Schriftenreihe des Instituts für Rundfunkrecht an der Universität zu Köln 109

Netzneutralität und Bedingungen kommunikativer Selbstbestimmung

Pflichten des freiheitlichen Verfassungsstaates zur Gewährleistung der Neutralität des Internets im Lichte der grundrechtlichen Schutzpflichtenlehre

von
Vyacheslav Bortnikov

1. Auflage

Thematische Gliederung:

Medien-, Presse- und Rundfunkrecht

Verlag C.H. Beck München 2013

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 65728 3

Inhaltsverzeichnis: Netzneutralität und Bedingungen kommunikativer Selbstbestimmung – Bortnikov

eingriffsausschließenden Grundrechtsverzicht impliziert[885]. In einem solchen Fall entfiele folglich auch eine eingriffsadäquate Beeinträchtigung des Art. 10 Abs. 1 GG und damit auch die staatliche Schutzpflicht[886].

An der „Einwilligungslösung" lassen sich jedoch Bedenken anmelden.

Neben einem in großen Teilen der Bevölkerung fehlenden Datenschutzbewusstsein und einer wenig ausgeprägten Sensibilität vieler Menschen für Datenschutzfragen[887] kann man sich der Tatsache nicht verschließen, dass die Entscheidung für den einen oder anderen Netzbetreiber in praxi durch einige andere Faktoren – wie die örtliche Verfügbarkeit, die Preisgünstigkeit oder die Qualität der Dienstleistung – determiniert wird[888].

Aufgrund der vielen Vorteile, die DPI bietet[889], ist darüber hinaus zumindest eine weit verbreitete Anwendung dieser Technologie zu erwarten. Unter diesen Umständen besteht für den Einzelnen die naheliegendste Alternative zur Einwilligung in die tiefgreifende Analyse und gegebenenfalls Sperrung seiner Datenpakete im Zweifelsfall darin, teurere Dienstleistungen in Anspruch zu nehmen oder die Inanspruchnahme des Internets gar zu unterlassen. Im Hinblick auf die zentrale Bedeutung des Internets für den individuellen und öffentlichen Meinungsbildungsprozess[890] bzw. angesichts seiner praktischen Unentbehrlichkeit in der heutigen Gesellschaft[891] ist dies wenig befriedigend[892].

Ob die Einwilligungslösung zum Schutz des Fernmeldegeheimnisses der User genauso geeignet ist wie ein Verbot von DPI, muss daher mit einem deutlichen Fragezeichen versehen werden.

c) Angemessenheit

Um die Angemessenheit eines Verbotes beurteilen zu können, muss die Intensität der dadurch verursachten Beeinträchtigung der Wirtschaftsfreiheiten der Netzbetreiber ins Verhältnis zu der Intensität der Beeinträchtigung des Fernmeldegeheimnisses gestellt werden.

---

[885] *Sachs*, in: Sachs (Hrsg.), GG, Vor Art. 1 Rn. 54 ff.; *Bethge*, in: Isensee/Kirchhof (Hrsg.), HStR IX, § 203 Rn. 125.

[886] Zur Wirkung des Grundrechtsverzichts aus Sicht der Schutzpflichtenlehre *Fischinger*, JuS 2007, 808 (812 f.).

[887] *Bull*, NVwZ 2011, 257 (259).

[888] Kap. 4, B, I, 1., b), bb), (3), (c), (aa) m. w. N. in Fn. 597.

[889] Dazu sogleich unter Kap. 4, C, II, 2.

[890] Kap. 3, C, I, 2., a).

[891] Statt vieler *Eberle*, in: Festschrift Bull, S. 979 (979).

[892] *Härting*, BB 2010, 839 (841); *Härting*, Internetrecht, Rn. 52.

Wie intensiv die Privatsphäre durch eine Maßnahme im Einzelfall berührt wird, hängt von der Art der betroffenen Daten – vor allem vom Grad ihrer Persönlichkeitsrelevanz –, von ihrem Umfang, denkbaren Verwendungsmöglichkeiten und der Gefahr ihres Missbrauchs ab[893].

Insofern ist festzustellen, dass die DPI-Analyse sich auf sämtliche Datenpakete erstreckt, die zwischen Clients und Servern sowie zwischen Clients untereinander ausgetauscht werden. Betroffen sind dabei nicht nur die Verkehrsdaten, sondern auch und gerade die Nutzdaten[894]. Dass DPI die Erstellung von Persönlichkeits- und Nutzungsprofilen ermöglicht[895] und mitunter den Kernbereich privater Lebensgestaltung betreffen kann, liegt vor diesem Hintergrund auf der Hand. Die große Streubreite und die Aussagekraft der betroffenen Daten begründet die Gefahr einer schweren Beeinträchtigung des Art. 10 Abs. 1 GG[896]. Die Tatsache, dass DPI vielfältige Verwendungs- und Missbrauchsmöglichkeiten eröffnet[897], erhöht zusätzlich die Intensität der Beeinträchtigung[898].

Demgegenüber stehen hinter dem Einsatz von DPI gewichtige Belange der Netzwerksicherheit. Angriffe aus dem Internet können nicht nur die technische Funktionsfähigkeit des Netzwerks zunichtemachen und enorme (volks-)wirtschaftliche Schäden hervorrufen[899], sondern auch das hier in Rede stehende Vertrauen der Nutzer in die Vertraulichkeit der Internet-Kommunikation zerrütten[900]. Der Werkzeugkasten moderner Hacker bietet eine Auswahl an Angriffstools an, mit denen persönliche Daten der Nutzer ausgespäht, abgefangen oder manipuliert werden können. Man denke nur an Trojaner, Keylogger oder Sniffer – um einige Beispiele zu nennen[901]. Solchen Bedrohungen kann etwa durch den Einsatz von Paketfiltern oder Stateful Packet Inspection, die über die Analyse von Schicht 4 im OSI-Referenzmodell nicht hinausgehen[902], nicht wirksam begegnet werden. Die meisten Angriffe finden heutzutage auf der Applikationsebene statt[903] und sind somit im Rahmen einer einfachen – weniger tiefgehenden – Packet Inspection nicht identifizier-

[893] BVerfGE 65, 1 (45 f.); BVerfG, NJW 2008, 1505 (1507 f.) m. w. N.
[894] Kap. 1, C, IV m. w. N. in Fn. 96.
[895] *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", S. 2.
[896] BVerfGE 125, 260 (318 ff.) (im Zusammenhang mit der „Vorratsdatenspeicherung").
[897] *Bedner*, CR 2010, 339 (340).
[898] In einer ähnlichen Konstellation BVerfGE 125, 260 (320).
[899] Kap. 4, B, I, 2., b).
[900] Die Bedeutung des technischen Datenschutzes hervorhebend auch *Härting*, BB 2010, 839 (842).
[901] Ausführlich dazu *Winterer*, Windows 7 Sicherheit, S. 145 ff., 169 ff., 237 ff.
[902] Kap. 1, C, IV, 1., a) und b).
[903] *Koch*, Systemarchitektur, S. 158; *Jarzyna*, IPv6 – Das Praxisbuch, S. 226.

bar[904]. Damit gewährleisten anwendungsorientierte Sicherheitssysteme die höchste Sicherheit[905]. Die Verweisung der Netzbetreiber auf ineffektive und unzeitgemäße Schutzmechanismen würde den Angreifern und damit der Nutzerverunsicherung Tür und Tor öffnen. Der Einsatz von DPI zum Zweck der Netzwerksicherheit ist deshalb unabdingbar[906].

Hinzu kommt noch, dass DPI an sich nicht auf die Erhebung oder sonstige Nutzung der betroffenen Daten angelegt ist. Die mit DPI in Zusammenhang gebrachten Begehrlichkeiten der Netzbetreiber, die Daten anderweitig zu nutzen, tragen potentiellen Charakter und können durch eine enge und konkrete Zweckbindung unter Androhung von Sanktionen für Zuwiderhandeln wirksam begrenzt werden. Gegen reale Bedrohungen aus dem Internet[907] kann die Vertraulichkeit der internetbasierten Kommunikation hingegen schwerlich mit rechtlichen Instrumentarien abgesichert werden. Ohne etablierte Telekommunikationsunternehmen in eine Kategorie mit „Black Hat Hackern“[908] stellen zu wollen, drängt sich die folgende Feststellung auf: Eine *potentielle* Gefahr der Zweckentfremdung der DPI-Technologie durch Netzbetreiber ist das deutlich kleinere Übel gegenüber den *realen* Gefahren der Datenspionage und Sabotage durch technikaffine kriminelle Elemente und muss deshalb hingenommen werden.

d) Ergebnis zu 1.

Nach Abwägung der beteiligten Interessen kann ein striktes Verbot der Sperrung vireninfizierter Datenpakete mittels DPI-Technik nicht gerechtfertigt werden.

2. Verbot des Einsatzes von DPI zwecks Sperrung von VoIP-Diensten in Mobilfunknetzen und zum Zweck des Netzwerkmanagements

Zu prüfen bleibt, ob ein Verbot, die DPI-Technologie zum Zweck der Sperrung von VoIP-Diensten in Mobilfunknetzen und aus Gründen des Netzwerkmanagements einzusetzen, einer Abwägung mit den Wirtschaftsgrundrechten der Netzbetreiber standhält.

Fraglich ist dabei allein die Angemessenheit eines solchen Verbotes.

---

[904] *Koch*, Systemarchitektur, S. 158.

[905] *Meyers/Harris*, CISSP, S. 226 (zu anwendungsorientierten Proxy-Firewalls); *Kammermann/a Campo*, CompTIA Security+, S. 260 (Application Level Gateway).

[906] *Ergen*, Mobile Broadband, S. 81.

[907] So in Bezug auf unterschiedliche Bedrohungslagen auch *Winterer*, Windows 7 Sicherheit, S. 25, 26, 100, 141, 174.

[908] Unter diesen Begriff werden Hacker gefasst, die mit krimineller Energie handeln und einen direkten oder indirekten Bezug zu Computerkriminalität aufweisen, *Winterer*, Windows 7 Sicherheit, S. 44.

Das Interesse der Netzbetreiber an dem Einsatz von DPI resultiert hier aus der Möglichkeit, mittels Orientierung an der Anwendungsschicht den Netzwerkverkehr zu optimieren[909]. Auf diese Weise lässt sich die physische Funktions- und Leistungsfähigkeit des Netzwerks erhalten respektive steigern, ohne die Netzwerkressourcen übermäßig erweitern und ausbauen zu müssen[910]. Dasselbe gilt für die Verhinderung der kostenlosen Nutzung von VoIP-Diensten in Mobilfunknetzen.

Die Gewichtigkeit des Interesses der Netzbetreiber am Einsatz der DPI-Technologie wird dabei, wenn überhaupt, so doch nur unerheblich dadurch gesenkt, dass ein Netzwerkmanagement grundsätzlich auch mit anderen Mechanismen betrieben werden kann[911]. Zwar lässt sich eine Priorisierung von Datenpaketen durch Bildung von bestimmten Service-Klassen oder durch individuelle Behandlung von Verkehrsflüssen auch ohne Zugriff auf die Anwendungsschicht bewerkstelligen. Im Hinblick auf ganz unterschiedliche Verkehrsgüteanforderungen bleibt es aber doch wichtig, die Datenpakete für die in Frage kommende Service-Klasse oder Gruppe von Datenpaketen adäquat und zu der jeweiligen Applikation passend zu sortieren[912].

Beispielsweise erweist sich die ehedem praktizierte Verkehrssteuerung anhand der Port-Nummer, mit der theoretisch auch der Zugang zu VoIP verhindert werden kann, heutzutage als obsolet[913]. Denn viele neuere Applikationen nutzen keine statisch vergebenen Port-Nummern mehr[914]. Vielmehr können Internet-Dienste auf jedem möglichen Port ausgeführt werden, der – auch von Nutzern – ständig dynamisch geändert werden kann[915]. Gewisse Peer-to-Peer-Applikationen – wie VoIP – können nur unter Zuhilfenahme von DPI zuverlässig als solche identifiziert werden[916].

---

[909] *Fritsch*, Linux-Magazin Online, S. 1, abrufbar unter: http://www.linux-magazin.de/Heft-Abo/Ausgaben/2005/02/Verkehrsplanung (zuletzt abgerufen am 8.9.2012).

[910] *Berger-Kögler/Kind*, N&R Beilage 4/2010, 1 (6); *Martini*, Speyerer Vorträge, Heft Nr. 96, S. 10 f.

[911] Kap. 1, C, IV, 2., b), aa) und bb) (zum DiffServ-Modell und MPLS).

[912] *Fritsch*, Linux-Magazin Online, S. 1 f., abrufbar unter: http://www.linux-magazin.de/Heft-Abo/Ausgaben/2005/02/Verkehrsplanung (zuletzt abgerufen am 8.9.2012); *Mochalski/Schulze*, Deep Packet Inspection, S. 4 betonend: "For this classification to work reliably, DPI is a necessity".

[913] *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", S. 10.

[914] *Mochalski/Schulze*, Deep Packet Inspection, S. 4; *Koch*, Systemarchitektur, S. 159; *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", S. 10.

[915] *Mochalski/Schulze*, Deep Packet Inspection, S. 4; *Bedner*, Rechtmäßigkeit der „Deep Packet Inspection", S. 10.

[916] *Evans/Filsfils*, Deploying IP and MPLS QOS for Multiservice Networks, S. 96; *Ergen*, Mobile Broadband, S. 81 f.

Aufgrund der mit DPI möglichen feineren Klassifizierung bzw. Granulierung werden die Telekommunikationsunternehmen in die Lage versetzt, ein größeres und flexibleres Portfolio an Dienstleistungen anzubieten[917].

Zwar bergen die Möglichkeiten von DPI ein erhebliches Missbrauchspotential[918], welches bereits durch die Installation der entsprechenden Soft- und Hardware entfesselt wird[919]. Jedoch rührt die Gefahr der missbräuchlichen Verwendung von DPI bereits aus der notwendigen Zulassung dieser Technologie im Bereich der Netzwerksicherheit her. Insofern begründet die Nutzung der – ohnehin bereits installierten – DPI-Systeme zum Zweck der Priorisierung von Datenpaketen oder Sperrung von VoIP-Diensten in Mobilfunknetzen kein eigenständiges Missbrauchspotential[920], das sich im Wege eines dagegen gerichteten partiellen Verbotes eliminieren ließe. Mit einem ausdrücklichen Verbot *missbräuchlicher* Verwendung der DPI-Technik lässt sich die an sich bestehende Missbrauchsgefahr hinreichend eindämmen.

Wer sich nicht den Vorwurf der Innovations- und Technikfeindlichkeit eintragen möchte, muss – zusätzlich zu den wirtschaftlichen Interessen der Netzbetreiber – auch von den innovativen Potenzen der DPI-Technologie Notiz nehmen. Eins der innovativen Anwendungsfelder der DPI-Technik ist – um nur ein Beispiel unter vielen herauszugreifen – die Entwicklung von Mechanismen zur Inhalte-Identifizierung[921], womit den Belangen der Urheber – eventuell de lege ferenda – zur Durchsetzung verholfen und einer der Herausforderungen der neueren Zeit entgegengetreten werden kann.

Der zarte Spross der DPI-Technologie, die zu Recht als eine „Technologie der Zukunft“ genannt wird[922], wurde bereits durch die Diskussion um die Netzneutralität in seinem Wachstum gebremst[923]. Durch eine – auch nur teilweise – Missbilligung durch den Staat droht jegliche Forschungsaktivität auf dem Gebiet der innovativen Netzwerkverkehrssteuerung zu ersticken.

Alles in allem kann festgestellt werden: Die Nachteile eines gesetzlichen Verbotes der anwendungsorientierten Priorisierung von Datenpa-

---

[917] *Bachmutsky*, Telecommunication Gateways, S. 163 mit Beispielen.

[918] Kap. 4, C, II, 1., c).

[919] *Koreng*, Zensur im Internet, S. 181 m. w. N., konstatiert die Gefahr, „[…] durch die Installation von Filtermechanismen gleichsam die `Büchse der Pandora` zu öffnen […]“.

[920] Ähnlich argumentiert *Losch*, Wissenschaftsfreiheit, S. 342 f. im Zusammenhang mit der Zulassung der künstlichen Befruchtung.

[921] In Bezug auf “Google YouTube Video Identification”, *Bachmutsky*, Telecommunication Gateways, S. 163.

[922] *Ufer*, K&R 2010, 383 (386).

[923] *Bachmutsky*, Telecommunication Gateways, S. 163 f.

keten und der Sperrung von VoIP überwiegen die damit einhergehende Beeinträchtigung des Fernmeldegeheimnisses.

Ein Verbot des Einsatzes von DPI ist mit den Grundrechten der Netzbetreiber nicht zu vereinbaren.

III. Maßnahmen zum Schutz der Vertraulichkeit der Internet-Kommunikation

Die Verfassungsmäßigkeit eines Informationseingriffs kann nur im Hinblick auf den damit konkret verfolgten Zweck beurteilt werden[924]. Um zu gewährleisten, dass die betroffenen Daten nur zu solchen Zwecken verwendet werden, die die Schwere der damit verbundenen Beeinträchtigung auch rechtfertigen, dürfen Informationseingriffe nach gefestigter Rechtsprechung des Bundesverfassungsgerichts nur zu bestimmten, bereichsspezifischen, präzise und normenklar festgelegten Zwecken vorgenommen werden[925].

Diese Rechtsprechung lässt sich ohne Weiteres auf Schutzpflichtkonstellationen wie die vorliegende ummünzen[926]. Zwecke der hier interessierenden Datenverwendung sind die der Netzwerksicherheit und des Netzwerkmanagements. Als Ergebnis der vorangegangenen Abwägung der beteiligten Interessen ist der Vorteil der Anwendung der DPI-Technologie höher zu veranschlagen als der zu erwartende Schaden. Dieses Ergebnis ist allerdings nur tragfähig, wenn der Einsatz von DPI durch eine gesetzliche Zweckbindung begrenzt wird. Der Gefahr des Missbrauchs muss durch Weitergabe- und Verwertungsverbote Einhalt geboten werden[927].

IV. Ergebnis zu C

Die dem Staat durch Art. 10 Abs. 1 GG auferlegte Abwägung zwischen Risiko und Nutzen von DPI fällt – unter der Voraussetzung einer engen gesetzlichen Zweckbindung – zugunsten des letzteren aus. Die Anwendung der DPI-Technologie zu Zwecken der Netzwerksicherheit und des Netzwerkmanagements ist deshalb zuzulassen.

---

[924] BVerfGE 125, 260 (345).

[925] BVerfG, NJW 2000, 55 (57); BVerfGE 125, 260 (315, 328, 345).

[926] Zur Anwendung der Prinzipien der Zweckbindung und der Normenklarheit auf den privatwirtschaftlichen Bereich *Welp*, Die Auskunftspflicht von Access-Providern, S. 267 f. m. w. N.

[927] So BVerfGE 65, 1 (46), 84, 239 (280) (in Bezug auf die Gefahren automatischer Datenverarbeitung).

5. Kapitel. Kontrolle der Erfüllung grundrechtlicher Schutzpflichten zugunsten der Netzneutralität anhand des Untermaßverbotes

Es wurde schon ausgeführt[928], dass das Untermaßverbot einen Maßstab für die Frage der Verletzung staatlicher Schutzpflichten bildet.

A. Untermaßverbot und seine Operationalisierung

Ungeachtet der – insbesondere vom Schrifttum[929] geleisteten – dogmatischen Aufbereitung des Untermaßverbotes kann der Gehalt dieser Rechtsfigur mitnichten als geklärt angesehen werden[930].

I. Das Untermaßverbot in der Rechtsprechung des Bundesverfassungsgerichts

Den neuralgischen Punkt bildet dabei die Grenzziehung zwischen den gesetzgeberischen und den verfassungsgerichtlichen Befugnissen[931]. Die Maxime, dass es der Judikatur von Verfassungs wegen verwehrt ist, sich die Befugnisse des Parlaments anzumaßen, durchzieht seit jeher die Rechtsprechung des Bundesverfassungsgerichts[932]. Diese demokratiestaatlich unterlegte Zurückhaltung darf indes nicht dahingehend missverstanden werden, als hätte der Gesetzgeber bei der Ausformung der Gesellschaftsordnung ganz freie Hand. Vielmehr tritt der Gedanke der legislativen Gestaltungsfreiheit in ein Spannungsverhältnis zu dem Prinzip des Verfassungsstaates[933], dessen Aufgabe es ist, die politische Macht in normativ geordnete Bahnen zu lenken[934]. Namentlich entspricht es der Funktion des Bundesverfassungsgerichts, die Staatsleitung

---

[928] Kap. 4, A, II.

[929] Siehe insbes. *Hain*, DVBl. 1993, 982 (982 ff.); *Hain*, ZG 1996, 75 (75 ff.); ausführlich dazu die Monographie von *Störring*, Das Untermaßverbot in der Diskussion.

[930] *Stern*, DÖV 2010, 241 (247).

[931] *Klein*, JuS 2006, 960 (961); *Stern*, DÖV 2010, 241 (247).

[932] *Laufer*, Verfassungsgerichtsbarkeit und politischer Prozess, S. 369 ff.

[933] *Meßerschmidt*, Gesetzgebungsermessen, S. 427 f.; sieh auch *Klein*, JuS 2006, 960 (961).

[934] *Sobota*, Das Prinzip Rechtsstaat, S. 27.

in die verfassungsrechtlichen Schranken zu weisen, wiewohl die Abgrenzung zwischen Verfassungsauslegung und Politik nicht einfach zu treffen ist[935].

Im Zusammenhang mit grundrechtlichen Schutzpflichten stellt sich speziell das Problem, dass die Verfassung lediglich das Ziel staatlicher Schutzaktivitäten vorgibt, nicht jedoch die Art und den Umfang des gebotenen Schutzes[936]. Wie das Bundesverfassungsgericht ausdrücklich feststellt, ist es Sache des Gesetzgebers, ein Schutzkonzept zu entwickeln und es normativ umzusetzen[937]. Das Untermaßverbot determiniert dabei eine Grenze des grundsätzlich weiten gesetzgeberischen „Einschätzungs-, Wertungs- und Gestaltungsspielraums“[938], der durch die – jeweils begründungsbedürftige[939] – Reduzierung der gerichtlichen Kontrolldichte gewahrt werden muss[940].

Daher beschränkt sich die Verfassungsrechtsprechung regelmäßig auf eine bloße Evidenzkontrolle[941]. Die untere Grenze des gesetzgeberischen Spielraums ist demnach erreicht, wenn „Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben“[942].

Bei Gefährdung bzw. Verletzung höherwertiger Schutzgüter wird allerdings über die Evidenzkontrolle hinaus gefordert, dass die vom Gesetzgeber getroffenen Maßnahmen „für einen angemessenen und wirksamen Schutz ausreichend“[943] sind.

---

[935] *Hain*, DVBl. 1993, 982 (984); *Störring*, Das Untermaßverbot in der Diskussion, S. 58; *Wolff*, NVwZ 2010, 751 (752) m. w. N.

[936] BVerfGE 88, 203 (254); *Gellermann*, Grundrechte in einfachgesetzlichem Gewande, S. 237 f.; *Klein*, JuS 2006, 960 (960 f.); *Nettesheim*, VVdStRL 70 (2011), 7 (40).

[937] BVerfGE 88, 203 (261); 96, 56 (64); 125, 39 (78); BVerfG, NJW 2010, 1943 (1944).

[938] BVerfGE 77, 170 (214 f.); 96, 56 (64); 125, 39 (78); BVerfG, NVwZ 2011, 991 (993).

[939] Im Hinblick auf die Kontrollbefugnis bzw. -funktion des BVerfG verdient *Störring*, Das Untermaßverbot in der Diskussion, S. 60 Zustimmung, wenn er ausführt, dass eine eingeschränkte Justitiabilität inhaltlich begründet werden muss.

[940] *Klein*, JuS 2006, 960 (962).

[941] *Klein*, JuS 2006, 960 (961); *Stern*, DÖV 2010, 241 (247 f.).

[942] BVerfGE 125, 39 (78 f.); siehe auch BVerfG, NVwZ 2010, 702 (703, 704); NVwZ 2011, 991 (994).

[943] BVerfGE 88, 203 (254).