HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 1/2015 ISSN 1862-7617 Aufsatz

Dr. Holger Greve, Berlin

Internetregulierung: Beschränkung oder Ermöglichung der Freiheit?*

Als globales Kommunikationsmedium sieht sich das Internet multidimensionalen Regulierungsansprüchen und somit auch Interessenkonflikten ausgesetzt. Dabei ist das Internet geprägt vom Pluralismus kultureller, gesellschaftlicher und damit auch rechtlicher Hintergründe, der in seinem digitalen Raum kollidiert. Nationalstaaten, supranationale Organisationen sowie Private gestalten das Internet im jeweiligen Wirkungsbereich und prägen folglich auch die Möglichkeit der Wahrnehmung zentraler Grund- und Menschenrechte im Netz.

Der Autor geht der Frage nach, ob die Regulierung des Mediums die Freiheit beschränkt oder ermöglicht. Einer einführenden Betrachtung der Internetregulierung schließt sich die Analyse des Internets als Grundrechtsverwirklichungsnetz an. Sodann konstatiert der Verfasser eine Belastungskumulation von netzbezogenen Eingriffen und bespricht Grundrechte als Ordnungsmaßstab und zur Absicherung von Freiheitssphären. Sein Beitrag endet mit der Untersuchung staatlicher Schutzpflichten und der Gewährleistung der Funktionalität grundrechtlicher Wahrnehmung sowie des Prinzips der Netzneutralität.

Herr Dr. Greve gelangt zu dem Ergebnis, dass sich die eingangs gestellte Frage nicht in einem abschließenden Gesamturteil bewerten lasse. Neben einerseits potenziellen Grundrechtsbeeinträchtigungen durch staatliche netzbezogene Eingriffe, können jene andererseits mittels der Schaffung eines Ordnungsrahmens oder im Rahmen der staatlichen Schutzpflicht, die Freiheiten des Einzelnen abzusichern, auch grundrechtliche Freiheit ermöglichen. Da ein Konsens zu einheitlichen Grundrechtsstandards im Internet derzeit nicht auf einem hohen Niveau zu erreichen sei, erscheine der Weg zu einem Internetvölkerrecht eher langwierig. Wenngleich auf eine Entwicklung zur Renationalisierung des Internets verwiesen wird, gehen auch von europäischer Ebene Impulse aus, wie aktuell die Gewährleistung von Netzneutralität betreffend. Angesichts des netzregulativen Ausbaus der Kontroll- und Einwirkungsmaßnahmen auf nationalstaatlicher Ebene, werde der Schutz der Freiheit im Internet indes am effektivsten durch die Grundrechte gewährleistet.

I. Einleitung

1 Mit der Entwicklung des World Wide Web als über das Internet abrufbares System von Hypertext-Dokumenten im Jahre 1989 am europäischen Kernforschungszentrum CERN durch den britischen Physiker und Informatiker *Tim Berners-Lee* wurde der Grundstein

* Der Verfasser ist Referent im Bundesministerium des Innern. Der Beitrag gibt nur die persönliche Auffassung des Vortragenden wieder. Er basiert auf einen Vortrag, den der Verfasser am 24.4.2014 an der Andrássy Universität in Budapest gehalten hat. Für Unterstützung und hilfreiche Hinweise danke ich *Dr. Attila Vincze, LL.M.* und *cand. iur. Nerina Buchmann*. Alle Internetadressen wurden zuletzt am 26.01.2015 abgerufen.

für die massentaugliche Nutzung des Internets[1] im digitalen Zeitalter gelegt.[2] Der freie Fluss von Informationen, der durch die global vernetzte elektronische Kommunikation des Internets geradezu seinen idealen Verbreitungsgrad gefunden hat, hinterlässt deutlich sichtbar seine Spuren in Gesellschaft, Wirtschaft, auch in Bezug auf die persönliche Lebensgestaltung.[3] Das Internet als Kommunikationsmedium ermöglicht einen grenzüberschreitenden Austausch von Ideen, Meinungen und Gütern, der in dieser Form historisch einzigartig ist.[4] Als territorial nicht zuordenbares Kommunikationsmedium sieht sich das Internet den unterschiedlichen Regulierungsansprüchen von Nationalstaaten, supranationalen Organisationen und Privaten und damit auch multidimensionalen Interessenkonflikten ausgesetzt, die ihrerseits das Internet und damit die Zugangs- und Nutzungsmodalitäten jeweils gestalten. Exemplarisch ist hier etwa die französische Initiative zu nennen, im europäischen Kontext eine Magna Carta für das Internet zu entwickeln.[5]

S. 2

2 ## II. Internetregulierung

1) Allgemeines

Das Internet als Freiheitsraum ist und war nie ein rechtsfreier Raum.[6] Neben internetspezifischen Regelungen war auch immer schon ein Großteil der bisherigen Rechtsordnung auf Internetsachverhalte unverändert oder ggf. modifiziert anwendbar.[7] Die transnationale elektronische Internetkommunikation setzt der Leistungsfähigkeit sowie Durchsetzbarkeit von nationalen Rechtsnormen dennoch faktische Grenzen. Hinzu tritt ein Nebeneinander einer Vielzahl von Normgebern, die dem staatlichen Ordnungsanspruch im Internet ebenfalls Einhalt gebieten. Der Pluralismus kultureller, gesellschaftlicher und damit auch rechtlicher Hintergründe, der im digitalen Raum des Internets kollidiert, erschwert den Nationalstaaten den Schutz sozialer Normen und ihre Durchsetzung durch nationales Recht.[8] Der digitale Raum sieht sich den unterschiedlichen Regulierungsansprüchen von Nationalstaaten, supranationalen Organisationen und Privaten[9] ausgesetzt, die ihrerseits im jeweiligen Wirkungsbereich das Internet gestalten und damit die Möglichkeit der Wahrnehmung zentraler Grund- und Menschenrechte im Netz entscheidend prägen.[10] Es zeichnet sich zusehends eine Fragmentierung des Internets ab, die aufgrund der differierenden Zugangs- und Nutzungsvoraussetzungen[11] zu einem digitalen Gefälle von Partizipationsmöglichkeiten an Information und Kommunikation führt.[12] Steuernde Wirkung entfaltet auch die technische Architektur des Internets, die maßgeblich durch den Code[13] und die verbindlichen Standards internationaler Organisationen[14] geprägt wird. Im Zuge der NSA-Enthüllungen und aufgrund

---

[1] Gab es im Dezember 2000 noch ca. 360 Millionen Internetnutzer weltweit, so ist momentan davon auszugehen, dass über 3,04 Milliarden Menschen (Stand: 30.06.2014) das Internet nutzen, Tendenz weiter steigend. Siehe http://www.internetworldstats.com/stats.htm.

[2] Vgl. http://home.web.cern.ch/about/birth-web; siehe auch *Abbate*, Inventing the Internet, 1999.

[3] Dazu etwa *Balkin*, N.Y.U. L. Rev. 79 (2004), 1 ff.; *Lessig*, Code 2.0. 2006; *Zittrain*, The Future of the Internet - And How to Stop It, 2008; ferner US Supreme *Court Reno v. ACLU*, 521 US 844 (1997); BVerfGE 120, 274 (304); BGH, NJW 2013, 1072 (1074).

[4] Vgl. dazu auch *Hoffmann-Riem*, JZ 2012, 1081 ff.

[5] Zu diesen Bestrebungen http://www.nzz.ch/mehr/digital/eine-magna-carta-fuer-das-internet-1.18354000.

[6] Siehe zur Regulierungsdiskussion *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 95 ff. m.w.N.

[7] Vgl. *Hoffmann-Riem*, AöR 137 (2012), 509 (530). Siehe etwa zur Entwicklung des IT-Strafrechts *Altenhain*, in: Weiß (Hrsg.), Rechtsentwicklungen im vereinten Deutschland, 2011, S. 117 ff.

[8] *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 135.

[9] Siehe hierzu *Hoffmann-Riem*, AöR 137 (2012), 509 (533 ff.); *Greve*, in: Franzius/Lejeune/v. Lewinski/Meßerschmidt/Michael/Rossi/Schilling/Wysk (Hrsg.), FS Kloepfer, 2013, S. 665 ff.

[10] *Greve*, K&R 2013, 87 (87).

[11] Ganz offensichtlich wird dies, wenn man etwa die Zugangsmodalitäten eines westlichen Industriestaates mit denen von China oder ähnlichen totalitären Staaten vergleicht.

[12] Vgl. *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 136.

[13] Hierzu *Lessig*, Code and Other Laws of Cyberspace, 1999; *ders.*, Code 2.0., 2006.

[14] Zu nennen sind hier etwa: International Telecommunication Union (ITU), Internet Society (ISOC), World Wide Web Consortium (W3C), Internet Assigned Numbers Authority (IANA), Internet Corporation for As-

wachsenden internationalen Drucks hat die US-Regierung am 14. März 2014 erklärt, dass sie eine Aufgabe ihrer Aufsicht über die ICANN[15] in Erwägung zieht, allerdings unter der Bedingung, dass keine andere nationale Behörde, auch keine Institution wie die Vereinten Nationen die Aufgabe als Kontrollorgan übernehme.[16] Inwieweit auch eine stärkere Rückbindung der ICANN an Grundrechte und hier namentlich die Kommunikationsfreiheiten sich durchsetzen lässt, wird derzeit kontrovers diskutiert.[17]

S. 3

3 **2) Kontrolle des Kommunikationsflusses**

Trotz der territorialen Entgrenzung, die der elektronischen Internetkommunikation innewohnt,[18] ist dennoch eine Renationalisierung bzw. Reterritorialisierung der Räume des Internets zu beobachten.[19] Die Entwicklung zu einem Internet Governance[20] im Sinne eines konstituierenden Internetvölkerrechts[21] gestaltet sich äußerst schwerfällig, was maßgeblich am fehlenden internationalen Konsens liegt. Die gescheiterten Verhandlungen auf der World Conference on International Telecommunications (WCIT-12) der Internationalen Fernmeldeunion (ITU) im Dezember 2012 im Hinblick auf einen verstärkten Einfluss auf die Internetverwaltung haben dies einmal mehr deutlich zutage gebracht.[22] Eine Übertragung von zentralen Aufgaben der Internetverwaltung auf die ITU hätte zwangsläufig dazu geführt, dass private Akteure weniger Mitwirkungsmöglichkeiten hätten, zudem wurde namentlich von westlichen Staaten befürchtet, dass stärkere Eingriffe in die Netzarchitektur zu befürchten seien, die vor allem auf die „Zensur" unliebsamer Meinungen abziele. Dennoch sind momentan Ansätze erkennbar, die insbesondere auf eine Stärkung von Grundrechten im Netz abzielen.[23] So hat An-

signed Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), Internet Architecture Board (IAB) und InterNIC. Dazu *Schonscheck*, Datenschutz PRAXIS 5/2013, 9 f. Regelungen werden vor allem durch die Internetprotokolle ("Gesetzbuch des Internets"), die sogn. Request for Comments (RFCs), getroffen. Mittlerweile gibt es fast 8000 Protokolle, die in offenen Arbeitsgruppen erstellt werden. Vgl. *Kleinwächter*, FAZ v. 23.4.2014, S. 13.

[15] Die Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert die Vergabe von einmaligen Namen und Adressen im Internet. Dazu gehört die Koordination des Domain Name Systems und die Zuteilung von IP-Adressen, was auch als IANA-Funktion bezeichnet wird.

[16] Hierzu *Weber* , in: Hoeren/Sieber/Holznagel (Hrsg.), Multimediarecht, Stand: 39. Erg. Lg. 2014, Teil 2 Rn. 35.

[17] Siehe dazu den Vorschlag des Europarats http://www.coe.int/t/informationsociety/icann-and-human-rights.asp.

[18] Zu diesem Aspekt bereits *Johnson/Post*, Stan. L. Rev. 48 (1996), 1367 ff.; *Lessig*, Stan. L. Rev. 48 (1996), 1403 ff.; *Goldsmith/Wu*, Who Controls the Internet?, 2006, S. 147 ff.

[19] In jüngster Zeit haben insbesondere Russland und China, gefolgt von der Türkei und zahlreichen Schwellenländern, die Forderung nach einer stärkeren Renationalisierung gestellt. Zu nennen sind hier aber auch Forderungen wie das sogn. Schengen-Routing. Siehe http://www.dw.de/wer-verwaltet-bald-das-internet/a-17518874.

[20] Vgl. *Weber* , in: Hoeren/Sieber/Holznagel (Hrsg.), Multimediarecht, Stand: 39. Erg. Lg. 2014, Teil 2; *ders.*, Shaping Internet Governance: Regulatory Challenges, 2009; *Waz/Weiser* , J. ON TELECOMM. & HIGH TECH. L. 10 (2013), 331 ff.; *Land*, Harv. Int. Law J. 54 (2013), 393 ff.; *Cerf/Ryan/Senges*, ISJLP 10 (2014), 1 ff. Nach einer von der VN entwickelten Definition im Jahre 2005 versteht man unter Internet Governance: „Entwicklung und Anwendung gemeinsamer Prinzipien, Normen, Regeln, Entscheidungsverfahren und Programme für die Fortentwicklung und die Anwendung des Internets durch Regierungen, den privaten Sektor und die Zivilgesellschaft."

[21] Zur Auseinandersetzung um die Internetverfassung nach völkerrechtlichen Maßstäben *Fischer-Lescano*, JZ 2014, 965 (967 ff.).

[22] Siehe dazu http://www.zeit.de/digital/internet/2013-05/ITU-Genf-WTPF.

[23] Zu nennen ist in diesem Zusammenhang etwa die brasilianische sogen. Internetverfassung „Marco Civil da Internet", die während der Netmundial in Sao Paulo von der brasilianischen Präsidentin *Dilma Roussef* unterzeichnet wurde. Durch das Gesetz soll insbesondere gewährleistet werden, dass die Daten von Internetnutzern vor Spionage und Missbrauch geschützt werden. Ferner werden elementare Grundprinzipien der Internetregulierung in Brasilien festgelegt (z.B. Erhaltung und Sicherung der Netzneutralität, Förderung des Rechts auf den Zugang zum Internet, Schutz der Privatsphäre, Sicherung der Kommunikationsfreiheiten, Interoperabilität, Förderung von offenen technischen Standards etc.). Die Regelung schafft damit eine explizite digitale Gewährleistung von Grundrechten und spezifischen Zielbestimmungen, die ausländische Anbieter von Kommunikationsdiensten dann bindet, wenn diese ihr Angebot für den brasilianischen Markt zur Verfügung stellen. Diese Reterritorialisierung des Internets führt zwangsläufig zu Kollisionen von unterschiedlichen Rechtsordnungen. Eine deutsche Übersetzung des Gesetzes ist abrufbar unter http://www.uni-muenster.de/Jura.tkr/oer/files/pdf/MarcoCivilDaInternetDeutscheÜbersetzungITM.pdf.

fang April 2014 die parlamentarische Versammlung des Europarats eine stärkere Absicherung von Grundrechten im Netz angemahnt,[24] in diesem Zusammenhang hat auch das Ministerkomitee des Europarats in Straßburg am 16. April 2014 einen „Grundrechtsführer" für Internetnutzer veröffentlicht, der die einschlägige Rechtsprechung des EGMR dokumentiert.[25] Ebenso hat bereits 2012 der Menschenrechtsrat der UN bekräftigt, dass Menschenrechte, die offline gelten, auch online ihre Gültigkeit haben.

S. 4

4 Zwar ist grundsätzlich eine Stärkung des Einflusses internationaler Organisationen auf die Gestaltung des Internets auszumachen,[26] dennoch hat etwa die Implementation von Sperr- und Filterungstechniken auf nationalstaatlicher Ebene – bedingt durch die jeweilige Rechtsordnung – die Tendenz, die Anreizwirkung zur internationalen Kooperation zwischen staatlichen, internationalen und privaten Normsetzenden zu verringern.[27] Exemplarisch für diese Entwicklungen sind einige im US-amerikanischen Kongress eingebrachte Gesetzesvorhaben (SOPA,[28] PIPA,[29] CISPA[30]) oder auch das Anti-Counterfeit Trade Agreement (ACTA)-Übereinkommen[31] sowie jüngst die Freihandelsabkommen CETA[32] und TTIP[33] zu nennen,[34] die weltweit für rege Diskussion im netzpolitischen Diskurs gesorgt haben.[35] Der Stop Online Piracy Act und der Protect IP Act sehen u.a. vor, dass seitens der Internet Service Provider die Sperrung bestimmter Inhalte und invasive Filtertechniken wie die Deep Packet Inspection eingesetzt werden sollten, um die Verbreitung geschützter Inhalte wirksamer zu verhindern. Vor allem die Bekämpfung von Urheberrechtsverletzungen durch "Internetpiraterie" hat weltweit zahlreiche Gesetze entstehen lassen, die u. a. das Sperren von Webseiten oder sogar als ultima ratio die Sperrung des Internetzugangs vorsehen.[36] Insbesondere webbasierte Peer-to-Peer-Plattformen, auf denen zum Teil zahlreiche Urheberrechtsverletzungen stattfinden, sind von gerichtlich angeordneten Sperrverfügungen betroffen.[37] Eingriffsmaßnahmen wie die Sperrung von Webseiten betrifft vor allem aber auch die politische Meinungsbildung, die vor einiger Zeit erfolgte Sperre von Twitter in der Türkei, die vom türkischen Verfassungsgericht aufgehoben wurde, zeigt dies ganz deutlich.[38]

---

[24] http://www.heise.de/newsticker/meldung/Europarat-Parlamentarische-Empfehlungen-zu-Grundrechten-im-Netz-2168008.html.

[25] https://wcd.coe.int/ViewDoc.jsp?id=2184807&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[26] Dazu bereits *F.C. Mayer*, ZfRSoz 23 (2002), 93 ff.

[27] Vgl. *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 135.

[28] Stop Online Piracy Act.

[29] Protect IP Act.

[30] Cyber Intelligence Sharing and Protection Act. Siehe dazu *Spies*, ZD-Aktuell 2013, 03457

[31] Zu diesem *Gounalakis/Helwig*, K&R 2012, 233 ff.; *Paal/Hennemann*, MMR 2012, 288 ff.; *Hoeren*, MMR 2012, 137 f.; *Uerpmann-Wittzack*, AVR 49 (2011), 103 ff.

[32] Comprehensive Economic and Trade Agreement. Siehe dazu *Fölsing*, RIW 2014, 500 ff.; *Müller/Schmid*, BWGZ 2014, 336 ff.

[33] Transatlantic Trade and Investment Partnership. Hierzu *Krajewski*, ZUR 2014, 396 ff.

[34] Auf Deutschland bezogen lässt sich das Zugangserschwerungsgesetz (BGBl. I 2010, 78) nennen, das ohne Anwendungspraxis aufgrund zahlreicher öffentlicher Proteste und erheblicher verfassungsrechtlicher Bedenken mit Gesetz vom 22.12.2011 (BGBl. I 2011, 2958) wieder aufgehoben wurde. Siehe dazu *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 179 ff., 228 ff.

[35] Dazu die Studie des Berkman Center for Internet and Society der Harvard University, abrufbar unter http://cyber.law.harvard.edu/publications/2013/social_mobilization_and_the_networked_public_sphere.

[36] Siehe *Gesmann-Nuissl/Wünsche*, GRUR Int. 2012, 225 ff.; *Greve/Schärdel* , ZRP 2009, 54 f.

[37] Der EuGH hat am 27.3.2014 (Az. C-314/12) entschieden, dass Provider, die den Zugang zum Internet ermöglichen, grundsätzlich nach nationalem Recht dazu verpflichtet werden können, ihren Kunden den Zugriff auf urheberrechtsverletzende Websites zu erschweren. Das Judikat wurde mittlerweile vom OGH, Beschl. v. 24.6.2014 - 4Ob71/14s aufgenommen. Hiernach sind gezielte Webseitensperrungen zulässig, die sich nicht auf den Zugang zu rechtmäßig verfügbaren Informationen auswirken. Demgegenüber kam das OLG Köln (Urt. v. 18.6.2014 - 6 U 192/11) zum dem Schluss, dass Access-Provider u.a. wegen der Gefahr des Overblocking nicht dazu verpflichtet sind, Netzsperren für Angebote einzurichten, die Links auf widerrechtlich angebotene Musikalben enthalten. Siehe hierzu auch *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 122 ff.; *Spindler*, GRUR 2014, 826 ff.

[38] Das türkische Verfassungsgericht sah in der Sperre eine Verletzung der Meinungsfreiheit nach Art. 26 der türkischen Verfassung. Aufgrund einer Gesetzesverschärfung bedarf es mittlerweile keines Gerichtsbeschlusses mehr, um Webseiten zu sperren. Die türkische Telekom-Behörde kann hiernach Sperranordnungen er-

S. 5

5 Die Kontrolle des Kommunikationsflusses im Internet ist im digitalen Zeitalter zur zentralen Machtfrage vor allem politischer und wirtschaftlicher Steuerungskraft geworden. Erhebliche Eingriffe in den Kommunikationsfluss werden in diesem Zusammenhang mit Aspekten des Rechtsgüterschutzes (z.B. Bekämpfung von Urheberrechtsverletzungen, Persönlichkeitsrechtsschutz) und gefahrenabwehrrechtlich determinierten Präventionsmaßnahmen (z.B. Terrorismusbekämpfung, Cyberwar etc.) begründet.

6 Ebenso können marktmächtige Unternehmen (Apple, Google, Facebook etc.) im Internet aufgrund ihrer faktischen Regelungsmacht[39] ein erhebliches Einwirkungspotenzial auf die Rahmenbedingungen der öffentlichen Kommunikation im Internet sowie die Entfaltungsfreiheit des Einzelnen ausüben.[40] Der öffentliche kommunikative Raum im Internet wird zusehends durch geschlossene Systeme verdrängt, die auf Grundlage vertraglicher Regelungen (in der Regel AGB) wie auch technischer Einschränkungen komplexe Zugangsbeschränkungen normieren können. Daneben kann durch das Zusammenwirken von Internetunternehmen mit staatlichen Stellen im Rahmen der hoheitlichen Indienstnahme Privater ein umfangreicher Zugriff auf Kommunikationsflüsse implementiert werden.[41] Die enorme Datenmacht und das faktische Regelungspotenzial marktmächtiger Internetunternehmen bilden einen erheblichen Anreiz, die Indienstnahme Privater zur Erfüllung öffentlicher Aufgaben als Mittel staatlicher Aufgabenerfüllung einzusetzen. Auch die Inanspruchnahme von Suchmaschinen[42] in ihrer Funktion als Gatekeeper[43] zur Kommunikationsregulierung zwecks Datenschutzes infolge des EuGH-Urteils in Sachen Google[44] läuft Gefahr, ein grundrechtliches Ungleichgewicht hervorzurufen. Denn die Auflösung der grundrechtlichen Spannungslage zwischen Kommunikationsfreiheit und Persönlichkeitsrecht durch Suchmaschinenbetreiber birgt angesichts des vom EuGH anerkannten Vorrangs der Grundrechte aus Art. 7 und 8 der EU-Charta gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden, das Risiko erheblicher Eingriffe in die Kommunikationsfreiheit.[45] Dies gilt umso mehr, da in der Regel die in Anspruch genommen Suchmaschinenbetreiber nicht über die erforderliche Informationsgrundlage verfügen, die es für eine solche komplexe Grundrechtsabwägung bedarf.[46] Demgegenüber wäre eine grundrechtliche Abwägung, die von einem Vorrang des Persönlichkeitsrechts gegenüber den wirtschaftlichen Interessen der Suchmaschinenbetreiber ausgeht, grundsätzlich nicht zu beanstanden.[47]

---

lassen, sofern dies aufgrund „der nationalen Sicherheit, der Wiederherstellung der öffentlichen Ordnung und zur Vorbeugung von Verbrechen" geboten ist.

[39] Siehe dazu *Hoffmann-Riem*, AöR 137 (2012), 509 (533 ff.).

[40] Hierzu etwa *Masing*, NJW 2012, 2305 (2308); *Di Fabio*, FAZ v. 18.9.2014, S. 6.

[41] Beispielhaft ist hier die Vorratsdatenspeicherung (RL 2006/24/EG) zu nennen, die aber aufgrund des Urteils vom EuGH vom 8.4.2014 (Az. C-293/12 u. C-594/12) zunächst erstmal verhindert sein dürfte. In den USA ist die Situation indes noch nicht abschließend geklärt, während ein Bundesrichter im District of Columbia die Vorratsdatenspeicherung als verfassungswidrig einstufte, wurde sie von einem Bundesrichter in New York als rechtlich zulässig qualifiziert. Siehe dazu *Gärditz/Stuckenberg*, JZ 2014, 209 ff.

[42] Zur grundrechtlichen Verortung von Suchmaschinen innerhalb von Art. 5 Abs. 1 GG siehe etwa *Blankenagel*, in: Nolte/Poscher/Wolter (Hrsg.), FG Schlink, 2014, S. 397 ff.

[43] Siehe etwa zur Suchmaschinenneutralität *Paal*, AfP 2011, 521 ff.; *Koreng*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245 (253 ff.); ferner *Dörr/Natt*, ZUM 2014, 829 ff. zu den Fragen den Netzneutralität siehe VII: sowie *Greve*, VR 2013, 109 ff.

[44] EuGH, Urt. v. 13.5.2014 - C-131/12 - Google Spain.

[45] *Feldmann/Piltz*, AnwBl 2014, 679 ff.; *Masing*, Vorläufige Einschätzung der "Google-Entscheidung" des Europäischen Gerichtshofs, 2014, abrufbar unter http://www.verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/#.U-090BZtTRY; *Zittrain*, New York Times v. 14.5.2014, abrufbar unter http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0 .

[46] *Hoeren*, ZD 2014, 325 (325).

[47] In diese Richtung wird das Urteil des EugH von *v. Danwitz*, SZ v. 17.9.2014, S. 6, interpretiert. Ähnlich auch *Lenaerts* in einem Interview mit der taz v. 19.9.2014.

S. 6

7 **3) Ausspähung der Internetkommunikation**

Die Steuerung, Begrenzung und Überwachung der Internetkommunikation im Nebeneinander der unterschiedlichen Normsetzenden führt zu multidimensionalen Grundrechtsgefährdungslagen, die vor allem die abwehrrechtliche Perspektive, aber auch die Schutzpflichtendimension von Grundrechten betrifft. Die Enthüllungen über das von der National Security Agency (NSA) auf Grundlage des Foreign Intelligence Surveillance Act[48] (FISA) betriebene Programm Planning Tool for Resource Integration, Synchronization, and Management (PRISM), das einen Zugriff auf Daten von Internetunternehmen wie Microsoft, Yahoo, Facebook, Apple, Google und Skype ermöglichen soll, dürfte beispielhaft für die grundrechtlichen Herausforderungen im Zeitalter elektronisch vernetzter Kommunikation stehen.[49] So soll durch die Anwendung von PRISM auch eine Echtzeitüberwachung von Internetkommunikation wie z.B. E-Mails, VoIP-Ströme und Chats möglich sein.[50] Eine Analyse der gewonnenen Daten erfolge mithilfe des Boundless Informant-Systems im Wege des Data Minings. In seiner Reichweite noch ausgreifender soll das vom Government Communications Headquarters des britischen Geheimdienstes (GCHQ) auf Grundlage des Regulation of Investigatory Powers Act 2000 verwendete Spähprogramm Tempora sein.[51] Gleichwohl handelt es sich bei den vorstehend beschriebenen Programmen offensichtlich nur um die Spitze des Eisbergs.[52] Der Ansatz der umfassenden Informationsausspähung und -auswertung scheint auf eine Komplettkartographierung der gesamten Internetkommunikation hinauszulaufen.[53]

---

[48] Der Foreign Intelligence Surveillance Act von 1978 wurde durch den Patriot Act von 2001 sowie durch den Protect America Act von 2007 und durch den FISA Amendment Act von 2008 erheblich erweitert (siehe dazu *Himmelmann*, Die Anti-Terrorismusgesetzgebung in Deutschland und den USA, Diss. jur. Münster 2014, S. 30 ff.). Eine Verfassungsbeschwerde wurde vom US Supreme Court mangels nicht hinreichend substantiierter Klagebefugnis – im Hinblick von Abhörmaßnahmen der NSA – zurückgewiesen, *Clapper v. Amnesty International*, 568 U.S. ___ (2013). Für die Aufsicht der geheimdienstlichen Überwachung elektronischer Kommunikation ist der Foreign Intelligence Surveillance Court (FISC) zuständig, der in geheimer Sitzung tagt und seine Entscheidungen bislang grundsätzlich nicht veröffentlicht (siehe aber FISC, ZD 2013, 501 ff. m. Anm. *Schröder*; FISC, CRi 2013, 142 ff.). Die Quote der Bewilligungen von Überwachungsgesuchen liegt seit der Gründung des Gerichts im Jahre 1979 bei 99,97 % bei 30.000 Überwachungsgesuchen. Auch hat eine Überprüfung der Rechtsprechung des FISC durch den US Supreme Court bisher nicht stattgefunden. Siehe auch *Morrison*, Stan. L. & Pol'y Rev. 25 (2014), 341 ff.; *Tinnefeld*, ZD 2013, 581 (584); *Wolf*, JZ 2013, 1039 (1041); http://www.lto.de/recht/hintergruende/h/prism-edward-nowden-geheimgericht-bespitzelung-nsa-internet-google/; http://www.guardian.co.uk/world/2013/jun/20/fisa-court-nsa-without-warrant. Verfassungsrechtlich betrachtet könnte PRISM einen Verstoß gegen den vierten Verfassungszusatz der US-amerikanischen Bundesverfassung darstellen, denn der Schutzbereich des vierten Verfassungszusatzes ist nach der Entscheidung *Katz v. United States*, 389 U.S. 347 (1967) dann berührt, wenn der Betroffene eine begründete Erwartung auf die Wahrung seiner Privatsphäre haben dürfe . Voraussetzung ist jedoch, dass US-Bürger von der Maßnahme betroffen sind. Vgl. http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html. Zum Schutzumfang des vierten Verfassungszusatzes *Slobogin*, Die Verwaltung 44 (2011), 465 ff.; *Wittmann*, ZaöRV 73 (2013), 373 (385 ff.); *ders.*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die U.S.-amerikanische Bundesverfassung, 2014.

[49] Siehe etwa *Richards*, Harv. L. Rev. 126 (2013), 1934 (1937 ff.); *Rottmann*, AnwBl 2014, 966 ff. Nach Angaben der NSA seien durch PRISM 50 Terroranschläge verhindert worden. Vgl. http://futurezone.at/netzpolitik/16573-haben-durch-prism-50-anschlaege-verhindert.php. Die hoheitliche Indienstnahme dieser faktischen Regelungsmacht privater Unternehmen zur Erfüllung öffentlicher Aufgaben findet sich vor allem im Bereich der Gefahrenabwehr. Dazu *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 214 f. Zu nennen ist hier etwa die Vorratsdatenspeicherung oder die Bestandsdatenauskunft.

[50] Vgl. *Bleich*, c´t 16/2013, 112 ff.; *Fox*, DuD 2013, 594; *Gercke*, ZUM 2013, 605 (611 ff.); *Petri*, ZD 2013, 557 (558); *Wolf*, JZ 2013, 1039 (1039 f.); BT-Drs. 17/14465; http://www.heise.de/newsticker/meldung/Bericht-PRISM-ueberwacht-in-Echtzeit-1908878.html.

[51] Die Ausspähung durch den britischen Geheimdienst könnte gegen europäisches Recht verstoßen. Insbesondere kommen die Garantien aus Art. 8 GRCh, Art 16 AEUV, der RL 95/46/EG sowie der RL 2002/58/EG in Betracht. Voraussetzung ist die Eröffnung des Anwendungsbereichs des Unionsrechts. Hier ist problematisch, inwieweit die Bereichsausnahme des Art. 3 Abs. 2 der RL 95/46/EG (öffentliche Sicherheit, Sicherheit des Staates) eingreift. Näher dazu *Schlikker*, NJOZ 2014, 1281 ff. Zum Schutz der EU-Grundrechte zwischen Mitgliedstaaten *Canor*, ZaöRV 73 (2013), 249 ff.

[52] Siehe dazu auch *Greenwald*, Die globale Überwachung, 2014.

[53] Jedenfalls scheinen dies die weiteren Enthüllungen nahezulegen. Exemplarisch seien hier nur einige der weiteren Programme genannt: PICASSO, RAGEMASTER, NIGHSTAND, TAO Tools, MonsterMind, Treasure

Laut Presseberichten sind von der Überwachung der elektronischen Kommunikation auch Internetknotenpunkte und transatlantische Datenverbindungen betroffen.[54] Eine Ausspähung der Daten hätte dann nicht mehr unter Zuhilfenahme Privater, sondern durch direkten Zugriff auf die Kommunikationsströme stattgefunden. Dies legen auch Berichte über das von der NSA und dem britischen Geheimdienst GCHQ betriebene Programm MUSCULAR nahe, wonach ohne Wissen der Unternehmen Google und Yahoo auf deren interne Netzwerke Zugriff genommen worden sei.[55] Die massenhafte Ausspähung von Daten durch ausländische Geheimdienste betrifft primär die Schutzpflichtendimension des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG), des Telekommunikationsgeheimnisses (Art. 10 GG) und auch der Kommunikationsgrundrechte (Art. 5 GG) als Aufgabe staatlichen Grundrechtsschutzes,[56] deren Umsetzung in erster Linie in der Hand des Gesetzgebers liegt.[57]

S. 7

8 Der Bundesnachrichtendienst verfügt seinerseits u.a. über die Möglichkeiten der strategischen Fernmeldeüberwachung auf Grundlage der §§ 5, 8 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10) und kann somit internationale Telekommunikationsbeziehungen einer Vielzahl von Personen mittels (formaler oder inhaltlicher) Suchbegriffe auswerten.[58] Nicht zulässig ist die gezielte Erfassung bestimmter Telekommunikationsanschlüsse oder die Verwendung von Suchbegriffen, die den Kernbereich der privaten Lebensgestaltung betreffen (§ 5 Abs. 2 Satz 1 G 10). Diese Einschränkung soll jedoch nicht für Telekommunikationsanschlüsse im Ausland gelten, sodass auch eine gezielte Filterung der Internetkommunikation möglich wäre. Eine solche Einschränkung des Schutzgehalts von Art. 10 Abs. 1 GG i.V.m. Art. 3 Abs. 1 GG erscheint verfassungsrechtlich durchaus problematisch.[59] Überdies ist zu berücksichtigen, dass die strategische Fernmeldeüberwachung, die ihren historischen Ursprung noch zu Zeiten des Kalten Krieges hat,[60] unter vollkommen anderen politischen und technologischen Bedingungen eingesetzt wurde, die erhebliche Unterschiede zum heutigen digitalen Zeitalter aufweisen. Unter Berücksichtigung der ungeheueren Datenmenge elektronisch vernetzter grenzüberschreitender Kommunikation dürfte eine Begrenzung der strategischen Fernmeldeüberwachung auf 20 % der Übertragungskapazität nach § 10 Abs. 4 Satz 4 G 10 kein wirksames Eindämmungskorrektiv mehr sein, das zu einer spürbaren Eingriffsminderung führt.[61] Die Ausweitung der Überwa-

---

Map, Packagedgoods und Dishfire. Ein Großteil der internetbezogenen Überwachungsmaßnahmen der NSA soll erstaunlicherweise auf die Executive Order 12333 (http://www.archives.gov/federal-register/codification/executive-order/12333.html) des US-Präsidenten *Reagan* aus dem Jahre 1981 gestützt sein. Siehe dazu https://www.aclu.org/blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools.

[54] http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; siehe auch SZ v. 24.6.2013, S. 1 f. Das NSA-Programm XKeyscore soll eine Koordinierung und Zusammenführung von verschiedenen Datenbanken zu Analysezwecken ermöglichen. Das Verhalten von Internetnutzern sei durch die Verwendung des Programms nahezu vollkommen abbildbar. Siehe http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[55] http://www.faz.net/aktuell/politik/ausland/neue-snowden-enthuellungen-nsa-zapft-millionen-nutzerdaten-von-google-und-yahoo-an-12641596.html; http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[56] Siehe auch *Lenski*, ZG 2014, 324 (329 f.); *Schaar*, ZRP 2013, 214 (214 f.).

[57] BVerfGE 39, 1 (44); 46, 160 (164); 121, 317 (356); 125, 39 (78); *Stern*, DÖV 2010, 241 ff.; siehe hierzu VI. Zur völker- und unionsrechtlichen Perspektive *Ewer/Thienel*, NJW 2014, 30 ff.; *Schmahl*, JZ 2014, 220 ff.

[58] Vgl. *Huber*, NJW 2013, 2572 (2573); *Holznagel/Enaux/Nienhaus*, Telekommunikationsrecht, 2. Aufl. 2006, Rn. 696; *Albers*, in: Wolff/Brink (Hrsg.), Beck OK Datenschutzrecht, 9. Ed. Stand: 1.8.2014, Syst. L Rn. 102; siehe hierzu auch *Foschepoth*, Überwachtes Deutschland, Post- und Telefonüberwachung in der BRD, 3. Aufl. 2013. Die angebliche Weitergabe von Daten deutscher Staatsbürger von BND an NSA könnte möglicherweise Gegenstand eines verfassungsgerichtlichen Verfahrens werden. Siehe dazu http://www.heise.de/newsticker/meldung/NSA-Skandal-FDP-will-wegen-Weitergabe-von-Daten-klagen-2431806.html.

[59] Siehe *Durner*, in: Maunz/Dürig (Hrsg.), GG, Stand: 57. Lfg. Januar 2010, Art. 10 Rn. 186; *Huber*, NJW 2013, 2572 (2574).

[60] Vgl. BVerfGE 67, 157 ff.

[61] Siehe auch *Bäcker*, K&R 2014, 556 (558).

chungsbefugnisse und damit auch die wachsende Streubreite von Informationseingriffen unter den Bedingungen der elektronischen Kommunikation führen zu einer veränderten Grundrechtsgefährdungslage, die ggf. rechtliche Anpassungen erforderlich macht, die zuvörderst vom Gesetzgeber zu leisten sind.[62] Hierzu gehört neben den verfassungsrechtlichen Anforderungen einer normenbestimmten und verhältnismäßigen Eingriffsgrundlage auch die Absicherung einer rechtsstaatlichen Kontrolle, die auf einer hinreichenden Transparenz gründen muss.[63]

S. 8 - HFR 1/2015 S. 8 -

9 **III. Internet als Grundrechtsverwirklichungsnetz**

Die netzwerkartige Struktur des Internets ermöglicht die Wahrnehmung eines vielfältigen Grundrechtsgebrauchs.[64] Netzbetreiber, Diensteanbieter und Netzbenutzter, aber auch mannigfaltige Hybridformen, agieren im digitalen Raum des Internets als maßgebliche Akteure der elektronischen Kommunikation, sodass es zu einer Vielzahl von Grundrechtsinanspruchnahmen und Grundrechtsbeziehungen kommt. Dabei handelt es sich weitgehend um die individuelle Wahrnehmung von grundrechtlichen Freiheiten, die jedoch durch die vernetzte Struktur elektronischer Kommunikation miteinander verwoben und zum Teil entsprechungsrechtlich aufeinander bezogen ist.[65] Die gegenseitige Vernetzung und Ergänzung spezieller Grundrechte kumuliert damit in einer Grundrechtskooperation im Sinne einer Hintereinanderschaltung von Grundrechten.[66] Gleichlaufende Interessen können sich daher durchaus auch grundrechtlich gesehen verstärken und so ein stärkeres Gewicht bei möglichen Abwägungsprozessen gewinnen. Aufgrund der Vielzahl unterschiedlicher Interessen, die ihrerseits grundrechtlich abgestützt sind, lassen sich multidimensionale Grundrechtsbeziehungen ausmachen,[67] die sich entsprechend potenzieren können. Die im Netz stattfindende Grundrechtskonzertierung als Addition des Grundrechtsgebrauchs der Vielen schlägt sich daher nicht nur in der subjektivrechtlichen Grundrechtsgewährleistung nieder, sondern entwickelt eine objektive Dimension, die im Grundrechtsverwirklichungsnetz als Einrichtungsgarantie Gestalt gewinnt.[68] Der Schutz der Funktionsfähigkeit elektronisch vernetzter Kommunikation stellt als Grundrechtsvoraussetzung und damit in seiner objektiv-rechtlichen Funktion eine Gemeinwohlaufgabe dar, die über die bloße Addition von Grundrechtspositionen hinausgeht.[69] Die digitale Verwirklichung von grundrechtlicher Freiheit findet im Internet ihre Grundrechtsvoraussetzung, wobei das Vertrauen in die Gewährleistung von Kommunikationsfreiheit und informationelle Selbstbestimmung wesentliche Vorbedingung ist. Die vernetzte Kommunikation schafft digitale Räume grundrechtlicher Entfaltungsmacht, in der sich die digitale Dimension der Grundrechte verwirklicht.[70] Die Digitalisierung der Grundrechte[71] auf der Ebene nationalen und europäischen Verfassungsrechts im Sinne eines Verfassungswandels ist Ausfluss der Umwälzungen und Herausforderungen der Informationsgesellschaft, die zu veränderten Grundrechtsgefährdungslagen geführt haben. Die Freiheit im digitalen Raum und ihre wechselseitige Beschränkung bedürfen daher der Absicherung durch grundrechtliche Gewährleistungen, die ihrerseits einer in den Grenzen des Verfassungswandels dynamischen Interpretation am

[62] Die letzte Entscheidung des BVerfG (E 100, 313 ff.) zu den Überwachungsmaßnahmen des BND nach dem G 10 datiert aus dem Jahre 1999. Die Befugnisse des BND wurden seitdem ausgeweitet. Angesichts des erheblichen Bedeutungszuwachses der elektronischen Kommunikation hat sich die Grundrechtsgefährdungslage erheblich verschärft.
[63] Vgl. *Petri*, ZD 2013, 557 (559 ff.); *Deiseroth*, ZRP 2013, 194 (196 f.).
[64] *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 83 ff.
[65] *Kloepfer/Kutzschbach*, AfP 1999, 1 (4).
[66] Vgl. *Kloepfer*, Grundrechte als Entstehenssicherung und Bestandsschutz, 1970, S. 17.
[67] Vgl. *Schumacher*, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 213 (214 ff.).
[68] Siehe zur Thematik auch *Kloepfer*, in: Sachs/Siekmann (Hrsg.), FS Stern, 2012, S. 405 ff.
[69] Vgl. *Kloepfer*, AfP 2010, 120 (122); *Hoffmann-Riem*, AöR 134 (2009), 513 (541); siehe aus völkerrechtlicher Perspektive *Kettemann*, ZaöRV 72 (2012), 469, (475 ff.).
[70] Siehe dazu *Luch/Schulz*, MMR 2013, 88 ff. Inwieweit neue Formen sozialer Emergenz durch Kollektivität im Internet eine Neuausrichtung des Art. 19 Abs. 3 GG im Hinblick auf juristische Personalität erforderlich machen, erscheint überlegenswert. Zu diesem Ansatz *Ingoldt*, Der Staat 2014, 193 ff.
[71] Vgl. bereits *Roßnagel/Wedde/Hammer/Pordesch*, Digitalisierung der Grundrechte?, 1990; *Karavas*, Digitale Grundrechte, 2007.

Maßstab der Verfassungswirklichkeit unterliegen und zu Grundrechtsinnovationen[72] kulminieren können.

S. 9 - HFR 1/2015 S. 9 -

10 **IV. Belastungskumulation von netzbezogenen Eingriffen**

Die horizontale Breitenwirkung von Grundrechten im Internet durch die Addition der beteiligten Grundrechtspositionen wirkt sich insbesondere im Hinblick auf netzbezogene Grundrechtseingriffe aus, die aufgrund ihrer großen Streubreite durchaus zu einer kumulativen Belastungswirkung führen können. Grundrechtsdämpfende und grundrechtsverstärkende Netzeffekte, die durch staatliche, netzbezogene Eingriffe verursacht werden, sind bei der verfassungsrechtlichen Beurteilung von Grundrechtseingriffen maßgeblich anhand des Übermaßverbots gegeneinander abzuwägen.[73] Staatlich veranlasste Eingriffe in die Netzarchitektur, unabhängig davon, ob sie unmittelbar, mittelbar oder auch nur faktisch bewirkt werden, sind daher im Zusammenhang mit der Funktion des Netzes als Grundrechtsvoraussetzung zu sehen. Die dezentrale Netzarchitektur sichert durch ihre steuernden Standards[74] einen Raum grundrechtlicher Entfaltungsmacht, dessen Einschränkung sich nicht nur technisch, sondern auch grundrechtsdämpfend auswirken kann. Die Verengung von Freiheitsräumen und Entfaltungsfreiheit durch staatliche Eingriffe in den elektronischen Kommunikationsfluss – etwa durch massive Eingriffe in den Kommunikationsfluss oder flächendeckende Ausspähung von Kommunikation – ist im Besonderen geeignet, Einschüchterungseffekte (chilling effects[75]) hervorzurufen und die Ausübung grundrechtlicher Freiheiten zu erschweren.[76] Dies gilt vor allem dann, wenn eine Gefährdung der Unbefangenheit des Verhaltens bzw. der Kommunikation und somit der grundrechtlich gewährleisteten Freiheit durch ein "Gefühl des Überwachtwerdens"[77] oder durch die Streubreite eines staatlichen Eingriffs[78] hervorgerufen wird.[79]

11 Die grundrechtliche Entsprechung derartiger – durch moderne Informationstechnologien hervorgerufenen - Gefahrenlagen liegt in einem vorverlagerten Grundrechtsschutz, der in seiner Abwehr- und Schutzfunktion effektiv Grundrechtsgefährdungen abschirmt.[80] Netzbezogene Eingriffe des Staates weisen aufgrund ihrer Reichweite eine neue Qualität und Schlagkraft auf. Die horizontale Belastungswirkung – es ist davon auszugehen, dass netzbezogene Eingriffe grundsätzlich eine Vielzahl von Grundrechtsträgern beeinträchtigen – führt zu einer Belastungskumulation des Eingriffs und somit

---

[72] Hierzu demnächst *Hornung*, Grundrechtsinnovationen, 2015.
[73] Vgl. *Kutzschbach*, Grundrechtsnetze, 2004, S. 152.
[74] Siehe *Lessig*, Code 2.0, 2006, S. 83 ff.
[75] Die Argumentationsfigur wurde ursprünglich vom U.S. Supreme Court (*Dombrowski v. Pfister*, 380 U.S. 479 [1965]) im Rahmen des ersten Verfassungszusatzes entwickelt. Dazu auch *Schauer*, B.U.L. Rev. 58 (1978), 685 ff.; zur Überwachungsproblematik *Richards*, Harv. L. Rev. 126 (2013), 1934 (1949 ff.). Die Rechtsprechung des EGMR und des Bundesverfassungsgerichts hat mittlerweile in der Sache diese Argumentationsfigur rezipiert, ohne jedoch eine dogmatische Einordnung vorzunehmen. In Betracht kommt etwa eine Qualifizierung als Grundrechtseingriff etwa in den Fallgestaltungen des mittelbaren Grundrechtseingriffs oder eine Berücksichtigung im Rahmen der Verhältnismäßigkeitsprüfung im Hinblick auf die objektiv-rechtliche Dimension der Grundrechte, die im Rahmen der Angemessenheit zu berücksichtigen ist. Zunächst wurde diese Argumentationsfigur vor allem im Rahmen der Meinungsfreiheit angewendet und mit der Zeit auch auf andere Kommunikationsfreiheiten ausgedehnt. Die vom Bundesverfassungsgericht verwendete Terminologie ist dabei nicht einheitlich, neben der Bezeichnung ‚Einschüchterungseffekte' wird zum Teil auch das Synonym ‚abschreckende Effekte' verwendet (vgl. etwa BVerfGE 93, 266 [292]; 113, 29 [46]; BVerfGK 9, 62 [77]).
[76] Vgl. BVerfGE 125, 260 (332); *Grabenwarter*, in: Maunz/Dürig (Hrsg.), GG, Stand: 68. Lfg. Januar 2013, Art. 5 Rn. 104; dazu auch *Oermann/Staben*, Der Staat 2013, 630 ff.; *Assion*, in: Telemedicus (Hrsg.), Überwachung und Recht, 2014, S. 31 ff. Siehe etwa zur Gefahr der lähmenden Wirkung auf das Geistesleben durch Kontroll- und Genehmigungsverfahren BVerfGE 33, 52 (72); ferner *Koreng*, Zensur im Internet, 2010, S. 211 ff.
[77] Vgl. BVerfGE 125, 260 (335).
[78] BVerfGE 125, 260 (320 f.).
[79] Zum Panoptismus im Zusammenhang mit transnationalen Überwachungsapparaten *Fischer-Lescano*, JZ 2014, 965 (965 f.) m.w.N.
[80] Vgl. *Lorenz*, in: Pitschas/Uhle (Hrsg.), FS Scholz, 2007, S. 325 (334 ff.); *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 561 (575 ff.).

zu einer Zunahme der Eingriffsintensität. Dies gilt namentlich bei der Absenkung von Eingriffsschwellen und verfahrensrechtlichen Absicherungen, die als Kontrollkorrektiv handhabbare Maßstäbe für eine verhältnismäßige Anwendung von staatlichen Eingriffsgrundlagen bilden sollen.[81] Als besonders eingriffsintensiv sind in diesem Zusammenhang vorverlagerte Präventivmaßnahmen zu bewerten, die von konkreten Gefahrenprognosen losgelöst ein nahezu anlassloses Tätigwerden des Staates ermöglichen.[82]

S. 10

12 ## V. Grundrechte als Ordnungsmaßstab und Absicherung von Freiheitssphären

1) Prüfungsmaßstab

Staatlich veranlasste Eingriffe in den Kommunikationsfluss im dezentralen Informationsnetz des Internets durch Filter- oder Sperrmaßnahmen beeinträchtigen im besonderen Maße die Kommunikationsgrundrechte, die primär durch Nutzer von Kommunikationsdiensten und Inhalteanbietern ihre Betätigung erfahren.[83] Prüfungsmaßstab sind hier zuvörderst die nationalen Verfassungen mit ihren Grundrechtskatalogen. Im Zuständigkeitsbereich der Europäischen Union kommt eine Anwendung der Grundrechtecharta nach Art. 51 GRCh nur in Betracht, wenn Organe, Einrichtungen und sonstigen Stellen der Union handeln oder für die Mitgliedstaaten bei der Durchführung des Rechts der Union. Spätestens seit der Entscheidung Akerberg Fransson des EuGH[84] und der Reaktion des BVerfG im Urteil zum Antiterrordateigesetz[85] ist hierüber ein veritabler Streit entstanden, wie weit dieser Begriff auszulegen ist.[86] Jedenfalls gilt bei rein nationalen Sachverhalten, die nicht durch EU-Recht determiniert sind, unzweifelhaft der Vorrang der nationalen Grundrechtskataloge. Darüber hinaus seien nach Ansicht des EuGH keine Fallgestaltungen denkbar, die vom Unionsrecht erfasst würden, ohne dass [die Charta-]-Grundrechte anwendbar wären. Dies gilt nicht nach der Rechtsprechung des EuGH nicht nur für zwingendes Unionsrecht, sondern auch im Rahmen von Umsetzungsspielräumen.[87] Dies führt letztlich zu einem Überlappungsbereich von Grundrechtsgewährleistungen der Mitgliedstaaten und der Charta, der möglicherweise anhand des Subsidiaritätsgrundsatzes stärker voneinander getrennt werden muss, um mitgliedstaatliche Einflussräume zu sichern.[88] Durch den immer stärker werdenden Bedeutungszuwachs des Unionsrechts auch im digitalen Bereich - vor allem im Privatrecht - ist daher die Frage der Einheit und der Vielfalt des europäischen Grundrechtsschutzes und der damit notwendigen Abgrenzungskriterien weiterhin virulent.

13 Eingriffe in den Kommunikationsfluss bestehen bereits seit Beginn der zivilen Nutzung des Internets. Dem Interesse an der uneingeschränkten Nutzung des Informationsflusses steht ebenso ein stetig wachsendes Interesse gegenüber, das darauf abzielt, den Informationsfluss in „geordnete" Bahnen zu lenken oder soweit dies „erforderlich" erscheint, gänzlich auszutrocknen. Die Evolution der Informationstechnik und immer komplexer werdende Anwendungen und Algorithmen ermöglichen mittlerweile neben dem Zugriff auf Metadaten auch die Überwachung und Kontrolle von Kommunikationsinhalten.[89] Neben direkten Eingriffen in den Kommunikationsfluss, die ihrerseits unmittelbar sichtbar und fühlbar sind, entwickeln sich vermehrt auch indirekte Eingriffe, die

---

[81] Vgl. dazu *Greve/v. Lucius*, DÖV 2012, 97 (100 ff.).
[82] Vgl. etwa zur Vorratsdatenspeicherung BVerfGE 125, 260 ff. und EuGH, EuZW 2014, 459 ff.; sowie zuletzt VerfGH Österreich, Erk. v. 27.6.2014 - G47/2012-49 u.a.
[83] *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 210.
[84] EuGH, NJW 2013, 1415 ff.
[85] BVerfGE 133, 277 (316).
[86] Vgl. hierzu etwa *v. Danwitz*, EuGRZ 2013, 253 ff.; *Kadelbach*, KritV 2013, 276 ff.; *F. Kirchhof*, NVwZ 2014, 1537 ff.; *Klatt*, Die praktische Konkordanz von Kompetenzen, 2014; *Kingreen*, EuR 2013, 446 ff.; *Lange*, NVwZ 2014, 169 ff.; *Ohler*, NVwZ 2013, 1433 ff.; *Scholz*, DVBl. 2014, 197 ff.; *Thym*, NVwZ 2013, 889 ff.
[87] Siehe dazu *Lenaerts*, AnwBl 2014, 772 ff.
[88] Vgl. *Masing*, AnwBl 2014, 786 f.
[89] Siehe dazu *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 134 ff. Die vielfältigen Möglichkeiten von Cyberangriffen sollen an dieser Stelle nicht erörtert werden.

weniger offensichtlich Beschränkungen umsetzen.[90] Aber auch die gezielte Desinformation mit dem Ziel, den Kommunikationsfluss unter Kontrolle zu bringen, ist als ein kommunikationsbeeinträchtigendes Instrument zu qualifizieren.[91]

S. 11 - HFR 1/2015 S. 11 -

14 Netzbezogene Eingriffe in den Informations- und Kommunikationsfluss im Internet finden ihre verfassungsrechtliche Eingrenzung primär durch die Kommunikationsfreiheiten im Internet (Art. 5 Abs. 1 GG) sowie durch die Gewährleistung eines spezifischen digitalen Informations- und Datenschutzes. Die Vertraulichkeit des digitalen Informationsaustausches (Art. 10 Abs. 1 GG), das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) sowie die informationstechnische Ausprägung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)[92] bilden einen sich ergänzenden Schutz. Die Umsetzung netzbezogener Eingriffe wird zumeist auf der Kontrollebene der Internetzugangsanbieter gesetzlich verankert, denn die maßgeblichen Dienstleistungen im Rahmen der Telekommunikation werden von Privaten erbracht, dem Staat kommt lediglich eine Gewährleistungsverantwortung zu (Art. 87f Abs. 2 GG). Es bedarf damit regelmäßig eines kooperativen Zusammenwirkens zwischen Staat und Privaten, das aufgrund der Grundrechtsrelevanz des Eingriffs regelmäßig eine gesetzliche Grundlage voraussetzt. Die Auferlegung von Handlungspflichten, die in der Implementierung und Durchsetzung gesetzlich normierter Kontroll- und Filterpflichten besteht, greift erheblich in die wirtschaftliche Betätigungsfreiheit (Art. 12 GG i.V.m. Art. 3 GG, 14 GG) der Verpflichteten ein.

15 Staatliche Eingriffe in die Internetarchitektur mit dem Ziel der Beschränkung des elektronischen Kommunikationsflusses beeinträchtigen auch immer das Grundrechtsverwirklichungsnetz des Internets. Die Eingriffsintensität wächst dabei proportional mit der Streubreite des Eingriffs und der damit betroffenen Zahl der Grundrechtsträger[93] sowie dem inhärenten Potenzial der Lähmung des Kommunikationsflusses. Netzbezogene Eingriffe, die mit Einschüchterungseffekten verbunden sind, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können, erhöhen die Eingriffsintensität.[94] Hierbei ist durchaus zu beobachten, dass Verfassungsgerichte oder etwa auch der EGMR die Anforderungen an die Rechtfertigung netzbezogener Eingriffe mittlerweile im Rahmen der Verhältnismäßigkeitsprüfung strikt kontrollieren und hierdurch einer Stärkung von Grundrechten im Internet Vorschub leisten.

S. 12 - HFR 1/2015 S. 12 -

16 **2) Zugangssperren**

Staatlich veranlasste Netzeingriffe sind aber nur bedingt einer hinreichenden Skalierbarkeit zugänglich, da aufgrund der komplexen Struktur des Internets punktgenaue Eingriffe schwer umzusetzen sind. In der Praxis hat sich vor allem bei der Umsetzung von Zugangssperren schon mehrmals gezeigt, dass es zu einem Missverhältnis zwischen verfolgtem Zweck und eingesetztem Mittel (Overblocking) kommen kann. Dies liegt umso näher, je weniger und undifferenzierter die Parameter für Umfang und Grenzen des Eingriffs vom Gesetzgeber vorgezeichnet sind und deren Realisierung zusätzlich in die Hände Privater gelegt wurde. Neben staatlich veranlassten Maßnahmen, die auf die Verhinderung der Zugänglichmachung bestimmter Inhalte im Internet abzielen, wird zum Teil auch die totale Kommunikationssperre durch die Sperrung des Internetzugangs als probates Mittel der Rechtsdurchsetzung – vor allem bei der Be-

[90] *Bambauer*, U. Chi. L. Rev. 79 (2012), 863 ff.
[91] Vgl. *Schmalenbach*, NVwZ 2005, 1357 ff.; umfassend *Ingold*, Desinformationsrecht: Verfassungsrechtliche Vorgaben für staatliche Desinformationstätigkeit, 2011.
[92] Vgl. BVerfGE 120, 274 ff.; *Hoffmann-Riem*, JZ 2008, 1009 ff.; *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 34 f.
[93] Vgl. BVerfGE 125, 260 (318 f.).
[94] BVerfGE 120, 378 (402).

kämpfung von Urheberrechtsverletzungen[95] – angesehen. Diese Maßnahme greift tief in elementare grundrechtliche Freiheiten ein und führt in einer digitalen Umwelt zu Ausgrenzungen in nahezu allen Lebensbereichen. Kommunikative Freiheit und Teilhabe sind zentrale Eckpfeiler grundrechtlicher Verwirklichung und besitzen konstituierende Bedeutung für den freiheitlich-demokratischen Staat.[96] Dazu gehört auch, dass der Einzelne die Möglichkeit haben muss, seine Vorstellungen zu verbreiten. Der Ausschluss von den digitalen Kommunikationswegen, die das Internet bietet, würde die Möglichkeit des Verbreitens i. S. v. Art. 5 Abs. 1 S. 1 GG in der heutigen Informationsgesellschaft faktisch unmöglich machen.[97] Überdies gehört es auch zu den elementaren Bedürfnissen des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten.[98] Es handelt sich um eine Freiheit, die zunehmend auf die Nutzung digitaler Quellen angewiesen ist. Mit in den Blick genommen werden sollte in dieser grundrechtlichen Gemengelage auch die grundrechtliche Gewährleistung eines menschenwürdigen Daseins aus Art. 1 Abs. 1 GG i. V. m. Art. 20 Abs. 1 GG, die auch die Teilhabe am gesellschaftlichen, kulturellen und politischen Leben umfasst,[99] die sich aufgrund der tektonischen Verschiebungen von Kommunikationsbeziehungen zunehmend im digitalen Raum des Internets verwirklicht. Letztlich ist damit verfassungsrechtlich vorgezeichnet, dass ein staatlich veranlasster Kommunikationsausschluss aufgrund der erheblichen Eingriffsintensität einer Internetsperre[100] nur in zwingenden Ausnahmefällen zulässig sein kann.

S. 13

17 ## VI. Staatliche Schutzpflichten und die Gewährleistung der Funktionalität grundrechtlicher Wahrnehmung

1) Allgemeines

Grundrechte haben neben ihrer primären Funktion als Abwehrrechte verschiedene Zielrichtungen,[101] die anhand ihrer subjektiv-rechtlichen Grundrechtswirkung und der objektiv-rechtlichen Grundrechtsdimension ausdifferenziert werden.[102] Die objektivrechtliche Funktion der Grundrechte gibt dem Staat u.a. auf, die Funktionalität von Grundrechten zu gewährleisten. Dies gilt vor allem auch dann, wenn Grundrechtsberechtigte auf spezifische Voraussetzungen für die Ausübung grundrechtlicher Freiheit angewiesen sind. Die Nutzung der elektronisch vernetzten Kommunikation des Internets gehört mittlerweile zur kommunikativen Grundversorgung der Bevölkerung,[103] die der Staat im Rahmen seiner verfassungsrechtlich determinierten Gewährleistungsverantwortung (Art. 87 f GG), aber auch in Umsetzung der objektiv-rechtlichen Gehalte der Grundrechte (Art. 5 GG) sowie des Sozialstaatsgebots (Art. 20 Abs. 1 GG) sicherzustellen hat.[104] Dienste und Infrastruktur, die für die Wahrnehmung grundrechtlicher Freiheit im Internet von zentraler Bedeutung sind, bilden die konstitutive Voraussetzung, um grundrechtliche Freiheit zu verwirklichen. Die Ermöglichung des Grundrechtsgebrauchs geht daher mit einer erhöhten Grundrechtspflichtigkeit des Staates einher.[105]

18 Maßnahmen ausländischer Staatsgewalt sind nicht der Grundrechtsbindung des Art. 1 Abs. 3 GG unterworfen, da sich die Bindung nur auf die deutsche Staatsgewalt er-

[95] Siehe auch *Greve/Schärdel*, ZRP 2009, 54 f.; *Schwartmann/Hentsch*, ZUM 2012, 759 ff.
[96] Vgl. BVerfGE 7, 198 (208).
[97] *Greve/Schärdel*, ZRP 2009, 54 (55).
[98] BVerfGE 21, 71 (81).
[99] Vgl. BVerfGE 125, 175 (223).
[100] Ein sog. Kill Switch würde die Eingriffsintensität aufgrund der Anzahl der betroffenen Grundrechtsträger noch potenzieren.
[101] Klassisch sind hier nach *Jellinek* status negativus, status positivus und status activus zu nennen. Siehe dazu *Brugger*, AöR 136 (2011), 1 ff.
[102] Siehe dazu *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 48 Rn. 11 ff.
[103] Vgl. BGH, NJW 2013, 1072 ff.
[104] Vgl. BVerfGE 125, 175 (223).
[105] Siehe zur Frage der Netzneutralität etwa *Greve*, VR 2013, 109 ff.; *Will*, ZVglRWiss 2013, 102 ff.; *Säcker/Mengering*, K&R 2013, 559 ff.

streckt.[106] Die Gewährleistung der grundrechtlich verbürgten Freiheiten ist bei einer Beeinträchtigung durch ausländische Staatsgewalt auf die Umsetzung der grundrechtlich determinierten Schutzpflichten durch die deutsche Staatsgewalt angewiesen. Der Staat muss sich bei Grundrechtsgefährdungen durch Dritte in seiner Funktion als Grundrechtsgarant schützend und fördernd vor das betroffene Grundrechtsgut stellen und kann namentlich durch Gesetz[107], durch Verwaltungsmacht oder durch Gerichtsschutz[108] eine Sicherung der Grundrechte gewährleisten.[109] Im Regelfall steht dem Staat ein weiter Ermessensspielraum hinsichtlich des ob und wie der Ausfüllung grundrechtlicher Schutzpflichten gegenüber fremden Staaten zu.[110] Eine Verpflichtung des Staates Grundrechtsgefährdungen schützend entgegen zu treten besteht insbesondere dann, wenn irreparable Grundrechtsverletzungen drohen oder der Betroffene nicht autonom Selbstschutzmaßnahmen[111] treffen kann.[112] Hierbei ist aber zu beachten, dass die Steuerungswirkung deutscher Grundrechte dann eingeschränkt ist, wenn die zu schützenden Interessen der Grundrechtsträger sich in einem Raum verwirklichen, der von der deutschen Rechtsordnung nicht mit alleinigem Gültigkeitsanspruch beherrscht wird.[113] Die Kollision von Rechtsordnung im Rahmen der grenzüberschreitenden elektronischen Kommunikation kann daher im gewissen Maße zu Abstufungen von Schutzgewährleistungen führen. Trotz des weiten staatlichen Gestaltungs- und Ermessensspielraums wäre aber ein vollständiges Untätigbleiben als Verletzung grundrechtlicher Schutzpflichten zu qualifizieren.

S. 14

19 **2) Ausspähung der Internetkommunikation**

Die flächendeckende Ausspähung der Internetkommunikation durch ausländische Staaten[114] (NSA etc.) dürfte nicht zuletzt die objektiv-rechtliche Grundrechtswirkung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG sowie des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 Var. 3 GG berühren. Der spezifische Gewährleistungsbereich des allgemeinen Persönlichkeitsrechts bezieht sich in besonderem Maße auf den Schutz vor einem heimlichen Zugriff auf informationstechnische Systeme, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können.[115] Neben dem abwehrrechtlichen Gehalt kommt der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eine objektiv-

[106] BVerfGE 1, 10 (11); *Hillgruber*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 21. Ed., Stand: 1.6.2014, Art. 1 Rn. 78.
[107] Auf internationaler Ebene wäre z.B. die Schaffung eines Zusatzprotokolls zum Art. 17 des Uno-Paktes für bürgerliche und politische Rechte – wie derzeit vorgeschlagen – ein gangbarer Weg. Siehe dazu *Piltz*, FAZ v. 31.7.2013, S. 3; ferner *Schiedermaier*, Der Schutz des Privaten als internationales Grundrecht, 2012, S. 72 ff..
[108] Zu möglichen Klagen gegen Internetüberwachungsprogramme der Beitrag von *Kettemann*, abrufbar unter http://www.lto.de/recht/hintergruende/h/eugh-igh-egmr-klagen-gegen-usa-grossbritannien-ueberwachung-prism-tempora/.
[109] Vgl. *Isensee*, in: Isensee/P. Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IX, 3. Auflage 2011, § 191 Rn. 7.
[110] Vgl. BVerfGE 40, 141 (177 f.); 41, 126 (182); 55, 349 (364); *Thiele*, AVR 51 (2013), 1 (9 f.).
[111] Zu denken ist etwa an Maßnahmen im Rahmen der informationellen Selbstverantwortung.
[112] Vgl. *Pieroth/Schlink*, Grundrechte – Staatsrecht II, 28. Auflage 2012, Rn. 114. Die Vernachlässigung der grundrechtlichen Schutzpflicht kann vom Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden (siehe BVerfGE 125, 39 <78> m.w.N.).
[113] BVerfGE 92, 26 (41 f.); *Heil/Greve*, ZD 2013, 481 (486); näher hierzu *Papier*, Gutachtliche Stellungnahme vor dem ersten Untersuchungsausschuss des Deutschen Bundestages der 18. Wahlperiode, Mai 2014, S. 9 f., abrufbar unter https://www.bundestag.de/blob/280842/9f755b0c53866c7a95c38428e262ae98/mat_a_sv-2-2-pdf-data.pdf; ferner *Hoffmann-Riem*, Stellungnahme zur Anhörung des NSA-Untersuchungsauschusses am 22. Mai 2014, Mai 2014, S. 14 ff., abrufbar unter https://www.bundestag.de/blob/280846/04f34c512c86876b06f7c162e673f2db/mat_a_sv-2-1neu--pdf-data.pdf.
[114] Siehe II. 3).
[115] Vgl. BVerfGE 120, 274 (314).

rechtliche Funktion[116] zu, die vor allem in ihrer Schutzpflichtenfunktion den Staat verpflichtet, sich schützend und fördernd vor dieses Rechtsgut zu stellen. Diese sich vor allem an den Gesetzgeber[117] wendende Funktion liegt darin begründet, dass die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erst ihre Wirkungen durch die rechtliche Ordnung entfalten kann, die es dem Einzelnen ermöglicht, von dieser grundrechtlichen Freiheit Gebrauch zu machen.[118] Denn eine Beeinträchtigung informationstechnischer Systeme droht nicht nur von staatlicher Seite, sondern im besonderen Maße aus der Hand Dritter[119], die gezielt versuchen, auf die Integrität und Vertraulichkeit informationstechnischer Systeme störenden Einfluss zu nehmen. Namentlich der Staat ist hinsichtlich dieser Gefahren berufen, in der Ausübung und Umsetzung der an ihn gerichteten Schutzpflicht im gebotenen Maße tätig zu werden. Der durch Art. 10 Abs. 1 Var. 3 GG gewährleistete Schutz der Vertraulichkeit der Kommunikation vermittelt auch in Anbetracht der Überwachungsmaßnahmen ausländischer Gewalten einen Schutzauftrag an den Staat, sich für das Telekommunikationsgeheimnis auf internationaler Ebene einzusetzen.[120] Die Gewährleistung des Telekommunikationsgeheimnisses zielt auf die Abwehr von spezifischen Gefahren für den laufenden Kommunikationsprozess mittels technischer Übertragung an individuelle Empfänger vor einer Kenntnisnahme durch die öffentliche Gewalt.[121] Die massenhafte und flächendeckende Erhebung, Speicherung und Auswertung elektronisch vernetzter Kommunikation durch Dritte nicht grundrechtsgebundene Akteure unterminiert die Vertraulichkeit konkreter Telekommunikationsvorgänge und adressiert an den Staat den Auftrag, Schutz auch insoweit vorzusehen, als dass sich Dritte Zugriff auf die Kommunikation verschaffen.[122] Indes unterliegen derartige Schutzaufträge im internationalen Kontext grundsätzlich begrenzteren Handlungsmöglichkeiten, als dies bei einem rein nationalen Sachverhalt der Fall wäre.

S. 15

20 **3) Grundrechtsgefährdungen im Internet durch Private**

Von einer Grundrechtsbeeinträchtigung ist nur dann auszugehen, wenn der Einwirkende selbst grundrechtsverpflichtet ist. Art. 1 Abs. 3 GG bindet die gesamte öffentliche Gewalt und Private dann, wenn sie sich im Eigentum der öffentlichen Hand befinden,[123] wenn sie mit hoheitlichen Befugnissen beliehen sind[124] oder von der öffentlichen Hand kontrolliert werden.[125] Explizite Ausnahmen von der grundsätzlich fehlenden Grundrechtsbindung Privater ergeben sich lediglich aus Art. 9 Abs. 3 Satz 2 GG[126] und wohl auch aus Art. 1 Abs. 1 Satz 1 GG.[127] Die Grundrechte sind aber nicht nur Abwehrrechte des Einzelnen, sondern zugleich auch konstituierende Elemente einer objektiven Wertordnung, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts

[116] Vgl. *Heckmann*, in: Rüßmann (Hrsg.), FS Käfer, 2009, 129 (136 ff.); *Luch*, MMR 2011, 75 (78); *Karavas*, in: Bieber/Eifert/Groß/ Lamla (Hrsg.), Soziale Netze in der digitalen Welt, 2009, 301 (320 f.); *Gusy/Worms*, APuZ 18–19 / 2009, 26 (32 f.); *Hoffmann-Riem*, AöR 134 (2009), 513 (533); *Petri*, DuD 2008, 443 (446); *Bäcker*, in: Lepper (Hrsg.), Privatsphäre mit System – Datenschutz in einer vernetzten Welt, 2010, 4 (14 ff.).

[117] Vgl. *Hoffmann-Riem*, JZ 2008, 1009 (1013 f.); zum rechtspolitischen Handlungsbedarf *Deiseroth*, ZRP 2013, 194 ff.; siehe auch *Mascolo/Scott*, FAZ v. 24.10.2013, S. 27.

[118] Dazu auch *Hoffmann-Riem*, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014, Mai 2014, S. 16 f.

[119] Dies können Private sein, aber z.B. auch ausländische Staaten.

[120] *Guckelberger*, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), GG, 13. Aufl. 2014, Art. 10 Rn. 31.

[121] BVerfGE 1230, 151 (179).

[122] Vgl. BVerfGE 106, 28 (37).

[123] Vgl. BVerfGE 128, 226 (245); BVerwGE 113, 208 (211); BGHZ 52, 325 (328 ff.); 65, 284 (287); 154, 146 (150); ferner *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 50 Rn. 20 ff.

[124] Vgl. BVerfG, NJW 1987, 2501.

[125] BVerfGE 128, 226 (246 ff.); vgl. dazu auch *Bews/Greve*, Jura 2012, 723 (725); *Greve*, in: Franzius u.a. (Hrsg.), FS Kloepfer, 2013, S. 665 ff.

[126] Vgl. etwa BVerfGE 57, 220 (245); BAGE 19, 217 (223); *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 64 Rn. 44; *Scholz*, in: Maunz/Dürig (Hrsg.), GG, Stand: 35. Lfg. Februar 1999, Art. 9 Rn. 4.

[127] Dazu *Greve*, ZIS 2014, 236 (239 f.) m.w.N.; ferner *Goos*, Innere Freiheit – Eine Rekonstruktion des grundgesetzlichen Würdebegriffs, 2011, S. 168 ff.

gilt.[128]

21 Die Verschiebung von privater Informationsmacht im Internet und die dadurch entstandenen Grundrechtsgefährdungslagen lassen sich angesichts des Gebots einer effektiven Sicherung grundrechtlicher Freiheitssphären[129] dennoch grundrechtlich hinreichend abbilden. So wirken die Grundrechte im Verhältnis zwischen Privaten nicht als stumpfes Schwert, sondern können auch hier eine mäßigende, regulierende Wirkung entfalten. Zuvörderst gilt im Privatverkehr aber die individuelle Selbstbestimmung des Einzelnen, die sich auch in der Freiheit sich zu offenbaren und die eigenen Daten der Kommerzialisierung preiszugeben, niederschlagen kann.[130] Der autonome vertragliche Interessenausgleich ist hinzunehmen und bedarf daher dem Grunde nach keiner staatlichen Korrektur. Ein paternalistischer sich aufdrängender Schutz liefe dieser grundrechtlich abgesicherten Möglichkeit der Freiheitsausübung zuwider. Die Ausstrahlungswirkung und damit die grundrechtliche Determinationskraft intensiviert sich aber in Fällen, in denen der Schutz personaler Freiheit von wirtschaftlicher und sozialer Macht erheblich bedrängt wird oder in denen sich eine krass ungleiche Handlungsmacht abzeichnet, welche die Autonomie des Einzelnen unangemessen begrenzt bzw. Fremdbestimmung Selbstbestimmung ablöst.[131] Die damit einhergehende mittelbare Drittwirkung kann dazu führen, dass Private trotz ihrer Grundrechtsberechtigung ähnlich oder auch genauso weit wie der Staat durch die Grundrechte in Pflicht genommen werden, sofern in tatsächlicher Hinsicht eine vergleichbare Pflichten- oder Garantenstellung besteht.[132] So hat das Bundesverfassungsgericht in seinem obiter dictum in der Fraport-Entscheidung zum Ausdruck gebracht, dass je nach Gewährleistungsinhalt und Fallgestaltung die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates vielmehr nahe oder auch gleichkommen kann.[133] Die zivilrechtliche Gleichordnung der Privatrechtssubjekte wird damit zwar kraft grundrechtlicher Einwirkung durchbrochen, dies findet aber seine Rechtfertigung gerade im Hinblick auf den Schutz hochwertiger Grundrechtsgüter, die in Fallgestaltungen evident ungleicher Verhandlungs- bzw. Machtpositionen nicht verwirklicht werden können.[134] Als eine solche Konstellation kommt nach Auffassung des Bundesverfassungsgerichts die Bereitstellung der Rahmenbedingungen öffentlicher Kommunikation durch private Unternehmen in Betracht, die früher vom Staat erbracht wurde.[135] Dieser Ansatz weist entsprechende Parallelen zur Rechtsprechung des EuGH zur Drittwirkung von Grundfreiheiten auf.[136] Auch hier kann eine Erweiterung des Kreises der Normadressaten bzw. eine verstärkte Verpflichtung aus der wirtschaftlichen und regulierenden Übermacht des Privaten erwachsen, sofern eine Qualifizierung als intermediäre Gewalt möglich erscheint. Die Nutzung der elektronisch vernetzten Kommunikation des Internets gehört mittlerweile zur kommunikativen Grundversorgung der Bevölkerung,[137] die der Staat im Rahmen seiner verfassungsrechtlich determinierten Gewährleistungsverantwortung (Art. 87f GG), aber auch in Umsetzung der objektiv-rechtlichen Gehalte der Grundrechte (Art. 5

[128] BVerfGE 7, 198 (Ls. 1, 205, 215); dazu auch *Rensmann*, Wertordnung und Verfassung , 2007; s. zur Entwicklung auch *Stolleis*, Geschichte des öffentlichen Rechts in Deutschland, Bd. 4, 2012, S. 216 ff. m.w.N.
[129] Vgl. *Bethge*, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte, Bd. III/2, 2009, § 58 Rn. 72, 80 f. m.w.N.; *Degenhart*, in: Scholz/Lorenz/Pestalozza/Kloepfer/Jarass/Degenhart/Lepsius (Hrsg.), Realitätsprägung durch Verfassungsrecht, 2008, S. 89 (91).
[130] Vgl. *Greve*, in: Franzius u.a. (Hrsg.), FS Kloepfer, 2013, S. 665 (672); *Schoch*, in: Sachs/Siekmann (Hrsg.), FS Stern, 2012, S. 1491 (1510).
[131] Vgl. *Jarass/Pieroth*, GG, 13. Aufl. 2014, Art. 1 Rn. 58; *Schoch*, in: Sachs/Siekmann (Hrsg.), FS Stern, 2012, S. 1491 (1511). Dies gilt vor allem in Fällen gestörter Vertragsparität, vgl. BVerfG, MMR 2007, 93 ff.; BVerfGE 89, 214 (232); 103, 89 (101); 114, 73 (90).
[132] BVerfGE 128, 226 (248).
[133] BVerfGE 128, 226 (249); s. auch *Schaefer*, Der Staat 51 (2012), 251 (277); kritisch *Gurlit*, NZG 2012, 249 (251); *Burkiczak*, in: Becker/Lange (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Bd. 3, 2014, S. 115 (134 ff.).
[134] *Greve*, in: Franzius u.a. (Hrsg.), FS Kloepfer, 2013, S. 665 (673).
[135] BVerfGE 128, 226 (249).
[136] Siehe dazu *Kloepfer/Greve*, DVBl 2013, 1148 ff. m.w.N.
[137] Vgl. auch BGH, NJW 2013, 1072 (1074). So hat der Bundesgerichtshof angesichts der Bedeutung der Internetnutzung Schadensersatz für den Ausfall des Internetanschlusses anerkannt.

GG) sowie des Sozialstaatsgebots (Art. 20 Abs. 1 GG) sicherzustellen hat.[138] Dienste und Infrastruktur, die für die Wahrnehmung grundrechtlicher Freiheit im Internet von zentraler Bedeutung sind, bilden die konstitutive Voraussetzung, um grundrechtliche Freiheit zu verwirklichen. Die Ermöglichung des Grundrechtsgebrauchs geht daher mit einer erhöhten Grundrechtspflichtigkeit einher, die zu einer Verstärkung der mittelbaren Drittwirkung der Grundrechte führen kann.[139] Dies gilt namentlich für marktmächtige Unternehmen im Internet, denen aufgrund ihrer faktischen Regelungsmacht[140] ein erhebliches Einwirkungspotenzial auf die Rahmenbedingungen der öffentlichen Kommunikation im Internet zukommt.[141] Sofern die faktische Regelungsmacht unter Umgehung der Selbstbestimmung des Betroffenen genutzt wird, dessen Daten zu verarbeiten, dürfte als ausgleichendes Korrektiv der Gewährleistungsinhalt des Rechts auf informationelle Selbstbestimmung eine verstärkte mittelbare Grundrechtsbindung implizieren. Das regulative Einwirkungspotenzial der grundrechtlichen Steuerungsvorgabe wird daher aller Voraussicht nach erheblich an Bedeutung gewinnen.

S. 16 - HFR 1/2015 S. 16 -

22 ## VII. Netzneutralität[142]

1) Allgemeines

Das Prinzip der Netzneutralität,[143] im weitesten Sinne verstanden als neutrale und diskriminierungsfreie Übermittlung von Datenpaketen ohne Ansehung des jeweiligen Inhalts,[144] hat wichtige Freiräume für Innovationspotenziale und die Gewährleistung kommunikativer Vielfalt im Internet geschaffen.[145] Firmen wie Amazon, Google, Facebook etc. hätten sich ohne diese Voraussetzungen kaum so erfolgreich entwickeln können, wenn die Marktzutrittsschwellen im Internet nicht so niedrig gewesen wären. Die digitale Evolution ist daher im erheblichen Maße abhängig von offenen Strukturen (im Sinne von Interoperabilität und Offenheit der Standards und Schnittstellen),[146] die eine sukzessive Weiterentwicklung erst ermöglichen.

23 ### 2) Netzneutralität als Netzdesignprinzip?

Datenpakete werden grundsätzlich nach dem Best-Effort-Prinzip übermittelt, d. h., es werden gleichermaßen alle Daten mit der jeweils im Netz maximal zu erreichenden Geschwindigkeit übermittelt.[147] Dieses in der Internetarchitektur angelegte Prinzip ist aber

---

[138] Vgl. *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 57 m.w.N.; vgl. auch BVerfGE 125, 175 ff.
[139] Vgl. *Masing*, NJW 2012, 2305 (2308).
[140] Dazu *Hoffmann-Riem*, AöR 137 (2012), 509 (533 ff.).
[141] Vgl. *Masing*, NJW 2012, 2305 (2308).
[142] *Greve*, VR 2013, 109 ff.
[143] Siehe z.B. die Beiträge bei Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011; Spiecker gen. Döhmann/Krämer (Hrsg.), Network Neutrality Open Access, 2011; ferner *Bortnikov*, Netzneutralität und Bedingungen kommunikativer Selbstbestimmung, 2013; *Greve*, VR 2013, 109 ff.; *Jäkel*, Netzneutralität im Internet, 2013; *Martini*, VerwArch 2011, 315 ff.; *Peucker-Minecka*, Netzneutralität als grundrechtliche Gewährleistungspflicht, 2014; *Säcker/Mengering*, K&R 2013, 559 ff.; *Schweitzer/Fetzer*, Wettbewerbsrechtliche Aspekte von Netzneutralität, 2012.
[144] Siehe etwa *Schlauri*, Network Neutrality, 2010, S. 33 ff.; *Kloepfer*, AfP 2010, 120 (122); *Bortnikov*, Netzneutralität und Bedingungen kommunikativer Selbstbestimmung, 2013, S. 33 ff. Der Gesetzgeber hat mit § 41a TKG erste Konturierungsversuche begonnen („...diskriminierungsfreie Datenübermittlung und den diskriminierungsfreien Zugang zu Inhalten und Anwendungen..."). Siehe bereits zur Definition von Netzneutralität *Tim Wu*: „Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are *less* specialized – when they are a platform for multiple uses, present and future", abrufbar unter http://timwu.org/network_neutrality.html.
[145] Dazu etwa die Stellungnahme von *Lawrence Lessig* vor dem US-Senat, abrufbar unter http://commerce.senate.gov/pdf/lessig-020706.pdf#search=%22lessig%20testimony%20network%20neutrality%22; zum Ganzen *van Schewick*, Internet Architecture and Innovation, 2010.
[146] *Lutterbeck*, in: Mehde/Ramsauer/Seckelmann (Hrsg.): Staat, Verwaltung, Information – FS Bull, 2011, S. 1017 ff.
[147] Vgl. *Greve*, in: Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011, S. 13 f.

längst nicht immer die Regel. Die technologische Entwicklung hat es ermöglicht, dass die Netzbetreiber die Header aller Schichten des Netzwerks, d.h. die Quelle, von dem das Datenpaket versandt wird, zu ermitteln sowie auf den Inhalt eines Datenpakets (Deep Packet Inspection[148] - DPI) und damit auf etwaige Individualkommunikation zuzugreifen.[149] Eine qualitative sowie quantitative Vorzugsbehandlung bei der Datenübertragung ist damit ebenso möglich wie die Filterung oder Blockierung unliebsamer Datenpakete.[150] Durch die Umstellung auf das Internetprotokoll Version 6 (IPv6)[151] wird die Priorisierung bestimmter Datenpakete nunmehr auch technisch implementiert, sodass insoweit ein Eingriff in die Netzneutralität stattfindet.[152]

S. 17 - HFR 1/2015 S. 17 -

24 Die Priorisierung von Datenpaketen aus technischen (etwa Netzwerkmanagement) oder aber ökonomischen Gründen (Quality-of-Service) oder anderen Interessen durch invasive Netzwerkeingriffe wie der Deep Packet Inspection führt letztlich zu einer Datendiskriminierung und damit zu einem Eingriff in die Netzneutralität. Durch die Kontrolle des Datenflusses ist es daher möglich, gezielt bestimmte Inhalte, Dienste und Angebote zu blockieren oder ihre Verfügbarkeit einzuschränken. Unbedenklich dürften hier aber Eingriffe sein, die letztlich dazu dienen, die Netzinfrastruktur zu gewährleisten (z.B. Verhinderung eines Datenstaus durch Netzauslastung) oder Schäden von Netznutzern (z.B. Bekämpfung von Schadsoftware) abzuwenden.[153]

25 Die wachsende digitale Abschottung durch geschlossene Systeme kann aber durchaus ein mögliches Resultat sein. Schon jetzt entscheiden große Plattformen darüber, welche Inhalte auf ihnen veröffentlicht werden können und nehmen dabei auch Eingriffe vor, die gesetzlich keineswegs vorgezeichnet sind. Ökonomische Interessen können daher durchaus dazu führen, dass bestimmte Inhalte keine oder nur eine sehr geringe Verbreitung erfahren. Netzwerkmessungen haben ergeben, dass bereits in vielen Ländern Internetprovider massiv in den Datenverkehr der Kunden eingreifen.[154] Aus neueren Untersuchungen wird zudem deutlich, dass vor allem Peer-to-Peer-Netzwerke[155] von Eingriffen in die Netzneutralität betroffen sind.[156] Ebenso finden aber erhebliche Einschränkungen im mobilen Internet statt, man denke nur an die Einschränkungen bei der Nutzung von Smartphones, die jedoch größtenteils durch AGB vertraglich vorgegeben sind.[157] Doch es finden nicht nur Eingriffe aufgrund möglicher Kapazitätsengpässe statt, sondern ebenso inhaltliche Einschränkungen, die mithin also die Kommunikati-

---

[148] Siehe dazu *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 55, 119, 262; *Bedner*, CR 2010, 339 ff.; *Mantz*, MMR 2015, 8 ff.

[149] Vgl. *Bortnikov*, Netzneutralität und Bedingungen kommunikativer Selbstbestimmung, 2013, S. 14 ff., 130 ff. Die Einschränkung der Kommunikationsvertraulichkeit durch DPI dürfte nur schwerlich mit datenschutzrechtlichen Vorgaben zu vereinbaren sein. Siehe auch *Weichert*, in: Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011, S. 141 ff.

[150] *Beckmann/Müller*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, Stand: 29. EL August 2011, Teil 10 Kartellrecht, Rn. 31.

[151] Hinsichtlich des erhöhten Informationspotentials, das eine fest zugewiesene IP-Adresse zu einem Anschlussinhaber mit sich bringt, trifft den Gesetzgeber eine Beobachtungs- und gegebenenfalls auch eine Nachbesserungspflicht, um Gefährdungen des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG grundrechtsschonend abzumildern, vgl. BVerfG, CR 2012, 245 (250).

[152] Vgl. *Federrath*, in: Schaar (Hrsg.), Internetprotokoll Version 6 (IPv6) – Wo bleibt der Datenschutz?, 2012, S. 14 (19)

[153] *Bäcker*, in: Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011, S. 109 (111).

[154] Vgl. die Übersicht auf http://netneutralitymap.org/. Siehe zur Untersuchung auch http://www.mpi-sws.org/~mmarcon/Glasnost-NSDI.pdf.

[155] Unter einem Peer-to-Peer-Netzwerk versteht man ein sich selbst organisierendes System gleichberechtigter, autonomer Einheiten (Peers), das vorzugsweise ohne Nutzung zentraler Dienste auf der Basis eines Rechnernetzes mit dem Ziel der gegenseitigen Nutzung von Ressourcen operiert – kurzum ein System mit vollständig dezentraler Selbstorganisation und Ressourcennutzung. Vgl. *Steinmetz/Wehrle*, Informatik-Spektrum Vol. 27 (2004), 51 (52).

[156] Vgl. http://dpi.ischool.syr.edu/Home.html; http://netzpolitik.org/2012/jetzt-auch-wissenschaftlich-belegt-netzneutralitat-wird-permanent-verletzt/; http://www.erg.eu.int/doc/2012/TMI_press_release.pdf; Netzneutralität: GEREK-Studie zum Einsatz von Traffic-Management in Europa veröffentlicht, MMR-Aktuell 2012, 333008.

[157] Siehe *Schlauri*, in: Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011, S. 153 (168 ff.); *Lapp*, CR 2007, 774 ff.

onsgrundrechte beeinträchtigen.[158]

S. 18

26 **3) Grundrechtliche Anknüpfungspunkte**

Grundrechtstechnisch gesehen ermöglicht das Internet als Grundrechtsverwirklichungsnetz die Grundrechtsinanspruchnahme unterschiedlichster Grundrechtsberechtigter (z.B. Netzbetreiber, Nutzer, Anbieter oder auch Hybridformen) und ist gleichsam als digitaler Freiheitsraum Voraussetzung für vielfältige sich überschneidende und ergänzende Grundrechtsausübung.[159] Insbesondere den Entfaltungsmöglichkeiten und Wirkungschancen der Kommunikationsfreiheiten, die für eine freiheitlich-demokratische Staatsordnung eine schlechthin konstituierende Wirkung besitzen,[160] kommen als grundrechtlichen Steuerungsvorgaben ein erhebliches Gewicht zu. Eine grundrechtsvorgeprägte Verpflichtung zur Netzneutralität lässt sich indessen nicht ableiten. Dennoch verpflichtet die erhöhte Grundrechtspflichtigkeit des Internets den Staat, den Schutz grundrechtlicher Freiheit in seiner objektiv-rechtlichen Funktion gesetzlich auszugestalten, sofern die Marktsteuerungskräfte zu versagen drohen und zu einer unzumutbaren Beeinträchtigung der Wahrnehmungsmöglichkeit vom Kommunikationsverhalten im Internet führen.[161] Die Offenheit des Internets kann in diesem Zusammenhang als Grundrechtsvoraussetzung für die Ausübung grundrechtlicher Freiheiten (vor allem der Kommunikationsfreiheiten) angesehen werden.[162]

27 In Anlehnung an die Rundfunkrechtsprechung des Bundesverfassungsgerichts trifft den Staat eine aus der Medienfreiheit des Art. 5 Abs. 1 Satz 2 GG resultierende Gewährleistungsverantwortung für die Offenhaltung der Meinungspluralität,[163] wobei zu berücksichtigen ist, dass die rundfunkrechtliche Vielfaltsdoktrin nicht ohne weiteres auf das Internet übertragen werden kann.[164] Regulierung bedeutet aber gleichsam eine Begrenzung von Freiheit, weshalb sich die Regulierungsintensität an der Abmessung und Gewichtung der unterschiedlichen Freiheitssphären orientieren muss. Das Maß der erforderlichen Regulierung knüpft dabei an die konkrete Bedrohungslage für die Gewährleistung der Meinungspluralität im Internet an.[165] Vor allem aber die Gefahren privater Inhaltsregulierung im Internet, die das Risiko der Selbstzensur bzw. der Zensur Privater durch Private oder aber über gesetzliche Beschränkungen von Kommunikation hinausgehender Regulierung in sich tragen, dürften überdies geeignet sein, grundrechtliche Schutzpflichten zu aktualisieren.[166] Eine übereilte und nicht auf einer hinreichenden Tatsachengrundlage[167] beruhende Marktregulierung wäre aber ebenso in einem erheblichen Maße freiheitsbeschneidend.[168] Daher dient die Schaffung von Transparenz hinsichtlich des Netzmanagements der Internetprovider – im Vorfeld möglicher regulatorischer Eingriffe – als Mittel selbstregulatorischer Steuerung. So führte etwa die Bundesnetzagentur von Juni bis Dezember 2012 eine Studie zur Dienstqualität von Internet-

[158] Vgl. *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 134 ff.
[159] Vgl. *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 54 ff.; 83 ff.; *Kloepfer*, Grundrechtskonzertierungen, in: Sachs/Siekmann (Hrsg.), Der grundrechtsgeprägte Verfassungsstaat – FS Stern, 2012, S. 405, 423 f.
[160] BVerfGE 7, 198 (208) – Lüth.
[161] *Greve*, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, 2012, S. 84.
[162] Vgl. *Kloepfer*, AfP 2010, 120 (123).
[163] Vgl. *Koreng*, CR 2009, 758 (759); *ders.*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245 (250).
[164] Siehe *Degenhart*, in: Kloepfer (Hrsg.), Netzneutralität in der Informationsgesellschaft, 2011, S. 67, (74 ff.).
[165] Vgl. *Koreng*, CR 2009, 758 (759).
[166] *Fiedler*, Meinungsfreiheit in einer vernetzten Welt, 2002, S. 180 ff.; *Koreng*, Zensur im Internet, 2010, S. 184 ff.; *Peucker-Minecka*, Netzneutralität als grundrechtliche Gewährleistungspflicht, 2014, S. 113 ff.; siehe auch *Schulze-Fielitz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 733 (760).
[167] Vgl. *Kloepfer*, VVDStRL 40 (1982), 63 (90 ff.).
[168] Vgl. auch *Di Fabio*, ZWeR 2007, 266 (272).

zugängen durch.[169] Ähnliche Ansätze werden auch von anderen Regulierungsbehörden verfolgt.[170]

S. 19 - HFR 1/2015 S. 19 -

28 Die Gewährleistung einer ausreichenden Informationsbalance mit dem Ziel der Erhaltung und Sicherung der Kommunikations- und Meinungsvielfalt als demokratiekonstitutives Element[171] dürfte ggf. gesetzgeberische Maßnahmen im Sinne der internetspezifischen Ausgestaltung der Kommunikationsordnung erforderlich machen („Offenheitspflege"). Dies beinhaltet auch, die Bedingungen kommunikativer Selbstentfaltung zu gewährleisten.[172] Netzbezogene Zugangsregeln im Gewande einer wettbewerbsrechtlichen Ausgestaltung können daher durchaus die technologische Konstruktion des Internets als Gemeinschaftsgut und Grundrechtsverwirklichungsnetz sichern.[173]

29 **4) Derzeitige Rechtslage**

In Deutschland hat der Gesetzgeber mit § 41a des Telekommunikationsgesetzes zwar eine Verordnungsermächtigung zur Ausgestaltung der Netzneutralität geschaffen, diese aber bisher nicht ausgefüllt. Die Bundesregierung teilte in diesem Zusammenhang auch erst jüngst mit, dass sie zunächst die EU-Vorgaben[174] für ein offenes Internet abwarten wolle. Das Europaparlament hat am 3.4.2014 mit großer Mehrheit für einen stärkeren Schutz der Netzneutralität gestimmt als vom federführenden Industrieausschuss ursprünglich vorgeschlagen wurde.[175] In der Abstimmung über die von der Kommissarin *Neelie Kroes* vorgelegten Telekommunikationsverordnung verabschiedeten die Abgeordneten Änderungen am bisherigen Entwurfstext. Die Verordnung soll so Drosselungen oder Blockaden des Datenverkehrs im offenen Internet zugunsten von Spezialdiensten verhindern. Nach Angaben von Netzaktivisten lässt sie allerdings offen, welche Anwendungen und Inhalte überhaupt als Spezialdienst angeboten werden dürfen. Damit durchkreuzen die Parlamentarier Vorhaben von Telekommunikationsunternehmen, bestimmte Datenpakete im Internet bevorzugt zu behandeln (Zwei-Klassen-Internet).[176]

S. 20 - HFR 1/2015 S. 20 -

30 Die geplante Verordnung sieht nun vor, dass Internetzugänge im *"Einklang mit dem Grundsatz der Netzneutralität"* zur Verfügung gestellt werden müssen (Artikel 2, Nummer 14). Diese entspricht dem Grundsatz, "dass der gesamte Internetverkehr gleich und ohne Diskriminierung, Einschränkung oder Störung unabhängig von Absender, Empfänger, Art, Inhalt, Gerät, Dienst oder Anwendung behandelt wird". Die Einrichtung von *"Spezialdiensten"* für Fernsehübertragungen, Videokonferenzen und Gesundheitsdiensten in einer *"verbesserten Qualität"* soll weiterhin ermöglicht werden. Diese Dienste sollen über *"logisch getrennte Kapazitäten"* und *"strenge Zugangskontrolle"* verfügen (Artikel 2, Nummer 14). Sie sollen *"durchgehend kontrollierte Quali-*

[169] http://www.initiative-netzqualitaet.de.
[170] Siehe hierzu den Bericht der französischen Regulierungsstelle für Tele- und Postkommunikation (ARCEP), abrufbar unter http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf.
[171] Siehe *Franzius*, N&R 2012, 126 (136); *Koreng*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245 (249 f.).
[172] Dazu *Bortnikov*, Netzneutralität und Bedingungen kommunikativer Selbstbestimmung, 2013.
[173] Vgl. *Wielsch*, Zugangsregeln, 2008, S. 252 f.; *Koreng*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245 (252).
[174] Entwurf einer Verordnung über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents und zur Änderung der Richtlinien 2002/20/EG, 2002/21/EG und 2002/22/EG und der Verordnungen (EG) Nr. 1211/2009 und (EU) Nr. 531/2012, COM(2013) 634 final.
[175] ITRE-Bericht vom 20.03.2014. Siehe hierzu auch *Hullen*, AnwZert ITR 8/2014 Anm. 2.
[176] Die US-amerikanische FCC plant derweil Regelungen zu erlassen, die eine schnellere Beförderung von Inhalten gegen Bezahlung ermöglichen sollen, sodass eine qualitative Unterscheidung von Inhalten vorgenommen werden kann. Siehe http://www.nytimes.com/2014/02/20/business/fcc-to-propose-new-rules-on-open-internet.html?_r=0. Die zuvor erlassenen Regelungen zur Netzneutralität der FCC wurden mangels Rechtsgrundlage jeweils vom United States Court of Appeals for the District of Columbia Circuit gekippt.

tätsmerkmale" gewährleisten, aber *"als Substitut für den Internetzugangsdienst"* weder vermarktet noch genutzt werden können.

31 **VIII. Schluss**

Die eingangs gestellte Frage, ob die Internetregulierung eine Beschränkung oder eine Ermöglichung der Freiheit mit sich bringt, lässt sich nicht in einem abschließenden Gesamturteil bewerten. Staatliche netzbezogene Eingriffe können zu spürbaren Grundrechtsbeeinträchtigungen führen, sie können aber auch grundrechtliche Freiheit ermöglichen, indem sie einen notwendigen Ordnungsrahmen schaffen oder im Rahmen der staatlichen Schutzpflicht, die Freiheit des Einzelnen absichern. Internetregulierung wird bestimmt auf mehreren Ebenen und von verschiedenen Akteuren. Auf internationaler Ebene können bestimmte allgemeinverbindliche Standards etwa durch internationale Organisationen vereinbart werden. Der Weg zu einem Internetvölkerrecht erscheint eher langwierig, da insbesondere der Konsens zu einheitlichen Grundrechtsstandards im Netz derzeit nicht auf einem hohen Niveau zu erreichen bzw. durchzusetzen ist.[177] Impulse gehen auch von der Unionsebene aus, dies betrifft aktuell z.B. die Gewährleistung von Netzneutralität. Die Entwicklung zu einer Renationalisierung des Internets hat mittlerweile dazu geführt, dass Nationalstaaten ihre Kontroll- und Einwirkungsmaßnahmen sukzessive ausbauen, sodass erhebliche Auswirkungen der Internetregulierung auf dieser Ebene zu verzeichnen sind. Der Schutz der Freiheit im Internet wird in diesem Zusammenspiel am effektivsten durch die Grundrechte gewährleistet. Hierbei kommt der Abmessung grundrechtlicher Freiheit im Internet aufgrund veränderter Gefährdungslagen entscheidende Bedeutung zu.

Zitierempfehlung: Holger Greve, HFR 2015, S. 1 ff.

[177] Exemplarisch hierzu die Sachverständigenstellungnahmen für den NSA-Untersuchungsausschuss des Deutschen Bundestages von *Aust* und *Talmon*, abrufbar unter https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848. Zur Zukunft des Internetvölkerrechts siehe einerseits http://voelkerrechtsblog.com/2014/05/02/grotius-goes-google/ und andererseits http://voelkerrechtsblog.com/2014/05/05/grotius-has-a-long-way-to-go/.