugnis...“. Damit wurden nicht nur Vorgaben des *BVerfG* auf den Kopf gestellt, sondern auch das eigene VSG konterkariert. Dort heißt es nämlich in Art. 3: Dem Landesamt für Verfassungsschutz steht die Befugnis zu polizeilichen Maßnahmen nicht zu.

bb) Anordnung gegen Unbekannt

Der neue Gefahrbegriff⁸⁴ stellt konkrete Anforderungen an die individuelle Bestimmbarkeit der Gefährder: „Über deren Identität muss zumindest so viel bekannt sein, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann“ (Rn. 251). Zudem: Als Gefahrverantwortlicher kommt nur der (potentielle) Gefahrverursacher in Betracht (Rn. 251), Dritte und Zustandsstörer sind als Adressat der Maßnahme grundsätzlich außen vor.⁸⁵ Diese Vorgaben wurden bei der legislativen Umsetzung missachtet. Denn Adressat der Anordnung kann nach Art. 6e Abs. 1 Satz 3 BayVSG auch ein „Nachrichtenmittler“, gemäß der Begründung zu Art. 34d Abs. 1 Satz 1 Nr. 3 PAG⁸⁶ sogar eine „Kontakt- und Begleitpersonen, die für die Störer Botentätigkeiten wahrnehmen oder (ihnen) *ihre*⁸⁷ informationstechnischen Systeme zur Verfügung stellen“, sein.

Die Anordnung des verdeckten Computerzugriffs bedarf zumindest dreier Elemente: Der Person des Betroffenen, des informationstechnischen Systems und der Zuordnung des Systems zur Person. Um dem rechtsstaatlichen Bestimmtheitsgrundsatz zu genügen, müssen alle drei Elemente *vor* der Maßnahme bekannt sein und nicht erst durch die Maßnahme bekannt werden. Soweit die Infiltration des Systems über das Netz, und nicht physisch vor Ort erfolgt, können diese Anforderungen erhebliche praktische Probleme aufwerfen.⁸⁸

Gemäß Art. 34d Abs. 3 Satz 4 PAG bzw. Art. 6f Abs. 5 Satz 2 BayVSG hat die Anordnung – soweit möglich – Name und Anschrift des Betroffenen sowie die Bezeichnung des informationstechnischen Systems zu enthalten. Dieser Dispens von der Spezifizierung des Eingriffsadressaten und/oder Eingriffsobjekts ist etwa den weniger intensiv eingreifenden strafprozessualen Maßnahmen der akustischen Wohnraum- wie Telekommunikationsüberwachung fremd.⁸⁹ Wollte man hier Parallelen ziehen, so hieße dies, dass – soweit nicht möglich – weder Name des Betroffenen noch Telefonanschluss bzw. Wohnung in der Anordnung erscheinen müssten. Die Maßnahme könnte sich also erst einmal auf Telefone und Wohnungen Dritter beziehen, bevor dann die Auswertung der abgehörten Gespräche ergibt, ob man denn beim richtigen Telefon oder in der richtigen Wohnung gelandet ist. Ähnliches schwebt dem bayerischen Gesetzgeber in Bezug auf den verdeckten Computerzugriff vor. So heißt es in der Begründung: „Es gibt durchaus

Fallkonstellationen, bei denen die Polizei den Gefährder nur über das informationstechnische System ermitteln kann.“⁹⁰ Wenn etwa bei einem ausländischen E-Mail-Provider ein Konto anonymisiert erstellt wurde und der Versand der Mail über öffentliche Internetzugriffspunkte erfolgt, dann können bei Auswertung der Verkehrsdaten der E-Mail diese weder einer Person noch einem spezifischen informationstechnischen System zugeordnet werden.⁹¹

Was erscheint in diesem Fall in der Anordnung zur Bestimmung von Eingriffsadressat und -objekt? Allein eine anonyme E-Mail-Adresse.⁹² Eine solche vom BayVSG und PAG gedeckte *Anordnung gegen Unbekannt* hat erhebliche Streuwirkung. Sie kann einen sehr intensiven Grundrechtseingriff bei vielen nicht betroffenen Personen und deren Systemen auslösen, bevor sie womöglich ans Ziel kommt. Dass ein solches Vorgehen nicht nur gegen den Gefahrbegriff des Urteils, sondern auch eklatant gegen das rechtsstaatliche Bestimmtheitsgebot und den Verhältnismäßigkeitsgrundsatz, mithin auch deshalb gegen die Verfassung verstößt, sollte keiner weiteren Erläuterung mehr bedürfen.

cc) Schrankensystematik des Art. 13 GG

Es sind nicht zuletzt diese, vom bayerischen Innenminister selbst eingeräumten hohen immanenten Risiken des zielgenauen Erreichens von Person und System bei der Online-Infiltration über das Netz,⁹³ welche den Freistaat Bayern dazu bewegen haben, gesetzliche Vorkehrungen für den Hauptanwendungsfall der viel zielsichereren Offline-Infiltration zu schaffen: Das heimliche Betreten der Wohnung zu Zwecken der Infiltration des informationstechnischen Systems. Die hierfür in Art. 6g BayVSG bzw. Art. 34e PAG geschaffene gesetzliche Grundlage genügt den formellen verfassungsrechtlichen Anforderungen. Fraglich bleibt, ob eine solche Offline-Infiltration über die Wohnung von den geschriebenen Gesetzesvorbehalten des Art. 13 Abs. 2-7 GG umfasst ist. Diese Frage dringt tief in die Systematik des Schrankengebäudes von Art. 13 GG ein. Sie ist nach hier vertretener Ansicht offen. Der Verfasser neigt dazu, eine Ergänzung des Schranken catalogs des Art. 13 GG, soweit das Eindringen in die Wohnung in Rede steht,⁹⁴ nicht für erforderlich zu halten,⁹⁵ das Anwenden der Maßstäbe des

⁹⁰ BayLT-Drs. 15/10345, S. 9.

⁹¹ BayLT-Drs. 15/10345, S. 9.

⁹² Die darauf aufbauende Ermittlung würde vermutlich so ablaufen: An diese E-Mail-Adresse wird eine E-Mail der Sicherheitsbehörden mit Trojaner-Software als Anhang geschickt. Sobald der (anonyme) Adressat der Mail diesen Anhang auf ein System herunterlädt, würde die Ausspäh-Software mit dem Programmablauf beginnen und nach und nach die auf dem Computer gespeicherten Daten zum Computer der Sicherheitsbehörden über das Netz transferieren. Mit der Zeit *könnte* so herausgefunden werden, ob es sich um die gesuchte Person und „ihr“ System handelt. Selbst wenn die Anordnung den Klarnamen des Adressaten und eine ihm zuordenbare E-Mail-Adresse nennt, wäre auch damit den Bestimmtheitsanforderungen nicht Genüge getan. Allein das Herunterladen eines E-Mail-Anhangs durch den Mail-Adressaten auf einen PC macht diesen noch nicht hinreichend bestimmt zu seinem Computer. Zudem ist das Risiko, hierdurch den Computer eines Unbeteiligten zu infizieren, zu groß.

⁹³ Vgl. hierzu BZ vom 17. 4. 2008, Ressort Politik; siehe auch *Roggan* (Fn. 29), S. 97, 111.

⁹⁴ Dies allerdings nur, sofern sich eine solche Begleitmaßnahme nur auf die physische Infiltration des Systems in der Wohnung beschränkt und durch gesetzliche Vorkehrungen (wie etwa ein absolutes Beweisverwertungsverbot für alle in der Wohnung gesicherten, potentiellen Beweisgegenstände außer dem informationstechnischen System).

⁹⁵ Denn die Eingriffsintensität einer solchen heimlichen Maßnahme in Bezug auf Art. 13 GG ist wesentlich geringer als etwa die der in Art. 13 Abs. 4 geregelten präventiven akustischen Wohnraumüberwachung, die als Ziel die vollumfängliche und heimliche akustische Raumüberwachung zum Gegenstand hat, während Ziel der Infiltration des Systems das heimliche Überwachen des Computers und nicht der Wohnung ist. Selbst bei einem Vergleich mit der offenen Durchsuchung ist es nicht eindeutig, ob diese in Bezug auf Art. 13 GG eine weniger intensive Eingriffsmaßnahme darstellt

⁸⁴ Vgl. hierzu auch *Roggan*, in: *ders.* (Fn. 29), S. 97, 103 ff.

⁸⁵ So bezüglich des Zustandsstörers auch *Baum/Schantz* ZRP 2008, 137, 139. Art. 34d Abs. 1 Nr. 1 PAG kann sich also trotz des weiten Wortlautes (Gefahrverantwortlicher), nur gegen den (potentiellen) Gefahrverursacher und nicht gegen (potentielle) Zustandsstörer richten.

⁸⁶ BayLT-Drs 15/10345, S. 9.

⁸⁷ Womöglich sind dem bayerischen Gesetzgeber bei der Erweiterung des Adressatenkreises die Zuordnungskriterien des Urteils von Person und System nicht vertraut gewesen. Denn die Anordnung, die den Nutzer eines Computers treffen soll, braucht nicht auf den Eigentümer oder Besitzer auszuweichen, der jenem das ihm gehörende System zur Verfügung stellt. Es reicht schon die vom Eigentümer/Besitzer eines Systems an einen Anderen erteilte tatsächliche Nutzungsberechtigung aus, um die passende Zuordnung des Nutzers zu „seinem“ System zu begründen. Siehe hierzu auch oben III.1.b. a. E.

⁸⁸ Vgl. hierzu *Hansen/Pfitzmann*, in: *Roggan* (Fn. 29), S. 131, 140 ff.

⁸⁹ Zwar ist es auch dort möglich, den Betroffenen nicht durch Name und Anschrift sondern, soweit sein „wahrer Name“ nicht bekannt ist, anderweitig zu identifizieren. Jedoch kann auf eine hinreichende Bezeichnung des Eingriffsobjektes wie etwa durch die Kennung des Telekommunikationsanschlusses (§ 100b II Nr. 2 StPO) oder durch Angabe der zu überwachenden Wohnung oder Wohnräume (§ 100d Abs. 2 Nr. 3 StPO) nicht verzichtet werden.

GVIIS auf die Infiltration und das weitere Vorgehen bleibt davon unberührt. Ob man nun eine Änderung des Art. 13 GG verlangt oder nicht, eindeutig ist jedenfalls, dass die dabei gefundene Antwort gleichermaßen gültig ist für den Fall des Eindringens in die Wohnung zwecks physischer Infiltration des Systems zu Zwecken der Quellen-Telekommunikation-Überwachung.⁹⁶

Letztlich handelt es sich hier um eine Frage, die nicht dogmatisch, sondern nur dezisionistisch durch eine Entscheidung des *BVerfG* gelöst werden kann. Verfassungsbeschwerden gegen die bereits in Kraft getretenen bayerischen Sicherheitsgesetze sind in Vorbereitung. Ein neues Verfahren böte nicht nur die Chance, Rechtssicherheit für die angesprochene Frage zu Art. 13 GG zu schaffen, sondern auch auf die Regelungsgehalte einzugehen, welche, mit unterschiedlicher Intensität, den Vorgaben des Urteils widersprechen. So könnte sich zeigen, in welchem Ausmaß das Gericht nicht nur verfassungsrechtliche Maßstäbe aufstellt, sondern auch auf deren Geltung bedacht ist.

b) Umsetzung im Bund

Zur Online-Durchsuchung hat der *BGH* im Januar letzten Jahres in Bezug auf die StPO, das *BVerfG* im Februar diesen Jahres in Bezug auf ein Landesverfassungsschutzgesetz geurteilt. Es war und ist jedoch ein Bundespolizeigesetz, das zwischen den beiden Urteilen den Großteil der öffentlichen Aufmerksamkeit in punkto Online-Durchsuchung absorbiert hat. Dementsprechend gestaltet sich nun die Umsetzung der Urteilsvorgaben im bundespolizeilichen BKA-Gesetz mühsam. Der am 16. 4. 2008 herausgebrachte Referententwurf bedurfte noch einiger Überarbeitungen, bevor er am 4. 6. vom Kabinett beschlossen und dann als Gesetzesentwurf⁹⁷ in den

als die heimliche Infiltration des Computersystems in der Wohnung. Stellt dort doch das Eindringen in die Wohnung nur den Durchgangsschritt zum Eindringen in den Computer und nicht zur Durchsuchung der Wohnung dar. Letztlich kommt es auf folgende Kriterien an: Sind die Voraussetzungen der Gesetzesvorbehalte in Art. 13 GG Abs. 2–7 GG Höchst- oder Mindestanforderungen für vergleichbar intensive Eingriffe? Was ist für die Bewertung der Eingriffintensität maßgeblich? Bedarf ein tatbestandlich neuer Eingriff (Betreten der Wohnung zum Zwecke der Computerinfiltration) eines eigenen geschriebenen Gesetzesvorbehaltes, wenn die Eingriffsschwellen bereits von geschriebenen Vorbehalten gedeckt sind, diese sich jedoch auf andere Tatbestände beziehen? Was bedeutet die in Art. 13 Abs. 7 GG enthaltene „im Übrigen“-Regelung? Zu berücksichtigen ist auch, dass ein präventiver Eingriff in das GVIIS hinter der Voraussetzung „dringende Gefahr“ des Art. 13 Abs. 4 GG zurückbleibt. Neben den spezifischen Besonderheiten des Straftatenkataloges wären im neuen Entwurf u. a. die bislang ausgesparte Einbeziehung von Zeugnisverweigerungsrechten, konsistente Regelungen zu Beweisverwertungsverboten und eine Anpassung des § 110 Abs. 3 StPO und ggf. der §§ 102 ff. StPO an das neue Grundrecht zu berücksichtigen.

96 Ob zu Zwecken der Quellen-TKÜ oder zu Zwecken der Online-Überwachung, die rechtstatsächliche Vorgehensweise ist bis auf die Frage, auf welche Daten auf dem System zugegriffen wird, die gleiche (interessanterweise wird die Eingriffsmaßnahme Quellen-TKÜ, nach Einblick des Verfassers, bisher nur durch physische Infiltration in der Wohnung und nicht durch Online-Infiltration bewerkstelligt, offenbar um das hohe Risiko des Einbeziehens fremder Telekommunikationsanschlüsse zu verhindern). Daher ist das Eindringen in die Wohnung, welches bei der Quellen-TKÜ das Eingreifen in Art. 10 GG vorbereitet, genauso wie das Eindringen in die Wohnung, dass bei der Online-Überwachung das Eindringen in Art. 2 Abs. 1 GG vorbereitet, an Art. 13 GG zu messen (Rn. 193) und bedarf einer ausdrücklichen gesetzlichen Regelung. Ob eine solche gesetzliche Grundlage von Art. 13 Abs. 2–7 GG gedeckt ist, ist offen (s. o.). Soweit jedoch, wie derzeit bei den aufgrund § 100a StPO durchgeführten Maßnahmen der Quellen-TKÜ, ohne formelle gesetzliche Grundlage in die Wohnung eingedrungen wird, sind diese Maßnahmen verfassungswidrig. Zutreffend hier also die Entscheidung des *LG Hamburg* MMR 2008, 423 ff.; wie auch *Sankol* CR 2008, 13 ff. Anders wohl die aufgrund eines laufenden Ermittlungsverfahrens noch nicht veröffentlichte Entscheidung des *BGH*-Ermittlungsrichters (vgl. *Bär* MMR 2008, 425) und *Bär*, ebd. S. 426, der dabei jedoch übersieht, dass Rn. 190 des Urteils nur Maßstäbe für den Vorgang der Überwachung aufstellt, Maßstäbe für die physische Infiltration des Systems jedoch in Rn. 193 zu finden sind.

97 BR-Drs./08 16/9588.

Bundestag eingebracht werden konnte. Dort fand am 20. 6. die erste Lesung statt, Expertenanhörungen, Änderungsanträge und weitere Parlamentsdebatten lassen den Gesetzgebungsprozess wahrscheinlich noch bis Ende des Jahres andauern.

Der Entwurf soll in § 20k BKA-G das Bundeskriminalamt zum „Eingriff mit technischen Mitteln in vom Betroffenen genutzten informationstechnischen Systemen ohne dessen Wissen“ ermächtigen. Einige Punkte des Entwurfs fordern zu einer Stellungnahme heraus.⁹⁸ Dieser Aufsatz soll sich jedoch darauf beschränken, das Augenmerk auf einen bereits im April 2008 zwischen den Koalitionsparteien geschlossenen Kompromiss zu lenken,⁹⁹ der dafür den denkbar ungünstigsten Ansatzpunkt wählte. BMJ und BMI hatten sich darauf geeinigt, genau die Variante der Infiltration des Computersystems auszuschließen, welche die technisch hinsichtlich Zielgenauigkeit und Qualität der Beweissicherung erfolversprechendste¹⁰⁰ und damit am meisten geeignete ist, die zugleich unbeteiligte Dritte am meisten schont¹⁰¹ und damit die am meisten verhältnismäßige Maßnahme darstellt: Die physische Infiltration des Computersystems, meist vorbereitet durch ein Betreten der Wohnung, in der das System steht.¹⁰²

Ein solches Vorgehen wird zwar noch von der Einschätzungsprärogative des Gesetzgebers gedeckt sein, will heißen: das Unterbinden der verhältnismäßigsten Methode der Infiltration macht das Gesetz im Ganzen noch nicht unverhältnismäßig. Allerdings stellt sich die Frage, ob hier nicht das Kind mit dem Bade ausgeschüttet wird. Sobald das *BVerfG* die oben thematisierte Frage zu den Gesetzesvorbehalten von Art. 13 GG entschieden hat, sollte eine Kursänderung in diesem Punkt noch einmal ernsthaft in Betracht gezogen werden.

c) Umsetzung in der StPO

„Deutschlands Marktführer Innere Sicherheit“¹⁰³ hat – um das von der bayerischen Staatsregierung gewählte Sprachspiel aufzugreifen, keine Mühen gescheut, das Rechtsprodukt Online-Durchsuchung nicht nur über das Verfassungsschutz- und Polizeigesetz, sondern auch über den Vertriebskanal Strafprozessrecht auf den Markt zu bringen. Dies entbehrt nicht einer gewissen ökonomischen Logik, denn die Wertschöpfungskette wäre unvollständig, würde man bei der polizeilichen Online-Durchsuchung gefundene Beweise mangels entsprechender Rechtsgrundlage nicht im Straf-

98 Wie z. B. die Möglichkeit der relativ unbeschränkten Weitergabe der durch das BKA-Gesetz gewonnenen Daten an den Verfassungsschutz oder das Überspringen der ersten Stufe des zweistufigen Schutzkonzeptes für den Kernbereich privater Lebensgestaltung. Vgl. zu diesen und anderen problematischen Gesichtspunkten auch *Baum/Schantz* ZRP 2008, 137 ff.

99 Siehe hierzu Meldung 106540 (15. 4. 2008) von heise online, abrufbar unter www.heise.de.

100 Vgl. hierzu nur statt vieler *Hansen/Pfitzmann*, in: *Roggan* (Fn. 29), S. 131, 145, die die Netzinfiltration auch vom Ergebnis der Beweissicherung wie von der Zielgenauigkeit als die schlechteste Methode und gegenüber der physischen Infiltration als deutlich unterlegen qualifizieren.

101 Da hier die Streuverluste und das Risiko, in die Grundrechte unbeteiligter Dritter einzugreifen, am geringsten sind. Vgl. hierzu *Hansen/Pfitzmann*, in: *Roggan* (Fn. 29), S. 131, 147 f. Nach dem Urteil ist das Ausmaß des Risikos des Eingreifens in Grundrechte Dritter ein gewichtiger Punkt der Angemessenheitsprüfung (Rn. 239, 241).

102 Soweit sich dieser (heimliche) Wohnungszutritt strikt auf das Betreten der Wohnung zu Zwecken der Systeminfiltration beschränkt und nicht zu einer heimlichen Wohnungsdurchsuchung missbraucht wird, stellt diese Maßnahme nach Auffassung des Verfassers trotz des Eingriffs in Art. 13 GG auch weiterhin die verhältnismäßigste dar.

103 Vgl. die Pressemitteilung des Bayerischen Innenministeriums vom 31. 5. 2008.

verfahren weiterverwerten können. So reichte der Freistaat Bayern am 27. 5. 2008¹⁰⁴ im Bundesrat einen Antrag zur Verabschiedung eines neuen § 100k StPO ein, der die Ermittlungsbehörden zum „Zugriff auf informationstechnische Systeme mit technischen Mitteln ohne Wissen des Betroffenen“ ermächtigen sollte. Dieser Antrag ist am 4. 7. 2008 im Plenum des Bundesrates gescheitert. Wahrscheinlich wird ein nächster Anlauf erst nach Einführung der Online-Durchsuchung im BKA-Gesetz erfolgen. Zeit genug also, über Anforderungen an die verfassungsrechtliche „Marktreife“ der Online-Durchsuchung in der StPO¹⁰⁵ nachzudenken.

Maßstäbe hierfür bietet das Urteil des *BVerfG* kaum. Es heißt dort lediglich, dass Eingriffe in das GVIIS auch zu Zwecken der Strafverfolgung gerechtfertigt sein können (Rn. 207). Ein erster Ansatz kann es allerdings nicht sein, so wie es der bayerische Vorschlag vorgesehen hatte, den Straftatenkatalog des § 100c Abs. 2 Nr. 1 StPO weitgehend unbeeinträchtigt zu übernehmen, denn die Eingriffsvoraussetzungen von Lauschangriff und Computerzugriff sind doch andere. So bedarf etwa der Eingriff in das GVIIS einer Gefahr für „überragende“ Rechtsgüter, die sich nicht per se als schwere (§ 100a Abs. 2 StPO) oder besonders schwere Straftaten (§ 100c Abs. 2 StPO), und damit im Wesentlichen über das Strafmaß definieren. Insbesondere sollte nicht übersehen werden, dass es hier nicht um Leib, Leben Freiheit *einer* Person, sondern *der* Person geht, die es zu schützen gilt. Dies wird auf eine Ebene mit Gefahren für Grundlage und Bestand des Staates und der Existenz *der* Menschen gestellt. In Anbetracht dieses weniger auf die individuelle Freiheit sondern mehr auf die Grundlagen der Freiheit abstellenden Rechtsgüterschutzes wäre die Frage zu stellen, ob es nicht in erster Linie nur die in § 100k Abs. 2 Nr. 1a, b StPO-E enthaltenen Straftatbestände sind, auf die sich der Verdacht zu richten hat. Außerdem haben sich die Anforderungen an eine konkrete Gefahr im Straftatenkatalog widerzuspiegeln, Vorfeld- wie abstrakte Gefährdungsdelikte haben es somit schwer, in den Katalog aufgenommen zu werden. Es wäre ersichtlich vom Gericht nicht gewollt, über die Hintertür des Strafverfahrens die für das Sicherheitsrecht ausdrücklich ausgeschlossene Vorfeldermittlung doch wieder zum Teil der zulässigen Netzermittlung werden zu lassen. Neben den spezifischen Besonderheiten des Straftatenkataloges wären im neuen Entwurf unter anderem die bislang ausgesparte Einbeziehung von Zeugnisverweigerungsrechten, konsistente Regelungen zu Beweisverwertungsverböten und eine Anpassung des § 110 Abs. 3 StPO und ggf. der §§ 102 ff. StPO an das neue Grundrecht zu berücksichtigen.¹⁰⁶

¹⁰⁴ BT-Drs. 365/08.

¹⁰⁵ Aufschlussreich zu den technischen und rechtstatsächlichen Herausforderungen der Strafverfolgungsbehörden bei der Netzermittlung *Gercke* MMR 2008, 291 ff.; siehe zu den rechtlichen Herausforderungen aufgrund des Urteils auch *Kühne*, in: *Roggan* (Fn. 29), S. 85 ff.

¹⁰⁶ Es verwundert etwas, dass der bisherige StPO-Entwurf, anders als sogar die Polizeigesetze, keine Zeugnisverweigerungsrechte als stets neuralgischen Punkt des Strafverfahrens, regelt. Anders als bei den bisherigen §§ 100a bzw. 100c StPO werden die dort uneingeschränkt geregelten Beweisverwertungsverböten in Bezug auf Kernbereichsdaten bei § 100k Abs. 4 Satz 3 StPO-E wieder einschränkt. Dort sollen die Verwertungsverböten bereits dann nicht mehr gelten, wenn (bloß) Anhaltspunkte dafür bestehen, dass (Kernbereichs-)Daten dem Zweck der Herbeiführung eines Erhebungsverbötes dienen sollten. Gesonderter Regelungen zu Beweisverwertungsverböten bedarf es bezüglich der Weiterverwertung der im präventiven Verfahren durch Computerzugriffe gewonnenen Informationen im Strafverfahren. Hier gilt es, strikt darauf zu achten, dass die Eingriffsvoraussetzungen des Strafverfahrens nicht durch geringere Anforderungen der Polizeigesetze unterlaufen werden. Vgl. zur Anpassung von § 110 Abs. 3 StPO und ggf. §§ 102 ff. StPO an das neue Grundrecht oben III. 2. b bb.

IV. Aufklärung des Internet

Der sich mit der „Aufklärung des Internet“ befassende Abschnitt II der Entscheidungsgründe steht in der bisherigen juristischen Rezeption wie in der öffentlichen Aufmerksamkeit im Schatten des Abschnittes I und der dort behandelten Online-Durchsuchung. Dies wird der Bedeutung dieses Abschnittes nicht gerecht, sind doch die dort gemachten Ausführungen zum RiS und zu Art. 10 GG ebenso erstmalig und grundlegend wie die zum neuen Grundrecht.

1. Neues zum Recht auf informationelle Selbstbestimmung

a) Rehabilitierung der Öffentlichkeitssphäre

Die eigentlichen Aussagen zum informationellen Selbstbestimmungsrecht finden sich nicht am Anfang des Urteils, bei der Herleitung des GVIIS aus den Schutzlücken des RiS, sondern nahezu am Ende der materiellen Begründung. Dort wird der Unterscheidung öffentlich/privat im Kontext des RiS wieder zur normativen Geltung verholfen: „Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt.“ Und danach folgt ein Satz, der manchem Apologeten des „belanglosen Datums“ als Kehrtwende erscheinen mag, tatsächlich doch nur eine Klarstellung mit Augenmaß und Realitätssinn ist: „Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können“ (Rn. 308). Die Rehabilitierung der Öffentlichkeitssphäre war dem Gericht so wichtig, dass es die betreffenden Aussagen in die Leitsätze aufnahm.

Das Gericht hat sich damit auch ausdrücklich der vom Verfasser seinerzeit in Auseinandersetzung mit dem APKR und dem RiS herausgearbeiteten Aussage angeschlossen, wonach sich bei der Suche nach Informationen im Netz die Schwelle für den Eingriff in Art. 2 Abs. 1 GG anhand der Unterscheidung einer geschützten Privatsphäre und einer grundsätzlich nicht geschützten Öffentlichkeitssphäre bestimmen lässt.¹⁰⁷ Damit hat es den Ansichten eine Absage erteilt, die in Anlehnung an die missverständliche Formulierung im Urteil zum RiS über ein „belangloses Datum“¹⁰⁸ Thesen, wonach der Schutz der Informationen in keinem Fall mehr von der Sphäre abhängt, aus der die Informationen stammen,¹⁰⁹ zur allumfassenden Geltung verhelfen wollten. Die Rehabilitierung der Öffentlichkeitssphäre im Netz bedeutet allerdings nicht, dass diese ein rechtsfreier Raum wäre. Im Gegenteil, die Veröffentlichung einer Information über das Internet ruft ganz eigene, neue Gefahren hervor,¹¹⁰ denen allerdings weniger durch die Abwehr staatlichen Handelns beizukommen ist.

In Ausnahmefällen soll allerdings auch die Datenerhebung in der Öffentlichkeitssphäre noch einen Eingriff in das RiS begründen können: Wenn allgemein zugängliche Inhalte gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten

¹⁰⁷ *T. Böckenförde* (Fn. 7), S. 184 ff.

¹⁰⁸ Diese Formulierung bezog sich nur auf die automatisch weiterverarbeiteten Daten, vgl. *BVerfGE* 65, 1, 45.

¹⁰⁹ Vgl. hierzu die Nachweise in *T. Böckenförde* (Fn. 7), S. 182, Fn. 75–77.

¹¹⁰ Zu denken ist hier z. B. an das längere digitale Gedächtnis der Web-Öffentlichkeit, den Wandel von der standardisierten Tages- zur individualisierten Minutenpresse, der etwa den presserechtlichen Gegendarstellungsanspruch nahezu funktionslos werden lässt, die Abwehr neuer Formen der Beleidigung bis Verleumdung (elektronischer Pranger), oder die Tatsache der immensen weltweiten Verbreitungsgeschwindigkeit digitaler Information.

ausgewertet werden und sich daraus eine besondere Gefährdungslage für die Persönlichkeit des Betroffenen ergibt (Rn. 309). Wann eine solche Gefährdungslage überhaupt gegeben sein kann, bleibt unklar. Die Nutzung von herkömmlichen Suchmaschinen im WWW kann damit jedenfalls nicht gemeint sein, ist doch der Gebrauch solcher Maschinen schon in der Hyperlink-Struktur des Web angelegt und als Bestandteil der Navigation dort so elementar, dass eine Einschränkung der Suchmaschinennutzung gleichsam hieße, das Surfen im Web an sich einzuschränken.

b) Eingriffsschwelle

Die Eingriffsschwelle bei der „Aufklärung des Internet“, also der Nutzung von Anwendungsdiensten des Internet, wie etwa WWW, Mailinglistendienste, Chatdienste (Rn. 308) oder Diskussionsforen (Rn. 311) wird vom Gericht im Wesentlichen anhand der vom Verfasser seinerzeit herausgearbeiteten Kriterien vorgenommen.¹¹¹ Bei der Bestimmung dessen, was im Netz zu einem offenen bzw. öffentlichen Bereich gehört, ist zunächst der Zugang zu dieser Information als wesentlicher Anknüpfungspunkt zu begreifen, dann aber nicht auf die Ausgestaltung des Zugangsmodus oder die Intensität des technischen Zugangsschutzes, sondern auf den *Verteilungsmodus* der *Zugangsberechtigung* abzustellen.¹¹² Soweit diesem Verteilungsmodus eine den Nutzer hinreichend individualisierende Funktion zukommt, vermittelt die so erlangte Zugangsberechtigung den Zugang zu einem geschlossenen oder privaten Bereich.¹¹³ Wenn es sich bei der Zugangsberechtigung z. B. um ein alphanumerisches Passwort handelt, kommt es darauf an, wie das Passwort verteilt wird. Bekommt der Nutzer das Passwort nur nach Vorlage eines Ausweises, nur aufgrund persönlicher Bekanntschaft oder nur aufgrund der Mitgliedschaft in einem Verein zugeeignet, dann vermittelt das Passwort den Zugang zum grundrechtlich geschützten Bereich etwa eines Chat-, Mailinglisten- oder Newsdienstes.

Das Beispiel im Urteil, wonach selbst bei Verdichtung von Kommunikationsbeziehungen innerhalb eines Diskussionsforums oder Chat-Raumes zu einer „elektronischen Gemeinschaft“ die Teilnahme daran keinen Eingriff darstellt, begründet sich genau damit, dass für die Identität der Kommunikationsteilnehmer keine Überprüfungsmechanismen bestehen (Rn. 311). Ergo: Durch einen hinreichend individualisierten Verteilungsmodus der Zugangsberechtigung wird eine solche Überprüfungsmechanismen geschaffen, die Gemeinschaft bzw. Kommunikationsbeziehung wird so von einer offenen zu einer geschlossenen und damit zur grundrechtlich schutzwürdigen. Allerdings soll in Ausnahmefällen selbst bei offenen Diensten in das RiS eingegriffen werden können, soweit der staatliche Aufklärer bei seinem Gegenüber das schutzwürdige Vertrauen in seine Identität und Motivation ausnutzt. Wo hier die Grenze zwischen der nicht schutzwürdigen elektronischen Gemeinschaft (Rn. 311) und dem schutzwürdigen Vertrauen in die Identität und Motivation des Kommunikationspartners liegt (Rn. 310), bleibt ein Geheimnis, das nur das *BVerfG* lüften kann.

2. Neues zu Art. 10 GG

a) Eine neue Unterscheidung

Im Urteil wird zum ersten Mal seit Bestehen des Art. 10 GG zwischen zwei verschiedenen Eingriffsformen in potentiell dieselben Telekommunikationsinhalte unterschieden: Der

Teilnahme an der Telekommunikation (Rn. 290–299) und der Überwachung der Telekommunikation (Rn. 182–190). Bei der Überwachung ist der Betroffene stets vor der staatlichen Wahrnehmung von Telekommunikationsinhalten geschützt (Rn. 290), bei der Teilnahme nur unter bestimmten Voraussetzungen. Dies kann zur Folge haben, dass die gleichen Inhalte desselben Kommunikationsdienstes, wie etwa eines bestimmten Chat-Dienstes, je nach Zugriffsform von Art. 10 GG unterschiedlich geschützt werden.

Wie kommt es zu dieser Unterscheidung? Sie stellt zum einen eine Fortführung des bereits in vorigen Urteilen eingeführten Grundsatzes dar,¹¹⁴ wonach die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner von Art. 10 GG nicht geschützt ist (Rn. 290). Da das Vertrauen in den Kommunikationspartner nicht geschützt ist, ist auch grundsätzlich die Kenntnisnahme der Inhalte als teilnehmender Kommunikationspartner „von drinnen“ rechtlich weniger problematisch als die Kenntnisnahme der Inhalte als unbeteiligt Überwachender „von draußen“. Zum anderen ist sie eine Konsequenz der nicht unbedingt nahe liegenden Wertung des Gerichts, die *Nutzung* der gebräuchlichsten Anwendungsdienste des Internet erst einmal im weitesten Sinne als Teilnahme an einer Kommunikation (Rn. 291 ff.) aufzufassen und damit Art. 10 GG als (Fern-)Kommunikationsgrundrecht für einschlägig zu erachten. Diese weite Öffnung des Schutzbereiches macht es notwendig, für Art. 10 GG einen im Unterschied zur herkömmlichen Überwachung ganz neuartigen Eingriffsbereich der Teilnahme zu schaffen.

b) Teilnahme an der Telekommunikation

Als Beispiel für die an Art. 10 GG zu messende Teilnahme an „Kommunikationsdiensten des Internet“ (Rn. 291) werden im Urteilstext Mail-Dienste (Rn. 293), Chat-Dienste (Rn. 292, 293), Diskussionsforen (Rn. 293) und der WWW-Dienst (Rn. 293) genannt. Als Beispiel für die am RiS zu messende Nutzung der (Kommunikations-)dienste des Internet werden Mailinglistendienste (Rn. 308), Chatdienste (Rn. 308), Diskussionsforen (Rn. 311) und der WWW-Dienst (Rn. 308) genannt. Bei der Aufklärung des Internet lässt sich die Trennlinie zwischen Schutz- und Eingriffsbereich dieser beiden Grundrechte überhaupt nur nachvollziehbar bestimmen und damit auch die im Urteil zu beiden Grundrechten getroffenen Aussagen in Einklang bringen (Rn. 291–293; Rn. 305; Rn. 308, 311), soweit auf das bereits herausgearbeitete Kriterium des Verteilungsmodus der Zugangsberechtigung abgestellt wird. Falls die Zugangsberechtigung die einzelnen Kommunikationspartner hinreichend individualisiert und dadurch ein geschlossener bzw. privater Bereich geschaffen wird, ist der Schutzbereich des Art. 10 GG eröffnet. In diesen wird eingegriffen, wenn sich die Ermittlungsbehörden den Zugang zu geschlossenen Diensten durch verdeckte Erhebung der Zugangsberechtigung (Rn. 292, Keylogging, Ausspähen des Computers) oder durch sonstiges unautorisiertes Erlangen der Zugangsberechtigung von einem autorisierten Kommunikationspartner (Rn. 291) verschafft haben. Soweit sich die Teilnahme an den Kommunikationsdiensten im öffentlichen bzw. allgemein zugänglichen Bereich bewegt, ist das RiS einschlägig und es gelten die im vorigen Abschnitt aufgezeigten Maßstäbe.

Selbst bei einem sehr weit gefassten Kommunikationsbegriff wird man nicht alle Nutzungsformen der Anwendungsdienste des Internet stets als Kommunikation auffassen

¹¹¹ Vgl. T. Böckenförde (Fn. 7), S. 191–206.

¹¹² T. Böckenförde (Fn. 7), S. 195 f.

¹¹³ T. Böckenförde (Fn. 7), S. 205 f.

¹¹⁴ Vgl. *BVerfGE* 106, 28, 37 f.

können. Zu denken ist hier etwa an die Nutzung des WWW als Plattform zum elektronischen Einkaufen, bezahlungspflichtiger Mediennutzung (Bilder, Video, Musik), Online-Banking, Präferenzlisten, Abonnieren von Nachrichten etc. Auch bei der Nutzung dieser Dienstleistungen gibt es private und geschlossene Bereiche, die durch individualisierte Verteilung einer Zugangsberechtigung (Benutzername, Passwort, PIN, TAN etc.) geschaffen werden, bei denen aber dem Grundrechtsträger kein individueller Kommunikationspartner gegenübersteht. Sind diese Bereiche, die ja zum Teil veritabler Teil der persönlichen Lebensentfaltung sind¹¹⁵, wenn nicht mehr von Art. 10 GG, so denn überhaupt noch geschützt? Sie sind es – und zwar vom GVIIS. Hier zeigt sich die Integrationskraft des Begriffs „informationstechnisches System“ und das brauchbare Kriterium der „tatsächlichen Nutzungsberechtigung“ als Maßstab für die personale Zuordnung eines Systems zum Grundrechtsträger. Denn diese vom eigenen System physisch ausgelagerten Bereiche der eigenen Persönlichkeitsentfaltung werden dann zum Teil des „eigenen“ Systems und damit Teil des fortgeführten Persönlichkeitsrechts, soweit die dort abgelegten Daten mittels einer hinreichend individualisierten Zugangs- und Nutzungsberechtigung vom eigenen Computer aus über das Netz erreichbar sind. Mit der Konsequenz, dass ein Zugriff auf die dort gespeicherten Informationen durch den Staat, etwa mit Hilfe eines heimlich erlangten Passwortes, sich nicht nach den Eingriffsmaßstäben des Art. 10 GG, sondern nach den strengeren Eingriffsvoraussetzungen des GVIIS richtet.

Daran ändert auch die einige Absätze weiter getroffene Entscheidung des Urteils nichts, nach der die Ermächtigung bei Kreditinstituten Auskünfte zu Kontodaten, Geldbewegungen und Geldanlagen einzuholen, am RiS zu messen ist (Rn. 314). Bei Kontodaten lässt sich die Abgrenzung zwischen RiS und GVIIS so ziehen: Soweit diese Daten auf dem System des Nutzers gespeichert sind, z. B. auf dem vom individualisierten Nutzer über das Web berechtigt erreichbaren Online-Banking-Server oder auf dem als Client fungierenden System des Nutzers zu Hause, stellt der Zugriff auf diese Systeme, sei es über eine Ausspäh-Software, sei es über eine verdeckt erlangte Zugangsberechtigung, einen Eingriff in das GVIIS dar. Soweit die Daten von dem Betreiber des Servers, wie hier etwa dem Kreditinstitut, auf Verlangen des Staates herausgegeben werden, stellt dies einen Eingriff in das RiS dar. Diese Wertung ist sachgerecht, da der erste Eingriff nicht nur auf höchst vertrauliche Daten zugreift, sondern auch die Integrität des eigenen informationstechnischen Systems erheblich beeinträchtigt. Allerdings macht dieser Fall auch klar, dass die Abgrenzung von RiS zu GVIIS noch weiter klärender und konturierender Aussagen des Gerichts bedarf.

c) Überwachung der Telekommunikation

Was bei der Teilnahme an der Telekommunikation die Abgrenzung von Art. 10 GG zum RiS, ist bei der Überwachung der Telekommunikation die Abgrenzung von Art. 10 GG zum GVIIS. Hier gilt es, die Trennlinie zwischen zwei Formen der Überwachung zu ziehen, die beide auf ein (ggf. auch das gleiche) informationstechnische System zugreifen, durch gleiche Methoden der Infiltration gekennzeichnet sind und die sich letztlich nur dadurch unterscheiden, dass sie auf dem System

auf andere Arten von Daten zugreifen:¹¹⁶ Die Quellen-Telekommunikations-Überwachung (Quellen-TKÜ) und die Online-Überwachung. Während die Online-Überwachung die „längerfristige Überwachung der Nutzung des Systems“ (Rn. 234) sowie die „längerfristige Überwachung der Internetkommunikation“ (Rn. 235, 236) ermöglichen soll, bezieht sich die Quellen-TKÜ „ausschließlich auf Daten aus einem „laufenden Telekommunikationsvorgang“ (Rn. 190). Und was also ist der Unterschied zwischen Internetkommunikation und Telekommunikation? Die Antwort auf die Frage ist ebenso interessant wie brisant. Wiewohl erst im August 2007 im Vorfeld der mündlichen Verhandlung an das Licht der Öffentlichkeit gedrungen, ist die Quellen-TKÜ und nicht die Online-Überwachung die bereits stetig praktizierte Methode der Überwachung, die eine Infiltration des informationstechnischen Systems voraussetzt. Und sie hat, da sie unter die hergebrachte TKÜ-Ermächtigungen (insbesondere § 100a StPO) subsumiert wird, deutlich geringere Eingriffshürden zu überwinden als die Online-Überwachung.¹¹⁷

Man wird die Abgrenzung weniger begrifflich¹¹⁸ oder teleologisch¹¹⁹, sondern in erster Linie nur phänomenologisch¹²⁰ vornehmen können. Zur „laufenden Telekommunikation“ gehört unstreitig die Sprachtelefonie-(Voice-over-IP), daneben wird man auch Videotelefonie- und Chatdienste (Textelefonie) dazurechnen können.¹²¹ Aber auch asynchrone Dienste, wie etwa E-Mail, sind ausdrücklich vom Telekommunikationsgeheimnis geschützt (Rn. 183); dann besteht kein Grund mehr, asynchronen Messagediensten wie Mailinglistendiensten die grundrechtliche Schutzwürdigkeit zu verweigern. Was nicht dazugehört, ist die Nutzung des WWW, von Blog-, News-, Streaming- und Dateitauschdiensten, ebenso wenig wie die Überwachung der Computernutzung an sich, zu der auch die Synchronisation mit selbst nicht notwendig schutzwürdigen Systemen (Kamera, MP3-Player, PDA etc.) gehört.

¹¹⁶ So auch die Antwort der Bundesregierung auf eine Abgeordneten-anfrage vom 30. 10. 2007 (BT-Drucks. 16/6885, Frage 14).

¹¹⁷ Vgl. zu den Anforderungen an die Eingriffsvoraussetzungen der Quellen-TKÜ Fn. 96.

¹¹⁸ Der Telekommunikationsbegriff ist schlichtweg überfordert, hier eine Abgrenzungsleistung erbringen zu können; vgl. zur Hermeneutik des Telekommunikationsbegriffs T. Böckenförde (Fn. 7), S. 431 ff.

¹¹⁹ Schutzzweck des GVIIS ist in diesem Zusammenhang, informationstechnische Systeme als Vehikel der Persönlichkeitsentfaltung auch dann zu schützen, wenn das System genutzt wird, um über das Internet oder andere Netzwerkprotokolle Informationen mit anderen Systemen auszutauschen, auch wenn es dabei zur sozialen Kommunikation mit anderen Nutzern kommt (Rn. 176, 235, 236). Schutzzweck von Art. 10 GG ist es, individuelle Kommunikation zu schützen, wenn sie wegen ihrer Vertraulichkeit auf die Übermittlung Dritter angewiesen ist (vgl. nur BVerfGE 115, 166, 182). Dieser Schutz kann sich auch auf die Endgeräte der Kommunikation wie etwa informationstechnische Systeme erstrecken (Rn. 184), soweit der Kommunikationsvorgang noch nicht abgeschlossen ist (Rn. 185, 190). Auf dem informationstechnischen System treffen also beide Schutzrichtungen ungeschützt aufeinander.

¹²⁰ Und zwar anhand ähnlicher Erscheinungsmerkmale wie den im Urteil der Telekommunikation zugerechneten Diensten der Sprachtelefonie (Rn. 272) und E-Mail (Rn. 183).

¹²¹ Videotelefonie als Vehikel der Gebärdensprache gehört ebenfalls zur laufenden Telekommunikation, schon um Ungleichbehandlungen tauber und stummer Grundrechtsträger zu vermeiden. Chatdienste haben mit Sprach- und Videotelefonie das Erscheinungsmerkmal der Synchronität gemeinsam und entsprechen damit einer wichtigen Schutzrichtung des Art. 10 GG, nach der „die Beteiligten weitestgehend so gestellt werden sollen, wie sie bei einer Kommunikation unter Anwesenden stünden“ (vgl. BVerfGE 115, 166, 182). Bis auf die Unterschiedlichkeit der Ausdrucksform (Texten/Sprechen), auf die es für die Schutzwürdigkeit nicht ankommt (vgl. nur Jarass, in: Jarass/Pieroth [Fn. 32], Art. 10 Rn. 9) sind Chatdienste vom Erscheinungsbild herkömmlichen Telefon-(Konferenz)diensten näher als asynchrone Mäildienste, die phänomenologisch zwischen traditionellem Brief- und Telefonverkehr oszillieren.

¹¹⁵ Wie etwa Bank- und Gehaltsdaten, Präferenzliste von Filmen, private Bilder, Lese- und andere Gewohnheiten etc.

Die Differenzierung des Eingriffsobjekts beider Überwachungen muss sich nicht nur rechtlich, sondern auch technisch vollziehen lassen, sonst leidet diese Abgrenzung, wie all die häufig vorkommenden rechtlichen Definitionen, die nicht auf die Kompatibilität von Recht und Technik achten, an intrinsischen Vollzugsdefekten. Rechtlich wie technisch¹²² wird man die Differenzierung nicht genauer als anhand typisierter¹²³ Anwendungsdienste vornehmen können, auch wenn so Restunschärfen verbleiben. Ein so weitgehender Individualisierungsgrad der Kommunikationspartner wie bei der *Teilnahme* ist zur Begründung der Eingriffsschwelle bei der *Überwachung* der Telekommunikation nicht veranlasst. Zudem wäre es technisch von vornherein kaum zu überprüfen, ob etwa das überwachte Chatten innerhalb eines geschlossenen oder offenen Chatraumes abläuft.

Bei auf dem System gespeicherten Verbindungsdaten (Nutzungsdaten) hört die Differenzierung zwischen Art. 10 GG und GVIIS auf. Diese Daten sind, egal ob sie Auskunft über Art und Umstände der Telekommunikation (Rn. 185) oder etwa über Art und Umstände der Web-Nutzung (Rn. 188, 236) oder anderer Dienste geben, nach der ausdrücklichen Wertung des Gerichts nur dem Schutz- und Herrschaftsbereich des GVIIS zuzurechnen.¹²⁴

V. Wie geht es weiter?

1. Vertraulichkeit

Das Urteil bringt Veränderungen. Das Gericht hat durch sehr großzügiges Hantieren mit dem Kommunikationsbegriff die Konvergenz der Schutzbereiche von Art. 10 GG und Art. 2 Abs. 1 GG beschleunigt. Ein neues (ungeschriebenes) Grundrecht wurde geschaffen. Im Internet wurde die Öffentlichkeitssphäre rehabilitiert. Das informationelle Selbstbestimmungsrecht ist in seinem Schutzbereich neu umrissen, hergebrachte Begründungslinien seines Schutzbereichs sind abgeschwächt worden. Die in der Literatur inzwischen auch monographisch aufgearbeitete Kritik an der realitätsfernen Gewährleistung eines eigentumsähnlichen Rechts,¹²⁵ jederzeit selbstbestimmt über sein Persönlichkeitsbild verfügen zu können¹²⁶, hat im Urteil implizit Widerhall gefunden durch eine Akzentverschiebung von der Autonomie hin zu einem anderen dogmatischen Leitbild: Vertraulichkeit bzw. Vertraulichkeitserwartung.

Fast wie ein roter Faden durchzieht der Begriff „Vertraulichkeit“ das Urteil.¹²⁷ Damit einhergehend wird die Figur des sich informationell selbst Bestimmenden zurückgedrängt, indem etwa Erwartungen an die Gewährleistung der Sicherheit des Systems durch technischen Selbstschutz zurückgeschraubt (Rn. 180), Erwartungen an den Staat, sich um die Sicherheit der Informationstechnologie zu bemühen, hochgeschraubt werden (Rn. 241). Ob die „normative Festlegung berechtigter Vertraulichkeitserwartungen“ sich eignet, „ein

zentraler Mechanismus der Zuteilung von Daten- und Informationsschutzrechten zu sein“,¹²⁸ darf bezweifelt werden. Damit würde lediglich die eine übersteigerte Erwartung, nämlich die, dass jeder selbstbestimmt über sein Persönlichkeitsbild in der Öffentlichkeit verfügen kann, durch eine andere übersteigerte Erwartung ersetzt, nämlich die des Vertrauens darauf, dass der Staat die Vertraulichkeit und Integrität der Computer- und Netzarchitektur seiner Bürger technisch zu sichern und schützen imstande ist. Gesucht wird ein anderer Begriff, der die Entwicklungen der Grundrechtsdogmatik in Art. 2 Abs. 1 GG wie Art. 10 GG und, als drittem im Bundeskommunikationsbezogener Freiheitsrechte, Art. 5 GG, in Bezug auf Netzsachverhalte bündeln und integrieren kann.

2. Privatsphäre

Hierzu ist auf die bislang ausgesparte Abgrenzung des GVIIS zu einer weiteren Ausprägung des APKR einzugehen: dem Schutz der Privatsphäre. Dieses Recht verwirft das Gericht als untauglich zum Schutz der neuen Gefährdungen, da es sich nur auf inhaltlich private Daten beziehe (Rn. 197). Ist dem so? Jedenfalls der Begriff Privatsphäre, wenn man zunächst das Augenmerk auf den zweiten Bedeutungsteil des Wortes lenkt („Sphäre“), stellt nicht in erster Linie auf einen privaten Inhalt der Daten ab, sondern auf einen abgrenzbaren Bereich, eine Zone, deren Umrisse sich nicht zwangsläufig durch das bestimmen, was umrissen wird. So verhält es sich etwa bei der räumlichen Privatsphäre, die das, was im Raum bzw. der Wohnung geschieht, als privat behandelt, unabhängig davon, wie privat der Inhalt der Gespräche nun sein mag.

Im Urteil verwendet das Gericht zweimal selbst die Struktur eines bereichsbezogenen Persönlichkeitsschutzes, bei dem die Schutzwürdigkeit der digitalisierten Information nicht an deren Inhalt festgemacht wird. Zum einen bei der Rehabilitierung der Öffentlichkeitssphäre als Komplementär zur Privatsphäre, die durch das Kriterium der allgemeinen Zugänglichkeit und Offenheit definiert wird und nicht durch den Inhalt der darin enthaltenen Informationen, die auch personenbezogen oder privat sein können. Und dann bei der Begründung des neuen Grundrechts selbst. Informationen auf dem Computer sind nicht ob ihres Inhaltes sondern deshalb der vom Gericht so benannten, „besonders geschützten Zone der Privatheit“ (Rn. 257) zuzurechnen, weil sie auf einem Vehikel der Persönlichkeitsentfaltung gespeichert sind: Dem eigenen informationstechnischen System. Erst die Bestimmung des „Kernbereichs privater Lebensgestaltung“ soll nahezu ausschließlich nach dem Inhalt der gespeicherten Informationen erfolgen, was dessen Bestimmbarkeit wesentlich erschwert.

Wo genau die Grenzen zwischen privat und öffentlich liegen, darüber lässt sich trefflich streiten, zudem unterliegen diese Begriffe einem steten Bedeutungswandel. So liegt der Vorteil der Dichotomie privat/öffentlich weniger in ihrer Präzision, sondern darin, ein Begriffspaar mit Bedeutungsgehalt zur Hand zu haben, *entlang dessen* sich die Bestimmung des rechtlich Schützenswerten und nicht Schützenswerten nachvollziehbar ausformen und konturieren lässt.¹²⁹ Zudem kommt dem Begriff „privat“ eine hohe integrative Kraft zu, Akzentverschiebungen der Grundrechtsrechtsprechung, wie etwa die oben dargestellte von Autonomie zu Vertraulichkeit, lassen sich von der „Privatsphäre“ gut auf-

¹²² Als technische Kennung eines standardisierten Anwendungsdienstes könnte etwa die im TCP-Paket der Datenübertragung enthaltene Post-Nummer des Dienstes fungieren.

¹²³ Mit „typisiert“ ist gemeint, dass sich Anwendungsdienste des Internet nur begrenzt systematisieren lassen und in ihren Merkmalen überschneiden können; vgl. hierzu T. Böckenförde (Fn. 7), S. 37 ff.

¹²⁴ Vgl. hierzu Buermeyer RDV 2008, 8 ff.

¹²⁵ Albers, Informationelle Selbstbestimmung, 2005, S. 152 ff.

¹²⁶ Vgl. hierzu Dutte Der Staat 36 (1997), 281, 303. Zu den in der Realität nicht lösbaren normativen Festsetzungen gehört auch der rechtlich formulierte Anspruch, jederzeit selbst bestimmen und wissen zu können, wer was wann wo über einen weiß, vgl. hierzu auch Gusy KritV 83 (2000), 52, 62.

¹²⁷ Sie steht Pate für die erste maßgebliche Schutzrichtung im zweigliedrigen Schutzbereich des GVIIS (Rn. 204, 206); anhand des nicht geschützten Vertrauens in den Kommunikationspartner wird die Eingriffsschwelle bei der Teilnahme der Telekommunikation bestimmt (Rn. 290). Die Grenzlinie des Schutzbereichs des RiS wird nicht nur anhand der Unterscheidung öffentlich/privat, sondern auch anhand des schutzwürdigen (Rn. 310) oder nicht schutzwürdigen (Rn. 311) Vertrauens gebildet, jedenfalls nicht mehr anhand des Autonomiegedankens (Selbstbestimmung).

¹²⁸ So Britz DÖV 2008, 411, 412.

¹²⁹ Vgl. hierzu T. Böckenförde (Fn. 7), S. 238.

fangen. Das Abstellen auf Zonen bzw. Bereiche, kurzum Sphären des Privaten und weniger auf private Inhalte hat den Vorteil, sich der genauen inhaltlichen Qualifizierung des Privaten nicht widmen zu müssen, zumal sich dieses in hohem Maße subjektiv bestimmt und daher ohnehin nur schwer normativ festlegbar ist.

3. Elektronische Privatsphäre

Zeigen sich also viele Vorteile bei der Verwendung des Begriffs „Privatsphäre“ als Ausdruck für rechtlich Schützenswertes, so bedarf es noch einer Akzentuierung, um diesen Begriff im Kontext von Netz- und Computertechnik, Cyberlaw und Cyberspace zu verankern. Auch wenn der Ausdruck „digitale Privatsphäre“ womöglich präziser ist, da er auf den technischen Prozess der Digitalisierung der Information als Quantensprung gesteigerter Chancen und Gefährdungen abstellt, wird hier der Ausdruck „elektronische Privatsphäre“ als geeigneter erachtet. Wenn man so will, ist die Elektrifizierung noch elementarer als die Digitalisierung von Informationen. Wichtiger ist jedoch, dass der Begriff „elektronische Privatsphäre“ kompatibel ist mit einem verbreiteten Sprachgebrauch der Beschreibung digitaler Netzsachverhalte, die durch Anfügung des vom Phonem zum Morphem mutierten Duo-Semeions „E-“ aus dem herkömmlichen einen Netzsachverhalt macht.¹³⁰ Und die Vermittelbarkeit ei-

nes rechtlich geprägten Begriffs „E-Privacy“ im allgemeinen Sprachgebrauch ist letztlich auch für die Vermittlung eines darauf aufbauenden Rechtsbewusstseins entscheidend.

Eingeführt werden soll damit zunächst keine weitere Konkretisierung des APKR, auch soll nicht der Titel des neuen Grundrechts ausgetauscht werden. Sondern vorgestellt wird ein so unbelasteter wie eingängiger, integrativer wie entwicklungsöffener, vermittel- wie merkbarer Begriff. Sowohl das GVIIS wie das RiS schützen Teile der elektronischen Privatsphäre, genauso wie Art. 10 GG und die Gesetzesvorbehalte des Art. 5 GG, der wiederum seine freiheitliche Wirkung im Netz vor allem in der elektronischen Öffentlichkeitssphäre entfaltet. Die elektronische Privatsphäre hat nicht nur das Potential, in Bezug auf Netzsachverhalte Klammerbegriff für geschriebene und ungeschriebene Grundrechte zu sein. Sie eignet sich auch gut als begrifflicher Anker für schon länger geplante Modernisierungen des Datenschutzes, sie kann zudem technische Entwicklungen integrieren, die sich noch nicht genau vorhersagen lassen. Die elektronische Privatsphäre identifiziert und definiert das rechtlich Schützenswerte im Netz, sie ist sich nicht nur selbst ihr eigenes Ziel, sondern formt auch den Weg dahin, man muss ihn nur gehen.

¹³⁰ Instruktiv hierzu *Amta Agamon*, Zur Hermeneutik des Bindestrichs, 2007, S. 43 ff., 102 f. Beispiele für solche auf dem Morphem „E-“ aufbauenden Wortschöpfungen gibt es zuhauf: E-Banking, E-Book, E-Business, E-

Commerce, E-Fax, E-Generation, E-Government, E-Learning, E-Mail, E-Paper, E-Procurement, E-Publishing, E-Shop, E-Solutions, E-Voting, E-Zine, etc.

Glückwunsch

Friedrich E. Schnapp zum 70. Geburtstag

Am 4. Oktober 2008 feiert Professor Dr. *Friedrich E. Schnapp*, vormals Ruhr-Universität Bochum, seinen 70. Geburtstag. Dazu gratulieren ihm Freunde, Schüler und Kollegen aus dem In- und Ausland sehr herzlich und widmen ihm in Anerkennung und Dankbarkeit eine Festschrift.

Friedrich Eberhard Schnapp wurde in Dortmund als Sohn eines Bergmanns geboren. Nach dem Besuch des Pestalozzi-Gymnasiums in Herne, unterbrochen durch ein Austauschjahr in East Syracuse/USA, für das er ein Stipendium des American Field Service erhielt, entschied er sich für das Studium der Rechtswissenschaften. Dieses begann und beendete *Schnapp* in Bonn, zwischenzeitlich verbrachte er zwei Studensemester in München. Nach der ersten juristischen Staatsprüfung im Jahre 1963 kehrte er dann zur Referendarzeit ins Ruhrgebiet zurück, legte 1967 das Assessorexamen ab und promovierte mit der Arbeit „Die Ersatzvornahme in der Kommunalaufsicht“. Anschließend habilitierte er sich unter der Betreuung von *Wilhelm Wertenbruch* mit der Schrift „Amtsrecht und Beamtenrecht. Eine Untersuchung über normative Strukturen des staatlichen Innenbereichs“. 1975 wurde *Friedrich E. Schnapp* Professor für Öffentliches Recht an der Westfälischen Wilhelms-Universität Münster. 1984 nach Bochum zurückberufen, bekleidete er bis zu seiner Pensionierung am 31. 3. 2004 den Lehrstuhl für Öffentliches Recht, Staats- und Verwaltungsrecht mit besonderer Berücksichtigung des Sozialrechts. Zugleich war *Schnapp* seit 1984

Mitglied des Instituts für Sozialrecht, lange Jahre als Geschäftsführender Direktor.

Wissenschaft und Praxis ist *Schnapp* ganz besonders als Sozialrechtler und hier als Spezialist für das Krankenversicherungsrecht bekannt. Von großem Einfluss auf die Rechtspraxis ist insbesondere das von ihm zusammen mit *Peter Wigge* herausgegebene Handbuch des Vertragsarztrechts (2002; 2. Aufl. 2006). *Schnapp* hat im Sozialrecht nicht nur die dogmatischen Grundlagen beackert, sondern immer auch den engen Austausch mit der Praxis gepflegt; die Erfahrungen, die er als nebenamtlicher Richter am Landessozialgericht, als Vorsitzender verschiedener Schiedsämter und als Gutachter sammeln konnte, haben oftmals Eingang in seine Schriften gefunden.

Im Selbstverständnis *Schnapps* nicht weniger zentral sind aber seine Arbeiten zum Organisationsrecht – eine staats- und verwaltungsrechtliche Querschnittsmaterie, zu deren wissenschaftlicher Durchdringung er seit seiner Habilitationsschrift nicht nur in Bezug auf ihre theoretischen Grundlagen maßgeblich beigetragen hat. Hervorgehoben seien hier nur sein Vortrag vor der Vereinigung Deutscher Staatsrechtslehrer über den „Verwaltungsvorbehalt“ (VVDStRL 43 [1985], S. 172 ff.) oder seine „Dogmatische(n) Überlegungen zu einer Theorie des Organisationsrechts“ (AöR 105 [1980], S. 243 ff.). Das Organisationsrecht hat aber auch im Rahmen seiner Beschäftigung mit Referenzgebieten wie dem Beamtenrecht, dem Kommunalrecht und dem Sozialversicherungsrecht immer wieder sein Interesse gefunden.

Grundfragen der Verfassungsrechtsdogmatik – etwa Überlegungen zu den Grundrechtsträgern, den Grundrechts-