

einen grundlegenden Wandel der vertraglichen Umstände. War dies rechtmäßig?

aa) Die dauerhafte Beendigung (Art. 70 WVK) oder die vorübergehende Suspendierung (Art. 72 WVK) eines völkerrechtlichen Vertrages ist zunächst durch eine übereinstimmende Regelung aller Vertragsparteien möglich (vgl. Art. 54, 57, 59 WVK), etwa aufgrund einer Bestimmung im Vertrag selbst (z. B. zum Auslaufen der Europäischen Gemeinschaft für Kohle und Stahl nach 50 Jahren gemäß Art. 97 EGKSV), aufgrund eines späteren Einvernehmens (z. B. zur Auflösung des Warschauer Paktes 1991) oder aufgrund eines späteren Vertrages (z. B. die Ablösung des alten EUV und EGV durch den neuen EUV und den AEUV mit dem Vertrag von Lissabon). In der Praxis problematischer sind diejenigen Fälle, in denen sich eine Partei einseitig – dauerhaft oder vorübergehend – vom Vertrag lösen möchte. Auch diesen Fall kann der Vertrag selbst geregelt haben, indem er etwa ein Recht zur Suspendierung vertraglicher Pflichten oder ein Kündigungs-, Austritts- oder Rücktrittsrecht – die letztgenannten Begriffe werden ohne wesentliche Bedeutungsunterschiede nebeneinander verwandt²⁸ – einräumt. So ist beispielsweise der Austritt aus der EU nach Art. 50 EUV ohne weiteres, die Kündigung des Nuklearen Nichtverbreitungsvertrages («Atomwaffensperrvertrag») unter Berufung auf höchste nationale Interessen nach dessen Art. X möglich – eine Möglichkeit, von der Nordkorea 2003 Gebrauch gemacht hat²⁹. Auch ist es gängige Praxis, dass Entwicklungshilfeverträge mit Menschenrechtsklauseln die Suspendierung von Hilfeleistungen für den Fall vorsehen, dass gegen diese Klauseln verstoßen wird.

Sofern der Vertrag selbst keine diesbezüglichen Bestimmungen enthält, kann sich ein Kündigungsrecht jedoch implizit aus dem Vertrag, nämlich nach dem stillschweigenden Willen der Vertragsparteien oder der Vertragsnatur (Art. 56 I WVK), und ein Kündigungs- oder Suspendierungsrecht aufgrund einer Vertragsverletzung (Art. 60 WVK) oder aufgrund einer grundlegenden Änderung der Umstände (Art. 62 WVK) ergeben. Wie man sieht, handelt es sich hierbei um Gründe, die auch das innerstaatliche Privatrecht kennt, etwa mit dem Kündigungsrecht für bestimmte Dauerschuldverhältnisse (etwa §§ 542 I, 608 II, 620 II, 671 I BGB), dem Rücktrittsrecht bei Vertragsverletzungen (etwa §§ 323 I, 324 BGB) oder den Regelungen zur Störung der Geschäftsgrundlage (§ 313 BGB).

bb) Ein Kündigungsrecht nach Art. 56 I WVK – entweder aufgrund des stillschweigenden Parteiwillens oder der Vertragsnatur – vermutet man beispielsweise regelmäßig für die Gründungsverträge Internationaler Organisationen, für Verträge über Handelsbeziehungen, militärischen Beistand oder wirtschaftliche, kulturelle oder wissenschaftliche Zusammenarbeit sowie für Abkommen über eine internationale Gerichts- und Schiedsgerichtsbarkeit³⁰. Dahinter steckt die Überlegung, dass sich ein Staat aufgrund seiner Souveränität von der Unterwerfung unter die internationale Gerichtsbarkeit bzw. von einer auf Dauer angelegten Zusammenarbeit lösen können muss, zumal letztere auch nur bei einer entsprechenden Bereitschaft der Beteiligten Sinn ergibt. Ein implizites Kündigungsrecht besteht andererseits aber etwa nicht für die Vereinbarung eines konkreten Projektes oder für endgültig gedachte Vereinbarungen wie Friedensschlüsse oder Grenzverlaufverträge³¹.

cc) Für eine Reaktion auf Vertragsverletzungen ist zwischen bilateralen und multilateralen Verträgen zu unterscheiden. In einem zweiseitigen Vertrag berechtigt eine erhebliche Vertragsverletzung die andere Seite stets zur Suspendierung oder Beendigung des Vertrages (Art. 60 I, III WVK). Verletzt ein Staat in erheblicher Weise einen multilateralen Vertrag, sind die übrigen Staaten gemeinsam dazu berechtigt, den Vertrag zu suspendieren oder zu beenden. Außerdem steht einer Partei das Recht der unilateralen Suspendierung zu, wenn sie von der Vertragsver-

letzung besonders betroffen ist (beispielsweise im Bereich des Diplomaten- oder Konsularwesens) oder wenn ein so genannter integraler Vertrag – dessen Ziel, beispielsweise der Abrüstung, nur erreicht werden kann, wenn alle Parteien unabhängig voneinander die eingegangenen Verpflichtungen erfüllen – verletzt wird (Art. 60 II, III WVK). Im letztgenannten Fall geht eine Vertragspartei die Verpflichtungen nämlich in dem Vertrauen darauf ein, dass jede andere Partei sie gleichfalls erfüllt, da andernfalls konkrete Nachteile (etwa militärischer Art) drohen.

In multilateralen Verträgen kann die Suspendierung oder Beendigung vertraglicher Pflichten für den gemeinsam verfolgten Zweck jedoch kontraproduktiv sein: Dem Menschenrechtsschutz wäre nicht gedient, wenn die Vertragsverletzung einer Partei die Suspendierung oder Beendigung des Vertrags und damit die Erlaubnis zur Menschenrechtsverletzung durch die übrigen Parteien nach sich zöge. Gleiches gilt etwa für das im Rahmen der WTO verfolgte Ziel eines freien Welthandels. Das Kooperationsvölkerrecht kennt hier zunehmend Mechanismen, mit denen das gemeinsame Ziel auch angesichts von Vertragsverletzungen verfolgt werden kann. Zum einen verbietet Art. 60 V WVK die Beendigung oder Suspendierung als Reaktion auf die Verletzung von Verträgen humanitärer Art, worunter man Verträge des humanitären Völkerrechts und des Menschenrechtsschutzes versteht³². Zum anderen werden insbesondere im Rahmen Internationaler Organisationen vertragliche Mechanismen, etwa eine eigene Gerichtsbarkeit, entwickelt, die über außervertragliche Mittel wie die Retorsion oder die Repressalie³³ hinaus eine vertragsbrüchige Partei zum Einlenken bewegen sollen.

dd) Schließlich kann der grundlegende Wandel der bei Vertragsschluss gegebenen Umstände eine Beendigung oder Suspendierung des Vertrages begründen. Allerdings gilt dieses Grundsatz des »rebus sic stantibus«³⁴ nur unter eingeschränkten Voraussetzungen, weil sonst die Verlässlichkeit vertraglicher Bindungen und damit die Rechtssicherheit erheblich beeinträchtigt wären. In der Formulierung des Art. 62 WVK muss es sich um eine *grundlegende* und von den Parteien nicht vorausgesehene Änderung der beim Vertragsschluss gegebenen Umstände handeln, deren Vorhandensein eine *wesentliche* Grundlage für die vertragliche Bindung darstellt und deren Änderung das Ausmaß der Vertragspflichten *tiefgreifend* umgestalten würde. Klassische Beispielfälle derart grundlegender und nicht vorhersehbarer Ereignisse sind Revolutionen und Kriege – für die Anwendbarkeit von Art. 62 WVK muss jedoch stets ein Bezug zum konkreten Vertrag hergestellt werden³⁵.

Lösung Fall 5: Ungarn hat nach Art. 62 WVK das Recht, den Vertrag zu beenden, wenn es einen grundlegenden Wandel der beim Vertragsschluss gegebenen Umstände darlegen kann. Der IGH verneinte, dass mit neuen Erkenntnissen und Normen des Umweltschutzes oder mit dem Wechsel des politischen und wirtschaftlichen Systems ein Beendi-

28 »Austritt« bezieht sich regelmäßig auf eine Internationale Organisation. »Kündigung« wird von »Rücktritt« – anders als im deutschen Sprachgebrauch – teilweise dadurch abgegrenzt, dass sie vertraglich vorgesehen ist; anders aber z. B. Art. 56 WVK. Zur Terminologie HEINTSCHEL VON HEINEGG, Fn. 9, § 15, Rdn. 65; GRAF VITZTHUM, Fn. 9, 65.

29 Zur (in ihrer Rechtswirksamkeit umstrittenen) nordkoreanischen Kündigung A. AUST Max Planck Encyclopedia of Public International Law, »Treaties, Termination«, Rdn. 8.

30 Corten/Klein/CHRISTAKIS, Fn. 11, Bd. III, Art. 56, Rdn. 76 ff.

31 Hierzu AUST, Fn. 29, Rdn. 18 f.

32 Dies ist nicht ganz unumstritten, hierzu Corten/Klein/SIMMA/TAMS, Fn. 30, Rdn. 44.

33 Zu diesen Maßnahmen etwa SCHRÖDER in Graf Vitzthum, Fn. 9, 630 ff.

34 Wörtlich: (unter der Voraussetzung,) dass die Dinge so bleiben.

35 Beispielfälle mit der älteren Staatenpraxis zum auch gewohnheitsrechtlich anerkannten Grundsatz des *rebus sic stantibus* bei HEINTSCHEL VON HEINEGG Max Planck Encyclopedia of Public International Law, »Treaties, Fundamental Change of Circumstances«, Rdn. 5 ff.

gungsgrund nach Art. 62 WVK vorliege: Mit ersterem sei bei Vertragsabschluss zu rechnen gewesen. Außerdem sei das politische und wirtschaftliche System bei Vertragsabschluss nicht so eng mit dem Vertragszweck verbunden gewesen, dass es eine wesentliche Grundlage für die vertragliche Zustimmung gebildet habe und dass seine Änderung die Vertragspflichten tiefgreifend umgestalten würde. Damit hat der IGH der Revolution von 1989 nicht grundsätzlich die Qualität eines grundlegenden Wandels i. S. d. Art. 62 WVK abgesprochen, wohl aber den notwendigen

Zusammenhang zwischen der kommunistischen Herrschaft in Ungarn und dem Gabcikovo-Nagymaros-Project verneint³⁶.

36 IGH (Gabcikovo-Nagymaros-Project), ICJ Rep. 1997, 7 (64 f.).

Die aktuelle Entscheidung

BVerfG, Ur. v. 27. 2. 2008 (1 BvR 370/07 u. a.) = NJW 2008, 822 ff.

Das »neue Grundrecht« auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Von Prof. Dr. Bernhard W. Wegener (M.A. – Brügge), Erlangen und Regierungsrat Sven Muth, München¹

Es kommt eher selten vor, dass das BVerfG ein »neues Grundrecht« entwickelt. Eine Quelle solcher neuen Grundrechte ist aber schon traditionell das »Allgemeine Persönlichkeitsrecht«, das selbst aus einer Zusammenschau von Art. 2 Abs. 1 und Art. 1 Abs. 1 GG entstanden ist. 1983 entwickelte das BVerfG im sog. Volkszählungsurteil aus dem Allgemeinen Persönlichkeitsrecht das »Recht auf informationelle Selbstbestimmung« (RiS). Mit dem hier vorgestellten Urteil zur Online-Durchsuchung wird dieses Recht ergänzt um ein »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« (GGVtIS). Das Urteil ist in den allgemeinen Medien weithin als Sieg des Rechtsstaates gegen eine überzogene Sicherheitspolitik gefeiert worden. In der juristischen Literatur überwiegen Stimmen, die der Entscheidung zwar im Ergebnis zustimmen, das neue Grundrecht aber für eine überflüssige und schädliche Erfindung halten. Welchen genauen Schutzbereich das neue Grundrecht hat, wie es sich von anderen Grundrechten abgrenzen lässt und unter welchen Voraussetzungen es beschränkbar ist, versucht dieser Beitrag aufzuzeigen.

A. Gegenstand und Inhalt der Entscheidung

Mit dem hier besprochenen Urteil hat das BVerfG Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalens (VSG-NW) für mit dem Grundgesetz unvereinbar und nichtig erklärt, die den Verfassungsschutzbehörden die sog. »Online-Durchsuchung« von Computern erlaubten. Das VSG-NW definiert die Online-Durchsuchung als »heimlichen Zugriff auf ein informationstechnisches System«. Für einen solchen Zugriff ist eine technische Infiltration des betroffenen Computers erforderlich. Im Regelfall wird diese durch die Installation einer speziellen Software (»Trojaner«) erreicht. Die Software erlaubt den Ermittlern den heimlichen, also unbemerkten Zugriff auf den Computer des Benutzers. Dadurch können dessen Nutzung überwacht und gespeicherte Informationen ausgelesen werden. Der Zugriff wird dem Nutzer dabei nach Möglichkeit verheimlicht².

Die Entscheidung zur Online-Durchsuchung war auch deshalb mit besonderer Spannung erwartet worden, weil der BGH zuvor den Versuchen, ein entsprechendes Vorgehen³ auf der Grundlage der StPO zu rechtfertigen⁴, eine Absage erteilt hatte⁵. Entscheidendes Merkmal von Online-Durchsuchungen sei ihre Heimlichkeit. Heimliche Ermittlungsmaßnahmen sehe die StPO aber allein in den §§ 100 a bis 100 i StPO vor, die insoweit tatbestandlich nicht einschlägig seien. Die »klassische« Durchsuchung nach den §§ 102 ff. StPO setze dagegen ein offenes Vorgehen der Behörden voraus⁶.

Nach Auffassung des BVerfG verletzt das VSG-NW mit seiner pauschalen Erlaubnis zur Online-Durchsuchung das Allgemeine Persönlichkeitsrecht in seiner besonderen Ausprägung als »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« (im Folgenden: GGVI-IS). Die einschlägige Vorschrift verstoße gegen das Gebot der Normenklarheit und Normenbestimmtheit⁷. Ferner wahre die einschlägige Vorschrift nicht das Gebot der Verhältnismäßigkeit. Angesichts der Schwere des Eingriffs sei die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen (und missbräuchlich auch manipuliert) werden können, verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestünden. Zudem sei der Eingriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Diesen Anforderungen werde § 5 Abs. 2 Nr. 11 S. 1 Alt. 2 VSG-NW nicht gerecht. Darüber hinaus fehle es auch an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.

B. Zum rechtspolitischen Hintergrund

Seit den Attentaten vom 11. September 2001 wird auch Deutschland intensiver als zuvor über die angemessene staatliche Reaktion auf die Gefahren des Terrorismus gestritten. Den Sicherheitsinteressen steht dabei regelmäßig das Interesse an einer möglichst ungeschmälerter Wahrung der Bürgerrechte, insbesondere des

1 Der Erstverfasser ist Inhaber des Lehrstuhls für Öffentliches Recht an der Friedrich-Alexander-Universität Erlangen-Nürnberg, der Zweitverfasser ist Regierungsrat im Bayerischen Staatsministerium des Innern.

2 Ausführlich zu den technischen Hintergründen und Details: BUERMEYER, HRRS 2007, 154 ff.

3 Schon 2005 sollen auf Grund von Anweisungen des damaligen Bundesinnenministers SCHILY Online-Durchsuchungen durchgeführt worden sein, vgl. dazu <http://www.stern.de/computer-technik/internet/Online-Durchsuchungen-Geheimdienste-Jahren/587865.html>. Das Bundesinnenministerium bestätigte im April 2007, dass es in Deutschland »seit einer Anweisung der rot-grünen Bundesregierung im Jahr 2005 deutlich weniger als ein Dutzend Online-Durchsuchungen« gegeben habe, vgl. <http://www.sueddeutsche.de/computer/76/321944/text>.

4 Vgl. dazu etwa HOFMANN, NStZ 2005, 121 ff.

5 Vgl. Beschluss v. 31. 1. 2007, StB 18/06, BGHSt 51, 211 ff.

6 Beschluss v. 31. 1. 2007, StB 18/06, BGHSt 51, 211; hierzu: KUDLICH, HFR 19/2007, 1 ff.

7 BVerfG Rdn. 211 ff. – die Randnummern beziehen sich – auch im Folgenden – auf die amtliche Internetteilfassung der Entscheidung, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

»Rechts privat zu sein«⁸, gegenüber⁹. Institutionell verkörpert werden die Sicherheitsinteressen vor allem in den Innenministerien des Bundes und der Länder. Diesen ist es unter dem Eindruck der Bedrohungslage vielfach gelungen, die Parlamente von der Notwendigkeit eines umfangreicheren und vorverlagerten Informationszugriffs zu überzeugen¹⁰. Aktuelle Erscheinungsformen dieses Zugriffs¹¹ sind die Rasterfahndung¹², der automatische KFZ-Kennzeichenabgleich¹³, die Wohnraumüberwachung (»großer Lauschangriff«)¹⁴, die Videoüberwachung öffentlicher Plätze¹⁵, die GPS-Observation¹⁶, die präventive Überwachung der Telekommunikation und der Post¹⁷, sowie die Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten¹⁸. Weil das BVerfG all diesen Überwachungsmaßnahmen zumindest korrigierend in den Arm gefallen ist¹⁹, wird es in der Öffentlichkeit vielfach als institutioneller Gegenspieler zu den Sicherheitsbehörden und dem (zu?) verschreckt reagierenden demokratischen Gesetzgeber angesehen. Bei dieser Einstufung des Gerichts als »Champion« der Bürgerrechte darf allerdings nicht übersehen werden, dass das BVerfG seiner Rolle als Verfassungsschutzorgan entsprechend im Wesentlichen (nur) formelle Anforderungen (explizite gesetzliche Grundlage, Richtervorbehalt, Straftatenkatalog) bzw. äußerste Grenzen (Bagatelldelicten, unantastbaren Kernbereich privater Lebensgestaltung) des informatorischen staatlichen Zugriffs entwickelt hat. Die Diskussion um das richtige Maß dieses Zugriffs bzw. um den notwendigen Schutz der bürgerlichen Privatsphäre muss deshalb – anders als dies derzeit vielfach geschieht – vor allem politisch und nur in zweiter Linie verfassungsrechtlich geführt werden²⁰.

C. »RiS«, »GGVIIS« oder besser »Recht auf Privatleben«?

Auch wenn das BVerfG das GGVIIS als eine »Ausprägung« des Allgemeinen Persönlichkeitsrechts bezeichnet, spricht es doch insoweit von einem »neuen Grundrecht«.

I. Die Bewertung des GGVIIS zwischen Euphorie und Kritik

In Kommentaren zum Online-Durchsuchungs-Urteil war deshalb schnell und euphorisch von der »Geburt eines neuen Sterns«²¹ die Rede. Eine beschwerdeführende Bürgerrechtlerin schwärmte bescheidener von der Geburt ihres neuen »Babys«²². Auch der Berichterstatter im Verfahren, der kurze Zeit später ausgeschiedene Bundesverfassungsrichter Hoffmann-Riem ordnete das Urteil in den Kontext »großer Tag[e] für den Ausbau des Grundrechtsschutzes in Deutschland« ein²³.

Demgegenüber reagierten andere eher irritiert. Sie sprachen dem neuen GGVIIS den Mehrwert ab. Die vom BVerfG unterstellte Schutzlücke bestehe nicht. Vielmehr könne das bewährte Recht auf informationelle Selbstbestimmung (RiS) auch den Schutz gegenüber den aktuell zu beobachtenden staatlichen Zugriffsversuchen adäquat gewährleisten. Die Erfindung eines neuen Grundrechts sei deshalb eine überflüssige Arabeske²⁴, die zudem die Gefahr der Schwächung des bewährten Grundrechtsschutzes mit sich bringe²⁵.

In der Tat ist gegenüber der Entdeckung immer neuer Grundrechte grundsätzlich Skepsis angezeigt. Sie birgt alle Gefahren der Kleinteiligkeit. Mit ihr wird der Grundrechtsschutz zwar spezifischer aber auch unübersichtlicher. Außerdem verringert sich mit jeder neuen Grundrechtsableitung der Bezug zum Verfassungstext. Damit entfernt sich die verfassungsgerichtliche Dogmatik von ihrer Legitimationsbasis.

II. Schwächen des Rechts auf informationelle Selbstbestimmung

All diese Einwände treffen allerdings das ältere Recht auf informationelle Selbstbestimmung kaum weniger als das neue GGVIIS.

iS. Außerdem ist dem BVerfG zuzugeben, dass es mit seiner Neuentdeckung des GGVIIS auf Schwächen des RiS reagiert. Zu diesen Schwächen gehören insbesondere die Totalität und damit die Undifferenziertheit des Selbstbestimmungsschutzes. Im Volkszählungsurteil hatte das BVerfG apodiktisch davon gesprochen, dass es in den Zeiten automatisierter Datenverarbeitung keine belanglosen Daten mehr gebe. Dementsprechend hat es das RiS zu einem vermeintlich allumfassenden Recht am eigenen Datum ausgebaut²⁶. Jedes Datum erfährt demnach jedenfalls dem Ansatz nach den gleichen Schutz gegenüber jedem noch so geringfügigen staatlichen Zugriff. Das bringt neben einem immer weiter ausufernden und mittlerweile auch für Experten nicht mehr überschaubaren Datenschutzrecht und einer dieses Recht verwaltenden Bürokratie vor allem eine Vielzahl alltäglicher Belästigungen und Erschwernisse mit sich. Gerade im Belanglosen wurde und wird der Datenschutz mit Liebe gepflegt. Die hier zu beobachtenden Exzesse sind aber geeignet, den Datenschutz als solchen zu desavouieren. Dies gilt umso mehr, als sich das RiS umfangreicheren und intensiveren staatlichen Informationszugriffen demgegenüber bislang nur sehr schwächlich in den Weg stellt. Solange nur eine entsprechende gesetzliche Grundlage besteht, so mochte es lange scheinen, solange ist von dieser Seite gegen Informationszugriffe wenig einzuwenden.

Zuzugeben ist dem BVerfG auch, dass das RiS problematisch ist, weil es eine datenbezogene Selbstbestimmung und Selbstbestimmungsmöglichkeit des Einzelnen voraussetzt bzw. suggeriert. Die Herrschaftsmacht des Einzelnen über »seine« Daten ist

8 Mit diesem Begriff lassen sich die einschlägigen Bürgerrechte anschaulich zusammenfassen. Er knüpft an die jahrhundertealte Auseinandersetzung an, in der zunächst die absolutistische Staatslehre dem Untertanen bei Strafe verbot »geheim zu seyn« und in der anschließend die bürgerliche Aufklärung den rechtlichen Schutz der Geheimnisse des Einzelnen erzwingt; vgl. dazu WEGENER, Der geheime Staat, 2006, S. 117 f., 187 ff., 284 ff.

9 Kritisch zu den informationellen staatlichen Zugriffen deshalb etwa PRANTL, ANWB 2002, 274 ff.; WEICHERT, RDV 2005, Sonderbeilage Heft 1, S. 6, 9; LEUTHEUSSER-SCHNARRENBERGER, Verdächtig ist jeder, Vortrag anlässlich der Römerberggespräche 2007 in Frankfurt/Main, <http://www.roemerberggespraeche-fm.de/pdf/Leutheusser.pdf>; eine Analyse des Spannungsfeldes nimmt GRAF VON WESTPHALEN, ANWB 2008, 801 ff. vor.

10 Vgl. etwa Gesetzentwurf zum Terrorismusbekämpfungsgesetz, BT-Drs. 14/7727 i. V. m. BT-Drs. 14/7386, S. 35.

11 In einem weiteren Sinne zählt hierzu auch noch das »Einfrieren« der Finanzen von Personen, die der Unterstützung des Terrors verdächtigt werden, vgl. hierzu die Entscheidung des EuGH in den Rs. C-402/05 P u. C-415/05 P (Kadi/Rat und Kommission), DVBl 2009, 175 ff. Der EuGH hat diese auf Beschlüsse des UN-Sicherheitsrats zurückgehende Praxis und ihre Umsetzung in das EU-Recht wegen des insoweit fehlenden Rechtsschutzes als unvereinbar mit dem Verfassungsrecht der EG bezeichnet.

12 Vgl. dazu BVerfGE 93, 181 ff.; 115, 320 ff.

13 Vgl. dazu BVerfG, NJW 2008, 1505 ff.

14 Vgl. dazu BVerfGE 109, 279 ff.

15 Vgl. dazu BVerfG, NVwZ 2007, 688 ff.

16 Vgl. dazu BVerfGE 112, 304 ff.

17 Vgl. dazu BVerfGE 110, 33 ff.; 113, 348 ff.

18 Vgl. dazu BVerfG, NJW 2010, 833 ff.

19 Eine »kommentierende Dokumentation der jüngsten Entscheidungen zu drei Sicherheitsgesetzen« gibt ERD, KJ 2008, 118 ff.

20 Hierzu etwa STEINKE, FoR 2008, 120 ff.

21 PRANTL, Süddeutsche Zeitung v. 28. 2. 2008, S. 4.

22 Die Beschwerdeführerin und Internet-Journalistin WINSEMANN in <http://www.heise.de/tp/blogs/5/104314>.

23 HOFFMANN-RIEM, JZ 2008, 1009 unter Hinweis auf das Volkszählungsurteil.

24 Vgl. HOEREN, MMR 2008, 365, 366.

25 Kritisch unter diesen Gesichtspunkten deshalb: EIFERT, NVwZ 2008, 521 f.; BRITZ, DÖV 2008, 411, 413; VOLKMAN, DVBl. 2008, 591; SACHS/KRINGS, JuS 2008, 481, 484; KUTSCHA, NJW 2008, 1042 ff.

26 Kritisch dazu HOFFMANN-RIEM, AöR 1998, 513, 520 f.; ALBERS, Informationelle Selbstbestimmung, 2005, S. 238 und öfters.

aber weithin Illusion. Der Einzelne ist gerade in den Zeiten wachsender informationeller Vernetzung – auch im privaten Bereich – auf die Preisgabe einer Vielzahl auch persönlichster Daten existenziell angewiesen²⁷. Diese Daten ergeben in vielen Fällen bereits heute ein sehr vollständiges Bild über die Persönlichkeit des Nutzers²⁸. Will er in der Informationsgesellschaft leben und handeln, kann er auf diese Selbstoffenbarung nicht verzichten. Zugleich kann der genaue Umfang dieser Selbstpreisgabe und damit auch der potentielle Missbrauch, der mit ihr getrieben werden kann, vom Einzelnen immer weniger vorhergesehen und gesteuert werden²⁹. Ein modernes Datenschutzrecht kann deshalb nur sehr eingeschränkt dem Autonomieschutz verpflichtet sein, sondern muss in erster Linie Missbrauchsbekämpfung leisten.

III. Die Alternative: Allgemeines Persönlichkeitsrecht/ Schutz des Privatlebens

Wenn das BVerfG das selbst geschaffene RiS deshalb mit einigem Recht für ungenügend erachtet, dann hätte es den Ausweg aber nicht in der Erfindung eines neuen Grundrechts, sondern in der Rückführung seiner Argumentation auf das Allgemeine Persönlichkeitsrecht suchen sollen. Der Schutz der Persönlichkeit und ihres Bedürfnisses nach einer privaten, d. h. einer wenigstens teilweise geheimen, nicht-öffentlichen Existenz, bildet nämlich den eigentlichen Kern des Schutzes vor informationellen Zugriffen.

Die Rückführung auf das Allgemeine Persönlichkeitsrecht hätte gegenüber den Ableitungen des RiS und des GGVIIS auch den Vorteil gehabt, zur europäischen Grundrechtsentwicklung hin offener zu sein. Insbesondere die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), die für den europäischen Grundrechtsraum immer prägender wird, knüpft insoweit an das Grundrecht auf »Privatleben« aus Art. 8 EMRK an. »Privatleben« wird dabei deutlich weiter verstanden, als dies das BVerfG derzeit in seiner Rechtsprechung zum gleichfalls aus dem Allgemeinen Persönlichkeitsrecht abgeleiteten Recht auf Schutz der »Privatsphäre« tut. Geschützt ist nicht allein der Kernbereich privater Lebensgestaltung, sondern auch die »privacy« bei der Ausübung und Ausgestaltung der eigenen bürgerlichen Existenz³⁰. Art. 8 EMRK kann somit beispielsweise auch zur Kontrolle der Überwachung privaten Verhaltens im öffentlichen Raum herangezogen werden³¹. Der gegenüber dem gemeineuropäischen Standard inhaltlich deutlich weiter entwickelte deutsche Persönlichkeitsschutz könnte den ihm gebührenden europäischen Einfluss gewinnen, wenn er sich im begrifflichen Ausgangspunkt auf die EMRK zu bewegen würde. Die Neuschöpfung des sperrigen GGVIIS ist aber kaum geeignet, diese Transportfunktion zu erbringen. Vorbildfunktion und Anschlussfähigkeit kann im gemeineuropäischen Rechtsraum nur eine Grundrechtsrechtsprechung haben, die eine weniger überzogene dogmatische Komplexität mit einer gleichzeitig schärferen Konturierung der Verhältnismäßigkeitsprüfung vereint.

D. Struktur des neuen Grundrechts

Auch wenn deshalb erhebliche Zweifel an der Neuschöpfung des GGVIIS angebracht sind, muss jedenfalls der Student und Prüfungskandidat mit dessen bundesverfassungsgerichtlich vorgegebener Existenz leben. Im Folgenden soll deshalb die wesentliche Struktur des neuen Grundrechts aufgezeigt werden.

I. Schutzbereich

Durch seinen eigenen Schutzbereich muss sich das GGVIIS von anderen bestehenden und teilweise ausdrücklich normierten Grundrechten abgrenzen.

Der Schutzbereich des GGVIIS ist nur eröffnet, soweit die Persönlichkeit nicht durch andere Grundrechte ausreichend geschützt ist. Dies ergibt sich daraus, dass das GGVIIS eine Ausprägung des Allgemeinen Persönlichkeitsrechts ist. Das GGVIIS schützt daher ergänzend (»lückenfüllend«) die Elemente der Persönlichkeit, die in ihrer »konstituierenden Bedeutung für die Persönlichkeit« den »bekannteren« Grundrechten nicht nachstehen (Auffangcharakter)³². Bekannte Grundrechte in diesem Sinne sind dabei einerseits die ausdrücklich im Grundgesetz kodifizierten Grundrechte als auch die vom BVerfG bereits anerkannten Ausprägungen des Allgemeinen Persönlichkeitsrechts (wie z. B. das Recht am eigenen Bild oder das Recht auf informationelle Selbstbestimmung³³).

Das BVerfG war vor diesem Hintergrund sichtlich bemüht, dem neuen Grundrecht den ihm zukommenden Schutzbereich zu sichern, in dem es die Schutzbereiche der Art. 10 und 13 GG und des RiS jeweils betont restriktiv interpretiert hat. Dennoch bleiben im Einzelnen schwierige Abgrenzungsfragen.

1. Definition des informationstechnischen Systems

Zunächst definiert das BVerfG den Schutzbereich über den Begriff des »informationstechnischen Systems«. Gemeint sind damit solche Systeme, die personenbezogene Daten des Nutzers in einem signifikanten Umfang enthalten können.

Das BVerfG führt insoweit eine »de minimis« oder Bagatellgrenze ein, als es nicht jedes informationstechnische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, dem besonderen Schutz durch die neue Grundrechtsausprägung unterstellt. Solche Systeme, die nach ihrer technischen Konstruktion lediglich Daten mit einem punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten (das BVerfG nennt als Beispiel »nicht vernetzte elektronische Steuerungsanlagen der Haustechnik«) soll es allein bei dem durch das RiS vermittelten schwächeren Schutz bleiben³⁴.

Schwieriger als diese Bagatellgrenze ist die Beschreibung des informationstechnischen Systems als solchem. Weil immer mehr personenbezogene Daten sich von der Speicherung in einem Gerät lösen und »ins Netz« verschoben werden, machte ein allein am konkreten Gerät festgemachter Grundrechtsschutz keinen Sinn. Das BVerfG definiert den Begriff des informationstechnischen Systems dementsprechend denkbar weit. Deutlich wird dies vor allem in seiner Definition des Internets. Danach ist dieses ein elektronischer Verbund von Rechnernetzwerken. In der Formulierung des BVerfG besteht es »aus informationstechnischen Systemen und kann zudem auch selbst als informationstechnisches System angesehen werden«³⁵.

Wenn demnach auch das Internet als solches grundsätzlich in den Schutzbereich der neuen Grundrechtsausprägung fällt, so muss sich das BVerfG in der Folge bemühen, den öffentlichen vom privaten und damit zu schützenden Teil dieses Systems zu trennen. Es greift insoweit auf den Begriff der Nutzung des Systems »als eigenes« zurück. Trotz seiner zivilrechtlichen Anmutung darf der Begriff des »eigenen« hier sicher nicht im Sinne

27 Ebenso GUSY, DuD 2009, 33, 34 f.

28 BVerfG Rdn. 170 ff.

29 Vgl. dazu HOFFMANN-RIEM, JZ 2008, 1009, 1011: »Kontrollverlust ist unvermeidbar«; 1013: »struktureller Verlust an Autonomie«.

30 In diesem weiteren Sinne spricht auch GUSY, DuD 2009, 33 ff. vom »Schutz der Privatheit«.

31 Eingehender dazu UERPMANN-WITZACK, in: Ehlers, Europäische Grundrechte und Grundfreiheiten, 32009, § 3 Rdn. 6; GRABENWARTHER, Europäische Menschenrechtskonvention, 32008, § 22, Rdn. 9 ff. m. N. zur entsprechenden Rspr. des EGMR.

32 BVerfG, Rdn. 169.

33 BVerfGE 65, 1, 43; 84, 192, 194.

34 BVerfG, Rdn. 202.

35 BVerfG, Rdn. 4.

von »Eigentum« verstanden werden. Auf die zivilrechtliche Zuordnung eines informationstechnischen Systems kann es insoweit nicht ankommen. Dies gilt für den virtuellen Speicherraum im Netz ebenso wie für einen vom Arbeitgeber bereitgestellten aber zugleich privat genutzten Computer. Entscheidend kann insoweit allein sein, ob und inwieweit der Einzelne mit einer Begrenzung des Zugriffs auf die von ihm in das informationstechnische System eingegebenen Informationen rechnen kann³⁶. Der Schutzbereich ist insoweit von vielerlei tatsächlichen wie normativen Rahmenseetzungen abhängig. Hier werden sich in Zukunft deshalb noch ganz erhebliche Abgrenzungsfragen stellen.

2. Abgrenzung von der Telekommunikationsfreiheit des Art. 10 GG

Nicht ganz einfach ist auch die Abgrenzung der neuen Grundrechtsgewährleistung von der des Art. 10 GG. Art. 10 Abs. 1 GG schützt das Brief-, Post- und Fernmeldegeheimnis. Zu den damit unter besonderen Schutz gestellten Kommunikationsvorgängen gehören nach ständiger Rechtsprechung auch solche, die über informationstechnische Systeme, insbesondere über das Internet, abgewickelt werden. So sind insbesondere auch der E-Mail-Verkehr und die Internettelefonie nach Art. 10 GG geschützt. Allerdings soll dieser Schutz grundsätzlich nur für die laufende Kommunikation gelten. Art. 10 GG schützt deshalb nicht vor dem Zugriff auf Daten, die auf informationstechnischen Systemen dauerhaft abgelegt sind. Dies soll nach Auffassung des BVerfG selbst dann gelten, wenn die fraglichen Informationen ursprünglich aus Kommunikationsvorgängen hervorgingen oder sich auf diese beziehen. Zudem soll der spezifische Schutz des Art. 10 GG nicht allein deshalb eingreifen, weil die Überwachungsbehörden Telekommunikationsvorgänge zum Zugriff auf informationstechnische Systeme benutzen³⁷.

3. Abgrenzung von Schutz der Wohnung nach Art. 13 GG

Betont eng definiert das BVerfG auch den Schutzbereich des Art. 13 GG mit Blick auf den Zugriff auf informationstechnische Systeme. Während in der Literatur der Zugriff auf die sich in einer Wohnung befindlichen Systeme vielfach pauschal unter Art. 13 GG subsumiert wurde³⁸ und teilweise der eigene Laptop sogar im Interesse eines umfassenden Systemschutzes zur »virtuellen Wohnung« stilisiert wurde³⁹, argumentiert das BVerfG sowohl wortlautgerechter wie praxisbezogener. Art. 13 GG ist danach für Zugriffe auf informationstechnische Systeme nur insoweit relevant, als entweder zum Zwecke des Zugriffs in die Wohnung physisch Eindringen oder aber das informationstechnische System selbst – durch Fernmanipulation von dessen Mikrofon oder Kamera – als Instrument gerade der Wohnraumüberwachung eingesetzt wird. Dagegen sei Art. 13 GG nicht einschlägig, wenn auf ein informationstechnisches System lediglich online zugegriffen werde. Dafür sei es unerheblich, ob sich das betroffene Gerät aktuell innerhalb oder außerhalb einer Wohnung befände. Für diese Sicht spricht, dass es für den online erfolgenden Gerätezugriff keiner Überwindung einer spezifischen Wohnraumgrenze bedarf⁴⁰. Für die zugreifenden Behörden ist der Standort der Geräte (Laptops, Mobiltelefone, PDAs) insoweit irrelevant und regelmäßig nicht einmal sicher einzuschätzen. Mit seiner restriktiven Definition des Art. 13 GG vermeidet das BVerfG schließlich auch die Problematik des fehlenden grundgesetzlichen Vorbehalts für entsprechende Zugriffe. In der Literatur war insoweit die Frage aufgeworfen worden, ob Online-Durchsuchungen möglicherweise nur durch eine Grundgesetzänderung »legalisiert« werden könnten, da Art. 13 GG bislang keinen »passenden« Gesetzesvorbehalt beinhalte⁴¹.

4. Abgrenzung vom Recht auf informationelle Selbstbestimmung

Wie bereits angesprochen, bringt die Entscheidung des BVerfG eine gewisse Abkehr vom RiS mit sich. Allerdings fällt auch dem BVerfG die Abgrenzung zwischen dem älteren Konzept der Selbstbestimmung und dem neueren der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht leicht. Wenig überzeugend erscheint etwa die Behauptung, das RiS schütze nur vor »einzelne[n] Datenerhebungen«⁴². Im Gegenteil hatte das BVerfG bereits früher zu Recht ausgeführt, dass das RiS »vor jeder Form der Erhebung personenbezogener Informationen« schütze⁴³.

Das RiS »gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«⁴⁴ Bei der Nutzung von IT-Systemen werden aber »zwangsläufig« dem IT-System persönliche Daten geliefert bzw. anvertraut. Der Schutzbereich des RiS ist deshalb nach Auffassung des BVerfG dann nicht eröffnet, wenn auf ein IT-System (z. B. im Rahmen einer Online-Durchsuchung) zugegriffen werde, wenn dabei keine »weitere[n] Datenerhebungs- und Datenverarbeitungsmaßnahmen« mehr erforderlich sind, obwohl sich der Zugreifende dabei »einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen« kann⁴⁵.

5. Abgrenzung vom Grundrecht auf »Schutz der Privatsphäre«

Aus dem allgemeinen Persönlichkeitsrecht ergibt sich das Grundrecht »Schutz der Privatsphäre«. Es ist thematisch und räumlich bestimmt. Es umfasst einerseits Angelegenheiten, die wegen ihres Informationsinhalts typischerweise als »privat« eingestuft werden, »weil ihre öffentliche Erörterung oder Zurschaustellung als unschicklich gilt, das Bekanntwerden als peinlich empfunden wird oder nachteilige Reaktionen der Umwelt auslöst, wie es etwa bei Auseinandersetzungen mit sich selbst in Tagebüchern, bei vertraulicher Kommunikation unter Eheleuten, im Bereich der Sexualität, bei sozial abweichendem Verhalten oder bei Krankheiten der Fall ist.« Weiterhin erstreckt sich der Schutz auf den »räumlichen Bereich, in dem der Einzelne zu sich kommen, sich entspannen oder auch gehen lassen kann«⁴⁶. Allerdings ist dieser Schutzbereich räumlich und thematisch bestimmt. Das Schutzbedürfnis eines IT-System-Nutzers beschränkt sich aber nicht nur auf den Bereich der Privatsphäre.

36 BVerfG, Rdn. 206.

37 BVerfG, Rdn. 182 ff. Ebenso oder ähnlich auch die h. M. im Schrifttum: KUDLICH, HFR 19/2007, 1, 6; BUERMAYER, HRRS 2007, 329, 330 f.; HORNING, DuD 2007, 575, 578 f.; a. A. HUBER, NVwZ 2007, 880, 883, wonach der Schutzbereich des Art. 10 GG auch eröffnet sein soll, wenn auf gespeicherte E-Mails zugegriffen wird.

38 Vgl. etwa KUDLICH, HFR 19/2007, 1, 6; HORNING, JZ 2007, 828, 831; BUERMAYER, HRRS 2007, 329, 333; KUTSCHA, NJW 2007, 1169, 1170 f.

39 Vgl. RUX, JZ 2007, 285, 293 f.; vgl. hierzu auch HORNING, JZ 2007, 828 ff. und RUX, JZ 2007, 831 ff.

40 BVerfG, Rdn. 194. Ebenso zuvor schon HOFMANN, NSTZ 2005, 121, 124; so auch: GERMANN, Gefahrenabwehr und Strafverfolgung im Internet, S. 541; BÖCKENFÖRDE, Die Ermittlung im Netz, S. 224.

41 KUDLICH, HFR 19/2007, 1, 4 f.; JAHN/KUDLICH, JR 2007, 57, 60; HORNING, JZ 2007, 828 ff.

42 BVerfG, Rdn. 200.

43 BVerfG, 2 BvR 2099/04 vom 2. 3. 2006, Rdn. 92; zur Bedeutung in privatrechtlichen Rechtsverhältnissen siehe BVerfG, 1 BvR 2027/02 vom 23. 10. 2006.

44 BVerfGE 65, 1, 43.

45 BVerfG Rdn. 200; die Abgrenzung des »neuen« Grundrechts vom Recht auf informationelle Selbstbestimmung sei nach EIFERT, NVwZ 2008, 521 f. zu unscharf, es sei nicht einsichtig, warum bei der Verarbeitung großer Datenmengen das Recht auf informationelle Selbstbestimmung nicht eingreifen solle; der Abgrenzung zum »neuen« Grundrecht ebenfalls widersprechend BRITZ, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411, 413.

46 BVerfGE 101, 361, 382 f.

Problematisch ist weiterhin, dass die Zuordnung zur Privatsphäre häufig von dem Kontext abhängt, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden⁴⁷.

II. Eingriff

Ein Eingriff in den Schutzbereich des GGVIIS liegt dann vor, wenn die Vertraulichkeit und Integrität des IT-Systems nicht mehr gewährleistet ist, also eingeschränkt oder aufgehoben wird. Der Eingriff kann dabei auch darin liegen, dass auf das IT-System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten⁴⁸. Die Begriffe Integrität und Vertraulichkeit werden vom BVerfG nicht besonders deutlich getrennt⁴⁹. Vertraulichkeit ist das Interesse des Nutzers, dass Daten, die im IT-System erzeugt, verarbeitet oder gespeichert werden, vertraulich bleiben. Andererseits liegt ein Eingriff in die Integrität vor, wenn ein Zugriff erfolgt, durch den die Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können⁵⁰.

III. Rechtfertigung

Das GGVIIS ist nicht schrankenlos gewährleistet. Für den Eingriff in das Allgemeine Persönlichkeitsrecht und damit auch in das GGVIIS besteht ein einfacher Gesetzesvorbehalt. Danach ist zur Rechtfertigung zunächst (als Schranke) ein Parlamentsgesetz erforderlich, das das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG beachten muss.

Online-Durchsuchungen wurden Ende 2006⁵¹ in den Katalog der nachrichtendienstlichen Mittel in das VSG-NW aufgenommen. Online-Durchsuchungen waren danach zulässig, wenn die Verfassungsschutzbehörde tatsächliche Anhaltspunkte für die Annahme hat, dass durch die Online-Durchsuchung Erkenntnisse über verfassungsfeindliche Bestrebungen gewonnen werden können (§ 5 Abs. 2, § 7 Abs. 1, § 3 Abs. 1 VSG-NW). Ferner verweist § 5 Abs. 2 Nr. 11 Satz 2 VSG-NW auf die »Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz«, sofern eine Maßnahme nach § 5 Abs. 2 Nr. 11 VSG-NW in das Brief-, Post- oder Fernmeldegeheimnis eingreift oder einem solchen Eingriff nach Art und Schwere gleichkommt.

Die Verfassung verbietet es dem Gesetzgeber beliebige Schranken zu schaffen. Diese Grenzen werden üblicherweise »Schranken-Schranken« genannt.

a) 1. Schranken-Schranke: Gebot der Normenklarheit und Normenbestimmtheit

Das Gebot der Normenklarheit und Normenbestimmtheit hat seine Grundlage im Rechtsstaatsprinzip. Es soll sicherstellen, »dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann.«⁵²

Nicht vereinbar mit dem Gebot ist die in § 5 Abs. 2 Nr. 11 Satz 2 VSG-NW enthaltene pauschale Verweisung auf die Voraussetzungen des Gesetzes zu Art. 10 GG für den Fall, dass die Maßnahme in Art. 10 GG eingreift. Da die Frage, ob eine Maßnahme in ein Grundrecht eingreift, »komplexe Abschätzungen und Bewertungen« erfordert, ist diese Frage vielmehr vom Gesetzgeber selbst und ausdrücklich zu beantworten.

b) 2. Schranken-Schranke: Verhältnismäßigkeitsgrundsatz

Darüber hinaus ist ein Eingriff nur dann gerechtfertigt, wenn er dem Verhältnismäßigkeitsgrundsatz genügt. Die Verhältnis-

mäßigkeitsprüfung wird in drei Stufen vorgenommen: Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne.

Der Eingriff ist geeignet, wenn er ein taugliches Mittel ist, um ein legitimes Ziel zu erreichen.

Das BVerfG führt dazu aus, dass Online-Durchsuchungen geeignet sind, die Aufgaben der Verfassungsschutzbehörde zu erfüllen (vgl. § 3 Abs. 1 VSG-NW). Verfassungsschutzbehörden haben die legitime Aufgabe »im Vorfeld konkreter Gefahren« die »freiheitliche[n] demokratische[n] Grundordnung«, den »Bestand[es] von Bund und Ländern sowie bestimmte[r] auf das Verhältnis zum Ausland gerichtete[r] Interessen der Bundesrepublik« zu sichern. »Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen«⁵³. Zur Gewährleistung dieser Sicherheit muss der Staat Gefahren durch terroristische oder andere Bestrebungen entgegen treten. Kriminelle nutzen zur Erreichung dieser terroristischen oder anderen Ziele moderne technische Mittel, so auch IT-Systeme. Der (heimliche) Zugriff hierauf ist geeignet, die aus der Nutzung von IT-Systemen resultierenden Gefahren für die Sicherheit des Staates oder der Bevölkerung abzuwehren⁵⁴.

Der Eingriff muss zur Erreichung des Ziels auch erforderlich sein, das bedeutet, es darf kein milderer Mittel geben, welches den gleichen Erfolg erzielen würde.

Schließlich muss der Eingriff auch verhältnismäßig im engeren Sinne sein. Bei Eingriffen in die Privat- und Sozialsphäre muss die Mittel-Zweck-Relation beachtet werden, das heißt, desto stärker der Eingriff in die Grundrechtspositionen der Betroffenen ist, desto überragender muss der Schutz der für die Allgemeinheit wichtigen Rechtsgüter sein.

Das BVerfG betont in seinen Entscheidungen insoweit immer wieder, dass nur konkrete Gefährdungslagen geeignet sind, um in hochrangige Grundrechte (insbesondere in das Allgemeine Persönlichkeitsrecht und damit in das GGVIIS) einzugreifen. Im Vorfeld der Gefahrenabwehr scheiden solche Eingriffe regelmäßig aus. Selbst eine allgemeine Bedrohungslage, wie sie nach dem 11. September 2001 bestanden hat, oder außenpolitische Spannungslagen sind für sich betrachtet nicht ausreichend⁵⁵. Das BVerfG macht deutlich, dass der Staat Grundrechte nicht nur gewähre, sondern darüber hinaus die Freiheitssphäre der Bürger aktiv schützen müsse⁵⁶. »Vermutungen oder allgemeine Erfahrungssätze allein« seien nicht ausreichend, »um den Zugriff zu rechtfertigen.«⁵⁷

Sofern der Zugriff auf ein IT-System heimlich – wie bei der Online-Durchsuchung – erfolgt, handelt es sich um einen besonders intensiven Eingriff, der besonderer Rechtfertigung bedarf, da die »Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme« ist⁵⁸.

c) 3. Schranken-Schranke

Das Gesetz muss weiterhin verfahrensrechtliche Vorgaben treffen, um den grundrechtlich geschützten Interessen des Betroffe-

47 BVerfG Rdn. 197.

48 BVerfG Rdn. 204 ff.

49 Hier setzt auch die Kritik von EIFERT, NVwZ 2008, 521, 522 an, wonach jeder Eingriff in die Vertraulichkeit zwingend einen Eingriff in die Integrität bedeutet (und weitgehend auch) umgekehrt.

50 BVerfG Rdn. 204.

51 Durch Gesetz vom 20. 12. 2006 mit Wirkung vom 30. 12. 2006, vgl. GV NRW S. 620.

52 BVerfG Rdn. 209.

53 BVerfG Rdn. 219 f.

54 BVerfG Rdn. 221 ff.

55 BVerfG Rdn. 231 ff.; BVerfG, 1 BvR 518/02 vom 4. 4. 2006, Rdn. 147 f.

56 Vgl. ADAMSKI, GWP 2008, 259, 267.

57 BVerfG Rdn. 256 ff.

58 BVerfG Rdn. 238.

nen Rechnung zu tragen⁵⁹. Sofern heimliche Ermittlungstätigkeiten vorgenommen werden sollen, sind diese grundsätzlich »unter den Vorbehalt richterlicher Anordnung zu stellen.« Hierdurch wird die »vorbeugende Kontrolle« durch eine »unabhängige und neutrale Instanz« ermöglicht und gewährleistet, »dass die Entscheidung über eine heimliche Ermittlungsmaßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn der Betroffene selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann.« Ausnahmen sind dabei nur unter engen Voraussetzungen (insbesondere eine anschließende Überprüfung durch den Richter) insbesondere bei Gefahr im Verzug zulässig⁶⁰.

d) *Schutz des Kernbereichs privater Lebensgestaltung*
Schließlich kann durch ein Gesetz nur dann ein Eingriff gerechtfertigt werden, wenn es Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung trifft. Hierzu ist ein zweistufiges Schutzkonzept⁶¹ erforderlich.

Zuerst muss versucht werden, soweit wie möglich, die Erhebung der Daten aus diesem Bereich zu unterlassen. Soweit dies nicht möglich ist, muss durch Verfahrensvorschriften sichergestellt sein, dass, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, »die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben«⁶².

Ein Problem in tatsächlicher Hinsicht ist hierbei, dass vor bzw. bei der Erhebung der Daten nicht differenziert werden kann, ob die erhobenen Daten in den Bereich der privaten Lebensgestaltung fallen. Das BVerfG betont aber, dass es verfassungsrechtlich nicht gefordert ist, »den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen«, sofern eine konkrete Gefahr für ein überragend wichtiges Schutzgut vorliegt⁶³. Es ist aber ein Verfahren zur Durchsicht der Daten gesetzlich vorzuschreiben, das eine unverzügliche Löschung der in den Bereich der privaten Lebensgestaltung fallenden Inhalte garantiert und eine Weitergabe oder Verwertung der Daten ausschließt.

E. Neuere Entwicklungen

Die Entscheidung des BVerfG hat schon zu ersten Reaktionen der Gesetzgebung geführt. In Bayern wurde am 22. Juli 2008⁶⁴ der Art. 34 d in das Polizeiaufgabengesetz (PAG) eingefügt, der Online-Durchsuchungen unter bestimmten, genau im Gesetz

regelten Voraussetzungen zulässt⁶⁵. Der bayerische Gesetzgeber hat versucht, dabei weitgehend die Maßgaben der Entscheidung des BVerfG zur Online-Durchsuchung in NRW umzusetzen. So ist insbesondere eine Online-Durchsuchung nur bei einem konkreten Verdacht der Begehung oder Planung schwerer, bestimmter Straftaten zulässig. Es sind detaillierte Regelungen zum Schutz des Kernbereichs der privaten Lebensgestaltung sowie von Berufsgeheimnisträgern vorgesehen. Die Online-Durchsuchung muss vom Richter angeordnet werden, bei Gefahr im Verzug allerdings auch durch den Dienststellenleiter der Behörde, wobei allerdings dann unverzüglich eine Bestätigung durch einen Richter einzuholen ist. Kritisiert wird die neue Gesetzeslage wegen der möglichen Anordnung von Maßnahmen gegen Unbekannt und damit verbundenen Streubreite erheblicher Grundrechtseingriffe⁶⁶.

Auch auf Bundesebene wurde inzwischen eine gesetzliche Grundlage für Online-Durchsuchungen geschaffen. Mit Wirkung zum 1. 1. 2009 wurde der Unterabschnitt 3 a (Abwehr von Gefahren des internationalen Terrorismus) in das Bundeskriminalamtgesetz eingefügt. Die Regelungen sind mit denen im bayerischen PAG vergleichbar, lassen aber auch bei Gefahr im Verzug keine Online-Durchsuchungen ohne richterliche Anordnung zu⁶⁷.

⁵⁹ BVerfG Rdn. 257.

⁶⁰ BVerfG Rdn. 258 ff.

⁶¹ BVerfG Rdn. 280.

⁶² BVerfG Rdn. 282.

⁶³ BVerfG Rdn. 279.

⁶⁴ Durch Art. 27 Abs. 1 des Gesetzes vom 22. Juli 2008 (GVBl S. 421).

⁶⁵ Art. 34 d PAG wurde inzwischen durch das Gesetz zur Änderung des Polizeiaufgabengesetzes, des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Datenschutzgesetzes vom 14. 7. 2009 (Drs. 16/1271, 16/1813) schon wieder geändert. Mit der Novelle entfällt die Befugnis zur Veränderung von Daten am IT-System. Schließlich ist nun für die Anordnung von Maßnahmen nach Abs. 2 (Ermittlung von Kennungen und des Standortes) grundsätzlich der Richter zuständig. Bemerkenswert ist auch, dass mit dieser Novellierung die Befugnis nach Art. 34 e PAG (sog. »notwendige Begleitmaßnahme«) entfällt, die es ermöglichte, verdeckt Sachen zu durchsuchen sowie die Wohnung des Betroffenen zu betreten und zu durchsuchen, wenn dies der Durchführung eines verdeckten Zugriffs auf IT-Systeme nach Art. 34 d PAG diene.

⁶⁶ BÖCKENFÖRDE, JZ 2008, S. 925, 933.

⁶⁷ Die Ausnahmen von der richterlichen Anordnungspflicht waren im ursprünglichen Gesetzesentwurf (§ 20 k des Entwurfes, BR-Drs. 404/08) enthalten, wurden aber im Verlauf des Gesetzgebungsvorhabens gestrichen, da ansonsten das Inkrafttreten zum 1. 1. 2009 gescheitert wäre.

Widerrechtlich abgestellte Fahrzeuge werden kostenpflichtig abgeschleppt. Dennoch nutzen seit geraumer Zeit immer mehr Innenstadtbesucher die Kundenparkplätze, um den teuren Park-

¹ Die Klausur wurde im Examenklausurenkurs der Albert-Ludwigs-Universität Freiburg in leicht modifizierter Form gestellt. Der Schnitt lag bei 4,8 Punkten, wobei 7,7% der Bearbeiter vollbefriedigend oder besser benotet wurden und 30,7% der Studenten nicht bestanden. Maïke Huneke ist akademische Mitarbeiterin am Institut für Rechtsgeschichte und geschichtliche Rechtsvergleichung (germ. Abt.) an der Albert-Ludwigs-Universität Freiburg. – §§ ohne Gesetzesangabe sind solche des BGB.

hausgebühren zu entgehen. E möchte dies nicht länger hinnehmen. Er beauftragt daher die A-GmbH, die im Internet mit einer ganz besonderen Geschäftsidee wirbt, mit der Feststellung von Falschparkern auf dem Supermarktparkplatz und dem Abschleppen unberechtigt parkender Fahrzeuge. Im Vertrag wird eine Pauschale von durchaus marktüblichen 180 € je abgeschlepptem Auto vereinbart, wobei E Ersatzansprüche gegen die Falschparker aus dem Abschleppvorgang an Erfüllung statt an die A-GmbH abtritt.

Eines Dienstags gegen 17.00 Uhr fährt Franzi (F), die mit ihrem Wagen in die Stadt gefahren ist, um sich dort mit ihrem Freund zu treffen, auf das Supermarktgelände. Da sie sich die Parkgebühr von 1,50 €/Stunde für die öffentlichen Parkplätze in der Innenstadt sparen möchte, parkt F ohne Kaufabsicht auf einem der Kundenparkplätze. Das Schild an der Einfahrt des Parkplatzes nimmt sie zwar zur Kenntnis, sieht aber Falschparken als Kavaliärsdelikt an – zumal überhaupt nur wenige Parkplätze besetzt sind.

M, ein Mitarbeiter der A-GmbH, beobachtet, wie F einparkt und zu Fuß das Supermarktgelände verlässt. Als sie um 20.00 Uhr noch immer nicht zurück ist, lädt M ihren Wagen schließlich auf seinen Abschlepper. Dann fährt er zum Firmengelände der A-GmbH, wo er das Auto der F im Hof ablädt.

Um 23.00 Uhr kommt F zum Supermarktparkplatz zurück, der nun zu ihrem großen Erschrecken vollkommen leer ist. An der Stelle, auf der sie das Auto abgestellt hatte, findet sie einen kleinen Aufkleber der A-GmbH, auf dem Anschrift des Abschleppunternehmens und Abholzeiten angegeben sind. Als F am nächsten Morgen dorthin fährt, möchte man ihr den Wagen nur gegen Zahlung von 180 € herausgeben. F ist über diese »Abzocke« empört, schließlich habe sie niemandem den Parkplatz weggenommen. Auch koste das Abschleppen selbst höchstens 150 €, zusätzliche Betriebskosten der A-GmbH für Parkplatzüberwachung, Werbung, Forderungsausfälle, usw. könne man nun wirklich nicht auf sie umlegen. Sie wolle jetzt jedenfalls sofort ihr Auto.

1. Kann F von der A-GmbH Herausgabe des Pkw verlangen?
2. Kann E von F für die Nutzung des Parkplatzes eine »Parkgebühr« verlangen?

F ist schließlich zur Zahlung der 180 € bereit, hat aber gerade nicht so viel Geld. Weil sie dringend auf das Auto angewiesen ist, um zur Arbeit zu fahren, bietet sie der A-GmbH im Austausch ihr Notebook im Wert von 500 € zum Pfand. M nimmt das Gerät zwar als zusätzliche Sicherheit entgegen, ist sich dann aber doch nicht sicher, ob sein Chef mit der Herausgabe des Autos einverstanden ist. Letztlich behält er Notebook und Auto.

F, die sich nun im Recht sieht, schleicht sich nachts auf den Hof der A-GmbH und fährt ihr Auto heimlich nach Hause. Die A-GmbH erhebt deshalb Klage gegen F auf Herausgabe des Pkw. Daraufhin beantragt F ihrerseits widerklagend, ihr Eigentum am Auto sowie das Fehlen eines Besitz- oder Zurückbehaltungsrechts der A-GmbH festzustellen.

3. Wie wird das Gericht entscheiden? Von der Zulässigkeit beider Klagen ist auszugehen.

Frage 1: Anspruch der F gegen die A-GmbH auf Herausgabe des Pkw

I. Anspruch der F gegen die A-GmbH gem. §§ 677, 681, 667

Ein Anspruch der F gegen die A-GmbH auf Herausgabe des Autos könnte sich zunächst aus §§ 677, 681 S. 2, 667 ergeben. Die A-GmbH müsste dazu ein Geschäft für F geführt haben, ohne von ihr beauftragt worden zu sein.

1. Geschäftsbesorgung

Der Begriff der Geschäftsbesorgung ist wie bei § 662 im weiten Sinne zu verstehen und umfasst Tätigkeiten aller Art². Es

sind keine Rechtsgeschäfte erforderlich, vielmehr genügen auch Handlungen rein tatsächlicher Art. Das Abschleppen des Pkw durch die A-GmbH ist damit eine Geschäftsbesorgung i. S. d. § 677.

2. Fremdes Geschäft

Die A-GmbH müsste das Auto »für einen anderen« abgeschleppt haben, also ein fremdes Geschäft mit Fremdgeschäftsführungswillen besorgt haben. Ein Geschäft ist fremd, wenn es nicht ausschließlich eine Angelegenheit des Geschäftsführers beinhaltet, sondern zumindest auch in den Interessenbereich eines anderen fällt³.

Die A-GmbH kam beim Abschleppen in erster Linie ihrer eigenen vertraglichen Verpflichtung gegenüber E nach, von dem sie mit der Entfernung unberechtigt parkender Fahrzeuge beauftragt worden ist⁴. Zugleich stellt das Falschparken aber eine rechtswidrige Besitz- und Eigentumsstörung dar, weshalb F gegenüber E als Zustands- und Handlungsstörer gem. § 862 I und § 1004 I verpflichtet ist, ihr Auto vom Parkplatz zu entfernen⁵. Der Abschleppvorgang ist damit gleichzeitig eine Angelegenheit der A-GmbH und der F. Es handelt sich um ein von den §§ 677 ff. grundsätzlich erfasst⁶ sog. auch-fremdes Geschäft.

3. Fremdgeschäftsführungswille

Problematisch ist aber das Vorliegen eines Fremdgeschäftsführungswillens, ob also die A-GmbH um die Fremdheit des Geschäfts wusste und auch im Interesse der F handeln wollte⁷. Ein Fremdgeschäftsführungsbewusstsein seitens der A-GmbH liegt vor, bzgl. des voluntativen Elements ergeben sich jedoch deshalb Zweifel, weil es sich bei der A-GmbH um eine sog. pflichtengedundene Geschäftsführerin handelt.

Teilweise wird auch bei diesem Unterfall des auch-fremden Geschäfts ein Fremdgeschäftsführungswille vermutet⁸. Jedenfalls gelte dies dann, wenn der Vertrag des Geschäftsführers mit dem Dritten Rechte und Pflichten des Geschäftsführers, insbesondere die Entgeltfrage, nicht abschließend regelt⁹.

Gegen die Anwendung der §§ 677 ff. bei vertraglicher Gebundenheit des Geschäftsführers spricht die Gefahr einer Denaturierung des Instituts der Geschäftsführung ohne Auftrag zum allgemeinen Regressanspruch. Die GoA bezweckt nicht, dem Handelnden zu seinem vertraglichen Vergütungsanspruch gegen den Vertragspartner einen weiteren Anspruch gegen einen Dritten hinzu zu geben¹⁰. Auch passen die Rechtsfolgen der §§ 677 ff. nicht ohne weiteres auf den pflichtengebundenen Geschäftsführer¹¹. Dieser wäre nämlich gegenüber dem Dritten gem. §§ 681 S. 2, 666 auskunfts- und rechenschaftspflichtig und müsste ihm

² BGHZ 38, 275; Erman/EHMANN Bd. 1, 12. Aufl. 2008, § 677 Rdn. 2; MüKoBGB-SEILER Bd. 4, 5. Aufl. 2009, § 677 Rdn. 2.

³ SCHWARZ/WANDT Gesetzliche SV, 3. Aufl. 2009, § 4 Rdn. 5; ähnlich Erman/EHMANN (Fn. 2) § 677 Rdn. 3; Palandt/SPRAU 69. Aufl. 2010, § 677 Rdn. 3.

⁴ Welchem Vertragstyp der zwischen E und der A-GmbH geschlossene Vertrag zuzuordnen ist, ist für die Fallfrage ohne Belang und kann daher offen bleiben.

⁵ Bereits hier kann diskutiert werden, ob das Falschparken eine Besitzstörung oder eine Besitzentziehung darstellt. Von der Einordnung der Besitzbeeinträchtigung hängt ab, ob F gem. §§ 862, 1004 oder §§ 861, 985 zur Autoentfernung verpflichtet ist.

⁶ So die h. M., vgl. BGHZ 110, 313; Palandt/SPRAU (Fn. 3) § 677 Rdn. 6 m. w. N.

⁷ Vgl. Palandt/SPRAU (Fn. 3) § 677 Rdn. 3.

⁸ StRsp; BGHZ 16, 12; 40, 28 (»Funkenflug«); 65, 357; 98, 240; BGH NJW 2000, 72; NVwZ 2002, 512.

⁹ So die neuere Rsp, vgl. BGH NJW-RR 2004, 81 und 956.

¹⁰ OLG Saarbrücken NJW 1998, 829; kritisch auch Erman/EHMANN (Fn. 2) § 677 Rdn. 10 m. w. N.; MEDICUS Bürgerliches Recht, 22. Aufl. 2009, Rdn. 414; SCHUBERT AcP 178 (1978), 425 ff.

¹¹ OLG Koblenz NJW 1992, 2368; MEDICUS (Fn. 10) Rdn. 414.

Abschleppen vom Supermarktparkplatz – Selbsthilfe oder Abzocke?¹

Von Akad. Mit. Maïke Huneke, Freiburg i. Br.

Besitzschutz – Delegation des Selbsthilferechts – Geschäftsführung ohne Auftrag – Deliktsrecht – Nutzungsersatz – petitorische Widerklage

E betreibt einen größeren Lebensmittelmarkt. Für seine Kunden hat er auf seinem Supermarktgelände einen Parkplatz mit ca. 40 Stellplätzen gebaut. Deutlich sichtbar wurde an der Einfahrt ein Schild angebracht: »Parken nur für Kunden des Supermarktes/Nur für die Dauer des Einkaufs, max. 90 min/Mo.–Sa. 08.00–20.00 Uhr/