ZUM

Zeitschrift für Urheber- und Medienrecht

45. Jahrgang · Heft 11/2001
ISSN 0177-6762

Inhaltsverzeichnis

Aufsätze

Rechtsprechung

Buchbesprechung

Beilagenhinweis: Dieser Ausgabe liegt ein Prospekt der Nomos Verlagsgesellschaft bei. Wir bitten freundlichst um Beachtung.

Manuskripte: Verlag und Redaktion haften 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 erwirbt der Verlag vom Verfasser alle Rechte, insbes. auch das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken im Wege des fotomechanischen oder eines anderen Verfahrens.

Sämtliche mit Verfasserangaben versehene Beiträge stellen nur die Meinungsäußerung des Verfassers, nicht die der Herausgeber oder der Schriftleitung dar.

Druck, Verlag und Anzeigenannahme: Nomos Verlagsgesellschaft mbH & Co. KG, Waldseestraße 3–5, 76530 Baden-Baden, Telefon: (0 72 21) 21 04-0, Telefax: (0 72 21) 21 04 27.

Bezugsbedingungen: Erscheinungsweise monatlich; Abonnementpreis jährlich 398,–- DM (inkl. MwSt.) zuzüglich Porto und Versandkosten; Einzelheft 41,50 DM (inkl. MwSt.); Bestellungen nehmen entgegen: Der Buchhandel und der Verlag; Abbestellungen vierteljährlich zum Jahresende. Zahlungen jeweils im voraus an Nomos Verlagsgesellschaft, Postscheckkonto Karlsruhe 736 36-751 und Stadtsparkasse Baden-Baden Konto 5-002 266.

ISSN 0177-6762

Möglichkeiten des Ordnungsrechts bei der Bekämpfung rechtsextremistischer Inhalte im Internet*

Zur Internet-Aufsicht auf der Grundlage des § 18 Mediendienste-Staatsvertrags

Von Dr. Michael Hornig**, Augsburg

Eine Beschäftigung mit ordnungsrechtlichen Instrumentarien im Bereich des Medienrechts, noch dazu im Bereich des dynamischen Internet-Rechts, mutet angesichts der regen Diskussion über »(regulierte) Selbstregulierung«, »Cyberlaw«[1], »intelligente Regulierung« und »prozedurale Designs« fast schon anachronistisch an. Wird doch im Rahmen der Reformdiskussion des Verwaltungsrechts immer wieder betont, dass gerade die Starrheit des klassischen Ordnungsrechts zu einem »Staatsversagen« führt oder – allgemeiner gesprochen – den Verwaltungsstaat in eine Krise geführt hat[2].

Der Blick auf den Realbereich der Internetkommunikation zeigt, dass die Verbreitung von Hass und politischer Intoleranz im Internet in den letzten Jahren außerordentlich stark zugenommen hat. Dass dies nicht nur eine bloße Vermutung eines subjektiv gesteigerten Sicherheitsbedürfnisses der Gesellschaft ist, dokumentieren die Beobachtungen des Verfassungsschutzes[3]: Demnach nutzen Neonazis verstärkt die Vorteile des Internet zur Verbreitung ihres Gedankenguts und sprechen dabei gezielt Jugendliche an, die – vermeintlich oder tatsächlich – leichter zu verführen sind. Zu diesem Zweck versehen sie Lügen über den Holocaust mit angeblichen wissenschaftlichen Beweisen, verbreiten Aufrufe zur Gewalt gegen Ausländer und publizieren schwarze Listen mit den Namen von Gegnern; in Einzelfällen gibt es konkrete Mordaufrufe und Anleitungen zum Bombenbau. Die entsprechenden Inhalte sind nicht nur im WWW abrufbar, sondern zirkulieren auch per E-Mail, in Newsgroups und Foren sowie in Chatrooms. Daneben werden – unter Ausnutzung der gerade auch bei Jugendlichen beliebten Computersimulationen – Spiele zum Download bereitgestellt, in denen z. B. der

---

* Geringfügig überarbeitete Fassung eines Vortrags, den der Verfasser am 28.5.2001 auf einem Forum der Bezirksregierung in Düsseldorf gehalten hat. Das Forum stand unter dem Motto: »Rechtsextremismus und Internet – Gegenstrategien und Handlungsmöglichkeiten des Staates«. Für wertvolle Hinweise dankt der Verfasser Eike Michael *Frenzel.*

** Der Verfasser ist Wissenschaftlicher Assistent an der Universität Augsburg.

1 Dazu beispielsweise *Johnson/Post,* And how Shall the Net Be Governed?, abrufbar unter: http://www.cli.org/Dpost/governance.html.

2 Vgl. dazu *Grimm,* Der Wandel der Staatsaufgaben und die Krise des Rechtsstaats, in: ders., Die Zukunft der Verfassung, 1994, S. 159 ff.; *Pitschas,* Verwaltungsverantwortung und Verwaltungsverfahren, 1990, 48, 53 ff.; *Voßkuhle,* Das Kompensationsprinzip, 1999, S. 1 ff.; *Voßkuhle,* »Schlüsselbegriffe« der Verwaltungsrechtsreform, VerwArch 2001, 184, 185 ff.; *Rossen,* Vollzug und Verhandlung. Die Modernisierung des Verwaltungsvollzugs, 1999; *Schuppert,* Verwaltungswissenschaft, 2000; *Hoffmann-Riem,* Modernisierung von Recht und Justiz, 2001, S. 87 u. ö.; *Hoffmann-Riem,* Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung. Einführung, in: Kops/Schulz/Held (Hrsg.), Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung?, 2001, S. 9, 13.

3 Bundesamt für Verfassungsschutz (Hrsg.), Rechtsextremistische Bestrebungen im Internet, 2000, abrufbar unter: http://www.verfassungsschutz.de. Auffällig ist jedoch in diesem Zusammenhang, dass auf dem »Index« der Bundesprüfstelle für jugendgefährdende Schriften außer einigen »Zündel«-Sites nur sehr vereinzelt rechtsextremistische Websites aufgenommen sind, was wohl daran liegt, dass extremistische politische Kommunikation weniger unter dem Gesichtspunkt des Jugendschutzes beleuchtet wird; vgl. dazu Bundesprüfstelle für jugendgefährdende Schriften (BPjS), Amtliches Mitteilungsblatt 1/2001, 46 ff.

Programmnutzer die Funktion eines KZ-Leiters übernimmt oder in denen bei dem bekannten »Moorhuhn«-Spiel abzuschießende Hühner mit Judensternen und Gebetskappen versehen werden. Im MP3-Audioformat kostenlos verbreitete rechtsradikale Songs dienen oft als »Einstiegsdroge« in die Szene[4]. Die verschiedenen legalen und illegalen Angebote von rechtsextremen Organisationen sind dabei über Links miteinander verknüpft, damit sich auch unerfahrene Nutzer in dem internationalen Netzwerk der rechtsradikalen Szene schnell zurechtfinden. Das Internet verschafft der rechten Szene damit neue (An-)Werbemöglichkeiten, vermittelt ihr ein Wir-Gefühl und lässt die – traditionell oftmals zerstrittenen – rechtsextremen Gruppen in virtuellen Organisationen zusammenwachsen[5].

I. Das Regulierungsumfeld des Internet

Wenn sich der (National-)Staat vor diesem Hintergrund nicht auf eine lediglich symbolische Form von Gesetzgebung mit einem ausschließlich moralischen Geltungsanspruch seiner Normen zurückziehen will, ist in einem ersten Schritt das Regulierungsumfeld des Internet zu analysieren, um dann in einem weiteren Schritt eine darauf abgestimmte Regulierungsstrategie zu entwickeln. Für das Regulierungsumfeld des Internet gelten dabei einige Besonderheiten: Aufgegriffen werden sollen in diesem Zusammenhang die technischen Spezifika des Internet sowie das Verhalten der Internet-User.

1. Das Internet als a-zentrisches »network of networks« und seine technische Dynamik

In technischer Hinsicht leistet das Internet eine für die neuere Informationstechnologie typische Verknüpfung standardisierter Datenaustauschprotokolle. Diese sind nicht an ein bestimmtes Netzwerk gebunden und schalten alle miteinander verbundenen Computer zu einem a-zentrischen, d. h. nicht hierarchisch aufgebauten Netzwerk zusammen[6]. Anders ausgedrückt handelt es sich hierbei also um ein weltweit verwobenes Kommunikationssystem, das seinen Ursprung gerade nicht an einem oder mehreren zentralen Rechnerknoten nimmt. Diese Struktur als »network of networks«[7] unterscheidet es auch von den herkömmlichen (Massen-)Kommunikationsnetzen, die wie die klassische Verbreitung von Rundfunk, die Distributionsketten von Presseunternehmen oder das Verlagswesen insgesamt hierarchisch und funktional relativ stabil aufgebaut sind und deshalb viel eher einer so genannten »top-down«-Regulierung zugänglich sind[8]. Vorschnellen Analogien, die bei der Regulierung des Internet z. B. mit der des Presserechts angestellt worden sind[9], ist deshalb grundsätzlich mit Vorsicht zu begegnen[10].

Mit Blick auf diese technische Struktur des Internet ist aus juristischer und regulierungsorientierter Sicht vor allem die hohe Variabilität der durch das Internet ermöglichten Funktionen zu beachten. Für Eingriffe in den Kommunikationsvorgang, wie dies z. B. bei der Sperrung von bestimmten Inhalten auf der Grundlage des § 18 MDStV der Fall ist, hat diese Variabilität zur Folge, dass ein unterbrochener Kommunikationsweg nicht zwangsläufig zur Unterbrechung der Kommunikation führen muss, da die Übertragungstechnologie in der Lage und darauf angelegt ist, alternative Kommunikationswege zu finden[11]. Technisch ist es für den Endnutzer (Client oder User) nicht besonders schwer, sich über eine solche Sperre hinwegzusetzen, wenn er diesen Schutz nicht wünscht. Eine solche Umgehung funktioniert dann, wenn der Client z. B. auf einen so genannten Proxy ausweicht, der innerhalb eines zweiten Providers (z. B. im Ausland) liegt und der den Zugang zu dem betroffenen Server nicht gesperrt hat[12]. Auch ein Anbieter (Server) ist in der Lage, eine Sperrung zu umgehen, indem er z. B. alle Minuten seine IP-Adresse ändert. Bei Inhalten in Newsgroups wird einfach der Inhalt in andere, bisher unverdächtige und einwandfreie Newsgroups »gepostet«. Auch über den Namenswechsel einer News-

---

4 Dies ist ein Hinweis darauf, dass auch rechtsextreme Provider nach den Regeln der Ökonomie der Aufmerksamkeit operieren, ganz allgemein zu diesem medientheoretischen Phänomen vgl. *Luhmann,* Die Realität der Massenmedien, 1996; *Groys,* Über das Neue. Versuch einer Kulturökonomie, 1999; *Groys,* Unter Verdacht. Eine Phänomenologie der Medien, 2000; *Schmidt,* Kalte Faszination, 2000, S. 70 ff.

5 So anschaulich *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 97 f.; vgl. dazu auch ausführlich zur Illustration Bundesamt für Verfassungsschutz (Hrsg.), Rechtsextremistische Bestrebungen im Internet, 2000, abrufbar unter: http://www.verfassungsschutz.de.

6 *Ladeur,* Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 377; allgemein auch *Federrath,* Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 177.

7 Zu diesem Begriff *Noam,* Beyond Liberalization: From the Network of Networks to the Systems of Systems, in: Hoffmann-Riem/Vesting (Hrsg.), Perspektiven der Informationsgesellschaft, 1995, S. 49 ff.; vgl. dazu auch *Hartmann,* Medienphilosophie, 2000, S. 309 ff.

8 Dies soll nicht heißen, dass eine ausschließliche top-down-Regulierung in diesen Bereichen die erfolgversprechendste Regulierungsstrategie darstellt, vgl. *Hoffmann-Riem,* Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung. Einführung, in: Kops/Schulz/Held (Hrsg.), Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung?, 2001, S. 9, 14.

9 Vgl. dazu die Hinweise bei *Vesting,* § 18 MDStV Rn. 1 ff., in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000.

10 *Ladeur,* Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 377; deutlich auch *Hartmann,* Medienphilosophie, 2000, S. 311 f.

11 *Federrath*, Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 177.

12 *Federrath*, Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 179 f.

group kann man zumindest für eine kurze Zeit die ungefilterte Verbreitung von Inhalten bewirken.

Damit wird deutlich, dass eine erfolgreiche Sperrung von Inhalten bestenfalls auf Zeit gelingen kann[13]. Hier zeigt sich, dass bei der Entwicklung des Internet-Transport-Protokolls TCP/IP Wert auf einen funktionsmäßigen Datentransport auch unter Störungen gelegt wurde. Schließlich wurde das Internet ursprünglich für das US-amerikanische Militär sowie als wissenschaftliches Kommunikationsnetz entwickelt, die Idee der Hochverfügbarkeit von Informationen stand also immer mit im Vordergrund[14]. Funktion des Netzes ist es damit in erster Linie, Daten zum Zielort zu transportieren, nicht jedoch, eine inhaltliche Kontrolle zu ermöglichen. Dass dieses Systemziel erreicht worden ist, mag aus heutiger Sicht im Hinblick auf das Problem des Rechtsradikalismus im Internet bedauerlich erscheinen, es lässt sich aber nachträglich nicht ändern[15].

Als weiterer Gesichtspunkt für die Schwierigkeiten bei der Regulierung des Internet und bei dessen nationaler Aufsicht kommt hinzu, dass die technische Entwicklung des Internet längst noch nicht abgeschlossen ist. Gerade daran zeigt sich, dass das Internet ein neues kollektives Phänomen ist, für das angepasste Rechtsregeln erst noch gefunden werden müssen[16]. Bei der Anonymisierung von Daten steht die Entwicklung sogar erst am Anfang. Die Bedeutung von Anonymisierungstechniken und so genannter »File-Sharing-Systeme« – wie z. B. Gnutella – wächst stark. Bei letzteren erfolgt der reine Datenaustausch nicht mehr über zentrale Serversysteme, sondern direkt von Nutzer zu Nutzer (Peer to Peer). Dabei ist es sogar möglich, dass die Daten – beispielsweise ein rechtswidriges Bild – verschlüsselt übertragen werden oder sich nicht vollständig auf einem einzelnen Computersystem (Host), sondern – in mehrere »Bruchstücke« aufgeteilt – auf verschiedenen Hosts befinden und erst für den Fall ihres Abrufs wieder zusammengesetzt werden[17]. Hier ist für die Regulierung zu beachten, dass das Bedürfnis, Daten so bereitzustellen und auszutauschen, dass Sender und/oder Empfänger anonym sind und auch Dritte (inkl. Netzbetreiber) nicht nachvollziehen können, wer mit wem kommuniziert[18], nicht a priori von rechtsfeindlichen Motiven getragen ist, sondern häufig zwingenden rechtsgeschäftlichen Erfordernissen folgt. So sind Rechts- und Datensicherheit zentrale Grundbedingungen z. B. für ein erfolgreiches E-Commerce, b2b- und b2c-Kommunikation.

2. Die »anarchistische« Mentalität der Internetnutzer

Gerade am Beispiel der Datenverschlüsselung lässt sich ein weiteres Phänomen des Internet beschreiben, das bei der Regulierung mit einzubeziehen ist: die prinzipiell »anarchistische« Tendenz der Nutzer, die den Widerstand der User und Provider gegen (staatliche) Regeln im Internet beschreibt[19]. In seiner Entwicklungsgeschichte ist das Internet ein Kommunikationsmedium, das seinen Siegeszug unter anderem auch auf der Grundlage weitgehender Staatsfreiheit angetreten hat. Das Schlagwort einer »herrschaftsfreien Kommunikation« stellt dies deutlich heraus.

Technisch wird dies dadurch unterstützt, dass es jederzeit ohne großen Aufwand möglich ist, im Cyberspace neuen »space« zu schaffen[20]. Neuer »space« kann dadurch geschaffen werden, dass man eine softwarebasierte Grenze errichtet und dadurch »space« vom übrigen Cyberspace abtrennt. So bilden auch Websites einen eigenen »space«, die nur nach Namensregistrierung zugänglich sind, also nach Passieren einer Grenze, oder die sich nur durch Gebrauch von Marken oder multimedialen Symbolen von anderen abheben. Auch die großen Online-Dienste repräsentieren solche abgetrennten Bereiche, für die Zugang nur nach Abschluss eines Vertrages, Zahlung und mit Nutzung proprietärer Software möglich ist[21].

Die Schaffung von neuem »space« im Netz geschieht aus unterschiedlichsten Motiven, sei es, um – wie Online-Provider – das Internet kommerziell zu nutzen, auf der anderen Seite aber auch, um ganz

---

13 *Federrath*, Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 180.

14 Zur Entwicklungsgeschichte des Internet vgl. z. B. *Grassmuck*, Freie Software. Geschichte, Dynamiken und gesellschaftliche Bezüge, 9/2000, 9 ff., abrufbar unter: http://mikro.org/Events/05/text/freie-sw.pdf; *Haffner/Lyon,* Where wizards stay up late: the origins of the Internet, 1998; *Werle,* Innovationspotenziale im Internet – Selbstregelung auf Strukturebene, in: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation, 2000, S. 141, 142 ff.

15 *Schneider,* Die Wirksamkeit der Sperrung von Internet-Zugriffen, MMR 1999, 571, 576.

16 *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 376.

17 *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 101; *Federrath*, Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 177; zur Bedeutung von »Peer to Peer«-Systemen am Beispiel von Gnutella, *Kneip,* Schmutziger kleiner Bruder, Der Spiegel 18/2001, 120.

18 Diese Verfahren (z. B. Remailer und Mixmaster, siehe http://obscura.com/~loki) sind auch einsetzbar, um Inhalte z. B. in Newsgrous zu verbreiten, ohne dass der Urheber der Nachricht rückverfolgbar ist; dazu *Federrath*, Zur Kontrollierbarkeit des Internet, ZUM 1999, 177, 177 f.

19 So *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 376. *Christiansen,* Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 126, spricht in diesem Zusammenhang von einem »anarchischen« Zustand des Internet; allgemein aus steuerungstheoretischer Perspektive *Hoffmann-Riem,* Modernisierung von Recht und Justiz, 2001, S. 34, 87.

20 *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 124.

21 *Christiansen,* ebd.

gezielt Gruppenkommunikation zu betreiben. Gerade letzteres ermöglicht es z. B. dem »harten Kern« der rechtsextremen Gruppierungen, sich vom öffentlichen Netz abzuschotten und relativ ungestört zu kommunizieren. Aus der Sicht der Regulierung ist eine solche Fragmentierung[22] des Internet[23] nicht von vornherein nur als Bedrohung anzusehen. Zwar eröffnet dies namentlich für Rechtsradikale Rückzugsmöglichkeiten in ungestörte Kommunikationsräume. Auf der anderen Seite ist es netzintern (also innerhalb des eröffneten »Sub-Space«) immerhin grundsätzlich wahrscheinlicher, dass die Interessen der Teilnehmer homogen sind. Dieses Phänomen nutzen z. B. Online-Provider für Maßnahmen der Selbstregulierung. Am Beispiel von Online-Providern heißt dies, dass typischerweise ein Vertrag zustande kommt, dessen Abschluss der Provider zur Bedingung für die weitere Gewährung des Netzzugangs macht. Damit kann der Provider aber auch auf netzspezifische Weise die Befolgung von Regeln durchsetzen, da er softwarebasierte Hindernisse oder Sanktionsmechanismen gegen Regelverstöße auf technischer Ebene in das Netz implementieren kann. Der Netzzugang kann gesperrt werden, wenn z. B. die Online-Gebühren nicht bezahlt werden, aber auch soweit indizierte Inhalte kommuniziert werden und der Provider Kenntnis davon erlangt[24]. Darauf wird später noch zurückzukommen sein, wenn es darum geht, neben dem Anbieter auch den Empfänger und Nutzer rechtsradikaler Kommunikation ins Visier der Internet-Aufsicht zu nehmen.

II. Zur Forderung nach alternativen Regulierungsstrategien für das Internet und ihre Wirksamkeit im Hinblick auf rechtsradikale Kommunikation im Internet

Wegen dieser genannten Spezifika, die eine jede (staatliche) Internet-Regulierung unter anderem zu beachten hat, will sie nicht auf dem Stand bedeutungsloser symbolischer Gesetzgebung verharren, werden zwei unterschiedliche Regulierungsoptionen vertreten, die beide dem nationalen Recht und damit auch den nationalen Aufsichtsbehörden allenfalls eine (passive) Beobachterposition einräumen. Die eine Seite propagiert hier das Völkerrecht, die andere Position glaubt, dass alleine Selbstregulierung durch die beteiligten Provider und User Möglichkeiten besitzt, einheitliche Standards für deren Nutzung hervorzubringen.

Beide Positionen gehen davon aus, dass sich aufgrund der Loslösung des Internet von jedem geographischen Ort[25] eine Inkompatibilität des Internet zu den Rechtsregeln der realen Welt ergibt, welche gerade durch ihren territorialen Bezug auf den Nationalstaat gekennzeichnet sind[26]. Hier ist als allgemeiner negativer externer Effekt nationaler Regulierung zu berücksichtigen, dass Daten und Aktivitäten problemlos dorthin verlegt werden können, wo die rechtlichen Rahmenbedingungen der Aktivität nicht entgegenstehen; letztlich würde nationale Internet-Regulierung damit dem Entstehen sog. »Online-Paradiese«[27] Vorschub leisten. Wie auch bei der Problematik des Rechtsextremismus zu beobachten ist[28], versucht man nationalstaatlichen Rechtsverstößen und den damit korrespondierenden Sanktionen dadurch zu entgehen, dass die betreffenden Anbieter von einer Jurisdiktion in die nächste flüchten (»exit-option«[29])[30]. Vor allem US-amerikanische und kanadische Provider gewähren hier deutschen Extremisten »Exil«; zum Teil existieren in diesen Ländern inzwischen auch Provider, die sich ausschließlich auf die Verbreitung rechtsextremer Websites spezialisiert haben.

1. Supranationale Regulierung

Bei realistischer Betrachtung stößt allerdings eine ausschließlich supranationale Internet-Regulierung zur

22 Eine solche Fragmentierung von Kommunikationsprozessen ist geradezu typisch für die moderne Gesellschaft; vgl. dazu am Beispiel der Meinungsfreiheit *Vesting,* Soziale Geltungsansprüche in fragmentierten Öffentlichkeiten, AöR 122 (1997), 337 ff.; vgl. auch am Beispiel des Rundfunks *Vesting/Holznagel,* Zielgruppen- und Spartenprogramme im öffentlich-rechtlichen Rundfunk, insbesondere im Hörfunk, 1999, S. 31 ff.

23 *Christiansen,* Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 126, meint in diesem Zusammenhang, dass der Freiheit des Internet eine autodestruktive Tendenz zu einer Fragmentierung des Cyberspace innewohnt.

24 Der Online-Provider wird damit zum Inhaber des Flaschenhalses (»bottleneck«) in Bezug auf den Internet-Zugang, so *Christiansen,* Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 125; ähnlich auch *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 434.

25 Ganz allgemein zum Verlust des geographischen Ortes in der modernen Gesellschaft *Augé,* Orte und Nicht-Orte, Vorüberlegungen zu einer Ethnologie der Einsamkeit, 1994.

26 *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 123; instruktiv dazu auch *Osthaus,* Die Renaissance des Privatrechts im Cyberspace, AfP 2001, 13, 15 ff.; *Engel,* The Internet and the Nation State, 1999 (MPP-Publikationen 1999/7), abrufbar unter: http://www.mpp-rdg.mpg.de/deutsch/pdf_dat/9907.pdf.

27 So *Hoeren,* Rechtsoasen im Internet, MMR 1998, 297 ff.; im Internationalen Privatrecht spricht man in diesem Zusammenhang von »forum shopping«, was die Suche des Klägers nach dem für seine Sache günstigsten Recht und Gericht bezeichnet, v. *Hoffmann,* Internationales Privatrecht, 2000, S. 10 f.

28 Bundesamt für Verfassungsschutz (Hrsg.), Rechtsextremistische Bestrebungen im Internet, 2000, 1, abrufbar unter: http://www.verfassungsschutz.de.

29 *Post,* Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace, abrufbar unter: http://www.law.cornell.edu/jol/jol.table.htm, par. 1.

30 *Hoeren,* Internet und Recht – Neue Paradigmen des Informationsrechts, NJW 1998, 2849, 2852.

Bekämpfung rechtsradikaler Hasstiraden im Internet schnell auf unüberwindbare Hürden. Mag eine Regulierung im Bereich technischer Standards oder bei Fragen des diskriminierungsfreien Zugangs zum Kommunikationsmedium Internet über internationale Organisationen wie der WTO und der ITU noch vorstellbar und realisierbar sein[31], so sind bei Fragen der Inhaltsregulierung doch berechtigte Zweifel angebracht, ob hier eine internationale Einigung auf einheitliche inhaltliche Mindeststandards zu erreichen ist[32]. Dies kann bei einem Phänomen wie der Kinderpornografie noch (annähernd) gelingen, da man hier von einer internationalen Wertegemeinschaft ausgehen kann[33]. Grundbedingung für eine inhaltliche Beschränkung rechtsradikaler Internet-Kommunikation wäre jedoch, einen weltweiten (Werte-)Konsens darüber herzustellen, rechtsradikale Inhalte global in ähnlicher Weise zu ächten und zu verfolgen wie in der Bundesrepublik. Angesichts der Tatsache, dass »hate-speech« in den USA[34] und in zahlreichen anderen Demokratien sogar positiv dem Grundrechtsschutz der Meinungsfreiheit unterliegt[35], ist es nicht schwer vorherzusagen, dass die deutsche Vorstellung einer Ächtung und staatlichen Verfolgung rechtsradikaler Äußerungen diesem globalen Mindeststandard nicht angehören würde. Hinzu kommt, dass bei der Durchsetzung einer entsprechenden deutschen Forderung beispielsweise auch Staaten wie China die Blockierung von politischen Meinungsäußerungen, islamische Staaten die Sperrung der Werbung für Alkohol, der Darstellung von Frauen mit nackten Brüsten oder in Damenunterwäsche verbieten wollten[36].

2. Selbstregulierung

Im Ergebnis erscheint aber auch die Vorstellung der Cyber-Enthusiasten von einer reinen Selbstregulierung des Internet als illusorisch[37]. Als Selbstregulierung im Internet gilt in diesem Zusammenhang eine Form der Regulierung, die durch einen freien, zu allgemeinem Konsens führenden Diskurs über Regeln und die völlige Abwesenheit staatlicher Eingriffe auf nationaler und internationaler Ebene gekennzeichnet ist[38]. Die spezifischen Vorzüge der Selbstregulierung liegen in einer höheren Akzeptanz der betroffenen User, einer größeren Flexibilität und Innovationsfähigkeit sowie nicht zuletzt in einer Kostenersparnis gegenüber hoheitlicher Regulierung[39]. Als Paradebeispiel funktionierender Selbstregulierung, das sich bezeichnenderweise nicht mit problematischen Inhalten im Internet befasst[40], wird häufig die Gründung von ICANN (»Internet Corporation for the Assigned Numbers and Names«) genannt. ICANN hat sich zur Aufgabe gestellt, weitgehend staatsfrei[41] und monopolistisch die technischen Protokolle des Internet zu koordinieren und die Verwaltung der Internet-Adressen und -Namen (»Domains«) zu überwachen[42].

---

31 Vgl. aber sogar hier die skeptischen und von einem eher kontinentalen Rechtsstaats- und Legitimationsverständnis getragenen Ausführungen von *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 126 m. w. N.; in die gleiche Richtung auch *Trute,* Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), 216, 248.

32 Zuversichtlicher hier *Zimmermann,* Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145, 3152.

33 Weitere Beispiele erwähnt *Osthaus,* Die Renaissance des Privatrechts im Cyberspace, AfP 2001, 13, 15 (sexuelle Ausbeutung, Drogenhandel, Geldwäsche).

34 Einschränkungen der free speech in den USA erfolgen allenfalls auf der Grundlage des sog. »clear-and-present-danger-test« und der Figur der »fighting words«.

35 Vgl. dazu *Holznagel,* Verantwortlichkeit im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte, ZUM 2000, 1007 ff.; *Vesting,* Soziale Geltungsansprüche in fragmentierten Öffentlichkeiten, AöR 122 (1997), 337, 364 f.; *Sieber,* Die Verantwortlichkeit von Internet-Providern im Rechtsvergleich, ZUM 1999, 196 ff.; *Sieber,* Verantwortlichkeit im Internet, 1999, S. 217 ff.; *Barton,* Multimedia-Strafrecht, 1999, S. 63 ff.

36 *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 101; in die gleiche Richtung auch *Schneider,* Die Wirksamkeit der Sperrung von Internet-Zugriffen, 571, 577; von »gewissen Werteverschiebungen« in globalen Netzen sprechen in diesem Zusammenhang auch *Holznagel/Kussel,* Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet, MMR 2001, 347, 352.

37 Vgl. auch *Osthaus,* Die Renaissance des Privatrechts im Cyberspace, AfP 2001, 13, 15 ff.; vorsichtiger hier unter Hinweis auf amerikanische Erfahrungen *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 434.

38 *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 123; vgl. auch *Osthaus,* Die Renaissance des Privatrechts im Cyberspace, AfP 2001, 13 ff.

39 Allerdings neigt eine reine Selbstregulierung häufig zu selbstblockierenden Effekten in ihrer Regulierung, die als »Capture-Phänomen« beschrieben werden, vgl. dazu im Hinblick auf die Selbstregulierung des Internet *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 124.

40 Im Hinblick auf die Technik vgl. auch *Mayer,* Selbstregulierung im Internet: Verfahren zur Setzung technischer Standards, K&R 2000, 13 ff.; allgemein auch *Werle,* Innovationspotenziale im Internet – Selbstregelung auf Strukturebene, in: Hoffmann-Riem (Hrsg.), Innovation und Telekommunikation, 2000, S. 141, 151 ff.

41 Immerhin wurde ICANN vom US-amerikanischen Wirtschaftsministerium initiiert; auch die Benennung der Direktoren war nicht frei von staatlicher Einflussnahme.

42 Vgl. ausführlich zur Wirkungsweise *Kleinwächter,* ICANN als United Nations der Informationsgesellschaft?, MMR 1999, 452 ff.; *Mayer,* Selbstregulierung im Internet: Verfahren zur Setzung technischer Standards, K&R 2000, 13, 16 f.; zur Autodestruktivtät des Internet und ihrer Selbstregulierung am Beispiel von ICANN vgl. jedoch auch *Ermert,* Drei Wohnungen mit der gleichen Adresse, Süddeutsche Zeitung v. 8.5.2001, V2/15. Als erste bescheidene Ansätze für eine Funktionsfähigkeit von Selbstregulierung für problematische Inhalte im Internet sind zwei Beispiele aus jüngerer Zeit des Medienunternehmens Yahoo! zu werten (vgl. *Schiessl,* Yahoo? Oohje!, Der Spiegel 18/2001, 84): Versuche des Unternehmens, dramatische Umsatzeinbußen mit einer Expansion ins Pornogeschäft zu kompensieren, scheiterten bereits nach wenigen Tagen, da sich zahlreiche amerikanische User über die drastische Bebilderung der angebotenen Produkte erregten. Kurz nach Eröffnung ihrer »virtuellen Lust-

Angesichts der fortschreitenden Fragmentierung der (post-)modernen Gesellschaft[43] ist es aber auch hier unwahrscheinlich, dass es zu einem (Werte-)Konsens in Bezug auf substanzielle inhaltliche Fragen (außer solcher Phänomene wie Kinderpornografie) kommen wird, und es ist noch unwahrscheinlicher, dass diese als das Recht des Internet befolgt werden[44].

Wenn nun im Weiteren die ordnungsrechtliche Strategie der bundesdeutschen Internet-Aufsicht untersucht wird, so muss das nationale Ordnungsrecht auf die gerade beschriebenen Gesetzmäßigkeiten und Rationalitäten des Regulierungsbereichs abgestimmt sein, um keine Dysfunktionalitäten oder bloße Scheinlösungen zu produzieren[45].

III. Die aufsichtliche Regulierungsstrategie des MDStV

Im Bewusstsein der deutschen juristischen Öffentlichkeit steht bislang die zivil-[46] und insbesondere strafrechtliche[47] Verantwortung von Providern im Vordergrund; dies beginnt spätestens mit dem CompuServe-Urteil des AG München[48] und setzt sich fort im Verfahren gegen die PDS-Bundestagsabgeordnete Angela *Marquardt*[49] sowie jüngst im Urteil des BGH zur extraterritorialen Anwendung nationalen Strafrechts wegen rechtsradikaler Propaganda[50]. Neben dem Straf- und Zivilrecht stellen sich die Fragen nach den Pflichten der Provider in gleicher Weise aber auch für den Bereich des Verwaltungsrechts[51] und damit der staatlichen Internetaufsicht und ihrer ordnungsrechtlichen Instrumente.

Ein Blick auf die einschlägige Literatur zeigt jedoch, dass das Verwaltungsrecht hier bislang eine eher stiefmütterliche Rolle einnimmt[52]. In diesem Zusammenhang verwundert es nicht, wenn auch die Verwaltungsgerichte – soweit ersichtlich – mit der Internetaufsicht des MDStV auf der Grundlage des § 18 MDStV bislang nicht befasst sind[53]. Aus diesen Phänomenen zu schließen, dass wir es hier mit einer funktionierenden und weitgehend akzeptierten Internetaufsicht zu tun hätten, wäre wohl eher zu kurz geschlossen. Viel näher liegt die Vermutung, dass die zuständigen Aufsichtsbehörden auch vier Jahre nach Einführung des MDStV ihre Position noch nicht gefunden haben[54].

1. Zur Funktion von Ordnungs- bzw. Sicherheitsrecht im Rahmen staatlicher Aufsicht

Wichtig ist an dieser Stelle zunächst einmal, allgemein die Funktion und Funktionsweise von Ordnungsrecht für staatliche Aufsichtsstrukturen zu beschreiben. Zentraler Anknüpfungspunkt eines jeden ordnungs- oder sicherheitsrechtlichen Vorgehens in einer liberalen Gesellschaft ist der Gefahrbegriff[55]. Erst das Vorliegen

bude« sah sich Yahoo! gezwungen, dem moralischen Aufruhr nachzugeben und das Zusatzangebot einzustellen. Kurz vorher schon beugte sich Yahoo! dem sanften Druck seiner Nutzer, als es die Versteigerung von Nazi-Memorabilia stoppte, hier allerdings erst nach der zusätzlichen Intervention des französischen Tribunal de Grande Instance de Paris (allerdings ohne die Entscheidung des Gerichts zu akzeptieren; dazu vgl. http://www.cdt.org/speech/international/001221yahoocomplaint.pdf; dazu auch *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 98).

43 Vgl. dazu zusammenfassend *Hornig,* Die Petitionsfreiheit als Element der Staatskommunikation, 2001, S. 18 f. m. w. N.; allgemein auch *Lipovetsky,* Narziss oder Die Leere, 1995, S. 144, 179 ff. und passim; *Kondylis,* Der Niedergang der bürgerlichen Denk- und Lebensformen, 1991.

44 So im Ergebnis auch *Christiansen*, Selbstregulierung, regulatorischer Wettbewerb und staatliche Eingriffe im Internet, MMR 2000, 123, 126.

45 Vgl. allgemein auch *Jarren,* Netzkommunikation: Von Institutionalisierungs- und notwendigen Regulierungspozessen, in: Kops/Schulz/Held (Hrsg.), Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung, 2001, S. 307, 310 f.

46 Vgl. dazu auf der Grundlage aktueller Entscheidungen nur *Engels,* Zivilrechtliche Haftung für Inhalte im World Wide Web, AfP 2000, 524 ff.; allgemein auch *Podehl,* Internetportale mit journalistisch-redaktionellen Inhalten, MMR 2001, 17 ff.; aus der Rspr. vgl. nur LG Düsseldorf MMR 2001, 183 ff.; LG München I ZUM-RD 2000, 553 = MMR 2000, 566 ff.; LG München I MMR 2000, 489 f.; LG München I ZUM 2000, 418 ff.; LG Bremen ZUM-RD 2000, 558 = MMR 2000, 375 f.; OLG Hamburg MMR 2000, 92 ff.; LG Potsdam ZUM-RD 2000, 35 = MMR 1999, 739 f.; LG München I MMR 1999, 552 f.; LG Lübeck ZUM-RD 1999, 505 = NJW-CoR 1999, 429 ff.; LG Frankfurt CR 1999, 45 ff.

47 Dazu *Satzger,* Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109 ff.; *Römer,* Verbreitungs- und Äußerungsdelikte im Internet, 2000; *Sieber,* Verantwortlichkeit im Internet, 1999; zur Rspr. vgl. außer den später genannten OLG Nürnberg MMR 1998, 535 ff. m. Anm. *Bär;* Generalbundesanwalt v. 26.11.1997, MMR 1998, 93 ff. m. Anm. *Hoeren.*

48 AG München ZUM 1998, 685 = MMR 1998, 429 ff. mit Kritik von *Sieber* (438 ff.); vgl. dazu auch das Berufungsurteil des LG München I ZUM 2000, 247 = CR 2000, 119 ff.

49 AG Tiegarten MMR 1998, 49 ff. (technische Anleitungen zum Bombenbau).

50 BGH ZUM-RD 2001, 103 = NJW 2001, 624 ff. (= MMR 2001, 228 ff. m. Anm. *Clauß);* zum Hintergrund des Falles ausführlich *Bremer,* Strafbare Internet-Inhalte in internationaler Hinsicht, 2000, S. 125 f.

51 So *Wimmer,* Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 437.

52 Ausführlicher damit beschäftigt hat sich neben allgemeineren Beiträgen *Zimmermann,* Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145 ff.; aus der Perspektive technischer Realisierbarkeit von Sperrungsanordnungen auch K. *Köhntopp/*M. *Köhntopp/Seeger,* Sperrungen im Internet, K&R 1998, 25 ff.

53 Vgl. dazu auch *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 99, wenn er feststellt, dass bisher keine ordnungsrechtliche Sperrungsanordnung bekannt geworden sei.

54 Deutlich wird dies z. B. auch daran, dass zahlreiche Bundesländer für die Aufsicht nach dem MDStV im Bereich ihres Territoriums lediglich mit Bruchteilen von Planstellen arbeiten; es ist davon auszugehen, dass die Aufsicht faktisch in einigen Bundesländern gar nicht stattfindet.

55 Allgemein dazu *Drews/Wacke/Vogel/Martens,* Gefahrenabwehr, 1986, S. 1 f., 220 ff.; *Gusy,* Polizeirecht, 2000, Rn. 318 ff.; *Denninger,* Polizeiaufgaben, in: Lisken/Denninger (Hrsg.), Hand-

einer potenziell gefahrträchtigen Situation für als schützenswert erachtete Rechtsgüter rechtfertigt den Einsatz staatlichen Ordnungsrechts und staatlicher Interventionen in gesellschaftliche Selbstorganisationsprozesse. Dementsprechend verfolgt das Ordnungsrecht in erster Linie das Ziel, derartige Gefahren zu verhindern oder zumindest zu reduzieren.

Mit der Konzentrierung auf die primäre Aufgabe der Gefahrenabwehr wird auch deutlich, worauf es das staatliche Ordnungsrecht gerade nicht abgesehen hat: auf die Sanktionierung individueller Pflichtverletzungen und die Berücksichtigung strenger Kausalitäten. Diese spielen im Gegensatz zu zivilrechtlicher Haftung und strafrechtlicher Verantwortlichkeiten eine eher untergeordnete Rolle. Dogmatisch spiegelt sich diese Situation auch in einem der beherrschenden Grundsätze des Ordnungsrechts wider, dem Prinzip der Effektivität der Gefahrenabwehr, das auf eine möglichst rasche und nachhaltige Beseitigung oder zumindest Reduzierung[56] einer bestehenden Gefahrenlage gerichtet ist[57].

Für die Strategie des ordnungsrechtlichen Verwaltungshandelns hält die verwaltungsrechtliche Dogmatik das so genannte Opportunitätsprinzip bereit[58]. Nach diesem Prinzip bleibt es regelmäßig dem Ermessen der Aufsichtsbehörde überlassen, ob (Entschließungsermessen), wie (Auswahlermessen) und gegenüber wem (Ermessen bei der Störerauswahl) sie im konkreten Fall die ihr durch Gesetz abstrakt zur Verfügung gestellten Mittel anwendet. Das Vorgehen der Aufsichtsbehörden nach dem Prinzip der Opportunität ermöglicht ihnen hierbei ein flexibles Vorgehen mit Blick auf den gerade erwähnten Effektivitätsgrundsatz und entspricht auch der empirisch seit langem zu beobachtenden Kontrollselektivität ordnungsrechtlichen Handelns[59]. Dadurch kann die Behörde ihr Einschreiten auch von der Schwere oder Evidenz einer drohenden Gefahr abhängig machen[60].

Ein modernes und zeitgemäßes Verständnis von Ordnungsrecht macht zudem eine Flexibilisierung des ordnungsrechtlichen Mitteleinsatzes erforderlich. Lediglich eine verkürzte Vorstellung ordnungsrechtlichen Verwaltungshandelns[61] beschränkt den ordnungsrechtlichen Mitteleinsatz auf einseitig hoheitliche verhaltenslenkende Steuerung durch (bußgeldbewehrte) Ge- und Verbote. Man spricht dann auch von sog. negativer Regulierung durch imperative Steuerung[62]. In dem gleichen Maße jedoch, wie Instrumente der negativen Regulierung an Wirkungskraft verlieren, muss nach Alternativen gesucht werden[63]. Dann kann es immer weniger darum gehen, in erster Linie eingetretene oder unmittelbare Gefahren abzuwehren, sondern es ist Vorsorge zu treffen gegen Gefahrenherde; Gefahrenabwehr weitet sich damit zur Gefahrenvorsorge[64]. Legt man ein solches ordnungsrechtliches Verständnis an, dann werden auch Maßnahmen im Vorfeld der imperativen Steuerung (Schlagwort: Kooperation durch Staatskommunikation[65]) zu wichtigen Elementen ordnungsrechtlicher Handlungsspielräu-

buch des Polizeirechts, 1996, Kap. E Rn. 1 ff.; *Schuppert,* Verwaltungswissenschaften, 2000, S. 84 f.

56 So auch mit Blick auf das Internet *Zimmermann,* Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145, 3150. Wenn in diesem Zusammenhang darauf abgestellt wird (so z. B. *Gusy,* Polizeirecht, 2000, Rn. 318 ff.), dass Ordnungsrecht im Gegensatz zum Polizeirecht auf endgültige Maßnahmen der Gefahrenabwehr gerichtet ist, so wird dies der Intention effektiver Gefahrenabwehr sicher nicht gerecht, da bereits die Reduktion einer bestehenden Gefahr ordnungsrechtlichen Intentionen entspricht, wenn eine vollständige und endgültige Gefahrbeseitigung nicht zu realisieren ist.

57 Vgl. dazu z. B. *Rachor,* Das Polizeihandeln, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 1996, Kap. F Rn. 143 ff.

58 Allgemein zum Opportunitätsprinzip *Voßkuhle,* Duldung rechtswidrigen Verwaltungshandelns?, Die Verwaltung 29 (1996), 511, 514 ff. m. w. N. (vgl. dort auch die Nachweise in Fn. 30); *Meyer,* Das Opportunitätsprinzip in der Verwaltung, 1963; *Drews/Wacke/Vogel/Martens,* Gefahrenabwehr, 1986, S. 370 ff.; *Schoch,* Grundfälle zum Polizei- und Ordnungsrecht, JuS 1994, 754; *Götz,* Allgemeines Polizei- und Ordnungsrecht, 1995, Rn. 351. *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 378, geht sogar noch weiter, indem er (versuchsweise) die Strafverfolgungsbehörden für den Bereich politischer Äußerungen im Internet dem Grundsatz der Opportunität unterstellen will. A. A. aber z. B. *Knemeyer,* Der Schutz der Allgemeinheit und der individuellen Rechte durch die polizei- und ordnungsrechtlichen Handlungsvollmachten der Exekutive, VVDStRL 35 (1977), 221, 233 ff.

59 So auch *Kahl,* Die Staatsaufsicht, 2000, S. 550 f.

60 Ordnungsrecht verlangt gerade keine Omnipräsenz staatlicher Ordnungsmacht, vgl. dazu im Hinblick auf die Internetregulierung *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 376; *Vesting,* § 18 MDStV Rn. 35, in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000. Vgl. auch *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 434, der ein solches Vorgehen als »neuen« Ansatz preist. Ohne weitere Begründung a. A. *Bysikiewicz,* Zulassung und Aufsicht von Tele- und Mediendiensten, in: Kröger/Gimmy (Hrsg.), Handbuch zum Internetrecht, 2000, S. 257, 272 (»Pflicht zum Einschreiten«).

61 *Di Fabio,* Risikosteuerung im öffentlichen Recht, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, S. 143, 158, bezeichnet eine solches Verständnis von Ordnungsrecht als ein »verengtes Denken des `End-of-the-Pipe`«.

62 Vgl. dazu *Hoffmann-Riem,* Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung, Einführung, in: Kops/Schulz/Held (Hrsg.), Von der dualen Rundfunkordnung zur dienstespezifisch diversifizierten Informationsordnung?, 2001, S. 9, 13.

63 *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 434; vorsichtiger und enger in diesem Zusammenhang *Kahl,* Die Staatsaufsicht, 2000, S. 378 f., der die Wirtschaftsaufsicht in erster Linie als negative Aufsicht beschreibt.

64 So *Schuppert,* Verwaltungswissenschaften, 2000, S. 86 f.; in die gleiche Richtung unter dem Schlagwort »Prävention« auch *Grimm,* Verfassungsrechtliche Anmerkungen zum Thema Prävention, KritV 1986, 38, 40.

65 Vgl. dazu auch allgemein *Voßkuhle,* Der Wandel von Verwaltungsrecht und Verwaltungsprozessrecht in der Informationsgesellschaft, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 349, 365 ff.

me der Verwaltung[66]. Hier muss es angesichts des in dynamischen Rechtsgebieten häufig eklatanten Wissensdefizits der Verwaltung[67] dann auch Aufgabe eines modernen Ordnungsrechts sein, den Aufbau privat-öffentlicher Kommunikations- und Regulierungsnetzwerke zu initiieren[68], um so z. B. die Entwicklung einheitlicher Standards zu fördern und damit überhaupt Handlungsfähigkeit zu erlangen sowie auf Dauer zu erhalten (Stichwort: lernende Verwaltung[69])[70]. Zusammenfassend heißt dies, dass sich ordnungsrechtliche Aufsichtsstrukturen viel stärker als bisher als Beobachter und Moderatoren gesellschaftlicher Prozesse und weniger als bloße Exekutoren einseitiger hoheitlich formulierter Vorgaben begreifen müssen[71]. Ein solches Vorgehen entspricht auch der im Rahmen der Verwaltungsreformdiskussion immer wieder erhobenen Forderung nach einer »Verantwortungsteilung« bei der Wahrnehmung öffentlicher Aufgaben, was deutlich machen soll, dass es im Rahmen der Neubestimmung der Beziehungen zwischen Staat und Gesellschaft gerade kein staatliches Problemlösungsmonopol mehr gibt[72].

2. Grundstruktur der Internetaufsicht auf der Grundlage des MDStV

Untersucht man die Aufsichtsstrategie des MDStV, dann stellt man fest, dass die Aufsicht des Staatsvertrages in einem Regulierungsmodell fundiert ist, das weitgehend dem traditionellen Ordnungsrecht verhaftet bleibt und stark an das Presseordnungsrecht angelehnt ist, ohne jedoch auch organisatorisch die entsprechenden Grundlagen dafür gelegt zu haben[73]. Gegenstände der Aufsicht sind neben dem Jugend- und Datenschutz die Überwachung presseähnlicher Ordnungspflichten für professionelle Anbieter – der MDStV umschreibt dies mit dem dem Presserecht entlehnten Begriff »journalistisch-redaktionell« – wie Anbieterkennzeichnung, Einhaltung journalistischer Sorgfaltspflichten und werberechtliches Trennungsgebot (§ 18 Abs. 2 und 4 MDStV)[74]. Mit Perspektive auf die hier interessierende Frage der Verhinderung problematischer rechtsradikaler Inhalte im Internet operiert § 18 Abs. 2 MDStV mit den Mitteln der Untersagung und Sperrung, die im Hinblick auf ihre Durchsetzbarkeit durch eine Bußgeldbewehrung in § 20 Abs. 1 Nrn. 15 und 16 MDStV unterstützt werden.

Schon hier wird deutlich, dass das verwendete ordnungsrechtliche Instrumentarium stark am Modell imperativer Steuerung orientiert ist und zumindest nach dem Gesetzeswortlaut allein aus Ge- und Verboten besteht[75]. Nur am Rande finden wir bislang prozedurale und selbstregulative Instrumente: In diesem Zusammenhang ist die Initiierung der »Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter« (FSM) zu nennen, durch deren Mitgliedschaft es Diensteanbietern ermöglicht wird, ihre gesetzlichen Pflichten zur Bestellung eines eigenen Jugendschutzbeauftragten nach § 8 Abs. 4 MDStV (und § 7 a GjS) zu erfüllen[76].

---

66 Dies beweist auch ein Blick auf weniger komplexe Regelungsgegenstände des besonderen Sicherheitsrechts wie dem Versammlungsrecht, dass die normativen Eingriffsgrundlagen und Eingriffsmittel (§ 15 VersammlG) aufgrund ihrer besonderen Grundrechtsrelevanz im Wege einer Ultima-ratio-Strategie auszulegen sind.

67 Vgl. dazu differenzierend auch *Ladeur*, Rundfunkaufsicht im Multimedia-Zeitalter zwischen Ordnungsrecht und regulierter Selbstregulierung, K&R 2000, 171, 177; *Ladeur*, Risiko und Recht, in: Bechmann (Hrsg.), Risiko und Gesellschaft, 1997, S. 209 ff.

68 Allgemein dazu *Hoffmann-Riem,* Modernisierung von Recht und Justiz, 2001, S. 87.

69 Vgl. dazu z. B. *Becker,* Öffentliche Verwaltung, 1989, S. 892 f.; *Vesting,* Zwischen Gewährleistungsstaat und Minimalstaat, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 101, 128 f.

70 Vgl. zu dieser Entlastungsfunktion der Verwaltung auch *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 434; allgemein in diese Richtung auch *Voßkuhle,* Duldung rechtswidrigen Verwaltungshandelns?, Die Verwaltung 29 (1996), 511, 512; *Schuppert*, Verwaltungswissenschaft, 2000, S. 911 ff.

71 Vgl. dazu auch *Schuppert*, Verwaltungswissenschaft, 2000, S. 125 ff. m. w. N.

72 Vgl. dazu *Hoffmann-Riem,* Modernisierung von Recht und Justiz, 2001, S. 21, 23; ausführlich dazu *Schuppert*, Die öffentliche Verwaltung im Kooperationsspektrum staatlicher und privater Aufgabenerfüllung: Zum Denken in Verantwortungsstufen, Die Verwaltung 31 (1998), 415 ff.; *Schuppert*, Zur notwendigen Neubestimmung der Staatsaufsicht im verantwortungsteilenden Verwaltungsstaat, in: ders. (Hrsg.), Jenseits von Privatisierung und »schlankem« Staat, 1999, S. 299 ff.; *Voßkuhle*, Gesetzgeberische Regelungsstrategien der Verantwortungsteilung zwischen öffentlichem und privatem Sektor, in: Schuppert (Hrsg.), Jenseits von Privatisierung und »schlankem« Staat, 1999, S. 47 ff.; *Hoffmann-Riem,* Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen – Systematisierung und Entwicklungsperspektiven, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, S. 261 ff., jeweils m. w. N.

73 Hier ist vor allem an die medienrechtlichen Regelungen zur Staatsfreiheit zu denken, denen die traditionellen Massenmedien unterliegen, vgl. *Vesting*, § 18 MDStV Rn. 7 f., in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000; aus der jüngeren Judikatur zur Pressefreiheit BVerfGE 95, 28, 34. In dieser Hinsicht ist z. B. die Übertragung der Internetaufsicht an Behörden der unmittelbaren Staatsverwaltung (vgl. zu der dadurch auch verursachten organisatorischen Zersplitterung der Aufsichtsstrukturen *Vesting*, § 18 MDStV Rn. 22 ff., in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000) zumindest zweifelhaft.

74 Dazu auch *Vesting*, § 18 MDStV Rn. 1 ff., in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000; *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 376; *Wimmer,* Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 437.

75 *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 427.

76 Vgl. dazu *Altenhain,* § 7 a GjS Rn. 29, in: Roßnagel (Hrsg.), Recht der Multimediadienste, Stand: Jan. 2000; *Schulz,* Jugendschutz bei Tele- und Mediendiensten, MMR 1998, 182, 185; *Bleisteiner,* Rechtliche Verantwortlichkeit im Internet, 1999, S. 230 ff.; zu den Einzelheiten der Wirkungsweise dieser Organisation freiwilliger Selbstkontrolle des Internet vgl. auch http://www.fsm.de.

Die bundesdeutsche Internetaufsicht steht dabei immer auch im Spannungsverhältnis zwischen dem Bestreben, rechtswidrige Inhalte im Netz bestmöglich zu bekämpfen, ohne dabei verfassungs- und grundrechtlich geschützte Güter der Meinungsfreiheit und der Privatsphäre sowie die Vorteile einer freien Datenkommunikation über Gebühr zu gefährden[77]. Gerade am herkömmlichen staatlichen Ordnungsrecht orientierte repressive Aufsichtsmaßnahmen laufen hier jedoch regelmäßig Gefahr, wegen der Vielfalt der möglichen Interessenkonflikte und der Ungewissheit der Abschätzung der neuen Kommunikationsnetzwerke in das Dilemma zu geraten, entweder an der Komplexität der Regelungsprobleme zu scheitern oder aber zu viele unbeabsichtigte schädliche (externe) Nebeneffekte durch Omnipräsenz zu erzeugen[78].

IV. Zur Handhabung des § 18 MDStV als zentrale Norm der bundesdeutschen Aufsicht über rechtsradikale Inhalte im Internet

Das bedeutet nicht, dass alle Unsitten, die sich im Internet herausbilden, hingenommen werden müssen[79]. Die vorangegangen Ausführungen sollten allerdings deutlich gemacht haben, dass die Wahrnehmung der Internetaufsicht in Bezug auf rechtsradikale Inhalte nicht die völlige und endgültige Eliminierung jeder rechtsradikalen Propaganda zum Ziel haben kann; dies wäre angesichts der technischen Gegebenheiten auch eine Illusion[80]. Vielmehr spricht dies dafür, auf der Grundlage der im Recht der Gefahrenabwehr zentralen Prinzipien der Opportunität und Effektivität eine flexible und komplexitätsangemessene Aufsichtsstrategie zu wählen[81]; dies gilt im Hinblick auf das eingeräumte Entschließungsermessen in gleicher Weise wie für das Auswahlermessen (»flexible response«)[82].

Das heißt, auch dort, wo von vornherein zu schützende Drittinteressen sichtbar sind, die ohne staatliche Intervention vernachlässigt zu werden drohen, sind Kompromisse und Abwägungen notwendig, die auch die auf dem Spiel stehenden Interessen und Werte berücksichtigen sowie die Erzeugung ungewollter/externer Nebeneffekte weitgehend verhindern. Welche Konsequenzen daraus für die Arbeit der Aufsichtsbehörden zu ziehen sind, soll im Folgenden an der Wahl der Aufsichtsmittel wie auch am Beispiel der Störerauswahl illustriert werden.

1. Entscheidung über aufsichtliche Intervention und Wahl der Aufsichtsmittel

Bei der Wahl der Aufsichtsmittel ist in diesem Zusammenhang zunächst in Rechnung zu stellen, dass sich zahlreiche radikale politische Äußerungen ohnehin faktisch nur auf ein begrenztes politisches Milieu auswirken und im Übrigen eher eine provokative Ausgrenzungsfunktion gegenüber der allgemeinen Öffentlichkeit haben.

a) Hier wäre im Hinblick auf das Entschließungsermessen der Aufsichtsbehörden im Internet zu überlegen, ob nicht nach bestimmten Kommunikationsforen zu differenzieren ist. Die Differenzierung müsste hier nach solchen Kommunikationsforen unterscheiden, die auf der traditionellen Annahme einer relativ einheitlichen Öffentlichkeit basieren (Rundfunk, Presse), und solchen, die sich aufgrund ihrer netzwerkartigen Verknüpfung eher einem Zwischenbereich der Selbstverständigung der (trotz formaler Offenheit) begrenzten Gruppenkommunikation zuordnen lassen. Für das Entschließungsermessen, also der Frage, ob überhaupt reagiert wird, ließe sich dann an Gesichtspunkte anknüpfen, die für den Schutz der Presse gegen die Vorzensur sprechen: Solange eine Kommunikation eine Sphäre der Vor-Publikation nicht verlassen hat, darf sie nicht Gegenstand staatlicher Interventionen sein[83]. Hintergrund einer solchen Aufsichtsstrategie ist folglich eine »Relativierung des sicherheitsrechtlichen Gefahrbegriffs«. Dies ist von der Überlegung getragen, dass rechtsradikale Propaganda, die den Bereich interner Gruppenkommunikation der »harten rechtsextremistischen Szene« nicht überschreitet, im Hinblick auf eine politisch labile Öffentlichkeit für weniger gefahrträchtig erachtet werden. Auch wenn es ein wünschenswertes politisches Ziel ist, intolerante Propaganda insgesamt zu verhindern, so erscheint die Effektivität von Aufsichtsmaßnahmen, die auf ein generelles Verbot extremistischer Äußerungen im Internet abzielen, angesichts der dargestellten Flexibilität der Kommunikationsnetzwerke des Internet doch äußerst begrenzt[84].

---

77 *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 100.

78 *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 376.

79 So auch *Ladeur*, ebd.

80 Ähnlich auch *Goldsmith,* The Internet, Conflicts of Regulation, and International Harmonization, in: Engel/Keller (eds.): Governance of Global Networks in the Light of Differing Local Values, 2000, S. 197, 207 (Learning to live with conflict).

81 Für eine Pflicht zum Einschreiten plädiert hier – allerdings ohne weitere Begründung – *Bysikiewicz,* Zulassung und Aufsicht von Tele- und Mediendiensten, in: Kröger/Gimmy (Hrsg.), Handbuch zum Internetrecht, 2000, S. 257, 272.

82 Nicht zuletzt deshalb reduziert *Voßkuhle*, Duldung rechtswidrigen Verwaltungshandelns?, Die Verwaltung 29 (1996), 511, 512, das Opportunitätsprinzip im Ordnungsrecht auf den Grundsatz der ordnungsgemäßen Ausübung des eingeräumten Ermessens.

83 So mit Blick auf die Erprobung differenzierter Kontrollmaßstäbe *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 378; ähnlich auch *Vesting*, § 18 MDStV Rn. 36, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Stand: Jan. 2000.

84 Von vergleichbaren Gedanken sind zum Beispiel auch die Werbeverbote für die Tabakindustrie getragen. Hier wird in erster Linie das Ziel verfolgt, jugendliche Nichtraucher nicht zum gesundheitsschädlichen Nikotingenuss zu verleiten und weniger, dem »etablierten Raucher« sein Suchtverhalten abzugewöhnen.

Für diese gruppeninternen Kommunikationen könnten Verbote in enger Abstimmung mit den Strafverfolgungsbehörden und dem Verfassungsschutz auf die Verbreitung der Anleitung zur Herstellung von Sprengstoffen, der offenen Aufrufe zu Gewalt, von »Todeslisten« und vergleichbaren, unmittelbar auf die Verübung von Gewalt angelegten Aufrufe beschränkt werden[85]. Erst ab dem Zeitpunkt der Erweiterung der Kommunikation auf eine breitere Öffentlichkeit steigt auch die Gefahr der Beeinflussung z. B. politisch labiler Jugendlicher, die erst durch MP3-Files und Computerspiele spielerisch an die radikale Szene herangeführt werden. In solchen Fällen sinkt die Eingriffsschwelle aufsichtlicher Maßnahmen und dementsprechend steigt das Bedürfnis nach aufsichtlicher Intervention.

Man kann zwar auch hier einwenden, dass eine Untersagung oder Sperrung nicht unbedingt die Verbreitung solcher Inhalte insgesamt verhindern wird, allerdings wird ein Anbieter dieser Inhalte über alternative Techniken seiner Kommunikation nachdenken müssen (Verschlüsselung; Verlagerung auf andere Server und damit Adressenänderung). Es kann daher zumindest erreicht werden, dass die Kommunikation insoweit gestört ist, als sie nur in organisierten Zusammenhängen eines »sub-space« weitergeführt werden kann, und damit die Gefahr einer beiläufigen oder zufälligen Kontaktaufnahme verhindert wird. (An-)Werbebemühungen der rechtsradikalen Szene wären damit durchaus erschwert.

b) Als zulässige Aufsichtsmittel nennt § 18 Abs. 2 Satz 2 MDStV die Untersagung und Sperrung[86] von Inhalten. Mit den nachfolgenden Sätzen 3 und 4 stellt der MDStV heraus, dass diese Instrumente im Rahmen eines verhältnismäßigen Mitteleinsatzes am Ende einer Skala nicht weiter spezifizierter Aufsichtsmaßnahmen stehen (ultima ratio)[87]. Mit Untersagungen und Sperrungen[88] ist schon deshalb bei der Internet-Aufsicht behutsam umzugehen, da eine effektive Verhinderung der betreffenden Inhalte bereits technisch selten auf die indizierten Inhalte beschränkt werden kann und durch derartige Maßnahmen in aller Regel der Kommunikationsfluss auch einer Vielzahl rechtmäßiger Inhalte massiv beeinträchtigt wird[89]. Hinzu kommt, dass technisch versierte Anbieter die Sperre relativ schnell und einfach unterlaufen werden[90]. Dies führt dazu, dass der Einsatz dieser genannten Aufsichtsmittel auf wirklich gewichtige Verstöße (Evidenz) beschränkt sein wird. Das Hauptziel der (repressiven) Aufsicht wird hier dann eher darin liegen, ein politisches Zeichen der Missbilligung derartiger Kommunikation zu setzen und der Internet-Öffentlichkeit eine Präsenz der Internet-Aufsicht ins Bewusstsein zu rufen.

Aufgrund seiner Ultima-ratio-Strategie eröffnet § 18 Abs. 2 MDStV den Aufsichtsbehörden jedoch auch die Möglichkeit, im Vorfeld des Einsatzes dieser repressiven Aufsichtsmittel tätig zu werden und in Kooperation mit den großen in Deutschland tätigen Content-, Host- und Access-Providern Standards zu entwickeln, die dann Vertragsgrundlage für den Abschluss der Verträge mit den Usern werden. Damit könnten die Provider dazu bewegt werden, ein zivilrechtliches Sanktionssystem zu entwickeln, an deren Ende auch ein log-off des Endnutzers problematischer Inhalte stehen könnte. Mit einer solchen Strategie könnte auch der bundesdeutsche User erreichbar werden, gegen den bislang auf der Grundlage des MDStV keine aufsichtlichen Maßnahmen gerichtet werden können. Ein solches kooperatives Vorgehen sollte von Seiten der öffentlich-rechtlichen Internet-Aufsicht mit Anreizen wie der Einführung und Verleihung eigener Zertifikate[91] verbunden werden, womit die Provider ihrerseits zusätzliche Werbemöglichkeiten erhalten.

2. Störerauswahl, § 18 Abs. 3 MDStV

Die das Ordnungsrecht dominierenden Grundsätze der Effektivität und Opportunität ordnungsrechtlichen Handelns spiegeln sich auch bei der Störerauswahl wider und ermöglichen auch hier eine flexible Handhabung der Gefahrbekämpfung. Gerade die Störerauswahl zeigt die unterschiedlichen Rationalitäten von Zivil-, Straf- und Verwaltungsrecht. Vor diesem Hintergrund ist es nur systemgerecht, dass das Zivil- und Strafrecht differenzierte Zurechnungen etwa von Verantwortung und Haftung entwickelt haben und auch Haftungsprivilegien

85 So auch *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 378.

86 Zu den unterschiedlichen Möglichkeiten der Sperrung vgl. K. *Köhntopp/*M. *Köhntopp/Seeger,* Sperrungen im Internet, K&R 1998, 25, 29 ff. (Eingriffe in Routingtabellen von Routern; Sperrung von IP-Adressen und der Einsatz von Firewalls; Sperrung beim Anbieter oder beim Abrufer).

87 Vgl. dazu auch den ultima-ratio-Einsatz der repressiven Maßnahmen im Versammlungsgesetz (§ 15 VersammlG).

88 Bei einer solchen Maßnahme widerspricht eine generelle Untersagung bzw. Sperrung rechtsradikaler Inhalte sicherlich dem Grundsatz der Verhältnismäßigkeit; lediglich Inhalte auf konkret bezeichneten Websites sind solchen aufsichtlichen Anordnungen zugänglich. Damit kann die Aufsicht allenfalls auf einen konkreten Weg der Weiterverbreitung, nicht auf die Unterbindung der Verbreitung als solche zielen, so *Wimmer,* Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 441.

89 *Satzger,* Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109, 110; K. *Köhntopp/*M. *Köhntopp/Seeger,* Sperrungen im Internet, K&R 1998, 25, 28 f.; *Wimmer,* Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 443.

90 Anschaulich hierzu K. *Köhntopp/*M. *Köhntopp/Seeger,* Sperrungen im Internet, K&R 1998, 25, 29 ff.

91 Erste Ansätze hierzu finden sich für den Bereich der Datensicherheit im Datenschutz-Audit nach § 17 MDStV. Weitergehende Anknüpfungspunkte liefert das Umweltrecht mit dem »Umweltengel« für besonders umweltfreundliche Produkte oder Produktionsverfahren sowie mit dem Öko-Audit.

insbesondere für Access-Provider vorsehen[92]. Diese Vorstellung basiert auf der Abschichtung von (persönlichen) Verantwortungsstufen, die nach Verkehrspflichten in unterschiedlichen Funktionsräumen unterscheidet und danach auch die Ansprüche von Geschädigten differenziert (Unterlassung, Beseitigung, Schadensersatz). Derartige Unterscheidungen (und Privilegierungen) basieren letztlich auf der Priorität der individuellen Handlungsverantwortung des Autors von Äußerungen und der Überlegung, dass die Verantwortung der Mediatoren auf ihre Funktion und ihren eigenen Beitrag zu Verkehrspflichtverletzungen abgestimmt werden muss, damit unerwünschte Nebeneffekte vermieden werden[93].

§ 18 Abs. 3 i. V. m. § 5 MDStV unterscheidet drei verschiedene Provider, die als Adressaten ordnungsrechtlicher Maßnahmen in Betracht zu ziehen sind: Content-, Service-/Host- und Accessprovider (Networkprovider). In einer Analogie zum allgemeinen Sicherheitsrecht kann man hier auch von Handlungs-, Zustands- und Nichtstörern bzw. -verantwortlichen sprechen[94]. Auch wenn der Wortlaut des § 18 Abs. 3 MDStV eine grundsätzlich vorrangige Inanspruchnahme von Content- und Host-/Service-Providern nahe legt, so entspricht ein solches Vorgehen rechtstechnisch keiner strengen Subsidiarität der Inanspruchnahme des Access-Providers[95]. Die Formulierung des § 18 Abs. 3 MDStV ist nach der hier vertretenen Auffassung lediglich Ausdruck eines seitens des Gesetzgebers unglücklichen Versuchs, die Ausübung des Auswahlermessens bei der ordnungsrechtlichen Störerauswahl mit einer Rückkoppelung an unterschiedliche Providertypen vorzustrukturieren. Der ausdrückliche Hinweis auf die technische Möglichkeit und Zumutbarkeit einer Nutzungsverhinderung bei der Inanspruchnahme von Access-Providern wird aber damit lediglich zur Wiederholung einer rechtsstaatlichen Selbstverständlichkeit: der Beachtung des Verhältnismäßigkeitsprinzips[96].

In zahlreichen Fällen wird es zwar dem Übermaßverbot entsprechen, bei der Störerauswahl auch den Beitrag zur Verursachung der Gefahr (mit) zu berücksichtigen. Allerdings steht zu dem auf Maßhaltung der Handlungsmöglichkeiten der Ordnungsbehörden angelegten Prinzip des Übermaßverbots prinzipiell der die gesamte ordnungsrechtliche Aufgabenerfüllung beherrschende Gedanke der Effektivität ordnungsrechtlichen Handelns in einem Spannungsverhältnis (Zielkonflikt). Das spricht aber dann auch dafür, unter mehreren ordnungsrechtlich »Verantwortlichen« denjenigen auszuwählen, der in der Lage ist, die Gefahr am schnellsten und am wirksamsten zu bekämpfen[97]. Deshalb ist es durchaus möglich und auch ermessensgerecht, dass die betreffende Ordnungsbehörde einen der mehreren in Betracht kommenden Verantwortlichen als Adressaten in Anspruch nimmt, der nach dem zivilrechtlichen Maß seiner zurechenbaren Mitursächlichkeit »an sich« erst an zweiter Stelle oder gar nicht heranzuziehen gewesen wäre, weil er aus ordnungsrechtlicher Perspektive als »Inhaber des Gegenmittels« unter Effizienzgesichtspunkten vorzugswürdig erscheint[98].

Zwar besteht unter Fachleuten im Bereich der Netztechnik weitgehend Einigkeit darüber, dass eine Verhinderung rechtswidriger Inhalte am wirksamsten bei den Content- und Host-/Service-Providern ansetzen kann. Schließlich werden dort strafbare Inhalte längerfristig gespeichert, sodass ihnen bei Kenntnis rechtswidriger Inhalte eine Prüfung und ggf. Sperrung konkret bekannter Daten möglich und zumutbar ist[99]. Allerdings ist der Rückgriff auf den Access- bzw. Network-Provider als tauglichen Adressaten nationaler Aufsichtsmaßnahmen schon deshalb häufig der einzig erfolgversprechende Weg, da sich die betreffenden Inhalte bereits heute in zahlreichen Fällen bei Host-/Service-Providern im Ausland befinden, die damit ihre beschriebene »exit-option« wahrgenommen haben. Das Strafrecht hat hier mit der

---

92 Zu den Haftungsprivilegien *Zimmermann,* Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145, 3148 f.; ein solches Vorgehen entspricht auch der Regulierung auf europäischer Ebene (vgl. Art. 12 der E-Commerce-RL des Rates und den damit korrespondierenden § 9 des Entwurfs zum Elektronischen Geschäftsverkehrs-Gesetz), dazu *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 99; allgemein auch *Freytag,* Haftung im Netz, 1999; *Sieber,* Verantwortlichkeit im Internet, 1999.

93 So *Ladeur*, Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internet, ZUM 1997, 372, 374.

94 *Wimmer,* Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 441; vgl. auch *Zimmermann,* Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145, 3148 f.

95 Ausdrücklich für eine Subsidiarität jedoch *Zimmermann*, Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145, 3149; *Bleisteiner,* Rechtliche Verantwortlichkeit im Internet, 1999, S. 222; zu kurz greifen in diesem Zusammenhang, da lediglich an der Oberfläche des Gesetzeswortlauts verharrend, auch *Holznagel/Kussel,* Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet, MMR 2001, 347, 351.

96 Soweit *Wimmer*, Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, ZUM 1999, 436, 443, das Kriterium der Zumutbarkeit in erster Linie auf technische und wirtschaftliche Zumutbarkeit reduziert, greift dies aus der Perspektive effizienter Gefahrenabwehr sicherlich zu kurz. Weitergehend hier *Satzger,* Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109, 110; *Barton,* Multimedia-Strafrecht, 1999, S. 232 ff.

97 Vgl. dazu ganz allgemein *Denninger,* Polizeiaufgaben, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 1996, Kap. E Rn. 107 m. w. N.

98 Angelehnt an *Denninger,* Polizeiaufgaben, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 1996, Kap. E Rn. 112; vgl. auch *Friauf,* Polizei- und Ordnungsrecht, in: Schmidt-Aßmann (Hrsg.), Besonderes Verwaltungsrecht, 1999, S. 105 ff., Rn. 98 ff.; zur Notwendigkeit der Flexibilisierung adressatenrechtlicher Vorschriften ganz allgemein auch *Lindner,* Die verfassungsrechtliche Dimension der allgemeinen polizeirechtlichen Adressatenpflichten, 1997, S. 166 f. und passim.

99 So *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 99 f.

Entscheidung des BGH v. 12.12.2000[100] und seiner »extraterritorialen« Anwendung des nationalen Strafrechts einen Weg eingeschlagen[101], der dem nationalen Verwaltungsrecht und damit auch der Internet-Aufsicht im Wege des § 18 MDStV verschlossen ist[102].

Dabei gilt jedoch immer auch zu berücksichtigen, dass der einzelne Access-Provider in den meisten Fällen nur eine sehr beschränkte physisch-reale Abwehrmöglichkeit besitzt. Eine Inanspruchnahme setzt in jedem Fall voraus, dass es dem Zugangsvermittler technisch möglich ist, erstens unbekannte rechtswidrige Inhalte, die er übermittelt, ausfindig zu machen und – zweitens – entsprechende Daten zu löschen bzw. zu sperren, sodass es zu einer Übertragung an den Nutzer nicht mehr kommt. Die immens große Fülle übertragbarer Daten, die auf einer unübersehbaren Vielzahl von Servern im Internet zum Abruf bereitgehalten wird, macht nach derzeitigem technischen Stand jedoch ein effektives Aufspüren unzulässiger Inhalte nahezu unmöglich. Einer Sperrung oder Löschung steht darüber hinaus häufig entgegen, dass die auf fremden Servern gespeicherten Daten nicht der Verfügungsgewalt des Zugangsvermittlers unterstehen und eine gezielte Zugangsunterbrechung angesichts der Echtzeit, und damit in Sekundenbruchteilen erfolgenden Datenübertragung derzeit effektiv nicht realisierbar ist, es sei denn, der Zugangsvermittler hat genaue Informationen über die strafbaren Inhalte. Er kann dann eventuell den Zugriff auf eine bestimmte Internet-Adresse bzw. auf ganze Web-Server verhindern. Dabei ist jedoch zu berücksichtigen, dass auf diese Weise u. U. auch der Zugriff auf eine Vielzahl rechtmäßiger Inhalte bewirkt wird[103]. Unter Beachtung dieser Voraussetzungen sind Access-Provider jedoch im Grundsatz taugliche Adressaten von Aufsichtsmaßnahmen.

V. Schlussbemerkung und Ausblick

Trotz aller Skepsis sollte der Beitrag kein Untergangsszenario des Ordnungsrechts in Bezug auf die Internet-Regulierung beschreiben. Mir ging es vor allem darum aufzuzeigen, dass die Möglichkeiten des Ordnungsrechts im Internet bei realistischer Betrachtung dann nur sehr beschränkt sind, wenn hier eine Fortschreibung klassischer Strukturen des Ordnungsrechts stattfindet, die Ordnungsrecht ausschließlich als Vollzug repressiver Aufsichtsinstrumente begreift. Das bedeutet selbstverständlich nicht, dass im Rahmen der technischen Möglichkeiten nicht auch repressive Instrumente zum Einsatz kommen können.

Eine im Rahmen der technischen und realen Gegebenheiten funktionierende Internet-Aufsicht muss als Teil eines privat-öffentlichen Netzwerks verstanden werden[104]. Das heißt vor allem, dass die zersplitterten bundesdeutschen Aufsichtsstrukturen, die zudem häufig in hierarchische Behörden der unmittelbaren Staatsverwaltung eingegliedert sind, stärker in Richtung einer Regulierungsbehörde (regulatory agency) nach Vorbildern aus dem angloamerikanischen Rechtskreis entwickelt werden müssen[105]. Dies würde zum einen die Ausprägung einheitlicher Nutzungs- und Eingriffsstandards erleichtern, auf der anderen Seite aber auch das Selbstverständnis dieser Behörden als Moderatoren globaler Kommunikationsprozesse fördern[106]. Auf dieser Grundlage könnte die bundesdeutsche Internet-Aufsicht eine wichtige Rolle in einer vor allem von *Sieber* beschriebenen arbeits- und verantwortungsteiligen »notice and take down procedure« spielen[107].

Als erste hoffnungsvolle Ansätze sind in diesem Zusammenhang auch Aktivitäten der EG-Kommission zu werten. Danach werden internationale Hotlines und Meldestellen gefördert, welche die Host-Service-Provider auf die von ihnen gespeicherten illegalen Inhalte hinweisen und ihnen die dabei auftretenden Beweisschwierigkeiten abnehmen[108]. Dabei bieten sich auch zahlreiche Möglichkeiten für eine Kooperation der Wirtschaft mit den Strafverfolgungs- und Aufsichtsbehörden, die für alle Beteiligten von Vorteil sein kann[109].

---

100 BGH ZUM-RD 2001, 103 = NJW 2001, 624 ff.

101 Dazu mit weiteren Erläuterungen auch *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 100.

102 Zur kritischen Bewertung aus strafrechtlicher Sicht *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 101.

103 *Satzger*, Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, CR 2001, 109, 110; in gleicher Weise auch *Sieber,* Verantwortlichkeit im Internet, 1999, Rn. 212 ff., 398.

104 Allgemein dazu auch *Schuppert*, Verwaltungswissenschaft, 2000, S. 887 ff.

105 In die gleiche Richtung auch *Koenig/Röder,* Plädoyer zur Überwindung der zersplitterten Aufsicht über neue Informations- und Kommunikationsmedien, K&R 1998, 417 ff.; *Rossen-Stadtfeld,* Medienaufsicht unter Konvergenzbedingungen, ZUM 2000, 36, 40, 44 ff.; *Holznagel,* Multimedia zwischen Regulierung und Freiheit, ZUM 1999, 425, 435; *Booz Allen & Hamilton*, Aufsicht auf dem Prüfstand. Herausforderungen an die deutsche Medien- und Telekommunikationsaufsicht, 1999.

106 Die Bedeutung der Bereitstellung geeigneter Organisationsstrukturen zur sachgerechten Aufgabenerfüllung betont allgemein auch *Pitschas,* Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des allgemeinen Verwaltungsrechts, 1993, S. 219, 270 m. w. N.

107 Vgl. dazu ausführlicher *Sieber,* Verantwortlichkeit im Internet, 1999, Rn. 210 f., 482 f., 533 f.

108 Sog. »Safer Internet Action Plan« der Europäischen Kommission, vgl. http://www.europa.eu.int/ISPO/iap/index.html.

109 *Sieber,* Die Bekämpfung von Hass im Internet, ZRP 2001, 97, 102.