

Zeitschrift für
Informations-,
Telekommunikations-
und Medienrecht

MMR

MultiMedia und Recht

4/2003

Beilage

HERAUSGEBER

Dietrich Beese, Geschäftsführer Corporate Affairs, O₂ Germany GmbH & Co oHG, München – **Dorothee Belz**, Kaufmännische Geschäftsführerin, BetaResearch GmbH, Ismaning – **Dr. Michael Bertrams**, Präsident VerfGH und OVG für das Land Nordrhein-Westfalen, Münster – **Dr. Herbert Burkert**, Wiss. Mitarbeiter GMD, St. Augustin – RA **Dr. Oliver Castendyk**, Erich Pommer Institut, Potsdam – **Jürgen Doetz**, Vorstand ProSieben SAT1 Media AG/Präsident Verband Privater Rundfunk und Telekommunikation e.V. (VPRT), Berlin – **Prof. Dr. Carl-Eugen Eberle**, Justitiar ZDF, Mainz – **Erich Gahrau**, Justitiar Bertelsmann AG, Gütersloh – **Hans-Willi Hefekäuser**, Leiter des Zentralbereichs Ordnungs- und Wettbewerbspolitik, Deutsche Telekom, Bonn – **Prof. Dr. Thomas Hoeren**, Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Bernd Holznapel**, Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Günter Knieps**, Direktor des Instituts für Verkehrswissenschaft und Regionalpolitik, Universität Freiburg – **Christopher Kuner J.D.**, LL.M., Attorney at Law, Hunton & Williams, Brüssel – **Matthias Kurth**, Präsident der Regulierungsbehörde für Telekommunikation und Post, Bonn – **Prof. Dr. Wernhard Möschel**, Vorsitzender des Wissenschaftlichen Beirats beim BMWi/Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Universität Tübingen – **Prof. Dr. Christoph Paulus**, Humboldt Universität zu Berlin – **Dr. Bernd Pill**, Leiter Recht und Regulierung Vodafone D2 GmbH, Düsseldorf – **Robert Queck**, Maître de Conférences, Centre de Recherches Informatique et Droit (CRID), Universität Namur, Belgien – RA **Prof. Dr. Peter Raue**, Hogan & Hartson Raue L.L.P. Berlin – RA **Dr. Wolfgang von Reinersdorff**, Justitiar Verband Privater Kabelnetzbetreiber e.V. (ANGA), Bonn/Heuking Kühn Lüer Wojtek, Hamburg – **Min.Dir. Dr. Eike Röhlings**, Leiter der Abt. IV – Technologie- und Innovationspolitik; Neue Bundesländer, BMWi, Berlin – **Prof. Dr. Alexander Roßnagel**, Universität GH Kassel/wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken – RA **Prof. Dr. Joachim Scherer**, Döser Amereller Noack/Baker & McKenzie, Frankfurt a.M. – **Prof. Dr. Gerhard Schricker**, Direktor des Max-Planck-Instituts für ausländisches und internationales Patent-, Urheber- und Wettbewerbsrecht, München – RA **Dr. Raimund Schütz**, Freshfields Bruckhaus Deringer, Düsseldorf – **Prof. Dr. Ulrich Sieber**, Universität München – **Prof. Dr. Gerald Spindler**, Universität Göttingen – RA **Dr. Arthur Waldenberger**, LL.M., Verband Deutscher Zeitschriftenverleger, Leitung Europaangelegenheiten und Medien, Berlin

REDAKTION

Anke Zimmer-Helfrich, Chefredakteurin –
RAin **Ruth Schrödl**, Redakteurin –
Marianne Gerstmeyer, Redaktionsassistentin
Wilhelmstr. 9, 80801 München

EDITORIAL

CHRISTOPH ENGEL

Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden

Eine Kritik an den Verfügungen der Bezirksregierung Düsseldorf

Keine Nazipropaganda auf deutschen Bildschirmen – so stellt der Düsseldorfer Regierungspräsident sein Anliegen dar. Wider die Globalisierung der Kommunikation – darum geht es wirklich. Und im nächsten Schritt geht es um Strukturveränderungen des Internet. Aus freier soll lückenlos zensierte Kommunikation werden. Die deutschen Access-Provider sollen zu Zensoren wider Willen werden.

Dieses Ansinnen bricht sich an einer Fülle von Rechtsregeln. Nach dem Verfassungsgrundsatz der Staatsferne fehlt dem Regierungspräsidenten von vornherein die Zuständigkeit. Er greift in den Zuständigkeitsbereich anderer Bundesländer über. Das völkerrechtliche Nichteinmischungsgebot steht entgegen. Materieellrechtlich bricht sich das Vorhaben am Zensurverbot und an dem abschließenden Charakter der Vorschriften zum Schutz der wehrhaften Demokratie. Die Verfügung überschreitet die Grenzen eines Vorgehens gegen Nichtstörer. Sie greift nicht nur in eine Vielzahl von Grundrechten der Access-Provider, sondern auch der Nutzer ein. Der Eingriff ist nicht einmal geeignet, insbesondere wegen der vielen Umgehungsmöglichkeiten. Nicht nur gleich viel, sondern mehr Schutz vor Nazipropaganda würde durch eine Kombination von sozialen Normen und einem Markt für Filtersoftware erreicht. Der Eingriff hat kaum mehr als symbolische Wirkung, greift aber tief in die Rechte der Access-Provider und der Nutzer ein. Deshalb steht er außer Verhältnis. Schließlich hätten die Access-Provider als Nichtstörer Anspruch auf Ersatz ihres finanziellen Aufwands.

■ Professor Dr. Christoph Engel ist Leiter der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter in Bonn. Der Beitrag basiert auf einem Gutachten, das im Auftrag von eco Electronic Commerce Forum – Verband der deutschen Internetwirtschaft e.V. erstellt wurde.

I. Einleitung

Wenn es nach dem *Düsseldorfer Regierungspräsidenten* (RP) geht, endet die Globalisierung vor den Düsseldorfer Stadttores. Er will das Internet regieren, als handle es sich dabei um ein rein deutsches Phänomen. Politisch hat sich der RP dafür einen guten Fall ausgesucht. Zwei amerikanische Websites halten rechtsradikale Propaganda vor. Sie machen dabei offene Anleihen an nationalsozialistisches Gedankengut. Im Lichte seiner Geschichte hat Deutschland solche Äußerungen tabuisiert. Es genügt deshalb nicht, sich persönlich von diesen Inhalten zu distanzieren. Geächtet wird bereits, wer für Toleranz oder für den offenen Wettbewerb der Meinungen eintritt.

Doch auch hier gilt die Einsicht von *Oliver Wendell Holmes*: „Hard cases make bad law.“ Der Tenor der Verfügung ist zwar auf die beiden rechtsradikalen Websites beschränkt.¹ Die Begründung ist aber so gefasst, dass sie auch auf alle anderen in Deutschland rechtswidrigen Inhalte von Websites ausgedehnt werden könnte. Setzt sich die Rechtsauffassung des RP durch, würden deutsche Ordnungsbehörden künftig auf breiter Fläche zu Sheriffs wider Schmutz und Schund im Internet. Die konkrete Ermächtigungsgrundlage des § 22 Abs. 3 MDStV deckt zwar offensichtlich kein Einschreiten wegen der Verletzung von Vorschriften des Urheber-, Persönlichkeits- oder Datenschutzrechts. Wenn die juristische Gedankenführung des RP von den Gerichten akzeptiert würde, könnten für diese Materien aber andere Ermächtigungsgrundlagen bemüht werden. Im Hintergrund stünde stets die allgemeine Generalklausel des Polizeirechts. Weil materielles deutsches Recht verletzt ist, wäre immer auch die öffentliche Sicherheit gefährdet.

Es geht also um viel mehr als die Bewahrung eines deutschen Tabus gegen eine skandalöse Verletzung. Der RP will nicht mehr und nicht weniger als ein Internet unter nationalstaatlicher Kontrolle. Die folgenden Überlegungen nehmen deshalb beides in den Blick: die zahlreichen Angriffsflächen der konkreten Entscheidung, aber auch die vorhersehbaren Folgen der vorgeschlagenen Auslegung des einfachen Rechts für die Struktur des Internet.

Das Vorgehen des RP wirft zahlreiche Kompetenzfragen auf (II.). Die Auslegung des materiellen Rechts und seine Vereinbarkeit mit höherrangigem Recht sind mehr als problematisch (III.). Schließlich dürfte der RP die Access-Provider als Nichtstörer jedenfalls nicht in Anspruch nehmen, ohne sie für den finanziellen Nachteil zu entschädigen (IV.).

II. Kompetenzen

Das Vorgehen der *Bezirksregierung* wirft zahlreiche Kompetenzprobleme auf. Am schwersten wiegt die Frage, ob solche Entscheidungen überhaupt Behörden der unmittelbaren Staatsverwaltung anvertraut werden dürfen (1.). Weiter fragt sich, ob die Zuständigkeit nicht richtigerweise beim Bund läge, oder ob das Land Nordrhein-Westfalen nicht zumindest auf parallele Zuständigkeiten des Bundes Rücksicht nehmen müsste (2.). Problematisch ist weiter die örtliche Zuständigkeit des Landes Nordrhein-Westfalen sowie ihre Abstimmung mit der Zuständigkeit anderer Bundesländer (3.). In einem weiter gefassten Sinne kann man auch die Abgrenzung zwischen Staat und Privaten als ein Kompetenzproblem begreifen. Auch aus dieser Perspektive ist die Verfügung fragwürdig (4.). Zu bestimmen ist weiter das Verhältnis zwischen den Zuständigkeiten der Bundesrepublik Deutschland und Europäischen Organen

(5.). Kritisch ist schließlich vor allem die Abstimmung des deutschen Vorgehens mit den legitimen Interessen ausländischer Staaten (6).

1. Staatsferne

Der *Düsseldorfer Regierungspräsident* ist eine Behörde der allgemeinen Staatsverwaltung. Er will eigentlich das Werben für nationalsozialistisches Gedankengut im Internet unterbinden. Er glaubt allerdings, dass er gegen die Urheber dieser Äußerungen nicht erfolgreich vorgehen kann. Deshalb möchte er subsidiär gegen die Unternehmen vorgehen, die deutschen Nutzern Zugang zum Internet gewähren. Er will sie verpflichten, den Zugang zu den nationalsozialistischen Äußerungen zu verhindern. Auch das ist eine Maßnahme der offenen Meinungskontrolle. Ob das verfassungsrechtlich überhaupt erträglich ist, wird uns noch zu beschäftigen haben.² Jedenfalls dürfen solche Entscheidungen von Verfassungen wegen aber nicht in der Hand der unmittelbaren Staatsverwaltung liegen.³ Denkbar wäre allenfalls die Entscheidung eines staatsfernen Gremiums. Das sehen offensichtlich auch die Länder Berlin, Brandenburg, Bremen und das Saarland so. Denn sie haben die Anwendung des Mediendienste-Staatsvertrags (MDStV) ihren Landesmedienanstalten anvertraut.⁴ Das entspricht i.Ü. auch der einhelligen Praxis bei der Regulierung des Rundfunks. Eine der zentralen Aufgaben der Landesmedienanstalten ist die Inhaltskontrolle.⁵ Weil nationalsozialistische Äußerungen im Rundfunk keine Rolle spielen, geht es dabei praktisch vor allem um den Jugendschutz.⁶

All das sind keine Fragen, die im Ermessen des jeweiligen Landesgesetzgebers stehen. Vielmehr hat das *BVerfG* das Gebot der Staatsferne der Inhaltskontrolle der Medien in einer ganzen Serie von Entscheidungen abgesichert: „So unverzichtbar der Staat damit als Garant einer umfassend zu verstehenden Rundfunkfreiheit ist, so sehr sind seine Repräsentanten doch selber in Gefahr, die Rundfunkfreiheit ihren Interessen unterzuordnen. Gegen die Gängelung der Kommunikationsmedien durch den Staat haben sich die Kommunikationsgrundrechte ursprünglich gerichtet, und in der Abwehr staatlicher Kontrolle der Berichterstattung finden sie auch heute ihr wichtigstes Anwendungsfeld.“⁷

Jeglicher staatliche Einfluss auf das Programm ist also verboten.⁸ Aus dem gerade wiedergegebenen Zitat ergibt sich

1) Verfügungen der *Bezirksregierung Düsseldorf* v. 6.2.2002 an im Lande Nordrhein-Westfalen niedergelassene Access-Provider; elektronisch verfügbar ist die Verfügung an *Oberon.net GmbH*, Az. 21.50.30, <http://www.odem.org/material/verfuegung/>. Mit B. v. 19.3.2003 (Az. 8 B 2567/02) hat das *OVG Münster* es abgelehnt, die aufschiebende Wirkung des Widerspruchs eines Access-Providers gegen die Verfügung des *Regierungspräsidenten* wiederherzustellen, http://www.artikel5.de/entscheidungen/ovg-muenster_20030319.html (die Entscheidung wird in der nächsten Ausgabe von MMR abgedruckt). Das *Gericht* hat dieses Gutachten dabei offensichtlich noch nicht zur Kenntnis genommen.

2) Näher unten III. 8. c).

3) So auch *Schulz*, MMR 1998, 184 f.

4) *Holznapel*, in: Hoeren/Sieber (Hrsg.), *Handbuch Multimediarecht*, 2000, Kap. 3.2, Rdnr.107; s. zu den unterschiedlichen Regeln der Länder über die Behördenzuständigkeit auch *Wimmer/Michael*, *Online-Provider*, 1998, 33 f.

5) Die Einzelheiten ergeben sich aus §§ 3 Abs. 1 u. Abs. 5 und 38 Abs. 1 RStV.

6) S. die gemeinsamen Richtlinien der Landesmedienanstalten über den Jugendschutz, http://www.nim.de/8js_ri.doc (Stand: 2.6.2002).

7) *BVerfGE* 90, 60, 88, unter Verweis auf *BVerfGE* 57, 295, 320.

8) *BVerfGE* 73, 118, 185; *Gersdorf*, *Staatsfreiheit des Rundfunks in der dualen Rundfunkordnung der Bundesrepublik Deutschland*, 1991, S. 89 spricht von einem „Verbot demokratiewidriger Beeinflussung des publizistischen Wirkungskreises“. Der „Rückkopplungskanal“ zwischen Staat und Gesellschaft darf nicht gestört werden, ders., S. 86; *Rühl*, *ZUM* 1995, 168 formuliert: „Jede Indienstnahme des Rundfunks für außerpublizistische Zwecke soll ausgeschlossen werden“.

eindeutig, dass das nicht nur für den Rundfunk gilt, sondern für alle Medien. Geschützt ist der gesamte Programmbereich.⁹ Das Gericht will nicht nur unmittelbaren, sondern auch jede Form von mittelbarem staatlichen Einfluss auf das Programm verhindern.¹⁰ Es „soll jede politische Instrumentalisierung des Rundfunks ausgeschlossen werden“.¹¹ Deshalb muss den staatlichen Behörden auch die Entscheidung über die Finanzierung des Rundfunks und über die Zuteilung von Übertragungskapazitäten entzogen werden.¹² All das sind keine bloßen Forderungen des objektiven Rechts. Die Inhaber der Mediengrundrechte können das Gebot der Staatsferne vielmehr mit der Verfassungsbeschwerde durchsetzen.¹³ Das *BVerfG* verlangt nicht die positive Zuweisung an die Landesmedienanstalten, billigt sie aber ausdrücklich.¹⁴ Zulässig wäre auch ein anderes, plural zusammengesetztes Gremium wie die *Bundesprüfstelle für jugendgefährdende Schriften*.¹⁵ Auch die Lösung, die die Länder für die Festsetzung der Rundfunkgebühren gefunden haben, entspricht nach allgemeiner Einschätzung dem Verfassungsgebot der Staatsferne.

Nordrhein-Westfalen hat diese verfassungsrechtlichen Anforderungen verletzt, indem es die Anwendung von § 22 Abs. 3 MDStV der *Bezirksregierung Düsseldorf* zugewiesen hat. Die *Bezirksregierung* ist eine Behörde der unmittelbaren Staatsverwaltung. Die Entscheidung über die Anwendung der inhaltlichen Vorgaben des § 12 MDStV betrifft das Programm der Mediendienste nicht nur mittelbar, sondern ganz unmittelbar. Das Verbot der Verbreitung nationalsozialistischen Gedankenguts richtet sich sogar

gegen eine ganz bestimmte Weltanschauung. Schließlich lässt sich die Zuständigkeit einer staatlichen Behörde auch nicht damit rechtfertigen, dass es dabei um die bloße Anwendung eines Gesetzes gehe. Denn die *Bezirksregierung* hält sich ja für zuständig, die Grenze zwischen gerade noch erlaubten und schon verbotenen Inhalten zu ziehen. Das ist eine Tätigkeit mit einem unvermeidbaren und erheblichen wertenden Element. Gerade solche wertenden Entscheidungen sollen den staatlichen Behörden nach dem Willen des *BVerfG* aber entzogen sein.¹⁶

Dieses Ergebnis wird durch einen Blick auf das materielle Recht noch verstärkt. Was der *Düsseldorfer Regierungspräsident* beabsichtigt, liegt zumindest ganz in der Nähe der Zensur; mit guten Gründen lässt es sich sogar unter das Zensurverbot in Art. 5 Abs. 1 Satz 3 GG subsumieren.¹⁷ Zensur ist von der Verfassung kategorisch verboten.¹⁸ Eine Rechtfertigung ist deshalb nicht möglich. Denkbar ist allenfalls, die Maßnahme so zu verändern, dass sie nicht mehr unter das kategorische Verbot fällt. Genau dies hat eine literarische Ansicht im Auge, die den Zusammenhang zwischen materiellem Recht und Behördenzuständigkeit herstellt. Erst die Staatsferne der Aufsichtsinstanz befreit vom Makel der Zensur. Denn dann ist ja nicht mehr zu besorgen, dass der Staat unmittelbar oder mittelbar seine eigene Kontrolle durch die Medien stumpf macht. So sieht das insbesondere auch der gegenwärtige *Berichterstatte* im *BVerfG* für das Medienrecht.¹⁹ Will man die Maßnahme bloß als zensurähnlich qualifizieren, folgt das gleiche Ergebnis aus der verfahrensrechtlichen Dimension des Grundrechts.²⁰

Schließlich gibt es auch einen Zusammenhang zwischen dem Gebot der Staatsferne und der Verteilung der Gesetzgebungszuständigkeiten zwischen Bund und Ländern. Der genaue Verlauf dieser Grenze ist lebhaft umstritten.²¹ Nach ganz überwiegender Auffassung sind die Länder aber jedenfalls nur dann zuständig, wenn der Inhalt Meinungsrelevanz hat. Genau dann bedarf es aber auch des Schutzes vor einer staatlichen Lenkung der Meinungsbildung. Daraus folgt, dass die Länder Gesetzgebungskompetenz zur Inhaltskontrolle jedenfalls nur dann in Anspruch nehmen können, wenn sie die Normanwendung einem staatsfernen Organ anvertrauen.

Die bisherigen Überlegungen werden mittlerweile auch durch den Gesetzgeber bestätigt. Der Beleg findet sich in dem abgeschlossenen, aber noch nicht in Kraft getretenen Jugendmediendienste-Staatsvertrag (JMStV).²² Der Staatsvertrag soll für den Rundfunk und die „Teledienste“ gelten. Mit diesem Sammelbegriff bezeichnet § 3 Abs. 2 Nr. 1 JMStV Mediendienste und Teledienste. Erfasst sind also gerade auch die hier in Rede stehenden Dienste.²³ Die Inhaltskontrolle dieser Dienste soll nach § 14 Abs. 2 Satz 1 JMStV künftig der *Kommission für Jugendmedienschutz (KJM)* anvertraut sein. Diese Kommission ist ein Organ der örtlich zuständigen Landesmedienanstalt, § 14 Abs. 2 Satz 2 JMStV. Der Staatsvertrag begründet diese Zuständigkeitsregel gerade mit dem Verfassungsgebot der Staatsferne.²⁴ Es ist allerdings mehr als zweifelhaft, ob die Zusammensetzung und das Verfahren der *KJM* diesem Gebot genügen.²⁵

2. Bund – Land

Die Schwierigkeiten bei der Abgrenzung der Gesetzgebungskompetenzen von Bund und Land zur Regelung der Internetnutzung sind offensichtlich. Sie sind zugleich aber auch Schwierigkeiten bei der Auslegung von MDStV und Teledienstegesetz (TDG). Wegen dieses engen systematischen Zusammenhangs sollen sie erst dort erörtert werden.²⁶

9) *Gersdorf* (o. Fußn. 8), S. 87 m.w.Nw.

10) *BVerfGE* 90, 60, 87; *BVerfGE* 73, 118, 183; das Gebot der Staatsferne schützt auch vor bloß latenten Gefahren, *Bumke*, Die öffentliche Aufgabe der Landesmedienanstalten. Verfassungs- und organisationsrechtliche Überlegungen zur Rechtsstellung einer verselbstständigten Verwaltungseinheit, 1995, S.146 m.w.Nw.

11) *BVerfGE* 90, 60, 88.

12) *BVerfGE* 90, 60, 88 f.

13) Das haben die öffentlich-rechtlichen Rundfunkanstalten mit dem Urteil über die Rundfunkfinanzierung auch praktisch getan, *BVerfGE* 90, 60. Man kann das Gebot der Staatsferne mit *Rühl*, ZUM 1995, 171 deshalb auch als Ausprägung des Grundrechtsschutzes durch Verfahren deuten.

14) *BVerfGE* 95, 220, 236; *BVerfG* v. 20.2.1998, ZUM 1998, 306, 310.

15) *BVerfGE* 83, 130, 153 und passim.

16) *BVerfGE* 73, 118, 182 f.; *BVerfGE* 90, 60, 89.

17) Näher unten III. 1. a).

18) *BVerfGE* 33, 52, 72.

19) *Hoffmann-Riem/Schulz*, Hamburgisches Medienrecht, 1997, S. 149 f.; s. auch *Hopf*, ZUM 2000, 744 f., 747; *Bethge*, ZUM 2002, 128.

20) Leitentscheidung zur verfahrensrechtlichen Dimension materieller Grundrechte, *BVerfGE* 49, 89, 112–119 – Kalkar; zur verfahrensrechtlichen Dimension von Art. 5 GG s. *BVerfGE* 27, 71, 88.

21) Näher unten III. 2. b).

22) Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telediensten v. 10.–27.9.2002. Der Staatsvertrag soll nach seinem § 28 Abs. 1 am 1.4.2003 in Kraft treten, wenn ihn bis dahin alle Landtage gebilligt haben.

23) Zu der schwierigen Abgrenzung zwischen Mediendiensten und Telediensten s. unten III. 2. b).

24) Amtl. Begr. zu § 14 Abs. 3 und Abs. 4 JMStV.

25) Problematisch ist schon die Zusammensetzung der *Kommission*. Denn sechs der zwölf Mitglieder werden unmittelbar von den obersten Behörden der Länder oder des Bundes ernannt, § 14 Abs. 3 Satz 1 JMStV. Ein schwaches Übergewicht der Landesmedienanstalten ergibt sich nur aus § 17 Abs. 1 Satz 2 i.V.m. § 14 Abs. 3 Satz 6 JMStV. Danach führt ein Direktor einer Landesmedienanstalt den Vorsitz. Bei Stimmgleichheit gibt seine Stimme den Ausschlag. Noch zweifelhafter sind die Vorgaben für das Entscheidungsverfahren. Nach § 14 Abs. 5 JMStV können Prüfungsausschüsse gebildet werden, die bei Einstimmigkeit an Stelle der *KJM* entscheiden. Ihnen gehört nur ein Mitglied der *KJM* an. Das kann jedes Mitglied sein, also gerade auch eines der von den Regierungen entsandten Mitglieder. In sich wäre verfassungsrechtlich schließlich nicht zu beanstanden, dass die *KJM* nicht als Repräsentation gesellschaftlich relevanter Gruppen ausgestaltet ist. Zusammen mit den übrigen Elementen verstärkt auch das aber die Zweifel an der Verfassungsmäßigkeit.

26) Näher unten III. 2. b).

Vor die Klammer gehört dagegen noch ein zweites, weniger beachtetes Zuständigkeitsproblem. Der *Düsseldorfer Regierungspräsident* will ganz offen ein politisches Zeichen setzen. Dieses Zeichen kann sich nur an das Ausland richten. Denn auf inländischen Servern gibt es praktisch keine rechtsradikalen Inhalte. Die beiden konkret ausgewählten URLs führen zu amerikanischen Servern. Der *RP* will der *amerikanischen Regierung* signalisieren, dass Deutschland nicht mehr länger gewillt ist, hinzunehmen, dass nationalsozialistische Gruppen das Internet zu ihrem Forum machen. Der *RP* will mit anderen Worten einen außenpolitischen Konflikt mit den USA anzetteln. Das ist natürlich vor allem ein völkerrechtliches Problem.²⁷ Zugleich entsteht daraus aber auch ein innerstaatliches Problem der Kompetenzabgrenzung zwischen Bund und Land.²⁸

Die Kompetenzverteilung in auswärtigen Angelegenheiten richtet sich nicht nach den Art. 30, 70 ff. und 83 ff. GG. Vielmehr enthält Art. 32 GG eine Sondervorschrift. Danach ist die gesamte Pflege der auswärtigen Beziehungen im Ausgangspunkt Sache des Bundes. Der Bund ist prinzipiell also nicht nur für die Gesetzgebung zuständig, sondern auch für Akte der Exekutive.²⁹ Was das für die *Rspr.* bedeutet, ist zwar nach wie vor nicht abschließend geklärt.³⁰ Darauf kommt es hier aber nicht an. Denn der *RP* hat sowohl ein Entschließungs- wie ein Auswahlermessens.³¹ Außerdem hat er sich mit seinem Schritt ganz gezielt an die Medien gewandt. An dem Potenzial zu einer Störung der abweichenden Außenpolitik des Bundes ist deshalb nicht zu zweifeln.

Art. 32 Abs. 1 GG will verhindern, dass die Bundesrepublik Deutschland in ihren außenpolitischen Beziehungen mit verschiedenen Stimmen spricht.³² Deshalb erfasst die Vorschrift nach ganz h.M. nicht nur völkerrechtsförmliches Handeln, sondern die gesamte Außenpolitik.³³ Die Kompetenz des Bundes aus Art. 32 Abs. 1 GG ist mit den Gesetzgebungs- und Verwaltungskompetenzen der Länder verschränkt. Es gibt unterschiedliche Vorstellungen darüber, wie diese Verschränkung dogmatisch zu erfassen ist. Auch in der länderfreundlichsten Lesart sind die Länder aus dem Gebot der Bundestreue aber verpflichtet, Handlungen zu unterlassen, mit denen sie sich in offenen Widerspruch zur Außenpolitik des Bundes setzen. Solch eine „Nebenaußenpolitik“ ist ihnen von der Verfassung eindeutig verboten.³⁴ So liegt es hier. Der Bund hat auf dem TDG gerade deshalb bestanden, weil er Absichten der Länder zu einer dichteren Regulierung des Internet zuvorkommen wollte.³⁵ Der spektakuläre *CompuServe-Fall*³⁶ sollte sich nicht wiederholen.³⁷ Für diese Entscheidung waren auch die außenpolitischen Verwicklungen mit den USA maßgeblich, zu denen dieser Fall geführt hat. An dieser Einschätzung hält die *Bundesregierung* nach wie vor fest. Sie setzt bei der Eindämmung rechtsradikaler Inhalte im Internet nicht auf einseitiges Handeln, sondern auf die Abstimmung in internationalen Gremien.³⁸

3. Land – Land

Die Bescheide des *RP* richten sich an im Lande Nordrhein-Westfalen niedergelassene Access-Provider. Bislang sind die Rechtsfolgen dieses Umstands nur unter dem – in der Tat unergiebigem – Gesichtspunkt des Gleichheitssatzes aus Art. 3 Abs. 1 GG diskutiert worden.³⁹ Ausschlaggebend ist dagegen die kompetenzrechtliche Seite. Viele dieser Unternehmen haben auch Kunden außerhalb dieses Bundeslands. Das führt zu einem Problem des horizontalen Föderalismus. Wieweit darf ein Land bezwecken und

bewirken, dass sich die Lebensverhältnisse in anderen Bundesländern ändern?

Zu einer strukturell verwandten Frage gibt es eine differenzierte wissenschaftliche Diskussion. Sie wird unter der Überschrift des Ländergrenzen überschreitenden Verwaltungsakts geführt.⁴⁰ Unmittelbar passen diese Überlegungen allerdings nicht. Denn die Geltung der Verwaltungsakte bleibt auf das Land Nordrhein-Westfalen beschränkt. Die Verwaltungsakte verlangen keinen Gehorsam von Personen außerhalb des Landes. Wohl erstrecken sich aber die Wirkungen des Verwaltungsakts auf andere Länder. Auch das ist ein beachtliches bundesstaatliches Problem. Es kann in denselben Kategorien diskutiert werden wie der länderüberschreitende Verwaltungsakt.⁴¹

Die Bundesländer sind zwar Staaten, zugleich aber Glieder des Bundes. Daraus leitet die ganz h.M. ab, dass Verwaltungsakte eines Landes auch in allen anderen Bundesländern gelten, wenn das Land Bundesrecht vollzogen hat.⁴² Das ist hier aber nicht der Fall. Der *RP* stützt seine Entscheidung gerade nicht auf das TDG des Bundes, sondern auf den MDStV der Länder.

Ein Land kann nicht ohne Wenn und Aber an die Verwaltungsakte anderer Länder gebunden sein. Denn zur verfassungsrechtlich geschützten Eigenständigkeit der Länder

27) Dazu näher unten III. 6.

28) Im Schrifttum finden sich lediglich zwei Andeutungen: *Engel-Flechsig/Maennel/Tettenborn*, Neue gesetzliche Rahmenbedingungen für Multimedia, 1997, S. 9 begründen die Bundeskompetenz für die Regelung der Teledienste auch mit der starken internationalen Dimension des Gegenstands; vgl. auch den Hinweis von *Koch*, JuS 2002, 212 auf die „außenpolitische Brisanz“ der Entscheidung des *BGH* zur Strafbarkeit eines Australiers für die von einem australischen Server aus verbreitete „Auschwitz-Lüge“.

29) Umfassend *Fastenrath*, Kompetenzverteilung im Bereich der auswärtigen Gewalt, 1986, 81–197.

30) Die einzige gründlichere Untersuchung ist schon recht alt: *Bolewski*, Zur Bindung deutscher Gerichte an Äußerungen und Maßnahmen ihrer Regierung auf völkerrechtlicher Ebene, Diss. 1971.

31) Näher unten III. 5. b.)

32) BVerfGE 2, 347, 378.

33) *Magiera*, in: FS Lüder, 1997, S.112 m.w.Nw.

34) BVerfGE 2, 347, 379; weitere Nw. aus der literarischen Diskussion bei *Magiera* (o. Fußn. 33), S. 111–115.

35) S. einstweilen nur den Vorspruch zur amtl. Begr. des IuKDG, BT-Drs. 13/7385, A; weitere Nw. unten III. 2. b.)

36) *AG München* MMR 1998, 429 = NJW-CoR 1998, 356.

37) *Popp*, Die strafrechtliche Verantwortung von Internet-Providern, 2002, S. 64 m.w.Nw.

38) Niedergelegt in dem umfangreichen Konzept des *BMI* gegen Rechtsextremismus und Fremdenfeindlichkeit v. 8.5.2002, http://www.bmi.bund.de/frame/dokumente/Artikel/ix_79389.htm. Unter Nr. 4 heißt es: „Das Internet ist ein globales Medium, dessen Kontrolle international sehr unterschiedlich gehandhabt wird. Während z.B. in den USA die Verbreitung rechtsextremer Internethinhalte unter Hinweis auf die Meinungsfreiheit weitgehend straffrei bleibt, wird sie in Deutschland als Straftat geahndet. Daher setzt sich die *Bundesregierung* in internationalen Gremien, vor allem im *Europarat* und i.R.d. *G-8 der Vereinten Nationen*, nachhaltig für eine einheitliche internationale Verfolgung rechtsextremistischer Straftaten im Internet ein“.

39) Die Stellungnahme des *RP* findet sich in seinem Widerspruchsbescheid, http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/THEMEN_Beitrug_druckbar.html?query=THBTR.ID%3d8229 (Stand: 25.10.2002).

40) S. vor allem *Bleckmann*, NVwZ 1986, 1; *Seibert*, Die Bindungswirkung von Verwaltungsakten, 1989, S. 274–288.

41) Genau genommen könnte es sogar zu einer Geltungserstreckung kommen. Das hängt davon ab, ob die Verwaltungsakte nicht nur einen verpflichtenden Gehalt gegenüber den Access-Providern haben, sondern auch eine Duldungsverpflichtung ggü. den Kunden der Access-Provider enthalten. Alternativ könnten sie ggü. den Kunden auch mit Rechtsverbindlichkeit feststellen, dass die Sperrung der im Tenor bezeichneten Websites rechtmäßig ist. Das wirft schwierige Fragen auf der Grenzlinie zwischen öffentlichem Recht und Zivilrecht auf, die nicht wichtig genug sind, um hier im Einzelnen entfaltet zu werden. S. dazu näher *Engel*, Planungssicherheit für Unternehmen durch Verwaltungsakt, 1992, S.18–37.

42) *Seibert* (o. Fußn. 40), S. 274 f.; *Ruffert*, Der transnationale Verwaltungsakt, 2001, S. 471, jew. m.w.Nw.

gehört ihre Freiheit, unterschiedliche regulatorische Programme zu entwickeln.⁴³ Das Gegenteil folgt auch nicht aus dem Gebot des Art. 35 Abs. 1 GG zur Amtshilfe.⁴⁴ Denn diese Pflicht setzt voraus, dass das Amtshilfeersuchen die verfassungsrechtlich geschützte Autonomie der anderen Länder respektiert. Ebenso unangemessen ist umgekehrt aber auch eine Analogie zum Territorialitätsprinzip des Völkerrechts. Daraus würde folgen, dass die Verwaltungsakte anderer Länder nur dann gelten, wenn sie von dem zweiten Land autonom und ausdrücklich anerkannt sind.⁴⁵ Vielmehr muss die Spannungslage zwischen der Eigenverantwortlichkeit der Länder und der von der Verfassung ebenfalls gewollten funktionellen Einheit des Bundesstaats gewahrt bleiben.⁴⁶ In anderen Fällen kann die Pflicht zur Anerkennung von Verwaltungsakten anderer Bundesländer auch aus den Grundrechten ihrer Adressaten folgen.⁴⁷ Dieser Gedanke passt aber nur auf begünstigende, nicht auf belastende Verwaltungsakte.⁴⁸

Scheinbar folgt aus diesen Überlegungen, dass die übrigen Bundesländer in dem hier betrachteten Fall die grenzüberschreitende Wirkung der nordrhein-westfälischen Verwaltungsakte hinnehmen müssten. Denn in der Lit. wird auf den Inhalt des angewendeten Sachrechts abgestellt. Ist die Regel beider Länder gleich oder zumindest ähnlich, soll der Verwaltungsakt Ländergrenzen überschreitende Wirkung haben.⁴⁹ Der *RP* hat eine Norm des MDStV angewendet. Sie hat nicht nur in allen Ländern den gleichen Inhalt. Vielmehr handelt es sich sogar rechtstechnisch um dieselbe Norm. Das Argument ist scheinbar sogar noch stärker. Denn der MDStV enthält in § 22 Abs. 5 ja sogar eine ausdrückliche Zuständigkeitsregel. Offenbar haben die Länder das Problem der grenzüberschreitenden Wirkung also gesehen und einvernehmlich durch die Zuständigkeitsregel gelöst.⁵⁰

Diese Ableitung ist jedoch vorschnell. Den Einwand kann man auf der Ebene des einfachen Rechts, aber auch des Verfassungsrechts formulieren. Die einfachrechtliche Vorschrift des § 22 Abs. 5 MDStV lautet: „Für den Vollzug dieses Abschnitts ist die Aufsichtsbehörde des Landes zuständig, in dem der betroffene Anbieter seinen Sitz, Wohnsitz oder in Ermangelung dessen seinen ständigen Aufenthalt hat. Ergibt sich danach keine Zuständigkeit, so ist diejenige Aufsichtsbehörde zuständig, in deren Bezirk der Anlass für die Amtshandlung hervortritt“.

Entscheidend ist, was dabei mit „der betroffene Anbieter“ gemeint ist. Der *RP* stellt auf den Access-Provider ab. Das ist falsch. Zunächst fallen Access-Provider selbst überhaupt nicht unter den MDStV, sondern unter das TDG.⁵¹ Außerdem wäre diese Auslegung systemwidrig. Die Anwendbarkeit von § 22 Abs. 3 MDStV auf den vorliegenden

Fall lässt sich nämlich allenfalls auf folgendem Wege begründen: Man stellt auch für das subsidiäre Eingreifen gegenüber dem Access-Provider ausschließlich darauf ab, ob der Anlass für den Eingriff von einem Mediendienst herührt. Dann wird unschädlich, dass der Access-Provider selbst gar kein Mediendienst ist.⁵² Konsequenz kann auch in § 22 Abs. 5 MDStV mit dem „betroffenen Anbieter“ nur der Anbieter des Mediendienstes gemeint sein, der Anlass zur staatlichen Intervention bietet.

Für diese Interpretation streitet vor allem aber ein teleologisches Argument. Beim Vorgehen gegen den Anbieter der Inhalte ist die Zuständigkeitsregel des § 22 Abs. 5 MDStV sinnvoll. Das Bundesland soll zuständig sein, in dem sich der Urheber der problematischen Inhalte befindet. Dort können nämlich ohne Mühe Verwaltungsverfahren gegen ihn durchgeführt werden.

Scheinbar kommt es auf all das allerdings gar nicht an. Denn nach § 22 Abs. 5 Satz 2 MDStV ist subsidiär die Aufsichtsbehörde des Landes zuständig, in deren Bezirk Anlass für die Amtshandlung hervortritt. Weil aus dem Internet Inhalte an jedem beliebigen Ort der Welt abgerufen werden können, ergibt sich daraus scheinbar die konkurrierende Zuständigkeit sämtlicher Bundesländer. Zunächst hat sich der *RP* auf diese Zuständigkeitsnorm jedoch nicht berufen. Vielmehr hat er gerade die Access-Provider mit Sitz im Lande Nordrhein-Westfalen herausgegriffen. Er selbst stützt sich also auf den – allerdings falsch interpretierten – § 22 Abs. 5 Satz 1 MDStV. Vor allem wäre es aber höchst überraschend, wenn die Länder wirklich eine konkurrierende Zuständigkeit jedes Landes hätten schaffen wollen. Zumindest wäre dann zu erwarten, dass sich in der Vorschrift Regelungen für den Fall finden, dass mehrere Länder zugleich die Zuständigkeit der Regelung ein und desselben Falls beanspruchen.

Vor allem wird aus § 22 Abs. 5 MDStV aber deutlich, dass die Länder bei der Zuständigkeitsregel nur innerstaatliche Sachverhalte vor Augen hatten. Dann wird es ganz regelmäßig einen feststellbaren Anbieter geben. Das Land, in dem er seinen Sitz hat, soll dann tätig werden. Nur wenn das ausnahmsweise scheitert, ist nach § 22 Abs. 5 Satz 2 MDStV subsidiär auch das Land zuständig, in dem der problematische Inhalt zu einem sozialen Konflikt führt. Solange das die seltene Ausnahme bleibt, erscheint es nicht verwunderlich, dass die Länder auf Regeln zur Bewältigung von Zuständigkeitskonflikten verzichtet haben. Aus dieser Einsicht kann man zwei unterschiedliche Folgerungen ziehen. Zunächst liefert sie ein zusätzliches Argument dafür, den internationalen Anwendungsbereich der Norm eng auszulegen.⁵³ Bleibt zumindest der Rest eines extraterritorialen Anwendungswillens, ist zugleich aber auch nach einer Auslegung zu suchen, die Zuständigkeitskonflikte vermindert und Lösungswege anbietet.

Eine erste Klasse von Fällen ist relativ einfach zu bewältigen. § 22 Abs. 5 Satz 2 MDStV führt nur dann zu Zuständigkeitskonflikten zwischen den Ländern, wenn „der Anlass für die Amtshandlung“ gleichzeitig in mehreren Bundesländern entsteht. Ob das so ist, hängt vom Schutzgut der materiellen Norm ab. Der MDStV enthält eine Reihe von Regeln, die zu bipolaren Konflikten zwischen einem Anbieter und einem potenziellen Verletzten führen. So liegt es etwa beim Gegendarstellungsrecht und typischerweise auch beim Datenschutz. Auch wenn man den MDStV auf grenzüberschreitende Sachverhalte anwendet, befindet sich der potenzielle deutsche Verletzte dann jeweils nur in einem einzigen Bundesland.⁵⁴

43) BVerfGE 11, 6, 19; *Seibert* (o. Fußn. 40), S. 276; *Ruffert* (o. Fußn. 42), S. 471.

44) *Anders Kopp/Kopp*, BayVBl. 1994, 231; *Ruffert*, Die Verwaltung 2001, 471.

45) Näher *Bleckmann*, NVwZ 1986, 1; *Seibert* (o. Fußn. 40), S. 279 f.

46) *Seibert* (o. Fußn. 40), S. 285; s.a. *Bleckmann*, NVwZ, 1, 3.

47) *Bleckmann*, NVwZ 1986, 4 f.; *Ruffert* (o. Fußn. 42), S. 471.

48) *Bleckmann*, NVwZ 1986, 5 spricht vom „Gedanken der wohlverworbenen Rechte“.

49) Vgl. o. Fußn. 48; *Seibert* (o. Fußn. 40), S. 286.

50) So dürfte *Holzengel* (o. Fußn. 4), Rdnr. 106 zu verstehen sein; vgl. auch *Zimmermann*, NJW 1999, 3147: „wo sich im Einzelfall die jeweilige polizeiliche Gefahr primär verwirklichen würde“.

51) Näher unten III. 2. b).

52) Näher unten III. 2. b).

53) S. unten 6. b).

54) Näher zu der Unterscheidung zwischen „one-to-one“ und „one-to-many“-Konflikten *Engel*, Preprint 2002/12 http://www.mpp-rdg-mpg.de/pdf_dat/2002_12.pdf.

Andere materielle Normen des Staatsvertrags schützen dagegen nicht vor konkreten, sondern vor abstrakten Gefahren.⁵⁵ Dann hat der Konflikt einen anderen Charakter. Es stehen sich nicht mehr ein potenzieller Verletzer und ein potenzieller Geschädigter gegenüber. Vielmehr steht dem einen potenziellen Verletzer die gesamte Gemeinschaft der potenziell Verletzten gegenüber. Daraus entsteht das schon herausgearbeitete Problem einer ubiquitären Zuständigkeit aller Bundesländer.

Theoretisch ließe sich das Problem dadurch lösen, dass jedes Bundesland nur Entscheidungen mit Wirkung für sein eigenes Staatsgebiet treffen darf. Die Lösung würde voraussetzen, dass das Internet technisch in geografische Zonen aufgelöst wird. Wir werden noch sehen, dass das nicht nur sehr hohe Kosten hätte, sondern an einer Fülle von Umgehungsmöglichkeiten scheitern würde.⁵⁶ Vor allem würde sich solch eine elektronische Kleinstaaterei aber am erklärten Willen des Bundesgesetzgebers stoßen. Der wichtigste Grund für die Verabschiedung des TDG war gerade die Sorge des Bundes, die schnelle Verbreitung des Internets könne an Differenzen zwischen der Politik verschiedener Bundesländer scheitern.⁵⁷ Der Wunsch des Bundes nach bundesweit einheitlichen Regeln war die Geschäftsgrundlage für den Kompromiss zwischen Bund und Ländern. Er hat zum aufeinander abgestimmten Erlass von TDG und MDStV geführt.⁵⁸ Der gemeinsame Wunsch von Bund und Ländern nach bundesweit einheitlichen Verhältnissen darf auch nicht durch eine Interpretation der Zuständigkeitsregel des § 22 Abs. 5 Satz 2 MDStV gestört werden.

Diese einfachrechtlichen Überlegungen werden durch einen Blick auf Grundrechte zusätzlich gestützt. Das Rundfunkrecht hat nämlich ein strukturell verwandtes Problem zu bewältigen. Rundfunk wird nicht nur über Kabel verbreitet, sondern auch terrestrisch und per Satellit. Terrestrische Wellen machen nicht an den Landesgrenzen halt. Die Ausleuchtzone eines Satelliten lässt sich nicht auf das Gebiet eines einzigen Bundeslands beschränken. Wenn ein Land einen privaten Rundfunkveranstalter zulässt, hat das deshalb unvermeidlich auch Folgen für die Verhältnisse in benachbarten Bundesländern. Das *BVerfG* hat deshalb zum Schutz der Veranstalter, vor allem aber der Rezipienten bundesweit einheitliche Entscheidungen verlangt.⁵⁹ Zum Schutz der Informationsfreiheit der Internetnutzer kann das hier nicht anders sein.⁶⁰

Um das Verfassungsgebot einheitlicher Entscheidungen zu erfüllen, haben die Länder den Rundfunkstaatsvertrag (RStV) abgeschlossen. Dort findet sich dann auch eine Lösung für die Zuständigkeitskonkurrenz zwischen den Ländern. § 38 RStV lautet:

„(1) Die zuständige Landesmedienanstalt überprüft vor und nach der Zulassung die Einhaltung der sonstigen für den privaten Veranstalter geltenden Bestimmungen dieses Staatsvertrags. Sie trifft entsprechend landesrechtlichen Regelungen die jeweilige Entscheidung.

(2) Die zuständigen Landesmedienanstalten stimmen sich mit dem Ziel einer länder einheitlichen Verfahrensweise hinsichtlich der Anwendung des Absatzes 1 untereinander ab. Sie sollen zu diesem Zweck, auch zur Vorbereitung von Einzelfallentscheidungen, gemeinsame Stellen bilden. Die Landesmedienanstalten sollen bei planerischen und technischen Vorarbeiten zusammenarbeiten.

(3) Jede Landesmedienanstalt kann gegenüber der Landesmedienanstalt des Landes, in dem die Zulassung erteilt

wurde, nach Absatz 1 beanstanden, dass ein bundesweit verbreitetes Programm gegen die sonstigen Bestimmungen dieses Staatsvertrages verstößt. Die zuständige Landesmedienanstalt ist verpflichtet, sich mit der Beanstandung zu befassen und die beanstandende Landesmedienanstalt von der Überprüfung und von eingeleiteten Schritten zu unterrichten.“

Über diese Vorschrift hinaus haben die Gerichte den Landesmedienanstalten anderer Länder mit Billigung des *BVerfG* auch im Verwaltungsprozess ein Klagerecht eingeräumt.⁶¹ Wie sonst auch gibt es zwei rechtstechnische Möglichkeiten, auf diesen Sachverhalt zu reagieren. Der Interpret könnte versuchen, durch Analogie zum Rundfunkrecht die Lösung für das übersehene Problem der Zuständigkeitskonkurrenz in den MDStV hineinzulesen. Dann wäre die Entscheidung des *RP* unwirksam, weil es an der notwendigen Abstimmung mit den anderen Bundesländern fehlt. Der Gesetzgeber muss den Zuständigkeitskonflikt für die Mediendienste aber natürlich nicht genau in derselben Weise auflösen wie für den Rundfunk. Deshalb wäre richterliche Zurückhaltung wohl die bessere Lösung. Da die beschriebenen verfassungsrechtlichen Probleme bestehen bleiben, kann das nur bedeuten: Der internationale Anwendungsbereich des MDStV wird auf solche Konflikte beschränkt, für die die Zuständigkeitsregeln aus § 22 Abs. 5 MDStV passen. Praktisch bedeutet das, dass der internationale Anwendungsbereich nur für bilaterale Konflikte und für konkrete Gefahren eröffnet ist, nicht dagegen für multilaterale Konflikte und abstrakte Gefahren. Das entspricht vermutlich nur zum Teil dem Willen der Landesgesetzgeber. Der weiter gehende Wille der Landesgesetzgeber kann aber jedenfalls erst dann zum Tragen kommen, wenn zugleich auch das Problem der Zuständigkeitskonflikte in einer verfassungskonformen Weise bewältigt ist. Zunächst muss der Landesgesetzgeber deshalb erneut tätig werden.

Schließlich wird auch das In-Kraft-Treten des JMStV an diesem Ergebnis nichts ändern. Denn § 20 Abs. 6 JMStV enthält die gleiche Zuständigkeitsregel wie § 22 Abs. 5 MDStV. Das Konfliktpotenzial wird allerdings deutlich kleiner, weil die jeweils örtlich zuständige Landesmedienanstalt dann nach § 14 Abs. 2 Satz 1 JMStV durch die *KJM* handeln wird. Nach § 14 Abs. 2 Satz 2 JMStV handelt diese *Kommission* aber als Organ der jeweils örtlich zuständigen Landesmedienanstalt. Im Außenverhältnis zu den Anbietern wird nach § 14 Abs. 1 JMStV allein die jeweilige Landesmedienanstalt tätig. Auch künftig muss die Frage der örtlichen Zuständigkeit also entschieden werden.

4. Staat – Private

Der *RP* hat seiner Verfügung eine harmlose Färbung gegeben. Es geht scheinbar bloß um Rechtsanwendung in einem Sachverhalt des besonderen Polizeirechts. Zwei Störer kann er nicht erreichen. Deshalb nimmt er subsidiär

55) Die Unterscheidung spielt vor allem in der Diskussion zum Internetstrafrecht eine zentrale Rolle, s. zunächst nur *Sieber*, NJW 1999, 2066-2069 und näher unten 6. b) und c).

56) Näher unten III. 9. b).

57) Der Bund hat das viele Male betont, s. nur BT-Drs. 13/7385, Begr. A, Begr. B zu Art. 1 A, Gegenäußerung der *Bundesregierung*, ebd. 26.

58) Zu dem Zuständigkeitsstreit und seiner Lösung näher III. 2. b).

59) *BVerfGE* 73, 118, 196 f.

60) Zur Bedeutung der Informationsfreiheit für den Sachverhalt s. noch näher unten III. 7.

61) *BVerfG* v. 9.7.1993, AfP 1993, 730, 731.

die erreichbaren Nichtstörer in Anspruch.⁶² Unter dieser Oberfläche verbirgt sich jedoch ein Sachverhalt von viel weiter tragender Bedeutung. In einer Presseerklärung hat der *RP* eingeräumt, worum es ihm wirklich geht. Er will das ganze Internet von rechtsradikalen Inhalten säubern und zielt dabei auf „bis zu“ 6.000 Websites.⁶³ Der schiere Regulierungsaufwand macht deutlich, dass der *RP* dieses Ziel mit Befehl und Zwang nie und nimmer erreichen könnte. Bei genauerer Lektüre der Verfügung zeigt sich, dass er das auch gar nicht will. Er will das konkrete Verfahren vielmehr dazu nutzen, Druck auf die deutschen Access-Provider auszuüben. Sie sollen an ihrem Ende das Internet technisch so verändern, dass es für den deutschen Staat leicht regulierbar wird.

In den USA sind solche staatlichen oder kommerziellen Versuche zu Recht zu einem Politikum geworden. Amerikanische Wissenschaftler haben darauf hingewiesen, dass solche Änderungen der Architektur des Netzes keineswegs unpolitisch sind. Vielmehr ist „Regulation by Code“ eine besonders wirksame Regelungstechnik. Weil die Regulierung dann in der Hand von Technikern liegt, sind die Ergebnisse vorhersehbar in eine bestimmte Richtung gelenkt. Technokratische Lösungen werden wahrscheinlich. Zugleich findet Regulierung auf eine Art statt, die von der politischen Öffentlichkeit kaum bemerkt und kontrolliert wird. Auch rechtsstaatliche Sicherungen sind weitgehend ausgehebelt. Das Ergebnis erhält nicht die Form eines gerichtlich kontrollierbaren Gesetzes. Vielmehr wird der Inhalt gleichsam in einen technischen Standard eingefroren. Ungehorsam ggü. diesem Standard ist praktisch ausgeschlossen. Wer ihn nicht befolgt, schließt sich nämlich selbst von der Kommunikation aus.⁶⁴

62) In dem Widerspruchsbescheid (a.E., zu § 14 OBG) bezeichnet der *RP* die Access-Provider allerdings als Zustandsstörer. Das ist offensichtlich falsch. Näher unten III 5 a.

63) *dpa*, xxx-fc yynwd kh 161754 Mai 02; s.a. die folgende Passage aus dem Widerspruchsbescheid (o. Fußn. 39): „Die Vielzahl extremistischer Homepages unterstreicht die Erforderlichkeit und Angemessenheit des staatlichen Vorgehens zusätzlich“.

64) Die amerikanische Diskussion wird angeführt von *Lessig*, *Code and other Laws*, 1999; s. außerdem *Reidenberg*, *Texas Law Review* 1998, insb. S. 571 und 583 f.

65) S. aber *Schulte*, in: *Rengeling*, *Umweltnormung*, 1998, S. 165 ff. und aus der politikwissenschaftlichen Diskussion *Genschel*, *Standards in der Informationstechnik*, 1995; *Voelzkow*, *Private Regierungen in der Techniksteuerung*, 1996.

66) Aus der reichen Lit. s. nur *di Fabio*, in: *VVDStRL* 1997, 235 ff.; *Schmidt-Preuß*, *VVDStRL* 1997, 160 ff.; *Engel*, *Staatswissenschaften und Staatspraxis*, 1998, 535 ff.; *Engel*, *Die Verwaltung* 2001, 1 ff.

67) *Leitentscheidung BVerfGE* 49, 89.

68) So etwa *Trute*, *DVBfL* 1996, 957; *Grewlich*, *DÖV* 1998, 57 f.

69) Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insb. des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), *ABl. EG* 2000 Nr. L 178/1.

70) S. insb. die 58. Erwägung der Präambel; so auch *Spindler*, *MMR* 1999, 205.

71) Entschließung des Europäischen Parlaments zum Evaluierungsbericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Empfehlung des Rats v. 24.9.1998 in Bezug auf den Jugendschutz und den Schutz der Menschenwürde (KOM (2001) 106. C5-0191/2001. 2001/2087(COS)).

72) *Lessig/Resnick*, *Michigan Law Review* 1999, 395.

73) „In Cyberspace, the First Amendment is a local ordinance“, *John P. Barlow*: *Leaving the Physical World*, http://www.eff.org/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html (Stand: 26.6.2002).

74) Dazu umfassend *National Research Council*, *Global Networks and Local Values*, 2002; s.a. *Engel*, *AfP* 2002, 119 ff.

75) In der jetzt geltenden Neufassung in § 12 Abs. 1 Nr. 1 MDStV heißt es nur noch allgemein „Angebote sind unzulässig, wenn sie 1. gegen Bestimmungen des StGB verstoßen“. In der hier relevanten Hinsicht hat sich dadurch aber nichts geändert. Denn nach wie vor wird auf das StGB verwiesen.

In der deutschen juristischen Diskussion gibt es bislang erst wenige Überlegungen über die Besonderheiten einer Regulierung durch technische Standards.⁶⁵ Breit erörtert ist dagegen die allgemeinere Frage nach der staatlich regulierten Selbstregulierung.⁶⁶ Dabei sind vor allem die Risiken aus der Perspektive des Demokratie- und des Rechtsstaatsprinzips herausgearbeitet worden. Zumindest geht es nach der Wesentlichkeitstheorie des *BVerfG*⁶⁷ nicht ohne eine ausdrückliche Entscheidung des Gesetzgebers für die regulierte Selbstregulierung.⁶⁸ Der MDStV spricht mit keinem Wort davon, dass die zuständigen Aufsichtsbehörden befugt wären, einen Prozess der technischen Selbstregulierung des Internet anzustoßen. Auch aus diesem Grunde hat der *RP* folglich die Grenzen der Ermächtigungsnorm überschritten.

5. Deutschland – Europa

Auf den ersten Blick könnte ein weiteres Hindernis in der E-Commerce-Richtlinie der EG liegen.⁶⁹ Art. 3 Abs. 4 der Richtlinie enthält komplizierte Regeln darüber, unter welchen Voraussetzungen ein Mitgliedstaat vom Herkunftslandprinzip abweichen darf. Bedeutsam sind vor allem zwei verfahrensrechtliche Voraussetzungen. Er muss den Herkunftsstaat erfolglos zum Einschreiten aufgefordert haben. Und er muss die Genehmigung der *EG-Kommission* einholen. Die Richtlinie gilt aber ausdrücklich nur im Verhältnis der EU-Mitgliedstaaten untereinander.⁷⁰

Richtig ist allerdings, dass sich der *RP* in offenen Widerspruch zum *Europäischen Parlament* setzt. In einer Entschließung aus dem Jahre 2001 hat es formuliert: „16. Das Europäische Parlament ist der Auffassung, dass die Zusammenarbeit und die Partnerschaft zwischen der Internetindustrie, den Regierungen und den nationalen und regionalen Behörden die wirksamste Möglichkeit darstellt, gegen schädigende und illegale Inhalte im Internet vorzugehen, und zeigt sich besorgt, dass die jüngsten Entscheidungen bzw. Strategien im Hinblick auf die Blockierung des Zugangs zu bestimmten Websites zur teilweisen Einschränkung des Internetzugangs bzw. zur Verhinderung des Zugangs zu rechtmäßigen Inhalten führen können und deshalb keine wirksame europäische Lösung für die Bekämpfung illegaler und schädigender Internetinhalte darstellen.“⁷¹

6. Deutschland – Ausland

Die Staaten sind sich nicht einig, welche Inhalte des Internet sie für akzeptabel halten: „What constitutes ‚political speech‘ in the United States (Nazi speech) is banned in Germany; what constitutes ‚obscene‘ speech in Tennessee is permitted in Holland; what constitutes porn in Japan is child porn in the United States; what is harmful to minors in Bavaria is Disney in New York.“⁷²

Im Internet prallen deshalb unterschiedliche Verfassungstraditionen⁷³ und Wertvorstellungen aufeinander.⁷⁴ Wenn ein Staat beginnt, den Inhalt des Internet zu regulieren, hat das unvermeidlich extraterritoriale Wirkungen (a). Dieser Umstand kann auf mehreren dogmatischen Wegen Wirkung für die Anwendung von § 22 Abs. 3 MDStV bekommen. Zunächst kann man unmittelbar nach dem internationalen Anwendungsbereich der Vorschrift fragen (b). Sodann stellt sich die gleiche Frage mittelbar noch einmal. Denn der *RP* beruft sich auf einen Verstoß gegen die Anforderungen des § 8 Abs. 1 Nr. 1 und des § 8 Abs. 1 Nr. 2 MDStV a.F.⁷⁵ Diese Vorschriften des MDStV nehmen Bezug auf die §§ 130 und 131 StGB. Deshalb kommt es auch auf den internationalen Anwendungswillen dieser beiden

strafrechtlichen Vorschriften an (c). Schließlich und vor allem gibt es differenzierte völkergewohnheitsrechtliche Regeln über die Grenzen der extraterritorialen Anwendung nationalen Rechts (e). Diese Normen zeitigen über Art. 25 GG auch innerstaatliche Wirkungen (d). Schließlich hat die völkerrechtliche Seite des Sachverhalts auch verfahrensrechtliche Folgen (f).

a) Extraterritoriale Wirkung

Auf den ersten Blick könnte man denken, dass der Sachverhalt gar kein Problem der Extraterritorialität aufwirft. Denn die Verwaltungsakte des RP wollen ja nicht im Ausland gelten. Die Regelungsautonomie anderer Staaten kann aber auch durch die faktischen Wirkungen einseitiger Handlungen beeinträchtigt werden. Dieselbe Unterscheidung ist uns ja schon im Verhältnis der Bundesländer untereinander begegnet.⁷⁶

Bedeutsamer scheint auf den ersten Blick ein zweiter Einwand. Der RP wendet sich nur an Access-Provider mit Sitz in Nordrhein-Westfalen. Hat er deshalb nicht selbst schon die Wirkungen seines Verwaltungsakts auf das Inland beschränkt? Bei näherem Zusehen ist das nicht richtig. Zunächst sagt die Niederlassung des Access-Providers nichts darüber aus, wo seine Kunden wohnen oder niedergelassen sind. Es ist auch praktisch keineswegs unwahrscheinlich, dass ein nordrhein-westfälischer Access-Provider ausländische Kunden hat. Schon technisch spielen Distanzkosten im Internet praktisch keine Rolle. Es genügt, wenn der Access-Provider auch ausländische Einwahlknoten schafft. Vor allem braucht der Firmensitz aber nicht identisch mit dem Absatzgebiet zu sein.

Während dieser erste Spillover nur ausnahmsweise auftreten wird, erfassen die beiden übrigen extraterritorialen Effekte sämtliche Verfügungen des RP. Der RP will ganz offen ein anderes Internet. Technischer gesprochen: Er will Druck aufbauen mit dem Ziel, die Architektur des Internet zu ändern. Auf welchem technischen Wege die Adressaten die Sperrung der fraglichen Websites bewirken, überlässt ihnen die Verfügung. Noch deutlicher wird die Absicht zur Änderung der Architektur des Netzes aber in einem anderen, bereits erwähnten Umstand sichtbar. Der RP betreibt ein Pilotverfahren. Wenn er Erfolg hat, will er die Access-Provider zur Sperrung sämtlicher rechtsradikalen Angebote zwingen. Er rechnet damit, dass dies bis zu 6.000 Websites sein können.⁷⁷ Diese Absicht ist durch Einzelverfügungen nicht zu verwirklichen. Jahrelange Rechtsstreitigkeiten wären die Folge. Oft genug würde sich der Gegenstand während des Verfahrens erledigen, weil die Websites mittlerweile eingestellt sind, ihren Inhalt in erheblicher Weise verändert oder andere Domainnamen angenommen haben. Auch der französische *Yahoo*-Fall zeigt, dass sich die Wirkungen einer nationalen Entscheidung nicht auf das Inland beschränken lassen. Das *Gericht* hatte *Yahoo* aufgegeben, dafür zu sorgen, dass die Seiten mit dem Angebot von Nazi-Memorabilia von Frankreich aus nicht mehr aufgerufen werden können. Tatsächlich hat *Yahoo* diese Angebote dann ganz von seinem Server genommen. Die Kosten für eine Aufspaltung in nationale Zonen wären prohibitiv gewesen.⁷⁸

Noch stärker ist das letzte Argument. Die Eingriffsbefugnis nach § 22 Abs. 3 MDStV ist überhaupt nur dann eröffnet, wenn das Vorgehen gegen den Anbieter des Inhalts scheitert. Voraussetzung für die Zulässigkeit eines Eingreifens nach § 22 Abs. 3 MDStV ist also, dass die Behörde auch unmittelbar nach § 22 Abs. 1 oder Abs. 2 MDStV hätte vor-

gehen dürfen. § 22 Abs. 3 MDStV erweitert nur den Kreis der Adressaten. Dagegen erweitert diese Vorschrift nicht die übrigen Eingriffsvoraussetzungen.

Der RP betont ausdrücklich, dass die fraglichen Inhalte auf Servern in den USA liegen. Er zitiert sogar die Entscheidung des *Bundesgerichts aus San Diego* im Fall *Yahoo*. Das *Gericht* stellt fest, dass der Verkauf von Nazi-Memorabilia über das Internet in den Vereinigten Staaten verfassungsrechtlich geschützt ist.⁷⁹ In der verfassungsrechtlichen Haltung der USA sieht der RP sogar den Grund für die innerstaatliche Rechtmäßigkeit seines Vorgehens.⁸⁰ Der RP will also den offenen verfassungspolitischen Konflikt zwischen dem deutschen Gedanken der wehrhaften Demokratie und dem amerikanischen Gedanken eines freien Marktplatzes der Meinung.⁸¹

b) Anwendbarkeit von § 22 Abs. 3 MDStV auf Auslandssachverhalte

Was im Privat- und Strafrecht selbstverständlich ist, erregt unter Öffentlichrechtlern immer noch häufig Verwunderung: der internationale Anwendungsbereich der Normen versteht sich nicht von selbst.⁸² Rechtstechnisch gibt es zwei Möglichkeiten. Das Privatrecht und das Strafrecht haben ein eigenes Kollisionsrecht. Diese Normen entscheiden darüber, ob auf einen Sachverhalt mit Auslandsberührung inländisches oder ausländisches Recht anzuwenden ist.⁸³ Stattdessen kann man auch jeder einzelnen Norm durch Auslegung entnehmen, in welchem Umfang sie auch auf Auslandssachverhalte angewendet sein will. Diese Technik ist im internationalen Wirtschaftsrecht üblich.⁸⁴ Letztlich spielt die Unterscheidung im öffentlichen Recht jedoch keine große Rolle. Ein selbstständiges Kollisionsrecht braucht man nämlich nur dann, wenn innerstaatliche Behörden oder Gerichte ermächtigt werden sollen, in manchen Auslandsfällen auch ausländisches Recht anzuwenden. Das steht beim MDStV nicht in Rede.

Der MDStV enthält keine expliziten Regeln über seinen internationalen Anwendungswillen. Deshalb muss man zu seiner Interpretation auf die parallelen Regeln im Privatrecht und im Strafrecht zurückgreifen. In beiden Rechtsgebieten ist die Frage lebhaft umstritten. Die international-privatrechtliche Diskussion war allerdings zentral mit einer anderen Klasse von Konflikten befasst. Ausgangspunkt der Diskussion ist die Grundregel des deutschen internationalen Deliktsrechts. Danach kann der Geschädigte an sich wählen, ob das Recht des Schädigers oder das Recht an dem Ort angewendet werden soll, an dem er geschädigt worden ist. Das ist ein vergleichsweise harmloses Problem. Mehr als zwei Rechtsordnungen kommen nur dann infrage, wenn der Geschädigte in Drittstaaten reist. Denn es geht dabei ja um bilaterale Konflikte. Typisch sind

76) S.o. 3.

77) S. erneut o. Fußn. 63.

78) *Reidenberg*, *Jurimetrics* 2002, dort bei Fußn. 66.

79) *U.S. District Court for the Northern District of California San Jose Division*, 11/7/2001, *Yahoo! Inc. v. La Ligue contre le racisme et l'antisémitisme*, <http://www.juris.com.net/en/txt/juris/ic/dccalifornia20011107.htm> (Stand: 16.4.2002).

80) *Widerspruchsbescheid* (o. Fußn. 39).

81) Rechtsvergleichend *Kübler*, in *Sitzungsberichte der Wissenschaftlichen Gesellschaft an der Johann Wolfgang Goethe-Universität Frankfurt/M.* 2000, S. 149 ff.; *Holzner*, *AfP* 2002, 128 ff.

82) Immer noch grundlegend *Neumeyer*, *Internationales Verwaltungsrecht*, 1936; s.a. jüngst *Linke*, *Europäisches Internationales Verwaltungsrecht*, 2001.

83) Einzelheiten etwa bei *Kropholler*, *Internationales Privatrecht*, 1997.

84) Grundlegend *Schnyder*, *Wirtschaftskollisionsrecht*, 1990.

Persönlichkeitsverletzungen. Selbst für diesen, viel einfacheren Fall ist aber lebhaft umstritten, ob und wie die Anwendbarkeit des Rechts am Erfolgsort eingeschränkt werden kann.⁸⁵

Das Strafrecht ist dagegen häufig mit den gleichen multi-polaren Konflikten befasst, die auch dem hier zu entscheidenden Fall zu Grunde liegen. Ja es gibt mit den Strafnormen gegen nationalsozialistische Äußerungen sogar ganz unmittelbare Parallelen. Der *Generalbundesanwalt*⁸⁶ und der *BGH*⁸⁷ haben hier zwei ausgesprochen problematische Entscheidungen gefällt. Sie sind dafür im Schrifttum zu Recht heftig kritisiert worden.

Grds. kennt das deutsche internationale Strafrecht mehrere alternative Anknüpfungsprinzipien. Für manche, besonders gravierende Straftaten gilt nach § 6 StGB das Weltrechtsprinzip. Die Vorschriften zum Schutz gegen nationalsozialistische Äußerungen fallen aber nicht darunter. Von den übrigen Prinzipien kommt nur § 3 i.V.m. § 9 Abs. 1 StGB in Betracht. Das deutsche Strafrecht gilt für Taten, die im Inland begangen worden sind. Das ist auch dann der Fall, wenn die Handlung zwar im Ausland stattfand, der tatbestandliche Erfolg aber im Inland eingetreten ist. Der *Generalbundesanwalt* hat den deutschen Erfolgsort einfach damit begründet, dass die fraglichen Inhalte vom Inland aus abgerufen werden können.⁸⁸ Der *BGH* war kaum vorsichtiger. Er hat einen australischen Staatsangehörigen verurteilt, weil er auf seinem australischen Server Äußerungen zum Abruf bereithält, die den Holocaust leugnen. Der *BGH* lässt für einen deutschen Erfolgsort genügen, dass die deutsche Öffentlichkeit wegen ihrer Geschichte besonders gefährdet sei.⁸⁹ Ähnliche Formulierungen finden sich nun auch in der Verfügung, mit der der *RP* die sofortige Vollziehung seiner Verfügung begründet.⁹⁰

Das kann nicht richtig sein.⁹¹ I.E. kommt es damit nämlich zu einem weltweiten Zuständigkeitsanspruch des deutschen Rechts. Im Schrifttum ist eine Vielzahl von Versuchen unternommen worden, dieses Ergebnis zu vermeiden. Ein deutscher Erfolgsort soll nur dann anzunehmen sein, wenn die Äußerungen spezifisch auf Deutschland zielen. Das wollen manche aus einem speziellen Angebot in deutscher Sprache ableiten.⁹² Andere verlangen den

Nachweis einer Absicht zur Wirkung in Deutschland.⁹³ Ein weiterer Vorschlag unterscheidet zwischen „push- und pull“-Technologien. Deutsches Strafrecht soll nur dann zur Anwendung kommen, wenn der Anbieter mit speziellen technischen Vorkehrungen dafür sorgt, dass sein Angebot in Deutschland auch tatsächlich wahrgenommen wird.⁹⁴ Ein letzter Vorschlag will darauf abstellen, ob die vom Tatbestand der Strafnorm umfasste abstrakte Gefährdung gerade „typischerweise“ im Inland eintritt.⁹⁵ Welcher dieser Vorschläge vorzugswürdig ist, braucht hier nicht entschieden zu werden. Auch die Suche nach noch besseren Lösungen kann unterbleiben. Denn zur Anwendbarkeit des deutschen Rechts könnte es im vorliegenden Fall nur kommen, wenn jegliche Einschränkung des Erfolgsorts abzulehnen wäre. Die Besonderheit der Ausgangsfälle liegt nämlich gerade darin, dass die Äußerung im Grunde nur über die Strafbarkeit nationalsozialistischer Äußerungen Bezug zu Deutschland hat. In seiner Anordnung der sofortigen Vollziehung seines Bescheids stellt der *RP* das ausdrücklich fest.⁹⁶

Dass dies nicht genügen kann, zeigt abschließend auch ein systematisches Argument. I.E. würde bei Internetäußerungen das Prinzip des Erfolgsorts dann nämlich durch das Weltrechtsprinzip ersetzt. In § 6 StGB gibt der Gesetzgeber aber eindeutig zu erkennen, dass das Weltrechtsprinzip für die Bestrafung nationalsozialistischer Äußerungen gerade nicht gelten soll. Für die Auslegung von § 22 Abs. 3 MDStV kann nichts anderes gelten.

c) Internationaler Anwendungsbereich der verwiesenen strafrechtlichen Normen

Zum gleichen Ergebnis führt auch noch ein zweiter dogmatischer Weg. Der *RP* hat die Unzulässigkeit der fraglichen Angebote mit einem Verstoß gegen § 8 Abs. 1 Nr. 1 und Nr. 2 MDStV a.F. begründet.⁹⁷ Diese Normen wiederholen nicht nur den Tatbestand von §§ 130 und 131 StGB. Vielmehr verweisen sie ganz offen auf diese strafrechtlichen Vorschriften. Da der MDStV keine expliziten Regelungen über seinen eigenen internationalen Anwendungsbereich enthält, liegt es nahe, diese Verweisungen nicht als bloße Sachrechtsverweisungen, sondern als Gesamtrechtsverweisungen zu interpretieren.⁹⁸ In einem Fall mit Auslandsberührung verlangt die Eingriffsgrundlage des § 22 Abs. 3 MDStV also zweierlei: Die sachlichen Tatbestandsmerkmale der §§ 130 oder 131 StGB müssen erfüllt sein; zugleich muss das deutsche Strafrecht auf den Auslandsfall aber auch anwendbar sein. In seiner Verfügung zur Anordnung der sofortigen Vollziehung seiner Bescheide sieht das mittlerweile auch der *RP* ausdrücklich so.⁹⁹

An sich führt dieser zweite dogmatische Weg natürlich zu denselben Überlegungen, die wir bereits angestellt haben. Um Aussagen zum internationalen Anwendungsbereich des MDStV selbst zu gewinnen, hatten wir ja gerade auf die parallelen Fragen im Strafrecht geblickt. Im Fall von §§ 130 und 131 StGB fällt die Entscheidung gegen ein implizites Weltrechtsprinzip nur besonders leicht. Denn bei einem anderen, verwandten Äußerungsdelikt ist der Strafgesetzgeber vor wenigen Jahren ausdrücklich zum Weltrechtsprinzip übergegangen. Dieser Straftatbestand ist ebenfalls Gegenstand einer Verweisung in § 8 Abs. 1 Nr. 4 MDStV a.F.¹⁰⁰ Es geht um pornografische Äußerungen. Nach § 6 Nr. 6 StGB gilt das Weltrechtsprinzip für solche pornografischen Äußerungen, die unter § 184 Abs. 3 oder Abs. 4 StGB fallen. Dazu gehören pornografische Schriften, die Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tie-

85) Zusammenfassend v. *Hinden*, Persönlichkeitsverletzungen im Internet, 1999.

86) *Generalbundesanwalt* MMR 1998, 93, 94.

87) *BGH* MMR 2001, 228.

88) *Generalbundesanwalt* MMR 1998, 93, 94.

89) *BGH* MMR 2001, 228.

90) Vfg. v. 6.9.2002: „Das Äußerungsdelikt des § 130 Abs. 1 StGB [...] will – wegen der besonderen Geschichte Deutschlands – dem Ingangsetzen einer historisch als gefährlich nachgewiesenen Eigendynamik entgegenwirken [...]. Ein besonderer Bezug des Leugnungstatbestands des § 130 Abs. 3 StGB zur Bundesrepublik Deutschland ergibt sich aufgrund der Einzigartigkeit der unter der Herrschaft des Nationalsozialismus an den Juden begangenen Verbrechen“.

91) Erstaunlicherweise fehlt bei *Spindler/Volkmann*, K&R 2002, 400 jedes Bewusstsein für die internationale Dimension des Problems.

92) *OLG Hamburg* MMR 2000, 92, 94; *Hilgendorf*, NJW 1997, 1876.

93) Vgl. o. Fußn. 92.

94) *Sieber*, NJW 1999, 2065 ff.; *Vec*, NJW 2002, 1538.

95) *Vassilaki*, CR 2001, 264.

96) Vfg. v. 6.9.2002.

97) Zu der – materiell nicht veränderten – Neufassung in § 12 Abs. 1 Nr. 1 MDStV s.o. Fußn. 75.

98) Die Unterscheidung stammt aus dem Internationalen Privatrecht, betrifft dort aber das Verhältnis verschiedener nationaler Rechtsordnungen, nicht verschiedener Rechtsgebiete innerhalb derselben Rechtsordnung, s. etwa *Kropholler* (o.Fußn. 83), § 24 Abs. 1.

99) Vfg. v. 6.9.2002.

100) Auch diese Norm ist – materiell unverändert – im neu gefassten § 12 Abs. 1 Nr. 1 MDStV aufgegangen, s.o. Fußn. 75.

ren zum Gegenstand haben. Diese Gesetzeslage legt einen Gegenschluss für §§ 130 und 131 StGB mehr als nahe: Für „hate speech“ gilt das Weltrechtsprinzip gerade nicht. Deshalb darf es auch nicht im Wege einer extensiven Interpretation des Erfolgsorts in § 9 Abs. 1 StGB hinein-gelesen werden.

Der *RP* hat sich allerdings nicht nur auf § 8 Abs. 1 Nr. 1 und Nr. 2 MDStV a.F. berufen, sondern „hilfsweise“ auch auf § 8 Abs. 1 Nr. 5 MDStV a.F.¹⁰¹ Danach sind Angebote in Mediendiensten unzulässig, wenn sie „offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden“. Die Begründungen, die der *RP* für dieses Tatbestandsmerkmal gibt, sind gewunden. Er kann keine Sachverhaltselemente anführen, die über das hinausgehen, was er schon unter § 8 Abs. 1 Nr. 1 und Nr. 2 MDStV a.F. verwertet. In dieser Lesart würde § 8 Abs. 1 Nr. 5 MDStV a.F. zur Generalklausel. Das hat der Gesetzgeber offensichtlich nicht so gemeint. Letztlich kann der Streit um die Interpretation von § 8 Abs. 1 Nr. 5 MDStV a.F. aber dahinstehen. Wenn dort nichts verwertet werden kann, was nicht zugleich auch unter § 8 Abs. 1 Nr. 1 und Nr. 2 MDStV a.F. fällt, dann muss der beschränkte internationale Anwendungsbereich von § 8 Abs. 1 Nr. 1 und Nr. 2 MDStV a.F. nämlich auch auf Nr. 5 der Vorschrift ausstrahlen.

d) Innerstaatliche Wirkung völkerrechtlicher Grenzen der Extraterritorialität

In welchem Umfang ein Staat auf den grenzüberschreitenden Charakter eines Sachverhalts Rücksicht nimmt, ist zunächst einmal seine eigene Angelegenheit. Seine autonome Gestaltungsfreiheit wird allerdings durch völkergewohnheitsrechtliche Regeln eingeschränkt. Das gewohnheitsrechtliche Nichteinmischungsgebot enthält Aussagen darüber, wieweit ein Staat mit der extraterritorialen Anwendung seines Rechts gehen darf.¹⁰² Völkerrechtlich kann ein Staat den Respekt vor der Souveränität anderer Staaten zwar weiter treiben. Hinter diesen gewohnheitsrechtlichen Grenzen darf er aber nicht zurückbleiben.

Zunächst einmal binden diese Sätze die Bundesrepublik allerdings nur im Verhältnis zu anderen Völkerrechtssubjekten. Deutschland geht, wie die meisten anderen Staaten auch, nämlich davon aus, dass Völkerrecht und Landesrecht zwei getrennte Rechtsordnungen sind. Im Ausgangspunkt gelten völkerrechtliche Regeln deshalb nur für die Bundesrepublik, nicht aber in der Bundesrepublik.¹⁰³ Dies ist aber nur der konzeptionelle Ausgangspunkt. In ihrem Verfassungsrecht hat sich die Bundesrepublik Deutschland autonom dafür entschieden, das Völkergewohnheitsrecht ohne weiteren Umsetzungsakt zum Inhalt des innerstaatlichen Rechts zu machen. Diese Entscheidung ist in Art. 25 GG enthalten. Nach ganz einhelliger Auffassung gehören zu den „allgemeinen Regeln des Völkerrechts“ jedenfalls die Regeln des Völkergewohnheitsrechts.¹⁰⁴ Sie gehen, wie es in Art. 25 und 2 GG heißt, den Gesetzen vor. Daraus leitet die h.M. ab, dass sie einen Rang zwischen einfachem Recht und Verfassungsrecht einnehmen.¹⁰⁵

Daraus folgt für den konkreten Fall: Die völkergewohnheitsrechtlichen Grenzen für die extraterritoriale Anwendung deutschen Rechts würden sich gegen einen weitergehenden internationalen Anwendungswillen von § 22 Abs. 3 MDStV durchsetzen.¹⁰⁶ Selbst wenn man den autonomen Anwendungswillen von § 22 Abs. 3 MDStV weiter ziehen wollte als gerade dargelegt, würde sich i.E. also nichts ändern. An die Stelle einer autonomen träte nur eine völkergewohnheitsrechtliche Begründung.

e) Völkerrechtliche Grenzen der Extraterritorialität

Dem *RP* fehlt jegliche Sensibilität für die völkerrechtliche Dimension des Sachverhalts.¹⁰⁷ Der *BGH* erwähnt die Notwendigkeit eines „völkerrechtlich legitimen Anknüpfungspunkts“ zwar. Er begnügt sich dann aber mit dem lapidaren Hinweis: „Denn die Tat betrifft ein gewichtiges inländisches Rechtsgut, das zudem objektiv einen besonderen Bezug auf das Gebiet der Bundesrepublik Deutschland aufweist“.¹⁰⁸

Das wird dem Entwicklungsstand des Völkergewohnheitsrechts nicht gerecht. Um die völkerrechtlichen Grenzen der extraterritorialen Anwendung nationalen Rechts gibt es eine jahrzehntelange literarische Diskussion.¹⁰⁹ Das Ergebnis dieser Diskussion ist in einem zwar nicht verbindlichen, aber doch allgemein als autoritativ anerkannten Text niedergelegt, dem „Restatement (Third) Foreign Relations Law of the United States“.¹¹⁰ Der Text unterscheidet drei Stufen. Auf der ersten Stufe steht mit Sec. 404 das Weltrechtsprinzip. Es ist aber nur für wenige Gegenstände eröffnet. Angesichts der fundamental abweichenden amerikanischen Verfassungstradition verwundert nicht, dass die Bestrafung von „hate speech“ nicht dazugehört. Auf der zweiten Stufe steht in Sec. 402 das Auswirkungsprinzip. Ein Staat darf sein nationales Recht auf Auslandssachverhalte erstrecken, wenn der Sachverhalt „substantial effects within its territory“ hat. Diese Befugnis wird auf der dritten Stufe allerdings durch Sec. 403 wieder eingeschränkt: „Even when one of the bases of the jurisdiction under [sec.] 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connection with another state when the exercise of jurisdiction is unreasonable“.¹¹¹

Von diesem Ausgangspunkt aus hat sich eine intensive Diskussion über die völkerrechtlichen Grenzen der Befugnis einzelner Staaten zur Inhaltskontrolle des Internet entwickelt.¹¹² Es besteht Einigkeit, dass die bloße Möglichkeit zum Abruf eines Inhalts nicht genügt, die völkerrechtliche Zuständigkeit des Staats zu begründen, von dem aus das

¹⁰¹ § 8 Abs. 1 Nr. 1 und 2 MDStV a.F. sind jetzt in § 12 Abs. 1 Nr. 1 MDStV n.F. aufgegangen. § 8 Abs. 1 Nr. 5 MDStV a.F. entspricht wörtlich § 12 Abs. 1 Nr. 3 MDStV n.F.

¹⁰² S. einstweilen nur *Meng*, Extraterritoriale Jurisdiktion im öffentlichen Wirtschaftsrecht, 1994, und näher sogleich e).

¹⁰³ Grundlegend *Bleckmann*, Grundgesetz und Völkerrecht, 1975, S. 264–341.

¹⁰⁴ Umstritten ist nur, ob darüber hinaus auch eine weitere völkerrechtliche Rechtsquelle umfasst ist; die allgemeinen Regeln des Völkerrechts, zusammenfassend etwa *Schweitzer*, Staatsrecht III, 2000, Rdnr. 470–487.

¹⁰⁵ Zusammenfassend *Schweitzer* (o. Fußn. 104), Rdnr. 479.

¹⁰⁶ Weitere Einzelheiten bei *Engel*, *RabelsZ* 1988, 275–286, insb. 278 f.

¹⁰⁷ Ebenso war es beim *Generalbundesanwalt* MMR 1998, 93, 94.

¹⁰⁸ *BGH* MMR 2001, 228, 231.

¹⁰⁹ Zusammenfassend *Ziegenhain*, Extraterritoriale Rechtsanwendung und die Bedeutung des Genuine-Link-Erfordernisses, 1992; *Meng* (o. Fußn. 102).

¹¹⁰ Zur Einschätzung des Texts unter Völkerrechtsjuristen s. etwa *Wilske/Schiller*, *Federal Communications Law Journal* 1997, 127; ebd. ist der Text der Norm auch abgedruckt.

¹¹¹ Bei *Wilske/Schiller*, *Federal Communications Law Journal* 1997, 124 f., 144–170, 172 f. finden sich differenzierte Überlegungen zu der weiteren völkergewohnheitsrechtlichen Unterscheidung zwischen der „jurisdiction to prescribe“, „jurisdiction to adjudicate“ und „jurisdiction to enforce“. Um Auslandsvollstreckung geht es hier jedoch nicht. Der *RP* nimmt zwar auch seine internationale Zuständigkeit in Anspruch. Das entscheidende Gravamen besteht jedoch in der Anwendung des deutschen Sachrechts auf den grenzüberschreitenden Sachverhalt. Darauf konzentrieren sich die folgenden Überlegungen deshalb.

¹¹² Besonders zu nennen sind *Ibid.* in; *Determann*, Kommunikationsfreiheit im Internet 1999, 134–197; *Bremer*, Strafbare Internetinhalte in internationaler Hinsicht, 2000; *Geist*, *Berkeley Technology Law Journal* 2001, 1345 ff.; *Bremer*, MMR 2002, 147 ff.

geschieht.¹¹³ Solch eine Lösung könnte auch Deutschland nicht wünschen. Es müsste sonst etwa mit der Bestrafung von Deutschen durch die türkischen Gerichte rechnen, wenn sie in Deutschland auf einer Website für ein freies Kurdistan werben.¹¹⁴ Ebenso würde es den Verlegern deutscher Frauenzeitschriften in arabischen Ländern gehen, wenn sie über ein erfülltes Sexualeben schreiben oder leicht bekleidete Models abbilden.

Auf welche Weise die Zuständigkeit nationaler Gerichte zur Regelung von Internetsachverhalten von Völkerrechts wegen beschränkt ist, ist noch nicht abschließend geklärt. Lange Zeit hat der von den amerikanischen Gerichten im Fall *Zippo* entwickelte Test¹¹⁵ erheblichen Zuspruch gefunden.¹¹⁶ Er unterscheidet im Kern zwischen dem aktiven Eindringen von Inhalten in ein fremdes Staatsgebiet und der bloß passiven Nutzung von dort aus.¹¹⁷ Alternativ wird auch ein sog. „Target-Test“ vorgeschlagen. Die völkerrechtliche Zuständigkeit eines Staats zur Regelung von Internetinhalten wäre eröffnet, wenn diese Inhalte spezifisch gerade auf die Bevölkerung dieses Landes abzielen.¹¹⁸

Welcher Test auch immer den Inhalt des Völkergewohnheitsrechts richtig wiedergibt: Die Entscheidung des *RP* enthält nicht genug Anhaltspunkte, um auf die völkerrechtliche Zuständigkeit der Bundesrepublik zur Regulierung der beiden Websites schließen zu können. Im Fall von <http://www.stormfront.org> stellt der *RP* sogar selbst fest, dass die Seite überwiegend Angebote in englischer Sprache bereithält.¹¹⁹ Dass der *RP* selbst Zweifel hat, ergibt sich auch aus der Formulierung: „hat das Gesamtangebot zugleich die Funktion einer Verteilerdrehzscheibe auch [sic!] für die deutsche rechtsextremistische Szene“. Die gleiche relativierende Formulierung findet sich auch bei der zweiten Website, zu der der *RP* den Zugang sperren möchte.

113) S. etwa *Wilske/Schiller*, *Federal Communications Law Journal* 1997, 139 f.; *Determann* (o. Fußn. 112), S. 158; *Koch*, *JuS* 2002, 124.

114) Das anschauliche Beispiel stammt von *Koch*, *JuS* 2002, 124.

115) *Zippo Manufacturing C. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa. 1997).

116) Einzelheiten bei *Geist*, *Berkeley Technology Law Journal* 2001, 1345 ff.; s.a. *Reidenberg*, *Jurimetrics* 2002, dort bei Fußn. 23.

117) Die zentrale Passage des Urteils lautet: „At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site, which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site“, 952 F.Supp. 1119, 1124; eine ausführliche Diskussion des Tests findet sich bei *Geist*, *Berkeley Technology Law Journal* 2001, 1345 ff. dort bei Fußn. 63–143.

118) *Wilske/Schiller*, *Federal Communications Law Journal* 1997, 141; *Geist*, *Berkeley Technology Law Journal* 2001, 1345 ff. dort bei Fußn. 205–305.

119) Zur Sprache als Indiz s. auch *Vassilaki*, *CR* 2001, 264.

120) *BVerfGE* 96, 68.

121) *BVerfGE* 96, 68.

122) *Engel-Flechsigt/Maennel/Tettenborn* (o. Fußn. 28), S. 17; *Spindler/Volkmann*, *K&R* 2002, 399.

123) *Determann* (o. Fußn. 112), S. 595.

124) Soweit sich TDG und MDStV widersprechen, geht schließlich auch das TDG nach Art. 31 GG vor, dazu näher unten 2 b).

125) Ausführliche Nw. bei *Fiedler*, *Die formale Seite der Äußerungsfreiheit*, 1999, S. 270–276; vgl. auch *Stadler*, *MMR* 2002, 343: § 22 Abs. 3 MDStV ist wegen der „Polizeifestigkeit der Presse“ verfassungswidrig.

126) So will *Stadler*, *MMR* 2002, 343 vorgehen; allgem. zu den Grenzen des Pressebegriffs etwa *Bullinger/Mestmäcker*, *Multimediendienste*, 1997, S. 61–65.

f) Verfahrensrechtliche Folgen

Es mag sein, dass sich bei einer sorgfältigeren Analyse des Sachverhalts schließlich ein genügender völkerrechtlicher Anknüpfungspunkt für die deutsche Regulierung der beiden Websites oder wenigstens von Teilen ihres Angebots findet. Angesichts der Ungewissheit über den genauen Inhalt der einschlägigen völkergewohnheitsrechtlichen Norm könnte das Verwaltungsgericht diese Entscheidung aber nicht einfach selbst treffen. Denn die Unsicherheit über den genauen Inhalt völkergewohnheitsrechtlicher Normen ist ein allgemeines Problem. Die Verfassung hat darauf mit Art. 100 Abs. 2 GG reagiert. Von der Parallelvorschrift in Art. 100 Abs. 1 GG unterscheidet sich diese Norm in einer maßgeblichen Hinsicht. Das erkennende Gericht ist nicht erst dann zur Vorlage an das *BVerfG* verpflichtet, wenn es eine Norm des einfachen deutschen Rechts unangewendet lassen will. Vielmehr besteht die Vorlagepflicht bereits dann, wenn begründete Zweifel am genauen Inhalt der Regeln des Völkergewohnheitsrechts bestehen.¹²⁰ Verstößt das erkennende Gericht gegen die Vorlagepflicht, verletzt es den verfassungsrechtlichen Anspruch der Parteien des Prozesses auf den gesetzlichen Richter.¹²¹ Allein aus diesem Grunde müsste das Urteil des Verwaltungsgerichts dann aufgehoben werden.

III. Materielles Recht

Der *RP* stützt seine Verfügungen auf § 22 Abs. 2 und Abs. 3 MDStV. Man kann sich schon fragen, ob das die richtige Eingriffsgrundlage ist (1.). Auch die sachliche Anwendbarkeit der Norm ist nicht zweifelsfrei (2.). Vorausgesetzt ist weiter die Rechtmäßigkeit des Eingriffs gegen den primär Verantwortlichen (3.). Der subsidiäre Eingriff gegen Access-Provider steht unter strengen, zusätzlichen Voraussetzungen (4.). Insbesondere sind die Grenzen eines Vorgehens gegen Nichtstörer zu beachten (5.). Weitere Beschränkungen ergeben sich aus den Grundrechten der Access-Provider selbst (6.) sowie außenstehender Dritter (7.). Manche dieser Grundrechte haben benannte Schranken (8.). Schließlich müsste der Eingriff geeignet sein. In der Dogmatik von § 22 Abs. 3 MDStV entspricht dem die technische Möglichkeit einer Verhinderung des Zugriffs (9.). Der Eingriff muss außerdem erforderlich (10.) sowie angemessen sein (11.). Letzterem entspricht in der Dogmatik von § 22 Abs. 3 MDStV der Maßstab der Zumutbarkeit.

1. Eingriffsgrundlage

Der *RP* stützt seine Entscheidung auf § 22 Abs. 2 und Abs. 3 MDStV. Die Norm ist eine Ermächtigungsgrundlage.¹²² In ihrem Anwendungsbereich geht sie als *lex specialis* der Generalklausel des Polizeirechts vor.¹²³ Bis hierhin liegen die Dinge einfach. Und doch ist zweifelhaft, ob § 22 Abs. 3 MDStV überhaupt als Eingriffsgrundlage zur Verfügung steht. Zwei Gruppen von Vorschriften erweisen sich bei näherem Zusehen nämlich als vorrangig: die Vorschriften über die Pressebeschlagnahme (a) und die Vorschriften zum Schutz der wehrhaften Demokratie (b).¹²⁴

a) Vorrang der Vorschriften über die Pressebeschlagnahme

Würde es sich bei den problematischen Inhalten nämlich um Pressezeugnisse i.S.d. Vorschriften der StPO über die Pressebeschlagnahme handeln, wären diese Vorschriften abschließend.¹²⁵ Das führt scheinbar zu einem Qualifikationsproblem: Welche Inhalte des Internet sind als „elektronische Presse“ zu begreifen?¹²⁶ Schon die genaue Lek-

türe der Kette des § 111m Abs. 1 StPO und der §§ 74d Abs. 1, 11 Abs. 3 StGB zeigt aber, dass der Anwendungsbereich der Sondervorschriften für die Pressebeschlagnahme weiter zu ziehen ist. Ihr stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen gleich. Erst recht erweist sich das scheinbare Qualifikationsproblem als irrelevant, wenn man sich den verfassungsrechtlichen Hintergrund der strafprozessualen Vorschriften über die Pressebeschlagnahme vor Augen führt.¹²⁷ Sie sind Ausdruck der „Polizeifestigkeit“ der Medien.¹²⁸ Dieser althergebrachte Rechtsbegriff ist das einfachrechtliche Äquivalent des verfassungsrechtlichen Zensurverbots.¹²⁹ Auch dann, wenn ein Medieninhalt i.E. tatsächlich rechtswidrig ist, versagt das Zensurverbot dem Staat das präventive Einschreiten.¹³⁰ Nur repressive Maßnahmen sind möglich. § 111n StPO legt sie im Regelfall in die Hand des Richters. Nicht einmal zur Vorbereitung des Strafverfahrens darf die Exekutive im Regelfall also tätig werden.

Streiten kann man deshalb allenfalls darum, ob § 22 Abs. 3 MDStV tatsächlich unter das Zensurverbot aus Art. 5 Abs. 1 Satz 3 GG fällt.¹³¹ Das BVerfG legt den Begriff der Zensur eng aus: „Als Vor- oder Präventivzensur werden einschränkende Maßnahmen vor der Herstellung oder Verbreitung eines Geisteswerks, insb. das Abhängigmachen von behördlicher Vorprüfung und Genehmigung seines Inhalts (Verbot mit Erlaubnisvorbehalt) bezeichnet“.¹³²

Immerhin beschreibt das Gericht die Grenze zur Nachzensur aber wie folgt: „Ist das Geisteswerk erst einmal an die Öffentlichkeit gelangt und vermag es Wirkung auszuüben“, so liegt keine Vorzensur mehr vor.¹³³

Nach der Auffassung des *Gerichts* schützt das Zensurverbot nicht vor den Vorwirkungen nachträglicher repressiver Maßnahmen. „Es bleibt der Entscheidung des Einzelnen überlassen, ob er dieses Risiko eingeht, während eine Zensur verhindern würde, dass sich eine Risikobereitschaft überhaupt bilden kann“.¹³⁴

In einer späteren Entscheidung hat das *Gericht* außerdem offen gelassen, ob ein staatliches Verfahren allein wegen „seiner praktischen Auswirkungen“ unter das Zensurverbot fallen kann.¹³⁵

Andererseits beschreibt das *Gericht* das Telos des Zensurverbots wie folgt: „Schon die Existenz eines derartigen Kontroll- und Genehmigungsverfahrens lähmt das Geistesleben. Das Zensurverbot soll die typischen Gefahren einer solchen Präventivkontrolle bannen“.¹³⁶

Auch in unserem Fall kann es zu einer lähmenden Kommunikationsbehinderung kommen.¹³⁷ Das wird besonders deutlich, wenn man die beabsichtigten Vorwirkungen auf künftige Fälle beachtet. Der *RP* will die Verbreitung nationalsozialistischen Gedankenguts im Internet für die Access-Provider so riskant machen, dass sie den Zugang von sich aus unterbinden.

Vor allem wird die formale Unterscheidung zwischen Vor- und Nachzensur der Eigenheit der Internet-Kommunikation gleich aus zwei Gründen nicht gerecht. Die typische Form der Nutzung ist nämlich der Abruf von Diensten, die jemand zuvor ins Netz gestellt hatte. Ein „nachträglicher“ staatlicher Eingriff hat im Internet deshalb viel gravierendere publizistische Wirkungen als bei dem Medium, für das die Unterscheidung entwickelt worden ist. Schlägt die *Ordnungsbehörde* die bereits erschienene Zeitung auf und leitet aus einem Artikel eine Gefahr für die öffentliche Sicherheit ab, ist ihr Eingreifen nun keine Vorzensur mehr.¹³⁸

Das lässt sich rechtfertigen. Denn bekanntlich ist nichts so alt wie die Zeitung von gestern. Die eigentliche Wirkungschance hat die Zeitung also bereits gehabt. Durch die Beschlagnahme wird höchstens dem kleinen Rest der Auflage seine Wirkungschance genommen. Aus dem gleichen Grunde spielt die Zensur beim Rundfunk keine Rolle. Hier ist das Verbot der Vorzensur praktisch gleichbedeutend mit dem Verbot jeder Zensur. Ganz anders im Internet, genauer im WWW. Hier liegt ganz regelmäßig ein zeitlicher Zwischenraum zwischen Äußerung und Wahrnehmung. Wichtiger: Die Wahrnehmung ist typischerweise zeitlich gestreckt. Verschiedene Nutzer nehmen die Inhalte zu verschiedenen Zeiten wahr. Praktisch bedeutet das, wenn man den Begriff der Nachzensur genauso interpretiert wie bei der Presse, hat man das kategorische Zensurverbot beiseite gelassen.¹³⁹ Beim näheren Zusehen sieht das wohl auch das BVerfG so. Es hat die Unterscheidung zwischen Vor- und Nachzensur nämlich wie folgt begründet: „Ist das Geisteswerk erst einmal an die Öffentlichkeit gelangt und vermag es Wirkung auszuüben, genügt der Schutz aus Art. 5 Abs. 2 GG“.¹⁴⁰ Genau an dieser realistischen Wirkungschance würde es fehlen, wenn jede Intervention nach dem Stellen der Inhalte ins Netz bereits Nachzensur wäre.¹⁴¹ Die Interpretation von Art. 5 Abs. 1 Satz 3 GG muss also an die Veränderungen der technischen und publizistischen Verhältnisse angepasst werden.¹⁴²

b) Vorrang der Vorschriften zum Schutz der wehrhaften Demokratie

Ein strukturell verwandter Zusammenhang ist bislang weniger gut ausgearbeitet. Wenn der Staat nach § 22 Abs. 3 MDStV vorgeht, greift er in die Äußerungsfreiheit der Content-Provider aus Art. 5 Abs. 1 GG ein.¹⁴³ Dieser Eingriff bedarf der Rechtfertigung durch die benannten Schranken aus Art. 5 Abs. 2 GG. Dafür kommt nur die Schranke der „allgemeinen Gesetze“ in Betracht. Ein Gesetz ist kein allgemeines im Sinne dieser Vorschrift, wenn es sich gegen die Äußerung bestimmter Meinungen als solche richtet.¹⁴⁴ Genau dagegen verstößt der *RP*. Er hebt ganz offen

127) So ausdrücklich *Fiedler*, Meinungsfreiheit in der vernetzten Welt, 2002, S. 62 ff.

128) *Ladeur*, NJW 1986, 2749; *Ladeur*, ZUM 1997, 382; *Fiedler* (o. Fußn. 125), S. 291 ff.

129) Grundlegend zum Zensurverbot *Fiedler* (o. Fußn. 125).

130) Das ist unstrittig, s. nur BVerfGE 33, 52, 71 f.

131) Bejahend *Jäger/Collardin*, CR 1996, 240; *Hoffmann-Riem/Schulz* (o. Fußn. 19), S. 149 f.; *Ladeur*, ZUM 1997, 382; *Schulz*, MMR 1998, 184 f.; *Fiedler* (o. Fußn. 127), S. 63 f.; a.A. *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, S. 432 f.

132) BVerfGE 33, 52, 72; s.a. dazu *Hopf*, ZUM 2000, 740.

133) BVerfGE 33, 52, 72.

134) BVerfGE 33, 52, 73.

135) BVerfGE 87, 209, 232.

136) BVerfGE 33, 52, 72.

137) Davon machen *Fiedler* (o. Fußn. 125), S. 100–140 u. 306 und *Hopf*, ZUM 2000, 742 den Zensurbegriff abhängig.

138) Aus den oben in 1. dargelegten Gründen wäre der Eingriff gleichwohl rechtswidrig. Denn möglich ist allein die Beschlagnahme durch die Staatsanwaltschaft in dem strengen Verfahren der StPO.

139) Erstaunlich *Spindler/Volkman*, K&R 2002, 407. Sie schreiben ausdrücklich, die Veröffentlichungschance bestehe im Internet nur für eine „logische Sekunde“, halten das aber nicht für ein Rechtsproblem.

140) BVerfGE 33, 52, 72.

141) Vgl. auch *Fiedler* (o. Fußn. 125), S. 305, der Zensur annimmt, „je früher innerhalb der Verbreitungskurve“ der Staat eingreift.

142) Wer dem nicht folgen wollte, müsste die Zensurnähe der Maßnahme jedenfalls bei der Anwendung des Verhältnismäßigkeitsgrundsatzes berücksichtigen. Sie würde das Schutzniveau der Äußerungsfreiheit erhöhen. Das gehört systematisch nur nicht an diese Stelle, s.u. III. 1.

143) Zu weiteren Grundrechten, insb. zu der Äußerungsfreiheit der Access-Provider, s. näher unten 6 a).

144) St. Rspr., s. nur BVerfGE 47, 198, 232.

auf den nationalsozialistischen Gehalt der Äußerungen ab. Die meisten Kommentatoren behandeln die Vorschriften gegen nationalsozialistisches Gedankengut wie die Lebenslüge von Art. 5 Abs. 2 GG. Sie finden irgendeinen durchsichtigen Grund, warum das angeblich doch allgemeine Gesetze sein sollen.¹⁴⁵ Die Parallele zum Zensurverbot und zur Pressebeschlagnahme legt eine sauberere Lösung nahe. Die Schranke der allgemeinen Gesetze in Art. 5 Abs. 2 GG steht in einem verfassungsinternen Spannungsverhältnis zu den Vorschriften über die wehrhafte Demokratie. Dieser Konflikt ist im Wege der praktischen Konkordanz aufzulösen. Das gelingt auf folgendem Wege: Ein Vorgehen gegen konkrete Meinungen ist gerade und nur dann verfassungsrechtlich zulässig, wenn die Staatsgewalt die besonderen Verfahren zum Schutz der wehrhaften Demokratie nutzt. Sie darf gegen die Äußerung also nur dann einschreiten, wenn das *BVerfG* zuvor nach Art. 21 Abs. 2 GG die Partei verboten hat. Dem steht gleich, dass eine Vereinigung nach Art. 9 Abs. 2 GG und den §§ 3 bis 9 VereinsG verboten worden ist. Ebenfalls steht gleich, dass das *BVerfG* nach Art. 18 GG festgestellt hat, ein Individuum habe die Freiheit der Meinungsäußerung zum Kampf gegen die freiheitlich demokratische Grundordnung missbraucht. Nichts davon ist hier geschehen. Deshalb bindet das Verbot des Vorgehens gegen konkrete politische Meinungen aus Art. 5 Abs. 2 GG.

2. Sachlicher Anwendungsbereich

§ 22 Abs. 3 MDStV steht also von vornherein als Eingriffsgrundlage gar nicht zur Verfügung. Nur um des Arguments willen wollen wir im Folgenden das Gegenteil unterstellen

145) Anschaulich etwa *Starck*, in: von Mangoldt/Klein/Starck, Das Bonner GG, Bd. I, 1999, zu Art. 5 GG, Rdnr. 233: kein allgemeines Gesetz, weil strafbar – dann hätte es der einfache Gesetzgeber in der Hand, die Schranke der allgemeinen Gesetze zu umgehen, indem er zunächst Strafnormen schafft.

146) *Determann* (o. Fußn. 112), S. 522; *Spindler/Volkman*, K&R 2002, 399; *Stadler*, MMR 2002, 344; vgl. auch *Germann* (o. Fußn. 131), S. 128 und 165–168: Damit es sich um einen Teledienst handelt, muss ein „Kommunikations-Mehrwert“ hinzutreten; *Popp* (o. Fußn. 37), S. 57 u. 59–61 verwendet als Abgrenzungskriterium das „Nicht-nur-der-Verbindungsherstellung-Dienen“; vgl. schließlich auch *Koenig/Loetz*, CR 1999, 438 ff. dort bei Fußn. 39; a.A. *Pankoke*, Von der Presse- zur Providerhaftung, 2000, S. 38 f.: § 5 TDG wollte eine umfassende Privilegierung erreichen, weshalb selbst Router und Gateways unter das Gesetz fallen.

147) S. oben II. 6. a).

148) Darauf weist auch BT-Drs. 14/1191 (LuKDG-Bericht), S. 8 hin; vgl. auch *Determann* (o. Fußn. 112), S. 575: Das TDG enthält keine § 22 Abs. 3 MDStV vergleichbare Ermächtigungsgrundlage, weil dem Bund dafür die Gesetzgebungskompetenz fehlen würde. Das kann man allerdings mit guten Gründen bezweifeln. So enthalten die Umweltgesetze des Bundes regelmäßig Ermächtigungsgrundlagen, obwohl sie funktional besonderes Polizeirecht darstellen.

149) *Maennel*, in: Beck'scher LuKDG-Komm., § 5 MDStV, Rdnr. 3; § 5 TDG, Rdnr. 20.

150) Näher *Germann* (o. Fußn. 131), S. 385–400.

151) Widerspruchsbescheid (o. Fußn. 39).

152) Übersehen bei *Stadler*, MMR 2002, 344; anders *Spindler/Volkman*, K&R 2002, 399 – die dort nachgewiesenen Absichten aus der Entstehungsgeschichte stehen dieser Interpretation der Norm jedoch nicht entgegen.

153) Anders *Stadler*, MMR 2002, 344 und anscheinend *Koenig/Loetz*, CR 1999, 438 ff. dort bei Fußn. 52.

154) Richtig *Spindler/Volkman*, K&R 2002, 400.

155) Beide Argumente finden sich im Widerspruchsbescheid, s.o. Fußn. 39.

156) Vgl. BT-Drs. 14/1191 (LuKDG-Bericht), 21: Die Abgrenzung hat „zu erheblicher Rechtsunsicherheit bei Anbietern und Nutzern“ geführt.

157) Teledienst: BT-Drs. 13/7385, Begr. zu § 2 Abs. 2 Nr. 2 TDG; *Engel-Flechsigt/Maennel/Tettenborn* (o. Fußn. 28), S. 11; in der Regel Teledienst: von *Heyl*, ZUM 1998, 116 und 119; i.d.R. Mediendienst: *Holznapel* (o. Fußn. 4), Rdnr. 54; Zuordnung im Einzelfall: *Kröger/Moos*, AfP 1997, 679; Mediendienst wenn redaktionell gestaltet: *Determann* (o. Fußn. 112), S. 533 f.; Mediendienst, wenn „Meinungsrelevanz“ vorhanden: *Wimmer/Michael* (o. Fußn. 4), S. 40; Mediendienst, wenn Element einer „elektronischen Bibliothek“: *Germann* (o. Fußn. 131), S. 169; Mediendienst, wenn kommerziell betrieben *Lent*, Rundfunk-, Medien-, Teledienste, 2001, S. 153; je nach Inhalt unterschiedlich *Zimmermann*, NJW 1999, 3146.

und die Anwendungsvoraussetzungen der Vorschrift beleuchten. Unklar ist zunächst ihr sachlicher Anwendungsbereich. Zweifel ergeben sich einmal im Verhältnis zum Telekommunikationsgesetz (TKG) (a), zum anderen im Verhältnis zum TDG (b).

a) Abgrenzungen zum TK-Recht

Im Schrifttum findet sich manchmal die These, reine Access-Provider seien Anbieter von TK-Dienstleistungen i.S.d. TKG.¹⁴⁶ Ob das richtig ist, kann jedoch offen bleiben. Denn an dieser Stelle bekommt erneut ein Umstand Bedeutung, den wir bereits verwendet haben. § 22 Abs. 3 MDStV erweitert subsidiär nur den Kreis der Adressaten. Für Fragen der Qualifikation kommt es deshalb nicht auf die Einordnung des Access-Providers an. Abzustellen ist vielmehr auf die Einordnung des Inhalts, gegen den sich der staatliche Eingriff richtet.¹⁴⁷ Das sind die beiden amerikanischen Websites mit nationalsozialistischen Inhalten. Sie sind zweifelsfrei keine TK-Dienstleistungen.

b) Abgrenzung zum TDG

Sehr viel schwieriger ist die Abgrenzung zwischen dem MDStV der Länder und dem TDG des Bundes. Die Abgrenzung ist praktisch bedeutsam, weil das TDG keine dem § 22 Abs. 3 MDStV vergleichbare Vorschrift enthält.¹⁴⁸ Mit der wörtlich identischen Vorgängernorm aus § 18 Abs. 3 MDStV a.F. haben sich die Länder im Gesetzgebungsverfahren nämlich einseitig über die mit dem Bund abgestimmte Fassung hinweggesetzt.¹⁴⁹ Wenn der Sachverhalt unter das TDG fiele, käme als Ermachtigungsgrundlage allenfalls die Generalklausel des allgemeinen Polizeirechts in Betracht.¹⁵⁰ Darauf stützt sich der *RP* in seinem Widerspruchsbescheid nun auch ausdrücklich hilfsweise.¹⁵¹ Wir werden sehen, dass der Unterschied i.E. nicht groß ist. Denn § 22 Abs. 3 MDStV wird sich als spezielle Vorschrift über die polizeiliche Nichtstörerhaftung erweisen. Immerhin wird im Anwendungsbereich des TDG aber der Begründungsaufwand und der Streitstoff kleiner.

Bei der Abgrenzung zwischen TDG und MDStV ist zunächst erneut der Untersuchungsgegenstand richtig zu wählen. Gelegentlich wird bestritten, dass ein Access-Provider selbst einen Teledienst anbietet. Das ergibt sich jedoch aus § 2 Abs. 2 Nr. 3 TDG.¹⁵² Vor allem kommt es für die Anwendung von § 22 Abs. 3 MDStV aber gar nicht auf den Streit an.¹⁵³ Entscheidend für die subsidiäre Inanspruchnahme des Access-Providers ist vielmehr, ob der Dienst unter den MDStV fällt, der Anlass zum Einschreiten gegeben hat.¹⁵⁴ Aus diesem Grunde liegen die umfangreichen Ausführungen des *RP* zur Qualifikation der Access-Provider als Mediendienst von vornherein neben der Sache. Das hätte dem *RP* eigentlich auch auffallen müssen. Denn seine Argumente sind an dieser Stelle besonders fadenscheinig. Er will allein darauf abstellen, dass die Access-Provider technische Protokollfunktionen übernehmen. Der relevante Unterschied zur Post oder einem TK-Unternehmen soll allein darin liegen, dass die nachgefragten Websites öffentlich zugänglich sind.¹⁵⁵

Die Abgrenzung zwischen TDG und MDStV führt in einen dogmatischen Irrgarten.¹⁵⁶ Auch die Neufassungen des TDG und des MDStV beseitigen die Rechtsunsicherheit nicht. Deshalb wollen wir diesen Streit im Folgenden, wenn auch nur knapp, nachzeichnen.

Ob einzelne Websites ein Teledienst sind oder ein Mediendienst, ist lebhaft umstritten.¹⁵⁷ Dieser Streit könnte in künftigen Fällen eine Rolle spielen, wenn der *RP* sich dann

tatsächlich einzelne Websites vornehmen würde. Das gegenwärtige Verfahren richtet sich aber gegen zwei Websites, die in koordinierter Weise Zugang zu einer Fülle weiterer Angebote organisieren.

Nach welchen Gesichtspunkten sich die Qualifikation solcher Portale oder Webhosts richtet, ist noch weitgehend ungeklärt. Drei Vorfragen sind miteinander verschränkt: Ist ein Webhost selbstständig zu qualifizieren, oder folgt seine Qualifikation der Qualifikation der fremden Inhalte, die er zur Nutzung bereithält? Kann ein und derselbe Dienst je nach Regelungsgegenstand unterschiedlich qualifiziert werden oder ist die Qualifikation einheitlich vorzunehmen?¹⁵⁸ Schließen sich MDStV und TDG gegenseitig aus, oder können sie ggf. nebeneinander angewendet werden?

Von der letzten Frage her lässt es sich auflösen. Die Entstehungsgeschichte legt zwar nahe, dass sich Bund und Länder bei ihren Verhandlungen nicht vollständig haben einigen können.¹⁵⁹ Gleichwohl haben Bund und Länder das TDG und den MDStV in Kraft gesetzt. Sie haben dabei erklärt, dass sie „einen in der Sache einheitlichen Rechtsrahmen in Form eines Bundesgesetzes und eines Länderstaatsvertrags“ geschaffen haben, der zu einer „Aufteilung“ der Rechtsmaterie geführt hat.¹⁶⁰ Es ist nun Sache der Interpreten, die Abgrenzungsaufgabe zu Ende zu führen.¹⁶¹

Die Abgrenzungsaufgabe wird einfacher, wenn der Interpret Möglichkeiten zur Trennung nutzt. Dann braucht der Geltungswille des TDG nämlich nicht mehr als unvermeidlich hinter dem konkurrierenden Geltungswillen des MDStV zurückzutreten und umgekehrt. Die Möglichkeiten zur Trennung sind größer, wenn Webhosts nicht selbstständig qualifiziert werden, sondern nach Maßgabe der fremden Inhalte, die sie zur Nutzung bereithalten. Praktisch kann die Frage insb. dann werden, wenn ein Webhost auf einer einheitlichen Benutzeroberfläche Dienste unterschiedlicher Qualität bereithält. So mag er etwa virtuelle Bankgeschäfte ermöglichen; das ist eindeutig ein Teledienst. Auf der gleichen Oberfläche könnte er aber auch Zugang zu Nachrichten über die Finanzmärkte eröffnen; das wäre ein Mediendienst. Beide Dienste könnten ohne weiteres getrennt reguliert sein. Will ein Regulator nicht gegen die Inhalteanbieter vorgehen, sondern gegen den Webhost, würde sich das im ersten Fall nach dem TDG richten, im zweiten Fall nach dem MDStV.

Diese Trennungslösung stößt nur dann an eine Grenze, wenn das Angebot des Webhosts nur einheitlich beurteilt werden kann. Das kommt im Grunde aber nur dann in Betracht, wenn der Webhost gerade durch das Zusammenführen der unterschiedlichen fremden Inhalte eine selbstständige publizistische Aussage macht. Auch dann muss es aber bei der Unterscheidung zwischen der Verantwortlichkeit für eigene und für fremde Inhalte bleiben. Sie ist ja nach den §§ 8–11 TDG n.F. und nach §§ 6–9 MDStV n.F. für beide Regelwerke prägend.¹⁶² Auch in diesem Fall wird deshalb nicht das gesamte Angebot zu einem Mediendienst. Vielmehr ist der Webhost dann für die eigene publizistische Aussage aus der Zusammenführung fremder Inhalte nach § 6 Abs. 1 MDStV n.F. verantwortlich. Insoweit handelt es sich dann um einen Mediendienst. Auch dann bleibt es i.Ü. aber bei der Trennungslösung.

Soll der Webhost nicht wegen seiner eigenen publizistischen Aussage in Anspruch genommen werden, sondern wegen des Bereithaltens fremder Inhalte, richtet sich die Qualifikation erneut nach dem Inhalt dieser Angebote. Ist

der problematische Teil des Buketts selbst ein Teledienst, ist der Webhost dann wegen der eigenen publizistischen Aussage aus der Zusammenstellung nach § 6 Abs. 1 MDStV n.F. verantwortlich, wegen der verwiesenen fremden Inhalte dagegen nach § 8 Abs. 2 TDG n.F.

Die Schilderung des Sachverhalts in der Verfügung des RP ist spärlich. Sie lässt nicht erkennen, ob der eigentliche Anlass zur Intervention gerade in einer selbstständigen publizistischen Aussage der beiden Webhosts durch die Zusammenstellung des Materials liegt. Vermutlich kommt es für die Qualifikation deshalb auf die einzelnen bereitgehaltenen fremden Inhalte an. Hier ist die Sachverhaltsschilderung noch spärlicher. Deshalb können im Folgenden nur die Kriterien für die Qualifikation aufbereitet werden. Für eine Subsumtion genügen die Angaben nicht.

Diese Kriterien sind lebhaft umstritten.¹⁶³ Vorgeschlagen werden insb.¹⁶⁴ die folgenden Abgrenzungskriterien: Eine erste Ansicht setzt Mediendienste mit Massenkommunikation gleich, Teledienste mit Individualkommunikation.¹⁶⁵ Das kann jedoch nicht richtig sein. Denn stilprägend für das Internet sind ja gerade Abrufdienste, die sich zwar an die Allgemeinheit richten, aber individuell genutzt werden.¹⁶⁶ Sie oszillieren also gerade zwischen Individual- und Massenkommunikation. Das gleiche Problem stellt sich auch bei einem zweiten Abgrenzungskriterium.¹⁶⁷ Es will all die Angebote zu den Mediendiensten rechnen, die sich „an die Allgemeinheit richten“.¹⁶⁸

Handhabbar wäre ein drittes Kriterium. Es stellt auf die Meinungsrelevanz des fraglichen Dienstes ab.¹⁶⁹ Es

158 Waldenberger, MMR 1998, 125: stets einheitlich zu qualifizieren; Zimmermann, NJW 1999, 1346; Pankoke (o. Fußn. 146), S. 30–32, insb. 31: ist eine Frage des Einzelfalls.

159 BT-Drs. 13/7385 (Amtl. Begr. zum IuKDG, Stellungnahme des Bundesrats, Nr. 1); Bröhl, CR 1997, 74; Kröger/Moos, AfP 1997, 680; Sieber, MMR 1999, 199 ff. dort bei Fußn. 14; vgl. auch Determann (o. Fußn. 112), S. 530–534 und Maunz/Dürig-Lerche, GG, Art. 87 f, Rdnr. 52, 78 u. 109.

160 Erklärung von Bund und Ländern v. 18.12.1996, LT-Drs. NRW 12/1954, 24, zitiert nach Engel-Flechsigt/Maennel/Tettenborn (o. Fußn. 28), S. 9.

161 Sieber, MMR 1999, bei Fußn. 14; Holznel (o. Fußn. 4), Rdnr. 45, 49; vgl. auch die folgenden Autoren, die betonen, dass sich TDG und MDStV gegenseitig ausschließen: Engel-Flechsigt/Maennel/Tettenborn (o. Fußn. 28), S. 12; Roßnagel, NVwZ 1998, 3; Germann (o. Fußn. 131), S. 152 f.

162 Vor der Neufassung beider Normwerke waren die einschlägigen Vorschriften in den §§ 5 TDG und 5 MDStV enthalten. Darauf bezieht sich auch der Großteil der Lit.

163 Manche Formeln sind nichtssagend: BT-Drs. 14/1191 (IuKDG-Bericht), 6: „ausschließlich funktionsbezogen nach dem inhaltlichen Schwerpunkt des einzelnen Angebots“; ebd. 7: „auf pragmatische und entwicklungssoffene Handhabung angelegt“; Engel-Flechsigt/Maennel/Tettenborn (o. Fußn. 28), S. 11: „funktionelle Betrachtung“.

164 S. außerdem: Für welches Offline-Angebot ist der Dienst ein „virtuelles Spiegelbild“? Lent (o. Fußn. 157), S. 134 dort bei Fußn. 491, 153, 154, 155: Teledienste sind nur kommerzielle Dienste; dem steht § 2 Abs. 3 TDG aber klar entgegen; a.A. auch Engel-Flechsigt/Maennel/Tettenborn (o. Fußn. 28), S. 11.

165 BT-Drs. 13/7385 (Amtl. Begr. IuKDG), Begr. A und Begr. zu § 2 Abs. 2 Nr. 1 TDG; BT-Drs. 14/1191 (IuKDG-Bericht), 7; Kröger/Moos, AfP 1997, 677; s.a. den Bericht bei von Heyl, ZUM 1998, 118; vgl. auch Mayer, Das Internet im öffentlichen Recht, 1999, S. 186 ein Mediendienst ist „Massenkommunikation mit meinungsprägendem Charakter“; Holznel (o. Fußn. 4), Rdnr. 45: ausschlaggebend für einen Teledienst ist die „individuelle Nutzung“.

166 Determann (o. Fußn. 112), S. 530; vgl. auch Holznel (o. Fußn. 4), Rdnr. 45: die Abgrenzung ist schwierig, wenn die Öffentlichkeit nur aus einer definierten Zielgruppe besteht.

167 So zu Recht von Heyl, ZUM 1998, 117.

168 Wimmer/Michael (o. Fußn. 4), S. 36–38; Holznel, ZUM 1999, 427; Zimmermann, NJW 1999, 3146; Spindler, in: Hoeren und Sieber (o. Fußn. 4) Kap. 29, Rdnr. 43; Lent (o. Fußn. 157), S. 149; vgl. auch BT-Drs. 13/7385 (Amtl. Begr. IuKDG, Gegenäußerung der Bundesregierung), Nr. 1 b.

169 BT-Drs. 14/1191 (IuKDG-Bericht), 7; Holznel, ZUM 1999, 427; Zimmermann, NJW 1999, 3146; Spindler (o. Fußn. 168), Rdnr. 81; vgl. auch Engel-Flechsigt/Maennel/Tettenborn (o. Fußn. 28), S. 13.

stimmt aber nicht mit dem Wortlaut des TDG überein. Dieses Gesetz nimmt seinen eigenen Anwendungswillen in § 2 Abs. 4 Nr. 3 TDG nur zurück für „inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des MDStV“.

Auch in der Neufassung des Gesetzes ist diese Formulierung unverändert geblieben.¹⁷⁰ Nach Art. 31 GG setzt sich diese bundesrechtliche Norm gegen einen allfälligen weitergehenden Geltungswillen des MDStV der Länder durch. Denn Bundesrecht bricht auch insoweit Landesrecht.¹⁷¹ Dem steht auch der Grundsatz der Bundestreue nicht entgegen.¹⁷² Anders könnte es vielmehr nur dann sein, wenn der Bund mit § 2 Abs. 4 Nr. 3 TDG die Grenzen seiner Gesetzgebungskompetenz überschritten hätte. Die einfachrechtliche Frage nach der Abgrenzung zwischen MDStV und TDG ist auf diese Weise also mit der verfassungsrechtlichen Frage nach der Grenze der Gesetzgebungskompetenzen verzahnt.¹⁷³

Diese verfassungsrechtliche Frage ist nicht weniger Streitig als die einfachrechtliche Frage, von der wir ausgegangen sind.¹⁷⁴ Im Schrifttum finden sich dabei nicht selten Überlegungen zum Ausmaß einer Landeskompetenz zur Regelung des Rundfunks,¹⁷⁵ der Medien¹⁷⁶ oder gar der Kultur.¹⁷⁷ Als Beschreibung der Verfassungswirklichkeit mögen solche Formeln akzeptabel sein. Verfassungsdogmatisch kommt es nach dem System der Art. 30 und 70 GG jedoch nur auf die Kompetenzen des Bundes an. Den Ländern bleibt zur Gesetzgebung nur das, was die Verfassung nicht zuvor dem Bund zugewiesen hat. Die Kataloge der Bundesgesetzgebungszuständigkeiten sind allerdings nicht kategorisch. Wenn der Bund nur eine Rahmengesetzgebungskompetenz hat, muss er den Ländern einen substanziellen Rest zur Regelung überlassen. Von seinen konkurrierenden Gesetzgebungskompetenzen darf der Bund nach Art. 72 Abs. 2 GG nur dann Gebrauch machen, wenn und soweit die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit sein Eingreifen erforderlich macht. Auch dann kann er die Gesetzgebung nach

Art. 72 Abs. 1 GG teilweise oder ganz den Ländern überlassen. Schließlich eröffnet Art. 71 GG auch im Bereich der ausschließlichen Gesetzgebungskompetenzen die Möglichkeit, dass der Bund die Länder zur Gesetzgebung ermächtigt. Deshalb kann § 2 Abs. 4 Nr. 3 TDG zwei unterschiedliche dogmatische Funktionen haben. Entweder stellt die Vorschrift nur deklaratorisch die verfassungsrechtliche Lage dar. Oder sie weist den Ländern konstitutiv Gesetzgebungsbefugnisse für solche Dienste zu, die redaktionell gestaltet sind.¹⁷⁸

Das TDG enthält Vorschriften über Kommunikationsinhalte. Deswegen ist literarisch vor allem über die Zuständigkeit des Bundes zur Inhaltsregulierung der Individualkommunikation gestritten worden.¹⁷⁹ Kritiker meinten, so weit reiche die Zuständigkeit aus Art. 73 Nr. 7 GG zur Regelung der Telekommunikation nicht. Der Bund könne sich nur auf seine Kompetenz aus Art. 74 Nr. 11 GG für das Recht der Wirtschaft berufen. Deshalb sei nur die Regelung der Inhalte kommerzieller Kommunikation erfasst.¹⁸⁰ Dieser literarische Streit verkennt jedoch den Regelungsgehalt des TDG. Es enthält zwar auch einige wenige Regeln zur positiven Inhaltskontrolle. Die eigentliche Aussage des Gesetzes ist aber eine negative. Die Regulierung des Internet soll soweit als irgend vertretbar unterbleiben.¹⁸¹ Diese Entscheidung hat der Bund in offen ausgesprochener wirtschaftspolitischer Absicht getroffen. Ihm geht es „um die Beseitigung von Hemmnissen für die freie Entfaltung der Marktkräfte im Bereich der neuen Informations- und Kommunikations-(LuK-)Dienste und die Gewährleistung einheitlicher wirtschaftlicher Rahmenbedingungen für das Angebot und die Nutzung dieser Dienste“.¹⁸²

Er erwartet davon einen Wachstumsschub für die Internetwirtschaft selbst und für fast alle anderen Wirtschaftszweige. Denn er sieht im Internet eine neue, leistungsfähige Infrastruktur für wirtschaftliches Handeln.¹⁸³ „Ziel des Gesetzes ist es, i.R.d. Bundeskompetenzen eine verlässliche Grundlage für die Gestaltung der sich dynamisch entwickelnden Angebote im Bereich der LuK-Dienste zu bieten und einen Ausgleich zwischen freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen herbeizuführen“.¹⁸⁴

Diese Absicht des Bundesgesetzgebers ergibt sich nicht nur aus der Regierungsbegründung. Vielmehr hat der Gesetzgeber sie ausdrücklich noch einmal in § 1 des Gesetzes niedergelegt. I.E. ist das TDG deshalb insgesamt von der Wirtschaftskompetenz des Bundes gedeckt. Die Gesetzgebungskompetenz der Länder für den MDStV ergibt sich nicht aus der Verfassung selbst, sondern erst aus § 2 Abs. 4 Nr. 3 TDG. Daraus folgt dann auch, dass das Tatbestandsmerkmal der redaktionellen Gestaltung in § 2 Abs. 4 Nr. 3 TDG den Ausschlag gibt. Denn nur in diesem Umfang ist die Gesetzgebung der Länder ja überhaupt eröffnet.¹⁸⁵

3. Rechtmäßigkeit des Eingriffs gegen den primär Verantwortlichen

Die Eingriffsbefugnis aus § 22 Abs. 3 MDStV ist nur dann eröffnet, wenn sich Maßnahmen ggü. dem primär Verantwortlichen als nicht durchführbar oder nicht erfolgversprechend erweisen. Wie sonst auch beim polizeilichen Vorgehen gegen Nichtstörer ist ein Eingriff nach § 22 Abs. 3 MDStV deshalb nur dann zulässig, wenn die Behörde an sich zum Eingreifen gegen den primär Verantwortlichen berechtigt wäre.

¹⁷⁰ Verwendet wird das Kriterium auch von BT-Drs. 13/7385 (Amtl. Begr. LuKDG), Begr. zu § 2 Abs. 2 Nr. 2 TDG; Gegenäußerung der Bundesregierung Nr. 1 a; BT-Drs. 14/1191 (LuKDG-Bericht), S. 7; Engel-Flehsig/Maennel/Tetenborn (o. Fußn. 28), S. 11, 13; vgl. auch Holznel, ZUM 1999, 433; Wimmer, ZUM 1999, 439; Zimmermann, NJW 1999, 3146; Popp (o. Fußn. 37), S. 61.

¹⁷¹ Waldenberger, MMR 1998, 126; Spindler (o. Fußn. 168), Rdnr. 48, 81.

¹⁷² Anders Holznel (o. Fußn. 4), Rdnr. 50.

¹⁷³ So auch Germann (o. Fußn. 131), S. 140 ff.

¹⁷⁴ Zusammenfassend etwa Determann (o. Fußn. 112), S. 216–242; Mayer (o. Fußn. 165), S. 135–154.

¹⁷⁵ Koch, CR 1997, 198; Freytag, Haftung im Netz, 1999, S. 41; Germann (o. Fußn. 131), S. 144.

¹⁷⁶ Ladeur, ZUM 1997, 383.

¹⁷⁷ Mayer (o. Fußn. 165), S. 139.

¹⁷⁸ Wimmer/Michael (o. Fußn. 4), S. 24; Germann (o. Fußn. 131), S. 151 f. deuten die Vorschrift im letzteren Sinne.

¹⁷⁹ Bejahend Wimmer/Michael (o. Fußn. 4), S. 19; grds. auch Bullinger/Mestmäcker (o. Fußn. 126), S. 144–156; verneinend Martenczuk, ZUM 1999, 106 f. und 108; Germann (o. Fußn. 131), S. 142.

¹⁸⁰ Martenczuk, ZUM 1999, 107; Germann (o. Fußn. 131), S. 142.

¹⁸¹ BT-Drs. 13/7385 (Amtl. Begr. LuKDG), Begr. A.

¹⁸² Ebd.

¹⁸³ Ebd.

¹⁸⁴ Ebd.

¹⁸⁵ Angesichts dieser eindeutigen und starken Begründung brauchen wir einer schwächeren Hilfsbegründung nicht nachzugehen. Sie würde darauf abheben, dass § 2 Abs. 4 Nr. 3 TDG das Ergebnis eines Zuständigkeitskompromisses zwischen Bund und Ländern wiedergibt, an den die Länder jetzt gebunden sind, vgl. dazu von Heyl, ZUM 1998, 117; Wimmer/Michael (o. Fußn. 4), S. 16.

Dass die Verbreitung der streitgegenständlichen Inhalte in der Bundesrepublik nach den §§ 130 oder 131 StGB strafbar wäre, ist vermutlich unstrittig. Wir hatten allerdings bereits gesehen, dass die Bundesrepublik völkerrechtlich und über Art. 25 GG auch innerstaatlich gehindert sein dürfte, ihr Recht auf die ausländischen Anbieter der Inhalte anzuwenden. Wegen Art. 25 GG darf diese Grenze auch nicht unter Berufung auf die Nichtstörerhaftung übersprungen werden.¹⁸⁶

Außerdem will der *RP* die Access-Provider ja nicht verpflichten, den Zugang zu konkreten Inhalten zu sperren. Vielmehr soll gleich der gesamte Zugang zu zwei Webhosts verhindert werden. § 22 Abs. 3 MDStV soll also nicht i.V.m. § 6 Abs. 1, sondern mit § 6 Abs. 2 MDStV n.F. zur Anwendung kommen.¹⁸⁷ An sich lässt § 22 Abs. 3 MDStV das ausdrücklich zu. Voraussetzung ist dann aber, dass der *RP* an sich rechtmäßig gegen die Hosts hätte vorgehen können. Polizeirechtlich gesprochen sind die Webhosts nicht Verhaltens-, sondern Zustandsstörer.¹⁸⁸ § 6 Abs. 2 MDStV eröffnet diese Möglichkeit zwar grundsätzlich. Ein Zustandsstörer kann aber nicht beliebig in Anspruch genommen werden.¹⁸⁹ Wie beim Handlungsstörer muss vielmehr auch hier eine besondere Verantwortlichkeit hinzutreten. Sie ist nur nicht Folge vorausgehenden Tuns. Vielmehr folgt sie aus der besonderen, rechtlichen Verantwortlichkeit für ein Risiko.¹⁹⁰ § 6 Abs. 2 MDStV bestimmt die Voraussetzungen, unter denen die Rechtsordnung diese Verantwortlichkeit annimmt. Der Host muss von den fraglichen Inhalten Kenntnis haben. Außerdem muss es ihm technisch möglich und zumutbar gewesen sein, deren Nutzung zu verhindern. Vermutlich sind diese Voraussetzungen in den beiden Ausgangsfällen zwar erfüllt. Den Nachweis hat der *RP* bislang aber nicht erbracht.

4. Eingreifen gegen Access-Provider als Ausnahme

Der *RP* begründet das Vorgehen gegen die Access-Provider lapidar: Ein Vorgehen direkt gegen die beiden Webhosts verspricht keinen Erfolg. Der Rest der Begründung betrifft dann schon nicht mehr das „Ob“ des Einschreitens, sondern das „Wie“. Die Sperrung der URLs sei technisch möglich, zumutbar und verhältnismäßig. Wenn es dabei bliebe, würden die deutschen Ordnungsbehörden zu den Zensoren des Internet.¹⁹¹ § 22 Abs. 3 MDStV böte die Handhabe zur nahezu vollständigen Renationalisierung des Internet. Der *RP* räumt selbst ein, dass es dabei nicht um ein marginales Problem geht. In der bereits erwähnten Pressemitteilung spricht er von „bis zu“ 6.000 rechtsradikalen Websites, gegen die er auf diese Weise vorgehen will.¹⁹² Auch etwas konservativere Schätzungen kommen zu sehr großen Zahlen. Das angesehene *Simon-Wiesenthal-Center* schätzt die Zahl rechtsextremer und volksverhetzender Websites auf mehr als 2.000.¹⁹³ Der Verfassungsschutz spricht von 1.300 rechtsextremen Websites allein in deutscher Sprache.¹⁹⁴ Kommerzielle Filter, die in den USA verkauft werden, filtern typischerweise sogar zwischen mehreren 100.000 und 2 Mio. Websites heraus.¹⁹⁵ Darunter ist sicher auch manches, was nach § 22 Abs. 3 MDStV nicht verboten werden könnte. Auch wenn nur ein Bruchteil dieser Sites unter die Vorschrift fiele, entstünde aber ein gigantisches Regelungspotenzial.

Dass § 22 Abs. 3 MDStV solch eine Regelungswut hätte entfesseln wollen, scheidet aus.¹⁹⁶ Die Notwendigkeit einer engeren Auslegung der Vorschrift lässt sich auf einer ganzen Reihe dogmatischer Wege aufzeigen. Zunächst einmal ist das, was die *Bezirksregierung* etablieren möchte, strukturell einem „notice and take down“-Verfahren

verwandt. Der einzige Schutz der Access-Provider würde darin bestehen, dass sie nicht auch noch von sich aus nach problematischen Inhalten des Internet fahnden müssen; selbst diese Grenze scheint der *RP* mittlerweile noch überschreiten zu wollen.¹⁹⁷ Wann immer die *Bezirksregierung*, vielleicht sogar ein Dritter auf rechtswidrige Inhalte hinweist,¹⁹⁸ müssten die Access-Provider den Zugang zu diesen Inhalten sperren. Dieses Ergebnis steht im klaren Widerspruch zur Richtlinie der Europäischen Gemeinschaft über den elektronischen Geschäftsverkehr. In ihrem Art. 21 Abs. 2 schreibt die Richtlinie einen Bericht vor, der die künftige Einführung eines „notice and take down“-Verfahrens erörtern soll. Ein solches Verfahren würde sich gegen die Betreiber der Ursprungsserver richten. Der bloße Hinweis auf die Rechtswidrigkeit des Inhalts würde die Rechtspflicht auslösen, den Inhalt zu entfernen. Was die *Bezirksregierung* will, geht darüber sogar noch hinaus. Denn sie will aus dem bloßen Hinweis auch eine Pflicht der Access-Provider ableiten, den Zugang zu Inhalten, die sich nicht in ihrem Herrschaftsbereich befinden, zu sperren. Sie will also den Kreis der Adressaten sogar noch erweitern. Aus Art. 21 Abs. 2 der Richtlinie ergibt sich im Gegenschluss, dass solche Verfahren einstweilen gerade nicht eingeführt werden sollen. Es ist auch nicht so, dass der deutsche Gesetzgeber nach Belieben über die Vorschriften der Richtlinie hinausgehen dürfte. Vielmehr will die Richtlinie den elektronischen Geschäftsverkehr durch die Einführung einheitlicher Bedingungen in ganz Europa fördern. Ihre Vorschriften sind deswegen als abschließende „Vollharmonisierung“ ausgestaltet.¹⁹⁹

Hinzu kommt ein systematisches Argument. Wenn § 22 Abs. 3 MDStV so auszulegen wäre, wie das der *RP* möchte,

186) S.o. II. 6. e).

187) In der ursprünglichen Fassung des Gesetzes war die Unterscheidung klarer. Dort war der Handlungsstörer in § 5 Abs. 1 MDStV erfasst, der Zustandsstörer in § 5 Abs. 2 MDStV. Hierauf bezieht sich der Bescheid des *RP*.

188) So ausdrücklich *Germann* (o. Fußn. 131), S. 393–395 u. 448.

189) Grundlegend *Lepsius*, JZ 2001, 22 ff.

190) *Pieroth/Schlink/Kniesel*, Polizei- und Ordnungsrecht, 2002, § 9 Rdnr. 42–45.

191) *Holzmagell/Kussel*, MMR 2001, 351: „Ob von dieser Regelung auch die Pflicht zum Einsatz vorkonfigurierter Filter abgeleitet werden kann, bedarf einer genauen Prüfung, bei der auch die durch eine solche Maßnahme beeinträchtigten Grundrechte der Inhaltsanbieter, der Internetnutzer und der Access-Provider berücksichtigt werden müssen. Auf keinen Fall darf die Bekämpfung rechtsradikaler Internetinhalte zum Anlass genommen werden, das Grundrecht der Meinungsfreiheit für den Bereich der Neuen Medien auszuhöheln“.

192) S. erneut o. Fußn. 63.

193) *Holzmagell/Kussel*, MMR 2001, 347.

194) <http://www.heise.de/newsticker/result.xhtml?url=newsticker/data/jk-29.04.02-004/default.shtml&words=Verfassungsschutz> (Stand: 19.5.2002); ebenso Bericht des Baden-Württembergischen Verfassungsschutzes: Extremisten im Internet – Eine Herausforderung für die Sicherheitsbehörden, Dezember 2001; das *BKA* hatte schon im Februar 2000 350 rechtsradikale Seiten gefunden (lt. Auskunft von *Dornbusch* bei einer Anhörung der *Bezirksregierung Düsseldorf* am 13.11.2001); s. auch BT-Drs. 14/9010 (Antwort der *Bundesregierung* auf eine kleine Anfrage der *CDU/CSU-Fraktion*): es gibt 620 deutsche Websites mit linksextremistischen Inhalten.

195) *National Research Council*, Youth, Pornography and the Internet, 2002, 12.1.1.

196) Dass solche Interventionen die Ausnahme bleiben müssen, fordern auch *Spindler/Volkman*, K&R 2002, 404, gestützt auf die Grenzen des allgemeinen Polizeirechts für ein Eingreifen gegen Nichtstörer; dazu sogleich unter 5.

197) Bei der Anhörung am 16.4.2002 hat er geäußert, Access-Provider müssten auch aktiv nach problematischen Inhalten im Netz suchen.

198) Bei der Anhörung am 16.4.2002 hat der *RP* verlangt, die Access-Provider sollten eine Hotline einrichten. Jedermann solle dort Internetseiten melden können, die er für problematisch hält. Die Access-Provider sollten die Vereinbarkeit dieser Seiten mit deutschem Recht prüfen und den Zugang ggf. sperren.

199) BT-Drs. 14/6098, Aml. Begr. TDG neu, 22.

würde diese Vorschrift zur Regel. Denn das Internet ist ja ein vollständig internationales Netz. Wenn ein Staat national gegen die Anbieter problematischer Inhalte vorgeht, erreicht er deshalb nicht viel. Sie verlagern ihre Inhalte dann eben auf ausländische Server. Ihre Wirkungschancen beeinträchtigt das praktisch nicht. Für die Nutzer ist es technisch wie wirtschaftlich gleichgültig, ob sie ein inländisches oder ein ausländisches Angebot abrufen. Auf diese Weise würden die Privilegierungen der §§ 6 Abs. 2, 7–9 MDStV also in ihr Gegenteil verkehrt.²⁰⁰ Der Access-Provider wäre nicht etwa regelmäßig von der Verantwortung frei. Vielmehr wäre er im Gegenteil regelmäßig der Büttel des Staats für dessen Absichten der Inhaltsregulierung.

Bei dieser Auslegung von § 22 Abs. 3 MDStV käme es zu einer radikalen Umkehr in der deutschen Internetpolitik.²⁰¹ Bei der Untersuchung der Gesetzgebungskompetenz des Bundes für das TDG hatten wir uns bereits die industriepolitische Zielsetzung des Gesetzes vor Augen geführt.²⁰² Der Bund fürchtete um die Entwicklung des Informationstechnologiestandorts Deutschland und berief sich deshalb erstmals im Bereich der Medien auf seine Wirtschaftskompetenz.²⁰³ Das Haftungsprivileg der Access-Provider war ganz offen als Anreiz für die Ansiedlung solcher Unternehmen gedacht.²⁰⁴ Der Gesetzgeber stand im Bann des *CompuServe*-Falls. Die Access-Provider sollten sicher sein dürfen, dass sich solch ein Fall nicht wiederholen würde.²⁰⁵ Der Gesetzgeber wollte ein glaubhaftes Zeichen der Vernunft setzen. Er wollte signalisieren, dass die von regulierungswütigen Heißspornen praktizierten Methoden dem Versuch gleich kommen, „den Ozean mit der Hand ausschöpfen zu wollen“.²⁰⁶

Von diesen Überzeugungen hat der Bund bis heute nicht abgelassen. Das *Bundeskanzleramt* glaubt nach wie vor,

dass technische Lösungen, wie sie die *Bezirksregierung* nun plant,²⁰⁷ keinen Erfolg versprechen. Das gilt auch und gerade für die Politik des Bundes zur Bekämpfung von Rechtsextremismus und Fremdenfeindlichkeit. Der *Bundesinnenminister* hat im Mai 2002 ein umfangreiches Konzept vorgelegt. Dort ist zwar auch vom Internet die Rede. Die einschlägige Passage lautet aber: „Das Internet ist ein globales Medium, dessen Kontrolle international sehr unterschiedlich gehandhabt wird. Während z.B. in den USA die Verbreitung rechtsextremer Internetinhalte unter Hinweis auf die Meinungsfreiheit weitgehend straffrei bleibt, wird sie in Deutschland als Straftat geahndet. Daher setzt sich die *Bundesregierung* in internationalen Gremien, vor allem im *Europarat* und i.R.d. *G-8 der Vereinten Nationen*, nachhaltig für eine einheitliche internationale Verfolgung rechtsextremistischer Straftaten im Internet ein“.²⁰⁸

5. Voraussetzungen eines Vorgehens gegen Nichtstörer

Weitere Schranken für ein Vorgehen gegen Access-Provider (b) ergeben sich aus der Tatsache, dass § 22 Abs. 3 MDStV eine spezialgesetzliche Regel über die Verantwortlichkeit von Nichtstörern darstellt (a).

a) § 22 Abs. 3 MDStV als Haftung von Nichtstörern

§ 22 Abs. 3 MDStV erlaubt grds. ein Vorgehen „gegen den Diensteanbieter von fremden Inhalten nach den §§ 7 bis 9 MDStV“. § 6 MDStV ist mit der „Verantwortlichkeit“ von Anbietern befasst. Diensteanbieter sind nach Abs. 1 der Vorschrift nur „für eigene Informationen, die sie zur Nutzung bereithalten, [...] verantwortlich“. Die Verantwortlichkeit für fremde Informationen ist von § 7 Abs. 1 MDStV dagegen auf den Fall begrenzt, dass ein Diensteanbieter die Übermittlung veranlasst, den Adressaten oder die übermittelten Informationen ausgewählt oder verändert hat.

Zu diesen neu gefassten Normen gibt es noch keine literarische Diskussion. Damit der folgende Bericht über die ältere Diskussion verständlich wird, muss zuerst an die frühere Fassung der einschlägigen Vorschrift erinnert werden. Auch der Bescheid des *RP* stützt sich auf diese Vorschriften.²⁰⁹ Die auf diese Weise gefundenen Ergebnisse lassen sich auf die neu gefassten Vorschriften übertragen. Nach § 5 Abs. 2 MDStV a.F. waren Webhosts für die von ihnen bereitgehaltenen fremden Inhalte nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar war, deren Nutzung zu verhindern. Access-Provider waren nach § 5 Abs. 3 MDStV a.F. dagegen „nicht verantwortlich“.

Obwohl die Regelungstechnik eigentlich zweifelsfrei sein müsste, ist im Schrifttum doch eine beinahe babylonische Sprachverwirrung entstanden. Sie dürfte vor allem darauf beruhen, dass sich in der Diskussion Vertreter aller drei juristischen Teildisziplinen zu Wort gemeldet haben. Wenn ein Zivilrechtler davon spricht, § 22 Abs. 3 MDStV sei eine Vorschrift zur Störerhaftung, meint er damit wohl, dass kein Verschuldensnachweis erforderlich ist.²¹⁰ In ähnlicher Weise könnte ein Strafrechtler sagen wollen, dass eine Strafbarkeit jedenfalls nicht in Betracht kommt, sondern allenfalls ein ordnungsrechtliches Vorgehen.²¹¹ Unverständlich ist dagegen, warum auch Öffentlichrechtler gelegentlich davon sprechen, die Access-Provider seien Störer.²¹² Die überwiegende Mehrheit sieht das anders und hält die Access-Provider für Nichtstörer.²¹³ Dem ist zuzustimmen.

Dass die Access-Provider Nichtstörer sind, ergibt sich zunächst einmal aus den allgemeinen polizeirechtlichen

200) Wieder war die a.F. des MDStV einfacher zu lesen. Dort ergab sich die Privilegierung klar aus § 5 Abs. 3 MDStV a.F.

201) Vgl. *Wimmer/Michael* (o. Fußn. 4), S. 60 dort bei Fußn. 155; *Koenig/Loetz*, CR 1999, 438 ff. dort bei Fußn. 32, 33; Anm. von *Hoeren* zur Entscheidung des *Generalbundesanwalts* v. 26.11.1997, MMR 1998, 93, 97; *LG Stuttgart* CR 2001, 626, Ls. 3.

202) S. erneut BT-Drs. 13/7385 (Amtl. Begr. IuKDG), Begr. A; wörtliche Zitate oben 2 b; bestätigt von den am Gesetzgebungsverfahren beteiligten Beamten *Bröhl*, CR 1997, 74; *Engel-Flechsig/Maennel/Tettenborn* (o. Fußn. 28), S. 8, 16.

203) *Wimmer/Michael* (o. Fußn. 4), S. 15 m.w.Nw.

204) Vgl. auch *Sieber*, CR 1997, 582.

205) *Popp* (o. Fußn. 37), S. 64 m.w.Nw.

206) *Sieber*, MMR 1999, 199 ff. dort bei Fußn. 82.

207) Dies berichtete *Maas* vom DFN-Verein bei einer Anhörung der *Bezirksregierung* am 13.11.2001.

208) http://www.bmi.bund.de/frame/dokumente/Artikel/ix_79389.htm (Stand: 2.7.2002).

209) Im Widerspruchsbescheid (o. Fußn. 39) hat der *RP* seine Begründung dann auf die neuen Vorschriften umgestellt.

210) So dürfte *Spindler* (o. Fußn. 168), Rdnr. 145, s.auch Rdnr. 355 zu verstehen sein. Vielleicht ist auch einfach nur die Begrifflichkeit unsauber. Dafür könnte sprechen, dass *Spindler/Volkman*, K&R 2002, 401 die Access-Provider zunächst zwar als „Störer“ bezeichnet, dann aber ausführlich begründen, dass sie Nichtstörer sind, S. 402–405.

211) Vgl. *Sieber*, MMR 1999, 199 ff. dort bei Fußn. 186.

212) *Koenig/Loetz*, CR 1999, 438 ff. dort bei Fußn. 49 f.; vielleicht auch *Holzmann/Kussel*, MMR 2001, 351; s. aber *Holzmann/Holzmann*, K&R 1999, 106: „Hier muss die Frage erlaubt sein, ob dadurch nicht die kommunikationsfördernde Funktion des Internet, die ja ganz wesentlich auf den Aktivitäten der Serviceprovider beruht und grundrechtlich geschützt wird, über Gebühr eingeschränkt wird“; jüngst schließlich auch der Widerspruchsbescheid des *RP* (a.E., zu § 5 OBG).

213) *Wimmer/Michael* (o. Fußn. 4), S. 31, 57, 61; *Sieber*, Verantwortlichkeit im Internet, 1999, S. 123; *Wimmer*, ZUM 1999, 441; *Zimmermann*, NJW 1999, 3149; *Germann* (o. Fußn. 131), S. 448; *Hornig*, ZUM 2001, 856; *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 16, s.a. Rdnr. 14; *Spindler/Volkman*, K&R 2002, 403; vgl. auch *Koch*, CR 1997, 201: Der „vereinzelte Missbrauch der Kommunikationsmöglichkeiten durch Dritte [...] ist grds. Teil des allgemeinen Lebensrisikos“.

Grundsätzen für die Abgrenzung zwischen Störer und Nichtstörer. Wer von seinen Freiheiten einen legalen Gebrauch macht, kann nicht Störer sein.²¹⁴ Störer ist nur, wer die Störung der öffentlichen Sicherheit unmittelbar verursacht.²¹⁵ Entscheidend ist dabei nicht die faktische, sondern die rechtliche Unmittelbarkeit. Wer Störer ist, ergibt sich also aus Wertungen der Rechtsordnung über den Verantwortungszusammenhang.²¹⁶ Genau diese Wertung war § 5 Abs. 3 MDStV a.F. zu entnehmen. Die Vorschrift sagte explizit, dass für rechtswidrige Internetinhalte nicht verantwortlich ist, wer lediglich den Zugang zu ihrer Nutzung vermittelt. Aus dieser Vorschrift ergibt sich auch, dass die Access-Provider nicht Zustandsstörer sind, auch nicht „Zustandsstörer sui generis“, wie der *RP* nun vortragen lässt.²¹⁷ Voraussetzung wäre auch dafür nämlich, dass die Access-Provider die rechtliche Verantwortung für ein Risiko tragen, dem der konkrete Belang der öffentlichen Sicherheit ausgesetzt ist.²¹⁸ Wiederum folgte aus § 5 Abs. 3 MDStV a.F., dass dem gerade nicht so war.²¹⁹ Daran kann – entgegen der Auffassung des *RP*²²⁰ – auch die Tatsache nichts ändern, dass eine öffentliche oder private Stelle den Access-Provider auf den rechtswidrigen Inhalt der transportierten Inhalte hinweist. Denn als Grundlage für die ordnungsrechtliche Inanspruchnahme eines Access-Providers kommt ja nur § 18 Abs. 3 MDStV a.F.²²¹ in Betracht. Dabei handelt es sich aber, wie gerade gezeigt, um eine Norm zur Inanspruchnahme eines Nichtstörers. Durch bloße Erklärung kann sie sich nicht zu einer Zuschreibung von (Zustands-)Verantwortlichkeit wandeln.

Im Strafrecht und im Zivilrecht hat sich eine breite Diskussion über die dogmatische Einordnung von §§ 5 MDStV a.F. und 5 TDG a.F. entwickelt.²²² Die Verfügungen des *RP* bieten dem öffentlichen Recht Anlass, diese Diskussion nachzuholen. Wegen § 22 Abs. 3 MDStV geht es im öffentlichen Recht aber um mehr als bloße systematische Geschlossenheit. In den beiden anderen Rechtsgebieten ist es letztlich gleichgültig, ob man § 5 Abs. 3 MDStV a.F. bzw. § 5 Abs. 3 TDG a.F. und die heutigen Nachfolgevorschriften als vorgeschalteten Filter deutet oder ob man den Vorschriften einen Platz in der entwickelten Dogmatik dieser Rechtsgebiete zuweist.²²³ Im öffentlichen Recht gibt die dogmatische Einordnung von § 5 Abs. 3 MDStV a.F. dagegen den Ausschlag für das Verständnis von § 22 Abs. 3 MDStV. Genau das geschieht, wenn man § 5 Abs. 1 MDStV a.F. mit dem Handlungsstörer gleichsetzt, § 5 Abs. 2 MDStV a.F. mit dem Zustandsstörer und § 5 Abs. 3 MDStV a.F. mit dem Nichtstörer.²²⁴

Diese Zuordnung überzeugt auch teleologisch. Die Richtlinie der EG über den elektronischen Geschäftsverkehr bringt den tragenden Gedanken zum Ausdruck: „Die in dieser Richtlinie hinsichtlich der Verantwortlichkeit festgelegten Ausnahmen decken nur Fälle ab, in denen die Tätigkeit des Anbieters von Diensten der Informationsgesellschaft auf den technischen Vorgang beschränkt ist, ein Kommunikationsnetz zu betreiben und den Zugang zu diesem zu vermitteln, über das von Dritten zur Verfügung gestellte Informationen übermittelt oder zum alleinigen Zweck vorübergehend gespeichert werden, um die Übermittlung effizienter zu gestalten. Diese Tätigkeit ist rein technischer, automatischer und passiver Art, was bedeutet, dass der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt“.²²⁵

Die bisherigen Überlegungen knüpfen allerdings an § 5 Abs. 3 MDStV a.F. an. Im Schrifttum gibt es einen wunder-

lichen Streit über die Frage, ob Access-Provider unter diese Vorschrift fallen.²²⁶ Manche wollen die Vorschrift bestenfalls analog anwenden,²²⁷ andere gar nicht. Sie begründen das damit, dass der Access-Provider selbst eine TK-Dienstleistung²²⁸ oder einen Teledienst erbringe.²²⁹ Dabei ist jedoch missverstanden, was die Aufgabe von § 22 Abs. 3 MDStV ist. Die Vorschrift soll unter engen Voraussetzungen ermöglichen, auch gegen die inhaltlich gerade nicht verantwortlichen Access-Provider vorzugehen. Deshalb kommt es für die Anwendbarkeit von § 22 Abs. 3 MDStV nicht darauf an, dass die Access-Provider als Mediendienst zu qualifizieren sind. Entscheidend ist, ob der Inhalt ein Mediendienst ist, gegen den sich die staatliche Intervention richtet.²³⁰ Konsequenterweise kann es dann aber auch für die Privilegierung des § 5 Abs. 3 MDStV a.F. nicht darauf ankommen, dass der privilegierte Dienst selbst ein Mediendienst ist. Oder deutlicher: Schon nach seinem Tatbestand setzt § 22 Abs. 3 MDStV voraus, dass sich die Intervention gegen eine Person richtet, die unter § 5 Abs. 3 MDStV a.F. fällt. Wären die Access-Provider nicht durch § 5 Abs. 3 MDStV a.F. privilegiert, würde dem staatlichen Eingriff also von vornherein die Ermächtigungsgrundlage fehlen. Für unseren Zusammenhang folgt daraus aber zugleich, wenn ein Access-Provider nach § 22 Abs. 3 MDStV in Anspruch genommen wird, ist er Nichtstörer.

Wie bereits angekündigt passt all das auch für den neu gefassten MDStV. Dort findet sich der einfache Dreischritt

214) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 16 m.w.Nw.

215) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 11.

216) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 13–19.

217) Ein Beamter der *Bezirksregierung* hat diese These bei einem Symposium am 31.10.2002 in Düsseldorf mündlich vorgetragen.

218) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 42–45; vgl. auch *Spindler/Volkman*, K&R 2002, 403: Der Access-Provider beherrscht nur die Leitungen, deren „Zustand“ für sich betrachtet ungefährlich ist.

219) Übersehen im Widerspruchsbescheid des *RP* (o. Fußn. 40, a.E., zum OBG).

220) In seinem Widerspruchsbescheid (o. Fußn. 39).

221) Bzw. § 22 Abs. 3 MDStV n.F.

222) Zum Strafrecht s. vor allem *Wimmer/Michael* (o. Fußn. 4), S. 55; *Sieber* (o. Fußn. 213), S. 114–123; *Sieber*, MMR 1999, 199 ff. dort bei Fußn. 31–43. Zum Zivilrecht s. vor allem *Freytag* (o. Fußn. 175), S. 132–147; *Haedicke*, CR 1999, 313 ff.; *Spindler* (o. Fußn. 168), Rdnr. 28–37.

223) Anders könnte das allerdings auch im Zivilrecht sein, wenn Unterlassungsansprüche nach § 1004 BGB in Rede stünden. Solche Ansprüche sind bislang aber nicht praktisch geworden.

224) So jetzt grds. auch *Spindler/Volkman*, K&R 2002, 402–404, mit einer Differenzierung für die Webhosts.

225) Richtlinie 2000/31/EG v. 8.6.2000, ABl. EG 2000 Nr. L 178/1, 42. Erwägung; ebenso *Council of Europe Group of Specialists on On-Line Services and Democracy* (MM-S-OD) Draft Declaration on Freedom of Information on the Internet of 8.4. 2002, Principle 4: „Liability for content of communications: When deciding which rules shall govern liability for content of Internet communications, member States should take into due account the situation of intermediaries in the communication chain, who should not be held liable for providing access, transmitting or hosting in good faith“; s. auch *Säcker*, MMR 2001, 2: eine weiter gehende Haftung der Access-Provider hätte einen „chilling effect“ auf die Entwicklung der Infrastruktur.

226) Dafür sprechen sich aus: *OLG Hamburg* MMR 2000, 92, 93; *Koch*, CR 1997, 200; *Waldenberger*, MMR 1998, 128; *Freytag* (o. Fußn. 175), S. 224; *Wimmer*, ZUM 1999, 439; *Pankoke* (o. Fußn. 146), S. 6 f.; vgl. auch *Sieber*, MMR 1999, 199 ff. dort bei Fußn. 170 zu Routern.

227) *Sieber*, CR 1997, 583 dort bei Fußn. 18; *Martenczuk*, ZUM 1999, 111 f.; *Freytag*, CR 2000, 606; vgl. auch *AG München* v. 28.5.1998, S. 10 f. des Umdrs. – Somm.

228) Für die Qualifikation als TK-Dienstleistung *Koch*, CR 1997, 199; *Germann* (o. Fußn. 131), S. 128–130; *Popp* (o. Fußn. 37), S. 59; vgl. auch *Spindler* (o. Fußn. 168), Rdnr. 77 f. zu Routern.

229) Für die Qualifikation als Teledienst *Kröger/Moos*, AfP 1997, 679; *Wimmer/Michael* (o. Fußn. 4), S. 51; *Holznel* (o. Fußn. 4), Rdnr. 57; *Lent* (o. Fußn. 157), S. 172; mittlerweile ist die Frage in Umsetzung der E-Commerce Richtlinie wohl durch § 2 Abs. 2 Nr. 3 des neugefassten TDG zu Gunsten der Qualifikation als Teledienst entschieden, vgl. dazu auch *Freytag*, CR 2000, 606; *Spindler*, MMR 2000, 17.

230) Näher oben unter 2.

des § 5 MDStV a.F. zwar nicht mehr. In Umsetzung der E-Commerce-Richtlinie der EG sind vielmehr die schwierig zu lesenden §§ 6–9 MDStV an seine Stelle getreten. I.E. hat sich aber nichts geändert. Für eigene Inhalte ist ein Diensteanbieter nach § 6 Abs. 1 MDStV n.F. verantwortlich. Für fremde Inhalte ist er nach § 7 Abs. 1 MDStV a.F. nur dann verantwortlich, wenn er durch die dort aufgezählten Akte die publizistische Verantwortung übernommen hat. I.Ü. ist er nach § 6 Abs. 2 Satz 1 MDStV n.F. nicht verantwortlich. In § 6 Abs. 2 Satz 2 MDStV n.F. ist nunmehr aber eine Vorschrift aufgenommen worden, die sich bislang in ähnlicher Form nur in § 5 Abs. 4 TDG a.F. fand:²³¹ „Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach diesem Staatsvertrag oder den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 7 bis 9 unberührt.“ Daraus folgt aber sogar explizit, was unter der a.F. aus der Systematik abzuleiten war, denn es geht gerade um die Inanspruchnahme als Nichtstörer.

b) Grenzen der Inanspruchnahme von Nichtstörern

Dass der Staat notfalls auch gegen Nichtstörer vorgehen darf, bedeutet nicht, dass er sich den Adressaten aussuchen könnte. Daran ändert auch der Umstand nichts, dass ein Nichtstörer Anspruch auf Kompensation hat.²³² Der Staat ist also auch dann nicht frei bei der Auswahl des Adressaten, wenn er sich das etwas kosten lässt. Die Haftung der Nichtstörer ist kein Fall des „Dulde und Liquidiere“. Vielmehr ist diese Haftung strikt subsidiär.²³³ Es geht um eine öffentlich-rechtliche „Notstandshaftung“.²³⁴

Diese Subsidiarität bedeutet zunächst einmal, dass die Behörde ein Auswahlermessen hat. Von diesem Ermessen macht sie nur dann einen fehlerfreien Gebrauch, wenn sie sich mit den besonderen Voraussetzungen für die subsidiäre Inanspruchnahme des Nichtstörers auseinander setzt. Solche Überlegungen sind der Verfügung des RP nicht zu entnehmen. Sie beschränkt sich auf die – dürftig belegte – Feststellung, Maßnahmen gegen die amerikanischen Webhosts versprechen keinen Erfolg. Notwendig wäre dagegen die Begründung gewesen, warum ausnahmsweise auf die Access-Provider als Nichtstörer zugegriffen werden darf.

An der Zulässigkeit eines Vorgehens gegen die Nichtstörer bestehen auch in der Sache erhebliche Zweifel.²³⁵ Denn die Gefahr für die öffentliche Sicherheit muss nach allgemeinem Polizeirecht gegenwärtig, also besonders nahe sein.²³⁶ Zur öffentlichen Sicherheit gehört zwar an sich jede Norm des einfachen öffentlichen Rechts, also auch § 12 Abs. 1 Nr. 1 MDStV. Diese öffentlich-rechtliche Norm nimmt auf die §§ 130 und 131 StGB Bezug. Diese straf-

rechtlichen Normen schützen aber nicht vor konkreten, sondern vor bloß abstrakten Gefahren.²³⁷ Man kann sich schon fragen, ob solche Normen überhaupt geeignet sind, den Begriff der öffentlichen Sicherheit im Polizeirecht auszufüllen. Denn das Polizeirecht unterscheidet ja selbst zwischen konkreten und abstrakten Gefahren. Polizeiverfügungen sind nur bei konkreter Gefahr zulässig. Solange die Gefahr bloß abstrakt ist, bleibt nur die Möglichkeit zum Erlass einer Polizeiverordnung.²³⁸ Jedenfalls lässt sich auf diesem Wege aber keine gegenwärtige, also besonders nahe Gefahr begründen.

Noch aus einem weiteren Grunde kommt ein Vorgehen gegen die Access-Provider als Nichtstörer hier nicht in Betracht. Der RP räumt selbst ein, dass auch nach seinem Eingriff zahlreiche Umgehungsmöglichkeiten bleiben.²³⁹ Er kann nur darauf verweisen, dass das Risiko einer Verletzung der Schutzgüter geringer wird. Das wäre schon im Verhältnis zu den Webhosts selbst eine verfassungsrechtlich problematische Begründung.²⁴⁰ Ggü. einem Nichtstörer kann diese Begründung jedenfalls nicht genügen. Wenn der Staat schon einen außenstehenden Dritten in Anspruch nehmen will, dann muss er das Regelungsziel auch wenigstens erreichen.

Noch aus einem dritten Grund scheidet ein Vorgehen gegen Nichtstörer aus. Man kann auch diese Grenze letztlich aus dem Erfordernis einer gegenwärtigen Gefahr ableiten. Der typbildende Fall eines Vorgehens gegen den Nichtstörer sieht so aus: Ein Damm droht zu brechen. Die Ordnungsbehörde hat selbst kein schweres Gerät. Sie nimmt deshalb einen örtlichen Bauunternehmer in Anspruch und verpflichtet ihn, den Damm mit seinen Maschinen zu verstärken. Nicht umsonst heißt das Institut in der polizeirechtlichen Tradition denn auch polizeilicher Notstand. Die Absicht des RP ist ganz anders. Er nimmt die Access-Provider nicht für etwas in Anspruch, was sie nach ihrer vorhandenen Ausrüstung ohne weiteres können. Vielmehr verlangt er von ihnen, dass sie ihre eigene technische Einrichtung in einer Weise verändern, die die Erfüllung der Wünsche des RP überhaupt erst erlaubt. Das ist offensichtlich bei der zweiten der drei Lösungen, die der RP den Access-Providern zur Wahl stellt. Bislang haben viele von ihnen keine Proxyserver. Sie müssten erst Investitionen tätigen, um diese Aufgabe zu erfüllen. Auch bei den beiden anderen Lösungen besteht das Problem aber. Alle Access-Provider nutzen zwar einen Domain-Name-Server (DNS). Alle vermitteln den Zugang zum Internet auch über Router. Bislang sind beides aber rein technische Vorkehrungen. Der RP verlangt von den Access-Providern dagegen, dass sie ihr Geschäftsmodell umstellen. Sie sollen ihr Personal anweisen, auf Dauer dafür zu sorgen, dass der DNS oder der Router zur Filterung der eingehenden Inhalte genutzt werden kann. Das hat mit einem punktuellen Vorgehen im polizeilichen Notstand nichts mehr zu tun.

6. Entgegenstehende Grundrechte der Access-Provider

Im öffentlichen Recht ist letztlich jede Frage des einfachen Rechts auch eine Frage des Verfassungsrechts. Deshalb hätten wir auch die Frage des Ob einer staatlichen Intervention bereits als Verfassungsfrage erörtern können. Andererseits enthält das einfache Recht auch Vorgaben für die Ausgestaltung der konkreten Maßnahme. Die Aufsichtsbehörde darf gegen die Access-Provider nach § 22 Abs. 3 MDStV nämlich nur dann vorgehen, wenn „eine Sperrung technisch möglich und zumutbar ist“. Die Auslegung des Tatbestandsmerkmals „technisch möglich“ ist aber praktisch nicht von der verfassungsrechtlichen Frage

231) § 8 Abs. 2 TDG n.F. ist wörtlich identisch mit § 6 Abs. 2 Satz 2 MDStV n.F., abgesehen von den anderen Nummern der verwiesenen Paragraphen.

232) Dazu noch näher unten IV.

233) Näher *Pieroth/Schlink/Kniesel* (o. Fußn. 190), Rdnr. 74; das sehen i.E. auch *Holzengel/Kussel*, MMR 2001, 351 so, obwohl sie § 22 Abs. 3 MDStV (fälschlich) als einen Fall der Störerhaftung bezeichnen; leicht anders *Hornig*, ZUM 2001, 856: keine strikte Subsidiarität, aber Bindung der Auswahl des Adressaten an das Verhältnismäßigkeitsprinzip.

234) So plastisch *Spindler/Volkmann*, K&R 2002, 404.

235) Eine Liste dieser Voraussetzungen findet sich bei *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 9 Rdnr. 74.

236) Vgl. o. Fußn. 235.

237) Zu dieser Unterscheidung und den Folgen für das deutsche internationale Strafrecht s. die Nw. oben II. 6. c).

238) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 4 Rdnr. 9–18.

239) S. zu den Umgehungsmöglichkeiten noch näher unten 9. b).

240) S. näher unten 9. g) zu der Frage, ob eine bloße Verminderung des Risikos ein legitimes Ziel darstellt.

nach der Geeignetheit des Eingriffs zu unterscheiden. Noch schwerer fällt die Unterscheidung zwischen dem einfachrechtlichen Maßstab der Zumutbarkeit und dem verfassungsrechtlichen Maßstab der Angemessenheit. Deshalb wollen wir im Folgenden die einfachrechtliche und die verfassungsrechtliche Untersuchung miteinander verbinden. Diese Art der Darstellung darf allerdings nicht zu einem Fehlschluss verleiten. Die im Folgenden entwickelten verfassungsrechtlichen Grenzen haben nicht nur für die Ausgestaltung der konkreten Maßnahme Bedeutung. Vielmehr unterstützen und verstärken sie auch die voranstehenden Überlegungen zum Ob einer staatlichen Intervention.

Eine schulmäßige Prüfung der Verfügung des *RP* würde noch in einem zweiten Punkt von der hier gewählten Darstellung abweichen. Sie würde sich Grundrechtsträger für Grundrechtsträger und Grundrecht für Grundrecht getrennt vornehmen. Erst nach Abschluss all dieser Einzelprüfungen würde sie die Elemente zu einem verfassungsrechtlichen Gesamturteil zusammenfügen. Das wäre in diesem Fall jedoch nicht nur ermüdend. Vielmehr müsste bei der Anwendung des Übermaßverbots künstlich jeweils unberücksichtigt bleiben, dass der *RP* nicht nur in ein Grundrecht eingreift, sondern in eine ganze Serie.

Schließlich hätte eine schulmäßige Grundrechtsprüfung zwei verschiedene Gegenstände: die Maßnahme des *RP* und die Eingriffsgrundlage, also § 22 Abs. 3 MDStV. Der eigentliche Streitpunkt ist in diesem Fall jedoch, ob der *RP* die Ermächtigungsgrundlage so weit dehnen darf, wie er das getan hat. Die Frage nach einer verfassungskonform engeren Auslegung von § 22 Abs. 3 MDStV fällt deshalb praktisch mit der Frage nach den verfassungsrechtlichen Grenzen für die konkrete Entscheidung des *RP* zusammen. Um das im Folgenden nicht ständig wiederholen zu müssen, wird jeweils nur von der Maßnahme des *RP* die Rede sein.

Diese Maßnahme greift in drei verschiedenen Richtungen in Grundrechte der Access-Provider ein: in ihre Äußerungsfreiheit (a), in ihre unternehmerischen Freiheiten (b) und in die Freiheiten, die sie vor einer aufgezwungenen Rolle als Regulator bewahren (c).

a) Äußerungsfreiheit

Dass die Access-Provider von Art. 5 Abs. 1 GG geschützt sind, wenn sie eine eigene publizistische Aussage machen, versteht sich von selbst. Diese Aussage könnte in der Zusammenstellung der Inhalte liegen, zu denen sie Zugang verschaffen. Wir hatten uns aber bereits vor Augen geführt, dass sie nach der Systematik des MDStV dann ohnehin nicht mehr Access-Provider wären, sondern Webhosts. Insoweit wäre gerade nicht mehr § 6 Abs. 2 MDStV einschlägig, sondern § 7 MDStV. Die Access-Provider wären nicht mehr Nichtstörer, sondern Zustandsstörer.

Auf den ersten Blick könnte man meinen, dass die Access-Provider darüber hinaus nicht von Art. 5 Abs. 1 GG geschützt sind. Dem widerspricht jedoch eine ganze Reihe von Entscheidungen aus dem Presserecht.²⁴¹ Das *BVerfG* schützt nämlich auch den Pressegehilfen mit Art. 5 Abs. 1 Satz 2 GG.²⁴² Es tut das, weil die Pressefreiheit nicht nur als subjektives Recht der im Pressewesen tätigen Personen geschützt ist, sondern auch als objektive Garantie. Eine solche „presseexterne Hilfstätigkeit“ ist dann in den Schutz des Grundrechts einbezogen, wenn sie „typischerweise pressebezogen ist, in enger organisatorischer Bindung an die Presse erfolgt, für das Funktionieren einer frei-

en Presse notwendig ist und wenn sich die staatliche Regulierung dieser Tätigkeit zugleich einschränkend auf die Meinungsverbreitung auswirkt“.²⁴³

So liegt es hier. Die publizistische Leistungsfähigkeit des Internet beruht gerade auf seinem extrem dezentralen Charakter. Nur dadurch wird es möglich, von jedem Computer der Welt mit jedem anderen zu kommunizieren. Diese Infrastruktur könnte kein Anbieter von Inhalten selbst vorhalten. Er muss sich darauf verlassen können, dass das andere für ihn tun, nämlich die Access-Provider und die hinter ihnen stehenden Anbieter des „backbone“. Schwächt der Staat diese Infrastruktur, hat das Auswirkungen auf sämtliche Anbieter von Inhalten im Internet. Diese Infrastruktur ist also für das Funktionieren der freien Kommunikation im Internet vollständig unerlässlich. Ihre Schwächung schlägt unmittelbar auf die Möglichkeiten zur elektronischen Meinungsäußerung durch.

Die Verfügung des *RP* greift in diese Freiheit ein. Das ist schon bei den beiden konkreten Websites der Fall, die unmittelbar Gegenstand des Verfahrens sind. Der *RP* betreibt das Verfahren aber selbst als Pilotverfahren. Er will die Rechtsgrundsätze durchsetzen, die ihm im nächsten Schritt die breitflächige Regulierung missliebiger Inhalte erlauben würden. Was er will, ist mit anderen Worten ein anderes, nämlich ein staatlich reguliertes Internet. Dieses Ziel kann er nur erreichen, wenn die Access-Provider ihr Geschäftsmodell umstellen. Wenn sie den Weg der Proxyserver gehen, müssen sie sogar ganz unmittelbar die technische Architektur des Netzes ändern.

b) Unternehmerische Freiheiten

Die Access-Provider sind Unternehmen. Sie wollen Gewinn erzielen. Durch die Verfügung des *RP* sind deshalb auch ihre unternehmerischen Freiheiten betroffen. Nach der bekannten Faustregel fallen die Gewinnerwartungen verfassungsdogmatisch unter Art. 12 Abs. 1 GG, das Unternehmensvermögen dagegen unter Art. 14 GG.

In beide Grundrechte greift die Verfügung ein. Die Access-Provider müssen zunächst einmal Aufwand treiben, um dem Verlangen des *RP* nachzukommen. Insb. die Installation von Proxyservern ist eine kostspielige Angelegenheit. Die Branche rechnet mit einem Gesamtaufwand von vielen Mio. €. Unterschiedlich leistungsfähige Proxyserver sind zwar auch unterschiedlich teuer. Der Mindestaufwand ist aber nicht unbedeutend. Ebenso liegt es bei den Personalkosten. Sobald Sperrverlangen keine seltene Ausnahme mehr sind, müsste ein Access-Provider dafür besonderes Personal beschäftigen. Ein Teil der zusätzlichen Kosten ist also fix. Seine Höhe hängt nicht vom Geschäftsvolumen des Access-Providers ab. Deshalb sind kleine Access-Provider besonders betroffen. Manche müssten vielleicht sogar ganz aus dem Markt ausscheiden. Dann würde die Maßnahme nicht nur in die Berufsausübungs-, sondern auch in die Berufswahlfreiheit eingreifen.

c) Aufgezwungene Rolle als Regulator

Der *RP* greift auf die Access-Provider nicht nur deshalb zu, weil sie grds. technisch zur Sperrung von Internetzugängen im Stande sind. Wenn er langfristig das Ziel einer Regulierbarkeit des Internet erreichen will, muss er vielmehr im Sinn haben, was mittlerweile modisch gern als regulier-

241) Übersehen bei *Spindler/Volkman*, K&R 2002, 407.

242) *BVerfGE* 77, 346, 354; *BVerfG NJW* 1999, 2106, 2107.

243) *BVerfGE* 77, 346, 354.

te Selbstregulierung bezeichnet wird.²⁴⁴ Er kann im Grunde nur darauf aus sein, durch diese und ähnliche Verfügungen ein Drohpotenzial ggü. den Access-Providern aufzubauen. Dieser Knüppel im Sack soll sie veranlassen, von sich aus so wirksame Sicherungen gegen unerwünschte Inhalte einzuführen, dass es weiterer staatlicher Interventionen gar nicht mehr bedarf. Nur auf diese Weise könnte der *RP* endlose Gerichtsverfahren vermeiden. Vor allem wäre es aber nur auf diese Weise möglich, dass sich die Inhaltskontrolle den schnellen Veränderungen der Inhalte anpasst. Das ist mit rechtsstaatlichen Mitteln nämlich nicht zu bewältigen.

Nimmt man diesen Zusammenhang in den Blick, wird eine dritte Grundrechtsdimension des Falls deutlich, die „grundrechtlichen Grenzen selbstregulativer Inpflichtnahme“.²⁴⁵ Welche Grundrechte einschlägig sind, ist nach wie vor nicht abschließend geklärt.²⁴⁶ Jedenfalls ist dabei die allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG betroffen. Ähnlich wie etwa bei dem Grundrecht auf informationelle Selbstbestimmung hat sie einen hohen Schutzgehalt. Denn der Staat überspielt auf diese Weise ja ganz offen die Trennung zwischen Staat und Gesellschaft. Er gefährdet die Autonomie der Individuen in einem ganz basalen Sinne. Er macht sie zu Bütteln seines eigenen Handelns.

7. Informationsfreiheit der Nutzer

Die Verfügung des *RP* greift nicht nur in die Grundrechte ihrer Adressaten ein, sondern auch in Grundrechte außenstehender Dritter. Zunächst und vor allem sind das die Grundrechte der Internetnutzer auf Information,²⁴⁷ aber

auch auf Äußerung. Sodann gehören aber auch die Grundrechte der Content-Provider sowie der Webhosts hierher.

Der Grundrechtsschutz von Kommunikation ist umfassend. Geschützt sind nicht nur Intermediäre, in unserem Fall also die Access-Provider, sondern auch die Äußernden und die Empfänger.²⁴⁸ Die Empfänger sind also nicht bloß mittelbar dadurch geschützt, dass sich die Äußernden auf Art. 5 Abs. 1 GG berufen können. Vielmehr haben die Empfänger ein selbstständig durchsetzbares Grundrecht.²⁴⁹ Die Vorschrift schützt auch nicht bloß aktives Handeln zur Informationsbeschaffung, sondern auch die schlichte Entgegennahme von Informationen.²⁵⁰ Geschützt ist ein Internetnutzer deshalb selbst dann, wenn sich hinter einem Link etwas Unerwartetes verbirgt oder wenn sich ein Internetangebot durch Push-Technologien selbst Aufmerksamkeit verschafft. Dieser weite Schutzbereich ist beabsichtigt. Das GG will eine möglichst umfassende Unterrichtung des Einzelnen gewährleisten.²⁵¹ Dahinter steht zunächst einmal ein demokratischer Gedanke. Information ist die Voraussetzung für die Meinungsbildung.²⁵² Darauf ist das Grundrecht nach der Überzeugung des *BVerfG* aber nicht beschränkt. Es hat vielmehr auch eine individualrechtliche Komponente, die das Gericht auf Art. 1 GG stützt: „Es gehört 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. Zudem ist in der modernen Industriegesellschaft der Besitz von Informationen von wesentlicher Bedeutung für die soziale Stellung des Einzelnen“.²⁵³

Diese weite Definition des Schutzbereichs schien dem *BVerfG* im Lichte der nationalsozialistischen Erfahrungen ebenso offensichtlich wie unerlässlich.²⁵⁴ Die Informationsfreiheit schützt den Zugang zu allen allgemein zugänglichen Informationsquellen. Das ist eine rein technische Frage.²⁵⁵ Insb. beeinträchtigt ein staatliches Importverbot den Grundrechtsschutz der Information nicht.²⁵⁶ Geschützt sind im Gegenteil gerade ausländische Informationsquellen.²⁵⁷ Die Versuche der nationalsozialistischen Machthaber, ausländische Informationsquellen zu verstopfen, waren ja gerade Anlass für den starken Schutz dieser Freiheit.²⁵⁸ Konsequenter genießt auch der Empfang strafbarer Äußerungen den Schutz dieses Grundrechts.²⁵⁹ Gegen die bloße Information über strafbare Inhalte dürfte der Staat erst dann einschreiten, wenn die Gefahren aus dem Informationsvorgang selbst das grundrechtlich geschützte Interesse an der freien Zugänglichkeit von Informationen überwiegen.²⁶⁰ Schließlich ist die Informationsfreiheit nicht auf den geistigen Vorgang der Kenntnisnahme beschränkt. Von dem Grundrecht sind vielmehr auch die technischen Voraussetzungen des Zugangs zu Informationsquellen mitgeschützt.²⁶¹

Die Rechtsanwendung ist ein taktisches Geschäft. Wer ein großes Ziel im Auge hat, versteckt sich gern hinter einem scheinbar harmlosen Fall. Auch der *RP* hat zu diesem Kunstgriff Zuflucht genommen. Das darf die Gerichte aber nicht dazu verleiten, die Grundrechtsprüfungen auf diesen scheinbar harmlosen Fall zu beschränken. Denn Gegenstand der Prüfung ist ja nicht bloß der Einzelfall, sondern auch die zu Grunde liegende Norm. Wenn das Vorgehen des *RP* in diesem einen Fall den Segen der Gerichte findet, werden der *RP* selbst und andere deutsche Regulatoren den neuen Freiraum schnell nutzen. Der wirkliche Verfahrensgegenstand sind nicht zwei nationalsozialistische Angebote. Es geht um den Erhalt des Internet als Infrastruktur.

244) Aus der reichen Lit. s. nur *di Fabio* in VVDStRL 1997, 235 ff.; *Schmidt-Preuß*, VVDStRL 1997, 160 ff.; *Engel*, Staatswissenschaften und Staatspraxis, 1998, 535 ff.; *Engel*, Die Verwaltung 2001, 1 ff.

245) *di Fabio*, VVDStRL 1997, 258.

246) Vgl. *Engel*, A Constitutional Framework for Private Governance, 2001. http://www.mpp-rdg.mpg.de/pdf_dat/001_4.pdf.

247) Darauf weist zu Recht auch *Stadler*, MMR 2002, 346 f. hin.

248) BVerfGE 27, 71, 79 f.: „...dass es sich bei dem Bezug von Zeitungen um einen zweiseitigen Kommunikationsvorgang handelt, der verfassungsrechtlich sowohl durch die Meinungsäußerungs- und -verbreitungsfreiheit als auch durch die Informationsfreiheit gesichert ist. Deshalb trifft ein Eingriff in den Kommunikationsvorgang beide Bereiche“; ähnlich BVerfGE 90, 27, 31 f.; s. auch *Engel*, ZUM 1988, 511.

249) BVerfGE 27, 71, 81.

250) BVerfGE 27, 71, 82 f.

251) BVerfGE 27, 71, 82 f.

252) BVerfGE 27, 71, 81.

253) BVerfGE 27, 71, 80; ähnlich BVerfGE 90, 27, 31 f.

254) BVerfGE 27, 71, 80 und 84.

255) BVerfGE 90, 27, 32.

256) BVerfGE 27, 71, 83.

257) BVerfGE 27, 71, 84; BVerfGE 90, 27, 32.

258) BVerfGE 27, 71, 84.

259) BVerfGE 27, 71, 85; s.a. *Spindler/Volkman*, K&R 2002, 407 m.w.Nw. Bei der Prüfung der Angemessenheit des Eingriffs beseitigen *Spindler/Volkman* diesen Schutz dann aber wieder vollständig. „Wenn aber gerade in dem möglichen Abruf eines Inhalts und damit gerade in der ‚Information‘ selbst nicht nur eine rechtswidrige Meinungsäußerung, sondern die tatbestandliche Gefahr liegt, kann die Informationsfreiheit die Abrufbarkeit des Inhalts nicht schützen“. Dass sie sich damit in Widerspruch zu ihrer früheren Äußerung setzen, scheinen sie nicht zu bemerken. Ebenso wenig scheint sie zu beunruhigen, dass es dann im Belieben des einfachen Gesetzgebers stünde, wie weit der verfassungsrechtliche Schutz der Informationsfreiheit reicht. Er bräuchte die Abwesenheit einer Information zu diesem Zweck nur zum Schutzgut einer Strafnorm zu machen.

260) BVerfGE 27, 71, 85.

261) BVerfGE 90, 27, 32: „Soweit der Empfang von technischen Anlagen abhängt, die eine an die Allgemeinheit gerichtete Information erst individuell erschließen, erstreckt sich der Grundrechtsschutz auch auf die Beschaffung und Nutzung solcher Anlagen. Andernfalls wäre das Grundrecht in Bereichen, in denen der Informationszugang technische Hilfsmittel voraussetzt, praktisch wertlos“; s. auch *BVerfG DVBl.* 1992, 556, 556.

In der Sprache des Grundrechts auf Informationsfreiheit: Es geht darum, ob dem Staat gestattet sein soll, diese Informationsquelle zu verstopfen. Das eigentliche Grundrechtsproblem für die Nutzer ist nicht der erschwerte Zugang zu den beiden inkriminierten Angeboten. Das eigentliche Problem sind vielmehr die Folgewirkungen für andere Internetangebote.²⁶²

Diese Folgewirkungen liegen auf drei Ebenen. Auf einer ersten Ebene geht es um künftige staatliche Interventionen in andere Inhalte. Bekommt der *RP* in diesem Fall Recht, werden schnell weitere Verfügungen gegen die Access-Provider folgen. Andere Behörden werden sich dem Vorbild anschließen. Schließlich sind nationalsozialistische Inhalte in Deutschland tabuisiert. Da wird sich kein Regulator sagen lassen wollen, er sehe der Erosion des Tabus tatenlos zu.

Auf einer zweiten Ebene liegt die Vorwegnahme solcher Interventionen durch die Anbieter von Inhalten.²⁶³ Wie wirksam dieser Effekt sein kann, zeigen die Angebote auf deutschen Servern. Unstreitig gibt es hier praktisch keine nach §§ 130 oder 131 StGB verbotenen Inhalte. Ebenso unstreitig ist Pornografie auf deutschen Servern durch wirksame technische Sicherungen vor dem Zugriff durch Minderjährige abgeschirmt. Beides ist nicht etwa die Folge einer Serie staatlicher Verfügungen. Vielmehr haben sich die Anbieter von sich aus auf die Forderungen deutscher Regulatoren eingestellt. Zur Verhaltenslenkung genügte die glaubhafte Erwartung, gegen Verletzungen dieser Anforderungen werde vorgegangen. Dieser vorausseilende Gehorsam ist an sich natürlich wünschenswert. Könnte sich die Rechtsordnung darauf nicht verlassen, würde der Regelungsaufwand in vielen Lebensbereichen schnell prohibitiv.

Problematisch sind die Vorwirkungen in unserem Fall aber deshalb, weil die Grenze zwischen erlaubten und verbotenen Äußerungen bei vielen Inhalten im Vorhinein nicht scharf gezogen werden kann. Im Bereich der Pornografie mag man noch Daumenregeln dafür aufstellen, was entblößt und womit in Berührung gebracht werden darf. Bei den rechtsradikalen Äußerungen, die Gegenstand dieses Verfahrens sind, sind solche einfachen Regeln aber schon viel schwerer zu bilden. Man mag den Gebrauch des Hakenkreuzes und Zitate aus Hitlers „Mein Kampf“ verbieten. Aber solche formalen Regeln sind leicht zu umgehen. Schreitet der Staat aber auch gegen die Umgehungen ein, ist das fast unvermeidbar, was das amerikanische Recht so plastisch einen „chilling effect“ nennt.²⁶⁴

Letztlich geht es dabei um ein altes philosophisches Problem. Eine maßgeschneiderte Lösung steht der Verfassung nicht zu Gebote. Sie muss vielmehr zwischen zwei Fehlern wählen. Der *RP* möchte möglichst viele problematische Inhalte auch wirklich aus dem Netz verbannen. Dieses Ziel kann er nur erreichen, wenn er hinnimmt, dass viele verfassungsrechtlich eigentlich tolerierbare Inhalte ebenfalls unzugänglich werden. Das amerikanische Verfassungsrecht schlägt sich eindeutig auf die Seite des spielbildlichen Fehlers. Damit nicht fälschlich verfassungsrechtlich tolerable Inhalte verboten werden, nimmt es hin, dass auch manche verbotenen Inhalte zugänglich bleiben.²⁶⁵ Die Entscheidung zwischen diesen beiden Fehlern verlangt offensichtlich ein Abwägungsurteil. Dieses Urteil gehört verfassungsdogmatisch erst zu den Grundrechtsschranken, genauer zur Prüfung der Angemessenheit. Die Verfassungsinterpretation darf den Weg zu diesem sachlich angemessenen Abwägungsvorgang nicht vorzeitig ab-

schneiden. Zum Schutzbereich der Informationsfreiheit müssen deshalb auch diese vorhersehbaren Wirkungen auf das Verhalten anderer Personen gehören, die sich äußern, äußern wollen oder ohne die Sorge um staatliche Eingriffe äußern würden.

Hat man die Zusammenhänge einmal so weit verstanden, erschließt sich die dritte, praktisch wichtigste verfassungsrechtliche Ebene. Behält der *RP* Recht, wird die von den Gerichten gebilligte neue Regel nämlich nicht nur Vorwirkungen auf das Verhalten anderer Anbieter von Inhalten haben. Vielmehr wird sie sich vor allem auf das Verhalten der Access-Provider auswirken. Kaum ein Access-Provider wird mit der Sorge um häufige staatliche Interventionen leben wollen. Sein Geschäft würde dadurch beständig gestört. Er käme immer wieder ggü. seinen Kunden in Erklärungsnot. Auch hier wird es deshalb zum vorausseilenden Gehorsam kommen. Noch wahrscheinlicher ist es, dass die Verbände der Access-Provider in Verhandlungen mit den Regulatoren treten. Sie werden anbieten, von sich aus für die Inhaltskontrolle der Angebote zu sorgen, wenn die Regulatoren glaubhaft versprechen, auf staatliche Interventionen zu verzichten. Das ist die mittlerweile gut eingespielte Logik der staatlich regulierten Selbstregulierung,²⁶⁶ von der schon die Rede war. Sie findet „im Schatten des Rechts“ statt.²⁶⁷ Die Regelungsmacht des Staats wandelt sich zum Drohpotenzial in Verhandlungen mit den organisierten Adressaten.²⁶⁸

Für die Nutzer des Internet ist private Regulierung nicht angenehmer als staatliche. Wenn der Staat private Unternehmen in die Rolle von Regulatoren zwingt, muss er für das Ergebnis auch die Verantwortung übernehmen.²⁶⁹ Dabei delegiert der Staat regelmäßig allerdings keine Regelungsmacht an Unternehmen oder Verbände. Er inkorporiert deren Normen meist auch nicht in die staatliche Rechtsordnung. Dann muss sich die juristische Kontrolle auf die Akte konzentrieren, mit denen der Staat Druck auf die künftigen privaten Regulatoren ausübt. Grundrechtsdogmatisch bedeutet das, dass die vorhersehbaren Folgen dieses Drucks mit den Grundrechten der künftigen Adressaten privater Regelungstätigkeit vereinbar sein müssen.

Die Sorge um die Wirkungen solcher privater Regulierung steht im Zentrum der amerikanischen verfassungsrechtlichen Diskussion über das Internet. Entsprechend der Verfassungstradition geht es dort allerdings weniger um rassistische oder nationalsozialistische Äußerungen und mehr um Pornografie. In der kürzesten Formel lautet die Sorge: „Es mag uns gelingen, das Internet für unsere Kinder sicher zu machen. Aber gleichzeitig machen wir es dadurch auch

262) So auch *Stadler*, MMR 2002, 346.

263) Dass hier das eigentliche Ziel liegt, hebt auch *Hornig*, ZUM 2001, 855 hervor.

264) Diese stehende Redewendung der amerikanischen Verfassungsrechtsprechung hat etwa die Aufhebung des Communications Decency Act CDA getragen, *U.S. Supreme Court, ACLU v. Reno*, 117 S.Ct. 2329 (1997).

265) Grundlegend zu dieser Unterscheidung zwischen einem Fehler erster und zweiter Ordnung *Lübbe*, in: Engel/Halfmann/Schulte (Hrsg.), *Wissen, Nichtwissen, unsicheres Wissen*, 2002; s.a. speziell für die Internetregulierung *Lessig/Resnick*, *Michigan Law Review* 1999, 416.

266) S. o. II. 4.

267) So die plastische Formulierung von *Scharpf*, *Games Real Actors Play*, 1997, S. 197.

268) Zur rationaltheoretischen Logik dieses Vorgehens näher *Scharpf* (o. Fußn. 267), S. 195–205; *Engel*, *Staatswissenschaften und Staatspraxis*, 1998, S. 535 ff.

269) Näher *Engel* (o. Fußn. 246).

anfällig für jede Art von Regulierung.²⁷⁰ Zunächst hätten private Regulatoren nicht weniger als der Staat zu entscheiden, welcher Fehler schwerer wiegt: zu viel oder zu wenig Inhalte zu sperren.²⁷¹ Das Problem wiegt bei privater Regulierung sogar noch schwerer.

Der Staat wird von den Access-Providern als privaten Regulatoren Leistungen erwarten, die er selbst gar nicht erbringen könnte. Denn der komparative Vorteil dieser Regulatoren liegt in ihrer Nähe zur Technik. Sie brauchen keine Verwaltungsakte zu erlassen, wenn ihnen Inhalte missfallen. Sie sperren einfach den Zugang zu ihnen. Auch bei der Auswahl dieser Inhalte würden die Access-Provider keine Gremien nach Art der Filmselfkontrolle einsetzen, sondern Text- oder Bilderkennungsprogramme. Solche Programme haben unvermeidlich eine beachtliche Fehlerrate.²⁷² Dieses Problem wiegt gerade bei dem Versuch schwer, nationalsozialistische Inhalte herauszufiltern. Anders als bei pornografischen Texten verschafft die bloße Suche mit einer kleinen Liste von Signalworten nämlich keine ausreichende Sicherheit.²⁷³

All das ist deshalb so bedeutsam, weil private Regulatoren noch stärker als jede staatliche Behörde geneigt sein werden, im Zweifel lieber zu viel als zu wenig zu blockieren.²⁷⁴ Denn ihre regulierende Tätigkeit ist ja mit keinerlei rechtsstaatlichen oder demokratischen Sicherungen verbunden. Jede einzelne versehentlich nicht gesperrte Seite mit rechtswidrigem Inhalt lässt das Risiko staatlicher Interventionen wiedererstehen. Umgekehrt brauchen die privaten Access-Provider bei zu viel Kontrolle nicht zu befürchten, dass ihnen die Kunden davonlaufen. Die Sperrtechnik lässt sich so programmieren, dass den Kunden die Sperrung regelmäßig gar nicht auffällt. Vor allem verhindert die Inpflichtnahme des Verbands aber, dass einzelne Verbandsmitglieder ein weniger stark gefiltertes Angebot als Wettbewerbsvorteil nutzen.

270) *Lessig/Resnick*, Michigan Law Review 1999, 423: „We might make the Net safe for kids, but in consequence make it a fundamentally regulable space“.

271) S.a. *National Research Council* (o. Fußn. 195), 12.1.2.

272) Technischer gesprochen: solche Programme arbeiten notwendig probabilistisch, intervenieren also ab einer vorab definierten Wahrscheinlichkeit, dass eine Seite einen problematischen Inhalt hat, näher *National Research Council* (o. Fußn. 195), C.1.

273) Vgl. o. Fußn. 195, C.1.1.

274) Vgl. o. Fußn. 195, 12.1.2 und 12.1.3. Weitere Belege aus der amerikanischen Praxis bei *Nachbar*, Minnesota Law Review 2000, 266 f.: Der kommerzielle Filter RSACi verwendet viel strengere Kriterien zur Filterung von „hate speech“ als nach amerikanischem Verfassungsrecht zugelassen; s. auch *Lessig/Resnick*, Michigan Law Review 1999, 425.

275) Aufmerksamkeit hat vor allem *Lessig* (o. Fußn. 64) erregt.

276) *Lessig* (o. Fußn. 64), S. 13.

277) *Lessig* (o. Fußn. 64), S. 15–17 spricht davon, dass die Lösungen „hardwired“ sind; s. auch schon *Reidenberg*, Emory Law Journal 1996, 911 ff. dort bei Fußn. 61.

278) *Reidenberg*, Texas Law Review 1998, 582 und 587.

279) *Reidenberg*, Emory Law Journal 1996, 911 ff. dort bei Fußn. 61.

280) Das berichtet *Nachbar*, Minnesota Law Review 2000, 265 über das Programm CYBERSitter; s.a. *Köhntopp/Köhntopp/Seeger*, K&R 1998, 25 ff.

281) *Köhntopp/Köhntopp/Seeger*, K&R 1998, 25 ff.

282) *Reidenberg*, Jurimetrics 2002, dort bei Fußn. 68: „To the extent that societies are censor-happy, they will be marginalized on the Internet. The potential risk to doing business in oppressive societies will serve to discourage companies from supporting those repressive regimes through commercial activities“.

283) *Samuelson*, in: Marsden, Regulating the Global Information Society, 2000, dort bei Fußn. 82.

284) Auf die nachteiligen Folgen für die Kultur des Internet heben ab *Lessig/Resnick*, Michigan Law Review 1999, 423; *Nachbar*, Minnesota Law Review 2000, 247–259.

285) *Lessig/Resnick*, Michigan Law Review 1999, 415.

Die Grundrechte der Internetnutzer werden außerdem durch die Regelungstechnik gefährdet, zu der die Access-Provider greifen werden. Wir hatten bereits darauf hingewiesen, dass sie das Regelungsziel des Staats mit hoher Wahrscheinlichkeit über technische Regeln erreichen werden. Solche „regulation by code“ ist zu einer zentralen Sorge der amerikanischen Verfassungspolitik geworden.²⁷⁵ Soziale Probleme können auf diese Weise „wegprogrammiert“ werden.²⁷⁶ Die Lösungen werden, wie bei einer integrierten Schaltung, eingebrannt.²⁷⁷ Diese Regelungstechnik entzieht sich fast vollständig öffentlicher, vor allem demokratischer Kontrolle.²⁷⁸ Außerdem ist sie extrem unflexibel.²⁷⁹

Durch die Drohung mit weiteren Verfügungen nach Art des *RP* nimmt der Staat zwar Einfluss auf das private Regulierungsgeschehen. Zur Feinsteuerung eignet sich diese Steuerungstechnik aber nur schlecht. Deshalb wird der Staat nicht verhindern können, dass auch Dritte von den neuen Chancen zur Kontrolle der Internetkommunikation Gebrauch machen. Weil der Staat diese Entwicklung veranlasst hat, ist sie ihm für Zwecke der Grundrechtsprüfung auch zuzurechnen. Zu besorgen ist zunächst einmal, dass die privaten Kontrolleure eigene Kontrollwünsche entwickeln. Dass dies keine bloß theoretische Sorge ist, zeigt sich bei den schon jetzt verkauften Filterprogrammen. So verhindern sie etwa oft auch den Zugang zu kritischen Diskussionen über ihr eigenes Tun.²⁸⁰ Manche verfolgen sogar eine eigene politische Agenda.²⁸¹ Ist die Kontrolltechnik einmal etabliert, würden die Access-Provider auch für gesellschaftlichen Druck anfällig. Dann wäre politische Korrektheit nicht mehr bloß eine soziale Norm. Das politisch Inkorrekte wäre vielmehr schlicht technisch unzugänglich.

Schließlich sind die Folgen eines solchen Prozesses für die Entwicklung des Internet zu bedenken. Aus verfassungsrechtlicher Perspektive mag das zunächst wie eine so entfernte und unsichere Entwicklung erscheinen, dass sie vernachlässigt werden kann. Die Logik der regulierten Selbstregulierung bedeutet aber, dass es keine späteren Akte mehr geben wird, die dem Staat zugerechnet werden können. Soll den Adressaten der Grundrechtsschutz nicht vollständig genommen werden, müssen auch solche ferneren Wirkungen deshalb sofort in die Untersuchung einbezogen werden.

Bleibe diese Entwicklung auf Deutschland oder wenigstens auf eine überschaubare Zahl von Staaten beschränkt, würden sich diese Staaten immer stärker vom Internet abkoppeln. Die ausländischen Anbieter von Inhalten würden nicht nur auf aktive Anstrengungen verzichten, auch in Deutschland zugänglich zu sein. Sie würden also etwa keine Angebote in deutscher Sprache mehr machen. Je größer die Sorge um deutsche Interventionen wird, desto eher würden sie vielmehr umgekehrt sogar technische Sicherungen vorsehen, um in Deutschland möglichst nicht zugänglich zu sein.²⁸² Zumindest im Inland würde außerdem die Dynamik der Entwicklung und Verbreitung des Internet gebremst.²⁸³ Die Wahrnehmung des Internet als ein dynamisches Forum, als ein Ort der schnellen und kreativen Entwicklung würde sich ändern.²⁸⁴ Nicht zuletzt würde sich die technische Fortentwicklung des Internet verlangsamen.²⁸⁵ Während die zuletzt genannten Wirkungen erst nach einiger Zeit sichtbar sein werden, tritt ein anderer Nachteil sofort ein: Jede Form der Filterung verlangsamt den Internetverkehr erheblich. Dass es dabei nicht um einen trivialen Effekt geht, sieht jeder, der auf einem etwas älteren Computer einen leistungsfähigen Virensch scanner in-

stalliert. Was er dort im Kleinen beobachten kann, würde bei den Access-Providern im Großen eintreten, wenn der *RP* Recht behielte.

Wenn sich die lokale Architektur des Internet ändert oder der Zugang zum Netz erschwert wird, greift das nicht nur in die Informationsfreiheit, sondern auch in die Äußerungsfreiheit außenstehender Dritter ein. Für sie wird es künftig schwieriger, über das Internet mit anderen Menschen in Kontakt zu kommen oder auf einer Website Äußerungen an eine begrenzte oder unbegrenzte Öffentlichkeit zu machen. Diese Freiheit ist ebenfalls von Art. 5 Abs. 1 GG geschützt.

Die bisherigen Überlegungen haben mit den unmittelbaren und mittelbaren Wirkungen der Verfügung des *RP* auf die Internetkommunikation argumentiert. Der darin enthaltene staatliche Anreiz zur Selbstregulierung lässt sich auch noch mit einem zweiten dogmatischen Instrument erfassen. Denn die Freiheitsgrundrechte haben auch eine verfahrensrechtliche Dimension. Zu ihrem Schutzbereich gehören auch solche Verfahrensvorschriften, die den sinnvollen Gebrauch des materiellen Grundrechts erst ermöglichen. Das hat das *BVerfG* ausdrücklich auch für die Informationsfreiheit bestätigt.²⁸⁶ Da der *RP* die Internetnutzer sehenden Auges der regulierenden Tätigkeit der Access-Provider aussetzt, greift seine Maßnahme auch in diese Dimension der Informationsfreiheit ein.

8. Schranken

Die Verfügung des *RP* greift also in die Freiheiten der Access-Provider aus Art. 5 Abs. 1, 12 Abs. 1 und 2 Abs. 1 GG ein sowie in die Informationsfreiheit und die Äußerungsfreiheit der Nutzer aus Art. 5 Abs. 1 GG, Art. 2 Abs. 1 GG enthält keine benannten Schranken. Zur „verfassungsmäßigen Ordnung“ gehört jedes formell und materiell verfassungsgemäß zu Stande gekommene Gesetz. Aus Art. 12 Abs. 1 Satz 2 GG hat das *BVerfG* zwar die bekannte Drei-Stufen-Lehre abgeleitet. Bei näherer Betrachtung enthält aber auch sie letztlich nur Vorgaben für die Gewichtung des Grundrechts bei der Anwendung des Verhältnismäßigkeitsgrundsatzes. Bei beiden Grundrechten genügt also ein vom Verfassungstext zunächst nicht weiter spezifiziertes legitimes Ziel (d). Art. 5 Abs. 1 GG hat dagegen benannte Schranken. Zensur ist kategorisch verboten (a). Diskutiert werden auch besondere Schranken der Informationsfreiheit (b). Jedenfalls sind Eingriffe in das Grundrecht nach Art. 5 Abs. 2 GG nur dann zulässig, wenn sie auf einem „allgemeinen Gesetz“ beruhen (c).

a) Zensurverbot

Zensur ist nach Art. 5 Abs. 1 Satz 3 GG kategorisch verboten. Eine Rechtfertigung scheidet also auch dann aus, wenn die Maßnahme an sich einem „allgemeinen Gesetz“ i.S.v. Art. 5 Abs. 2 GG genügen würde.²⁸⁷ Dass die Verfügungen des *RP* tatsächlich als Vorzensur zu qualifizieren sind, haben wir bereits dargelegt, als wir das Verhältnis von § 22 Abs. 3 MDStV zu den strafprozessualen Vorschriften über die Pressebeschlagnahme untersucht haben.²⁸⁸ Gerade am Zensurverbot lag es ja gerade, dass § 22 Abs. 3 MDStV unanwendbar ist.

b) Schranken der Informationsfreiheit

Der ausdrückliche verfassungsrechtliche Schutz der Informationsfreiheit ist eine direkte Reaktion auf die nationalsozialistischen Verhältnisse. Dort musste bekanntlich gravierende Sanktionen gewärtigen, wer beim Hören von

BBC erwischt wurde. Vor diesem Hintergrund ließe sich begründen, dass jeder Eingriff in die Informationsfreiheit von vornherein unzulässig ist. So weit geht das *BVerfG* allerdings nicht. Eingedenk des historischen Zusammenhangs lässt es für Eingriffe in die Informationsfreiheit aber nicht genügen, dass die Äußerung von Verfassungen wegen verboten werden dürfte. Vielmehr muss der Staat nachweisen, dass auch die Kenntnisnahme der verbotenen Äußerung eine ernst zu nehmende Gefahr darstellt.²⁸⁹

c) Allgemeine Gesetze

Wir haben uns bereits klar gemacht, dass § 22 Abs. 3 MDStV im konkreten Fall von den Vorschriften zum Schutz der wehrhaften Demokratie überlagert wird.²⁹⁰ Das liegt gerade an den Anforderungen, die Art. 5 Abs. 2 GG an ein „allgemeines Gesetz“ stellt. Unstreitig ist ein Gesetz nämlich kein allgemeines im Sinne dieser Vorschrift mehr, wenn es eine ganz bestimmte Meinung verbietet oder an ihre Äußerung Nachteile knüpft.²⁹¹ Genau das geschieht hier. Der *RP* hat die beiden Websites gerade deshalb herausgegriffen, weil sie nationalsozialistische Äußerungen zum Gegenstand haben. Die Rechtfertigung seines Eingriffs scheitert deshalb von vornherein an Art. 5 Abs. 2 GG. Denn Art. 5 Abs. 2 GG wird nur von den verfassungsgemäß zu Stande gekommenen Vorschriften zum Schutz der wehrhaften Demokratie durchbrochen.

d) Legitimes Ziel

Wer all dem nicht folgen will, muss schließlich danach fragen, welches Ziel der *RP* denn verfolgt, und ob es i.S.d. Grundrechte legitim ist, in die seine Maßnahmen eingreifen. Der *RP* stützt sich auf § 12 Abs. 1 Nr. 1 MDStV i.V.m. §§ 130 und 131 StGB. Er will also nationalsozialistische Äußerungen verhindern, weil er sie für volksverhetzend hält. Hält man all die gerade analysierten benannten Schranken nicht für einschlägig, wird man dieses Ziel nicht für illegitim halten können. Das eigentliche Problem bei der Bestimmung des legitimen Ziels sind die Verfeinerungen, zu denen der *RP* greift. Er will genügen lassen, dass seine Maßnahme die Gefahr verringert. Vielleicht genügt ihm auch bloß ihr symbolischer Effekt. Diese Verfeinerungen immunisieren seine Maßnahmen gegen das Übermaßverbot. Wir müssen sie deshalb im Zusammenhang mit den einschlägigen Maßstäben des Übermaßverbots diskutieren.

9. Geeignet/technisch möglich

a) Einführung

Normalerweise ist die Aussage zur Geeignetheit nichts als eine dogmatische Pflichtübung. Natürlich gibt es theoretisch viele ganz unsinnige staatliche Eingriffe in den Schutzbereich der Grundrechte. Aber in unseren geordneten Verhältnissen weiß der Staat für gewöhnlich, was er tut. Die Grundrechte werden deshalb praktisch ausschließlich für die Abwägung zwischen dem Steuerungsziel des Staats und den Freiheiten seiner Bürger gebraucht. Der Staat wird auf diesem Wege veranlasst, nach weniger freiheitsschädlichen Lösungen zu suchen. Gelegentlich verlangt ihm die Verfassung auch einmal ab, dass er ein Steuerungsziel um der Freiheit seiner Bürger willen ganz aufgibt. In unserem

²⁸⁶ BVerfGE 27, 71, 88.

²⁸⁷ BVerfGE 33, 52, 72.

²⁸⁸ S. oben 1. a).

²⁸⁹ BVerfGE 27, 71, 86 f.

²⁹⁰ S.o. 1. b).

²⁹¹ BVerfGE 27, 104, 110 f.; BVerfGE 95, 220, 235 f.

Fall ist das jedoch anders. Bereits die Geeignetheit der Verfügung des *RP* ist mehr als zweifelhaft. Das liegt am Regelungsgegenstand. Normalerweise ist nämlich allenfalls zweifelhaft, was der Staat darf. Dass er sein Regelungsziel mit Hilfe seiner souveränen Regelungsmacht erreichen kann, steht außer Frage. Genau das staatliche Können ist in unserem Fall dagegen das Problem.²⁹²

Vor diesem Hintergrund wird dann auch deutlich, warum der verfassungsrechtliche Maßstab der Geeignetheit in einem engen inneren Zusammenhang mit dem Erfordernis in § 22 Abs. 3 MDStV steht, das geforderte Handeln müsse technisch möglich sein. § 22 Abs. 3 MDStV formuliert natürlich keine Anforderungen für den regulierenden Staat, sondern für die Access-Provider als Regelungsadressaten. Was die Access-Provider technisch nicht leisten können, kann der Staat aber auch nicht von ihnen verlangen. Außerdem darf er sich wegen der Subsidiarität eines Vorgehens gegen Nichtstörer auf § 22 Abs. 3 MDStV ja nur berufen, wenn ein Vorgehen gegen die eigentliche Quelle der Gefahr für die öffentliche Sicherheit keine Aussicht auf Erfolg hat. Was die Access-Provider nicht können, kann der Staat deshalb regelmäßig auch auf keinem anderen Wege erreichen.

Aus diesem verfassungsrechtlichen Hintergrund folgt zugleich, dass es für das Ergebnis keinen Unterschied machen würde, dass das Tatbestandsmerkmal „technisch möglich“ mittlerweile aus dem Text des MDStV gestrichen wurde. In § 6 Abs. 2 Satz 2 MDStV heißt es stattdessen jetzt: „Verpflichtungen zur Entfernung der Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters unberührt“.

In dieser Norm ist also nicht mehr ausdrücklich davon die Rede, die Sperrung müsse technisch möglich sein. Die amtliche Begründung hebt jedoch zu Recht hervor, dass dadurch keine Änderung in der Sache beabsichtigt war. Vielmehr wollte sich der Gesetzgeber nur so eng als möglich an Struktur und Wortlaut der Richtlinie der EG über den elektronischen Geschäftsverkehr anlehnen.²⁹³

Ob der *RP* im Stande ist, sein normatives Ziel zu erreichen, hängt zunächst einmal von den technischen Möglichkeiten ab (b). Manches, was theoretisch technisch möglich wäre, ist allerdings prohibitiv teuer (c), anderes ist leicht zu umgehen (d). Außerdem ist mit dem Widerstand ausländischer Staaten (e) und mit kontraproduktiven Effekten zu rechnen (f). Kann sich der *RP* gegen all diese Einwände immunisieren, indem er die Definition seines Regelungsziels ändert (g)?

292) Ähnlich Zimmermann, NJW 1999, 3150.

293) BT-Drs. 14/6098, 23 zur Parallelvorschrift in § 8 Abs. 2 Satz 2 TDG.

294) S. aus dem reichen Schrifttum insb. Sieber, CR 1997, 581 ff. u. 653 ff.; Weinberg, Hastings Communications and Entertainment Law Journal 1997, 453; Köhntopp/Köhntopp/Seeger, K&R 1998, 25 ff.; Reidenberg, Texas Law Review 1998, 557–560; Sieber (o. Fußn. 213), S. 43–96; Fox, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, 2001, S. 79 ff.; Lemaire, Filtering Techniques and Methods, 2001; National Research Council (o. Fußn. 196), insb. Chapter 12.

295) Die noch radikalere Lösung, ganze Klassen von Internetdiensten zu sperren, hat der *RP* zu Recht nicht in Betracht gezogen, dazu National Research Council (o. Fußn. 195), 12.1.1. Seit der Entscheidung des Generalbundesanwalts MMR 1998, 93, 96 f. wird außerdem immer wieder einmal der Gedanke eines sog. „Web-Block“ in die Diskussion eingeführt. Das ist auch in diesem Verfahren unter der Bezeichnung „Filter-Pilot“ erneut geschehen. Diese Lösung hat sich jedoch nicht als leistungsfähig erwiesen.

296) Mehr zum technischen Hintergrund <http://www.internic.net/faqs/authoritative-dns.html> (Stand: 19.5.2002).

b) Diskutierte technische Lösungen

„Wo nichts ist, hat der Kaiser sein Recht verloren“, hieß es schon im Gemeinen Recht. Und im Römischen Recht hieß es: „impossibilia nulla est obligatio“; niemand ist verpflichtet, etwas Unmögliches zu tun. Die Access-Provider denken, dass der *RP* genau das von ihnen verlangt. Ein erhebliches Indiz ist schon die Struktur der Verfügung. Der Tenor lautet nur lapidar: „Hiermit gebe ich Ihnen auf, den Zugang zur Nutzung der Internetseiten [...] i.R.d. von Ihnen vermittelten Nutzungsangebotes zu sperren“.

In den Gründen heißt es dann bloß: „Als Ergebnis der von mir durchgeführten technischen Recherchen und des Anhörungsverfahrens ergeben sich für mich nach dem derzeitigen Stand der Technik drei Sperrmöglichkeiten: [...]. Darüber hinaus sind derzeit weitere technische Möglichkeiten in der Erprobung“.

Im Klartext heißt das, dass der *RP* noch gar nicht weiß, welches Verhalten er wirklich von den Adressaten seiner Verfügung erwartet. Ja mehr noch, er weiß nicht einmal, ob eine der von ihm geschilderten Handlungen überhaupt Erfolg haben würde.

Mit dieser Unsicherheit ist der *RP* nicht allein. Vielmehr gibt es im in- und ausländischen Schrifttum seit vielen Jahren eine intensive Diskussion über denkbare Lösungen.²⁹⁴ Diese Diskussion konzentriert sich in der Tat auf die drei in der Verfügung erwähnten Lösungen.²⁹⁵

Die erste Lösung setzt am DNS des Access-Providers an. Das Internet ist ein paketvermittelter Dienst. Anders als etwa beim Telefon wird für die Dauer der Kommunikation also kein Kommunikationsweg zwischen den Kommunikationspartnern geschaltet. Vielmehr wird jeder Kommunikationsakt in kleine Datenpakete zerlegt. Diese Pakete erhalten eine Art elektronischen Briefumschlag. Auf diesem Umschlag steht, für welche Adresse sie bestimmt sind. Da der einzelne Kommunikationsakt fast immer aus mehreren Datenpaketen besteht, steht auf dem Umschlag außerdem, wie die einzelnen Pakete beim Empfänger zusammengesetzt werden sollen. Damit die Pakete ihr Ziel erreichen, müssen Sender und Empfänger eindeutige Adressen haben. Sie bestehen aus einer langen Nummernfolge, den sog. IP-Adressen. Solche langen Nummernfolgen kann man sich schwer merken. Deshalb werden diese Nummern regelmäßig in Buchstabenfolgen übersetzt, die sog. Domainnamen. Wenn der Internetnutzer seine Anfrage an solch einen Domainnamen richtet, muss die Buchstabenfolge in die Zahlenfolge zurückübersetzt werden.

Damit das Internet funktionieren kann, darf es bei dieser Übersetzung keine Fehler geben. Dafür sorgen auf der obersten Ebene 13 von der Internationalen Organisation ICANN betriebene Server. Nur Domainnamen, deren Schlusskürzel (etwa .de) dort eingetragen ist, dürfen verwendet werden. Auf diese Weise sorgt ICANN dafür, dass Domainnamen wirklich eindeutige Adressen sind. Würden die gesamten Anfragen aber über diese 13 Server geführt, könnte das Internet nur ganz kleine Datenmengen verarbeiten. Die massenhafte Nutzung des Internet wird erst dadurch möglich, dass die Domainnamen hierarchisch strukturiert sind und die Anfragen daher verteilt bearbeitet werden können. Jeder Access-Provider betreibt in der Regel einen oder mehrere Server, die für seine Kunden die Umsetzung der Domainnamen in Zahlenfolgen bewerkstelligen. Technisch geschieht die Übersetzung also dezentral. Das Lexikon wird, um im Bilde zu bleiben, aber von ICANN zentral geführt.²⁹⁶

Wenn die Access-Provider auf Geheiß des *RP* problematische Domainnamen auf ihren lokalen DNS sperren, sind diese Inhalte für ihre Kunden auf diesem Wege nicht mehr zu erreichen. Damit ist allerdings nicht viel gewonnen. Zunächst ist die Übersetzung der IP-Adressen in Domainnamen ja nur eine Erleichterung für die Nutzer. Sie können die Inhalte nach wie vor erreichen, wenn sie statt des Domainnamens unmittelbar die IP-Adresse in ihren Browser eingeben.²⁹⁷ Diese Adresse können sie sich über eine Suchmaschine besorgen. Außerdem kann ein Nutzer statt des zensierten DNS seines eigenen Access-Providers auch einen anderen DNS benutzen. Die gängigen Browser sind dafür auch vorbereitet. Mit wenigen Handgriffen lassen sie sich auf einen anderen DNS umstellen. Der *Chaos Computer Club* hat in Reaktion auf die Verfügungen des *RP* eine Anleitung ins Netz gestellt, die auch Unkundigen erklärt, wie man das macht.²⁹⁸ Oft gibt es weitere Auswege. Die Sperrung der Domainnamen im DNS des Access-Providers erfasst Links auf diese Seiten nur dann, wenn sie unmittelbar auf den Domainnamen führen, nicht auf die dahinter stehende IP-Adresse. Auch der Aufruf der Seiten über eine Suchmaschine bleibt offen. Die Sperrung wird auch dann umgangen, wenn die Nutzer ihren Verkehr über einen Anonymisierer leiten. Mit Unterstützung des *Bundeswirtschaftsministeriums* stellt das *Unabhängige Landeszentrum Datenschutz Schleswig-Holstein* eine wirksame Anonymisierungstechnik online zur Verfügung.²⁹⁹

Schließlich ist niemand in Nordrhein-Westfalen gezwungen, einen Access-Provider mit Sitz im Lande zu nutzen. Er kann vielmehr zu einem Provider aus einem anderen Bundesland oder aus dem Ausland wechseln.³⁰⁰ Angesichts immer stärker fallender Preise für TK-Verbindungen ist das auch ökonomisch eine realistische Option. I.U. richtet sich die Verfügung des *RP* ja nur gegen solche Access-Provider, die im Lande Nordrhein-Westfalen niedergelassen sind. Die Verfügung setzt deshalb einen Anreiz für Access-Provider mit Niederlassung außerhalb von Nordrhein-Westfalen, in den nordrhein-westfälischen Ortsnetzen Einwahlmöglichkeiten zu schaffen. Dann gibt es überhaupt keinen finanziellen Unterschied mehr zwischen der Nutzung von Access-Providern aus dem Lande und von außerhalb.

Die Umgehung wird noch einfacher, wenn der Content-Provider oder der Webhost daran mitwirken.³⁰¹ Sie können ihrem Angebot einfach einen anderen Domainnamen geben.³⁰² Die Betreiber vieler rechtsradikaler Seiten verfügen vorsorglich bereits über weitere Domainnamen, unter denen sie ihr Angebot parallel anbieten können. Die Nutzer können ihre Browser so programmieren, dass sie eine Anfrage automatisch auf den neuen Domainnamen umleiten.³⁰³ So ist eine der beiden Websites, gegen die der *RP* vorgeht, mittlerweile auch unter der URL <http://www.nordrhein-westfalen.biz> greifbar.³⁰⁴ Das braucht der Urheber der inkriminierten Inhalte nicht einmal selbst zu besorgen. Vielmehr gehört solche Gegenwehr zum Ehrenkodex der Internetgemeinschaft. Deshalb haben Dritte die fraglichen Seiten mittlerweile schon vielfach erneut unter anderen Domainnamen ins Netz gestellt.

Als zweite Lösung erwähnt die Verfügung des *RP* das Blockieren der IP-Adresse. Wie erwähnt brauchen die Datenpakete eindeutige Adressen. Dass diese Pakete den richtigen Weg durchs Netz finden, ist die Leistung der Router. Jeder Access-Provider hat einen solchen Router. Er kann ihn so konfigurieren, dass Datenpakete mit einer bestimmten

IP-Adresse als Empfänger oder Absender nicht transportiert werden. Weil diese Lösung unmittelbar an den IP-Adressen ansetzt, ist sie durch die Wahl eines anderen DNS nicht zu umgehen. Auch bei dieser Methode bleiben aber zahlreiche andere Umgehungsmöglichkeiten. Die einfachste schaltet zwei Internet-Service-Provider (ISP) hintereinander. Der Nutzer wählt sich von seinem eigenen ISP bei einem zweiten ISP ein, der nicht von Nordrhein-Westfalen kontrolliert wird.³⁰⁵ Dann sieht der Router seines eigenen Providers nur die IP-Adresse des zweiten Providers.

Dieser zweite Provider kann dem fremden Kunden unmittelbar gestatten, seine Vermittlungsdienste in Anspruch zu nehmen. Auch wenn das nicht so ist, wird ein nordrhein-westfälischer Nutzer aber regelmäßig fündig werden. Denn die Inhalte des Internet sind regelmäßig nicht nur auf dem einen Server greifbar, der sie ursprünglich ins Netz gestellt hat. Je häufiger sie abgerufen werden, desto häufiger werden sie vielmehr auf weiteren Servern gespiegelt. Diese Technik macht das Internet schneller und spart Transportkosten. Wenn ein nordrhein-westfälischer Nutzer auf solch eine Spiegelung zugreift, gibt es keinen Transportvorgang mit der IP-Adresse des Urhebers mehr.³⁰⁶ Wiederrum vermehren sich die Umgehungsmöglichkeiten, wenn der Urheber mitwirkt. Insb. kann er ein und demselben Domainnamen häufig wechselnde IP-Adressen zuweisen.³⁰⁷ Solange der DNS weiß, wo sich der Inhalt gerade befindet, ist das technisch kein Problem. Wechselnde IP-Adressen sind auch nicht etwa missbräuchlich. Vielmehr gibt es gute technische Gründe für diese Praxis, etwa bei der Nutzung einer Firewall.

Scheinbar vermeidet die dritte von dem *RP* erwogene Technik diese Nachteile. Die Access-Provider müssten dann zusätzliche Computer installieren, sog. Proxyserver. In diesen Computern würden Filter installiert, die unmittelbar am Inhalt problematischer Seiten ansetzen. Das kann man dem einzelnen Datenpaket regelmäßig nicht ansehen. In dem Proxyserver muss deshalb regelmäßig zunächst das gesamte Dokument zusammengesetzt, kontrolliert und dann als Ganzes oder in Teilen weitergegeben werden. Schon diese wenigen Bemerkungen machen deutlich, dass dabei Quantität leicht in Qualität umschlägt. Der Rechenaufwand wird schnell astronomisch. Soll das Netz überhaupt noch nutzbar bleiben, muss die Kontrollaufgabe deshalb beschränkt werden. So kann man den Filter etwa so konfigurieren, dass er nur Datenpakete mit bestimmten IP-Adressen kontrolliert.³⁰⁸ Dann wird zwar der technische Aufwand überschaubar. Dafür wird die Umgehung aber auch viel leichter.

Vor allem teilt ein staatlich erzwungener Proxyserver aber alle Nachteile von Programmen, die missliebige Inhalte aus dem Netz herausfiltern sollen.³⁰⁹ Selbst wenn solche

297) Stadler, MMR 2002, 343 ff.

298) <http://www.ccc.de/censorship/dns-howto/index.html> (26.5.2002).

299) <http://www.datenschutzzentrum.de/projekte/anon/index.htm> (6.12.2002).

300) Sieber, CR 1997, 664.

301) Lessig/Resnick, Michigan Law Review 1999, 414; National Research Council (o. Fußn. 195), 12.1.2, jew. m. w. Einzelheiten.

302) Lemaire (o. Fußn. 294), S. 10.

303) Lemaire (o. Fußn. 294), S. 9.

304) Stadler, MMR 2002, 343 ff.

305) Köhntopp/Köhntopp/Seeger, K&R 1998, 25 ff.

306) Sieber, CR 1997, 663.

307) Lemaire (o. Fußn. 294), S. 6–9.

308) Köhntopp/Köhntopp/Seeger, K&R 1998, 25 ff.; s. auch Popp (o. Fußn. 37), S. 43.

309) Umfassend National Research Council (o. Fußn. 195), insb. 12.1.2 und 12.1.7.

Programme keinen rechtsstaatlichen Schranken unterliegen, ist ihre Wirksamkeit höchst unsicher. Das gilt, wie bereits erwähnt, ganz besonders bei der Kontrolle auf rassistische oder nationalsozialistische Inhalte. Bei solchen Äußerungen besteht, anders als bei Pornografie, nämlich kein hinreichend sicherer Zusammenhang zwischen der Verwendung einer geringen Zahl von Worten und der Angreifbarkeit des Inhalts.³¹⁰ Schließlich fallen an einem Proxyserver des Access-Providers „logfiles“ an. Auf diese Weise wird das Nutzungsverhalten seiner Kunden also an einer zentralen Stelle vollständig gespeichert. Aus Datenschutzgründen ist das eine höchst problematische Gestaltung.

Auch die Erfahrungen mit vergangenen Versuchen zur Sperrung von missliebigen Inhalten des Internet gemahnen zur Vorsicht. Der Versuch deutscher Ermittlungsbehörden, den Zugang zu dem rechtsradikalen Internetangebot des kanadischen Neonazis *Ernst Zündel* zu sperren, ist kläglich gescheitert. Amerikanische Universitäten spiegelten das Angebot auf ihren Servern. Die Sperrung dieser Server hätte so große Nachteile für die deutsche Wissenschaft gehabt, dass sie praktisch nicht in Betracht kam. Auch das Ermittlungsverfahren des *Generalbundesanwalts* gegen die elektronische Verbreitung des Magazins „radikal“ ist gescheitert. Im Januar 1997 wurde gegen die *stellvertretende Vorsitzende der PDS* ein Ermittlungsverfahren eingeleitet, weil sie auf ihrer deutschen Homepage einen Link zu dem Magazin eingerichtet hatte. Das Magazin befürwortet den Umsturz von Regierungen mit terroristischen Mitteln. Die deutschen ISP hatten sich seinerzeit vom *Generalbundesanwalt* bewegen lassen, den Zugriff auf den holländischen Webhost *XS4ALL* zu blockieren, der die fragliche Ausgabe von „radikal“ bereithielt. Der Host ließ jedoch keine Gelegenheit ungenutzt, IP-Adressen und Ports zu wechseln. Zahlreiche Mirror Sites entstanden. Das Magazin wurde alternativ auch über das File Transfer Protocol (FTP) zur Verfügung gestellt. Schließlich wurden über das Internet 25 niederländische Telefonnummern verbreitet, mit denen sich Nutzer unter Umgehung ihres ISP direkt einwählen und das Magazin abrufen konnten. Nach zwei Wochen gab der *Generalbundesanwalt* den Versuch auf, den Zugang zu der Ausgabe von „radikal“ zu verhindern.³¹¹

c) Prohibitive Regulierungskosten

Das GG konzipiert Deutschland als eine wehrhafte Demokratie. Grundrechtseingriffe sind auf dieser Grundlage prinzipiell möglich, wenn sie zum Schutz der freiheitlich demokratischen Grundordnung erforderlich sind. Prinzipiell kann man das bei einem Vorgehen gegen rechtsradikale Propaganda schwerlich verneinen. Wenn es dem *RP* aber bloß gelingt, den Zugang zu ganzen zwei Websites zu sperren, ist für das in sich legitime Regelungsziel praktisch nichts gewonnen. Der *RP* geht, wie schon mehrfach erwähnt, selbst davon aus, dass es etwa 6.000 Websites mit ähnlich radikalen Inhalten gibt. Der *RP* müsste also in getrennten Verfügungen an alle Access-Provider Tausende

von Domainnamen auflisten. Zuvor müsste er die nötigen Informationen erheben und dazu ständig das Internet durchsuchen. Jede dieser Verfügungen könnte mit Widerspruch und Anfechtungsklage angegriffen werden. Für jede einzelne Website müsste der *RP* den Beweis des strafbaren Inhalts antreten.

An sich werden Verwaltungsakte mit Ablauf der Widerspruchs- oder Klagefrist bestandskräftig. Urteile der Verwaltungsgerichte werden rechtskräftig. Beides gilt aber nur für den Sachverhalt, auf den sich die Entscheidung bezogen hat. Der Inhalt von Websites verändert sich dagegen ständig. Deshalb muss der Access-Provider vortragen können, dass eine gesperrte Seite mittlerweile keine rechtswidrigen Inhalte mehr enthält. Am ehesten kann man dem verfahrensrechtlich mit dem Gedanken des Dauer-Verwaltungsakts bzw. eines Urteils mit Dauerwirkung entsprechen. Konsequenter muss der Access-Provider dann die Möglichkeit zur Abänderungsklage haben. Im Verwaltungsverfahren verengt sich aus diesem Grunde das Ermessen der Behörde bei der Entscheidung über das Wiederaufgreifen des Verfahrens. Auch ohne ausdrücklichen Antrag der Access-Provider hat die Behörde nach §§ 48 Abs. 1 Satz 1, 49 Abs. 1 VwVfG ein Ermessen für die Aufhebung rechtswidrig gewordener Verwaltungsakte.³¹² Da die abstrakte Wahrscheinlichkeit hoch ist, dass sich der Inhalt von Websites ändert, wird man annehmen müssen, dass die Behörde zur Beobachtung verpflichtet ist. Auch aus diesem Grunde kommt es also zur Regulierung und zum Rechtsschutz als Dauerzustand.

Solche Sperrungen sind belastende Verwaltungsakte mit belastender Drittwirkung. Denn den Anbietern der Websites wird ja durch Hoheitsakt die Verbreitungschance genommen. An sich müssten ihnen die Verfügungen deshalb amtlich zugestellt werden. Wenn sich das als praktisch undurchführbar erweist, bleibt die Wirksamkeit der Verfügung lange in der Schwebe. Denn bis ein Jahr, nachdem sie nachweislich von der Sperrung Kenntnis erlangt haben, können sich die Anbieter der Websites dagegen mit Widerspruch und Anfechtungsklage zur Wehr setzen. So lange sind die Verfügungen nicht bestandskräftig. Vor allem würden die Anbieter dieser Websites den Sperrungen aber nicht tatenlos zusehen. Sie würden anfangen, ihre Websites umzubenennen, zu ändern oder auf andere Server zu verlagern. Darauf müsste der *RP* mit neuen, erneut angreifbaren Verfügungen reagieren. Es käme zu einem Wettlauf zwischen Hase und Igel. Von vornherein steht fest, dass der *RP* diesen Wettlauf nur verlieren kann. Die Regulierungskosten sind nicht nur hoch, sie sind prohibitiv hoch. Auch aus diesem Grunde ist die Maßnahme nicht geeignet, das Ziel zu erreichen.

d) Gegenwehr der Internetgemeinde

Ungeeignet ist die Maßnahme außerdem deshalb, weil sie die Möglichkeiten zu einer Änderung der Struktur des Internet außer Acht lässt. Einen derart massiven Versuch zur staatlichen Inhaltskontrolle des Internet hat es bislang in einem modernen, freiheitlichen Land noch nicht gegeben. Umso intensiver wird sich die Internetgemeinde wehren, sollte der *RP* Recht behalten.³¹³ Die Möglichkeiten dazu sind zahlreich. Sie würden dazu führen, dass das Internet schließlich sogar noch schlechter zu kontrollieren ist als bislang.

Im ersten Schritt können die Nutzer den Internetverkehr verschlüsseln. Dann sieht ein Filterprogramm nur noch inhaltsleere Zahlenreihen.³¹⁴ Außerdem können sie ihren

310) Vgl. o. Fußn. 195, C.1.1.

311) Sieber (o. Fußn. 213), Rdnr. 194 f.

312) Auf die streitige Frage, ob es sich dabei um einen Fall der Rücknahme oder des Widerrufs handelt, kommt es an dieser Stelle nicht an.

313) Charakteristisch für die Einstellung der Internetgemeinde ist das geflügelte Wort von *John Gilmore*: „The Net interprets censorship as damage and routes around it“, zit. n. *Boyle*, University of Cincinnati Law Review 1997, 178.

314) *Lemaire* (o. Fußn. 294), S. 10; grundlegend zur Kryptographiepolitik *National Research Council* Cryptography's Role in Securing the Information Society, 1996.

Verkehr über Anonymisierer und Remailer umleiten. Dann sieht der DNS die ursprüngliche Domain nicht mehr. Der Router sieht nur noch die IP-Adresse des Anonymisierers.³¹⁵ Genügt den Nutzern das noch nicht, können sie die verschlüsselten und anonymisierten Datenpakete noch zusätzlich mit harmlosen Inhalten gleichsam ummanteln. Das pornografische Bild gelangt dann als religiöse Hymne verkleidet in ein arabisches Land.³¹⁶ Eine zwar primitive, häufig aber wirksame Gegenwehr besteht auch in der Nutzung anderer Zugänge zum Internet. Wer sich zu Hause oder in seinem Unternehmen zu sehr kontrolliert fühlt, greift dann eben von einem mobilen Anschluss, über Satellit oder von einem Cybercafé aus auf die gewünschten Inhalte zu.³¹⁷

Die radikalste Reaktion ist bislang noch kaum ins deutsche öffentliche Bewusstsein gedrungen. Sie firmiert unter Namen wie *Gnutella* und *FreeNet*.³¹⁸ Der Grundgedanke ist einfach. Wenn eine Inhaltskontrolle im Internet überhaupt möglich ist, dann deshalb, weil Inhalte an einem genau definierten technischen Ort vorgehalten werden. *Gnutella* und *FreeNet* lösen auch noch diesen einzigen Angriffspunkt für staatliche Interventionen auf. Wer sich an einem solchen System beteiligt, stellt der Gemeinschaft der Nutzer einen Teil seiner Festplatte zur Verfügung. Das Programm ist so gestaltet, dass er nicht weiß, welche Inhalte auf seiner Festplatte lagern. Ja, er kann das durch technische Sicherungen nicht einmal erfahren. Im Gegenzug wird er zum Mitglied einer Gemeinschaft von etwa 10.000 Nutzern. Er erhält eine Art Suchmaschine, um auf all diesen 10.000 Festplatten nach den Inhalten zu suchen, die ihn interessieren. Wird die Suchmaschine fündig, übermittelt sie ihm den Inhalt, ohne dass der Eigentümer der Festplatte davon etwas erfährt. Wenn er selbst der Gemeinschaft einen Inhalt zur Verfügung stellen will, transportiert die Software ihn auf eine Festplatte, die niemand kennt. Diese Technik ist ganz bewusst entwickelt worden, um staatliche und rechtliche Kontrolle praktisch unmöglich zu machen.

e) Widerstand ausländischer Staaten

Die Verfügungen des *RP* richten sich direkt gegen zwei Angebote, die in den USA verfassungsrechtlichen Schutz genießen. Ebenso direkt richtet sich der *RP* gegen die libertäre Internetgemeinde. Sie ist nicht nur in den USA gewachsen. Vielmehr hat sie auch nach wie vor dort ihren Schwerpunkt. Weder der amerikanische Staat noch die amerikanischen Internetaktivisten werden den *RP* einfach gewähren lassen. Vielmehr ist mit harschen Reaktionen zu rechnen.³¹⁹ Sie werden nach Kräften danach trachten, der Maßnahme des *RP* ihre Wirksamkeit zu nehmen. Für sich allein wäre diese Erwartung zwar zu wenig spezifiziert, um die Geeignetheit der Maßnahme auszuschließen. Im Zusammenhang mit all den übrigen Gründen stützt sie die Zweifel an der Geeignetheit aber zusätzlich.

f) Kontraproduktive Effekte

Eine Maßnahme, die das Gegenteil des Gewünschten erreicht, ist offensichtlich ungeeignet. Die Gefahr solcher kontraproduktiver Effekte ist bei der Maßnahme des *RP* groß. Zunächst einmal gibt es keine bessere Werbung für die rechtsradikalen Seiten als das Vorgehen des *RP*.³²⁰ Der *RP* hat seine Verfügung und seinen Widerspruchsbescheid sogar ins Netz gestellt. Dort findet dann jeder die genauen Domainnamen der rechtsradikalen Webhosts. Auch wenn der *RP* darauf verzichtet hätte, hätte die Internetgemeinde doch für die nötige Aufmerksamkeit gesorgt. Wir hatten

schon gesehen, dass die beiden Seiten mittlerweile vielfach gespiegelt sind. Allenthalben finden sich genaue Hinweise, wie man doch an die gesperrten Inhalte gelangt.

Sobald sich die bereits geschilderten Möglichkeiten zu einer vorbeugenden Veränderung der Struktur des Internet realisieren, ist auch das ein beachtlicher kontraproduktiver Effekt. Für die Zukunft wird dadurch auch die staatliche Kontrolle aller anderen problematischen Internethalte viel schwerer.³²¹

Schließlich und vor allem ist mit kreativen Reaktionen der Inhalteanbieter zu rechnen.³²² Gerade weil der *RP* auf Öffentlichkeitswirksamkeit zielt, werden auch viele nach Ausweichstrategien suchen. Auch die Arbeit des Verfassungsschutzes wird schwerer, wenn radikale Angebote als Reaktion auf die Sperrungen in den (virtuellen) Untergrund abwandern. Dass die Suche nach Ausweichstrategien Erfolg hat, ist sehr wahrscheinlich. Denn radikale Gruppen können sich dabei ja gerade der Leistungsfähigkeit von Datenverarbeitung und Vernetzung bedienen. Die stürmische technische Entwicklung wird ihnen zu Hilfe kommen. Realistische Schätzungen nehmen an, dass Rechenleistungen in zehn Jahren verglichen mit heute nur noch ein Hundertstel kosten werden. Speicherplatz wird etwa 1.000-mal und Bandbreite etwa 10.000-mal billiger sein.³²³ Gerade der Zugriff auf verbotene oder sozial geächtete Inhalte hat in der Vergangenheit immer wieder die Entwicklung der Kommunikationstechnik angetrieben.³²⁴ Man kann deshalb mit Überzeugung vorhersagen, dass die technische Entwicklung immer schneller sein wird als die Entwicklung der Regulierung.³²⁵

g) Immunisierende Definition des legitimen Ziels?

Dem *RP* ist zwar nicht das volle Ausmaß des Problems bewusst geworden. Die Verfügung geht aber auf die Gefahr von Umgehungen ein. Der *RP* hält das jedoch für unschädlich. Ihm genügt „eine Förderung der Beseitigung der durch das Angebot drohenden Rechtsgutsverletzung“. Ihm genügt, „dass mit Hilfe der Maßnahme der gewünschte Erfolg näher rückt und gefördert wird“. Das soll der Fall sein, weil durch die Sperrung „eine Erschwernis oder Behinde-

315) Näher zu diesen Techniken *Froomkin*, University of Pittsburgh Journal of Law and Commerce 1996, 395 ff.

316) Das plastische Beispiel stammt von *Dertouzos*, What Will Be 1997, S. 290; s.a. *Lessig/Resnick*, Michigan Law Review 1999, 414 zu der Möglichkeit des Tunnelns von Inhalten.

317) Näher *National Research Council* (o. Fußn. 195), 2.5 und 12.1.2.

318) Vgl. o. Fußn. 195: Einen ersten Überblick über diese peer-to-peer Techniken geben http://www.gnutellanews.com/information/what_is_gnutella.shtml (8.7.2002); *Reber/Schorr*, ZUM 2001, 672 ff.

319) Vgl. etwa *Reidenberg*, Jurimetrics 2002, dort bei Fußn. 68: „To the extent that societies are censor-happy, they will be marginalized on the Internet. The potential risk to doing business in oppressive societies will serve to discourage companies from supporting those repressive regimes through commercial activities“.

320) *Sieber*, CR 1997, 665 f.; *Sieber*, ZRP 2001, 99.

321) *Sieber*, CR 1997, 582; *Sieber*, ZRP 2001, 99.

322) Grundlegend *Wegner*, Wirtschaftspolitik zwischen Selbst- und Fremdsteuern – ein neuer Ansatz, 1996.

323) *National Research Council* (o. Fußn. 195), 2.5.

324) Vgl. o. Fußn. 195: „What has been true over the years is that those who produce and consume sexual content – both for commercial and non-commercial purposes – have stayed on the leading edge of new technologies. Thus, whatever the technological future is like in detail, it seems safe to predict with reasonably high confidence that sexual content will be disproportionately present in the initial stages of adoption of any new technology. Because technology changes rapidly, no final technological solutions are possible“.

325) Vgl. o. Fußn. 195, 2.5.

rung im Zugang zu den unzulässigen Angeboten für den durchschnittlichen Nutzer entsteht“.³²⁶

Diese Begründung passt zunächst einmal nur für einen Teil der Einwände, die wir gerade zusammengestellt haben. Über das Problem prohibitiver Transaktionskosten hilft diese Begründung ebenso wenig hinweg wie über die zu erwartenden kontraproduktiven Effekte der Maßnahme. Vor allem ist die Begründung in sich aber höchst problematisch. Denn diese Umdefinition des legitimen Ziels hat ja den erklärten Zweck, den Maßstab der Geeignetheit leer zu machen. Gesteht man Gesetzgeber und Verwaltung die Freiheit zu dieser Definition des legitimen Ziels zu, wird das Übermaßverbot gegenstandslos.³²⁷ Andererseits wird man dem Staat auch schlecht jegliche Annäherung an ein höhergestecktes Regelungsziel verbieten können.³²⁸

Damit bleibt nur ein Weg, den das *BVerfG* bei Art. 5 Abs. 1 GG bereits früh beschritten hat. Bei der Definition des legitimen Ziels müssen Gesetzgeber und Verwaltung auf den konkreten Schutzgehalt des jeweiligen Grundrechts Rücksicht nehmen. In der juristischen Diskussion wird das meist als Wechselwirkungslehre bezeichnet.³²⁹ Zur Abwägung kommt es also nicht erst bei dem Merkmal der Angemessenheit. Vielmehr ergibt sich bereits das Ausmaß der Freiheit des Gesetzgebers bei der Definition des legitimen Ziels aus einem Abwägungsvorgang. Verfassungsdogmatisch heißt das, dass auf der Stufe der Geeignetheit der abschließende Vorgang der Abwägung bereits vorstrukturiert wird. Das Gewicht des staatlichen Regelungsanliegens ist umso geringer, je stärker das legitime Ziel immunisierend definiert werden muss, um das Verdikt der Ungeeignetheit zu vermeiden. Wir haben gerade gesehen, wie weit der *RP* das eigentliche Ziel verfehlt, die freiheitlich demokratische Grundordnung zu schützen. Im besten Fall könnte er die Gefahr ein bisschen weniger wahrscheinlich machen, wenn sie denn überhaupt besteht. Das ist sehr wenig. Die entgegenstehenden Rechtsgüter der Grundrechtsträger brauchen deshalb kein hohes Gewicht, um die Maßnahme verfassungswidrig zu machen.

Ein schriftlich erlassener Verwaltungsakt ist zu begründen. D.h. aber nicht, dass das überprüfende Gericht an diese Begründung gebunden wäre. Es muss sich zwar mit ihr auseinandersetzen. Erweist sich die Begründung aber als vorgeschoben oder inkonsistent, kann das Gericht selbst auf die Suche nach alternativen Begründungen gehen. All

das gilt auch bei Gesetzen.³³⁰ Wenn man die begleitenden politischen Aktivitäten des *RP* in den Blick nimmt, zeigt sich, dass er in Wahrheit eine ganz andere Absicht verfolgt. Bei einer Anhörung der Access-Provider hat er erklärt, „dass insb. der Staat hier nicht tatenlos zusehen darf“.³³¹ Es geht dem *RP* also darum, ein politisches Zeichen zu setzen.³³² Wiederum wird man dem Staat symbolisches Handeln nicht kategorisch aus der Hand schlagen können. Er leistet damit einen Beitrag zur Bildung oder Aufrechterhaltung sozialer Normen. Das ist aber ein sehr schwaches Regelungsziel. Gravierende Grundrechtseingriffe lassen sich damit nicht begründen.³³³

Noch schwächer wird es, wenn sich der Staat darauf zurückziehen muss, dass eigentlich gar kein wirkliches soziales Problem besteht. Dann kann der Staat nur noch vortragen, er reagiere auf die Unruhe in der Bevölkerung.³³⁴ Auch das wird man dem Staat schließlich nicht kategorisch verbieten können. Denn die soziale Unruhe kann selbst das soziale Problem darstellen.³³⁵ Aber diese Sorge muss schon ein sehr hohes Gewicht haben, um gravierenden Grundrechtseingriffe rechtfertigen zu können.

10. Erforderlich

Für den verfassungsrechtlichen Maßstab der Geeignetheit gibt es mit dem Merkmal „technisch möglich“ ein funktionelles Äquivalent in der Dogmatik von § 22 Abs. 3 MDStV. In ähnlicher Weise hat der verfassungsrechtliche Maßstab der Angemessenheit sein Pendant in dem Tatbestandsmerkmal „zumutbar“ in § 22 Abs. 3 MDStV. Im Wortlaut von § 22 Abs. 3 MDStV findet sich dagegen kein drittes Tatbestandsmerkmal, das in einen inneren Zusammenhang mit dem verfassungsrechtlichen Maßstab der Erforderlichkeit gebracht werden könnte. Ein Grundrechtseingriff ist nicht erforderlich, wenn dem Staat ein milderes, gleich geeignetes Mittel zu Gebote steht. Verlangt ist also ein Institutionenvergleich. § 22 Abs. 3 MDStV ermächtigt den Staat, von Nichtstörern die Sperrung von Inhalten zu verlangen. Vorgesehen ist also nur eine einzige Maßnahme. Deshalb verwundert nicht, dass die Norm der zuständigen Behörde nicht ausdrücklich einen Vergleich auferlegt. Trotzdem lässt sich das verfassungsrechtliche Gebot der Erforderlichkeit auch in der Dogmatik dieser Norm verankern. Man kann auf diese Weise entweder begründen, dass der Behörde ein Entschließungsermessen eröffnet sein muss. Oder man kann dem einfachrechtlichen Maßstab der Zumutbarkeit eine doppelte Aufgabe zuweisen. In dieser Lesart ist die Sperrung nicht nur unzumutbar, wenn das Ausmaß der Grundrechtsbeeinträchtigung außer Verhältnis zu dem konkreten staatlichen Wunsch nach Inhaltskontrolle des Internet steht. Vielmehr fehlt es an der Zumutbarkeit erst recht, wenn der Staat auf sein Steuerungsziel gar nicht verzichtet, sondern es nur auf anderen Wegen verfolgen müsste.

Auf den ersten Blick braucht man sich in unserem Fall mit dem Vergleich von Institutionen nicht lang aufzuhalten. Der Staat will ja befahlen. Mit den Access-Providern hat er auch Adressaten, die sich seinem Zwang schließlich nicht entziehen können. Was auch immer man alternativ erwägen mag: Scheinbar ist es jedenfalls nicht gleich geeignet. Diese These ist jedoch zu kurz gegriffen. Denn zur Erforderlichkeit kommt man ja überhaupt nur, wenn sich eine Maßnahme zuvor als geeignet erwiesen hat. Das ist, wie wir gesehen haben, in diesem Fall ein schwieriges Problem. Der globale Charakter des Internet, die vielen technischen Möglichkeiten zur Umgehung und die schon sichtbaren oder zu erwartenden Reaktionen der Internetgemeinde: All das bewirkt, dass sich die Wirkung rechtsra-

³²⁶ Ähnliche Formulierungen finden sich auch im Widerspruchsbescheid (o. Fußn. 39). Dort ist davon die Rede, „dass ein Zugriff nur noch technisch versierten Nutzern möglich ist“. Es soll genügen, wenn „eine deutliche Erschwerung des Zugangs zu den verbotenen Webseiten für den durchschnittlichen Internetnutzer“ eintritt. Zustimmung und ohne jedes Problembewusstsein *Spindler/Volkman*, K&R 2002, 405 f.

³²⁷ Umfassend zu diesem Problem *Engel*, in: *Brugger/Kirste/Anderheiden* (Hrsg.), *Gemeinwohl in Deutschland, Europa und der Welt*, 2002, S. 103 ff.

³²⁸ So auch *Zimmermann*, NJW 1999, 3150.

³²⁹ Leitentscheidung *BVerfGE* 7, 198, 208 f.; in *BVerfGE* 54, 129, 137 heißt es dann plastisch, die Wechselwirkungslehre stelle die Auslegung der allgemeinen Gesetze unter „die Vermutung für die Zulässigkeit der freien Rede“.

³³⁰ Näher *Engel* (o. Fußn. 327), S. 48 f.

³³¹ Protokoll der Anhörung v. 13.11.2001, S. 1.

³³² So ausdrücklich *Hornig*, ZUM 2001, 855, der dem *RP* erkennbar nahe steht. Auch sonst wird dieser Gedanke im Schrifttum zur Inhaltskontrolle des Internet immer wieder formuliert, so etwa von *Penfold*, *Journal of Information, Law and Technology* 2001, dort bei Fußn. 125; *Reidenberg*, *Jurimetrics* 2002, dort bei Fußn. 72.

³³³ So hält *Vassilaki*, CR 2001, 265 bloßes symbolisches Handeln nicht für ausreichend, um Strafsanktionen zu rechtfertigen.

³³⁴ Näher zu der Unterscheidung von „risk“ und „perceived risk“ *Pildes/Sunstein*, *University of Chicago Law Review* 1995, 1 ff.

³³⁵ Näher *Engel* (o. Fußn. 327), S. 42 ff., insb. zu der Entscheidung des *BVerfG* zum rituellen Schächten, *BVerfG* v. 15.1.2002.

dikaler Angebote aus dem Internet bestenfalls etwas abschwächt. Wenn der Staat das legitime Ziel auf eine bloße Verminderung des Risikos für das Schutzgut zurücknehmen muss, gewinnt der Maßstab der Erforderlichkeit an Gewicht. Die tatsächlich ergriffene Maßnahme ist nun mit allen anderen Maßnahmen zu vergleichen, die einen mindestens gleich großen Schutzeffekt gehabt hätten. Da der Schutzeffekt in unserem Fall klein ist, sind das sehr viele Maßnahmen.

Ein Weiteres muss hinzukommen. An sich gesteht das *BVerfG* dem Gesetzgeber bei der Wahl zwischen alternativen Institutionen eine relativ weite Einschätzungsprärogative zu. Wenn man dem Staat aber überhaupt erlaubt, um bloßer Risikominderungen für das Schutzgut willen in Grundrechte einzugreifen, muss man zumindest kompensierend die Einschätzungsprärogative verkleinern. Sonst würde sich der Staat nämlich schließlich von jeder verfassungsrechtlichen Kontrolle freizeichnen.

Über Internet-Governance im Allgemeinen und über die Möglichkeiten zur Einwirkung auf die Inhalte des Internet im Besonderen ist viel geschrieben worden.³³⁶ Hier ist nicht der Ort, diese Diskussion erneut nachzuzeichnen. Als Ergebnis lässt sich aber festhalten: Einseitige staatliche Interventionen gelten als ausgesprochen schwierig. Sehr viel wirksamer wäre es, zunächst die Internetarchitektur so zu ändern, dass nationales Recht größere Wirkungschancen zurückgewinnt. Das ist technisch vielleicht möglich.³³⁷ Einseitig kann Deutschland diese Veränderungen aber nicht bewirken. Einstweilen scheint vor allem in den USA die Neigung gering, an solchen Änderungen mitzuwirken. Daran hat i. E. auch der 11.9.2001 nichts geändert. Man hört zwar, dass die *amerikanische Regierung* Druck auf die Organe und Unternehmen ausübt, die für die Internetarchitektur verantwortlich sind. Die *amerikanische Regierung* will aber gerade keine Renationalisierung des Internet erreichen. Vielmehr arbeitet sie auf Änderungen der Netzarchitektur hin, die allein ihr Einwirkungsmöglichkeiten eröffnen, die Einwirkungschancen anderer Regierungen nach Möglichkeit dagegen sogar zusätzlich schwächen.

Bei anderen problematischen Inhalten, etwa den Anleitungen zum Bau von Bomben oder bei Kinderpornografie, verspricht die grenzüberschreitende Kooperation von Regulierungsbehörden durchaus Erfolg.³³⁸ Die Anbieter rechtsradikaler Inhalte verlagern ihren Sitz ja aber nicht zufällig in die USA. Weil auch solche Äußerungen in den USA verfassungsrechtlichen Schutz genießen, werden die USA zu keiner Kooperation bereit sein.³³⁹

Scheinbar verspricht bei rechtsradikalen Äußerungen auch eine Lösung wenig Erfolg, die sich sonst bei Problemen der Internet-Governance oft empfiehlt: der Übergang zur Selbsthilfe der Adressaten.³⁴⁰ Das ist deshalb ein elegantes Instrument, weil die eigentliche Kontrolltätigkeit dann nicht mehr befohlen wird. Vielmehr kauft sich jeder Mann so viel und so guten Schutz, wie er das möchte. Die Fortentwicklung der Schutztechniken leisten also die Märkte. Das hat einen doppelten Vorzug. Der Wettbewerb wirkt als Entdeckungsverfahren.³⁴¹ Er ist viel leistungsfähiger, als das auch die findigsten Beamten sein könnten. Außerdem wird der Schutz dann nicht mehr befohlen. Die Entwicklung der Schutztechniken muss deshalb nicht mehr in gleichem Maße rechtsstaatlich und demokratisch kontrolliert sein.³⁴² Wenn er möchte, kann der Staat die Entwicklung der Schutztechniken durch Subventionen sogar zusätzlich fördern.

Scheinbar passt all das auf die Kontrolle rechtsradikaler Inhalte aber nicht. Denn der Staat will ja verhindern, dass anfällige Personen in Berührung mit solchen Äußerungen kommen. Das ist jedoch beim Jugendschutz auch nicht anders. Dort hat sich mittlerweile ein breiter Konsens für technische, von den Märkten entwickelte Mechanismen der Selbsthilfe entwickelt.³⁴³ Die Situation ist auch nur auf den ersten Blick anders, weil der Jugendliche unter dem Einfluss seiner Eltern steht. Natürlich können die Eltern diesen Einfluss nutzen und ihren Kindern nur gefilterten Zugang zum Internet eröffnen. Letztlich sind auch solche Techniken aber zu umgehen. Die Kinder können sich von anderen Orten als dem Elternhaus Zugang zum Internet verschaffen. Auch hier wird der Zugang zu pornografischen oder anderen jugendgefährdeten Inhalten also nur schwierig, nicht unmöglich, genau wie bei der Sperrung rechtsradikaler Inhalte, zu der die *Bezirkregierung* die Access-Provider zwingen will.

Andererseits steht der Zugang zu rechtsradikalen Inhalten regelmäßig nicht im freien Belieben anfälliger Personen. Soweit es Jugendliche sind, gilt vielmehr genau dasselbe wie beim übrigen Jugendschutz. Die Eltern haben auch die Möglichkeit, auf den Internetkonsum junger Erwachsener einzuwirken, solange sie in ihrem Haushalt leben. Je stärker sich die Personen aus der Bindung an ihr Elternhaus lösen, desto mehr müssen andere sozialen Bindungen an die Stelle treten. Wer eine eigene Familie gründet, steht hier unter sozialer Kontrolle. Nationalsozialistische Inhalte sind in Deutschland nach wie vor tabuisiert. Die Medien tragen erheblich zur Stabilisierung des Tabus bei. Auch der Staat kann etwas dazu tun. Wiederum kann das Vorgehen gegen pornografische Inhalte als Vorbild dienen. Nach § 184 Abs. 3 StGB ist nämlich nicht nur strafbar, wer pornografische Inhalte verbreitet. Handelt es sich um Kinderpornografie, werden mittlerweile vielmehr auch die Nutzer bestraft. In gleicher Weise könnte der Staat – in den von der Informationsfreiheit gezogenen Grenzen – auch die bloße Nutzung rechtsradikaler Inhalte im Internet bestrafen. Dadurch würde er ein sehr wirksames Signal für die soziale Ächtung solcher Äußerungen setzen.

Das Vorgehen gegen die Access-Provider ist also mit einer Kombination aus sozialen Normen und technischen Lösungen der Selbsthilfe zu vergleichen. Gewiss gewährt die zweite Lösung keinen absoluten Schutz. Aber wir haben ja gesehen, dass die Wirkungschancen eines Vorgehens nach § 22 Abs. 3 MDStV gegen die Access-Provider bei realistischer Abschätzung noch viel geringer sind. Zwingt der Staat die Access-Provider bloß zur Sperrung der beiden

336) S. aus dem reichen Schrifttum nur *Grewlich*, Governance in Cyberspace, 1999; *Engel*, in: Berichte der Deutschen Gesellschaft für Völkerrecht 2000, S. 353 ff.; *Bremer*, MMR 2002, 147; *National Research Council*, Global Networks and Local Values, 2002.

337) *Lessig* (o. Fußn. 64), S. 43 ff.; konkreter etwa *Jacobus*, Taming the Web. Building Fences, One by One 2001, <http://news.com.com/2009-1023-255774-2.html>.

338) S. nur *Lessig/Resnick*, Michigan Law Review 1999, 423 und konkret *Goldsmith*, University of Chicago Law Review 1998, 1199 ff. dort bei Fußn. 134; *Engel* (o. Fußn. 336), S. 404–406.

339) *Holznapell/Kussel*, MMR 2001, 350.

340) Grundlegend *Dam*, Journal of Legal Studies 1999, 393 ff.

341) So das berühmte Wort von *von Hayek*, Freiburger Studien. Gesammelte Aufsätze von Friedrich-August von Hayek, 1969, S. 249 ff.

342) Die Notwendigkeit zur demokratischen und rechtsstaatlichen Kontrolle entfällt aber auch nicht vollständig. Der Staat verantwortet das Ergebnis aber nicht mehr selbst, sondern muss nur noch grundrechtliche Schutzpflichten beachten, s. dazu zusammenfassend *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, und spezifisch für privates Regieren *Engel* (o. Fußn. 246).

343) Charakteristisch *National Research Council* (o. Fußn. 195).

Domainnamen, ist für das eigentliche normative Ziel gar nichts gewonnen. Der Staat macht sogar noch Werbung für diese beiden Seiten. Sie sind über andere DNS und unter anderen Domainnamen vielfach greifbar. Bei dem Versuch, den ganzen rechtsradikalen Sumpf mit Befehl und Zwang auszutrocknen, wird der Staat dagegen kläglich scheitern. Gewiss ist die Einsicht nicht angenehm, dass unsere Demokratie in einer globalen Umwelt nur begrenzt wehrhaft ist. Aber die Anwendung von § 22 Abs. 3 MDStV ist nichts als der trotzig Versuch eines Lokalpolitikers, mit dem Kopf durch die Wand zu gehen. Die alternative Strategie eines Aufbaus sozialer Normen und eines Anstoßes zur Fortentwicklung von Schutztechniken ist nicht nur gleich, sondern sogar besser geeignet. Die Anwendung von § 22 Abs. 3 MDStV verstößt deshalb gegen das Verfassungsgebot der Erforderlichkeit. Der *RP* hat sein Entschließungsermessen überschritten. Alternativ kann man seine Verfügungen aus diesem Grunde auch für unzumutbar i.S.v. § 22 Abs. 3 MDStV halten.

11. Angemessen/Zumutbar

Dieser letzte einfachrechtliche Maßstab der Zumutbarkeit ist dem verfassungsrechtlichen Maßstab der Angemessenheit sehr ähnlich. Denn auch die Zumutbarkeit verlangt eine umfassende Interessenabwägung.³⁴⁴ Der einfachrechtliche Maßstab ist nur möglicherweise auf die Zumutbarkeit der Intervention für den Access-Provider beschränkt. Bei dem verfassungsrechtlichen Maßstab der Angemessenheit sind dagegen zweifelsfrei die Grundrechte aller Grundrechtsträger in die Abwägung einzubeziehen.

Der *RP* kann das Interesse der Demokratie an ihrer Wehrhaftigkeit in die Waagschale werfen.³⁴⁵ Er kann auf die wachsende Zahl rechtsradikaler Angebote im Internet hinweisen³⁴⁶ und auf deren höchst unerfreulichen Inhalt.³⁴⁷ Auf der anderen Waagschale liegen die Grundrechte der Nutzer, der Access-Provider sowie anderer Anbieter und Hosts von Inhalten.³⁴⁸

Wie regelmäßig sonst auch führt der abstrakte Vergleich dieser Rechtsgüter noch nicht zum Abwägungsergebnis.

344) Sieber, CR 1997, 585; Freytag (o. Fußn. 175), S. 190, 197–201; Sieber, MMR 1999, 199 ff. dort bei Fußn. 200 u. 210; s. auch Ladeur, in: German Yearbook of International Law 1998, S. 74.

345) Mankowski, MMR 2002, 277.

346) Nach dem Verfassungsschutzbericht gibt es gegenwärtig etwa 1.300 solcher Angebote, <http://www.heise.de/newsticker/result.xhtml?url=newsticker/data/jk-29.04.02-004/default.shtml&words=Verfassungsschutz> (Stand: 19.5.2002).

347) Beschreibungen finden sich bei Holznagel/Kussel, MMR 2001, 347; Sieber, ZRP 2001, 97 f.

348) Näher oben unter V.6. und 7.

349) Grundlegend zur Struktur des Abwägungsvorgangs Alexy, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 2002, S. 7 ff., und noch differenzierter Alexy, in: GS Sonnenschein, 2003, S. 771 ff.

350) Je leichter eine Sperrtechnik zu umgehen ist, desto weniger ist sie zumutbar i.S.v. § 22 Abs. 3 MDStV: Engel-Flehsig/Maennel/Tettenborn (o. Fußn. 28), S. 18; a.A. Generalbundesanwalt MMR 1998, 93, 96 f.

351) S. oben unter 5. b).

352) S. zunächst oben 8. a) zum Zensurverbot. Auch wenn man dem nicht folgen wollte, macht die Zensurnähe Eingriffe doch regelmäßig unverhältnismäßig, s. dazu BVerfGE 33, 52, 90 (abweichende Meinung); [Ladeur, NJW 1986, 2749; Fiedler (o. Fußn. 125), S. 302 f. m.w.Nw.; Hopf, ZUM 2000, 741 m.w.Nw.]; Alternativkomm.-Hoffmann-Riem, GG, Art. 5 Abs. 1, 2 Rdnr. 77 f.

353) S.o. unter 8. c).

354) Sieber, CR 1997, 581, 586.

355) Freytag (o. Fußn. 175), S. 226.

356) Zum technischen Hintergrund s. <http://www.marth.com/tech/was.htm> (Stand: 6.12.2002).

357) Froomkin, University of Pittsburgh Journal of Law and Commerce 1996, 395 ff. dort bei Fußn. 194 f.; Yurcik/Tan, The Great (Fire)Wall of China. Internet Security and Information Policy Issues in the People's Republic of China 1996, <http://www.tprc.org/abstracts/tan.txt>; Kalathil/Boas, The Internet and the State Control in Authoritarian Regimes, 2001; Sieber, ZRP 2001, 99.

Entscheidend ist, wie sehr einerseits das staatliche Ziel durch die Maßnahme des *RP* gefördert wird und wie sehr dadurch andererseits die Grundrechte aller Grundrechtsträger beeinträchtigt werden.³⁴⁹

Das staatliche Ziel besteht in dem Wunsch, die Verbreitung rechtsradikaler oder gar nationalsozialistischer Gedanken zu verhindern. Schutzobjekt ist also die geistige und politische Kultur des Landes. Weil sich das GG für eine wehrhafte Demokratie entschieden hat, ist das ein Anliegen von Gewicht. Die konkrete Maßnahme des *RP* hat aber bestenfalls einen symbolischen Effekt. Vergleichbare Inhalte sind in großer Zahl und ohne Mühe auf anderen Servern und unter anderen Domainnamen greifbar. Ein ernstlicher Effekt wäre allenfalls dann denkbar, wenn man das Verfahren von vornherein als Pilotverfahren deutet. Bei dem Versuch, flächendeckend gegen rechtsradikale Inhalte im Netz vorzugehen, müsste der *RP* aber scheitern. Der schiere Regelungsaufwand würde unübersehbar. Denkbar ist allenfalls, dass der *RP* die Drohung mit einseitigen staatlichen Interventionen dazu nutzt, die Access-Provider zur Selbstregulierung zu zwingen. Auch das verspricht aber nicht wirklich Erfolg. Alle denkbaren technischen Lösungen sind relativ leicht zu umgehen.³⁵⁰ Der Staat würde einen Anreiz dafür setzen, dass sich rechtsradikale Inhalte in praktisch gar nicht mehr zu kontrollierende Teile des Netzes verlagern. Weil er das deutsche Recht extraterritorial anwendet, wäre überdies mit heftigem ausländischen, vor allem amerikanischen Widerstand zu rechnen.

Das staatliche Schutzanliegen hat im konkreten Fall also recht geringes Gewicht. Das Gewicht der entgegenstehenden Grundrechte ist dagegen ausgesprochen hoch. Am stärksten wiegt der Umstand, dass der Staat die Access-Provider als Nichtstörer in Anspruch nimmt. Das allgemeine Polizeirecht bringt die Höhe des Schutzniveaus dadurch zum Ausdruck, dass der Staat nur bei einer gegenwärtigen Gefahr auf Nichtstörer zugreifen darf. Wir haben gesehen, warum das nicht der Fall ist.³⁵¹ Sehr hohes Gewicht hat auch der Umstand, dass die Maßnahme zumindest in enger Nähe zur Zensur steht.³⁵² Sehr hohes Gewicht hat schließlich weiter der Umstand, dass der Staat hier Sanktionen gegen die Äußerung einer ganz bestimmten politischen Meinung ergreifen will. Dogmatisch zeigt sich dieses Gewicht in der Tatsache, dass die Schranke der allgemeinen Gesetze in Art. 5 Abs. 2 GG aus diesem Grunde nicht zur Verfügung steht. Vielmehr kann die Maßnahme nur auf die speziellen Vorschriften zum Schutz der wehrhaften Demokratie gestützt werden.³⁵³

Erhebliches Gewicht haben außerdem die absehbaren Folgen für die Leistungsfähigkeit des Internet als Kommunikationsnetz.³⁵⁴ Wenn der Staat den Zugang zu rechtsradikalen Inhalten auch nur marginal erschweren will, muss er fundamentale Änderungen der Architektur des Internet erzwingen. Vor allem durch den Zwang zum Einsatz von Proxyservern würde sich der Internetverkehr stark verlangsamen.³⁵⁵ Je nach Wahl der Sperrtechnik sind Dritte auch ganz unmittelbar betroffen. Ein Beispiel ist die Sperrung der IP-Adresse eines virtuellen Servers. Von einem virtuellen Server spricht man, wenn sich mehrere Content-Provider oder Webhosts ein und denselben Webserver teilen. Wird die IP-Adresse gesperrt, ist gleichzeitig der Zugang zu sämtlichen – und damit auch zu legalen, nicht störenden – Angeboten verhindert.³⁵⁶ Den Verfassungsinterpreten sollte zu denken geben, dass Deutschland dann genau zu der Technik greifen würde, mit der sich autoritäre Staaten wie China, Kuba oder Singapur umgeben.³⁵⁷ Außerdem kann die staatliche Intervention ihr Ziel nur errei-

chen, wenn sie zum Drohmittel wird, das die Access-Provider zu einer strikten Form der privaten Regulierung zwingt. Dann wird den Anbietern der herausgefilterten Inhalte, vor allem aber deren potenziellen Nutzern, praktisch jeder Rechtsschutz genommen. Diese Form der Regulierung entbehrt zugleich praktisch jeder demokratischen Kontrolle und Legitimation.³⁵⁸

Weil die übrigen Schutzgüter noch viel höheres Gewicht haben, rückt im konkreten Fall für das Abwägungsurteil sogar in den Hintergrund, was sonst im Zentrum stehen würde, nämlich der technische und ökonomische Aufwand für die Erfüllung der Vorstellungen des RP.³⁵⁹ Dieser Aufwand ist erheblich. Wie hoch er genau ist, hängt von der gewählten technischen Lösung ab. Das Programmieren der DNS oder der Router mag für zwei Domainnamen oder zwei IP-Adressen überschaubar bleiben. Darum geht es hier ja aber auch nicht. Vielmehr geht es darum, ob § 22 Abs. 3 MDStV die Ermächtigungsgrundlage wäre, die Sperrung aller Websites mit nationalsozialistischen oder rechtsradikalen Inhalten zu verlangen. Dann wird auch bei diesen beiden technischen Lösungen der Aufwand groß. Da die Anbieter der Inhalte mit Sicherheit reagieren werden, ist es nicht einmal mit der einmaligen Sperrung getan. Vielmehr müssten die Access-Provider ständig neue Domainnamen oder neue IP-Adressen sperren. Noch sehr viel höher ist der Aufwand bei der dritten Lösung. Einstweilen verfügen die Access-Provider gar nicht über Proxyserver. Sie müssten Hard- und Software also erst kaufen. Sie müssten die Architektur ihres eigenen Betriebs auf dieses neue Element abstimmen. Und auch hier müsste die Software ständig gepflegt werden.³⁶⁰

Man bräuchte nicht einmal diese große Zahl von Argumenten. Nimmt man die Argumente zusammen, liegt die Unangemessenheit und damit die Unverhältnismäßigkeit des Eingriffs aber außer Zweifel. § 22 Abs. 3 MDStV darf nicht in einer Weise ausgelegt werden, die das Vorgehen des RP gestatten würde. Weil seine Maßnahme von der Ermächtigungsgrundlage nicht gedeckt ist, ist sie rechtswidrig.

IV. Kompensation

Auch wer sich all den übrigen Argumenten versagen wollte, die wir vorgebracht haben, müsste doch ein Letztes gelten lassen: Die Access-Provider sind Nichtstörer.³⁶¹ Der Staat verlangt von ihnen also ein Sonderopfer.³⁶² Wenn er das überhaupt darf, muss er die Adressaten zumindest für den Vermögensnachteil entschädigen.³⁶³ Man kann dieses Ergebnis auf einem einfachrechtlichen und auf einem verfassungsrechtlichen Wege begründen. Der einfachrechtliche Weg wendet die Vorschriften des jeweiligen Landespolizeirechts über den Ersatzanspruch der Nichtstörer analog auf § 22 Abs. 3 MDStV an. Die Regelungslücke ergibt sich gerade aus Verfassungsrecht. Weil die Access-Provider Nichtstörer sind, würde ihnen der Staat ohne Ausgleichsanspruch ein Sonderopfer abverlangen. Die Adressaten könnten die Ermächtigungsgrundlage deshalb nach den Grundsätzen angreifen, die das BVerfG in dem Nassauskiesungs-Urteil entwickelt hat.³⁶⁴ Die Nichtigerklärung der Ermächtigungsgrundlage wird gerade durch die analoge Anwendung der polizeirechtlichen Regeln vermieden. Letztlich ist das für unseren Fall aber gleichgültig. Wer die Analogie nicht ziehen will, muss die Ermächtigungsgrundlage dann eben wegen des nicht kompensierten Sonderopfers für verfassungswidrig halten.

Aus der Perspektive des Entschädigungsanspruchs wird außerdem die Unbestimmtheit der Verfügung zu einem noch größeren Problem. Der RP weigert sich im Widerspruchsbeseid sogar ausdrücklich, die konkrete Maßnahme festzulegen, die er von den Access-Providern verlangt.³⁶⁵ Damit überwälzt er das Kostenrisiko auf die Adressaten. Ergreifen sie eine besonders wirksame Maßnahme und verlangen vom Land Nordrhein-Westfalen Ersatz der Kosten, wird es einwenden, das sei ja gar nicht vorgeschrieben gewesen.³⁶⁶ Das ist rechtsstaatlich unerträglich. Zugleich sinkt aus diesem Grunde die praktische Wirksamkeit des Eingriffs weiter. Denn oben ist ja dargelegt, dass er sein materielles Ziel nur erreichen kann, wenn er als Drohpotenzial wirkt und die Access-Provider zu Maßnahmen veranlasst, die der Staat weder befehlen noch vollziehen könnte.³⁶⁷ Solange die Kostenfrage offen bleibt, werden sich die Access-Provider dazu aber gewiss nicht hergeben. Der Eingriff verpufft.

V. Thesen

1. Die Verfügung des *Düsseldorfer Regierungspräsidenten* gegen Internet-Access-Provider aus dem Lande Nordrhein-Westfalen ist rechtswidrig. Dem RP fehlt die Kompetenz zum Erlass der Verfügung. Die Verfügung verstößt gegen einfaches Recht und gegen Verfassungsrecht. Sie ist schließlich deshalb rechtswidrig, weil der RP die Access-Provider nicht für die Vermögensnachteile kompensiert, die ihnen entstehen.
2. Der RP als Behörde der unmittelbaren Staatsverwaltung verstößt gegen das Verfassungsgebot der Staatsferne, wenn er den Inhalt des Internet reguliert.
3. Dem Land Nordrhein-Westfalen fehlt die Gesetzgebungskompetenz. Der MDStV darf deshalb nicht in einer Weise ausgelegt werden, die den RP zum Einschreiten ermächtigen würde. Das ergibt sich einmal aus den entgegenstehenden, kompetenzgemäß erlassenen Vorschriften des TDG. Zum anderen setzt sich der RP in Widerspruch zur Außenpolitik des Bundes.
4. Dem RP fehlt auch deshalb die Zuständigkeit, weil die Länder es versäumt haben, im MDStV Regeln für den Fall der Zuständigkeitskonkurrenz bei der Verfolgung von Auslandssachverhalten zu treffen. Die Gestaltungsmöglichkeiten sind zu zahlreich, als dass die Lücke durch Rückgriff auf die entfernt parallel Regeln des RStV gefüllt werden könnte.
5. Der Sache nach will der RP die Säuberung des Internet von rechtsradikalen Inhalten gar nicht selbst bewerkstelligen. Mit Hilfe des Verfahrens gegen die Access-Provider will er vielmehr nur staatliches Drohpotenzial aufbauen. Er will es dazu nutzen, die Access-Provider zur regulierten Selbstregulierung zu zwingen. Wenn dieses staatliche Vorgehen verfassungsrechtlich überhaupt zulässig ist, dann

358) S. erneut *Lessig* (o. Fußn. 64) und zu den verfassungsrechtlichen Maßstäben für die Beurteilung privater Regulierung *Engel* (o. Fußn. 246).

359) BT-Drs. 13/7385 (Amtl. Begr. zum IuKDG), Begr. zu § 5 Abs. 2 TDG; ebd., Gegenäußerung der Bundesregierung zur Äußerung des Bundesrats, S. 4; Antwort der Bundesregierung auf eine Kleine Anfrage, BT-Drs. 13/8153, S. 16.

360) Einen Überblick gibt *National Research Council* (o. Fußn. 195), 2.5 und 12.1.5.

361) S. oben unter III. 5. a).

362) *Pieroth/Schlink/Kniesel* (o. Fußn. 190), § 22 Rdnr. 7.

363) So auch *Spindler/Volkman*, K&R 2002, 405; *Stadler*, MMR 202, 343.

364) BVerfGE 58, 300, 317 ff.

365) Widerspruchsbeseid (o. Fußn. 39).

366) *Spindler/Volkman*, K&R 2002, 405 weisen zu Recht auf dieses Risiko hin.

367) S.o. unter III. 6. c).

jedenfalls nur mit ausdrücklicher gesetzlicher Ermächtigung. Daran fehlt es.

6. Die Eingriffsgrundlage aus § 22 Abs. 3 MDStV ist subsidiär. Sie setzt voraus, dass der *RP* an sich berechtigt wäre, nach § 22 Abs. 1 MDStV gegen den Anbieter der Inhalte oder nach § 22 Abs. 2 MDStV gegen den Host der Inhalte vorzugehen. Anbieter und Host befinden sich in den USA. Die Verfügung des *RP* ist also nur dann rechtmäßig, wenn die extraterritoriale Anwendung des MDStV auf einen Sachverhalt in den USA zulässig wäre.

7. Der internationale Anwendungswille des MDStV erfasst die Inhalte nicht, zu denen der *RP* den Zugang sperren lassen möchte. Die Äußerungen haben zu Deutschland keinen Bezug, der über ihren nationalsozialistischen Inhalt hinausginge. Das genügt selbst dann nicht, wenn man an sich ausreichen lässt, dass Deutschland der Erfolgsort ist. Denn es besteht sowohl im internationalen Privatrecht wie im internationalen Strafrecht Einigkeit, dass der Erfolgsort jedenfalls nicht zu einem versteckten Weltrechtsprinzip führen darf.

8. Zum gleichen Ergebnis kommt man auch auf einem indirekten Wege. Der *RP* leitet die Rechtswidrigkeit der Äußerungen aus § 12 Abs. 1 Nr. 1 MDStV ab. Diese Norm verweist ihrerseits auf §§ 130 und 131 StGB. Das StGB hat vor kurzem für den strukturell parallelen Fall der Kinderpornografie das Weltrechtsprinzip eingeführt. Daraus folgt im Gegenschluss, dass es für volksverhetzende Äußerungen gerade nicht gilt.

9. Die Bundesrepublik Deutschland ist nicht frei, den internationalen Anwendungsbereich von § 22 MDStV zu bestimmen. Sie muss dabei vielmehr die engen Grenzen des völkergewohnheitsrechtlichen Interventionsverbots beachten. Wegen Art. 25 GG haben diese Regeln auch innerstaatliche Wirkungen. Welchen genauen Inhalt diese Regeln für Internetsachverhalte haben, ist lebhaft umstritten. Sehr viel spricht dafür, dass die deutsche Regulierung der beiden amerikanischen Webhosts völkerrechtswidrig wäre. Jedenfalls muss das erkennende Gericht wegen dieser Unsicherheit über den Inhalt des Völkergewohnheitsrechts nach Art. 100 Abs. 2 GG das Verfahren aber aussetzen und die Sache dem *BVerfG* zur Entscheidung vorlegen.

10. § 22 Abs. 3 MDStV wird durch die strafprozessualen Vorschriften über die Pressebeschlagnahme verdrängt. Das ist nicht nur aus einfachrechtlichen, sondern auch aus verfassungsrechtlichen Gründen geboten. Die Sondervorschriften über die Pressebeschlagnahme sind nämlich Ausdruck der verfassungsrechtlich abgesicherten Polizeifestigkeit der Medien.

11. § 22 Abs. 3 MDStV wird außerdem durch die Sonderregeln zum Schutz der wehrhaften Demokratie verdrängt. Auch dieses Ergebnis folgt aus dem Verfassungsrecht. Der *RP* will gegen die Äußerungen gerade wegen ihres politischen Inhalts vorgehen. Dieses Vorgehen ist vom Vorbehalt der allgemeinen Gesetze in Art. 5 Abs. 2 GG nicht gedeckt. Nur für die Sondervorschriften zum Schutz der wehrhaften Demokratie gilt eine Ausnahme.

12. Für die Abgrenzung zum TKG und zum TDG kommt es nicht auf die Qualifikation der Tätigkeit des Access-Providers selbst an. Die Anwendbarkeit von § 22 Abs. 3 MDStV hängt vielmehr daran, ob der angegriffene Inhalt ein Mediendienst ist.

13. Die Verfügung des *RP* richtet sich nicht unmittelbar gegen die Anbieter von Inhalten, sondern gegen zwei Hosts. Diese Hosts sind dann ein Mediendienst, wenn sie selbst eine publizistische Aussage machen. I.Ü. kommt es auf die Qualifikation der Inhalte an, die sie zur Nutzung

bereithalten. Der Sachverhalt der Verfügung des *RP* ist zu spärlich, um diese Frage entscheiden zu können. Es kommt darauf an, ob die Angebote redaktionell gestaltet sind.

14. Der *RP* sprengt die Grenzen von § 22 Abs. 3 MDStV. Er will diese Ausnahmenvorschrift zur Regel machen. Was er will, mag strukturell einem „notice and take down“-Verfahren verwandt sein, aber selbst zu dessen Einführung haben sich weder die deutschen noch die europäischen Gesetzgeber einstweilen entschließen können. Der *RP* will sich überdies in radikalen Widerspruch zur Internetpolitik des Bundes setzen, die im TDG Ausdruck gefunden hat.

15. Zusätzliche Grenzen ergeben sich aus der Tatsache, dass der *RP* polizeirechtlich gesprochen gegen Nichtstörer vorgeht. § 5 MDStV a.F. und die komplizierten Nachfolgevorschriften der §§ 6–9 MDStV n.F. sind nämlich in folgender Weise in die Dogmatik des öffentlichen Rechts einzufügen. Die Inhalteanbieter sind polizeirechtlich Handlungstörer; die Webhosts sind polizeirechtlich Zustandsstörer; die Access-Provider sind polizeirechtlich dagegen Nichtstörer. Der *RP* hat die polizeirechtlichen Grenzen eines Vorgehens gegen Nichtstörer missachtet. Insbesondere fehlt es an einer gegenwärtigen Gefahr. Die strafrechtlichen Vorschriften, auf die der *RP* sich stützt, schützen nämlich nur vor abstrakten Gefahren.

16. Die Verfügung des *RP* greift in Grundrechte der Access-Provider, der Internetnutzer und der Anbieter von Inhalten ein. Die Verfügung verletzt die benannten Schranken der einschlägigen Grundrechte. Sie verletzt außerdem das allgemeine Übermaßverbot.

17. Die Verfügung greift in drei verschiedene Grundrechte der Access-Provider ein. Als notwendige Intermediäre für die Internetkommunikation sind auch die Access-Provider selbst von Art. 5 Abs. 1 Satz 2 GG geschützt. Geschützt sind außerdem ihre unternehmerischen Freiheiten aus Art. 12 Abs. 1 und 14 GG. Schließlich schützt sie Art. 2 Abs. 1 GG vor der aufgezwungenen Rolle als Regulierungsinstanz.

18. Die Verfügung greift nicht nur in Grundrechte der Access-Provider ein. Vielmehr greift sie insb. auch in die Informationsfreiheit der Nutzer ein. Im Lichte der nationalsozialistischen Vergangenheit schützt Art. 5 Abs. 1 GG grds. auch die Kenntnisnahme strafbarer Inhalte. Außerdem sind die Nutzer vor den Folgewirkungen der Intervention für die Funktionsfähigkeit des Internet geschützt. Aus dem gleichen Grunde greift die Verfügung auch in die Äußerungsfreiheiten der Anbieter anderer Inhalte und anderer Webhosts ein.

19. Die Verfügung verletzt das kategorische Zensurverbot aus Art. 5 Abs. 1 Satz 3 GG. Die Unterscheidung zwischen Vor- und Nachzensur muss auf das Internet als Abrufmedium angemessen angewendet werden. Dass ein Inhalt vor dem Eingreifen der Zensurbehörde ungehindert ins Netz gestellt worden ist, genügt noch nicht für die Qualifikation als Nachzensur. Anders als etwa bei der Presse hat dem Inhalt nämlich noch eine realistische Wirkungschance gefehlt.

20. Die Maßnahme ist nicht geeignet, das Regelungsziel des *RP* zu erreichen. Welche Technik die Access-Provider auch immer auf Geheiß des *RP* wählen, die Sperrung ist leicht zu umgehen. I.Ü. würde die bloße Sperrung der beiden Domainnamen auch gar nichts nützen. Vor einer Verbreitung rechtsradikaler Inhalte würde das geistige und politische Leben in der Bundesrepublik erst dann geschützt, wenn der *RP* auch den Zugang zu allen anderen rechtsradikalen Websites sperren ließe. Nach seiner eigenen Erklärung sind das bis zu 6.000 Websites. Mit rechts-

staatlichen Mitteln ist dieses Ziel offensichtlich nicht zu erreichen. Außerdem ist mit dem Widerstand ausländischer Staaten, vor allem der USA zu rechnen. Ja, die Maßnahme wird sogar kontraproduktiv wirken. Zunächst macht der *RP* Werbung für die beiden Webhosts. Mittelfristig werden die Anbieter rechtsradikale Inhalte in praktisch unkontrollierbare Teile des Internet verlagern.

21. Gegen den Vorwurf der Ungeeignetheit kann sich der *RP* auch nicht einfach durch eine andere Definition seines Regelungsziels immunisieren. Er kann sich nicht einfach darauf beschränken, den Zugang zu nationalsozialistischen Inhalten bloß zu erschweren. Erst recht kann er sich nicht einfach damit zufrieden geben, ein politisches Zeichen zu setzen oder auf Unruhe in der Bevölkerung zu reagieren. Denn solche Undefinitionen des legitimen Ziels machen den verfassungsrechtlichen Maßstab der Geeignetheit stumpf. Sie sind verfassungsrechtlich nur dann ausnahmsweise erträglich, wenn das normative Anliegen des Staats im konkreten Fall sehr hohes Gewicht hat. Geeignetheit und Angemessenheit fallen bei dieser Art der Definition des legitimen Ziels also praktisch zusammen.

22. Wer dem nicht folgen will, muss die Maßnahme des *RP* jedenfalls für nicht erforderlich halten. Er muss diese Maßnahme nunmehr nämlich mit anderen Maßnahmen vergleichen, die ebenfalls zu einer gleichen oder sogar weitergehenden Annäherung an das eigentliche Regelungsziel führen. Der günstige Effekt der Maßnahme des *RP* ist bestenfalls schmal. Ein alternatives Arrangement ist geeignet, das geistige und politische Leben in Deutschland vor dem Eindringen rechtsradikaler Inhalte mindestens so intensiv zu schützen. Es besteht aus einer Verbindung des Aufbaus sozialer Normen mit der Entwicklung nutzerautonom (technischer) Filter durch den Wettbewerb. Wenn er möchte, kann der Staat beide Elemente dieses Arrangements aktiv fördern. Er könnte Subventionen für die schnellere Entwicklung von nutzerautonomen Filtern vergeben. Und er könnte die schon vorhandenen sozialen Normen stärken, indem er nach dem Vorbild der Kinder-

pornografie Strafverfahren gegen die deutschen Nutzer nationalsozialistischer Inhalte möglich macht.

23. Schließlich verstößt die Maßnahme des *RP* auch deshalb gegen das Übermaßverbot, weil sie den Maßstab der Angemessenheit missachtet. Auf der Seite des Staates kommt die Verfassungsentscheidung für eine wehrhafte Demokratie auf die Waagschale. Auf der anderen Seite der Waage liegen die Grundrechte der Access-Provider, der Nutzer und der Anbieter anderer Inhalte. Abstrakt überwiegt keines dieser Rechtsgüter das andere. Es kommt vielmehr auf einen Vergleich der konkreten Wirkungen der Verfügung des *RP* an.

Auf der staatlichen Seite vermindert sich das Gewicht sehr stark, weil das eigentliche Ziel unerreichbar bleibt. Bestenfalls kommt der Staat ihm ein kleines Stück näher. Wahrscheinlicher hat die Maßnahme überhaupt bloß einen symbolischen Effekt. Auf der Seite der Grundrechtsträger wiegt der Eingriff dagegen sehr schwer. Das ergibt sich zunächst und vor allem aus der Tatsache, dass der Staat hier ja gegen Nichtstörer vorgeht. Das darf er nicht, wenn die Maßnahme kaum etwas erreicht. Hoch ist das Gewicht des Eingriffs auch wegen der benannten Grundrechtsschranken. Wenn die Maßnahme schon keine Zensur darstellt, dann liegt sie doch jedenfalls in enger Nähe zur Zensur. Und wenn sie mit dem Maßstab der allgemeinen Gesetze in Art. 5 Abs. 2 GG überhaupt zu rechtfertigen wäre, dann muss dieser Vorbehalt auf das Äußerste angespannt werden. Hohes Gewicht hat die Maßnahme aber auch wegen der Folgen für die Funktionsfähigkeit des Internet. Die Gefahr ist groß, dass deshalb sehr viele Menschen am wirksamen Gebrauch ihrer Freiheit gehindert werden. Schließlich ist der wirtschaftliche Aufwand beträchtlich, der den Access-Providern abverlangt wird. Das gilt ganz besonders, wenn sie zur Anschaffung von Proxyservern gedrängt werden.

24. Selbst wer all dem nicht folgen wollte, müsste den Access-Providern als Nichtstörern doch jedenfalls in analoger Anwendung der Polizeigesetze der Länder einen Ausgleichsanspruch für den Vermögensnachteil zubilligen.

Inhalt

I. Einleitung	2	4. Eingreifen gegen Access-Provider als Ausnahme	16
II. Kompetenzen	2	5. Voraussetzungen eines Vorgehens gegen Nichtstörer	17
1. Staatsferne	2	a) § 22 Abs. 3 MDStV als Haftung von Nichtstörern	17
2. Bund – Land	3	b) Grenzen der Inanspruchnahme von Nichtstörern	19
3. Land – Land	4	6. Entgegenstehende Grundrecht der Access-Provider	19
4. Staat – Private	6	a) Äußerungsfreiheit	20
5. Deutschland – Europa	7	b) Unternehmerische Freiheiten	20
6. Deutschland – Ausland	7	c) Aufgezwungene Rolle als Regulator	20
a) Extraterritoriale Wirkung	8	7. Informationsfreiheit der Nutzer	21
b) Anwendbarkeit von § 22 Abs. 3 MDStV auf Auslandssachverhalte	8	8. Schranken	24
c) Internationaler Anwendungsbereich der verwiesenen strafrechtlichen Normen	9	a) Zensurverbot	24
d) Innerstaatliche Wirkung völkerrechtlicher Grenzen der Extraterritorialität	10	b) Schranken der Informationsfreiheit	24
e) Völkerrechtliche Grenzen der Extraterritorialität	10	c) Allgemeine Gesetze	24
f) Verfahrensrechtliche Folgen	11	d) Legitimes Ziel	24
III. Materielles Recht	11	9. Geeignet / technisch möglich	24
1. Eingriffsgrundlage	11	a) Einführung	24
a) Vorrang der Vorschriften über die Pressebeschlagnahme	11	b) Diskutierte technische Lösungen	25
b) Vorrang der Vorschriften zum Schutz der wehrhaften Demokratie	12	c) Prohibitive Regulierungskosten	27
2. Sachlicher Anwendungsbereich	13	d) Gegenwehr der Internetgemeinde	27
a) Abgrenzungen zum Telekommunikationsrecht	13	e) Widerstand ausländischer Staaten	28
b) Abgrenzungen zum Teledienstegesetz	13	f) Kontraproduktive Effekte	28
3. Rechtmäßigkeit des Eingriffs gegen den primär Verantwortlichen	15	g) Immunisierende Definition des legitimen Ziels?	28
		10. Erforderlich	29
		11. Angemessen / Zumutbar	31
		IV. Kompensation	32
		V. Thesen	32

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); RAin Ruth Schrödl, Redakteurin; Marianne Gerstmeyr, Redaktionsassistentin, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/ 381 89-427, Telefax: 089/ 38189-695, E-Mail: mmr@beck.de

Manuskripte: Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht für die Zeit bis zum Ablauf des Urheberrechts. Eingeschlossen sind insbesondere auch die Befugnis zur Einspeicherung in eine Datenbank sowie das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken im Wege eines fotomechanischen oder eines anderen Verfahrens. Dem Autor verbleibt die Befugnis, nach Ablauf eines Jahres anderen Verlagen eine einfache Abdruckgenehmigung zu erteilen; ein Honorar hieraus steht dem Autor zu.

Urheber- und Verlagsrechts: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Dies gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Redaktion erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlages in irgendeiner Form – durch Fotokopie, Mikrofilm oder andere Verfahren – reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsanlagen verwendbare Sprache übertragen werden.

Anzeigenabteilung: Verlag C.H. Beck, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 400340, 80703 München, Media-Service: Telefon: 089/381 89-781, Telefax: 089/381 89-782, media-service@beck.de, Media-Disposition (Herstellung Anzeigen, technische Daten): Telefon 089/381 89-603, Telefax (Auftragsservice): 089/381 89-589, Verantwortlich für den Anzeigenteil: Fritz Leberherz.

Anzeigenpreise: Es gilt Anzeigenpreisliste Nr. 6.

Verlag: Verlag C.H. Beck oHG, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank: München Nr. 62 29-802, BLZ 70010080.

Erscheinungsweise: Monatlich.

Bezugspreise 2003: halbjährlich € 138,- (darin € 9,03 MwSt.). Einzelheft: €25,80 (darin enthalten € 1,69 MwSt.); für Studenten und Rechtsreferendare € 70,- (darin enthalten € 4,58 MwSt.). Versandkosten: jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden.

Bestellungen über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag Basel, Auslieferung: Verlag Sauerländer, Laurenzerworstadt 89, CH-5001 Aarau, Tel.: 064/26 86 26, Telefax: 064/24 57 80.

Abo-Service: Tel.: 089/3 81 89-549, Fax: 089/3 81 89-297, E-Mail: abo.service@beck.de

Abbestellungen müssen 6 Wochen vor Halbjahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.

Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Bezieher kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

Satz: Medien Dienst Lorenz & Partner, München.

Druck: C.H. Beck'sche Buchdruckerei, Bergerstr. 3, 86720 Nördlingen.

ISSN 1434-596X