Bernd Holznagel, Miriam Meckel, Norbert Schneider (Hrsg.)

Rassistische und Fremdenfeindliche Inhalte im Internet – Probleme und Lösungsansätze

Publikation zum Workshop

LfM-Dokumentation
Band 24

Bernd Holznagel, Miriam Meckel, Norbert Schneider

Rassistische und fremdenfeindliche Inhalte im Internet – Probleme und Lösungsansätze

Publikation zum Workshop

›lfm:

Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Postfach 10 34 43
40025 Düsseldorf
http://www.lfm-nrw.de

Impressum

Herausgeber:
Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Bereich Tagungen und Öffentlichkeitsarbeit
Zollhof 2, 40221 Düsseldorf

Verantwortlich: Dr. Joachim Gerth
Redaktion: Sandra Brüggemann (ITM), Dagmar A. Rose

Gestaltung: disegno visuelle kommunikation, Wuppertal
Druck: Woeste Druck, Essen

Oktober 2003

Vorwort

Die Verbreitung rassistischer und fremdenfeindliche Inhalte im Internet hat in den letzten Jahren sprunghaft zugenommen. Hatte man in den Anfängen des Cyberspace die Kontrolle des Mediums noch mehr oder minder den Internetakteuren selbst überlassen, schalten sich zunehmend staatliche Stellen ein, um dieses Problem in den Griff zu bekommen. Die notwendige Folge sind intensive juristische und rechtspolitische Debatten um die Vor- und Nachteile eines solchen Vorgebens. In Nordrhein-Westfalen haben vor allem die „Sperrverfügungen" des Düsseldorfer Regierungspräsidenten vehement Kritik, aber auch viel Zuspruch gefunden. Sie waren der Anlass, am 31.10.2002 in Düsseldorf einen internationalen Workshop zum Thema „Rassistische und fremdenfeindliche Inhalte im Internet – Probleme und Lösungsansätze" zu veranstalten. Der Workshop wurde von der Staatskanzlei des Landes NRW, der Landesanstalt für Medien NRW (LfM) und dem Institut für Informations-, Telekommunikations- und Medienrecht (ITM) gemeinsam veranstaltet.

Mit der Entscheidung des OVG Münsters vom 19. März 2003 haben die Auseinandersetzungen um die rechtliche Zulässigkeit von Sperrverfügungen erneut an Aktualität gewonnen. Vorerst steht danach fest: Die Provider sind zur Sperrung der beiden rechtsextremistischen Homepages „stormfront" und „nazilauck" verpflichtet. Es gilt abzuwarten, ob dies durch die Entscheidungen in den Hauptverfahren bestätigt wird. Inzwischen ist auch der Jugendmedienschutz-Staatsvertrag in Kraft getreten. Seit dem 1. April diesen Jahres finden sich Vorgaben für alle elektronisch verbreiteten Medien in einem Regelwerk. Zudem ist nunmehr die Verantwortung für den Jugendschutz zum Teil auf Einrichtungen der Selbstkontrolle verlagert worden, die wiederum einer Zertifizierung und Kontrolle durch die neue Kommission für Jugendmedienschutz (KJM) unterliegen. Spätestens seit der Yahhoo-Entscheidung des Tribunal de Grand Instance de Paris[1] ist die Bedeutung des Themas „Globales Medium versus nationales Recht" auch einer breiten Öffentlichkeit bewusst geworden. Um hier zu internationalen (Mindest-)Standards zu gelangen, ist am 7.11.2002 das Zusatzprotokoll des Europarats zur Cybercrime-Konvention verabschiedet worden. Es steht seit Januar diesen Jahres den Mitgliedstaaten zur Annahme offen. Nicht unerwähnt bleiben darf in diesem Zusammenhang der Vorschlag für einen Rahmenbeschluss zur „Bekämpfung von Rassismus und Fremdenfeindlichkeit", den die Europäische Kommission kürzlich vorgelegt hat.

(1) Urt. V. vom 20.11.2000, TGI Paris, MMR 2001, 309.

So unterschiedlich die Ansätze zur Lösung des Problems auch sind, haben sie doch ein gemeinsames Ziel: einen möglichst effektiven Schutz der betroffenen Bevölkerungsgruppen und ethnischen Minderheiten vor strafbaren rassistischen und fremdenfeindlichen Inhalten im Netz. Dieses Vorhaben kann nicht allein durch rechtliche Mittel erreicht werden. Staat und Internetwirtschaft sind vielmehr gefordert, im Wege der Zusammenarbeit und der gegenseitigen Unterstützung zu seiner Realisierung beizutragen. Der Workshop darf als erster Schritt in diese Richtung verstanden werden.

Wir freuen uns, die zahlreichen interessanten Beiträgen des Workshops dokumentieren zu können und bedanken uns bei allen Beteiligten für ihre Mitwirkung.

Münster, im Oktober 2003

Prof. Dr. Miriam Meckel
Dr. Norbert Schneider
Prof. Dr. Bernd Holznagel

Inhaltsverzeichnis

1. Autorenverzeichnis

Doris Brocker
Bereichsleiterin Recht, Landesanstalt für Medien NRW. Studium der Rechtswissenschaft von 1976 bis 1981 an der Universität zu Köln. Nach verschiedenen Tätigkeiten seit 1992 im Bereich Recht der Landesanstalt für Medien NRW. Seit 1999 Justiziarin.

Sandra Brüggemann
Wissenschaftliche Mitarbeiterin und Doktorandin in der öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster. Promotionsvorhaben über „Gegenwärtige und zukünftige Möglichkeiten und Grenzen der Regulierung von Internetinhalten durch nationales Recht (unter Berücksichtigung von Europarecht und internationalem Recht)".

Prof. Dr. Christoph Engel
Leiter der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter in Bonn. Mitglied des Wissenschaftlichen Beirats des Ministeriums für Wirtschaft und Arbeit; Mitglied der Akademia Europaea; Mitglied des Wissenschaftlichen Beirats des Zentrums für europäische Wirtschaftsforschung (ZEW) in Mannheim; Mitglied des Wissenschaftlichen Beirates des Forschungsinstituts für Verwaltungswissenschaften in Speyer. Redakteur von „Rabels Zeitschrift", Herausgeber der Zeitschrift „Archiv für Presserecht".

Gianluca Esposito
Stellvertretender Vorsitzender der Abteilung für Privatrecht im Generaldirektorat I (Justiz) des Europarats. Abschluss des rechtswissenschaftlichen Studiums an der rechtswissenschaftlichen Fakultät der Universität Neapel, anschließend anwaltliche Tätigkeit, hauptsächlich als Strafverteidiger.

Sabine Frank
Geschäftsführerin des Vereins freiwillige Selbstkontrolle Multimedia Diensteanbieter (FSM). Studium der Rechtswissenschaften in Osnabrück und Münster. Seit Mai 2002 Vizepräsidentin der Organisation Internet Hotline Providers in Europe (INHOPE).

Dr. Thomas Hart
Projektleiter für Medienpolitik in der Bertelsmann Stiftung. Studium der Volkswirtschaftslehre an der Universität Nürnberg und „Film & Media Studies" an der University of Stirling, Schottland, Promotion am Nürnberger Volkswirtschaftlichen Institut zur europäischen Telekommunikationspolitik.

Prof. Dr. Bernd Holznagel, LL.M.
Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), öffentlich-rechtliche Abteilung an der Westfälischen Wilhelms-Universität Münster, Professor für Staats- und Verwaltungsrecht.

Prof. Dr. Miriam Meckel
Staatssekretärin für Europa, Internationales und Medien im Geschäftsbereich des Ministerpräsidenten.

Wolf Osthaus
Rechtsanwalt und Bereichsleiter Telekommunikations- und Medienpolitik beim Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM).

Dr. Isabelle Rorive
Wissenschaftliche Mitarbeiterin am Zentrum für Rechtsvergleichung der Université Libre de Bruxelles. Wissenschaftliche Mitarbeiterin am Programm Comparative Media Law and Policy (PCMLP) der Universität Oxford.

Dr. Norbert Schneider
Direktor der Landesanstalt für Medien NRW. Studium der ev. Theologie und Publizistik an den Universitäten Tübingen, Marburg und Hamburg.

Dr. Torsten Schreier
Rechtsanwalt bei Freshfields Bruckhaus Deringer, Köln. Studium der Rechtswissenschaften in Saarbrücken, Lausanne und Bonn; vertritt im verwaltungsgerichtlichen Verfahren um die Düsseldorfer Sperrungsverfügung den vor dem OVG erfolgreichen Provider.

Jürgen Schütte
Regierungsdirektor bei der Bezirksregierung Düsseldorf. Hauptdezernent in dem für Medienaufsicht in Nordrhein-Westfalen zuständigen Dezernat, das für die „Düsseldorfer Sperrverfügung" verantwortlich ist.

Pascal Schumacher
Studentische Hilfskraft in der öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster.

Christian Volkmann
Wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung und Steuerrecht der Universität Göttingen. Studium der Rechtswissenschaften an den Universitäten Marburg und Heidelberg, Referendardienst in Essen. Seit Anfang 2002 Promotionsvorhaben in dem Bereich Internet-Recht / E-Commerce bei Prof. Dr. Spindler in Göttingen.

Carsten Welp
Rechtsanwalt und Referent für Medienpolitik bei der Bertelsmann Stiftung.

2. Abkürzungsverzeichnis

a.A.	anderer Ansicht
a.a.O.	am angegebenen Ort
a.E.	am Ende
a.F.	alte Fassung
ABA	Australian Broadcasting Authority
Abb.	Abbildung
ABlEG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
Alt.	Alternative
Amtl. Begr.	Amtliche Begründung
Anh.	Anhang
Anl.	Anlage
Anm.	Anmerkung
Art.	Artikel
Aufl.	Auflage
baden-württPolG	baden-württembergisches Polizeigesetz
bayPAG	Gesetz über die Organisation der Bayerischen Staatlichen Polizei
bbgOBG	Brandenburgisches Ordnungsbehördengesetz
Beil.	Beilage
BGB	Bürgerliches Gesetzbuch

BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
BITKOM	Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien
BKA	Bundeskriminalamt
BKartA	Bundeskartellamt
br PolG	Bayerisches Polizeigesetz
bspw.	beispielsweise
BR-Drs.	Drucksachen des Deutschen Bundesrates
bremPolG	Bremisches Polizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Drucksachen des Deutschen Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungssammlung des Bundesverwaltungsgerichts
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa

CDPC	Europäischer Ausschuss für Strafrechtsfragen
CERD	Konvention von New York zur Beendigung rassischer Diskriminierung
CR	Computer und Recht
CTCPEC	Canadian Trusted Computer Evaluation Criteria
d.h.	das heißt
DB	Der Betrieb
ders.	derselbe
DNS	Domain Name System
Dr.	Doktor
DVBl	Deutsches Verwaltungsblatt
eco	Verband der deutschen Internetwirtschaft
ECRI	Europaratskommission gegen Rassismus und Fremdenfeindlichkeit
EG	Europäische Gemeinschaft
EGG	Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
Entsch	Entscheidung
etc.	et cetera
ETS	Educational Testing Service
EU	Europäische Union

EUR	Euro
e.V.	eingetragener Verein
evtl.	eventuell
f., ff.	folgende
FCC	Federal Communications Commission
Fn.	Fußnote
FS	Festschrift
gem.	gemäß
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
grds.	grundsätzlich
GRUR	Gesetzlicher Rechtschutz und Urheberrecht
GSM	Global System for Mobile Communication
GV	Gesetzesverkündungsblatt
GVBl.	Gesetz- und Verordnungsblatt
GWB	Gewerberecht
Hmb SOG	Hamburgisches Gesetz zur öffentlichen Sicherheit und Ordnung
h.M.	herrschende Meinung
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung

http	Hypertext Transfer Protocol
ICH	Internet Content Host-Provider
ICRA	Internet Content Rating System
ICTF	Internet Content Task Force
IIA	Internet Industry Association
INHOPE	Internet Hotline Providers in Europe Association
i.d.R.	in der Regel
i.R.d.	im Rahmen des/der
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
inc.	Aktiengesellschaft
inkl.	inklusive
insb.	insbesondere
IP	Internet Protocol
ISP	Internet Service-Provider
IT	Information Technology/Informationstechnik
ITM	Institut für Informations-, Telekommunikations- und Medienrecht, Münster
IuK	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienstegesetz
IuR	Informatik und Recht

JA	Juristische Arbeitsblätter
JMStV	Jugendmedienschutz-Staatsvertrag
JR	Juristische Rundschau
Jura	Juristische Ausbildung
JuS	Juristische Schulung
JW	Juristische Wochenschrift
JZ	Juristenzeitung
KJM	Kommission für Jugendmedienschutz
K&R	Kommunikation und Recht
KOM	Zeitschrift für Kommunalpolitik
Kap.	Kapitel
lit.	Buchstabe
LL.M.	Master of Law
LPresseG	Landespressegesetz
LVwG SH	Landesverwaltungsgesetz in Schleswig-Holstein
m.w.N.	mit weiteren Nachweisen
max.	maximal
MDR	Monatsschrift für Deutsches Recht
MDStV	Mediendienstestaatsvertrag
Mio	Millionen
MMR	Multimedia und Recht

n.F.	neue Fassung
NGO	Regierungsunabhängige Organisationen
NGefAG	Niedersächsisches Gefahrenabwehrgesetz
NJW	Neue Juristische Wochenschrift
NJW-CoR	Neue Juristische Wochenschrift, Computerreport
No.	Nummer
Nr.	Nummer
NRW	Nordrhein-Westfalen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht, Rechtsprechungsreport
NWVBl.	Nordrhein-Westfälische Verwaltungsblätter
o.ä.	oder ähnlich(e)
OBG NRW	Ordnungsbehördengesetz Nordrhein-Westfalen
o.k.	okay
OECD	Organisation for Economic Co-operation and Development
OFLC	Office for Film and Literature Classification
öffentl.	öffentlich
OLG	Oberlandesgericht
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OVG	Oberverwaltungsgericht
PICS	Platform for Internet Content Selection

POG RP	Polizei- und Ordnungsgesetz Rheinland-Pfalz
Prof.	Professor
RA	Rechtsanwalt
RC	Refused Classification
RD	Regierungsdirektor
Rn.	Randnummer
RP	Regierungspräsient
RStV	Rundfunkstaatsvertrag
RTKom	Zeitschrift für das Recht der Telekommunikation und das Recht der elektronischen Medien
S.	Satz, Seite
sächsPolG	Sächsisches Polizeigesetz
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SOG MV	Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern
sog.	sogenannte/r
SPolG	Sächsisches Polizeigesetz
SSL	Secure Socket Layer
Std.	Stunde/n
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

TDG	Teledienstegesetz
thürOBG	Thüringisches Ordnungsbehördengesetz
thürPAG	Thüringisches Gesetz über die Aufgaben und Befugnisse der Polizei
TK	Telekommunikation
TKG	Telekommunikationsgesetz
u.	und
u.a.	unter anderem, und andere
u.U.	unter Umständen
UN	United Nations
URL	Uniform Resource Locator
Urt.	Urteil
US	United States
USA	United States of America
usw.	und so weiter
v.	von, vom
v.a.	vor allem
Vfg.	Verfügung
VG	Verwaltungsgericht
vgl.	vergleiche
VgV	Verordnung über die Vergabe öffentlicher Aufträge
VHS	Volkshochschule

VOB	Verdingungsordnung für Bauleistungen
VOF	Verdingungsordnung für freiberufliche Leistungen
VOL	Verdingungsordnung für Leistungen
VRS	Verkehrsrechtssammlung
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WuW	Wirtschaft und Wettbewerb
WWW	World Wide Web
z.B.	zum Beispiel
zit.	zitiert
z.T.	zum Teil
ZUM	Zeitschrift für Urheberrecht und Medien
zw.	zwischen

3. Internationale Erfahrungen

3.1 Strategien zur Bekämpfung von Rassismus und Fremdenfeindlichkeit im Internet – Wo stehen wir in Europa?[2]

Dr. Isabelle Rorive

1. Einleitung

Bei der Regulierung von Internetinhalten geht es in erster Linie um die Bekämpfung von Rassismus, Fremdenfeindlichkeit und Aufruf zu Hass und Gewalt im Internet.

Hierbei stellt sich sowohl das Problem der Strafbarkeit der Inhalte als auch jenes der effektiven strafrechtlichen Verfolgung. Einige Inhalte, wie z.B. Kinderpornografie oder Urheberrechtsverletzungen, gelten heute nach gemeinsamen internationalen Maßstäben als strafbar. Andere Inhalte hingegen, wie beispielsweise jugendgefährdende, lassen sich weniger eindeutig einordnen. Ihre Verbreitung ist nicht generell gesetzeswidrig, sodass ein grundsätzliches Verbot dieser Inhalte nicht möglich ist.

Die größte Herausforderung im Zusammenhang mit Rassismus und Fremdenfeindlichkeit im Internet ist die grundlegende Diskrepanz zwischen den Rechtssystemen der USA und Europas. Ein und dieselbe Rede kann auf der einen Seite des Atlantiks erlaubt sein, während sie zugleich auf der anderen Seite streng verboten ist. Das sog. First Amendment der amerikanischen Verfassung verbietet es dem amerikanischen Kongress u.a., Gesetze zu erlassen, welche die Meinungs- und Pressefreiheit übermäßig einschränken. Der Rechtsprechung des US Supreme Court zufolge sind auch rassistische und fremdenfeindliche Propaganda verfassungsmäßig als Ausdruck politischer Meinungsfreiheit geschützt. Den US-Behörden ist die Einflussnahme auf den Inhalt solcher Kommunikationsbereiche daher grundsätzlich untersagt.

In Europa ist die Situation grundverschieden. Nach Art. 10 der Konvention zum Schutze der Menschenrechte und der Grundfreiheiten (Convention for the Protection of Human Rights and Fundamental Freedoms, EMRK) sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte wird das Recht auf freie Meinungsäußerung keineswegs schrankenlos gewährleistet. So erstreckt es sich beispielsweise nicht auf Äußerungen, die die Menschenwürde und die menschliche Integrität bedrohen, in Abrede stellen oder gar zu ihrer Zerstörung führen. Auch Äußerungen, die unmittelbar zu Hass und Gewalt gegenüber anderen Menschen aufrufen, werden nicht

(2) Der Beitrag wurde aus dem Englischen übersetzt von Pascal Schumacher.

von dem Recht auf Meinungsfreiheit geschützt. In Art. 17 der Europäischen Konvention ist ausdrücklich festgelegt, dass keine Konventionsbestimmung dahingehend ausgelegt werden darf, dass sie für irgendjemanden das Recht einräumt, die Rechte und Freiheiten anderer Menschen zu verletzen. Diese Maßstäbe stimmen mit den Bestimmungen des Internationalen Übereinkommens über Bürgerrechte und politische Rechte (Covenant on Civil and Political Rights) überein, das 1966 von den Vereinten Nationen beschlossen wurde. Angelehnt an die Grundsätze der Europäischen Menschenrechtskonvention definiert das Internationale Übereinkommen das Recht auf freie Meinungsäußerung als ein qualifiziertes Recht, also als ein Recht, welches sowohl Freiheiten als auch Pflichten und Verantwortung mit sich bringt (Art. 19).

Die strenge europäische Sicht gewinnt zunehmend auch in der Welt des Common Law an Bedeutung. Dies wird mit Blick auf zwei aktuelle Fälle deutlich, die revisionistische Propaganda zum Gegenstand haben. In Kanada wurde vom Gerichtshof für Menschenrechte (Human Rights Tribunal) am 18.1.2002 im berühmten „Zundel-Fall" entschieden, dass die den Holocaust leugnende Website, die in den Vereinigten Staaten gehostet, aber in Kanada von Ernest Zundel unterhalten wurde, rechtswidrig ist. Ähnlich hat der australische Bundesgerichtshof am 17.9.2002 entschieden. In der höchstrichterlichen Entscheidung wurde Mr. Toben, der Direktor eines namhaften revisionistischen Forschungs- und Verlagszentrums des Adelaide Instituts, angewiesen, im Internet veröffentlichtes anstößiges Material zu entfernen.

Aber auch innerhalb von Europa gibt es wesentliche Unterschiede im Umgang mit problematischen Inhalten. So mögen zwar rassistische und fremdenfeindliche Äußerungen generell unter Strafe gestellt sein. Die Verleugnung von Verbrechen gegen die Menschlichkeit jedoch erfüllt beispielsweise lediglich in vier EU-Ländern einen Straftatbestand (in Deutschland, Österreich, Frankreich und Belgien). Die EU nimmt sich neuerdings ebenfalls dieses Problems an. Im November 2001 legte die Kommission einen Vorschlag für eine Rahmenentscheidung des Rates zur Bekämpfung von Rassismus und Fremdenfeindlichkeit vor. Ziel dieses Vorschlags ist die Harmonisierung der unterschiedlichen nationalen Gesetze gegen Rassismus. Hierbei werden strenge Kriterien festgelegt. Rassismus und Fremdenfeindlichkeit werden als „der Glaube an Rasse, Hautfarbe, Abstammung oder Religion, nationale oder ethnische Herkunft als Faktoren, die Abneigung gegen Individuen oder Gruppen verursachen", definiert (Art.3 lit. a). Die in dem Vorschlag genannten Verstöße sind umfangreich:

- Die öffentliche Aufforderung zu Gewalt oder Hass zu rassistischen oder fremdenfeindlichen Zwecken.
- Öffentliche, rassistisch motivierte Beleidigungen oder Drohungen.
- Die Verleugnung oder Trivialisierung von Verbrechen gegen die Menschlichkeit.
- Die öffentliche Weitergabe oder Verbreitung von Material, welches Äußerungen von Rassismus und Fremdenfeindlichkeit enthält, unabhängig davon, auf welche Art und Weise, einschließlich der Verbreitung über das Internet (Art. 4).

Angesichts der grundlegenden Unterschiede zwischen den Wertvorstellungen in Europa und den USA stellen sich folgende Fragen:

- Sollten rassistische Inhalte im Internet überhaupt reguliert werden?
- Ist es möglich und realistisch, nationale Gesetze auf das Internet anzuwenden?
- Sollte das Internet durch internationale Regelungen reguliert werden?
- Welche Rolle könnte hier internationalen Vermittlern zukommen?

2. Regulierung rassistischer Inhalte im Internet

Vor noch nicht allzu langer Zeit gab es de facto keinerlei Regulierung anti-rassistischer Inhalte im Internet. Die Websites, die sog. Hate-Speech beinhalten, größtenteils in den Vereinigten Staaten gehostet, wurden als unerreichbar angesehen. Es war generelle Politik, diese Situation hinzunehmen. Eine solche Haltung entspricht exakt der Position, die von Verfechtern der freien Meinungsäußerung verteidigt wird. Ihnen zufolge soll das Internet eine Sphäre uneingeschränkter und absoluter Freiheit bleiben, unabhängig von jeglicher Gesetzgebung. Hier dreht sich die Debatte also um die Tauglichkeit der Regulierung selbst. Zugleich wurden die europäischen Behörden, ebenso wie nationale Regierungen und regierungsunabhängige Organisationen (NGO`s), die sich dem Kampf gegen Rassismus und Diskriminierung widmen, mit dem dramatischen Anstieg der sog. Hate-Speech im Internet konfrontiert. Statistiken des Simon-Wiesenthal-Zentrums zufolge waren im Jahr 2000 mehr als 2.300 Websites problematisch. Sie alle wurden in den Vereinigten Staaten gehostet, wo sie unter verfassungsmäßigem Schutz standen. Angeblich wurden 500 dieser Websites von Europäern ins Netz gestellt. Inzwischen liegt die Zahl der problematischen Websites bei weit über 3.000. Den neuesten Statistiken des Europarates zufolge werden von den 4.000 fremdenfeindlichen, weltweit aufgelisteten Websites mehr als 2.500 in den Vereinigten Staaten gehostet. Im Vergleich dazu gab es im Jahr 1995 nur 160 dieser Websites. Ein derartiges Wachstum des Geschäfts mit Hass und Gewalt im Internet, gekoppelt mit der stetig zunehmenden Zahl an Internetnutzern in Europa – Europa hat derzeit fast 186 Millionen Internetnutzer (Tendenz steigend), während Kanada und die Vereinigten Staaten 182 Millionen verzeichnen – verlangt nach der grundsätzlichen Anwendung von Gesetzen auch im Internet.

3. Anwendung von nationalen Anti-Rassismus-Gesetzen auf das Internet

Nationalstaaten haben aus diesem Grunde bereits versucht, nach dem Prinzip „was offline illegal ist, ist auch online illegal" ihre nationalen Gesetze auch auf das Internet anzuwenden. Hierbei galt es wiederum, die enorme Diskrepanz zwischen dem

nationalen Kompetenzbereich der Hoheitsgewalt und der Globalität des virtuellen Raums zu überwinden. Der Yahoo!-Fall ist in diesem Zusammenhang von besonderer Bedeutung. Im Jahr 2000 wies ein französischer Richter die Yahoo! Aktiengesellschaft (Yahoo! Inc.) an, entsprechende Maßnahmen zu treffen, sodass Internetnutzer in Frankreich nicht mehr auf Versteigerungsangebote von Nazi-Artikeln sowie allgemein auf jegliche auf ihren Servern gehostete nazifreundliche Websites (hauptsächlich auf Geocities) zugreifen können. Auf Ersuchen der Yahoo! Inc. entschied ein amerikanisches Bundesbezirksgericht (US Federal District Court) im November 2001, dass das First Amendment der amerikanischen Verfassung die rechtliche Durchsetzung der französischen Gerichtsentscheidung innerhalb der USA ausschließe. Ein gegen diese Entscheidung eingelegtes Rechtsmittel ist gegenwärtig vor dem amerikanischen Berufungsgericht für den Neunten Gerichtsbezirk (US Court of Appeals for the Ninth Circuit) anhängig. Gleichzeitig ist der ehemalige Yahoo!-Vorstandsvorsitzende, Tim Koogle, vor einem französischen Strafgericht wegen wissenschaftlicher Rechtfertigung von Kriegsverbrechen und Verbrechen gegen die Menschlichkeit verklagt worden. Der Yahoo!-Fall verdeutlicht, dass die Koexistenz sich widersprechender Gerichte zu einem juristischen Chaos und zu einer Sackgasse für die Gerichtsbarkeit führt. Dies zu vermeiden, ist heutzutage die eigentliche Herausforderung. Daher gibt es plötzlich Projekte, die das Internet „renationalisieren" oder „in Zonen einteilen" wollen. Sie haben es sich zur Aufgabe gestellt, juristische Probleme und Mehrkosten zu minimieren, die durch verschiedene nationale Gesetze verursacht werden. Die Einrichtung neuer technischer Vorrichtungen, welche es ermöglichen, die Internetinhalte jedem Rechtssystem entsprechend zu „formatieren", wurde erwogen. Solch eine „Formatierung" des Internet würde allerdings zum Verlust seines Charakters als globales Forum führen. Des Weiteren birgt dieser Weg die Gefahr der Unterstützung nicht-demokratischer Staaten in sich, die es darauf abgesehen haben, ihr eigenes Volk daran zu hindern, auf kontroverse Informationen und Meinungen von außen zuzugreifen.

4. Internationale Maßstäbe, die sich mit Rassismus und Fremdenfeindlichkeit befassen

Die Schaffung einheitlicher internationaler Maßstäbe hinsichtlich des Umgangs mit rassistischen und fremdenfeindlichen Äußerungen dürfte wohl die sinnvollste Lösung des Problems darstellen. Tatsächlich sind im internationalen Recht bereits derartige Maßstäbe vorgesehen. So setzt eine Bestimmung des Übereinkommens über Bürgerrechte und politische Rechte von 1966 (1966 Covenant on Civil and Political Rights) fest, dass „jegliche Unterstützung von nationalem, religiösem Hass oder von Rassenhass, welche zu Diskriminierung, Feindseligkeit oder Gewalttätigkeit aufruft, gesetzlich verboten sein soll" (Art. 20 Abs. 2). Diese Verpflichtung wurde in der

im Jahre 1969 in Kraft getretenen Konvention der Vereinten Nationen über die Beseitigung aller Formen von Rassendiskriminierung (UN Convention on the Elimination of all Forms of Racial Discrimination) präzisiert. Hier ist vorgesehen, dass die Mitgliedstaaten „jegliche Verbreitung von Gedanken, welche auf Rassenüberlegenheit oder –hass basieren, jegliche Anstiftung zu Rassendiskriminierung (...) zu einem gesetzlich strafbaren Delikt erklären sollen" (Art. 4 lit. a). Aus der UN-Konferenz gegen Rassismus aus dem Jahre 2001 in Durban ging eindeutig hervor, dass sich dieses Verbot auch auf das Internet bezieht. Die USA fühlen sich jedoch durch solche internationalen Bestimmungen nicht verpflichtet. Vielmehr haben sie sich immer wieder grundlegend dagegen gewehrt, rassistische Meinungsäußerungen gesetzlich zu verbieten.

Der Europarat (Council of Europe) befasste sich mit diesem Problem in der Konvention über Verbrechen im virtuellen Raum (Convention on Cybercrime), welche im November 2001 verabschiedet und von 30 Ländern, unter ihnen Kanada, Japan, Südafrika und nicht zuletzt die USA, unterzeichnet wurde. Diese Konvention enthält einige strafbare Handlungen im Zusammenhang mit Internetinhalten. Sowohl Kinderpornografie als auch die Verletzung von Urheberrechten sind danach strafbar. Vorherige Entwürfe enthielten als Straftatbestände auch rechtsextremistische Äußerungen. Die US-Delegation machte jedoch klar, dass derartige Bestimmungen dem First Amendment der amerikanischen Verfassung zuwiderlaufen und sie davon abhalten würden, das Übereinkommen zu unterzeichnen. Als Kompromiss wurde beschlossen, diese umstrittenen Bestimmungen zum Gegenstand eines gesonderten Protokolls zu machen, welches am 7.11.2002 vom Europarat verabschiedet worden ist. Tatsächlich haben die Vereinigten Staaten auch hier Abstand davon genommen, dieses Protokoll zu unterzeichnen. Derzeit gibt es weder offline noch online internationale Vereinbarungen mit den USA über Maßstäbe für rassistische Meinungsäußerungen. Und es scheint äußerst unwahrscheinlich, dass solch eine Vereinbarung jemals getroffen werden wird.

5. Die Rolle der Vermittler bei der Regulierung rassistischer Inhalte im Internet

Ein letzter Lösungsweg ist es, die Internet-Service-Provider (ISPs) aufzufordern, rassistische und fremdenfeindliche Internetinhalte selbst oder in Zusammenarbeit mit den Behörden zu regulieren. In den Vereinigten Staaten erließ der Kongress die so genannte „Barmherziger-Samariter-Bestimmung" („Good Samaritan provision"), enthalten im Gesetz über den Anstand in der Kommunikation (1996 Communication Decency Act, Paragraph 230-c-2). Die Regelungen dienen dem Schutz jener Internet-Service-Provider, die freiwillig handeln, „um den Zugang oder die Verfügbarkeit von Material einzuschränken, welches als schamlos, obszön, unzüchtig, wollüstig,

schmutzig, unmäßig, brutal, belästigend oder sonst anstößig angesehen wird (...)". Diese Bestimmung umfasst zweifellos auch rassistische und fremdenfeindliche Meinungsäußerungen. In der Praxis eröffnet sie den amerikanischen Internet-Service-Providern die Möglichkeit, problematische Websites trotz ihres verfassungsmäßigen Schutzes rechtmäßig zu blockieren und zu sperren. Gleichzeitig immunisiert dasselbe Gesetz die Internet-Service-Provider in Bezug auf illegales, schädigendes oder schädliches Material, welches von ihnen gespeichert oder verbreitet, aber von anderen verfasst wurde. Amerikanische Gerichte haben diese Bestimmung sehr weitreichend angewendet. Sie haben beispielsweise angeordnet, dass der die Websites hostende Anbieter selbst dann nicht zur Verantwortung gezogen werde, wenn er von dem illegalen Charakter des Inhalts Kenntnis hatte. Dies gelte selbst in den Fällen, in denen dem Service-Provider diese Tatsache zuvor von einem Opfer angezeigt worden war und er nicht darauf reagiert hatte oder in denen er das umstrittene Material bezahlt hatte. Mit anderen Worten sind Internet-Service-Provider in den Vereinigten Staaten von jeglicher Haftung aus unerlaubter Handlung freigestellt.

In Europa wurde die Angelegenheit mit der E-Commerce-Richtlinie, welche seit dem 17.1.2002 in den Mitgliedstaaten der Europäischen Union in Kraft ist, auf andere Weise geregelt. Die Richtlinie findet sowohl auf die Verbreitung und die Speicherung rassistischen und fremdenfeindlichen Materials als auch auf den unmittelbaren Aufruf zu Hass und Gewalt Anwendung. Sie legt fest, dass ISPs weder dazu verpflichtet werden können, das Internet zu überwachen noch dazu, nach illegalen Aktivitäten im Internet zu suchen (Art. 15). Die Mitgliedstaaten können sie jedoch dazu anhalten, die Behörden über illegale Gegebenheiten und Rechtsverstöße zu informieren, welche ihnen von ihren Kunden angezeigt werden. Auch kann den ISPs auferlegt werden, auf Ersuchen der Behörde Informationen mitzuteilen, die die Identifikation ihrer Abonnenten ermöglichen. Darüber hinaus erwähnt die Richtlinie ausdrücklich die Möglichkeit für nationale Gerichte und Verwaltungsbehörden, sowohl Access-, als auch Service-Providern vorzuschreiben, illegales Material wie beispielsweise rassistische und fremdenfeindliche Meinungsäußerungen, herauszufiltern oder zu entfernen (Art. 12 Abs. 3 und 14 Abs. 3). Diese Möglichkeit wurde vom Regierungspräsidenten der Bezirksregierung Düsseldorf, Jürgen Büssow, wahrgenommen, der die in seinem Kompetenzbereich niedergelassenen Access-Provider verpflichtet hat, den Zugang zu zwei im Ausland, hauptsächlich in den Vereinigten Staaten, gehosteten Naziseiten und rassistischen Websites zu blockieren. Die Verfügungen wurden unter Androhung einer Geldbuße von bis zu 200.000 Euro erlassen.

Ähnliche Maßnahmen wurden gelegentlich auch andernorts ergriffen. So wurde zum Beispiel in der Schweiz ein ehemals einflussreiches, aus den USA stammendes, nazifreundliches Internetportal (Front14.org) auf eine „schwarze Liste" gesetzt. An diese Liste halten sich die meisten Internet-Service-Provider und sperren freiwillig

den Zugang zu den problematischen Seiten. Auch viele andere Länder sind mit derartigen „schwarzen Listen" vertraut, wenn auch häufiger im Zusammenhang mit strafbarem sexuellen Material (wie zum Beispiel Kinderpornografie). Im Gegensatz dazu steht eine Gerichtsentscheidung des durch das „Yahoo-Urteil" bekannt gewordenen französischen Richters Jacques Gomez. In dem im Jahr 2001 von ihm entschiedenen sog. „Ich-klage-an-Fall" (J´accuse case) war er der Ansicht, dass es keinen Rechtsgrund gäbe, aufgrund dessen er die französischen Access-Provider anweisen könne, das in den USA gehostete Nazi-Portal Front.14 herauszufiltern.

Die E-Commerce-Richtlinie hält ferner ein neues Instrument bereit, welches nicht auf Geldstrafen oder gerichtlichen Anordnungen basiert, sondern bestimmte Verhaltensweisen belohnt. Art. 14 der E-Commerce-Richtlinie legt fest, dass der Service-Provider solange nicht verantwortlich für von ihm gespeichertes rechtswidriges Material ist, wie er von dessen illegalem Charakter keine Kenntnis hat. Sobald er Kenntnis von den rechtswidrigen Inhalten erlangt, muss er allerdings umgehend Schritte einleiten, um dieses Material zu entfernen oder zu blockieren. Ansonsten verliert er den Vorteil seiner Immunität. Diese „save-heavens-clause" soll die hostenden Provider dazu animieren, freiwillig illegales Material zu entfernen, sobald sie entweder formell von Behörden oder informell von einer Überwachungsorganisation, einem Opfer oder jedem beliebigen privaten Beteiligten von den illegalen Daten in Kenntnis gesetzt werden. Das neue, von der E-Commerce-Richtlinie zur Verfügung gestellte Instrument ist insbesondere zur Bekämpfung von Hate-Speech sehr effizient einsetzbar. Denn den ISPs ist grundsätzlich daran gelegen, den Vorteil ihrer Immunität sicherzustellen. Dies gilt grundsätzlich auch für amerikanische ISPs, die ihre Geschäfte weltweit betreiben. Für sie ist es von Bedeutung, ihren internationalen Ruf zu pflegen und ihre Vermögenswerte in Europa zu schützen. In diesem Zusammenhang setzte das Bundesamt für Verfassungsschutz dem Unternehmen eBay, welche die weltgrößte E-Shopping-Website betreibt und in Kalifornien ansässig ist, über den Verkauf von Nazi-Liedern, -Büchern, -Kleidung und -Ausrüstungen auf seiner Auktions-Seite in Kenntnis. Im Gegensatz zu Yahoo! reagierte eBay jeweils positiv auf die Mitteilungen und deaktivierte umgehend den Zugang zu den umstrittenen Internetseiten. Darüber hinaus erklärte das Unternehmen im Jahr 2001 förmlich, dass es „den Verkauf von Nazi-Artikeln sowie jedweden Gegenständen, die von fanatischen Gruppen stammen, nicht länger hosten werde".

Die Kombination der Bestimmungen der E-Commerce-Richtlinie einerseits und die amerikanische „Barmherziger-Samariter"-Bestimmung andererseits erlauben es den Europäern, „hinter dem Rücken" der Verfassung der Vereinigten Staaten von Amerika zu handeln. Sie animiert aus den USA stammende, international tätige ISPs nachhaltig dazu, eine „Anti-Hate-Speech-Politik" anzuwenden, die mit den Maßstäben des internationalen Rechts im Einklang steht. Bislang ergeben sich aus der E-Commerce-

Richtlinie zwei Strategien für die Mitgliedstaaten, um in den USA ins Netz gestelltes rassistisches Material aus dem Internet zu verbannen: Zum einen sind die europäischen Access-Provider aufgefordert, die illegalen Inhalte herauszufiltern; zum anderen sollen die US-Service-Provider davon überzeugt werden, die illegalen Inhalte insgesamt aus dem Netz zu entfernen. Es gibt jedoch noch eine dritte Strategie, welche weder darin besteht, den Zugang zu blockieren noch darin, auf eine Entfernung zu drängen: Es soll auf die Betreiber der sog. Suchmaschinen (wie Google, Altavista etc.) eingewirkt werden. Einem solchen Betreiber vorzuschreiben, nicht länger zu „problematischen" Websites zu verlinken, ist unbestreitbar eine effiziente Methode. Die meisten Internetnutzer gelangen nämlich durch eine Suchmaschine auf die gewünschte Website, mit der sie sich über einen Link verbinden lassen. Zugleich ist diese Strategie relativ unkompliziert praktizierbar, weil es nur eine Handvoll leistungsfähiger Suchmaschinen gibt, die unter Internetnutzern in Europa gebräuchlich sind. Aus diesem Grund dürften Suchmaschinen zunehmend zum Objekt der Regulierung werden. Aus einem Bericht des Berkman Zentrums für Internet und Gesellschaft der Harvard Universität (Berkman Center for Internet and Society of Harvard University) vom 24.10.2002 geht hervor, dass das in Kalifornien ansässige Unternehmen Google stillschweigend (!) 65 Websites von den auf Google.de und 113 von den auf Google.fr abrufbaren Auflistungen entfernt hat. Die meisten dieser Seiten sind antisemitisch, nazifreundlich oder stehen in Zusammenhang mit rassistischen Äußerungen (wie z.B. die Homepage stormfront.org). Aber auch „Jesus-is-Lord.com" („Jesus-ist-der-Herr.com"), eine fundamentalistische christliche Website, die unnachgiebig gegen Abtreibungen vorgeht, wurde gesperrt. Der Sprecher von Google, Nate Tyler, sagte in einem Presseinterview: „Um uns der gesetzlichen Haftung zu entziehen, entfernten wir von den Suchergebnisseiten von Google.de die Websites, die mit deutschem Recht im Widerspruch stehen können". Er deutete an, dass jede Website nach einer spezifischen Beanstandung einer ausländischen Regierung von der Liste genommen wurde, lehnte es jedoch ab, eine Auflistung der anvisierten Websites weiterzugeben.

Suchmaschinen werden von der E-Commerce-Richtlinie nicht erfasst. Dies bedeutet, dass der für Access- und Host-Provider eingerichtete Haftungsausschluss auf sie keine Anwendung findet. Artikel 21 Abs. 2 der E-Commerce-Richtlinie sieht aber vor, dass die Kommission bis zum 17.6.2003 die „Notwendigkeit für Vorschläge in Bezug auf die Haftung von Providern von Hypertext-Links und Suchmaschinen" überprüfen soll. Gegenwärtig scheint es jedenfalls so, als ob sich Google entschieden hätte, auf „Nummer Sicher" zu gehen und den offiziellen Beanstandungen der europäischen Behörden Folge zu leisten.

6. Ergebnis und Schlussfolgerung

Bei der Bekämpfung von Rassismus im Internet gilt es eine schwierige Gratwanderung vorzunehmen. Einerseits muss Zugang zu allen Informationen erhalten bleiben. Andererseits darf der Schutz elementarer Menschenrechte nicht aus den Augen verloren werden. Die E-Commerce-Richtlinie gibt uns in Europa nun Instrumente in die Hand, um Rassismus und Aufrufe zu Hass und Gewalt im Internet effektiv zu bekämpfen. Bei ihrem Gebrauch werden Informationsdienste und Überwachungsorganisationen eine wichtige Rolle spielen, um illegale Websites aufzufinden und die hierfür Verantwortlichen zu identifizieren.

3.2 Das Zusatzprotokoll zur Cybercrime-Konvention[3]

Gianluca Esposito[4]

3.2.1 Hintergrund

Seit der Verabschiedung der Menschenrechtserklärung im Jahre 1949 hat die internationale Gemeinschaft wichtige Fortschritte im Kampf gegen Rassismus, rassische Diskriminierung, Fremdenfeindlichkeit und andere Formen der Intoleranz gemacht. Es wurden Gesetze erlassen und eine Reihe internationaler Menschenrechtsabkommen verabschiedet. Besonders hervorzuheben ist in diesem Zusammenhang die aus dem Jahre 1966 stammende internationale Konvention von New York zur Beseitigung jeder Form von Rassendiskriminierung (Convention on the Elimination of All Forms of Racial Discrimination, CERD), die unter dem Dach der Vereinten Nationen geschlossen wurde. Doch trotz all dieser Fortschritte wurde das Ziel einer Welt frei von Rassenhass und rassistischen Vorurteilen bisher nur zum Teil erreicht.

Die Revolution im Bereich der Informationstechnologie hat zwar auf der einen Seite beispiellose wirtschaftliche und soziale Veränderungen in unserer Gesellschaft bewirkt. Probleme wie die der Rassendiskriminierung und Fremdenfeindlichkeit sind jedoch geblieben. Die Globalisierung bringt zudem Risiken mit sich, die zur Isolation bestimmter Gruppen und zur Verschärfung der gesellschaftlichen Unterschiede vor allem zwischen verschiedenen rassischen und ethnischen Bevölkerungskreisen führen können. Auch erleichtern die neuen Technologien kriminelle Handlungen auf vielfältige Weise. All dies stellt unsere Rechtstradition auf den Prüfstand: Informationen können per Knopfdruck in weltweiten Kommunikationsnetzen übermittelt und ausgetauscht werden. Rechtsextremistische Gruppierungen verfügen so über moderne und wirkungsvolle Mittel, um Rassismus und Fremdenfeindlichkeit zu unterstützen. Sie erlauben es ihnen, Äußerungen, die entsprechendes Gedankengut enthalten, auf einfache Weise weltweit zu verbreiten. Landesgrenzen stellen keine Hindernisse mehr dar. Immer häufiger befinden sich Straftäter nicht an den Orten, an denen sich ihre Taten auswirken. Nationale Gesetze sind aber generell auf ein bestimmtes Territorium beschränkt. Um solche Personen strafrechtlich verfolgen zu können, ist eine internationale Zusammenarbeit daher unerlässlich.

Lösungen für die aufgezeigten Probleme müssen deshalb durch das internationale Recht gefunden werden. Dies erfordert wiederum die Schaffung adäquater internationaler Rechtsinstrumente. Die Cybercrime-Konvention und das neue Zusatzprotokoll sollen diesen Anforderungen entsprechen und dabei den Menschenrechten in der

(3) Der Beitrag wurde aus dem Englischen übersetzt von Pascal Schumacher.
(4) Die in dem Beitrag präsentierten Meinungen sind die des Autors, sie entsprechen nicht notwendigerweise der Auffassung des Europarates.

neuen Informationsgesellschaft die nötige Beachtung schenken. Das Protokoll ist vom Komitee der Außenminister am 7.11.2002 beschlossen worden und steht seit Januar 2003 den Mitgliedsstaaten zur Annahme offen.

- Beide Dokumente treffen Bestimmungen zu den folgenden Straftaten: Computerbezogene Delikte: rechtswidriger Zugang/Zugriff, rechtswidrige Überwachung, Eingriffe in Daten, Eingriffe in Systeme, Missbrauch von Vorrichtungen, computerbezogene Fälschungen, Computerbetrug.
- Inhaltsbezogene Straftaten: Kinderpornografie (Art. 9 der Cybercrime-Konvention), Rassismus und Fremdenfeindlichkeit im Internet.

3.2.2 Die Cybercrime-Konvention

Gegenseitige Hilfe zur Bekämpfung von Computerstraftaten jedweder Art auf moderne und flexible Weise zu ermöglichen, ist das Ziel der Cybercrime-Konvention. Diese Konvention gehört zu den wichtigsten Verträgen in der über 50-jährigen Tradition des Europarates. Sie steht seit dem 23.11.2001 den Staaten zum Beitritt offen und wurde bisher von 34 europäischen und nicht-europäischen Staaten unterzeichnet sowie von einem Staat (Albanien) ratifiziert. Das Dokument hat bei Rechtssetzern und Rechtsanwendern sowohl innerhalb als auch außerhalb Europas ein sehr positives Echo gefunden. Kritik wurde an der Cybercrime-Konvention hingegen von Vertretern einiger Industriezweige und vor allem von Organisationen zum Schutz der Meinungsfreiheit ausgeübt. Gleiches gilt für das Zusatzprotokoll.

An inhaltsbezogenen Straftaten befasst sich die Cybercrime-Konvention mit Kinderpornografie und Urheberrechtsverletzungen. Das mit der Ausarbeitung der Konvention beauftragte Komitee hatte zwar die Möglichkeit diskutiert, andere inhaltsbezogene Verbrechen, wie etwa das Verbreiten rassistischer Propaganda über Computersysteme, mit in das Dokument einzubeziehen. Es sah sich jedoch außer Stande, hierüber einen Konsens zu erzielen. Obwohl es viele Stimmen gab, die sich für eine Einbeziehung aussprachen, waren andere Delegationen aus Gründen der Meinungsfreiheit nicht gewillt zuzustimmen.

Die Parlamentarische Versammlung empfahl in ihrer Stellungnahme 226 (2001) zur Konvention daher sofort die Anfertigung eines Protokolls unter dem Titel "Erweiterung des Anwendungsbereiches der Konvention zur Erfassung neuer Verbrechenstypen". Dabei sollte unter anderem das Ziel verfolgt werden, die Verbreitung rassistischer Propaganda als Straftat zu definieren. Der damit betraute Europäischen Ausschuss für Strafrechtsfragen (Committee on Crime Problems, CDPC) sowie das Expertenkomitee für die Kriminalisierung rassistischer und fremdenfeindlicher virtueller

Straftaten sollten ein bindendes Rechtsdokument erstellen. Dieses sollte von den einzelnen Staaten ohne Weiteres unterschrieben und ratifiziert werden können. Das Zusatzprotokoll sollte sich insbesondere mit den folgenden Punkten befassen:

- Definition und Festlegung der Reichweite von Tatmerkmalen, die nötig sind, um rassistische und fremdenfeindliche Handlungen zu kriminalisieren, die über Computernetzwerke begangen werden. Die Produktion, das Anbieten und die Verbreitung von Materialien oder Nachrichten solchen Inhalts sollte mit einbezogen werden.
- Bestimmung des Anwendungsbereichs der wesentlichen prozessrechtlichen Bestimmungen sowie der internationalen Kooperationsvorschriften der Cybercrime-Konvention für die Untersuchung und Verfolgung der im Zusatzprotokoll definierten Straftaten.

3.2.3 Das Zusatzprotokoll

a. Ziele und Aufbau

Das Protokoll in seiner heutigen Fassung verfolgt zwei verschiedene Zwecke: Zum einen soll das materielle Strafrecht im Kampf gegen Rassismus und Fremdenfeindlichkeit im Internet harmonisiert, zum anderen soll die internationale Zusammenarbeit in diesem Bereich verbessert werden. Die Angleichung nationaler Strafgesetze kann dazu beitragen, den Missbrauch von Computersystemen in solchen Staaten zu verhindern, deren Gesetze in diesem Bereich noch nicht eindeutig genug gefasst sind. Als Folge dieser Harmonisierung kann auch der Austausch von Erfahrungen im praktischen Umgang mit Fällen verbessert werden. Zudem wird die internationale Kooperation (besonders bei Auslieferungen und gegenseitiger Rechtshilfe) erleichtert, z.B. in Bezug auf Anforderungen der doppelten Strafbarkeit.

Das Zusatzprotokoll enthält vier Kapitel: Das erste Kapitel befasst sich mit der Verwendung von gemeinsamen Begriffen und Begriffsbestimmungen. Im zweiten Kapitel werden Maßnahmen auf nationaler Ebene und das materielle Recht behandelt. Die internationale Zusammenarbeit ist in Kapitel drei geregelt, während Kapitel vier Schlussbestimmungen enthält.

b. Begriffsbestimmungen

Das erste Kapitel des Zusatzprotokolls enthält die Definition von rassistischem und fremdenfeindlichem Material. Es bezieht sich auf Geschriebenes (z.B. Texte, Bücher, Zeitschriften, Äußerungen, Mitteilungen, usw.), Abbildungen (z.B. Bilder, Fotos, Zeich-

nungen, usw.) und jede andere Verkörperung rassistischer und fremdenfeindlicher Gedanken oder Theorien, die so beschaffen ist, dass sie mittels eines Computersystems aufbewahrt, weiterverarbeitet oder übertragen werden kann. Die in Art. 2 des Protokolls enthaltene Definition ist eher auf Verhalten ausgerichtet, zu dem das Material führen kann, als auf den bereits in dem Material enthaltenen Ausdruck von Gefühlen, Überzeugungen und Aversionen. Die Definition lehnt sich so weit wie möglich an bestehende nationale und internationale Definitionen und Dokumente an.

Es sind verschiedene rechtliche Instrumente auf nationaler und internationaler Ebene ausgearbeitet worden, um Rassismus und Fremdenfeindlichkeit zu bekämpfen. Bei der Ausarbeitung dieses Zusatzprotokolls wurden besonders berücksichtigt: (i) die Konvention zur Beseitigung jeder Form von Rassendiskriminierung (International Convention on all Forms of Racial Discrimination, CERD), (ii) das Protokoll Nr. 12 (ETS 177) zur Europäischen Menschenrechtskonvention (EMRK), (iii) die gemeinsame Maßnahme der Europäischen Union vom 15.7.1996, betreffend Maßnahmen zur Bekämpfung von Rassismus und Fremdenfeindlichkeit, die vom Rat aufgrund des Art. K. 3 des Europäischen Unionsvertrages beschlossen wurde, (iv) die Weltkonferenz gegen Rassismus, Rassendiskriminierung, Fremdenfeindlichkeit und ähnliche Intoleranz (Durban, 31.8. – 8.9.2001), (v) die Beschlüsse der Europäischen Konferenz gegen Rassismus (Straßburg, 13.10.2000), (vi) die umfassende Studie, die von der Europaratskommission gegen Rassismus und Fremdenfeindlichkeit (European Commission against Racism and Intolerance, ECRI) im August 2000 veröffentlicht wurde (CRI(2000)27), und (vii) der Vorschlag der Europäischen Kommission für eine Rahmenentscheidung zum Kampf gegen Rassismus und Fremdenfeindlichkeit vom November 2001.

Art. 10 der EMRK erkennt das Recht auf Meinungsfreiheit an. Dieses umfasst die Freiheit, Meinungen zu haben und über Informationen und Ideen zu kommunizieren, sie zu empfangen und zu äußern. Art. 10 der EMRK ist nicht nur anwendbar auf Informationen und Ideen, die positiv oder neutral aufgenommen oder als unbedenklich angesehen werden, sondern auch auf solche, die den Staat oder irgendeinen Teil der Bevölkerung angreifen, schockieren oder beunruhigen"[5] . Der Europäische Gerichtshof für Menschenrechte hat jedoch auch geurteilt, dass staatliche Maßnahmen zur Einschränkung der Meinungsfreiheit unter den Voraussetzungen von Art. 10 Abs. 2 EMRK gerechtfertigt sind, und zwar insbesondere dann, wenn solche Gedanken und Ausdrücke dazu genutzt werden, die Rechte anderer zu verletzen. Das Protokoll legt auf der Basis nationaler und internationaler Regularien fest, inwieweit die Verbreitung rassistischer und fremdenfeindlicher Äußerungen und Ideen die Rechte anderer verletzt.

(5) Vgl. z.B. das Handyside-Urteil v. 7.12.1976, Serie A, Nr. 24, 23, Abs. 49.

Nach der Definition in Art. 2 des Zusatzprotokolls wird vorausgesetzt, dass das betreffende Material Hass, Diskriminierung oder Gewalt befürwortet, unterstützt oder dazu aufruft. „Befürworten" meint eine positive Stellungnahme, „unterstützen" bedeutet eine Ermutigung oder Förderung des benannten Verhaltens, während „dazu aufrufen" die nachdrückliche Aufforderung zu demselben bedeutet. Der Begriff „Gewalt" steht für den illegalen Gebrauch von körperlichem Zwang, während „Hass" intensive Ablehnung oder Feindschaft meint. Bei der Interpretation des Begriffs der „Diskriminierung" sollten die EMRK (Art. 14 und Protokoll 12) und die entsprechende Rechtsprechung sowie Art. 1 der CERD beachtet werden.

Das Verbot von Diskriminierung in der EMRK garantiert allen, die sich im Gebiet eines Vertragsstaates befinden, Gleichheit bei der Ausübung und Wahrnehmung der in der EMRK gewährleisteten Rechte. Art. 14 EMRK stellt somit - als Anhang zu den anderen in der EMRK benannten Rechten - eine generelle Verpflichtung der Staaten auf. In diesem Zusammenhang bezieht sich der im Zusatzprotokoll gebrauchte Begriff der Diskriminierung auf eine unterschiedliche, nicht gerechtfertigte Behandlung von einer Person oder einer Gruppe von Personen aufgrund bestimmter Merkmale. In den verschiedenen Urteilen des Europäischen Gerichtshofs für Menschenrechte (etwa in dem Belgischen Sprachenfall oder in den Abdulaziz, Cabales und Balkandali Urteilen[6]) wird festgestellt, dass „eine unterschiedliche Behandlung diskriminierend ist, wenn sie keine objektive und vernünftige Rechtfertigung hat, d.h. wenn sie kein legitimes Ziel verfolgt oder wenn kein angemessenes Verhältnis zwischen den eingesetzten Mitteln und dem verfolgten Ziel besteht". Ob eine Behandlung diskriminierend ist, muss im Einzelfall unter Einbeziehung aller Umstände entschieden werden. Anhaltspunkte für die Interpretation des Begriffs „Diskriminierung" finden sich auch in Art. 1 der CERD, wo der Begriff „Rassendiskriminierung" „jede unterschiedliche Behandlung, jeden Ausschluss, jede Beschränkung oder Bevorzugung aufgrund von Rasse, Hautfarbe, Abstammung oder nationaler oder ethnischer Herkunft" meint, „die die Aufhebung oder Beschränkung der Anerkennung, der Wahrnehmung oder der gleichen Ausübung von Menschenrechten und Grundfreiheiten im politischen, sozialen, kulturellen oder in jedem anderen Bereich des öffentlichen Lebens zum Zweck oder zur Auswirkung hat".

Hass, Diskriminierung oder Gewalt müssen sich gegen eine einzelne Person oder eine Gruppe von Individuen richten, und zwar aus dem Grund, dass sie zu einer Gruppe gehören bzw. eine Gruppe darstellen, die sich aufgrund von Rasse, Hautfarbe, Abstammung, nationaler bzw. ethnischer Herkunft oder aufgrund ihrer Religion von anderen unterscheidet. Die Religion gilt dabei nur dann als von dem Zusatzprotokoll erfasster Anknüpfungspunkt für Gewalt etc., wenn diese als Vorwand für eines der anderen Merkmale gebraucht wird.

(6) Abdulaziz, Cabales und Balkandali Urteil v. 28.5.1985, Serie A, Nr. 94, 32, Abs. 32, 62.

Es sollte beachtet werden, dass diese Gründe nicht identisch sind mit jenen in Art. 1 des Protokolls Nr. 12 zur EMRK. Denn einige der im Protokoll zur EMRK genannten Gründe lassen sich nicht auf die Begriffe des Rassismus und der Fremdenfeindlichkeit übertragen. Die in Art. 2 des Zusatzprotokolls aufgeführten Gründe stimmen auch nicht exakt mit denen der CERD überein, da letztere auf Rassendiskriminierung im Generellen und nicht auf Rassismus als solchen ausgerichtet ist. Grundsätzlich sollten die benannten Gründe zwar im Lichte des bestehenden nationalen und internationalen Rechts interpretiert werden. Für manche Gründe bedarf es allerdings zusätzlicher Erläuterungen hinsichtlich ihrer speziellen Bedeutung in dem Zusatzprotokoll.

Das Merkmal „Abstammung" bezieht sich auf Personen oder Personengruppen, deren Vorfahren durch bestimmte Merkmale (etwa Rasse oder Hautfarbe) identifiziert werden konnten. Es müssen nicht unbedingt alle diese Merkmale bei den betroffenen Personen vorliegen, damit sie wegen ihrer Abstammung zu Opfern von Hass, Diskriminierung oder Gewalt werden können. „Abstammung" bezieht sich zudem auch nicht auf die soziale Herkunft.

Der Begriff „nationale Herkunft" muss in einem weiten Sinne verstanden werden. Er bezieht sich auf die individuelle Geschichte einer Person. Es geht dabei nicht nur um die Nationalität oder Herkunft ihrer Vorfahren, sondern auch um die eigene nationale Zugehörigkeit, und zwar unabhängig davon, ob die Person die Nationalität rechtlich noch besitzt oder nicht. Insbesondere solche Personen, die über mehr als eine Nationalität verfügen oder staatenlos sind, sollen durch die weite Interpretation des Begriffs geschützt werden, soweit sie wegen dieser Tatsachen diskriminiert werden. Darüber hinaus muss sich der Begriff der „nationalen Herkunft" nicht auf die Zugehörigkeit zu einem international anerkannten Staat beziehen. Auch Minderheiten oder andere Gruppen, die bestimmte gemeinsame Merkmale haben, sind erfasst.

Das Merkmal „Religion" taucht häufig in internationalen Rechtsinstrumenten und in nationalen Gesetzen auf. Es bezieht sich auf die Überzeugung und den Glauben. Die Einbeziehung dieses Merkmals als solches würde die Gefahr mit sich bringen, den Rahmen des Zusatzprotokolls zu sprengen. Religion kann aber als Vorwand, Alibi oder Ersatz für einen anderen in der Definition genannten Begriff dienen. Der Anknüpfungspunkt der „Religion" ist daher in diesem begrenzten Sinne zu verstehen.

Eine Besonderheit der definierten Straftaten ist, dass für ihr Vorliegen explizit vorausgesetzt wird, die betreffenden Handlungen müssten ohne Rechtfertigung vorgenommen werden. Dies spiegelt die Einsicht wieder, dass die beschriebenen Verhaltensweisen nicht per se strafwürdig sind, sondern legal oder gerechtfertigt sein können. Und dies nicht nur in Fällen, in denen klassische Rechtfertigungsgründe, wie Einwilligung, Selbstschutz oder Notwendigkeit, sondern auch in Fällen, in denen andere

Prinzipien oder Interessen (etwa das Ziel der Rechtsdurchsetzung oder Forschungszwecke) die Strafwürdigkeit ausschließen. Das Zusatzprotokoll nimmt daher solche Verhaltensweisen aus dem Straftatbestand heraus, die aufgrund der Wahrnehmung legaler staatlicher Autorität erfolgen (etwa dann, wenn die Regierung eines Mitgliedsstaates handelt, um die öffentliche Ordnung aufrecht zu halten, die nationale Sicherheit zu schützen oder Verbrechen aufzuklären).

Zudem müssen die im Protokoll genannten Straftaten vorsätzlich begangen werden, um eine Strafbarkeit zu begründen. In einigen Fällen ist ein spezielles Absichtsmerkmal Teil des Tatbestandes. Die Urheber des Protokolls und der Konvention kamen überein, dass die genaue Bedeutung des Begriffs „vorsätzlich" der nationalen Auslegung überlassen bleiben soll. So ist es z.B. für die Strafbarkeit eines Service-Providers nach dem Protokoll nicht ausreichend, wenn er Mittler verbotenen Materials war oder einen verbotenes Material enthaltenden Newsroom bzw. eine entsprechende Website betrieben hat. Es bedarf für die Strafbarkeit im Einzelfall auch des jeweils nach nationalem Recht zu bestimmenden Vorsatzes. Außerdem ist ein Service-Provider nicht verpflichtet, das Verhalten der Nutzer zu überwachen, um seine eigene Strafbarkeit zu vermeiden.

c. Straftatbestände

Das Zusatzprotokoll enthält die folgenden Straftatbestände:

- Verbreitung rassistischen und fremdenfeindlichen Materials durch Computersysteme.
- Rassistisch und fremdenfeindlich motivierte Drohungen.
- Rassistisch und fremdenfeindlich motivierte Beleidigungen.
- Leugnung, massive Trivialisierung, Billigung oder Rechtfertigung von Völkermord oder Verbrechen gegen die Menschlichkeit.
- Hilfeleistung zu und Förderung von einer der im Zusatzprotokoll genannten Straftaten.

aa. Verbreitung rassistischen und fremdenfeindlichen Materials durch Computersysteme

Das Zusatzprotokoll verpflichtet die Mitgliedstaaten, die Verbreitung oder anderweitige Zurverfügungstellung rassistischen und fremdenfeindlichen Materials für die Öffentlichkeit über Computersysteme unter Strafe zu stellen. Die Handlung des Verbreitens oder anderweitigen Zurverfügungstellens ist nur strafbar, wenn der Vorsatz auch auf den rassistischen und fremdenfeindlichen Charakter des Materials gerichtet ist.

Das Merkmal „für die Öffentlichkeit", das in Art. 3 des Zusatzprotokolls verwendet wird, macht deutlich, dass private Äußerungen, die über Computersysteme ausgetauscht und übertragen werden, nicht unter diese Bestimmung fallen. Solche individuelle Kommunikation und private Äußerungen sind vielmehr, wie auch traditionelle Kommunikationsformen, von Art. 8 der EMRK geschützt. Ob die Übermittlung rassistischen und fremdenfeindlichen Materials als private Kommunikation oder als Verbreitung für die Öffentlichkeit anzusehen ist, muss anhand der Umstände des Einzelfalles entschieden werden. In erster Linie ist die Absicht des Absenders maßgeblich, ob die Mitteilung nur von einem bestimmten Adressaten empfangen werden soll oder nicht. Das Vorliegen dieser subjektiven Absicht lässt sich anhand einiger objektiver Faktoren ermitteln. Als solche sind etwa der Inhalt der Mitteilung, die eingesetzte Technologie, die angewandten Sicherheitsmaßnahmen und der Kontext, in dem die Mitteilung übermittelt wird, zu nennen. Wenn entsprechende Mitteilungen gleichzeitig an mehrere Empfänger geschickt werden, sind die Anzahl der Empfänger und die Beziehung zwischen dem Absender und den Empfängern maßgebliche Faktoren für die Einordnung der Kommunikation als privat. Der Austausch rassistischen Materials in Chat-Rooms und die Bereitstellung von solchem Material in Newsgroups oder Diskussionsforen sind Beispiele für das Zurverfügungstellen von Inhalten für die Öffentlichkeit. In solchen Fällen ist das Material für jede Person zugänglich. Selbst wenn der Zugang die Autorisierung mittels eines Passworts erfordert, ist der Inhalt doch der Öffentlichkeit zugänglich, wenn eine solche Autorisierung jedem bzw. jeder Person, die bestimmte Kriterien erfüllt, gewährt wird. Hierbei sollte auch die Beziehung zwischen den betroffenen Personen berüksichtigt werden.

bb. Rassistisch und fremdenfeindlich motivierte Drohungen

Die meisten nationalen Gesetzeswerke stellen „Drohungen" ohnehin bereits generell unter Strafe. Die Urheber des Zusatzprotokolls sind übereingekommen, in diesem Dokument trotzdem zu betonen, dass durch rassistische und fremdenfeindliche Motive veranlasste Drohungen zweifelsfrei unter Strafe zu stellen sind. Der Begriff der „Drohung" meint eine Äußerung, die bei dem Adressaten die Angst auslöst, das Opfer einer schweren Straftat (etwa gegen das Leben, die körperliche Unversehrtheit, die Sicherheit des Adressaten bzw. seiner Angehörigen oder auch in schwerer Form gegen sein Eigentum) zu werden. Es bleibt den Mitgliedstaaten überlassen, festzulegen, welche Delikte in diesem Zusammenhang als schwere Straftaten anzusehen sind. Gemäß dem Protokoll muss die Drohung (i) sich entweder gegen eine Person richten, und zwar aus dem Grund, dass sie zu einer Gruppe gehört, die durch Rasse, Hautfarbe, Abstammung, nationale oder ethnische Herkunft oder Religion gekennzeichnet ist oder (ii) eine Personengruppe betreffen, die durch eines der genannten Merkmale bestimmt wird. Es besteht keine Begrenzung dahingehend, dass die Drohung öffentlich sein muss. Der entsprechende Artikel deckt somit auch Drohungen in privater Kommunikation ab.

cc. Rassistisch und fremdenfeindlich motivierte Beleidigungen

Art. 5 des Zusatzprotokolls betrifft die öffentliche Beleidigung von Personen und Personengruppen, weil sie zu einer Gruppe gehören, die aufgrund bestimmter Merkmale abgegrenzt wird. Der Begriff „Beleidigung" meint jede angreifende, abwertende oder schmähende Äußerung, die die Ehre oder die Würde der Person beeinträchtigt. Es muss sich aus der Äußerung selbst ergeben, dass sich die Beleidigung direkt auf die Zugehörigkeit der beleidigten Person zu der entsprechenden Gruppe bezieht. Anders als in Fällen der Drohung ist eine Beleidigung in privater Kommunikation nicht von der Bestimmung erfasst.

dd. Leugnung, massive Trivialisierung, Billigung oder Rechtfertigung von Genozid oder Verbrechen gegen die Menschlichkeit

In den vergangenen Jahren hatten die nationalen Gerichte mit einer Reihe von Fällen zu tun, in denen Personen in den Medien oder sonst in der Öffentlichkeit Ideen oder Theorien geäußert haben, die darauf abzielten, insbesondere die im zweiten Weltkrieg begangenen Verbrechen (speziell den Holocaust) zu leugnen, massiv zu trivialisieren, zu billigen oder zu rechtfertigen. Als angebliche Motivation für solche Verhaltensweisen wird oft der wissenschaftliche Forschungsdrang angeführt, während in Wahrheit diejenigen Gedanken und Überzeugungen, die zum Holocaust geführt haben, gefördert und verbreitet werden sollen. Darüber hinaus hat dieses Verhalten auch rassistische und fremdenfeindliche Gruppen zu ihren Taten, auch zu solchen über Computersysteme, inspiriert, angestiftet und ermutigt. Die Äußerung solcher Ideen beleidigt die Personen, die zu den Opfern dieser Gräuel wurden, ihr Andenken sowie ihre Angehörigen. Schließlich bedroht es auch die Würde der menschlichen Gemeinschaft. Art. 6 des Zusatzprotokolls, der eine ähnliche Struktur hat wie Art. 3, befasst sich mit diesem Problem. Die Urheber des Protokolls haben beschlossen, dass es wichtig sei, Äußerungen, in denen Handlungen, die Genozid oder Verbrechen gegen die Menschlichkeit darstellen, geleugnet, massiv trivialisiert, gebilligt oder gerechtfertigt werden, unter Strafe zu stellen.

Die Begriffe „Genozid" und „Verbrechen gegen die Menschlichkeit" sind dabei anhand der Definitionen des internationalen Rechts und gemäß den abschließenden und bindenden Entscheidungen des internationalen Militärgerichtshofes, der gemäß dem Londoner Statut vom 8.4.1945 errichtet wurde, zu bestimmen. Grund dafür ist, dass die entscheidenden Taten, die Völkermord und Verbrechen gegen die Menschlichkeit zur Folge hatten, zwischen 1939 und 1945 begangen wurden. Die Urheber des Protokolls haben jedoch erkannt, dass auch in der Folgezeit andere Fälle von Genozid und Verbrechen gegen die Menschlichkeit vorgekommen sind, die massiv durch rassistische und fremdenfeindliche Ideen und Theorien motiviert wurden. Daher wurde es für notwendig erachtet, den Anwendungsbereich der Bestimmungen nicht auf die von den

Nazis während des zweiten Weltkrieges begangenen Verbrechen, wie sie vom Nürnberger Kriegsverbrechertribunal festgestellt wurden, zu beschränken. Es sollen vielmehr auch Völkermord und Verbrechen gegen die Menschlichkeit miteinbezogen werden, auf die von anderen internationalen Gerichten, welche nach 1945 durch entsprechende Beschlüsse eingesetzt wurden (UN-Sicherheitsratsbeschlüsse, multilaterale Verträge etc.) erkannt wurde. Als solche Gerichte sind etwa das Internationale Kriegsverbrechertribunal für Jugoslawien, dasjenige für Ruanda und der Internationale Strafgerichtshof zu nennen. Der Artikel erlaubt die Bezugnahme auf endgültige und bindende Entscheidungen von zukünftigen Gerichtshöfen, soweit die unterzeichnenden Staaten die Kompetenz eines solchen Gerichtshofes anerkennen.

Die Bestimmung verdeutlicht, dass Tatsachen, deren historisches Vorliegen positiv festgestellt wurde, nicht geleugnet, massiv relativiert, gebilligt oder gerechtfertigt werden dürfen, um diese furchtbaren Meinungen und Theorien zu unterstützen. Der Europäische Gerichtshof für Menschenrechte hat klargestellt, dass das Leugnen und die Revision von "klar festgestellten historischen Fakten- wie dem Holocaust – (...) vom Schutz des Art. 10 durch Art. 17" der EMRK ausgeschlossen wird (in diesem Zusammenhang ist das Lehideux und Isorni Urteil vom 23.9.1998 zu beachten)[7] .

ee. Hilfeleistung und Förderung

Sinn dieser Bestimmung ist es, auch die Hilfeleistung bei der Begehung der im Protokoll aufgeführten Delikte sowie ihre Förderung unter Strafe zu stellen. Hilfeleistung und Förderung sind wie alle in dem Protokoll definierten Verbrechen, nur bei entsprechendem Vorsatz strafbar. Zum Beispiel kann ein Service-Provider, obwohl die Übertragung von rassistischem und fremdenfeindlichem Material nur mittels seiner Hilfe über seine Infrastruktur geschehen kann, sich nicht nach diesem Abschnitt strafbar machen, wenn ihm der Verbrechensvorsatz fehlt. Im Übrigen gibt es auch hier keine Pflicht eines Service-Providers, aktiv die Inhalte in seinem Service zu überwachen, um einer Strafbarkeit nach diesem Abschnitt zu entgehen.

d. Prozessrechtliche Instrumente, Kompetenzen und Internationale Zusammenarbeit

Die Bestimmungen der Cybercrime-Konvention über prozessrechtliche Instrumente, Kompetenzen und internationale Zusammenarbeit sind auch auf das Zusatzprotokoll anwendbar bzw. müssen im Einzelfall auf dieses ausgedehnt werden.

(7) Lehideux und Isorni Urteil v. 23.9.1998 – VII, Abs. 47.

aa. Prozessrechtliche Instrumente

Die Verfahrensvorschriften der Konvention sollen gemeinsame Regelungen hinsichtlich der verfahrensrechtlichen Instrumente in den Unterzeichnerstaaten schaffen. Dies geschieht einerseits durch die Implementierung traditioneller verfahrensrechtlicher Instrumente (z.B. Durchsuchung und Beschlagnahme) in das neue technologische Umfeld. Andererseits werden aber auch entsprechende neue Instrumente (z.B. schnelle Datensicherung) geschaffen, sodass die Effektivität traditioneller Beweissicherungsmaßnahmen in dem dem steten Wandel unterliegenden technologischen Umfeld gewährleistet ist. Mithilfe der benannten Verfahren wird es möglich sein, elektronische Beweismittel zu finden und zu sammeln, und zwar zur Aufklärung sowohl der in der Konvention genannten Straftaten (z.B. Kinderpornografie) als auch anderer Verbrechen (etwa Geldwäsche). Die prozessrechtlichen Bestimmungen haben daher einen weiteren Anwendungsbereich als die Abschnitte, die materielles Recht betreffen.

Die Bestimmungen betreffen nur spezifische strafrechtliche Untersuchungsverfahren und dienen nicht, wie teilweise vermutet wird, der Installation eines umfassenden "Orwellschen" Systems elektronischer Überwachung. Zwar ermöglichen die Bestimmungen die Beschlagnahme und Verwahrung von Daten sowie die Verpflichtung zur Offenlegung bestimmter Daten. Jedoch ist in keiner Weise die Überwachung persönlicher Kommunikation oder Kontakte durch Service-Provider oder Strafverfolgungsbehörden vorgesehen, ohne dass ein offizielles Ermittlungsverfahren eröffnet ist. Im Rahmen der Ausarbeitung der Konvention wurde diskutiert, ob eine Verpflichtung der Service-Provider, routinemäßig Daten zu sammeln und für eine bestimmte Zeit aufzubewahren, in die Konvention mit aufgenommen werden sollte. Dies geschah jedoch mangels eines Konsenses hinsichtlich dieser Frage nicht.

Ferner wurde eine große Anzahl an verfahrensrechtlichen Garantien in die Konvention aufgenommen, die den Missbrauch der Verfahrensinstrumente verhindern soll. Zunächst legt der Text fest, dass die Einführung, Umsetzung und Anwendung der in der Konvention vorgesehenen Verfahren und Kompetenzen grundsätzlich den Bedingungen und rechtsstaatlichen Sicherungen der jeweiligen Rechtsordnungen der Mitgliedstaaten unterliegt. Dabei ist auf einen adäquaten Schutz der Menschenrechte wie sie insbesondere in internationalen Abkommen (speziell in der EMRK und im Internationalen Pakt über bürgerliche und politische Rechte) festgelegt sind, zu achten. Es wird weiterhin bestimmt, dass zukünftige Mitgliedstaaten, bevor sie die vorgesehenen verfahrensrechtlichen Mittel anwenden, sicherstellen sollten, dass diese im angemessenen Verhältnis zu der Art und Weise und den Umständen des zu untersuchenden Verbrechens stehen. Schließlich ist im Text des Protokolls vorgesehen, dass für jeden einzelnen Verfahrensschritt die entsprechenden, im nationalen Recht vorgesehenen Bedingungen und Sicherungselemente angewendet werden müssen. So ist es etwa vom

nationalen Recht abhängig, ob vor einer Untersuchung ein Richter oder Minister eine Genehmigung erteilen muss. Diese in den nationalen Rechtsordnungen bereits existenten Schutzvorschriften sollen in allen Staaten Europas einen ähnlichen Standard beim Schutz der Menschenrechte gewährleisten.

Die Konvention befasst sich mit den folgenden prozessrechtlichen Instrumenten:

- Beschleunigte Sicherung gespeicherter Computerdaten
- Beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten
- Herausgabeanordnung
- Durchsuchung und Beschlagnahme gespeicherter Computerdaten
- Erhebung von Verbindungsdaten.
- Abfangen von Inhaltsdaten

bb. Internationale Kooperation

Auch die Vorschriften der Cybercrime-Konvention hinsichtlich der internationalen Kooperation sind bei der Anwendung der Regelungen im Zusatzprotokoll zu berücksichtigen. Sie bilden in den Augen Vieler den wichtigsten Teil der Konvention, da sie eine schnelle und effektive Kooperation, wie sie für Ermittlungen von Computerstraftaten notwendig ist, ermöglichen. Aufgrund des steten Wandels der elektronischen Beweismittel ist es außerordentlich wichtig, dass Strafverfolgungsbehörden dazu in der Lage sind, Ermittlungen für andere Staaten durchzuführen und die Ermittlungsergebnisse mit großer Schnelligkeit an sie weiterzuleiten. Zusätzlich zu den traditionellen Formen der internationalen Kooperation (gegenseitige Rechtshilfe und Auslieferung) sieht die Konvention vor, dass die Mitgliedstaaten die in den vorangegangenen Bestimmungen festgelegten verfahrensrechtlichen Instrumente (etwa die Beschlagnahme oder die Sicherstellung von Daten für einen anderen Mitgliedsstaat) als neue Formen der gegenseitigen Hilfe anerkennen und anwenden sollen. Die Konvention macht deutlich, dass internationale Kooperation zwischen den Vertragsstaaten „in weitest möglichem Umfang" zu erfolgen hat. Der generelle Umfang der Kooperationspflicht leitet sich aus den im Vertrag definierten prozessrechtlichen Instrumenten ab: Kooperation muss daher in Bezug auf alle im Vertrag festgelegten und sich auf Computersysteme und Daten beziehenden Straftaten sowie bei der Sammlung von Beweisen in elektronischer Form zur Aufklärung einer Straftat gewährt werden.

Die Cybercrime-Konvention schafft außerdem die rechtliche Basis für ein spezielles Kooperationsnetzwerk für Computerstraftaten. Hierbei handelt es sich um ein permanentes Netzwerk zwischen nationalen Kontaktstellen (sog. 24/7 Netzwerk). Wie schon diskutiert, erfordert die effektive Bekämpfung der mittels Computersystemen begangenen Verbrechen und die Sammlung elektronischer Beweismittel ein sehr schnelles

Vorgehen. Per Mausklick können in einem Teil der Welt Handlungen vorgenommen werden, die in Sekundenbruchteilen Konsequenzen in einem anderen Teil der Welt haben. Aus diesem Grund bedürfen die herkömmlichen polizeilichen Kooperationsverfahren und die gegenseitigen Rechtshilfeeinrichtungen zusätzlicher Kooperationskanäle. Nur so können die Herausforderungen des Computerzeitalters effektiv bewältigt werden. Der in der Konvention etablierte Kooperationskanal basiert auf Erfahrungen mit einem bereits funktionierenden Netzwerk, das im Rahmen der G8-Staatengruppe geschaffen wurde. Gemäß der Konvention haben alle Mitgliedstaaten die Verpflichtung, eine nationale Kontaktstelle, welche rund um die Uhr und sieben Tage in der Woche verfügbar ist, einzurichten, um sofortige Hilfe bei Verfahren und Untersuchungen im Rahmen der Konvention sicherzustellen. Die Schaffung dieses Netzwerkes zählt zu den wichtigsten Mitteln, die die Konvention bereitstellt, um eine effektive Strafverfolgung durch die Mitgliedstaaten zu gewährleisten. Das Netzwerk soll die traditionellen Kanäle der Kooperation jedoch nicht ersetzen, sondern sie lediglich ergänzen.

Jede nationale Kontaktstelle muss Möglichkeiten zur Einholung technischer Ratschläge, zur Aufbewahrung von Daten, zur Sammlung von Beweismitteln, zur Erteilung rechtlicher Informationen, zur Suche nach und zum Auffinden von Verdächtigen entweder selbst anbieten oder vermitteln. Die Staaten können eigenständig festlegen, auf welcher Hierarchieebene ihrer Strafverfolgungsbehörden sie die Kontaktstelle ansiedeln. Manche werden sich für eine Ansiedlung bei der zentralen Behörde für Rechtshilfe, andere für eine Angliederung an eine spezielle Polizeieinheit zur Bekämpfung von Computerstraftaten entscheiden. Da die 24/7-Kontaktstellen sowohl technische Hilfe bei der Verfolgung bzw. bei der Vermeidung eines Verbrechens oder eines Angriffs mittels Computersystemen leisten sollen, als auch traditionelle Kooperationsverpflichtungen wie die des Lokalisierens von Verdächtigen zu erfüllen hat, gibt es keine eindeutige Antwort auf die Frage ihrer Organisationsstruktur. Diese dürfte sich mit der Zeit entwickeln.

Eine effektive Kommunikation zwischen den einzelnen Kontaktstellen setzt insbesondere auch eine angemessene technische Ausstattung voraus. Moderne Fax-, Telefon- und Computeranlagen sind beispielsweise von fundamentaler Bedeutung für das Funktionieren des Netzwerkes. Neue Formen der Kommunikationstechnologie und neue analytische Geräte müssen im Zuge der technologischen Fortentwicklung in das Netzwerk integriert werden. Die Konvention verlangt auch, dass das Personal, welches in den nationalen Kontaktstellen tätig wird, ausreichend im Hinblick auf Computerstraftaten und ihre effektive Bekämpfung ausgebildet ist.

Schließlich ist in diesem Zusammenhang erwähnenswert, dass es zum gegenwärtigen Zeitpunkt keine Pläne für tatsächliche internationale Ermittlungen, wie etwa grenzüberschreitende Durchsuchungen von Computersystemen, gibt. Die verhandelnden Staaten konnten sich bislang nicht auf solche Maßnahmen einigen.

cc. Zuständigkeit

Ein wichtiger Aspekt ist zudem die Frage der Zuständigkeit im Hinblick auf Straftaten, die mittels Informationstechnologie begangen werden. Dies betrifft z.B. die Bestimmung des Ortes, an dem das Verbrechen begangen wurde (locus delicti) und die Festlegung des dem entsprechend anzuwendenden Rechts. Von Bedeutung ist auch das Problem des „ne bis in idem", und zwar für den Fall, dass multiple Zuständigkeiten begründet sind. In diesem Zusammenhang muss auch der Frage nachgegangen werden, wie positive Kompetenzkonflikte zu lösen und negative Kompetenzkonflikte zu verhindern sind. Die Bestimmung legt eine Reihe von Kriterien fest, nach denen die Mitgliedstaaten verpflichtet sind, ihre Zuständigkeit für die in den Art. 2-11 der Konvention aufgeführten Straftaten festzustellen.

Um nationale Straftaten zu verhindern und zu bestrafen, müssen die Mitgliedstaaten die Möglichkeit haben, die in der Konvention genannten Verbrechen, die innerhalb ihrer Territorien begangen werden, zu untersuchen und zu verfolgen. Art. 22 Abs. 1 lit. a, der auf dem Territorialitätsprinzip basiert, verpflichtet die Mitgliedstaaten sogar ausdrücklich hierzu. Die Mehrheit der Staaten, die an den Verhandlungen teilgenommen haben, erkennt die Zuständigkeit für exterritorial begangene Verbrechen in bestimmten Fällen an. Dies ist z.B. dann der Fall, wenn das Verbrechen von einem ihrer Staatsangehörigen oder an Bord eines bei ihnen registrierten Schiffs oder Flugzeugs begangen wird. Art. 22 Abs. 1 lit. b, c und d der Konvention verpflichtet die Mitgliedstaaten in diesen Fällen dazu, ihre Zuständigkeit festzustellen. Dabei besteht jedoch für die Staaten, deren nationale Rechtsordnungen die Anwendung der Prinzipien der Exterritorialität nicht zulassen, die Möglichkeit, teilweise oder vollständige Vorbehalte erklären zu lassen. Die Staaten werden zudem verpflichtet, ihre Maßnahmen in bestimmten Fällen miteinander abzustimmen. Dies gilt etwa dann, wenn die Opfer eines Verbrechens sich in verschiedenen Staaten befinden. In diesen Fällen ist die Koordination von Ermittlungen und Strafverfolgung wichtig, um die Effektivität der Maßnahmen im Kampf gegen Cyber-Verbrechen zu maximieren.

3.2.4 Zusammenfassung

Fest steht, dass globale Bedrohungen und Herausforderungen auch nach globalen Antworten verlangen. Aus diesem Grund setzt sich der Europarat für den Kampf generell gegen Cyber-Verbrechen und speziell gegen Rassismus und Fremdenfeindlichkeit im Internet ein. Auch einige nicht-europäische Staaten werden hierbei in den Verhandlungsprozess miteinbezogen. Ihnen wird die Möglichkeit geboten, den ausgehandelten Verträgen beizutreten. So haben bereits die USA, Mexiko, Japan, Kanada und Südafrika die Cybercrime-Konvention unterzeichnet und werden wahrscheinlich auch dem Zusatzprotokoll beitreten.

Das World Wide Web ist eine neue Welt. Eine Welt, in der Individuen aufeinander treffen und in der und durch die Verbrechen begangen werden. Selbstregulierung allein vermag hier leider nicht weiterzuhelfen. Der Europarat, der seit mehr als 50 Jahren die individuellen Menschenrechte in der realen Welt durch seinen Europäischen Gerichtshof für Menschenrechte schützt, will dieselben Rechte mutatis mutandi auch mit bestimmten Sicherungen in der virtuellen Welt bewahren. Mittel hierzu ist das Zusatzprotokoll. Es bestimmt, inwieweit die Verbreitung von rassistischen und fremdenfeindlichen Äußerungen und Meinungen die Rechte anderer verletzt und stellt dieses Verhalten entsprechend unter Strafe. Schließlich ist eine engere Kooperation zwischen Strafverfolgungsbehörden und Internet Service-Providern in einem international vereinbarten rechtlichen Rahmen notwendig. Dieser rechtliche Rahmen wird durch das neue Zusatzprotokoll des Europarates ebenfalls gewährt.

3.3 Ko-Regulierung von Internet-Inhalten in Australien

Dr. Thomas Hart (in Zusammenarbeit mit Andree Wright, Director Industry Performance and Review, Australian Broadcasting Authority, ABA, Melbourne)

3.3.1 Einleitung

Australien führte am 1.1.2000 ein Schema zur Regulierung von Internet-Inhalten ein. Das Regulierungsprogramm ist ein dezidiert ko-regulatorisches: Es umfasst eine Aufgabenteilung zwischen allen beteiligten Akteuren, nimmt Regierung, Industrie und die Gesellschaft insgesamt in die Verantwortung, insbesondere den Anforderungen des Online-Jugendschutzes im 21. Jahrhundert gerecht zu werden. Die Hauptbestandteile dieses Regulierungs-Programms sind eine Beschwerde-Hotline, Verhaltenskodexe für die Industrie sowie ein Programm zur Aufklärung und Erziehung der Bevölkerung hinsichtlich potenzieller Gefahren des Internet bzw. Lösungsansätzen und Hilfsmitteln. Zuständige Regulierungsinstitution ist die Australian Broadcasting Authority (ABA).

3.3.2 Reichweite des Programms

Australien versucht mit dem Ko-Regulierungsansatz, den Bedenken der Bevölkerung hinsichtlich Gefährdungspotenzialen durch das Internet Rechnung zu tragen, dies aber auf eine Weise zu tun, die der Verbreitung und Nutzung des Internet zuträglich ist. Um dies zu erreichen, wurde ein umfangreicher Maßnahmenkatalog etabliert, darunter:

- Definition bestimmter Typen von Internet-Inhalten als „verboten" (prohibited content) oder „potenziell verboten" (potential prohibited content).
- Gewährleistung der Entwicklung industrieller Verhaltenskodexe (industry codes of practice) oder ABA-Standards für Internet Service-Provider (ISPs) und Internet Content Hosts (ICHs).
- Schaffung einer speziellen Institution (NetAlert)[8], die als Berater hinsichtlich der Entwicklung von Verhaltenskodexen konsultiert werden kann.
- Einrichten eines Mechanismus, der es der Bevölkerung ermöglicht, sich bei der ABA über „verbotene" Inhalte (oder die als solche wahrgenommen werden) zu beschweren.
- Verpflichtung der ISPs und ICHs, bestimmte Maßnahmen in Bezug auf solche Inhalte zu ergreifen, die als „verboten" klassifiziert wurden.
- Etablierung des Rechts für die ABA, Beschwerden nachzugehen und, sofern angemessen, die ISPs oder ICHs anzuweisen, bestimmte Maßnahmen gegen diese Inhalte zu ergreifen.

(8) Die Institution NetAlert wurde am 6.12.1999 gegründet.

Wichtig ist die Feststellung, dass der Broadcasting Services Act, in dem dieses Ko-Regulierungsschema festgeschrieben wurde, zwar einen rechtlichen Rahmen und ein „Sicherheitsnetz" für die Regulierung darstellt, dass innerhalb dieses Konzeptes aber den von der Industrie selbst entwickelten Maßnahmen zur Handhabung illegaler oder potenziell schädlicher Inhalte Vorrang eingeräumt wird.

3.3.3 „Verbotene Inhalte" (Prohibited content)

Als Grundsatz des Ko-Regulierungssystems gilt die Feststellung, dass Inhalte, die offline illegal sind, auch online illegal sein sollen. Die Regierung kam zu der Auffassung, dass solche Inhalte als unzulässig zu gelten haben, die, würden sie in anderer Form veröffentlicht, illegal wären oder mit eingeschränkten Vertriebsmöglichkeiten belegt würden. Deshalb wurde der Anwendungsbereich bestimmter Elemente des bereits bestehenden Klassifikationssystems für Film, Fernsehen und andere Medien auch auf das Internet ausgeweitet. Die Klassifikationsstufen des Office for Film and Literature Classification (OFLC) dienen damit auch als Referenzpunkt für die Bewertung von Internet-Inhalten.

Zu den „verbotenen" Inhalten gehören somit[9]:

- Inhalte, die die Klassifikation RC oder X erhalten. Dazu gehören:
    - Material, das detaillierte Anleitungen zu kriminellen Handlungen, Gewalt oder Drogengebrauch enthält;
    - Kinderpornographie;
    - Sodomie;
    - übermäßig gewalttätige oder sexuell gewalttätige Inhalte;
    - Darstellungen tatsächlicher sexueller Handlungen.

- Inhalte, die in Australien gehostet werden, als Kategorie R klassifiziert und nicht mit einem Zugangskontrollsystem ausgestattet sind[10]. Solche R-Inhalte gelten als nicht geeignet für Kinder und Jugendliche und umfassen:
    - Darstellung starker Gewalttätigkeit oder sexueller Gewalt;
    - Darstellung angedeuteter oder simulierter sexueller Betätigung;
    - Inhalte, die sich um Sachverhalte drehen oder Darstellungen beinhalten, die eine erwachsene Perspektive erfordern.

(9) Genauere Informationen zu den OFLC Guidelines For Classification of Films and Videotapes sind abrufbar unter: http://www.oflc.gov.au/content.html?p:79.
(10) Die Kriterien für solche Zugangskontrollsysteme sind festgelegt in: Restricted Access Systems Declaration 1999 (No.1) v. 3.12.1999.

Inhalte, die von der OFLC nicht klassifiziert wurden, bei denen aber wahrscheinlich ist, dass sie im Falle einer Klassifizierung als „verboten" eingestuft würden, gelten als „potenziell verboten" (potential prohibited). In den meisten Fällen werden solche Inhalte wie „verbotene" Inhalte behandelt.

3.3.4 Verhaltenskodexe der Industrie

a. Entwicklung und Registrierung der Kodexe

Nach intensiver internationaler Recherche und Analyse (in Deutschland etwa im Zusammenhang mit dem Projekt „Selbstregulierung" der Bertelsmann Stiftung) wurde ein Katalog von Kriterien entwickelt, denen ein Verhaltenskodex genügen solle[11].

- Entwicklung des Kodexes durch den oder die jeweils relevanten Industrieverband bzw. -verbände.
- Freiwilligkeit bei der Unterzeichnung des Kodexes, gestützt durch Regulierungsmechanismen, die Anreize zur Zeichnung des Kodexes setzen.
- Beteiligung der relevanten Regulierungsinstitutionen bei der Entwicklung des Kodexes.
- Beteiligung der Nutzer und der Öffentlichkeit bei der Entwicklung des Kodexes sowie bei der regelmäßigen Evaluation der Umsetzung.
- Die Kodexe sollen Vorgehensweisen für den Umgang mit illegalen Inhalten enthalten. Außerdem soll er Maßnahmen umfassen, mit denen der Öffentlichkeit Informationen und Hilfsmittel zum Umgang mit möglicherweise schädlichen Inhalten angeboten werden können.

Die drei von der Internet Industry Association (IIA) entwickelten Kodexe widmen sich den in „clause 60" des Gesetzes dargelegten Aspekten: Die Content Codes 1 und 2 decken die Aktivitäten der ISPs ab, während Code 3 sich mit der Verantwortung der ICHs befasst[12]. Obwohl die Kodexe von der IIA entwickelt wurden, deren Mitglieder eine Mehrheit der australischen Internet-Nutzer (etwa 80 Prozent) bedienen, sind sie für alle Akteure in diesem Marktsegment gültig. Die ABA hat das Recht, jeden Marktakteur ggf. anzuweisen, sich nach den Kodexen zu richten.

Nach einem von der IIA durchgeführten öffentlichen Konsultationsprozess (in den die Öffentlichkeit, Industrie und die neu geschaffene Beratungsinstitution NetAlert einbezogen waren), wurden die ursprünglichen IIA-Codes im Dezember 1999, die Nach-

(11) Machill/Rewer, Internet Hotlines – Evaluation and Self-regulation of Internet Content, 2001; Price/Verhulst, Codes of Conduct and Other Self-regulatory Documents, Studie vorgestellt i.R.d. Workshops der Bertelsmann Stiftung: "Self-regulation of the Internet" v. 30.6.2000.
(12) Die aktuellen Kodexe sind abrufbar unter: http://www.iia.net.au/contentcode.html.

folge-Codes am 9.5.2002 bei der ABA registriert. In der Summe enthalten die Kodexe eine Palette an Möglichkeiten, End-Nutzern bei der Kontrolle des Zugangs zu Internet-Inhalten zu unterstützen. Außerdem sind spezifische Vorgaben für den Umgang mit verbotenen und außerhalb Australiens gehosteten Inhalten enthalten.

Content Code 2 enthält ein „designated notification scheme", eine Vorgehensweise zur Meldung potenziell oder tatsächlich verbotener Inhalte, die außerhalb Australiens angeboten werden. Die ISPs müssen demnach ihren Nutzern eines der Filterprodukte oder der Dienste anbieten, die „scheduled", also von der ABA als geeignet bewertet und als solche registriert worden sind. Die ISPs dürfen dafür zwar Gebühren erheben, diese Gebühren dürfen jedoch nicht die Kosten übersteigen, die den ISPs für die Beschaffung, das Angebot und die Unterstützung des Filters entstehen. Nach diesem „notification scheme" teilt die ABA die Details der verbotenen und potenziell verbotenen Inhalte den Herstellern und Anbietern der registrierten Internet-Filter mit. Diese haben sich verpflichtet, ihre Produkte nach Eingang einer solchen Mitteilung zu aktualisieren. Sie müssen nach den Vorgaben des „Codes" die ABA auch darüber informieren, wie sie nach dem Eingang einer ABA-Meldung mit dieser umgehen und wie sie sie umsetzen.

Wichtig ist, dass die Filter in diesem Schema eine andere Rolle spielen als sie es sonst vielleicht tun. Während sich die ABA durchaus darüber im Klaren ist, dass gegenwärtige Filtertechnologien für sich genommen keinen ausreichenden Schutz vor potenziell schädlichen Internet-Inhalten gewährleisten können, stellen sie doch nach Ansicht des Regulierers in Kombination mit einer angemessenen Aufsicht durch die Eltern oder die Etablierung von Nutzungsregeln in den Familien effektive ergänzende Hilfsmittel dar, um den Zugriff von Kindern auf Internet-Inhalte besser zu steuern.

b. Einhaltung der Kodexe

Die Einhaltung der Kodexe wird durch die ABA überwacht. Sie ist auch ermächtigt, einen ISP oder ICH ggf. zur Einhaltung anzuweisen. Verstöße gegen den Kodex können einen Verstoß nach dem Broadcasting Act darstellen und entsprechend sanktioniert werden.

Nach Angaben der IIA hat sich die Mehrheit ihrer Mitglieder bislang vollständig Kodex-konform verhalten. Die ABA hat bislang keine Beschwerden über Nicht-Einhaltung erhalten. Es gab lediglich kleinere Unstimmigkeiten im Zusammenhang mit kleineren ISPs, die aber nach Angaben der ABA unmittelbar zur vollständigen Zufriedenheit der ABA geregelt werden konnten.

3.3.5 Beschwerden

a. ABA Hotline

Die Untersuchung von Internet-Inhalten ist im australischen Regulierungsmodell in erster Linie beschwerdebasiert. Die Regierung beschloss, dass der ISP idealerweise nicht der erste Ansprechpartner für Beschwerden über Internet-Inhalte sein sollte. Deshalb - und um die Bearbeitung von Beschwerden möglichst effektiv und rasch zu gewährleisten - wurde beschlossen, dass die ABA selbst als Beschwerdestelle fungieren sollte. Ein bedeutender Aspekt für das Funktionieren des Systems ist, dass den ISPs und ICHs Anreize gesetzt wurden, sich dem Code anzuschließen. Der möglicherweise wichtigste Anreiz ist, dass ISPs und ICHs für Inhalte, auf die durch ihre Netze oder Dienste zugegriffen werden kann oder die von ihnen gehostet werden, aus der Verantwortung genommen wurden. Sie müssen die Inhalte nicht systematisch überwachen und prüfen, und sind nicht für sie verantwortlich, sofern sie sich an die Bestimmungen des Kodex halten. Das Gesetz sieht für eine Beschwerde zwingend die Schriftform vor. Um das Abgeben und Bearbeiten von Beschwerden möglichst einfach zu machen, bietet die ABA auf ihrer Website ein Online-Beschwerdeformular an[13]. Damit kann der Nutzer, sobald er problematischen Inhalten begegnet, jederzeit seine Beschwerde abgeben. Durch die Gestaltung des Formulars wird zudem gewährleistet, dass alle Beschwerden sämtliche für die weitere Untersuchung notwendigen Informationen beinhalten.

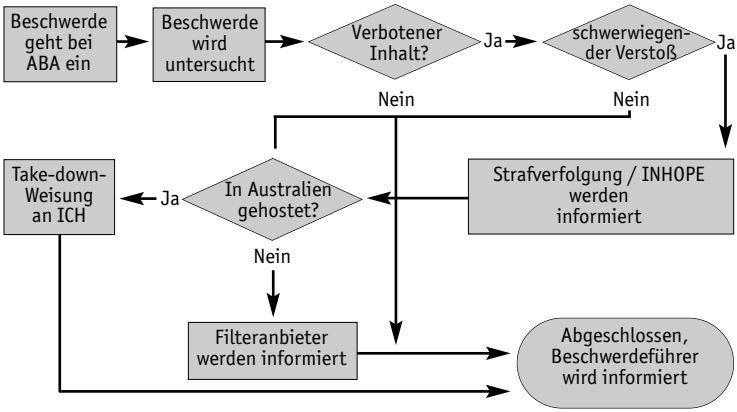


Abb. 1: Das ABA-Beschwerdesystem

(13) Abrufbar unter: http://www.aba.gov.au/internet/.

b. Untersuchung von Beschwerden

Die ABA untersucht alle gültigen Beschwerden über verbotene oder potenziell verbotene Inhalte. Teil der Untersuchung kann es dabei sein, dass die ABA die OFLC bittet, den fraglichen Inhalt zu klassifizieren. Wird der Inhalt in Australien gehostet und als verboten (oder wahrscheinlich verboten) eingestuft, weist die ABA den ICH an, den Inhalt vom Netz zu nehmen. Ist der Inhalt nicht klassifiziert, so erhält der ICH von der ABA eine Interims-Take-Down-Weisung. Die OFLC wird dann gebeten, den Inhalt zu klassifizieren. Anschließend wird dann ggf. eine endgültige Take-Down-Weisung ausgesprochen. Ist der Inhalt (tatsächlich oder wahrscheinlich) verboten, der Host jedoch nicht in Australien ansässig, so informiert die ABA die Anbieter der dem Verhaltenskodex angeschlossenen Filter. Wird der Inhalt zudem als „serious" eingeschätzt (etwa illegales Material wie Kinderpornographie), so verweist die ABA den Fall außerdem an die zuständige Strafverfolgungsbehörde oder eine andere zuständige Hotline.

c. Verstöße und Durchsetzung

Das Gesetz sieht vor, dass ein ICH auf eine Meldung der ABA bis 18 Uhr des auf die Meldung folgenden Arbeitstages reagiert haben muss. Um dies durchzusetzen, stehen der ABA eine Reihe von Sanktionsmöglichkeiten zur Verfügung, darunter das Einholen einer Verfügung des Federal Court sowie die Möglichkeit der Strafverfolgung. Bislang haben jedoch alle ICHs fristgemäß und korrekt auf Meldungen der ABA reagiert. Die Sanktionsinstrumente der ABA sind insofern bisher noch nicht zur Anwendung gekommen.

3.3.6 Erfahrungen aus der Praxis

Die ABA hat zwischen Januar 2000 und Juni 2002 etwa 1300 Beschwerden über Internet-Inhalte erhalten. Ungefähr 85 Prozent der Beschwerden bezogen sich dabei auf WWW-Inhalte, der Rest (ca. 14 Prozent) hauptsächlich auf Usenet-Inhalte.

Gegenstand	**Zeitraum**			**Gesamt**
	2000 (Jan. - Dez.)	2001 (Jan. - Dez.)	2002 (Jan. - Juni)	
Eingegangene Beschwerden	491	446	383	1320
Abgeschlossene Untersuchungen	381	384	289	1054
Abgebrochene Untersuchungen	93	75	96	264
Inhalte, gegen die Maßnahmen ergriffen wurden (gehostet in Australien)	129	104	20	253
Inhalte, gegen die Maßnahmen ergriffen wurden (gehostet im Ausland)	230	299	245	774
Weiter verwiesen an State oder Territory Police Force	89	43	3	135
Weiter verwiesen an Bundespolizei oder ausländische Hotline	156	197	126	479

Abb. 2: Eingegangene Beschwerden und Maßnahmen (1. Januar 2000 bis 30. Juni 2002)

Als Ergebnis der Beschwerden und der darauf folgenden ABA-Untersuchungen wurden im Zusammenhang mit 1027 Inhalten Maßnahmen eingeleitet. 78 Prozent davon waren oder wären der Kategorie Refused Classification (RC) zuzuordnen. Etwa ein Viertel der Inhalte, gegen die Maßnahmen eingeleitet wurden, waren in Australien gehostet.

Klassifikation und Beschreibung des Inhalts (Original-Bezeichnungen des OFLC-Klassifikations-Schemas)	gehostet in Australien („take-down"-Anweisung)	gehostet im Ausland (an die Filter-Anbieter gemeldet)	Gesamt
R – Adult themes	8	N/A	8
R – Implied/simulated sexual activity	22	N/A	22
R – Sexualised nudity	8	N/A	8
X – Actual sexual activity	30	163	193
RC – Depiction of bestiality	18	26	44
RC – Instruction in crime	4	5	9
RC – Child pornography	100	410	510
RC – Detailed violence or cruelty	0	11	11
RC – Offensive/abhorrent fantasies	23	88	111
RC – Offensive/abhorrent sexual activity	13	21	34
RC – Pedophile activity	24	31	55
RC – Sexual violence	3	19	22
Gesamt	**253**	**774**	**1027**

Abb. 3: Maßnahmen in Zusammenhang mit verbotenen und potenziell verbotenen Internet-Inhalten (1. Januar 2000 bis 30. Juni 2002)

3.3.7 Kooperation mit der Strafverfolgung und anderen Hotlines

Internet Hotlines können eine wichtige Rolle einnehmen, wenn es darum geht, schnell und effektiv auf illegales Material wie Kinderpornographie zu reagieren. Das gilt umso mehr, wenn sie in ein internationales Netzwerk eingebunden sind und eng mit den Strafverfolgern zusammen arbeiten. Das schnelle Untersuchen und Beurteilen solcher Inhalte ist essentiell dafür, seine Verfügbarkeit zu unterbinden und damit auch z.B. des Kindesmissbrauchs, der mit der Herstellung dieses Materials einhergeht, Herr zu werden.

Bei über der Hälfte aller Inhalte, gegen die die ABA vorgegangen ist, handelte es sich um Kinderpornographie. Bis zum 30.6.2002 hatte die ABA 470 solcher im Ausland gehosteten Fälle der australischen Bundespolizei und / oder der Hotline des jeweiligen Landes zugeführt. In 135 Fällen war das Material in Australien gehostet und wurde an die zuständige Polizeibehörde in den Regionen gemeldet.

Kommt die ABA zu der Auffassung, dass ein bestimmter Inhalt ernsthaft problematisch ist („of a sufficiently serious nature") – wie etwa im Fall von Kinderpornographie -, so erfolgt eine Meldung nicht nur an die australische Bundespolizei, sondern außerdem auch an ein Mitglied von INHOPE, den Verband europäischer Internet-Hotline-Betreiber (Internet Hotline Providers in Europe Association)[14].

3.3.8 Aufklärung und Erziehung

International ist es mittlerweile anerkannt, dass das Schaffen von Aufmerksamkeit und die Erziehung zu bewussterem Verhalten - man könnte sagen, die Vermittlung einer breit verstandenen Medienkompetenz - eine zentrale Komponente von Strategien zum Umgang mit problematischen Internet-Inhalten sein müssen. Dies vor allem, da durch die Größe und Vielfalt der Internet-Inhalte und ihrer globalen Herkunft und Verbreitung die Effektivität traditioneller Regulierung von Inhalten zurückgeht[15].

Dies ist auch im Broadcasting Services Act zentrales Element: ISPs und ICHs verpflichten sich mit der Unterzeichnung der Verhaltenskodexe dazu, ihre Nutzer mit entsprechenden Informationen und Instrumenten (z.B. Filtern, Sicherheitshinweisen und -informationen oder auch Verweisen auf externe Quellen) zu versorgen. Industrie und Regierung teilen sich dabei die Verantwortung, nicht nur auf Seiten des Internet-Angebotes, sondern auch auf Seiten der Nutzer eine Kultur des Verantwortungs-

(14) Genauere Informationen zu INHOPE finden sich unter: www.inhope.org.

(15) Vgl. Hamm/Hart (Hrsg.), Kommunikationsordnung 2010, Märkte und Regulierung im interaktiven Zeitalter, Gütersloh 2001, abrufbar unter: www.ko2010.de; Waltermann/Machill (Hrsg.), Verantwortung im Internet - Selbstregulierung und Jugendschutz, Gütersloh 2000.

bewusstseins zu fördern. So vergibt die IIA etwa ein Gütesiegel „Family Friendly ISPs“, um den Nutzern die Orientierung zu erleichtern und gleichzeitig für die ISPs einen Anreiz zu setzen[16]. Die ABA führt regelmäßig Untersuchungen zu Nutzerverhalten und Nutzerbedürfnissen durch und gibt Informationsbroschüren etwa zum Vermeiden von und Umgang mit Spam-Mails oder zur Filter-Nutzung heraus und arbeitet dazu auch mit den Erziehungsministerien und den Schulen zusammen.

3.3.9 Abschlussbemerkung

Das australische Ko-Regulierungsprogramm stellt weniger „Regulierung“ im hergebrachten Sinne, sondern vielmehr einen Versuch dar, mit Hilfe eines abgestimmten Maßnahmenbündels den Online-Kinder- und Jugendschutz auf die Erfordernisse des Internet-Zeitalters anzupassen. Die Maßnahmen reichen von legislativen Einzelregelungen bis hin zur breit verstandenen Aufgabe, den Nutzern ein besseres Wissen über mögliche Gefahren des Internet zu vermitteln und sie zu ermutigen und zu befähigen, selbst Initiative zu ergreifen. Das Modell kann insofern vorbildlich auch für die Ausgestaltung des europäischen und deutschen Vorgehens sein. Wenngleich es noch immer als Best-Practice-Beispiel recht einsam auf weiter Flur steht, zeigt das große internationale Interesse daran doch, dass hier eine Möglichkeit geschaffen wurde, den Spagat zwischen Regulierungserfordernissen und den neuen Bedingungen eines internationalen (oder nicht-nationalen) Mediums gerecht zu werden.

(16) Abrufbar unter: http://www.iia.net.au/familyfriendly.html

4. Die juristische Diskussion um die Düsseldorfer Sperrverfügung

4.1 Ordnungsrechtliches Vorgehen gegen Rechtsextremismus im Internet

Jürgen Schütte

Als erste deutsche Aufsichtsbehörde hat die Bezirksregierung Düsseldorf Sperrverfügungen gegen Access-Provider (Zugangsvermittler) wegen zweier rechtsextremistischer, strafbarer Internet-Inhalte angeordnet. Von 76 angeschriebenen Providern haben diese 60 befolgt. Gegen die 16 übrigen klagenden Provider wurde kürzlich die sofortige Vollziehung angeordnet, da diese Provider ansonsten bis zum rechtskräftigen Abschluss der Gerichtsverfahren die Inhalte hätten weiterverbreiten können. Ich möchte Ihnen an dieser Stelle einige Gründe und Hintergründe für das Vorgehen der Bezirksregierung Düsseldorf als für das Land Nordrhein-Westfalen zuständige Aufsichtsbehörde nach dem Mediendienste-Staatsvertrag und dem Teledienstgesetz darlegen.

4.1.1 Ausgangspunkt

Seit Mitte der 90er Jahre beobachten deutsche Sicherheitsbehörden ein ständiges Anwachsen rechtsrextremistischer Internet-Seiten. Waren im Jahre 1996 nur ca. 80 rechtsextremistische Internetseiten aufzufinden, so war bis zum Jahr 2000 ein Anwachsen auf 800 rechtsextremistische Seiten zu verzeichnen. Im Jahre 2001 erhöhte sich diese Zahl auf 1.300. Anfang 2002 stellte das Bundesinnenministerium einen Rückgang auf 920 rechtsextremistische Seiten fest. Im zweiten Halbjahr 2002 wurde jedoch wiederum ein Zuwachs auf 1.300 rechtsextremistische Internetseiten verzeichnet.

Bei diesen Seiten handelt es sich nicht nur um politisch missliebige Angebote aus dem rechten Spektrum. Einer Einschätzung des Bundesamtes für Verfassungsschutz zufolge enthalten 15 % der rechtsextremistischen Seiten strafbare Inhalte: dies sind ca. 200 Homepages. Mit jeder Darbietung dieser Seiten auf deutschen Endgeräten werden ständig, dauernd und immer wiederholt deutsche Strafgesetze verletzt.

Als Straftatbestände sind hier insbesondere die Volksverhetzung (§ 130 StGB) – zum Teil mit dem qualifizierenden Tatbestand des Verbreitens der Auschwitzlüge – das Verwenden von Kennzeichen verfassungswidriger Organisationen (§ 86 a StGB), Bedrohung (§ 240 StGB), usw. zu nennen. Konkret geht es inhaltlich bei diesen Angeboten z. B. um das Anbieten von nachgebildeten Zyklon-B-Kanistern oder „Seife“ der Marke Auschwitz, das Freigeben zum Abschuss von Juden und Ausländern in

Computerspielen, das Werben für eine völkische Weltordnung, Geschichtsrevisionismus, das Anbieten von volksverhetzenden Liedern und Videos.

Fast alle rechtsextremistischen Inhalte, die für Deutschland relevant sind, werden über ausländische (zumeist amerikanische) Host-Service-Provider verbreitet. Das BKA meint, dass es sich dabei um mehr als 90 % der rechtsextremistischen Inhalte handelt, der Generalstaatsanwalt NRW geht davon aus, dass „nur einige Dumme noch über deutsche Service-Provider" ihre Inhalte verbreiten. Offensichtliche Absicht dieser Verbreitungsform ist es, sich dem deutschen Recht, insbesondere der Strafverfolgung, zu entziehen. Hintergrund ist nämlich, dass das deutsche Strafrecht hier leerläuft, weil die Täter (Content-Provider), soweit sie aus Deutschland agieren, unerkannt bleiben und die Service-Provider durch die amerikanische Verfassung (First Amendment) geschützt werden. Auch das Ordnungsrecht kann im Hinblick auf die Content- und Service-Provider hier ebenfalls nicht zur Störungsbeseitigung beitragen. Wer also wirksam und verbindlich etwas gegen den illegalen Rechtsextremismus im Internet in Deutschland unternehmen will, muss etwas gegen die zu 90 % im Ausland eingestellten strafbaren Inhalte unternehmen.

4.1.2 Der rechtliche Rahmen

Bei strafbaren, unzulässigen Internet-Inhalten sieht der Mediendienste-Staatsvertrag – dies ist keine Erfindung der Bezirksregierung Düsseldorf – ausdrücklich die Inanspruchnahme der Access-Provider vor, wenn die Content- oder Service-Provider nicht greifbar sind, §§ 12 Abs. 1, 22 Abs. 3 Mediendienste-Staatsvertrag (MDStV). Diese Voraussetzungen liegen hier u. U. vor. Wenn das Vorgehen der Bezirksregierung Düsseldorf grundsätzlich kritisiert wird, dann wäre die Kritik eigentlich gegen die Landesgesetzgeber, die den MDStV gerade wieder im Juli dieses Jahres neu gefasst haben, zu richten. Auch die Neufassung sieht ausdrücklich die Haftung der Access-Provider vor. Dass die Access-Provider-Haftung Sinn macht und eben nicht abgeschafft wurde, liegt daran, dass andernfalls aufgrund einer Haftungslücke das Internet als rechtsfreier Raum zu bezeichnen wäre. Dass strafbare Inhalte über das Ausland in das Internet eingestellt werden, ist nämlich nicht nur ein Problem des Rechtsextremismus. Generell wird jeder Internet-Straftäter, der als Inhalte-Anbieter seinen Content anonym einstellen kann, seine Inhalte dort verbreiten, wo dies nicht strafbar ist. Er nutzt also das globale Medium Internet, das keine Nationalstaaten kennt, um das Recht einzelner nationaler Rechtsordnungen zu verletzten. Dann können die einzelnen Nationalstaaten ihre Rechtssouveränität nur dadurch gewährleisten, indem sie ihren Bürgern den Zugang zu diesen Inhalten verwehren. Täten die Nationalstaaten dies nicht oder würden sie nicht wenigstens diese Möglichkeit vorsehen, würde der einzelne Nationalstaat – für das Internet – faktisch seine Rechtssouveränität preisgeben, bzw. sich auf das Niveau der Rechtsordnung mit den niedrigsten Anforderungen begeben.

4.1.3 Aktivitäten der Bezirksregierung Düsseldorf

Ausgehend von diesem Befund hat die Bezirksregierung Düsseldorf zunächst keine Sperrverfügung erlassen, sondern – im Gegenteil – alles andere versucht, um die Provider zur nachhaltigen Verbannung strafbarer rechtsextremistischer Internet-Inhalte, also zu einer selbstregulierenden Situation, zu bewegen.

Im ersten Halbjahr 1998 veranstaltete die Bezirksregierung Düsseldorf einen Workshop zur Medienaufsicht, sie stellte die Homepage „Freiheit schützen – Missbrauch verhindern" vor. In einer Presseerklärung wurde an die Verantwortlichkeit der Provider erinnert. Im ersten Halbjahr 1999 gab es zu diesem Workshop eine Folgeveranstaltung. Im zweiten Halbjahr 1999 wurden alle Provider in Nordrhein-Westfalen von der Bezirksregierung eingeladen. Im Rahmen dieser Veranstaltung hat die Bezirksregierung verdeutlicht, dass die Gesellschaft erwartet, dass Vorkehrungen gegen den Missbrauch in den neuen Medien getroffen werden, ansonsten bestehe ein Handlungsgebot der Exekutive. Folgen hatte dieser Aufruf nicht. Im August 2000 wurden rund 190 Provider in NRW von der Bezirksregierung angeschrieben, um zu erreichen, dass rechtsextremistische Inhalte nicht länger über deutsche Provider im Internet frei zugänglich gemacht werden. In Gesprächen haben sich die Unternehmen und Firmen dazu bereit erklärt, ihre Server auf rechtsextremistische Inhalte hin zu überprüfen und sie aus dem Netz zu nehmen (siehe auch die Presseerklärung vom 25.08.2002). Tatsächlich geschah aber nichts. Auf der Fachtagung „Rechtsextremismus im Internet" am 28.05.2001, zu der die Bezirksregierung Düsseldorf insbesondere auch die nordrhein-westfälischen Zugangs-Provider geladen hatte, ist erneut an diese appelliert worden, mit der Bezirksregierung Düsseldorf als Ordnungsbehörde zusammen zu arbeiten und rechtsextremistische Inhalte zu sperren. Alle rechtsextremen Angebote waren aber weiter abrufbar, Sperrungen sind nicht erfolgt. Im Rahmen der mündlichen Anhörung zu nunmehr beabsichtigten Sperranordnungen am 13.11.2001, zu der neben den Zugangsanbietern noch weitere Fachleute geladen waren, fanden abermals Verhandlungen mit den Providern statt. Um einen möglichst großen Konsens bei den Access-Providern zu erreichen, wurde als Fortsetzung der mündlichen Anhörung ein Arbeitskreis beschlossen, der sich am 19.12.2001 getroffen hatte und zusammengesetzt war aus Vertretern der Provider-Wirtschaft, der Hochschulen, der regionalen Carrier, den sogenannten Backbone-Providern, des Bundesamtes für Sicherheits- und Informationstechnik. Nachdem seitens der Access-Provider bis zum Februar 2002 noch immer keine Selbstregulierungsmaßnahmen ergriffen waren, wurden im Februar 2002 die ersten Sperrverfügungen erlassen. Die Bezirksregierung Düsseldorf hat es im Übrigen nicht dabei belassen, an die deutschen Provider zu appellieren, sie hat die amerikanische Aufsichtsbehörde FCC zum Einschreiten aufgefordert, sie hat den amerikanischen Generalkonsul angeschrieben, sie hat Gespräche mit dem Generalstaatsanwalt NRW und mit dem Simon Wiesental Institut geführt. Alle diese Versuche, die zu einem Verbot

oder der Untersagung rechtsextremistischer Internet-Inhalte hätten führen können, sind jedoch erfolglos geblieben. Erst nach Erlass der Sperrverfügungen im Februar 2002 wurden erste Seiten gesperrt.

4.1.4 Die Zielrichtung des Vorgehens der Bezirksregierung Düsseldorf

Ziel des Vorgehens der Bezirksregierung Düsseldorf ist es, die Internet-Anbieter zu verbindlichen Selbstregulierungs-Verpflichtungen anzuregen. Wenn die Provider von vornherein verhindern, dass verbotene Inhalte abrufbar sind, könnte dies ein staatliches Vorgehen weitgehend überflüssig machen. Ziel ist es also, dass die allgemeinen Geschäftsbedingungen der Provider, die ebenfalls zumeist Verbote dieser Inhalte vorsehen, aber praktisch nicht umgesetzt werden, praktische Relevanz bekommen. Nach gerichtlicher Klärung, die hoffentlich dazu führt, dass eine Sperrverpflichtung der Access-Provider festgestellt wird, könnte die praktische Umsetzung z. B. so aussehen, dass ein regelmäßiger Runder Tisch, z. B. im Vierteljahresrhythmus stattfindet, an dem außer Vertretern der Medienaufsichtsbehörde auch große deutsche Internet-Provider, wie z. B. T-Online, Google, AOL, Isis, City-Web, Compu-Serve teilnehmen. Im Rahmen dieser Treffen würde dann festgelegt, welche Internet-Inhalte als strafbewehrt gesperrt werden müssen. Diese Liste könnte dann im Verwaltungsblatt veröffentlicht und über eine Online-Verteilerliste an alle deutschen Internet-Anbieter weitergeleitet werden.

Vorstellbar wäre auch ein Marktmodell dahingehend, dass man eine Positiv-/Negativ-Liste der Provider erstellt und an die Verbraucherzentralen weitergibt, so dass sich die User darüber informieren können, welche Anbieter sie wählen, um sich und ihre Kinder vor strafbaren Internet-Inhalten zu schützen. Ziel ist es eindeutig nicht, eine Internet-Überwachung, wie sie unter der dänischen EU-Ratspräsidentschaft – unter dem Stichwort „Vorratsspeicherung aller Verbindungsdaten" – im November 2002 vorgeschlagen wurde. Damit entstünde eine komplette Bürgerüberwachung, die mit elementaren Grundrechten und mit dem Datenschutz nicht vereinbar wäre. Die Bezirksregierung sieht sich als Teil einer EU-Initiative (Empfehlung des Europäischen Parlaments an die Kommission vom April 2002), wonach die Behörden der Mitgliedstaaten zur Bekämpfung strafbarer Internet-Inhalte verstärkt und besser zusammenarbeiten sollen. Im Übrigen haben sich die Länder der Europäischen Union auf der Ebene des Europarats verpflichtet, rechtsradikale Inhalte im Internet unter Strafe zu stellen (Cyber-Crime-Convention).

4.1.5 Zur gesellschaftspolitischen Notwendigkeit des Kampfes gegen Rechtsextremismus im Internet

Der in allen Bundesländern geltende, im Jahre 1997 beschlossene MDStV erklärt Angebote, die gegen Strafgesetze verstoßen, den Krieg verherrlichen, die Menschenwürde verletzen, geeignet sind Kinder und Jugendliche sittlich schwer zu gefährden, für unzulässig. Der MDStV verpflichtet die Aufsichtsbehörden der Länder zur Sperrung oder Untersagung von unzulässigen Angeboten. Den Behörden wird dabei kein Ermessensspielraum eingeräumt. Da mehr als 90 % der von deutschen anonym bleibenden Content-Providern verantworteten rechtsextremistischen Inhalte über ausländische (insbesondere amerikanische) Host-Service-Provider im Internet verbreitet werden, sieht der MDStV als einzig verbleibende Lösung die Verpflichtung der Access-Provider zur Sperrung vor. Auf die Möglichkeit der Inanspruchnahme der Zugangs-Provider zu verzichten, bedeutet nicht nur ihre gesetzliche Mitverantwortung für die Verbreitung dieser Inhalte zu ingnorieren. Die staatlichen Aufsichtsbehörden würden darüber hinaus ihren Verpflichtungen nicht gerecht und müssten sich zu Recht vorwerfen lassen, das ihnen Mögliche gegen den zunehmenden Rechtsextremismus im Internet nicht unternommen zu haben. Dass Sperrungen bei den Zugangs-Providern die rechtsextremistischen Inhalte nicht, wie es wünschenswert wäre, aus dem Internet verbannen, wussten auch die Gesetzgeber. Trotzdem ist es sinnvoll, solche Sperrungen vorzusehen, weil dadurch die Verbreitungslogistik der vernetzten rechtsextremistischen Szene gestört wird. Die gegenwärtigen Sperrungen beweisen, dass die rechtsextremistische Szene gezwungen ist zu reagieren. So sehen sich die gesperrten rechtsextremistischen Provider zum Teil gehalten, ihre verbotenen Inhalte auf weitere Seiten – mit einem anderen Domain-Namen – zu spiegeln. Technische Anleitungen werden verbreitet, um für die Nutzer durch Manipulation ihres Rechners die Sperrungen zu umgehen. Nicht zuletzt massive Drohungen gegen Beschäftigte der Aufsichtsbehörde sprechen dafür, dass die rechtsextremistische Internet-Szene getroffen wurde.

Wer bei dieser Sachlage Sperrungen deswegen ablehnt, weil sie keine hundertprozentige Zugangsbehinderung bewirken können, folgt einer technokratischen Funktionslogik, die die Wirkungen staatlicher Ge- und Verbote verkennt. Straßenverkehrszeichen z. B. werden auch nicht deswegen abgeschafft, weil ihnen oft genug zuwidergehandelt wird. Sperrungen von unzulässigen Internet-Angeboten haben nichts mit diktatorischen Zensurmaßnahmen zu tun. Sperrungen in einem Rechtsstaat wie der Bundesrepublik Deutschland sind transparent, nicht diskriminierend und vor allen Dingen anfechtbar und korrigierbar vor den unabhängigen Verwaltungsgerichten und evtl. sogar vor dem Bundesverfassungsgericht. Es dürfte Ausdruck einer Unschärfe im Differenzierungsvermögen mancher Diskussionsteilnehmer sein, hier Parallelen zu

den Diktatoren im Iran oder in China zu konstruieren. Es ist daran zu erinnern, dass mit Bestehen der Bundesrepublik Deutschland die Gesetzgebung immer wieder deutlich gemacht hat, dass strafbare rechtsextremistische Propaganda nicht zur tolerierbaren Alltagskultur gehört.

Insofern gibt es aus historischen Gründen Unterschiede zum amerikanischen Freiheits- und Verfassungsverständnis. Die Bundesrepublik Deutschland ist nach dem Zweiten Weltkrieg bewusst in antifaschistischer Tradition aufgebaut worden. Das Bekenntnis zur Menschenwürde, das Widerstandsrecht und das Fortgelten der Vorschrift über die Entnazifizierung sind verfassungsrechtlicher, zahlreiche spezifische Strafvorschriften repressiver Ausdruck dieser Tradition. Die Bundesrepublik Deutschland versteht sich als wehrhafte Demokratie, die den Feinden der Freiheit, der Demokratie und des Rechtsstaats nicht noch einmal die Möglichkeit einräumen will, durch den Missbrauch von Freiheitsrechten die freiheitlich demokratische Grundordnung abzuschaffen. Eine Demokratie ist dem Minderheitenschutz verpflichtet. Bezogen auf den Rechtsextremismus entsteht dadurch die staatliche Pflicht, die Aggression zu bekämpfen und mögliche Opfer zu schützen. Wer rechtsextremistische Inhalte im Internet zulassen will, duldet rechtswidrige Taten und liefert ethnische und religiöse Minderheiten der aggressiven neonazistischen Hasspropaganda aus. Der Rechtsextremismus verschafft sich durch das Internet seinen gesellschaftlichen Resonanzboden, obwohl es kein Online-Recht gibt, dass nicht bereits Offline Gültigkeit hat.

Die an die Allgemeinheit gerichtete Nazipropaganda im Internet in Form von Schrift, Ton und Bild unterscheidet sich nicht von der Propaganda in Form von Büchern, Schallplatten und Filmen. Wenn staatliche Maßnahmen dazu beitragen, dass die Regeln, die im Zeitschriften-, Buch- und Tonträgerhandel im Rundfunk und Fernsehen gelten und zumeist eingehalten werden, sich auch im Internet durchsetzen, dann hat staatliche Ordnungspolitik ihr Ziel erreicht.

4.2 Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden – Eine Kritik an den Verfügungen der Bezirksregierung Düsseldorf[17]

Prof. Dr. Christoph Engel

4.2.1 Einleitung

Wenn es nach dem Düsseldorfer Regierungspräsidenten (RP) geht, endet die Globalisierung vor den Düsseldorfer Stadttoren. 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. 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 Düsseldorfer Regierungspräsidenten 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.

(17) Mit freundlicher Genehmigung des Verlags C. H. Beck und der Redaktion MultiMedia und Recht (MMR). Das Gesamtgutachten ist veröffentlicht in der Beilage zu Heft 4/2003 der MMR.

4.2.2 Thesen

- 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.
- Der RP als Behörde der unmittelbaren Staatsverwaltung verstößt gegen das Verfassungsgebot der Staatsferne, wenn er den Inhalt des Internet reguliert.
- 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.
- Dem RP fehlt auch deshalb die Zuständigkeit, weil 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 parallelen Regeln des RStV gefüllt werden könnte.
- 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 jedenfalls nur mit ausdrücklicher gesetzlicher Ermächtigung. Daran fehlt es.
- 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.
- 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.

- 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.
- 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.
- § 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.
- § 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.
- 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.
- 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. Im Übrigen 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.
- Der RP sprengt die Grenzen von § 22 Abs. 3 MDStV. Er will diese Ausnahmevorschrift 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.

- 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 Handlungsstörer; 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.
- 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.
- 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 GG und Art. 14 GG. Schließlich schützt sie Art. 2 Abs. 1 GG vor der aufgezwungenen Rolle als Regulierungsinstanz.
- Die Verfügung greift nicht nur in Grundrechte der Access-Provider ein. Vielmehr greift sie insbesondere auch in die Informationsfreiheit der Nutzer ein. Im Lichte der nationalsozialistischen Vergangenheit schützt Art. 5 Abs. 1 GG grundsätzlich 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.
- 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.
- 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. Im Übrigen 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 rechtsstaatlichen 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.

- 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 Staates im konkreten Fall sehr hohes Gewicht hat. Geeignetheit und Angemessenheit fallen bei dieser Art der Definition des legitimen Ziels also praktisch zusammen.
- 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 nutzerautonomer (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 Kinderpornografie Strafverfahren gegen die deutschen Nutzer nationalsozialistischer Inhalte möglich macht.
- 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 Proxy-Servern gedrängt werden.

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.

4.3 Die Düsseldorfer Sperrverfügung aus Providersicht

Dr. Torsten Schreier

4.3.1. Einleitung

Die Eilverfahren um die Düsseldorfer Internet-Sperrverfügung sind abgeschlossen[18]. Bilanz vor dem OVG Nordrhein-Westfalen: Fünf Provider scheiterten, nur einer hatte Erfolg[19]. Der Beitrag zeigt auf, warum die Sperrverfügung aus Providersicht rechtswidrig ist und warum die Eilverfahren unterschiedlich endeten.

Zum Hintergrund:

Im Frühjahr 2002 ergingen insgesamt 76 Sperrverfügungen gegen nordrhein-westfälische Provider wegen rechtsradikaler Internetseiten. Nach erfolglosem Widerspruchsverfahren erhoben einige der betroffenen Unternehmen im Sommer 2002 gegen diese Verfügungen Klage, woraufhin der Sofortvollzug angeordnet wurde. Da die Bezirksregierung Düsseldorf zwar zentral für die Internetaufsicht in Nordrhein-Westfalen zuständig ist, die gerichtliche Zuständigkeit sich jedoch nach dem Sitz des Providers richtet (§ 52 Nr. 3 Satz 2 VwGO), waren erstinstanzlich verschiedene Verwaltungsgerichte mit den Eilverfahren der Provider befasst. Mit konträren Ergebnissen: Nur das VG Minden gab einem Provider in der Sache recht[20], ein Verfahren hatte aus formalen Gründen Erfolg, weil die Bezirksregierung die Anordnung der sofortigen Vollziehung an eine nicht existierende Gesellschaft gerichtet hatte[21], die restlichen Entscheidungen bestätigten den Sofortvollzug[22].

4.3. Die Ermächtigungsgrundlage

Die Bezirksregierung Düsseldorf hat die Sperrverfügung auf § 22 Abs. 3 MDStV gestützt. Nach dieser Vorschrift können gegen Diensteanbieter von fremden Inhalten (§§ 7 bis 9 MDStV) Sperrverfügungen erlassen werden.

(18) Die erstinstanzlichen Gerichtsentscheidungen um die Düsseldorfer Sperrverfügung sowie die Sperrverfügung und der Widerspruchsbescheid sind im Volltext abrufbar unter: http://www.brd.nrw.de/BezRegDdorf/hierarchie/.

(19) Ebenfalls abrufbar unter: http://www.brd.nrw.de/BezRegDdorf/hierarchie/. Näher zum Verlauf der Eilverfahren: Schreier, MMR 2003, 297 f.

(20) Beschl. v. 31.10.2002, Az. 11 L 1110/02.

(21) VG Gelsenkirchen, Beschl. v. 17.12.2002, Az. 1 L 2547/02.

(22) VG Arnsberg, Beschl. v. 6.12.2002, Az. 13 L 1848/02; VG Gelsenkirchen, Beschl. v. 18.12.2002, Az. 1 L 2528/02; VG Düsseldorf, Beschlüsse v. 19.12.2002, Az. 15 L 4149/02, Az. 15 L 4148/02 und Az. 15 L 3749/02; VG Aachen, Beschlüsse v. 05.02.2003, Az. 8 L 1284/02 und Az. 8 L 1028/02; VG Köln, Beschl. v. 07.02.2003, Az. 6 L 2495/02.

a. § 22 Abs. 3 MDStV keine Ermächtigungsgrundlage gegen Netzwerk-Provider

Der Adressat einer Sperrverfügung gemäß § 22 Abs. 3 MDStV muss also zumindest ein Diensteanbieter sein. Nach der Legaldefinition des § 3 Nr. 1 MDStV ist Diensteanbieter auch ein Unternehmen, dass den Zugang zur Nutzung von Mediendiensten vermittelt (sog. Access-Provider). Derartige Access-Provider sind durch folgende Merkmale qualifiziert: Die Unternehmen müssen selbst Nutzern direkt den Zugang zu Computernetzen vermitteln und sie müssen die Endkundenbeziehungen zu den Nutzern unterhalten[23]. Ein anderes Geschäftsmodell verfolgen demgegenüber die sog. Netzwerk-Provider. Diese Unternehmen stellen Access-Providern als deren Dienstleister Netz- und sonstige Infrastruktur zur Verfügung, mit der dann die Access-Provider Nutzern den Zugang zum Internet und damit auch zu den im Internet verbreiteten Mediendiensten ermöglichen. Netzwerk-Provider vermitteln folglich weder direkt den Zugang zum Internet, noch unterhalten sie Endkundenbeziehungen zu den Internetnutzern. Auf Netzwerk-Provider ist § 22 Abs. 3 MDStV nicht anwendbar[24].

Gegen Netzwerk-Provider können im Übrigen auch nach anderen Rechtsgrundlagen keine Sperrverfügungen ergehen. Netzwerk-Provider unterfallen als reine Telekommunikationsdienstleister im Sinne des § 3 Nr. 16 und Nr. 18 TKG ausschließlich dem TKG (siehe auch § 2 Abs. 1 Satz 3 MDStV). Die Vorschriften des TKG ermächtigen zu im einzelnen aufgeführten Zugriffen auf die über Netze verbreiteten Kommunikationsinhalte. Es werden z.B. Überwachungsmaßnahmen ermöglicht oder Auskunftspflichten über die Telekommunikation statuiert (§§ 88 ff. TKG). Nicht vorgesehen ist jedoch die Befugnis, von Netzbetreibern die Sperrung von Anschlüssen oder den Zugriff auf bestimmte Internetangebote zu verlangen. Das TKG ist auch als abschließende Regelung der staatlichen Eingriffsbefugnisse in bezug auf mittels Telekommunikationsdienstleistungen übertragene Inhalte anzusehen. Es entspricht allgemeinen Grundsätzen, dass sich staatliche Eingriffe bzgl. Inhalten in der Telekommunikation seit jeher gegen den Sender, nicht den Betreiber des Übertragungsmediums richten. Hieraus folgt, dass die Inanspruchnahme des Telekommunikationsdienstleisters für rechtswidrige Übertragungsinhalte Dritter aus allgemeinen Vorschriften (etwa der ordnungsbehördlichen Generalklausel) ausgeschlossen ist[25]. So haben es die Ordnungsbehörden, soweit ersichtlich, auch niemals erwogen, beispielsweise gegen die Deutsche Telekom AG mit Anordnungen zur Sperrung von Telefonanschlüssen vorzugehen, weil über die betreffenden Rufnummern rechtsradikale Infotelefone oder Infofaxe betrieben werden.

(23) AG München, K&R 1998, 407 (409) zu § 5 Abs. 3 TDG a.F., der ebenfalls das Tatbestandsmerkmal der Zugangsvermittlung enthielt.

(24) Wie hier: Stadler, Haftung für Informationen im Internet, Berlin 2002, 59; sowie bereits zu §§ 5 Abs. 3, 18 Abs. 3 MDStV a.F.: Spindler, in: Hoeren/Sieber, Handbuch Multimediarecht, München 2001, Teil 29, Rn. 356; Koenig/Loetz, CR 1999, 438 (439).

(25) Koenig/Loetz, CR 1999, 438 (439); Koch, CR 1997, 197 (199); vgl. auch Spindler, in: Hoeren/Sieber, Handbuch Multimediarecht, München 2001, Teil 29, Rn. 356.

b. § 22 Abs. 3 MDStV auch keine Ermächtigungsgrundlage gegen Access-Provider

Richtiger Ansicht nach kann indessen auch gegen Access-Provider keine Sperrverfügung auf der Grundlage des § 22 Abs. 3 MDStV ergehen, falls sich die Tätigkeit dieser Provider auf die reine Zugangsvermittlung beschränkt.

aa. Wortlaut

Dies ergibt sich bereits aus dem Wortlaut des Gesetzes: § 22 Abs. 3 MDStV normiert ausdrücklich, dass der Adressat der Maßnahme ein „Diensteanbieter von fremden Inhalten gemäß §§ 7 bis 9 MDStV" sein muss. Zwar sind Access-Provider „Diensteanbieter" im Sinne von § 3 Nr. 1 MDStV, da sie den Zugang zur Nutzung des Internet und damit auch zu Mediendiensten vermitteln. Gemäß § 22 Abs. 3 MDStV können Sperrungsanordnungen jedoch nicht gegen jeden Diensteanbieter im Sinne der §§ 7 bis 9 MDStV gerichtet werden, sondern nur gegen solche, die fremde Inhalte anbieten. Gegen Access-Provider sind Sperrungsanordnungen somit nur dann zulässig, wenn diese dem Nutzer nicht nur den reinen Internetzugang, sondern zugleich fremde Inhalte anbieten, z. B. den Betrieb einer Suchmaschine[26]. Insofern kann nicht eingewandt werden, § 22 Abs. 3 MDStV liefe leer, wenn man die Norm nicht auf reine Access-Provider anwenden würde. Denn auch ohne Anwendung der Norm auf reine Access-Provider können nach § 22 Abs. 3 MDStV Sperrverfügungen gegen Host-Provider gem. § 9 MDStV (und zwar auch dann, wenn diese wegen der Haftungsprivilegierung gem. § 9 Ziffern 1 und 2 nicht verantwortlich sind) sowie gegen Access-Provider, die gleichzeitig fremde Inhalte anbieten, erlassen werden.

bb. Systematik/Sinn und Zweck

Selbst wenn man reine Access-Provider entgegen der hier vertretenen Ansicht unter den Wortlaut des § 22 Abs. 3 MDStV subsumieren wollte, würde eine an verfassungsrechtlichen Grundsätzen orientierte Auslegung gleichwohl gebieten, diese Provider im Wege einer „systematisch-teleologischen Reduktion" aus dem Kreis der Adressaten einer behördlichen Sperrungsverpflichtung auszunehmen, da ihre Tätigkeit dem Wesen nach eine Telekommunikationsdienstleistung ist[27]. Wie der Netzwerk-Provider, auf den der MDStV nicht anwendbar ist, bietet auch der Access-Provider eine technische Plattform zur Übermittlung von Informationen, ohne Einfluss auf die übermittelten Inhalte zu haben. Auch seine Tätigkeit besteht darin, Nachrichten auszusenden, zu übermitteln und zu empfangen (§ 3 Nr. 16 TKG). Was der reine Access-Provider darüber hinaus an

(26) So bereits zu § 18 Abs. 3 MDStV a.F.: Hoeren, Stellungnahme vom 8.11.2001 zur geplanten Sperrverfügung der Bezirksregierung Düsseldorf (nicht veröffentlicht). Nach Koenig/Loetz, CR 1999, 438 (441 f.), verbleiben bei Nichtanwendung auf reine Access-Provider noch Anbieter von Hyperlinks, Navigatoren und ähnlicher Hilfsmittel zur Nutzung von Mediendiensten im Anwendungsbereich von § 18 Abs. 3 a. F.

(27) Koenig/Loetz, CR 1999, 438 (441 f.); im Ergebnis ebenso: Stadler, MMR 2002, 243 (344).

Funktionen anbietet, um den Rechner des Nutzers in ein Datennetz einzubinden, entspricht der Bereitstellung eines Anschlusses und der Vergabe einer Rufnummer in einem herkömmlichen Telekommunikationsnetz, schafft also nur die Voraussetzungen, um Telekommunikation zu ermöglichen. Die Dienstleistung des reinen Access-Providers ist deshalb mehr Telekommunikationsdienstleistung als Tele- oder Mediendienst, seiner Funktion nach ist der reine Access-Provider genau wie der Netzwerk-Provider inhaltsneutraler Telekommunikationsdienstleister[28]. Dies entspricht auch der Auffassung der Bundesregierung (als Initiatorin des Informations- und Kommunikationsdienstegesetzes – IuKD –), die in ihrer Antwort auf eine parlamentarische Anfrage der Fraktion Bündnis 90/DIE GRÜNEN ausführt, Access-Provider hätten „nur eine Transportfunktion inne [...], die insoweit gleich oder ähnlich einem Angebot von Telekommunikationsdienstleistungen zu beurteilen ist"[29].

Jedenfalls aber würde die Anwendung von § 22 Abs. 3 MDStV auf reine Access-Provider eine gleichheitswidrige unterschiedliche Behandlung gegenüber Netzwerk-Providern bedeuten. § 22 Abs. 3 MDStV wäre insoweit wegen Verstoßes gegen den Gleichheitssatz des Art. 3 Abs. 1 GG verfassungswidrig. Darüber hinaus wäre die Regelung des § 22 Abs. 3 MDStV, wenn man sie auf reine Access-Provider anwendet, auch wegen Verstoßes gegen die grundgesetzliche Kompetenzordnung verfassungswidrig. Die Tätigkeit der reinen Access-Provider ist, wie soeben dargelegt, ihrem Wesen nach eine Telekommunikationsdienstleistung, die im wirtschaftlich-gewerblichen Bereich angesiedelt ist. Deshalb unterfällt ihre Regulierung der Kompetenz des Bundes nach Art. 74 Abs. 1 Nr. 11 bzw. Art. 73 Nr. 7 GG. Eine inhaltlich-redaktionelle Seite, die es rechtfertigen würde, dass die Länder diese Tätigkeit im MDStV regulieren, hat die Kommunikationsdienstleistung der reinen Access-Provider nicht[30].

c. Die Ansicht des OVG Nordrhein-Westfalen

In bezug auf Access-Provider ist das OVG Nordrhein-Westfalen den genannten Bedenken nicht gefolgt und hat die Düsseldorfer Sperrverfügung auf § 22 Abs. 3 MDStV gestützt[31]. Auf dieser Grundlage hält das Gericht die Sperrungsanordnung im Ergebnis auch für gerechtfertigt und hat deshalb die Beschwerden von fünf Access-Providern zurückgewiesen, die bereits erstinstanzlich vor den Verwaltungsgerichten unterlegen waren[32].

(28) Stadler, MMR 2002, 343 (344); Spindler/Volkmann, K&R 2002, 398 (401); Koenig/Loetz, CR 1999, 438 (442).
(29) BT-Drs. 13/7757, S. 10.
(30) Koenig/Loetz, CR 1999, 438 (443).
(31) Beschl. v. 19.3.2003, Az. 8 B 2567, Umdruck, S. 5.
(32) Zum Verlauf der Eilverfahren siehe näher: Schreier, MMR 2003, 297 f.

Der Provider hingegen, der schon erstinstanzlich vor dem VG Minden erfolgreich war [33], hatte gegen die Sperrverfügung unter anderem eingewandt, dass nur ein geringer Teil seiner Geschäftstätigkeit das Access-Providing betrifft, während er im übrigen Netzwerk-Providing betreibt. Da der erkennende Senat diesen Einwand für relevant hielt, erging ein Hinweis an die Bezirksregierung: Hatte diese den Sachverhalt falsch ermittelt, weil sie den Provider unrichtigerweise als Access- statt als Netzwerk-Provider behandelt hatte? Hatte sie ihr Ermessen falsch ausgeübt, weil die Kosten für die Sperrung angesichts der Größe des Netzes des betroffenen Providers um ein vielfaches höher gewesen wären, als von der Bezirksregierung angenommen? Das Gericht fragte deshalb an, ob die Bezirksregierung ihre Beschwerde gegen den Beschluss des VG Minden fallen lassen wolle. Zu den Bedenken des Gerichts ließ sich die Bezirksregierung nicht ein: Sie nahm ihre Beschwerde gegen den Mindener Beschluss zurück und verhinderte so eine abweichende Sachentscheidung des OVG.

Offenbar teilt das OVG also die hier vertretene Ansicht, dass gegen Netzwerk-Provider keine Sperrungsanordnungen ergehen können. Im Mindener Fall bot das betroffene Unternehmen indessen sowohl Netzwerk- als auch Access-Providing an. Beide Produkte wurden jedoch über dieselbe technische Infrastruktur abgewickelt, weshalb der Provider faktisch nicht in der Lage war, die Sperrungsanordnung nur bezüglich des Access-, nicht aber hinsichtlich des Netzwerk-Providings umzusetzen. Selbst wenn man der Auffassung des OVG folgt, dass Sperrungsanordnungen gegenüber Access-Providern ergehen können, sind solche Anordnungen gegenüber kombinierten Access- und Netzwerk-Providern jedenfalls dann unverhältnismäßig, wenn das Geschäftsvolumen des Netzwerk-Providings das des Access-Providings erheblich übersteigt. Dieser Argumentation verschloss sich auch die Bezirksregierung nicht: Wenige Tage nach ihrem Rückzug vor dem OVG hob sie gegenüber dem erfolgreichen Provider auch die Sperrverfügung mit der Begründung auf, deren Verhältnismäßigkeit sei in Frage gestellt.

4.3.3 Die Voraussetzungen von § 22 Abs. 3 MDStV

Selbst wenn man mit dem OVG Nordrhein-Westfalen und entgegen der hier vertretenen Auffassung § 22 Abs. 3 MDStV auf reine Access-Provider anwendet, lagen im Fall der Düsseldorfer Sperrungsanordnung die sachlichen Voraussetzungen für den Erlass einer Verfügung nicht vor.

(33) Beschl. v. 31.10.2002, Az. 11 L 1110/02.

a. Gebot der lediglich subsidiären Inanspruchnahme von Access-Providern

aa. Reichweite der Subsidiarität verkannt

Gemäß § 22 Abs. 3 MDStV kann eine Sperrung gegenüber einem Access-Provider nur angeordnet werden, wenn Maßnahmen gegenüber dem Anbieter eigener Inhalte (Content-Provider) „nicht durchführbar oder nicht erfolgversprechend" sind. Aus dem Verhältnismäßigkeitspostulat ergibt sich das gleiche für das Verhältnis von Access-Provider und Host-Provider. Damit darf der Access-Provider lediglich subsidiär in Anspruch genommen werden[34].

Die Bezirksregierung geht von der Undurchführbarkeit bzw. Erfolglosigkeit des Vorgehens gegen die primär Verantwortlichen bereits deshalb aus, weil die von ihr per e-Mail kontaktierten amerikanischen Host-Provider nicht auf die Aufforderung reagiert haben, die inkriminierten Angebote zu entfernen, und eine Bitte an die amerikanische Medienaufsichtsbehörde (Federal Communications Commission - FCC) um Beseitigung der inkriminierten Inhalte fruchtlos geblieben ist. Weitere Versuche, die primär Verantwortlichen in Anspruch zu nehmen, hat die Bezirksregierung laut ihrer Einlassung im Verfahren nicht unternommen. Ein Vorgehen gegen die in den unzulässigen Internet-Angeboten aufgeführten deutschen Content-Provider ist nach Auffassung der Bezirksregierung bereits deshalb nicht möglich, weil diese anonym agieren und offensichtlich Scherz- bzw. Deckadressen verwenden.

Die Bezirksregierung verkennt die Tragweite der Subsidiarität, wenn sie meint, diese Maßnahmen seien ausreichend, um die Undurchführbarkeit bzw. Erfolglosigkeit zu begründen. § 22 Abs. 3 MDStV darf auf Access-Provider vielmehr nur äußerst restriktiv angewandt werden. Dies ergibt sich zum einen aus der Nähe der Access-Provider zu Telekommunikationsdienstleistern, gegen die, wie unter I.1 dargelegt, überhaupt keine Sperranordnungen wegen rechtswidriger Kommunikationsinhalte ergehen können[35]. Ein weiterer und entscheidender Grund für eine restriktive Auslegung des § 22 Abs. 3 MDStV bei Access-Providern folgt aus der Systematik der Haftungsregelungen (§§ 6 ff.) des MDStV, die ein Regel-/Ausnahmeverhältnis für die Inanspruchnahme von Zugangsvermittlern etablieren. Dieses Regel/-Ausnahmeverhältnis würde umgekehrt, wenn zum Nachweis der Undurchführbarkeit bzw. Aussichtslosigkeit der Inanspruchnahme der primär Verantwortlichen im Rahmen des § 22 Abs. 3 MDStV bereits die fehlende Reaktion des ausländischen Providers auf eine e-Mail und die Fruchtlosigkeit einer an die FCC gerichteten Bitte um Beseitigung der Inhalte genügen würde. Dass eine Reaktion der Provider ausbleibt, dürfte der Regelfall sein. Gleiches gilt für die ablehnende Haltung der FCC, die von Rechts wegen daran gehindert ist, den amerika-

(34) Spindler/Volkmann, K&R 2002, 398 (404 f.); Stadler, Haftung für Informationen im Internet, Berlin 2002, 123.
(35) Vgl. Koenig/Loetz, CR 1999, 438 (442).

nischen Providern die Entfernung der Angebote aufzugeben, da die betreffenden Inhalte nach amerikanischem Recht zulässig sind. Um der Subsidiarität zu genügen ist es vielmehr erforderlich, sämtliche zur Verfügung stehenden Möglichkeiten auszuschöpfen, um die Sperrung rechtswidriger Inhalte durch die primär Verantwortlichen - auch wenn sie im Ausland ansässig sind – herbeizuführen.

bb. Weiteres Vorgehen gegen Host- und Content-Provider möglich

So hätte die Bezirksregierung beispielsweise im Wege der Rechtshilfe von den zuständigen US-Behörden verlangen können, dass diese die Host-Provider dazu anhalten, den Zugang zu den inkriminierten Angeboten in Deutschland zu unterbinden. Dies wäre sicher sinnvoller gewesen, als die Entfernung der Angebote zu verlangen, wie die Bezirksregierung es getan hat, denn dies ist nach amerikanischem Recht nicht möglich. Den besseren Weg, gegen derartige Angebote vorzugehen, beschreibt die Entscheidung des Tribunal de Grande Instance de Paris vom 20.11.2000 in Sachen „Yahoo!“[36]. Das französische Gericht ordnete an, den Zugang zu (nach französischem Recht) rechtswidrigen Inhalte für lokale Internetnutzer unmöglich zu machen. Dies erfordert aber gerade nicht die vollständige Sperrung einer Seite, sondern lediglich technische Maßnahmen, die die lokalen Internetnutzer von dem Zugang ausschließen. Diese Möglichkeit hatte auch der Bezirksregierung offen gestanden. Hiergegen hat die Bezirksregierung eingewandt, ein Vorgehen nach dem Muster des französischen Gerichts im „Yahoo!“-Fall sei nicht erfolgversprechend. Sie verweist auf das Urteil des United States District Court for the Northern District of California vom 9.11.2001, nach dem das französische Urteil im „Yahoo!“-Fall in den USA nicht vollstreckbar ist. Die Bezirksregierung fehlinterpretiert damit jedoch die amerikanische Entscheidung. Diese besagt keineswegs, dass eine ausländische Verfügung an amerikanische Provider, den Zugang zu bestimmten Internetseiten für ausländische Nutzer zu sperren, generell wegen Verstoßes gegen den ersten Zusatz zur US-Verfassung nicht vollstreckbar sein kann. Das Gericht verweigert der französischen Entscheidung vielmehr zunächst wegen mangelnder Bestimmtheit die Anerkennung, da sie anordne, dass alle Seiten unzugänglich gemacht werden müssen, die „als Entschuldigung oder Leugnen von Nazi-Verbrechen verstanden werden könnten“. Zur Vereinbarkeit der Sperrverfügung mit amerikanischem Verfassungsrecht führt das Gericht aus, die französische Seite habe es versäumt darzulegen, wie das Urteil in Übereinstimmung mit dem ersten Verfassungszusatz in den USA vollstreckt werden könne[37]. Nach den Gründen der amerikanischen Entscheidung ist es also keinesfalls ausgeschlossen, dass durch eine entsprechend formulierte und begründete deutsche Verfügung die Sperrung des Zugangs zu amerikanischen Internetseiten aus Deutschland erreicht werden kann.

(36) Im Internet abrufbar unter: http://www.chez.com/aipj/ordonnance30oct2001.htm.

(37) Urteil des United States District Court for the Northern District of California vom 7. November 2001, Yahoo! Inc. v. La Ligue contre le Racisme et L'antisemtitisme, Case No. C-00-21275 JF, Entscheidungsumdruck, S. 13 f.,
im Internet abrufbar unter: http://www.eff.org/Cases/LICRA_v_Yahoo/20011107_us_distct_decision.pdf.

Weiter hat die Bezirksregierung im Verfahren ausgeführt, ein Vorgehen gegen die in den unzulässigen Internet-Angeboten aufgeführten deutschen Content-Provider sei gescheitert, da diese anonym agierten und offensichtlich Scherz- bzw. Deckadressen verwendeten. Mit dieser Feststellung hat die Bezirksregierung ihrer Pflicht, vorrangig gegen die Content-Provider vorzugehen, allerdings keineswegs genüge getan, da es möglich ist, die Content-Provider zu identifizieren. Beispielsweise ist es dem Bundesamt für Verfassungsschutz aufgrund seiner Szenekenntnisse gelungen, die hinter dem Decknamen „Neogermania" stehende Person in Deutschland zu ermitteln, deren Inhalte bis dahin auf der Seite „nazi-lauck-nsdapao", einer der von der Sperrungsanordnung betroffenen Websites also, gehostet worden waren. Auf diese Information hin hat die zuständige Staatsanwaltschaft ein Ermittlungsverfahren eingeleitet und eine Hausdurchsuchung bei dem Beschuldigten durchgeführt[38]. Dies zeigt, dass es bei hinreichenden Bemühungen möglich ist, die deutschen Urheber der inkriminierten Seiten zu ermitteln und gegen sie vorzugehen. Schon deshalb verstößt ein Vorgehen gegen die Access-Provider gegen den Subsidiaritätsgrundsatz.

cc. Diplomatisches Vorgehen erforderlich

Auch unterstellt, nach derzeitiger Rechtslage bestünde keine Möglichkeit, gegen die amerikanischen Provider vorzugehen, hätten der Bezirksregierung noch andere Möglichkeiten offengestanden: Der District Court for the Northern District of California hat ausgeführt, dass ausländische Verfügungen in den Vereinigten Staaten anzuerkennen seien, sobald es international verbindliche Standards über die Regulierung von Meinungsäußerungen im Internet gibt[39]. Die deutsche Bundesregierung hat im Mai 2002 ein Konzept zur Bekämpfung des Rechtsextremismus vorgelegt. Darin heißt es: „Das Internet ist ein globales Medium, dessen Kontrolle international sehr unterschiedlich gehandhabt wird. Während beispielsweise in den USA die Verbreitung rechtsextremer Internetinhalte unter Hinweis auf die Meinungsfreiheit weitgehend straflos bleibt, wird sie in Deutschland als Straftat geahndet. Daher setzt sich die Bundesregierung in internationalen Gremien, vor allem im Europarat und im Rahmen der G-8 der Vereinten Nationen, nachhaltig für eine einheitliche internationale Verfolgung rechtsextremistischer Straftaten im Internet ein"[40].
Die Bezirksregierung sollte über die nordrhein-westfälische Landesregierung diese Initiative der Bundesregierung unterstützen, statt mit einem Sonderweg, der beispielsweise auch vom Europaparlament verurteilt wird[41], gegen einheimische Access-

(38) Diese Information stammen aus einem Vortrag, den der zuständige Beamte des Bundesamtes für Verfassungsschutz bei dem von der Bezirksregierung am 17.09.2002 veranstalteten Kongress „Hass und Gewalt im Internet" gehalten hat.

(39) Urteil des United States District Court for the Northern District of California vom 7. November 2001, Yahoo! Inc. v. La Ligue contre le Racisme et L'antisemitisme, Case No. C-00-21275 JF, Entscheidungsumdruck, S. 19,
im Internet abrufbar unter: http://www.eff.org/Cases/LICRA_v_Yahoo/20011107_us_distct_decision.pdf.

(40) Im Internet abrufbar unter http://www.bmibund.de/dokumente/pressemitteilung/ix_79389.htm.

(41) Siehe Mitteilung über die Resolution des Europäischen Parlaments gegen nationale Sperrungen ausländischer Websites vom 11.4.2002, ITRB 2002, S. 125.

Provider vorzugehen. Vor dem Hintergrund der drohenden Umkehrung der höchstens subsidiären Inanspruchnahme zu einer vom Gesetzgeber ausdrücklich nicht gewollten Regelinanspruchnahme deutscher Access-Provider für ausländische Inhalte wäre es gerechtfertigt und angezeigt gewesen, dass die Bezirksregierung den Erfolg der internationalen Bemühungen der Bundesregierung abgewartet hätte.

b. Unverhältnismäßigkeit der Verfügung

aa. Relevanz der Umgehungsmöglichkeiten

Die technischen Methoden zur Implementierung von Sperrverfügungen und deren Umgehungsmöglichkeiten sind in jüngster Zeit intensiv diskutiert worden[42]. Ohne auch an dieser Stelle auf die technischen Einzelheiten einzugehen, kann als wohl einstimmiges Ergebnis dieser Debatte festgehalten werden: Eine Sperrung der inkriminierten Inhalte ist technisch nicht möglich, da es für jede in Betracht kommende Methode (die Bezirksregierung hatte die sog. Domain-Name-Server-Lösung, die sog. Router-Lösung und die sog. Proxy-Server-Lösung vorgeschlagen) einfache Umgehungsmöglichkeiten gibt. Das OVG Nordrhein-Westfalen hält dies allerdings für kein entscheidendes Argument gegen die Verhältnismäßigkeit der Verfügung: Es reiche aus, dass die Sperrungsanordnung einen Beitrag zur Förderung des gewünschten Erfolgs leiste, also ein Schritt in die richtige Richtung sei. Eine vollständige Gefahrenabwehr sei nicht erforderlich[43]. Hiermit unterschätzt das OVG allerdings die Relevanz der Umgehungsmöglichkeiten.

Die Möglichkeit, die Sperrung von Inhalten zu umgehen, ist im Rahmen des § 22 Abs. 3 MDStV von erheblicher Bedeutung[44]. Dies ist letztlich eine Folge des Verhältnismäßigkeitspostulats, dem eine den Adressaten intensiv belastende gefahrenabwehrrechtliche Maßnahme dann nicht Rechnung trägt, wenn im Ergebnis die Gefahr nur unwesentlich verringert wird. Die Bundesregierung (als Initiatorin des IuKD) hat das Kriterium der Umgehungsmöglichkeit folgendermaßen auf den Punkt gebracht:
„Maßnahmen zur Verhinderung des Zugriffs auf fremde Inhalte sind insbesondere unzumutbar, wenn sie einen erheblichen Aufwand erfordern, ihre Wirksamkeit jedoch durch einen Zugriff auf entsprechende Informationsangebote im Ausland oder über andere Netzverbindungen mit einem vergleichsweise geringen Aufwand umgangen werden kann.“[45]

(42) Siehe nur aus der juristischen Literatur Stadler, Haftung für Informationen im Internet, Berlin 2002, S. 123 ff., sowie aus technischer Sicht Schneider, MMR 1999, 571 ff. Vgl. weiterhin die Umgehungsanleitung des Chaos Computer Clubs, im Internet abrufbar unter http://www.ccc.de/censorship/dns-howto/index.html.

(43) Beschl. v. 19.3.2003, Az. 8 B 2567, Umdruck, S. 18 f.

(44) Vgl. Sieber, Verantwortlichkeit im Internet, München 1999, 212 f.

(45) Antwort der Bundesregierung auf eine parlamentarische Anfrage der Fraktion Bündnis 90/DIE GRÜNEN, BT-Drucksache 13/7757, S. 22.

In der Rechtsprechung der Zivilgerichte wurde die Relevanz der Umgehungsmöglichkeiten in entsprechender Weise rezipiert. Das OLG München führt zur Verhinderung rechtswidriger Internetinhalte aus, dass „der Diensteanbieter nicht jeden nur denkbaren Aufwand betrieben muss, um die Nutzung rechtswidriger Inhalte zu vermeiden, sondern die Bedeutung des Einzelfalls und der erforderliche technische und wirtschaftliche Aufwand sowie die Auswirkungen auf andere Teile des Dienstes und andere Nutzer im Verhältnis zueinander gesehen werden müssen. Hiernach sind Maßnahmen zur Verhinderung des Zugangs auf fremde Inhalte dann als unzumutbar anzusehen, wenn sie, wie vorliegend, einen erheblichen Aufwand erfordern, ihre Wirksamkeit jedoch durch einen Zugriff über andere Netzverbindungen mit einem vergleichsweise geringen Aufwand umgangen werden kann“[46].

Ob die Umgehungsmöglichkeiten leicht oder weniger leicht zu implementieren sind, ob sie nur für technisch versierte Nutzer oder auch für Durchschnittsnutzer in Betracht kommen, darüber herrschte im Verfahren zwischen der Bezirksregierung und den Providern Streit. Fakt ist, dass die Klientel der inkriminierten Inhalte die Umgehungsmöglichkeiten umgehend untereinander kommuniziert. Hierfür gab es in der Vergangenheit Beispiele: Nachdem die Netzadresse des niederländischen Providers „xs4all“ mit der www-Seite der linksextremistischen Zeitschrift „radikal“ auf Initiative des Generalbundesanwalts gesperrt worden war, wurden die neuen Abrufmöglichkeiten in verschiedenster Form publik gemacht. Eine weit verbreitete Nachricht teilte beispielsweise 36 neue www-Adressen in aller Welt mit, unter denen „radikal“ abrufbar war[47]. Auch bezüglich der Düsseldorfer Sperrverfügung ist dieser Effekt eingetreten: Das Angebot von *www.nazi-lauck-nsdapao.com* kann derzeit unter zahlreichen weiteren Domains erreicht werden (u.a. unter der Domain *www.nordrhein-westfalen.biz*), deren Namen über Foren und News-Groups veröffentlicht worden sind. Als Reaktion auf den Vorstoß der Bezirksregierung wurde das Gedankengut des Neonazis Lauck sogar in den Rechtsstaat herabwürdigender Weise in den Kommunikationsbereichen der Internetseite des Landes NRW zugänglich gemacht. Zudem werden auf zahlreichen rechtsradikalen Seiten Hinweise auf freie Proxy-Server, z. B. in Korea, kommuniziert, mit denen alle Maßnahmen umgangen werden können. Es ist deshalb davon auszugehen, dass die Sperrungsanordnung nur zu einem geringen Rückgang der Abrufe der betreffenden Seiten führen wird. Zudem ist zumindest im vorliegenden Fall die Annahme des OVG Nordrhein-Westfalen zweifelhaft, bereits eine Gefahrverringerung rechtfertige den Erlass der Sperrverfügung. Zwar ist es richtig, dass eine Gefahr oftmals nicht durch eine Ordnungsverfügung gegen einen einzelnen Verantwortlichen beseitigt werden kann, sondern der angestrebte Erfolg nur im Zusammenspiel mehrerer behördlicher Maßnahmen eintritt. Vor diesem Hintergrund hat dann die einzelne Ordnungsverfügung in der Tat lediglich eine Gefahrverringerung zur Folge. Vorliegend fehlt es

(46) OLG München, Urteil vom 03.02.2000 - 6 U 5475/99, K&R 2000, S. 356 ff.
(47) Siehe Sieber, Verantwortlichkeit im Internet, München 1999, 93.

indessen gerade an einem nachvollziehbaren Konzept der Bezirksregierung, das insgesamt zu einer Gefahrbeseitigung oder möglichst weitgehenden Gefahrverringerung führen würde: Bereits oben (3.a.cc) ist dargelegt worden, dass zur Gefahrbeseitigung diplomatische Bemühungen um einen international verbindlichen Internetstandard erforderlich wären. Selbst wenn man jedoch die internationale Dimension außer Acht lässt, so wäre doch wenigstens ein deutschlandweites Vorgehen gegen die Access-Provider erforderlich gewesen, um eine erhebliche Verringerung der Gefahr zu erreichen. Denn nach derzeitiger Sachlage steht jedem Nutzer neben den technischen Umgehungsmöglichkeiten der Sperrung noch eine denkbar einfache weitere Möglichkeit zur Verfügung: Er kann zu einem in einem anderen Bundesland ansässigen Access-Provider wechseln. Demgegenüber erscheint es formalistisch, wenn die Bezirksregierung sich auf die begrenzte Reichweite der nordrhein-westfälischen Ordnungsgewalt beruft. Im Rahmen des kooperativen Föderalismus gab es vor Erlass der Sperrverfügung mannigfaltige Möglichkeiten zu einem deutschlandweit abgestimmten Vorgehen, beispielsweise im Rahmen der Innenministerkonferenz der Länder. Hätte die Bezirksregierung die Gefahr konsequent reduzieren wollen, hätte sie diese Möglichkeiten nutzen und zusammen mit den anderen Bundesländern ein effektives Konzept entwickeln müssen. Insgesamt erweist sich die Düsseldorfer Sperrverfügung deshalb aufgrund der Umgehungsmöglichkeiten als unverhältnismäßig.

bb. Verstoß gegen Übermaßverbot und Zensurverbot

Hinzu kommt ein weiteres: Nach der Verfügung der Bezirksregierung müssen nicht konkrete Inhalte, sondern ganze Internet-Adressen (URLs) gesperrt werden. Die Sperrungen ganzer URLs verstoßen jedoch gegen das Zensurverbot des Art. 5 Abs. 1 Satz 3 GG. Die konkreten Inhalte, die unter den betreffenden URLs abrufbar sind, werden von den Content-Providern in unregelmäßigen Abständen „gepflegt", d.h. aktualisiert und ausgewechselt. Von der URL-Sperrung werden folglich auch Inhalte erfasst, die erst zukünftig in Folge der Site-Pflege auf den betreffenden Seiten eingestellt werden. Da die Bezirksregierung durch ihre Verfügung mithin die Veröffentlichung der betreffenden Inhalte ex ante unterbindet, übt sie eine Vorzensur aus. Die Vorzensur ist jedoch nach Art. 5 Abs. 1 Satz 3 GG ausnahmslos verboten[48].

Weiterhin sind unter den betroffenen URLs mehrere hundert Einzelinhalte abrufbar. Die Bezirksregierung hat niemals dargelegt, dass sämtliche dieser Einzelinhalte rechtswidrig sind, sondern immer nur mit einigen wenigen Inhalten argumentiert, die unzweifelhaft gegen deutsches Recht verstoßen. Soweit indessen rechtmäßige Inhalte von der Sperrung betroffen werden, verstößt die Verfügung gegen das Übermaßverbot

(48) Bethge, in: Sachs, GG-Kommentar, Art. 5, Rn. 129 ff.; Schulze-Fielitz, in: Dreier, GG-Kommentar, Art. 5 Abs. 1 und 2, Rn. 138 ff.; Starck, in: v. Mangoldt/Klein/Starck, GG-Kommentar, 3. Auflage, Art. 5 Abs. 1 und 2, Rn. 156.

und greift in ungerechtfertigter Weise in die durch Art. 5 Abs. 1 Satz 1 GG geschützte Informationsfreiheit der Internetnutzer ein[49]. Im Lichte des Zensurverbots des Art. 5 Abs. 1 Satz 3 GG und des Übermaßverbotes ist § 22 Abs. 3 MDStV folglich verfassungskonform dahingehend auszulegen, dass - soweit dies technisch möglich ist - höchstens die Sperrung konkreter, bereits in das Internet eingestellter Inhalte, nicht aber die Sperrung ganzer URLs (mit wechselnden Inhalten) angeordnet werden darf[50]. Ist die Bezirksregierung aber der Auffassung, dass derzeit keine technischen Möglichkeiten zur Sperrung konkreter Inhalte, etwa in Gestalt leistungsfähiger Filterprogramme, zur Verfügung stehen, hätte sie sich einer Sperrverfügung bis zur Praxisreife derartiger Systeme enthalten müssen, statt auf die zensorische Sperrung ganzer URLs auszuweichen.

4.3.4 Inanspruchnahme allenfalls als Nichtstörer

Selbst wenn – entgegen der hier vertretenen Auffassung – ein behördliches Vorgehen gegen die Access-Provider möglich wäre, könnten diese jedenfalls nicht als Störer in Anspruch genommen werden. Denn nach § 22 Abs. 3 MDStV ist allenfalls die Inanspruchnahme von Access-Providern als Nichtstörer möglich[51]. Dies ergibt sich aus der Regelungssystematik des MDStV: In § 6 ff. MDStV ist die Verantwortlichkeit der verschiedenen Anbieter geregelt. § 7 MDStV bestimmt dabei ausdrücklich, dass Anbieter für fremde Inhalte, zu denen sie lediglich den Zugang vermitteln, nicht verantwortlich sind, wenn sie die Übermittlung nicht veranlasst, den Adressaten nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben, was alles bei den betroffenen Providern nicht der Fall ist. § 22 MDStV regelt demgegenüber die Adressaten von Ordnungsverfügungen. Nach der grundsätzlichen Regelung der § 22 Abs. 2 i.V.m. § 22 Abs. 3 Satz 1, 1. Halbsatz MDStV korrespondiert die Adressateneigenschaft mit der Verantwortlichkeit des Anbieters. Von dieser Regel macht § 22 Abs. 3 Satz 1, 2. Halbsatz MDStV jedoch eine Ausnahme, in dem die Norm ausnahmsweise und subsidiär auch eine Ordnungsverfügung gegen den Nicht-Verantwortlichen erlaubt. Dies ändert indessen nichts daran, dass ein Zugangsvermittler gemäß der – ausnahmslos geltenden – Regelung des § 7 MDStV nicht verantwortlich ist[52].

(49) Sieber, Verantwortlichkeit im Internet, München 1999, 210; Stadler, Haftung für Informationen im Internet, Berlin 2002, 125.
(50) Vgl. auch Stadler, MMR 2002, 343.
(51) Wimmer, ZUM 1999, 441; Spindler/Volkmann, K&R 2002, 398 (404 ff.); Stadler, MMR 2002, 343 (347); im Ergebnis auch Koenig/Loetz, CR 1999, 438 (442).
(52) Vgl. Vesting, in: Roßnagel, Recht der Multimedia-Dienste, München 2001, § 18 MDStV, Rn. 38 („Divergenz von Haftung und Aufsicht").

Der nichtverantwortliche Adressat einer Ordnungsverfügung ist jedoch nach den Regeln des Ordnungsrechts ein Nichtstörer[53]. Die Inanspruchnahme eines Nichtstörers ist nur unter erheblich strengeren Voraussetzungen als die Inanspruchnahme eines Verantwortlichen zulässig[54]. Auf diese Frage ist die Bezirksregierung nicht eingegangen. Zudem löst die Inanspruchnahme eines Nichtstörers einen Entschädigungsanspruch aus. Diese Entschädigung ist - entsprechend dem Rechtsgedanken des enteignenden Eingriffs - deshalb gerechtfertigt, weil dem Access-Provider durch seine Inanspruchnahme ein Sonderopfer auferlegt wird. Der Anspruch ist auf Ausgleich des Vermögensschadens gerichtet, der dem Nichtstörer unmittelbar durch die ordnungsbehördliche Maßnahme entstanden ist. Folglich wären den Access-Providern im Fall der Düsseldorfer Sperrverfügung zumindest die Kosten für die Anschaffung und Implementierung der zur Sperrung notwendigen Infrastruktur (Hard- und Software) und der bei der Abwicklung der Sperrung entstandene Personalaufwand zu ersetzen.

4.3.5 Fazit

Die im Eilverfahren unterlegenen Provider dürften den Hauptsacheverfahren nicht allzu euphorisch entgegen sehen, nachdem die Verwaltungsgerichte ihrer Argumentation bereits in den Eilverfahren nicht gefolgt waren und sich hierin vom OVG Nordrhein-Westfalen bestätigt sehen. Immerhin können diese Provider hoffen, von den Gerichten als Nichtstörer qualifiziert zu werden und deshalb Kostenersatz für die Sperrungsmaßnahmen zu erhalten. Das OVG Nordrhein-Westfalen hat die Frage des Entschädigungsanspruchs ausdrücklich offen gelassen[55]. Eine Behandlung von Access-Providern als Nichtstörer wäre nicht nur rechtlich zutreffend, sondern würde wohl in der Zukunft schon aus fiskalischen Erwägungen einer ausufernden Sperrungspraxis der Internetaufsicht Einhalt gebieten.

Zudem muss sich die Internetaufsicht aus Münster ins Stammbuch schreiben lassen, zukünftig die Verhältnisse bei den Providern genau zu untersuchen. Dies gilt nicht nur für die Qualifikation als Access- oder Netzwerk-Provider. Das OVG hat die Verhältnismäßigkeit der Verfügung gegenüber dem im Eilverfahren erfolgreichen Provider auch deshalb bezweifelt, weil dessen Netz über viele hundert Domain-Name-Server und Router-Rechner verfügt, deren technische Anpassung einen weit höheren Aufwand bedeutet hätte, als die Bezirksregierung zunächst wahrhaben wollte. Es kommt also auch auf die individuellen technischen Gegebenheiten an.

(53) § 19 OBG NRW über den Nichtstörer lautet: „Die Ordnungsbehörde kann Maßnahmen gegen andere Personen als die nach den § 17 [scil.: Verhaltensstörer] und § 18 [scil.: Zustandsstörer] Verantwortlichen richten, wenn [...]" (Hervorhebungen durch Verf.; siehe auch § 6 PolG).

(54) Koenig/Loetz, CR 1999, 438 (442); Spindler/Volkmann; K&R 2002, 398 (404 f.).

(55) Beschl. v. 19.3.2003, Az. 8 B 2567, Umdruck, S. 18 und 23.

4.4 Sperrverfügungen und ihre rechtliche Einordnung

Christian Volkmann

4.4.1 Einleitung

Im Februar 2002 verfügte die Bezirksregierung Düsseldorf die Sperrung von zwei amerikanischen Websites mit jeweils rechtsradikalen Inhalten. Adressaten der Maßnahme waren eine Vielzahl von in Nordrhein-Westfalen ansässigen Internet-Zugangsvermittlern. Die erhobenen Widersprüche hat die Behörde zurückgewiesen; der erste rechtskräftige Beschluss ist ergangen[56].

Sperrverfügungen gegen Access-Provider sind mit Problemen auf nahezu allen Ebenen im Prüfungsaufbau der materiellen Rechtmäßigkeit eines ordnungsrechtlichen Verwaltungsaktes behaftet. Schon die Bestimmung der richtigen Ermächtigungsgrundlage ist problematisch, gleiches gilt für die Störereigenschaft der Access-Provider sowie die Verhältnismäßigkeit der vorgeschlagenen Maßnahmen.

4.4.2 Die richtige Ermächtigungsgrundlage für Sperrverfügungen

Sperrverfügungen bedürfen als Verwaltungsakte im Bereich der Gefahrenabwehr einer Ermächtigungsgrundlage. Im Gegensatz zum Teledienstegesetz (TDG) hält der Mediendienstestaatsvertrag (MDStV) mit § 22 eine - gegenüber der polizei- und ordnungsrechtlichen Generalklausel spezielle - Rechtsgrundlage zur Gefahrenabwehr im Netz bereit. Diese umfasst in Abs. 3 ausdrücklich auch Maßnahmen gegen Access-Provider. Dennoch scheint das Access-Providing nicht in den gesetzlichen Anwendungsbereich des Staatsvertrages zu passen. Denn diese Provider bieten keine an die Allgemeinheit gerichteten, redaktionell gestalteten Beiträge zur Meinungsbildung an. Sie vermitteln den Zugang zu solchen Angeboten, d.h. sie übermitteln Daten. Die bloße Datenübermittlung ist aber als Akt der Telekommunikation kein Mediendienst. Das spricht eigentlich schon gegen die Anwendung des Mediendiensterechts auf die Access-Provider und damit auch gegen § 22 Abs. 3 MDStV als spezielle Ermächtigungsgrundlage für entsprechende Maßnahmen. Als Rückgriff für Sperrverfügungen gegen Mediendienste bliebe allein die ordnungsrechtliche Generalklausel. Dass die Access-Provider wegen des eindeutigen Telekommunikationsbezuges und der Ausschlussklausel des § 2 Abs. 4 Nr. 1 TDG auch nicht in den Anwendungsbereich des TDG fallen, ist im Hinblick auf die Bestimmung der richtigen Ermächtigungsgrundlage allerdings ohne Bedeutung. Denn in Ermangelung einer im TDG geregelten Ermächtigungsgrundlage für ein ordnungsrechtliches Vorgehen gegen Teledienste, kann sowohl im Falle des

56) OVG Münster, MMR 2003, 348 ff. m. Anm. Spindler/Volkmann (S. 353)

Anwendungsbereichs des TKG als auch des TDG die polizei- und ordnungsrechtliche Generalklausel als Rechtsgrundlage herangezogen werden.

a. Abgrenzung § 14 OBG NRW - § 22 MDStV

Obwohl Access-Provider weder Medien- noch Teledienste, sondern Telekommunikationsdienste sind, rechtfertigt sich die Eröffnung der Anwendungsbereiche des MDStV und des TDG und damit auch die Heranziehung des § 22 Abs. 3 MDStV als Ermächtigungsgrundlage für Sperrverfügungen. Denn wäre der Anwendungsbereich von TDG und MDStV für Access-Provider ausgeschlossen, könnten diese Anbieter konsequenterweise auch nicht in den Genuss der dort ebenfalls geregelten Haftungsprivilegierungen kommen. Diese sind aber nicht nur auf Content- und Host- sondern eben auch auf das Access-Providing ausgerichtet. Dieser schon nach TDG a.F. und MDStV a.F. in deren jeweiligen §§ 5 Abs. 3 normierte Umstand wird nunmehr auch von der E-Commerce-Richtlinie in Art 12 ausdrücklich verlangt[57]. Access-Provider müssen daher richtlinienkonform in TDG und MDStV in der Haftung privilegiert sein. Kehrseite dieser Medaille sind dann aber auch die dort enthaltenen Sperrungsverpflichtungen mit der hiermit korrelierenden behördlichen Anordnungsbefugnis nach § 22 MDStV.

Zieht man die Trennlinie zwischen Telekommunikations- und Teledienst/Mediendienstrecht nunmehr anhand der Unterscheidung von Technik und Inhalten, ergibt sich eine Abgrenzung von TDG und MDStV, welche nicht auf die Person des Access-Providers abstellt, sondern auf den konkreten Inhalt, zu dem im Einzelfall der Zugang vermittelt wird[58]. Ist dieser Inhalt ein Mediendienst, so ist § 22 MDStV die richtige Eingriffsgrundlage. Ist es ein Teledienst, kommt mangels einer dem § 22 MDStV entsprechenden spezialgesetzlichen Regelung die ordnungs- und polizeirechtliche Generalklausel zur Anwendung.

b. Rassistische und fremdenfeindliche Homepages als Tele- oder Mediendienste?

Da die Abgrenzung von TDG und MDStV anhand des vermittelten Inhaltes erfolgt, ist zur Bestimmung der richtigen Ermächtigungsgrundlage in der schulmäßigen juristischen Subsumtion an dieser Stelle ein Eingehen auf die zu sperrenden Seiten nötig. Ob Homepages Mediendienste oder Teledienste sind und wie es sich mit dieser Frage im Einzelnen bei den zu sperrenden Seiten verhält übersteigt den abstrakten Rahmen dieses Beitrages und ist zudem nach wie vor nicht ganz unproblematisch. Letztlich ist eine Unterscheidung aber auch nicht von großer Bedeutung für die öffentlich-rechtliche Praxis. Denn allgemeines Ordnungsrecht und Länderstaatsvertrag liegen in ihren jeweiligen Anforderungen an die Sperrverfügungen nicht weit auseinander.

(57) Spindler, MMR 2000 Beilage Nr. 7, 4 (17); Freytag, CR 2000, 600 (606); Satzger, CR 2000, 109 (116 f.).
(58) Spindler/Volkmann, K&R 2002, 398 (399 f.) m.w.N.; OVG Münster MMR 2003, 348 (348 f.)

4.4.3 Materielle Voraussetzungen der Ermächtigungsgrundlagen

Die Sperrung eines Teledienstes nach der Generalklausel kann dann verfügt werden, wenn die öffentliche Sicherheit gefährdet ist. Gefahr ist eine Sachlage, die in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden für die öffentliche Sicherheit oder Ordnung führen würde[59]. Die öffentliche Sicherheit umfasst die Unverletzlichkeit der subjektiven Rechte und Rechtsgüter des Einzelnen, der objektiven Rechtsordnung sowie den Bestand und das Funktionieren des Staates und seiner Einrichtungen[60]. Damit verweist der Begriff der öffentlichen Sicherheit auf die Gesamtheit der öffentlich-rechtlichen Rechtsnormen[61].

Eine Gefahr für die öffentliche Sicherheit ist ohne weiteres zu bejahen, wenn volksverhetzende Inhalte von der Sperrung getroffen werden. § 22 MDStV setzt im Gegensatz zum allgemeinen Ordnungsrecht keine bloße Gefahr für die öffentliche Sicherheit oder Ordnung voraus, sondern noch weitergehend einen Verstoß gegen bestimmte (und zwar die in § 22 Abs. 2, S. 1 MDStV gerade nicht genannten) Vorschriften des Vertrages. Da dort aber § 11 auf die gesamte verfassungsmäßige Ordnung verweist und damit etwa auch beim Tatbestand der Volksverhetzung einspringt, ist dies letztendlich nur ein formaler Unterschied zum allgemeinen Ordnungsrecht.

a. Der Geltungsbereich des Ordnungsrechts

Zur Eröffnung des Geltungsbereichs nationalen Ordnungsrechts muss sich die Gefahr in Deutschland verwirklichen. Dies ist auch bei Inhalten der Fall, die auf ausländischen Servern gespeichert sind, sofern sie im Inland abgerufen werden können[62]. Der Geltungsbereich des deutschen Ordnungsrechts ist unter dem Stichpunkt der Inlandsauswirkung einer Gefahr - ähnlich dem Kartellrecht[63], dem Wettbewerbsrecht[64] oder dem Kapitalmarktrecht[65]- eröffnet. Dies hat der BGH kürzlich auch für das Strafrecht entschieden als es um die Verbreitung der Auschwitz-Lüge über das Internet ging[66]. Das Gericht setzte hier voraus, dass die volksverhetzende Äußerung konkret zur

(59) Ausdrücklich: §§ 2 Nr. 1a NGefAG, 2 Nr. 3a brPolG, 3 Nr. 3a SOG LSA, 54 Nr. 3a thürOBG; allgemein zum Gefahrenbegriff BVerwGE 45, 51, 57; Drews/Wacke/Vogel/Martens, Gefahrenabwehr, 1986, 220 ff.; Gusy, Polizeirecht, 4. Aufl., 2000, Rn. 318 ff.; Denninger in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 3. Aufl., 2001, Kap. E., Rn. 29 ff.; Schuppert, Verwaltungswissenschaften, 2000, 84 f.; Götz, Allgemeines Polizei- und Ordnungsrecht, 13. Aufl., 2001, Rn. 140; Röhrig, DVBl 2000, 1658.

(60) Götz (a.a.O.), Rn. 89.

(61) Drews/Wacke/Vogel/Martens (a.a.O.), 236.

(62) Siehe auch: Germann, Gefahrenabwehr und Strafverfolgung im Internet, 2000, 237.

(63) Vgl. zum Begriff der Inlandsauswirkung im Kartellrecht: Rehbinder in: Immenga/Mestmäcker, GWB – Kommentar, 3. Aufl., § 130 II, Rn. 39 ff.; BGHSt 25, 208 (212) – Ölfeldrohre; BGHZ 74, 322 – Organische Pigmente; BKartA, WuW/E 1971, 1376 (1383) – Linoleum.

(64) Vgl. hierzu: BGHZ 35, 329 (333); BGH NJW 1988, 664 (665); BGH GRUR 1995, 424 (425).

(65) Vgl. hierzu: Spindler, WM 2001, 1689 (1700).

(66) Vgl. zur Auschwitz-Lüge und der internationalen Anwendbarkeit des deutschen Strafrechts im Rahmen des Tatortprinzips: BGH NJW 2001, 624 (627) = CR 2001, 260 (m. Anm. v. Vassilaki) = MMR 2001, 228 (m. Anm. v. Clauß) = NStZ 2001, 305 (m. Anm. v. Hörnle).

Friedensstörung im Inland geeignet ist[67]. Wenn derartige Inhalte verbreitet werden, ist auch eine Gefahr für die öffentliche Sicherheit und Ordnung im Sinne der ordnungsrechtlichen Generalklausel ohne weiteres zu bejahen[68]. Ebenfalls ist dann ein Verstoß zumindest gegen § 11 MDStV gegeben, was im Falle der Sperrung eines Mediendienstes wiederum den Anwendungsbereich des § 22 MDStV eröffnet.

b. Die Haftungsprivilegierungen des TDG und des MDStV im Ordnungsrecht

Die Verantwortlichkeit der Access-Provider für die Inhalte anderer wird schon seit langem sowohl im Zivil- als auch im Strafrecht diskutiert. Die Haftungsprivilegierungen in TDG und MDStV haben hier die Rechtsprobleme, jedenfalls was die verschuldensabhängige Haftung angeht, zumindest etwas entschärft. Im Vergleich zu diesen beiden Rechtsgebieten besteht im öffentlichen Recht aber ein entscheidender Unterschied: Die Haftungsprivilegierungen in TDG und MDStV finden gem. § 8 II 2 TDG und § 6 II 2 MDStV im Bereich der Störerhaftung und damit auch im öffentlich-rechtlichen Gefahrenabwehrrecht keine Anwendung. Im Vergleich zur früheren Rechtslage unter TDG a.F. und MDStV a.F., stellt dies in praxi jedoch keine Haftungsverschärfung dar. Die hiernach noch gem. § 5 IV TDG a.F. und § 18 III MDStV a.F. erforderliche Kenntnis konnte regelmäßig schon mit der Verfügung selbst hergestellt werden[69].

4.4.4 Die Störerauswahl

Zur Störerauswahl unterscheidet das Polizei- und Ordnungsrecht traditionell die Verhaltens-, Zustands- und Nichtstörer. Die Aufteilung der ordnungsrechtlich Verantwortlichen unter den Providern wird zumeist dem bekannten Dreiklang aus dem Ordnungsrecht eins zu eins angepasst: Der Content-Provider ist Verhaltensstörer, der Host Provider Zustandsstörer und der Access-Provider Nichtstörer[70]. Soweit die Access-Provider betroffen sind, ist diese Einordnung richtig[71]. Eine Zustandshaftung kommt nicht in Betracht. Als Zustandsstörer haftet nur, wer die tatsächliche Sachherrschaft über eine gefährliche Sache hat. Die Infrastruktur aber, über welche die Zugangsvermittlung stattfindet und welche der Access-Provider beherrscht, ist als Sache nicht gefährlich. Erst wenn rechtswidrige Inhalte über die Leitung befördert werden, kann diese überhaupt erst als gefährlich eingestuft werden. Zu diesem Zeitpunkt aber hat der Access-Provider zwar Sachherrschaft über seine Leitung, nicht aber über die durch diese transportierten Inhalte. Der Access-Provider ist nicht in

(67) BGH NJW 2001, 624; siehe zu dieser Problematik auch: Hörnle, NJW 2002, 1008 (1013).
(68) Spindler/Volkmann, K&R 2002, 398 (400).
(69) Spindler, NJW 1997, 3193 (3196); Koch, CR 1997, 193 (199); Zimmermann, NJW 1999, 3145 (3148).
(70) Wimmer, ZUM 1999, 436 (441); Zimmermann NJW 1999, 3145 (3148 f.); Hornig, ZUM 2001, 846 (856).
(71) Ebenso: Zimmermann, NJW 1999, 3145 (3148); Hornig, ZUM 2001, 846 (856); insoweit zutreffend: Stadler, MMR 2002, 343 (344).

der Lage rechtswidrige Inhalte in seinem Leitungsnetz zu bekämpfen, da er lediglich den Nutzer von den Inhalten abschotten und insoweit allein den Aufruf einer Seite verhindern kann[72].

4.4.5 Die Notstandshaftung im Netz

Die Eigenschaft der Access-Provider als Nichtstörer bringt im Fall ihrer ordnungsrechtlichen Inanspruchnahme zunächst Entschädigungsansprüche mit sich. Dies ist in den Polizei- und Ordnungsgesetzen der Länder ausdrücklich so geregelt[73]. Fehlt eine gesetzliche Regelung, wie etwa im MDStV, so folgt die staatliche Verantwortlichkeit entweder aus einer analogen Anwendung der entsprechenden ordnungs- und polizeirechtlichen Vorschriften[74] oder aber aus dem allgemeinen Aufopferungsanspruch[75]. Aber der Entschädigungsanspruch entbindet nicht vom Vorliegen der besonderen Voraussetzungen der Notstandshaftung. Diese sind erheblich strenger als die der Verhaltens- und Zustandsverantwortlichkeit. Zu nennen sind hier insbesondere höhere Anforderungen an den Gefahrentatbestand sowie der Grundsatz der Subsidiarität, d.h. die vorrangige Haftung von Verhaltens- und Zustandsstörer.

a. Erhebliche Gefahr

Nach den Polizei- und Ordnungsgesetzen der Länder ist für die Heranziehung eines Nichtstörers nicht nur eine bloße Gefahr erforderlich, sondern eine erhebliche Gefahr, d.h. eine Gefahr für bedeutsame Rechtsgüter[76]. Dass solche bedeutsamen Rechtsgüter durch Internet-Inhalte – etwa im Falle des Tatbestandes der Volksverhetzung – betroffen sein können, ist wiederum eine Frage des konkreten Inhaltes einer Website und an dieser Stelle nicht zu bestreiten.

Der Staatsvertrag scheint im Gegensatz zu den allgemeinen Regelungen der Notstandshaftung eine Gefahr für bedeutsame Rechtsgüter nicht zu verlangen. Durch den Verweis auf die gesamte verfassungsmäßige Rechtsordnung in § 11 scheint der ordnungsrechtliche Notstand vielmehr schon bei jeder bloßen Gesetzesverletzung einzutreten. Die Voraussetzungen der Inanspruchnahme der Access-Provider nach

(72) So auch: Stadler, Haftung für Informationen im Internet, 2002, Rn. 127.

(73) § 51 BGSG, Art 70 bay PAG, §§ 55 bad- württ PolG; 59 ASOG (Bln); 38 bbgOBG, 56 I brem PolG; 10 III Hmb SOG; 64 HSOG; 72 SOG MV; 80 I NGefAG; 39 I a OBG NRW; 68 I 1 POG RP; 68 SPolG; 52 I Sächs PolG; 69 SOG LSA; 221 LVwG SH; 68 Thür PAG, 52 Thür OBG.

(74) Zimmermann, NJW 1999, 3145 (3149); Stadler (a.a.O.), Rn. 140.

(75) Vgl. zum Aufopferungsentschädigungsanspruch des Nichtstörers: Schenke, in: Steiner, Besonderes Verwaltungsrecht, 1999, Rn. 347; Friauf, in: Schmidt-Aßmann, Besonderes Verwaltungsrecht, 11. Aufl., Rn. 116; Götz (a.a.O.), Rn. 429; Rachor, in: Lisken/Denninger, (a.a.O.), Kapitel L, Rn. 33; Rüfner, in: Erichsen, Allgemeines Verwaltungsrecht, 11. Aufl., Rn. 82 ff.

(76) Vgl. Götz (a.a.O.), Rn. 266: Hierzu gehören etwa der Bestand des Staates, Leben, Gesundheit, Freiheit, nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter.

§ 22 Abs. 3 MDStV scheinen gegenüber dem allgemeinen Ordnungsrecht mit dem Erfordernis der erheblichen Gefahr dadurch sehr viel weiter zu sein. Der polizeiliche Notstand ist aber auch im Mediendiensterecht als eben solcher und damit als Ausnahmefall zu behandeln[77]. § 11 MDStV kann zwar für Verhaltens- und Zustandsstörer – im übrigen genauso wie im allgemeinen Ordnungsrecht – eine Verantwortlichkeit nach dem MDStV schon bei der Verletzung von jeder erdenklichen Rechtsnorm begründen. Für in Anspruch genommene Nichtstörer geht § 11 MDStV indes zu weit[78]. Nur wenn bedeutsame Rechtsgüter gefährdet sind, rechtfertigt sich eine Notstandspflicht. Bedeutsame Rechtsgüter zählt freilich § 12 Abs. 1 MDStV auf; für die Beurteilung der erheblichen Gefahr kann die Vorschrift als Richtschnur dienen.

b. Die Subsidiarität in der Notstandshaftung

Neben diesem Erfordernis der erheblichen Gefahr gilt der Grundsatz der Subsidiarität der Nichtstörerhaftung. Dieser ist nun nicht nur im Ordnungsrecht, sondern auch ausdrücklich in § 22 Abs. 3 des Staatsvertrages festgeschrieben. Nur wenn ein Vorgehen gegen Verhaltens- oder Zustandsstörer erfolglos oder von vornherein aussichtslos ist, können dem Nichtstörer überhaupt Maßnahmen auferlegt werden. Bei Inhalten, die auf Servern in Deutschland liegen, dürfte eine Inanspruchnahme der Access-Provider daher in den meisten Fällen ausscheiden. Und bei Auslandsinhalten muss die Behörde zunächst einmal versuchen, mit Amts- und Rechtshilfe an Content-Provider und Hosts heranzukommen[79]. Dass hierdurch die Ausnahme, Nichtstörerhaftung, zur Regel wird, muss nicht unbedingt sein. Entsprechenden – und sicherlich dann auch schädlichen Tendenzen – könnten die Gerichte durchaus begegnen.

4.4.6 Verhältnismäßigkeit von Sperrverfügungen

Die Diskussion um die Sperrverfügungen dreht sich um drei mögliche Verpflichtungen der Access-Provider:

Erstens: Als Eingriff am Domain-Name-Server und der damit verbundenen Verhinderung der Umwandlung der sog. URL in eine IP-Adresse;

Zweitens: Durch Zwischenschaltung eines Proxy-Servers, der den Datenstrom zunächst unterbrechen könnte, um dann unter der Verwendung von vordefinierten Regelwerken bestimmte Inhalte auszufiltern;

(77) Denninger, in: Lisken/Denninger (a.a.O.), Kapitel E, Rn. 126.
(78) Spindler/Volkmann, K&R 2002, 398 (404).
(79) So auch Mayer, Das Internet im öffentlichen Recht, 1999, 230.

Drittens: Als Blockade von IP-Adressen; hier würde die Anfrage des Nutzers erst gar nicht zum Zielrechner weitergeleitet werden. Der gesamte Zielrechner wäre für den User unerreichbar.

a. Geeignetheit

Alle drei Maßnahmen sind relativ leicht zu umgehen. Dass eine endgültige Gefahrenbeseitigung durch die Sperrverfügungen nicht möglich ist, kann daher auch nicht ernsthaft bestritten werden[80]. Für die Geeignetheit von behördlichen Anordnungen ist dies aber auch nicht erforderlich. Es genügt die ausreichende Verminderung der Gefahr[81]. Und bei allen technischen Bedenken dürfte ein Teil der Nutzer tatsächlich nicht in der Lage sein, diese Sperrungen zu umgehen. Ein anderer Teil verspürt vielleicht keine Motivation Maßnahmen zu ergreifen, mit denen er wieder Zugriff auf die gesperrten Inhalte erlangen könnte, und manch ein Nutzer wird durch Sperrungen womöglich auch an Moral und Ethik gepackt. Festzuhalten bleibt jedenfalls, dass der zeitliche und intellektuelle Aufwand, der zum Zugriff auf eine gesperrte Seite betrieben werden muss, höher ist, als der www-Aufruf einer nicht gesperrten Seite. Die von der Bezirksregierung Düsseldorf vorgeschlagenen Maßnahmen zur Gefahrenbeseitigung - der Eingriff am Domain-Name-Server, die Zwischenschaltung eines Proxy-Servers sowie die Blockade von IP-Adressen - sind daher allesamt geeignet, die von Inhalten ausgehenden Gefahren, wenn schon nicht zu beseitigen, so doch wenigstens zu minimieren[82].

b. Angemessenheit

Die Verhältnismäßigkeitsprüfung dreht sich schwerpunktmäßig um die Rechtfertigung von Eingriffen in die ohne weiteres betroffenen Grundrechte wie Eigentums- und Berufsfreiheit der Access-Provider, Meinungs- Presse- und/oder Rundfunkfreiheit der Content- und Host-Provider sowie die Informationsfreiheit der Internet-Nutzer.
Auch das Zensurverbot findet langsam Eingang in die fachjuristische Auseinandersetzung um Löschungen und Sperrungen im Internet. Mit der zur Zeit (noch) gängigen und höchstrichterlichen Auffassung, dass vom grundrechtlich verbürgten Zensurverbot nur die sog. Vor- oder Präventivzensur, d.h. die staatliche Kontrolle von Presseerzeugnissen vor deren Veröffentlichung[83], erfasst ist, ist ein Verstoß gegen das Zensurverbot des Art 5 Abs. 1 Satz 3 GG durch Sperrungsmaßnahmen nicht zu bejahen.

(80) Vgl. allgemein zu den Sperrungen im Internet sowie zu deren Umgehung: Köhntopp/Köhntopp/Seeger, K&R 1998, 25 (29ff.); Sieber, CR 1997, 581 ff. und 653 ff.; Federrath, ZUM 1999, 177 ff.

(81) Hornig, ZUM 2001, 846 (852); Zimmermann, NJW 1999, 3145 (3150); Rachor, in: Lisken/Denninger (a.a.O.), Kapitel F, Rn. 222.

(82) Spindler/Volkmann (a.a.O.), 398 (404); OVG Münster, MMR 2003, 348 (351 f.).

(83) Ausdrücklich: BVerfGE 87, 209 (230); vgl. auch BVerfGE 33, 52 (71); BVerfGE 83, 130 (155); Schulze-Fielitz, in: Dreier (Hrsg.), GG-Komm., Bd. 1, 1996, Art 5 I, II, Rn. 139; Starck, in: v. Mangold/Klein/Starck (Hrsg.), GG-Komm., Bd. 1, 1999, Art 5 I, II, Rn. 158; Wendt, in: v.Münch/Kunig, GG-Komm., Bd. 1, 2000, Art 5, Rn. 62; Pieroth/Schlink, Staatsrecht II, 17. Aufl., Rn. 605.

Solange staatliche Verbote erst nach der Publikation erfolgen, wie etwa bei Sperrungen bereits abrufbarer Websites, ist das nach diesen Maßstäben noch keine Zensur[84]. Es sind dann vielmehr die Schranken anderer Grundrechte zu beachten und hier wiederum die der Presse- und der Meinungsfreiheit in Art. 5 Abs. 2 GG[85].

Sämtliche der genannten Grundrechte finden daher ihre Grenzen in den allgemeinen Gesetzen und/oder in kollidierendem Verfassungsrecht. Die erforderliche Interessenabwägung – auch unter Berücksichtigung von Allgemeininteressen wie etwa der Schnelligkeit des allgemeinen Datenverkehrs – ist schwierig. Dies gilt vor allem auch vor dem Hintergrund der nur eingeschränkten Geeignetheit der möglichen Maßnahmen. Die Sperrung ganzer Zielrechner wegen eines gefährlichen Inhaltes als zwangsläufige Nebenwirkung einer Blockade der betreffenden IP-Adresse dürfte mit dem Erfolg der Maßnahme nicht mehr gerechtfertigt sein. Eingriffe am Domain-Name-Server sind weit weniger Erfolg versprechend, auf der anderen Seite aber nicht mit derartig schwerwiegenden Nachteilen verbunden. Am viel versprechendsten ist die Zwischenschaltung von Proxy-Servern. Freilich geht diese Maßnahme mit erheblichen wirtschaftlichen Aufwendungen einher, welche über Entschädigungsansprüche für die Notstandsverpflichtung am Ende den Steuerzahler treffen würden.

Das Opportunitätsprinzip ermöglicht es, die Inanspruchnahme der Access-Provider nach der der Sinnfrage auszurichten. Dies sollte in der aktuellen Diskussion nicht aus den Augen verloren werden.

(84) Siehe zur anderen, im Vordringen begriffenen Auffassung insbesondere Hoffmann-Riem, Kommunikationsfreiheiten, 2002, Rn. 89 ff., mit ausdrücklichem Bezug auch auf Internet-Sachverhalte.

(85) BVerfGE 33, 52 (72); Jarass, in: Jarass/Pieroth, GG-Komm., 6. Aufl., 2002, Art. 5, Rn. 63; Schulze-Fielitz (Fn. 81), Art 5 I, II, Rn. 139; Wendt (Fn. 81), Art 5, Rn. 62; Pieroth/Schlink (a.a.O.), Rn. 604.

4.5 Sperrverfügungen im Lichte der aktuellen Rechtsprechung

Sandra Brüggemann

4.5.1 Einleitung

Die Bezirksregierung Düsseldorf, Medienaufsichtsbehörde für Nordrhein-Westfalen, hatte im Februar 2002 sämtlichen nordrhein-westfälischen Access-Providern aufgegeben, zwei rechtsextremistische Internet-Homepages – „nazi-lauck-nsdapao" und „stormfront" – zu sperren. Im Unterschied zu den sog. Content- und Service-Providern vermitteln die Access-Provider lediglich den Zugang zu den inkriminierten Homepages.

Die Hälfte der angeschriebenen Provider hat die beiden Homepages aufgrund der Verfügung gesperrt. Alle anderen haben Widerspruch erhoben, welche von der Bezirksregierung Düsseldorf als unbegründet zurückgewiesen wurden. Gegenüber den 16 daraufhin klagenden Providern ordnete die Bezirksregierung Düsseldorf im Oktober 2002 die sofortige Vollziehung ihrer Sperrverfügung an. Damit sollte verhindert werden, dass die Anbieter die strafbaren Webseiten bis zum rechtskräftigen Abschluss der Gerichtsverfahren weiter verbreiten. Die Provider haben daraufhin bei den Verwaltungsgerichten einstweiligen Rechtsschutz beantragt.

Während die Verwaltungsgerichte Arnsberg[86], Gelsenkirchen[87], Düsseldorf[88], Aachen[89] und Köln[90] die Vollziehungsanordnung der Bezirksregierung Düsseldorf in den einstweiligen Rechtsschutzverfahren materiell bestätigt haben, hat das Verwaltungsgericht Minden[91] dem Aussetzungsantrag des Antrag stellenden Providers stattgegeben[92]. Auch das Oberverwaltungsgericht Münster – in den Eilverfahren die letzte Gerichtsinstanz – hat nunmehr entschieden[93]: Die beiden Websites müssen von den Access-Providern vorerst gesperrt werden.

(86) Az.: 13 L 1848/02 v. 6.12.2002.
(87) Az.: 1 L 2528/02 und 1 L 2547/02, beide v. 18.12.2002.
(88) Az.: 15 L 3749/02, 15 L 4148/02 und 15 L 4149/02, alle v. 19.12.2002.
(89) Az.: 8 L 1028/02 und 8 L 1284/02, beide v. 5.2.2003.
(90) Az.: 6 L 2495/02 v. 7.2.2003.
(91) Az.: 11 L 1110/02 v. 31.10.2002.
(92) Sämtliche Verwaltungsgerichtsentscheidungen sind im Internet abrufbar unter: http://www.brd.nrw.de/BezRegDdorf/hierarchie/themen/Sicherheit_und_Ordnung/Medienmissbrauch/Gerichtliche_Entscheidungen_zu_den_Sperrverf__gungen_bzgl_rechtsextremistischer_Internet___Inhalte.php.
(93) Az.: 8 B 2567/02, siehe Anhang.

4.5.2 Gegenstände des Rechtsstreits

a. Anwendbarkeit des MDStV

Die Bezirksregierung Düsseldorf stützt ihre Sperrverfügung auf § 22 Abs. 3 Mediendienste-Staatsvertrag (MDStV). Nach dieser Vorschrift können Maßnahmen zur Sperrung von Angeboten, die gegen den MDStV verstoßen, auch gegen Mediendiensteanbieter von fremden Inhalten gerichtet werden, vorausgesetzt, Maßnahmen gegenüber den Content- und Service-Providern erweisen sich als nicht durchführbar oder nicht Erfolg versprechend und eine Sperrung ist technisch möglich und zumutbar.

aa. Access-Provider als Diensteanbieter?
Die Access-Provider befürchten für den Fall eines endgültigen Obsiegens der Aufsichtsbehörde, künftig einer Vielzahl von Sperrungsanordnungen und einem damit verbundenen wachsenden Arbeitsaufwand ausgesetzt zu sein. Die Sperrverfügung ist ihrer Ansicht nach in vielerlei Hinsicht rechtswidrig. So halten sie bereits die Ermächtigungsgrundlage (§ 22 Abs. 3 MDStV) für falsch gewählt. Für sie handelt es sich bei den Access-Providern nicht um Diensteanbieter im Sinne des MDStV bzw. des Teledienstegesetzes (TDG), sondern um Unternehmen, die den Usern lediglich die technische Infrastruktur zur Nutzung des Internet zur Verfügung stellen. Daher seien nicht der MDStV oder das TDG, sondern vielmehr das TKG anzuwenden. Für die Aufsichtsbehörde hingegen stellen sich die Access-Provider wegen ihrer zahlreichen Funktionen als typische Diensteanbieter im Sinne des MDStV bzw. des TDG dar. Bei ihnen finde die „Übersetzung" der vom Nutzer eingegebenen www-Adresse in die dazu gehörige IP-Nummer statt. Sie seien es, die über das sog. „Routing" die Verbindung zu dem Server herstellten, bei dem die relevante Seite gespeichert ist. Und auch bei allen weiteren Interaktionen des Users verbinde der Zugangsanbieter diesen mit den jeweiligen Servern. So z.B. wenn der Nutzer von einer Homepage aus über einen dort gesetzten Link zu einer anderen Internetseite gelangen will.

bb. Mediendienste oder Teledienste?

Die Aufsichtsbehörde geht davon aus, dass es sich bei den zu sperrenden Websites um Medien-, nicht aber um Teledienste handelt, mit der Folge, dass der MDStV, nicht aber das TDG anzuwenden sei. Ihrer Ansicht nach sind die Seiten redaktionell gestaltet und richten sich an die Allgemeinheit, sodass die Voraussetzungen eines Mediendienstes erfüllt seien. Nach Auffassung der Provider hingegen steht die individuelle Nutzung der beiden Websites im Vordergrund, sodass sie Teledienste i.S.d. § 2 Abs. 2 Ziff. 2 TDG seien.

b. Maßnahme durchführbar und Erfolg versprechend?

Nach § 22 Abs. 3 MDStV können Anbieter von fremden Inhalten nur dann in Anspruch genommen werden, wenn sich Maßnahmen gegenüber den primär Verantwortlichen als nicht durchführbar oder nicht Erfolg versprechend erweisen. Diese Voraussetzungen waren nach Ansicht der Aufsichtsbehörde erfüllt. Die eigentlich für den Inhalt der beiden Homepages verantwortlichen rechtsextremistischen Content-Provider blieben anonym, während die Service-Provider mit Sitz in den USA durch das First Amendment der amerikanischen Verfassung geschützt seien. Als einzige Möglichkeit zur Bekämpfung unzulässiger Internetangebote aus dem Ausland komme daher die ordnungsrechtliche Inanspruchnahme der Access-Provider im Inland in Betracht.

Die Provider setzen dem u.a. entgegen, dass die Sperrverfügung dem Sinn und Zweck des MDStV zuwiderlaufe. Der sehe nämlich lediglich eine subsidiäre, also ausnahmsweise Inanspruchnahme der Access-Provider vor. Da der Großteil aller in Deutschland verbotenen Internetinhalten im Ausland ins Netz gestellt werde, sei zu befürchten, dass das Regel-Ausnahme-Verhältnis auf Dauer verkehrt werde und die Access-Provider mit einer Vielzahl von Sperrverfügungen rechnen müssten.

c. Strafrechtlich relevanter Erfolg in Deutschland?

Im Kern stützt sich die Sperrverfügung darauf, dass die beiden Websites gegen Vorschriften des Strafgesetzbuches – und damit auch gegen den MDStV (§ 12 Abs. 1 lit. 1) – verstoßen. Nach Ansicht der Provider fehlt es jedoch bereits an einem strafrechtlich relevanten Erfolg in Deutschland. Die Websites würden im Ausland ins Netz gestellt und seien zudem teilweise in englischer Sprache verfasst. Allein die Abrufbarkeit führe noch nicht zur Verwirklichung des Tatbestands in Deutschland.

Die Ordnungsbehörde hingegen betont mit Blick auf die relevanten Straftatbestände (Volksverhetzung nach § 130 StGB und „Auschwitzlüge" nach § 130 Abs. 3 StGB) ihren konkreten Bezug zum Gebiet der Bundesrepublik Deutschland. Sie bezieht sich dabei auf die BGH-Entscheidung zur Verbreitung der „Auschwitz-Lüge" im Internet[94]. Hier hatte der BGH entschieden, dass der zum Tatbestand gehörende Erfolg im Sinne des § 9 Abs. 1 Alt. 3 StGB bereits dann im Inland eintrete, wenn die volksverhetzenden Äußerungen den Internetnutzern in Deutschland zugänglich seien. Soweit die verbotenen Websites jedoch über einen ausländischen Server ins Internet gestellt würden, müssten die Äußerungen konkret zur Friedensstörung im Inland geeignet sein.

(94) BGH, NJW 2001, 624 ff.

d. Verfassungsmäßigkeit der Sperrverfügungen

aa. Bestimmtheit der Verfügung

Die Bezirksregierung Düsseldorf hatte in ihren Verfügungen den Access-Providern drei verschiedene Sperrmethoden genannt. Da sie sich damit nicht auf eine bestimmte Methode festgelegt hat, sei die Sperrverfügung nach Auffassung der Provider zu unbestimmt und verstoße gegen § 37 Abs. 1 VwVfG NRW. Hiergegen argumentiert die Behörde, dass es genüge, wenn in der Verfügung das Ziel – hier also die Sperrung der beiden Websites – festgelegt werde. Die Wahl des Mittels zur Erreichung dieses Ziels könne dabei ohne weiteres den Providern überlassen werden.

bb. Grundrechtseingriffe

Die Access-Provider machen zudem den Verstoß gegen Grundrechte geltend. Durch die Sperrung der beiden Webseiten werde sowohl das Grundrecht der Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 Satz 1 GG) als das der Berufsausübungsfreiheit (Art. 12 Abs. 1 Satz 2 GG) verletzt. Dies sieht die Bezirksregierung Düsseldorf anders. Ihrer Ansicht nach werden die genannten Grundrechte – wenn überhaupt – durch die Sperrverfügung rechtmäßig, also im gesetzlich vorgesehenen Rahmen eingeschränkt.

cc. Verhältnismäßigkeit der Maßnahme

Bedenken haben die Provider ebenfalls hinsichtlich der Verhältnismäßigkeit der Maßnahme. Sie halten die Verfügung für nicht geeignet, da eine vollständige Sperrung der rechtsextremistischen Seiten bereits technisch nicht möglich sei. Der Zweck der Verfügung – die Sperrung der beiden Websites - könne niemals vollständig erreicht werden, da es immer Möglichkeiten zur Umgehung der Sperrungen geben werde. Die Bezirksregierung Düsseldorf hingegen beruft sich darauf, dass es bei der ordnungsrechtlichen Gefahrenabwehr nicht auf die vollständige Gefahrenbeseitigung ankomme. Vielmehr genüge es bereits, wenn der Zugang zu den Seiten jedenfalls für den Durchschnittsnutzer verhindert bzw. erschwert werde.

Auch hinsichtlich der Zumutbarkeit sind sich die Streitbeteiligten uneinig. Während die Provider die Auffassung vertreten, dass sämtliche in Betracht kommenden Sperrmethoden zu arbeits- und kostenintensiv und damit den Providern nicht zumutbar seien, sei nach Ansicht der Aufsichtsbehörde insbesondere die DNS-Sperrung ohne viel Aufwand möglich.

dd. Ermessen

Nach Ansicht der Zugangsanbieter hat die Aufsichtsbehörde das ihr eingeräumte Entschließungsermessen nicht ausgeübt. Dass der Behörde ein Ermessensspielraum dabei zustand, ob sie die Access-Provider tatsächlich in Anspruch nimmt, folgern die Provider aus dem Wortlaut des § 22 Abs. 3 MDStV („können Maßnahmen ... auch gegen Diensteanbieter von fremden Inhalten ... gerichtet werden"). Die Regelung des § 22 Abs. 2 MDStV, wonach die Behörde verpflichtet sei, Maßnahmen zu ergreifen, sobald sie einen Gesetzesverstoß feststellt, gelte lediglich für die Inanspruchnahme der Content- und Service-Provider. Für die Bezirksregierung Düsseldorf hingegen ergibt sich aus dem § 22 Abs. 2 MDStV, dass die Behörde zum ordnungsrechtlichen Einschreiten verpflichtet sei, sobald ein Verstoß gegen den MDStV vorliege. Die Regelung des § 22 Abs. 3 MDStV stelle es lediglich in das Ermessen der Behörde, gegen welchen Provider sie einschreitet, konstituiere also ein Auswahl-, aber kein Entschließungsermessen.

ee. Inanspruchnahme der Access-Provider nach § 14 Abs. 1 OBG i.V.m. § 8 Abs. 2 TDG

Auch für den Fall, dass man das TDG und nicht den MDStV für anwendbar erachtet, hält die Bezirksregierung die Sperrverfügung für rechtmäßig. Ihrer Ansicht nach kann dann der § 14 Abs. 1 Ordnungsbehördengesetz Nordrhein-Westfalen (OBG NRW) i.V.m. § 8 Abs. 2 TDG als Ermächtigungsgrundlage herangezogen werden. Nach der ordnungsrechtlichen Generalklausel des § 14 Abs. 1 OBG NRW können die nordrhein-westfälischen Ordnungsbehörden notwendige Maßnahmen zur Abwehr von konkreten Gefahren für die öffentliche Sicherheit und Ordnung ergreifen. Dadurch, dass durch die Websites Straftatbestände verwirklicht würden, liege bereits eine Störung für die öffentliche Sicherheit und Ordnung vor. Die Access-Provider, die ja bereits den Eintritt des strafrechtlichen Erfolges verneinen, halten bereits aus diesem Grunde auch den § 14 Abs. 1 OBG nicht für anwendbar.

ff. Störereigenschaft der Access-Provider

Von besonderer Bedeutung ist die Frage der Störereigenschaft der Access-Provider. Entscheidet sie doch darüber, ob den Anbietern im Falle der rechtmäßigen Inanspruchnahme Schadensersatzansprüche zustehen. Nur wenn sie als sog. Nichtstörer i.S.v. § 19 Abs. 1 OBG NRW qualifiziert werden, können sie die ihnen durch die Sperrung der Webseiten entstandenen Aufwendungen von der Behörde ersetzt verlangen. Erwartungsgemäß machen die Provider genau dies geltend. Sie argumentieren, dass sie in keiner Weise verantwortlich für die strafbaren Inhalte der zu sperrenden Webseiten seien, sondern lediglich den Zugang zu ihnen vermittelten.

Die Medienaufsichtsbehörde hingegen hält bereits die Vorschriften über die Störereigenschaft (§§ 17 ff. OBG NRW) i.V.m. dem MDStV nicht für anwendbar. Der MDStV sei abschließend und sehe eine Schadensersatzpflicht gegenüber dem Access-Provider als einem „Störer sui generis" ausdrücklich nicht vor. Warum den Providern in diesem Fall kein Anspruch aus dem gewohnheitsrechtlich anerkannten Institut der Aufopferung zustehen sollte, führt die Behörde allerdings nicht aus.

Selbst wenn man aber die Vorschriften der §§ 17 ff. OBG NRW anwenden sollte, geht die Aufsichtsbehörde davon aus, dass die Provider als Zustandsstörer i.S.d. § 18 Abs. 1 OBG NRW zu qualifizieren seien, denen kein Schadensersatzanspruch zustehe. Spätestens mit der Kenntniserlangung von den strafbaren Webseiten hätten sie nämlich den Status des „nicht Verantwortlichen" i.S.d. Vorschrift des § 19 Abs. 1 OBG NRW verloren.

4.5.3 Die Entscheidungen der Verwaltungsgerichte

Alle sechs Verwaltungsgerichte kommen im Rahmen der im Eilverfahren erfolgenden summarischen Prüfung zu dem Schluss, dass die Sperrverfügungen weder offensichtlich rechtswidrig noch offensichtlich rechtmäßig sind. Die Beschlussbegründungen unterscheiden sich jedoch sowohl in ihrem Umfang als auch in ihrem Aufbau und in den unterschiedlichen Interessenbewertungen.

a. Die Entscheidungen der Verwaltungsgerichte Minden und Arnsberg

Die Verwaltungsgerichte Arnsberg und Minden nehmen in ihren Beschlüssen ohne nähere Prüfung der Rechtmäßigkeit der Sperrverfügung eine von den Erfolgsaussichten der Hauptsache unabhängige allgemeine Interessenabwägung vor[95]. Diese fällt in dem Mindener Beschluss zu Gunsten des Access-Providers, in der Arnsberger Entscheidung zu Gunsten des öffentlichen Interesses aus. Den Verzicht auf eine nähere Prüfung der Rechtmäßigkeit der Verfügungen begründen die Gerichte mit der Komplexität der zu klärenden Rechtsfragen und mit dem Umfang der streitbefangenen Bescheide und Schriftsätze[96].

Die Entbehrlichkeit einer summarischen Prüfung der relevanten Rechtsfragen wird damit im Kern mit dem großen Umfang des Schriftwechsels zwischen den Beteiligten begründet. Dies aber dürfte dem Sinn und Zweck der Durchführung des Eilverfahrens und der Vornahme der summarischen Prüfung zuwiderlaufen. Die im Rahmen des Eilverfahrens vorzunehmende summarische Prüfung bedeutet zunächst, dass

(95) Vgl. VG Arnsberg (a.a.O.), 4; VG Minden (a.a.O.), 2.
(96) Vgl. VG Arnsberg (a.a.O.), 4; VG Minden (a.a.O.), 2.

Tatsachen nicht voll bewiesen werden müssen, sondern vielmehr grundsätzlich die Glaubhaftmachung seitens der Beteiligten genügt[97]. Sie bedeutet hingegen nicht, dass sich das Gericht gar nicht erst mit den streitigen Rechtsfragen auseinander setzen muss[98]. Erst wenn es entscheidende Rechtsfragen konkret benennt und darlegt, warum diese ausnahmsweise nicht zu klären sind, kann es auf eine allgemeine Interessenabwägung abstellen. Dies gilt vorliegend umso mehr, als es u.a. um die Verletzung von Grundrechten geht[99]. Eine eingehendere Prüfung der Sach- und Rechtslage wie auch der abzuwägenden Interessen hält auch das Bundesverfassungsgericht grundsätzlich für erforderlich, wenn besonders geschützte Grundrechte betroffen sind[100]. In verfahrensrechtlicher Hinsicht hätte die Schlussfolgerung der Gerichte zudem zur Folge, dass die am Verwaltungsrechtsstreit Beteiligten generell durch Einreichen möglichst umfangreicher Schriftsätze das Verfahren manipulieren und erreichen könnten, dass das Gericht, ohne sich näher mit den rechtlichen Problemen auseinander zu setzen, eine davon unabhängige allgemeine Interessenabwägung vornimmt.

aa. Allgemeine Interessenabwägung im Beschluss des Verwaltungsgerichts Minden

Auch die vom Verwaltungsgericht Minden vorgenommene allgemeine Interessenabwägung selbst weist einige Unklarheiten auf. So geht das Gericht zunächst davon aus, dass bereits der Umstand, dass Rechtsbehelfe gegen belastende Verwaltungsakte grundsätzlich aufschiebende Wirkung haben sollen (vgl. § 80 Abs. 1 VwGO), dafür spreche, dass die allgemeine Interessenabwägung zu Gunsten des Providers ausfalle und die aufschiebende Wirkung seines Rechtsbehelfs wieder hergestellt werden müsse[101].

Diese Schlussfolgerung dürfte jedoch so nicht ganz unproblematisch sein. Der in § 80 Abs. 1 VwGO festgelegte Grundsatz des Regel- und Ausnahmeverhältnisses kann im konkreten Verfahren nicht ohne weiteres als Argument dafür dienen, dass das Aufschubinteresse des Providers gegenüber dem öffentlichen Interesse an der sofortigen Vollziehung überwiegt. Der Grundsatz ist vielmehr lediglich neben den Erfolgsaussichten der Hauptsache und den Interessen der Beteiligten zu berücksichtigen[102]. Die Richter hätten sich daher zunächst mit den Erfolgsaussichten der Hauptsache und den sich gegenüber stehenden Interessen der Beteiligten auseinander setzen und diese gegeneinander abwägen müssen. Der Grundsatz der aufschiebenden Wirkung hat insofern nur Indizcharakter und kann nur dann heran gezogen werden, wenn eine

(97) Vgl. Schmidt, in: Eyermann, VwGO-Kommentar, 11. Auflage, 2000, § 80, Rn. 81.
(98) Ausführlich hierzu: Pietzner/Ronellenfitsch, Das Assessorexamen im Öffentlichen Recht, 10. Auflage, 2000, 655 ff.; Happ, in: Eyermann (a.a.O.), § 123, Rn. 48.
(99) Vgl. Schmidt, in: Eyermann (a.a.O.), § 80, Rn. 82.
(100) Vgl. BVerfG, NJW 1991, 1530; Kopp/Schenke, VwGO-Kommentar, 13. Auflage, 2003, § 80 Rn. 127, m.w.N.
(101) Vgl. VG Minden (a.a.O.), 2 f.
(102) Vgl. Schenke, Verwaltungsprozessrecht, 7. Auflage, 2000, Rn. 1003

allgemeine Interessenabwägung nicht möglich ist. Auch bleibt in dem Beschluss des Verwaltungsgerichts Minden unberücksichtigt, dass es in dem Verfahren um Internetinhalte geht, die nach Aussage der Aufsichtsbehörde gegen Normen des materiellen Strafrechts verstoßen (§§ 130 Abs. 1, Abs. 2 und Abs. 3; 130 a; 86 a StGB). Um eine sachgerechte Interessenabwägung vornehmen zu können, hätte das Verwaltungsgericht zunächst klären müssen, ob durch die Abrufbarkeit der Internetseiten tatsächlich ein strafrechtlich relevanter Erfolg eingetreten ist. Die von den Straftaten ausgehenden Gefahren für die öffentliche Sicherheit und Ordnung hätten dann von den Richtern in die allgemeine Interessenabwägung miteinbezogen werden müssen.

Auch an anderer Stelle ist die Argumentation des Verwaltungsgerichts Minden in sich widersprüchlich: Zum einen beurteilt es den dem Provider durch eine Sperrung der beiden Websites entstehenden finanziellen Nachteil als „mit großer Wahrscheinlichkeit erheblich" und „nicht ohne Weiteres wieder gut zu machen". Zum anderen wird eingeräumt, dass genau diese Frage, nämlich wie groß der Aufwand für die in der Verfügung angeordneten Sperrungen tatsächlich ist, zwischen den Beteiligten streitig und ungeklärt ist[103]. Das Gericht bewertet weder diese unterschiedlichen Auffassungen noch legt es dar, welche Behauptung es für zutreffend hält. Um das Ausmaß der Nachteile des Providers beurteilen zu können, hätten sich die Richter zunächst mit der streitigen Frage auseinander setzen müssen, wie groß der Aufwand für die Sperrung der beiden Homepages tatsächlich ist.

Die Mindener Richter stellen zudem die Effektivität der Sperrverfügung in Frage. Dies jedoch weniger aus technischen Gründen als wegen der räumlichen Beschränkung der Maßnahme auf Nordrhein-Westfalen. So führt das Gericht aus, dass im Falle einer Sperrung interessierte Nutzer ohne Weiteres jederzeit zu anderen Anbietern, insbesondere zu solchen in den übrigen Bundesländern wechseln könnten, über die der Zugriff zu den Seiten nach wie vor möglich sei[104]. Dieses Kernproblem der territorialen Begrenztheit der Maßnahme ist tatsächlich nicht von der Hand zu weisen. Juristisch betrachtet verkennt das Verwaltungsgericht mit dieser Begründung jedoch, dass die Bezirksregierung Düsseldorf als Trägerin öffentlicher Gewalt ordnungsrechtlich nur innerhalb ihres Zuständigkeitsbereichs eingreifen kann. Dass in anderen Zuständigkeitsbereichen nicht die gleichen Maßnahmen ergriffen werden, kann daher nicht als Argument der Rechtswidrigkeit des Einschreitens der Behörde gereichen. Zudem legt das Verwaltungsgericht seiner Auffassung die Prämisse zugrunde, dass allein das Vorhandensein von Umgehungsmöglichkeiten – bedingt durch die räumliche Begrenzung der Sperrverfügung – ihre grundsätzliche Effektivität in Frage stellt. Diesem immer wieder bemühten Argument muss mit dem OVG Münster und den anderen Verwaltungsgerichten entgegengehalten werden, dass im Polizei- und Ordnungs-

(103) Vgl. VG Minden (a.a.O.), 3.
(104) Vgl. VG Minden (a.a.O.), 3.

recht eine Maßnahme bereits dann als geeignet angesehen wird, wenn sie die Gefahr minimiert bzw. den gewünschten Erfolg fördert[105]. Zur Verdeutlichung kann in diesem Zusammenhang auch auf andere Fälle des Polizei- und Ordnungsrechts verwiesen werden. So werden beispielsweise polizeirechtliche Platzverweise oder längerfristige Aufenthaltsverbote zur Bekämpfung von Straftaten in der sich auf verschiedene Ortsteile konzentrierenden Drogenszene ausgesprochen. Hierbei wird bewusst in Kauf genommen, dass die Drogen kurze Zeit später in weiter außerhalb gelegenen Stadtteilen weiterhin erhältlich sind und somit lediglich eine Verlagerung des Problems erreicht wird. Die Maßnahme wird aber schon deshalb als geeignet angesehen, weil Zufallskunden und Passanten nicht mehr in dem Ausmaß gefährdet sind, als wenn der Drogenhandel an öffentlichen Plätzen stattfindet.

bb. Allgemeine Interessenabwägung im Beschluss des Verwaltungsgerichts Arnsberg

Das Verwaltungsgericht Arnsberg kommt im Rahmen der allgemeinen Interessenabwägung zu dem Schluss, dass das öffentliche Interesse am Sofortvollzug der Sperrverfügung gegenüber dem Aussetzungsinteresse des Access-Providers überwiegt. Für die Richter besteht das öffentliche Interesse in der Verschonung von Volksverhetzung im Internet. Es bestehe „keinerlei Anlass, den strafbaren Umtrieben im Internet ihren Lauf zu lassen und angesichts der zahlreichen Umgehungsmöglichkeiten sowie der Anonymität bzw. Nichtgreifbarkeit der Urheber die Hände in den Schoß zu legen“[106]. Schützenswerte Interessen des Access-Providers vermag das Gericht demgegenüber nicht zu erkennen[107]. Da der Provider die Sperrung der beiden Sites bereits vorgenommen hatte, verzichten die Richter auf eine nähere Prüfung des Aufwandes und der technischen Durchführbarkeit. Das Argument des Providers, dass wegen der Sperrung eine Abwanderung der Kunden zu befürchten sei, lässt das Verwaltungsgericht nicht gelten. Ein solcher mittelbarer Schaden werde von der Rechtsordnung nicht geschützt, wenn – wie im Falle der Volksverhetzung – die freiheitliche demokratische Grundordnung betroffen sei[108].

Zwar hat sich das Verwaltungsgericht Arnsberg damit in seiner Entscheidung wesentlich ausführlicher mit den streitigen Problemen auseinandergesetzt als das Verwaltungsgericht Minden. Allerdings unterstellen die Richter, dass durch die streitbefangenen Websites ein in Deutschland strafrechtlich relevanter Erfolg verwirklicht wird, ohne dies näher zu untersuchen. Eine ausführlichere Auseinandersetzung mit diesem Problem wäre hier jedoch geboten gewesen, zumal die Richter das Überwiegen des öffentlichen Interesses am Sofortvollzug in erster Linie mit den von den Straftaten ausgehenden Gefahren begründen.

(105) Vgl. Zimmermann, NJW 1999, 3145 (3150); Spindler/Volkmann, K & R 2002, 398 (406).
(106) Vgl. VG Arnsberg (a.a.O.), 4 f.
(107) Vgl. VG Arnsberg (a.a.O.), 5.
(108) Vgl. VG Arnsberg (a.a.O.), 5.

b. Die Entscheidungen der Verwaltungsgerichte Gelsenkirchen, Düsseldorf, Aachen und Köln

Auch die Verwaltungsgerichte Gelsenkirchen, Düsseldorf, Aachen und Köln vermögen im Rahmen der summarischen Prüfung im Eilverfahren weder eine offensichtliche Rechtmäßigkeit noch Rechtswidrigkeit der Sperrungsanordnung festzustellen[109]. Die vier Gerichte prüfen zunächst, ob die angefochtene Sperrverfügung offensichtlich rechtswidrig ist und untersuchen sämtliche Voraussetzungen der von der Bezirksregierung Düsseldorf herangezogenen Ermächtigungsgrundlage. Sie kommen zu dem Schluss, dass keine offensichtliche Rechtswidrigkeit der Grundverfügung vorliegt, sondern vielmehr Vieles für ihre Rechtmäßigkeit spricht. Die sich daran anschließenden allgemeinen Interessenabwägungen fallen erwartungsgemäß jeweils zu Lasten der Provider aus.

aa. Ermächtigungsgrundlage

Nach Auffassung aller vier Gerichte hat die Bezirksregierung Düsseldorf die Sperrverfügungen auf die richtige Ermächtigungsgrundlage, nämlich § 22 Abs. 3 S. 1 MDStV gestützt. Die Verwaltungsgerichte Düsseldorf und Köln nehmen zunächst eine Abgrenzung der Anwendungsbereiche des MDStV bzw. des TDG im Vergleich zum TKG vor[110]. Sie kommen dabei zu dem Schluss, dass die Access-Provider keine Telekommunikationsdienstleister im Sinne des § 4 TKG, sondern Medien- bzw. Teledienstanbieter i.S.v. § 3 Nr. 1 MDStV bzw. § 3 Nr. 1 TDG sind. Dies deshalb, da nicht lediglich die technische Seite, also der Datentransport betroffen sei, sondern es vielmehr in erster Linie um inhaltliche Angebote gehe. Eine solche Abgrenzung zwischen den Anwendungsbereichen der verschiedenen Gesetze lassen die Beschlussbegründungen der Verwaltungsgerichte Gelsenkirchen und Aachen hingegen vermissen. Diese aber dürfte allerdings unverzichtbar für eine sachgerechte Interessenabwägung gewesen sein. Denn im TKG findet sich keine dem § 22 Abs. 3 MDStV entsprechende Ermächtigungsgrundlage, sodass die Entscheidung über seine Anwendbarkeit maßgebliche Bedeutung für das Ergebnis der Beschlüsse gehabt hätte.
Die vier Verwaltungsgerichte sehen in den beiden zu sperrenden Webseiten Medien- und keine Teledienste. Die redaktionelle Gestaltung stehe bei beiden Angeboten im Vordergrund[111]. Sie seien an die Allgemeinheit gerichtet und zielten auf eine beliebige Öffentlichkeit ab, nicht jedoch lediglich auf geschlossene Nutzergruppen oder reine Individualkommunikation. Die Gerichte beurteilen dabei das gesamte Erscheinungsbild der beiden Homepages und sehen in ihnen die journalistische Ausgestaltung zur Verbreitung nationalsozialistischen Gedankenguts.

(109) Vgl. VG Gelsenkirchen (a.a.O.), 3; VG Düsseldorf (a.a.O.), 12; VG Aachen (a.a.O.), 4; VG Köln (a.a.O.), 13.
(110) Vgl. VG Düsseldorf (a.a.O.), 13 ff.; VG Köln (a.a.O.), 14 ff.
(111) Vgl. VG Gelsenkirchen (a.a.O.), S. 5 ff.; VG Düsseldorf (a.a.O.), S. 14 ff.; VG Aachen (a.a.O.), S. 4 f.; VG Köln (a.a.O.), 14 ff.

bb. Verstoß gegen § 12 Abs. 1 MDStV

Der Verstoß gegen § 12 Abs. 1 MDStV wird von den Verwaltungsgerichten unterschiedlich begründet. So hält das Verwaltungsgericht Aachen die betroffenen Internetseiten bereits deshalb für unzulässig, weil sie offensichtlich geeignet seien, Kinder und Jugendliche sittlich schwer zu gefährden (§ 12 Abs. 1 Nr. 3 MDStV)[112] und die Menschenwürde verletzten (§ 12 Abs. 1 Nr. 5 MDStV) . Auf eine Klärung des heftig umstrittenen Problems des strafrechtlich relevanten Erfolges in Deutschland können die Aachener Richter daher verzichten.

Nicht so die anderen drei Gerichte. Sie stellen unmittelbar auf einen Verstoß der beiden Websites gegen Strafgesetze[113] und damit gegen § 12 Abs. 1 Ziff. 1 MDStV ab[114]. Die Verwaltungsgerichte Gelsenkirchen und Köln schließen sich hinsichtlich der Beurteilung der strafrechtlichen Relevanz im Inland der Aufsichtsbehörde an und verweisen auf das BGH-Urteil zur Auschwitzlüge. Die Beschlussbegründung des Verwaltungsgerichts Düsseldorf lässt eine Auseinandersetzung mit dieser Frage gänzlich vermissen, was aufgrund der bereits unter Punkt 2.a. angestellten Erwägungen problematisch sein dürfte.

cc. Festlegen auf eine bestimmte Sperrmethode nicht erforderlich

Dass die Aufsichtsbehörde sich nicht auf eine bestimmte Sperrmethode festgelegt, sondern den Providern drei Möglichkeiten zur Auswahl genannt hat, halten die Verwaltungsgerichte für unproblematisch. Im Gelsenkirchener Beschluss wird ausgeführt, dass es nach § 21 S. 1 OBG NRW genüge, wenn ein Mittel zur Gefahrenabwehr bestimmt werde, selbst wenn zur Abwehr der Gefahr mehrere Mittel in Betracht kämen[115]. Die Düsseldorfer, Aachener und Kölner Richter argumentieren, dass zwar grundsätzlich nicht nur das Ziel, sondern auch das Mittel zur Zweckerreichung festgelegt werden müsse. Allerdings reiche es aus, wenn die Behörde – wie vorliegend – mehrere Mittel aufzeige, dem Ordnungspflichtigen jedoch die Wahl überlasse, auf welchem Wege er seiner Ordnungspflicht nachkomme[116].

dd. Technische Möglichkeit der Sperrung

Für die Gelsenkirchener, Düsseldorfer und Kölner Richter stellt sich die Sperrung der beiden Homepages ebenso wie für die Bezirksregierung Düsseldorf als technisch machbar dar. So hält das Verwaltungsgericht Gelsenkirchen insbesondere die Router-Sperr-

(112) Vgl. VG Aachen (a.a.O.), 6.
(113) Verwendung von Kennzeichen verfassungswidriger Organisationen (§ 86 a StGB); Volksverhetzung (§ 130 Abs. 1 und 2 StGB).
(114) Vgl. VG Gelsenkirchen (a.a.O.), 6 f.; VG Düsseldorf (a.a.O.), 16 f.; VG Köln (a.a.O.), 17.f.
(115) Vgl. VG Gelsenkirchen (a.a.O.), 8.
(116) Vgl. VG Düsseldorf (a.a.O.), 18 f.; VG Aachen (a.a.O.), 7; VG Köln (a.a.O.), 19 f.

methode (Ausschluss der IPs durch Sperrung im Router) für funktionstauglich[117]. Gestützt wird diese Aussage primär auf die von der Aufsichtsbehörde bemühte Stellungnahme des Leiters des Hochschulrechenzentrums der Universität Dortmund. Die Richter der Verwaltungsgerichte Düsseldorf und Köln hingegen führen die technische Möglichkeit in erster Linie darauf zurück, dass bereits mehrere Access-Providerdie Websites gesperrt hätten[118].

ee. Geeignetheit und Erforderlichkeit der Sperrverfügung

Trotz vorhandener Umgehungsmöglichkeiten halten die Richter die Maßnahme der Bezirksregierung Düsseldorf zur beabsichtigten Gefahrenabwehr auch für geeignet. Sie verweisen in diesem Zusammenhang wie die Bezirksregierung auf den im Ordnungsrecht herrschenden Grundsatz der effektiven Gefahrenabwehr, wonach es nicht erforderlich sei, dass das angeordnete Mittel eine vollständige Gefahrbeseitigung bewirke[119]. Die Aachener und Kölner Verwaltungsrichter stufen diesen Punkt als nicht ganz unproblematisch ein. Sie betonen in diesem Zusammenhang, dass sie die Maßnahme aufgrund ihrer begrenzten Effektivität lediglich als „noch geeignet" ansehen[120].

ff. Grundrechte der Provider

Während die Verwaltungsgerichte Gelsenkirchen und Aachen keinerlei Ausführungen hinsichtlich der Verhältnismäßigkeit der Maßnahme im engeren Sinne machen, prüfen die Düsseldorfer Verwaltungsrichter in diesem Zusammenhang ausführlich, ob die Sperrungsanordnung gegen grundgesetzliche Gleichheits- oder Freiheitsrechte der Provider verstößt[121]. Diese Ausführungen macht sich das Verwaltungsgericht Köln in seinem Beschluss ausdrücklich zu Eigen[122]. Die Grundrechte der Informations- und Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 und 2 GG sieht das Verwaltungsgericht Düsseldorf nicht verletzt, da ein Eingriff jedenfalls durch die grundgesetzliche Schranke des Art. 5 Abs. 2 GG gedeckt sei[123]. Auch verstoße die Sperrverfügung nicht gegen das Zensurverbot des Art. 5 Abs. 1 S. 3 GG. Denn auch dieses verbiete nicht jeden rechtsstaatlichen Eingriff eines staatlichen Organs, soweit es um einen Verstoß gegen strafrechtliche Normen und die Verletzung der freiheitlich-demokratischen Grundordnung gehe[124].

(117) Vgl. VG Gelsenkirchen (a.a.O.), 8.
(118) Vgl. VG Düsseldorf (a.a.O.), 19 f.; VG Köln (a.a.O.), 20 f.
(119) Vgl. VG Gelsenkirchen (a.a.O.), 8 f.; VG Düsseldorf (a.a.O.), 20; VG Aachen (a.a.O.), 8; VG Köln (a.a.O.), 21 f.
(120) Vgl VG Aachen (a.a.O.), 8; VG Köln (a.a.O.), 23.
(121) Vgl. VG Düsseldorf (a.a.O.), 20 ff.
(122) Vgl. VG Köln (a.a.O.), 23.
(123) Vgl. VG Düsseldorf (a.a.O.), 21.
(124) Vgl. VG Düsseldorf (a.a.O.), 21 f.

Eine Verletzung der Grundrechte des Access-Providers aus Art. 12 Abs. 1 S. 1 und Art. 14 Abs. 1 Satz 1 GG lehnt das Verwaltungsgericht Düsseldorf ebenfalls ab. Selbst wenn man bei der Sperrverfügung von einem Eingriff in die Berufsfreiheit des Access-Providers ausgehe, so handele es sich bei § 22 Abs. 3 MDStV bzw. einer hierauf beruhenden Verfügung um eine Berufsausübungsregelung. Diese jedoch sei durch vernünftige Gründe des Allgemeinwohls gerechtfertigt[125]. Für den Fall der Annahme eines Eingriffs in das Grundrecht aus Art. 14 Abs. 1 GG stelle die Maßnahme der Aufsichtsbehörde eine zulässige Inhalts- und Schrankenregelung im Sinne des Art. 14 Abs. 1 S. 2 GG dar[126].

gg. Ermessen

Die Verwaltungsgerichte gehen ebenso wie die Aufsichtsbehörde davon aus, dass letzterer kein Entschließungsermessen hinsichtlich des Vorgehens gegenüber den Access-Providern zustand. Nach der Vorschrift des § 22 Abs. 2 S. 1 MDStV habe die Aufsichtsbehörde die erforderlichen Maßnahmen zu „treffen", ohne dass ihr dabei ein Ermessen eingeräumt werde. Das nach § 22 Abs. 3 MDStV lediglich bestehende Auswahlermessen habe die Aufsichtsbehörde korrekt ausgeübt[127]. Nach Einschätzung der Richter haben sich nämlich Maßnahmen gegenüber den primär Verantwortlichen nach § 6 Abs. 1 MDStV tatsächlich als nicht durchführbar bzw. nicht Erfolg versprechend erwiesen. Auch sei die Bezirksregierung Düsseldorf in Bezug auf den Adressatenkreis nach einem „klaren System, nämlich einer möglichst flächendeckenden Wirkung in ihrem Zuständigkeitsbereich" vorgegangen[128]. In dem Düsseldorfer Beschluss findet sich eine solche Ermessensfehlerprüfung nicht.

hh. Rechtmäßigkeit der Maßnahme nach § 14 Abs. 1 OBG i. V. m. § 8 Abs. 1 TDG

Die Verwaltungsgerichte Düsseldorf und Köln halten die Sperrverfügung auch für den Fall der Annahme der Anwendbarkeit des TDG für rechtmäßig. Ebenso wie die Aufsichtsbehörde sehen sie in den Vorschriften der § 14 Abs. 1 OBG NRW i.V.m. § 8 Abs. 2 S. 2 TDG eine mögliche Ermächtigungsgrundlage. Die Zuständigkeit der Bezirksregierung Düsseldorf als Sonderordnungsbehörde im Sinne des § 12 Abs. 1 OBG NRW ergebe sich dann aus Art. III des Gesetzes zum 5. Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge vom 12.12.2000[129] zur Überwachung der Einhaltung der Bestimmungen des TDG[130].

(125) Vgl. VG Düsseldorf (a.a.O.), 22 f.
(126) Vgl. VG Düsseldorf (a.a.O.), 23.
(127) Vgl. VG Gelsenkirchen (a.a.O.), 9 f.; VG Düsseldorf (a.a.O.), 19; VG Aachen (a.a.O.), 7 f.; VG Köln (a.a.O.), 21.
(128) So: VG Gelsenkirchen (a.a.O.), 9.
(129) GVBl NRW 2000, 706.
(130) Vgl. VG Düsseldorf (a.a.O.), 23 ff.; VG Köln (a.a.O.), 24, wo auf die Ausführungen des VG Düsseldorf Bezug genommen wird.

jj. Störereigenschaft der Access-Provider

Allein das Verwaltungsgericht Düsseldorf äußert sich zu der Problematik der Störereigenschaft der Access-Provider. Im Unterschied zu der Aufsichtsbehörde halten die Richter die Access-Provider keineswegs für Zustandsstörer im Sinne des § 18 Abs. 1 OBG NRW oder gar Störer „sui generis", sondern ordnen sie als Nichtstörer im Sinne des § 19 Abs. 1 OBG NRW ein[131]. Diese Problematik dürfte indes im vorliegenden Verfahren nicht entscheidungserheblich sein. In den vorliegenden Verfahren ging es zunächst um die Rechtmäßigkeit der Inanspruchnahme der Access-Provider als solche. Erst im Zusammenhang mit möglichen Entschädigungsansprüchen der Provider werden sich die (Zivil-)Gerichte mit dieser Frage eingehender beschäftigen müssen.

kk. Allgemeine Interessenabwägung

Nachdem die Verwaltungsgerichte die offensichtliche Rechtswidrigkeit der Sperrungsanordnung ausgeschlossen haben, nehmen sie nunmehr die allgemeine Interessenabwägung vor. Nach Auffassung der Verwaltungsgerichte Gelsenkirchen, Aachen und Köln besteht das überwiegende öffentliche Interesse in der Verhinderung der Verwirklichung der genannten Straftatbestände[132]. Insbesondere die Volksverhetzung nach § 130 StGB betreffe ein gewichtiges Rechtsgut. Das Äußerungsdelikt des § 130 StGB schütze Teile der inländischen Bevölkerung schon im Vorfeld und wolle dem Ingangsetzen einer historisch als gefährlich nachgewiesenen Eigendynamik entgegen wirken. Letztlich gehe es darum, „schon frühzeitig eine Vergiftung des politischen Klimas durch die Verharmlosung der nationalsozialistischen Gewalt- und Willkürherrschaft zu verhindern"[133]. Die Gelsenkirchener Richter stellen zusätzlich mit Blick auf Frankreich fest, dass dort bereits vergleichbare Verbote verhängt worden seien[134] und verweisen in diesem Zusammenhang auf das Yahoo-Urteil des Tribunal de Grand Instance de Paris vom 20.11.2000[135]. In dem Kölner Beschluss werden als Schutzgüter außerdem der öffentliche Friede, der Jugendschutz und die Würde des Menschen hervorgehoben[136]. Für die Düsseldorfer Verwaltungsrichter genügt bereits die Wahrscheinlichkeit der Rechtmäßigkeit der Grundverfügung, um ein überwiegendes öffentliches Interesse zu bejahen[137].

(131) Vgl. VG Düsseldorf (a.a.O.), 26.
(132) Vgl. VG Gelsenkirchen (a.a.O.), 10; VG Aachen (a.a.O.), 9; VG Köln (a.a.O.), 24.
(133) So: VG Gelsenkirchen (a.a.O.), 10.
(134) Vgl. VG Gelsenkirchen (a.a.O.), 10.
(135) TGI Paris, MMR 2001, 309.
(136) Vgl. VG Köln (a.a.O.), 24.
(137) Vgl. VG Düsseldorf (a.a.O.), 26.

Überwiegende Interessen der Access-Provider, einstweilig von der Sperrung verschont zu bleiben, vermögen die vier Verwaltungsgerichte demgegenüber nicht zu erkennen[138]. Ein Interesse der Provider daran, auch weiterhin den Zugang zu inkriminierten Webseiten vermitteln zu können, werde von der Rechtsordnung nicht geschützt[139]. Die wirtschaftlichen Auswirkungen schätzen die Richter als relativ gering ein[140]. Ausführungen zu der Problematik etwaiger künftig zu erwartender weiterer Sperrverfügungen machen die Richter nicht. Diese seien nicht Bestandteil des vorliegenden Verfahrens[141].

4.5.4 Die Entscheidung des Oberverwaltungsgerichts Münster

Die Entscheidung des OVG Münster[142] stimmt in weiten Teilen mit dem Beschluss des Verwaltungsgerichts Düsseldorf überein. Hervorzuheben sind lediglich die Ausführungen der Richter zur Problematik des Ermessens. Nach Ansicht des OVG Münster stand der Aufsichtsbehörde hinsichtlich ihres Einschreitens gegenüber den Access-Providern nicht lediglich ein Auswahlermessen, sondern zusätzlich auch ein Entschließungsermessen zu. Die Richter schließen wie die Access-Provider aus der Formulierung des § 22 Abs. 3 MDStV („... können Maßnahmen auch...“), dass es im Ermessen der Bezirksregierung gestanden habe, ob sie gegen die Access-Provider vorgeht oder nicht[143]. Anders als die Aufsichtsbehörde und die Verwaltungsgerichte betrachten die Richter des OVG den § 22 Abs. 3 MDStV damit als Ermächtigungsgrundlage mit einer eigenständigen Ermessensregelung. Sie beziehen das sich aus § 22 Abs. 2 MDStV ergebende fehlende Entschließungsermessen nicht auf das Vorgehen gegenüber den Access-Providern. Dies hat indes das Ergebnis der Entscheidung nicht beeinflusst. Denn die Richter des OVG halten das Entschließungsermessen für „der Sache nach“ ausgeübt. Das deshalb, weil die Behörde im Rahmen ihrer Erwägungen hinsichtlich der Inanspruchnahme nach § 14 Abs. 1 OBG NRW hinreichend dargelegt habe, warum sie sich zum Vorgehen gegen die Access-Provider entschieden habe. Die Aufsichtsbehörde hatte nämlich – zumindest subsidiär – den § 14 Abs. 1 OBG NRW im Verwaltungsverfahren als Ermächtigungsgrundlage herangezogen und in diesem Zusammenhang ihr Entschließungsermessen ausgeübt.

(138) Vgl. VG Gelsenkirchen (a.a.O.), 11; VG Düsseldorf (a.a.O.), 26 f.; VG Aachen (a.a.O.), 9 f. ; VG Köln (a.a.O.), 24 f.
(139) So: VG Düsseldorf (a.a.O.), 26.
(140) Vgl. VG Gelsenkirchen (a.a.O.), 11; VG Düsseldorf (a.a.O.), 26 f.; LVG Aachen (a.a.O.), 10; VG Köln (a.a.O.), 24 f.
(141) So ausdrücklich: VG Aachen (a.a.O.), 9.
(142) Die Entscheidung ist im Anhang abgedruckt.
(143) OVG Münster (a.a.O.), 16 f.

4.5.5 Fazit

Zwar handelt es sich bei den Gerichtsentscheidungen lediglich um vorläufige Beschlüsse im Eilverfahren. Erst eine abschließende Entscheidung in der Hauptsache wird hier endgültig Klarheit bringen. Dies dürfte jedoch noch einige Zeit in Anspruch nehmen, zumal die Provider bereits angekündigt haben, notfalls bis vor das Bundesverfassungsgericht zu gehen. Die Beschlüsse können daher als erste wichtige Schritte hin zu mehr Rechtsklarheit hinsichtlich der ordnungsrechtlichen Regulierbarkeit von Internetinhalten gewertet werden. Sie dürften allein wegen ihres Präzedenzcharakters Maßstäbe für zukünftige Entscheidungen setzen. Mussten und müssen die Gerichte sich doch vor allem mit Fragen von grundsätzlicher Bedeutung auseinandersetzen, die die Anwendbarkeit nationalen Rechts auf das Internet als globales Medium aufwirft.

Es bleibt abzuwarten, ob die Ergebnisse der vorläufigen Beschlüsse im Hauptverfahren bestätigt werden. Sollten die Maßnahmen der Bezirksregierung endgültig für rechtmäßig befunden werden, wird insbesondere die Frage der Störereigenschaft des Access-Providers und des damit verbundenen möglichen Schadensersatzanspruches der Provider nach § 39 Abs. 1 OBG NRW (noch) zu klären sein.

4.6 Bekämpfung rassistischer und fremdenfeindlicher Inhalte nach dem Jugendmedienschutz-Staatsvertrag

Doris Brocker

4.6.1. Einleitung

In den vergangenen Monaten ist der Jugendmedienschutz-Staatsvertrag (JMStV) Gegenstand sehr grundsätzlicher Diskussionen gewesen. Die folgenden Ausführungen befassen sich mit den eher alltäglichen Problemen, die dieses Thema aufwirft. Auf dieser Ebene lässt sich die Situation wohl am plastischsten mit einer Textzeile aus einem Song von Herbert Grönemeyer beschreiben: „Es bleibt alles anders".

4.6.2 Rechtliche Situation vor Inkrafttreten des JMStV

Der JMStV ist am 1.4.2003 in Kraft getreten. Die Gesetzesbegründung wird seine Anwendung sicher erleichtern. Im Folgenden soll kurz der alte geltende Rechtszustand in Erinnerung gerufen werden. Angebote im bzw. des Internet konnten sowohl der rechtlichen Kategorie Mediendienst und Teledienst als auch der Kategorie Rundfunk zuzuordnen sein. Daraus folgten im Hinblick auf den Jugendschutz und den Schutz der Menschenwürde zum Teil unterschiedliche materielle Anforderungen, vor allem aber unterschiedliche Aufsichtszuständigkeiten, -strukturen und -verfahren. Das war besonders unbefriedigend im Hinblick darauf, dass im Zuge fortschreitender Konvergenz Angebote inhaltsgleich sind und häufig schwierige Abgrenzungsfragen auftreten. Vorrangiges Ziel des JMStV ist daher die Schaffung eines einheitlichen Rechtsrahmens im Bereich des Jugendschutzes und des Schutzes der Menschenwürde, wobei in materieller Hinsicht Gleiches gleichgestellt ist. Zur Steigerung der Effektivität sind Kompetenzen neu sortiert und Aufsichtsstrukturen neu gestaltet und verzahnt worden.

4.6.3 Was bleibt nun alles anders?

Es bleibt zunächst dabei, dass es – auch im Internet – weiterhin die rechtlichen Kategorien Rundfunk, Mediendienst und Teledienst geben wird, und dass diese Angebote, mit Ausnahme der im JMStV geregelten Sachverhalte, weiterhin dem Rundfunkstaatsvertrag, dem Mediendienste-Staatsvertrag und dem Teledienstegesetz unterfallen. Wenig Änderung bringt der JMStV auch im Hinblick auf die materiellen Maßstäbe für die Zulässigkeit solcher Angebote. Die Verbotsbestimmungen orientieren sich im Wesentlichen an den bislang geltenden. Einige Bestimmungen waren aufgrund des neuen Jugendschutzgesetzes des Bundes neu aufzunehmen. In einigen Fällen wurden

Klarstellungen vorgenommen. Neu sind Regelungen für virtuelle Darstellungen und das grundsätzliche Sendeverbot indizierter Filme, auch nach wesentlichen Änderungen. Drittens bleibt es auch nach der Neuaufteilung der Kompetenzen zwischen Bund und Ländern dabei, dass die Aufsicht über den Jugendschutz und den Schutz der Menschenwürde keine Bundessache ist. Sie ist keine Ländergemeinschaftsaufgabe, sondern wird unter Wahrung der Länderkompetenz von der örtlich zuständigen Stelle, jetzt der Landesmedienanstalt, ausgeübt. Im Übrigen bleibt es auch dabei, dass die Aufsicht über die Angebote des öffentlich-rechtlichen Rundfunks nach wie vor von diesem bzw. seinen internen Aufsichtsgremien wahrgenommen wird, wenn auch nicht nach denselben materiellen Maßstäben.

Eine Änderung gibt es im Bereich des Jugendschutzes und des Schutzes der Menschenwürde. Für die Angebote Rundfunk, Mediendienst und Teledienst wird ein einheitliches Regelwerk bestehen, dessen allgemeiner Teil auf alle Anbieter Anwendung findet und nur dort durch besondere Bestimmungen ergänzt wird, wo die Besonderheit des Angebots dies erfordert. Das ist zunächst einmal eine gute Nachricht für die redlichen Anbieter im Internet. Die im Einzelfall mitunter schwierige Abgrenzung zwischen Rundfunk, Mediendienst und Teledienst entfällt. Anbieter von Rundfunk und Telemedien – wie es jetzt zusammenfassend für Mediendienste und Teledienste heißt – finden leichter Orientierung und Beratung. Mit Blick auf die unredlichen Anbieter stärkt es die Aufsicht, wenn nicht zunächst Kompetenzen herausgearbeitet werden müssen.

Neu ist die Sortierung von Aufgaben zwischen Bund und Ländern. Die Länder sind danach für alle elektronischen, übertragenen Medien zuständig, der Bund für so genannte Trägermedien, Videokassetten, CD-ROMs u.a. Die Arbeit der nach dem Jugendschutzgesetz zuständigen Bundesprüfstelle für Medien und die Arbeit der nach dem JMStV zuständigen Stellen sind bei Telemedien verzahnt.

Neu ist auch die KJM, die Kommission für den Jugendmedienschutz, bestehend aus sechs Mitgliedern aus dem Kreis der Direktoren der Landesmedienanstalten, vier Mitgliedern der für den Jugendschutz zuständigen obersten Landesbehörden und zwei Mitgliedern der für den Jugendschutz zuständigen obersten Bundesbehörden. Die KJM wird als Organ der zuständigen Landesmedienanstalt in Sachen Einhaltung der Bestimmungen dieses Staatsvertrags abschließend und mit für die Landesmedienanstalt bindender Wirkung tätig. Eine ähnliche Konstruktion findet sich im Bereich der Vielfaltsicherung nach dem Rundfunkstaatsvertrag, wo die KEK diese Rolle spielt. Für Telemedienangebote - auch und gerade im Internet - gibt es gegenüber den für Rundfunkangeboten geltenden Verfahren Besonderheiten: Hier existiert eine Schnittstelle oder Verzahnung zwischen der KJM und der Bundesprüfstelle. Die KJM kann selbst Indizierungsanträge nach dem Jugendschutzgesetz stellen.

Im Übrigen ist sie – soweit die Bundesprüfstelle von Amts wegen tätig wird – zu hören, wobei die Stellungnahme der KJM maßgeblich zu berücksichtigen ist.
Weiter bleibt die von den Ländern eingerichtete Stelle Jugendschutz.net bestehen, die organisatorisch an die KJM angebunden wird und diese bei ihrer Arbeit unterstützt. Jugendschutz.net ist zuständig für die Überprüfung der Telemedien. Sie weist Anbieter auf Verstöße hin und informiert die KJM und die anerkannten Einrichtungen der freiwilligen Selbstkontrolle hierüber. Daneben nimmt die Stelle auch Aufgaben der Beratung und Schulung der Telemedienanbieter wahr.

Die Regelungen im Zusammenhang mit den „anerkannten Einrichtungen der freiwilligen Selbstkontrolle" sind aus Sicht der Landesmedienanstalten wohl die gravierendsten Neuerungen. Statt des bisherigen Systems rein staatlicher, bzw. mit Blick auf die Landesmedienanstalten, behördlicher Aufsicht billigt der JMStV nun der Selbstkontrolle eine wesentliche Bedeutung zu. Grundgedanke dieses Konzepts ist dabei, im Sinne effektiven Jugendschutzes die Prüfung der Einhaltung der Bestimmungen des JMStV weitgehend anerkannten Einrichtungen der Selbstkontrolle zu überlassen. Bei nicht vorlagefähigen Sendungen und bei Telemedienangeboten, bei denen wegen der Aktualität oder der Art des Angebotes eine Beurteilung der Natur der Sache nach vor Ausstrahlung bzw. Bereitstellung nicht möglich ist, hat die KJM zunächst die Selbstkontrolleinrichtung zu befassen. Auch hier ist die KJM auf die Prüfung beschränkt, ob die Selbstkrontolleinrichtung bei ihrer Bewertung die rechtlichen Grenzen des Beurteilungsspielraums eingehalten hat. Sie prüft nicht, ob materielles Recht richtig angewendet wurde. Dies gilt allerdings nicht bei Angeboten, die nach § 4 Abs. 1 JMStV grundsätzlich unzulässig sind.

4.6.4 Hass und Gewalt im Internet – auch nach Inkrafttreten des JMStV

Dass in den Ausführungen bislang weder von „Hass und Gewalt" die Rede war, noch konkrete Vorschläge zur Verhinderung oder Verfolgung solcher Angebote im Internet gemacht wurden, liegt schlicht daran, dass es eine Patentlösung für dieses Problem derzeit noch nicht gibt. Auch nach dem 01. April 2003 sind Angebote im Internet verboten, die z. B. die Menschenwürde verletzen, die mit dem Anspruch nationaler, rassischer oder religiöser Überlegenheit Hass und Gewalt gegen ausländische oder jüdische Mitmenschen propagieren, die Ausschwitzlüge verbreiten oder kinderpornographische Inhalte haben. Noch immer werden Anbieter solcher Dinge schwer zu identifizieren und zu verfolgen sein. Meines Erachtens ist damit die Zeit gekommen, in der gewisse Grundsatzdiskussionen in den Hintergrund treten sollten. Wir sollten nach vorn schauen und uns um praktische Fragen der Vollziehung kümmern, Gestaltungsspielräume finden und nutzen und uns bereit für den großen Praxistest machen. Debatten darüber, ob auch in Bezug auf solche Angebote nicht die Meinungsfreiheit höher zu bewerten ist, oder,

ob diese Angebote nicht einen wesentlichen Beitrag zur politischen Meinungsbildung leisten können oder gar für den pädagogischen Prozess unerlässlich sind, sollten in diesem Zusammenhang nicht mehr geführt werden müssen.

Der JMStV enthält hier Klarstellungen und ist bemüht, bislang vorhandene Lücken zu schließen. Er erfindet jedoch keineswegs Verbote von Hass und Gewalt grundsätzlich neu. In ihm kommen vielmehr Grundwerte zum Ausdruck, die für unsere Gesellschaft – und nicht nur für unsere – prägend sind oder es zumindest sein sollten. Auch wenn diese Angebote im Internet verbreitet oder bereitgestellt werden, führt das zu keiner anderen Beurteilung. Das Internet mag seinen besonderen Wert in seinen fast anarchischen Strukturen haben, ein rechtsfreier Raum ist es nicht. Es ist auch kein rein privater Raum, sondern in seinen unterschiedlichen Erscheinungsformen auch auf Breitenwirkung angelegt. Auch dies stellt der JMStV klar. Zwar wird darin erstmals die Kategorie der geschlossenen Gruppe erwachsener Nutzer im Internet rechtlich eingeführt und ein gewisser Vorrang ihrer Bedürfnisse akzeptiert. Dies gilt aber gerade nicht für grundsätzlich unzulässige Hass- und Gewaltinhalte.

Wenig hilfreich ist auch der Hinweis, dass die Ermittlung der Verantwortlichen im Internet schwierig, unmöglich oder wegen der Ausweichmöglichkeit auf z.B. amerikanische Server folgenlos sei. Auch auf anderen Gebieten bestehen solche Schwierigkeiten. Jedoch käme beispielsweise niemand auf die Idee, die Eigentumsgarantie in Art. 14 GG abzuschaffen, weil bei Autodiebstählen durch international agierende Täter die Aufklärungsquote ohnehin gering ist. Der JMStV trägt seinen Teil bei. In der Begründung wird klargestellt, dass, wenn der Anbieter nicht zu greifen ist, unter bestimmten Voraussetzungen durchaus gegen den Access-Provider vorgegangen werden kann.

Sicher ist es vor allem für die Landesmedienanstalten ungewohnt, dass Verstöße im Internet im Gegensatz zu Verstößen im klassischen Rundfunk nicht in aller Öffentlichkeit stattfinden und von der breiten Öffentlichkeit wahrgenommen werden. Auch in technischer Hinsicht werden sie – wie bisher auch – ständig dazulernen. Natürlich reicht es auch nicht aus, Verbotsnormen aufzustellen und zu hoffen, damit wären Jugendschutz und Schutz der Menschenwürde ausreichend sichergestellt. Bemühungen um internationale Standards, um eine funktionierende Selbstkontrolle und die Verbesserung der Situation des Nutzers durch Kompetenzvermittlung, Bereitstellung von Filtersystemen oder Kennzeichnung von Angeboten müssen flankierende Maßnahmen sein.

4.6.5 Ausblick

Die Installierung der KJM und der Selbstkontrolleinrichtungen sowie der Erlass der notwendigen Satzungen und Richtlinien sind die ersten Herausforderungen, vor die uns der JMStV stellt. Es bleibt zu hoffen, dass sich auch für das Internet Einrichtungen der freiwilligen Selbstkontrolle bilden werden. Gerade weil das Internet für Millionen redlicher Anbieter und Nutzer eine einmalige Chance zu einer Weltgemeinschaft bietet, sollte das Interesse groß sein, sich von denjenigen, die das Medium missbrauchen, zu distanzieren. Auch zukünftig wird die Diskussion über Möglichkeiten und Grenzen der Aufsicht im Internet nicht an Bedeutung verlieren. Allerdings sollte der Schwerpunkt hierbei nicht bei dem „Ob" des Tätigwerdens, sondern beim „Wie" der Optimierung liegen.

Die Landesmedienanstalten werden von Zeit zu Zeit, auch zuletzt noch in Bezug auf den JMStV, mit Papiertigern verglichen. Viel passender erscheint hier ein Vergleich der Landesmedienanstalten und aller am Prozess des Schutzes der Jugend und der Menschenwürde Beteiligten mit anderen Tieren, den Ameisen: Sie sind viele, sie sind zu komplexer Zusammenarbeit fähig, verfolgen unbeirrbar ihre Ziele und – sie können sehr lästig sein.

5. Alternative Lösungsansätze: Verzahnung von Regulierung und Selbstregulierung

5.1 Vorschläge der Politik

Prof. Dr. Miriam Meckel

Nach empirischen Studien erfährt antisemitisches oder volksverhetzendes Gedankengut eine immer rasantere Verbreitung im Internet. Diese Inhalte gilt es zu bekämpfen: Es darf und kann schlichtweg nicht in Frage gestellt werden, dass Straftaten immer verhindert oder verfolgt werden sollten, egal ob sie mittels Internet oder anders begangen werden. In Betracht kommen drei Handlungsansätze: Eine Selbstkontrolle der Provider, ein Selbstschutz der Internetnutzer und die staatliche Kontrolle oder Intervention.

Die Sperrverfügungen der Düsseldorfer Bezirksregierung können letztlich nur ein Instrument sein, um die schlimmsten Auswüchse unter Kontrolle zu bringen. Es ist evident, dass sowohl den Nutzern als auch den Anbietern Methoden zu Verfügung stehen, Sperrmechanismen zu unterlaufen. Auch setzt die Sperrung die Kenntnis der zuständigen Behörden von den unzulässigen Inhalten voraus: Die Masse der Internetinhalte wird es hoheitlichen Stellen nahezu unmöglich machen, flächendeckend eine wirksame Kontrolle durchzuführen.

Erfolg versprechend erscheint eine Kombination aller gangbaren Wege: Weder kann sich der Staat unter Berufung auf Mechanismen der Selbstkontrolle aus der Verantwortung verabschieden, noch können umgekehrt Provider und Nutzer durch staatliche Regulierung aus der Verantwortung entlassen werden. Zum einen wäre allein staatliche Regulierung schlichtweg zu langsam und kann nicht alles erfassen. Zum anderen würde damit möglicherweise ein falsches Signal gesetzt: Die Bereitschaft der User, z.B. Hotlines zu nutzen oder in virtuellen Polizeirevieren Informationen zu hinterlassen, ist ungebrochen und es wäre leichtfertig, dieses Potenzial ungenutzt zu lassen.

Die Frage ist nicht: Welches Instrument wählen wir? Sondern: Wie können wir die Instrumente verbessern? Und hier heißt das Stichwort: Verzahnung. So stellt sich doch die Frage, ob nicht die bestehenden Selbstregulierungsmaßnahmen noch stärker auf die Bekämpfung rechtsextremistischer und fremdenfeindlicher Inhalte ausgerichtet werden können. Für eine solche Konzeption könnte das in Australien gebräuchliche Modell wertvolle Hinweise geben: Die Aufsichtsbehörde übernimmt gewichtige Initiativ-, Koordinierungs- und Beratungsaufgaben. Sie betreibt Hotlines, empfiehlt Filtersoftware usw. Andererseits erklären sich Host- und Access-Provider dazu bereit, Filtersoftware zum Herunterladen zur Verfügung zu stellen und die Nutzer in ihren Gebrauch einzuweisen.

Nur im Wege einer Selbstverpflichtung kann erreicht werden, dass sich die Provider engagieren und z.B. Filter zum Herunterladen bereitstellen. Sicher: Eine solche Selbstverpflichtung schützt im Zweifelsfalle nicht vor weiteren hoheitlichen Eingriffen. Andererseits gilt es hier vorbildliches Providerverhalten zu belohnen, etwa über die Verleihung von Qualitätskennzeichen. Für ein solches Vorgehen enthält das neue Landesmediengesetz Nordrhein-Westfalen eine gesetzliche Grundlage: Das Gesetz sieht vor, dass die Landesmedienanstalt ein solches „Siegel" vergeben kann, soweit dies der Förderung der Belange der Mediennutzer dient – ihnen z.B. eine Hilfestellung bei der Providerauswahl gibt.

Letztlich muss die Kooperation von Internetnutzern, von Anbietern und Aufsichtsbehörden die Verzahnung von Regulierung und Selbstkontrolle zielorientiert sicherstellen. Hoheitliche Maßnahmen können in globalen Computernetzen nur eine begrenzte Wirkung entfalten. Um unsere Werte- und Rechtstradition zu bewahren, bedarf es darüber hinaus eines verstärkten Engagements der Net-Community selbst, wie aber auch der gesamten Zivilgesellschaft. Letztlich wird es zu einer Kooperation von Internetnutzern, von Anbietern und Aufsichtsbehörden kommen, um die Verzahnung von Regulierung und Selbstkontrolle zielorientiert sicherzustellen.

5.2 Selbstregulierung in der Praxis

Sabine Frank

5.2.1 Grundlagen einer effektiven Selbstkontrolle

Die Bezeichnung „Selbstkontrolle" bezeichnet Kontrollaktivitäten bestimmter Organisationseinheiten, um ein Fehlverhalten in ihrem Innenbereich zu vermeiden bzw. zu beseitigen. Deshalb stellt Selbstkontrolle als ein Element der Bürgergesellschaft eine besondere Form gestärkter gesellschaftlicher Eigenverantwortung der sich einer Selbstkontrolle anschließenden Unternehmen dar. Die Selbstkontrolle ist dabei das Korrelat von Freiheit und Verantwortung; es ist das Zeichen der verantwortungsbewussten Ausübung von Grundrechten.

Voraussetzungen von Selbstkontrolle sind zunächst der Zusammenschluss mehrerer Beteiligter einer Branche und deren Übereinstimmung über ein bestimmtes Verhalten (Verhaltenskodex). Darüber hinaus muss eine Selbstkontrolleinrichtung Kontrollmöglichkeiten besitzen und gegebenenfalls ein Fehlverhalten ihrer Mitglieder ahnden. Die Wirksamkeit der Selbstkontrolle hängt dabei unter anderem von der Zahl der Unternehmen ab, die den Verhaltenskodex und die Sanktionen anerkennen.

5.2.2 Freiwillige Selbstkontrolle Multimedia – ein Beispiel für eine effiziente Selbstkontrolle

Die Freiwillige Selbstkontrolle Multimedia (FSM) existiert seit 1997. Der Verein widmet sich besonders dem Jugendschutz und der Bekämpfung illegaler Inhalte in Online-Medien. Seine Mitglieder sind Medien- und Telekommunikationsverbände sowie Unternehmen, die Online-Angebote betreiben. Rund 440 Unternehmen haben bis heute den Verhaltenskodex der FSM schriftlich anerkannt und die FSM mit der Wahrnehmung der Aufgaben des Jugendschutzbeauftragten betraut. Die Tendenz ist steigend. Die FSM erbringt Dienstleistungen für die Allgemeinheit und spezielle Dienstleistungen für ihre Mitglieder. So betreibt die FSM eine Beschwerdestelle, an die sich jedermann kostenlos mit Beschwerden über rechtswidrige und jugendgefährdende Inhalte wenden kann. Das Beschwerdeformular und der Verhaltenskodex sind auf der Website der FSM *http://www.fsm.de* abrufbar. In den letzten zwei Jahren hat die FSM ca. 2.800 Beschwerden bearbeitet, von denen sich weniger als 1% der Beschwerden gegen ein Mitglied der FSM richteten. Gleichzeitig konnten wir bei über 80% der Beschwerden, die Angebote aus Deutschland betrafen, erreichen, dass die Inhalteanbieter die Angebote entfernt bzw. so verändert haben, dass es den gesetzlichen Anforderungen entspricht.

Ergibt sich aus einer Beschwerde der Verdacht, dass eine konkrete Gefahr für Leib, Leben oder Freiheit von Personen besteht, so teilt die FSM der zuständigen Behörde den Inhalt der Beschwerde mit. Name und Anschrift des Beschwerdeführers werden dabei jedoch streng vertraulich behandelt und nicht bekannt gegeben.

Die FSM hat frühzeitig erkannt, dass in einem internationalen Medium wie dem Internet die internationale Kooperation der einzige Weg ist, um gegen die Schattenseiten des Internet effektiv vorgehen zu können. Aus diesem Grunde hat die FSM 1999 mit sieben weiteren Organisationen den europäischen Dachverband der Beschwerdehotlines INHOPE (Internet Hotline Providers in Europe, abrufbar unter: *http://www.inhope.org* gegründet, der von der Europäischen Kommission gefördert wird. Mittlerweile hat INHOPE 15 Mitglieder aus 13 Ländern, darunter auch assoziierte Mitglieder aus den Vereinigten Staaten und Australien.

5.3 Das ICRA-Selbstklassifizierungs-, Kennzeichnungs- und Filtersystem

Carsten Welp, Dr. Thomas Hart

Noch nie waren weltweit so viel Meinungen, Informationen und Inhalte für jedermann so leicht zugänglich wie im Zeitalter des Internet. Doch dies bringt auch Gefahren mit sich: Internet-Seiten mit pornographischen, rassistischen oder politisch extremistischen Inhalten sind frei zugänglich und oft in den Ländern, in denen sie in das Internet gestellt werden, auch nicht strafbar. Besonders Eltern sind darüber besorgt, dass ihre Kinder mit diesen potenziell schädlichen Inhalten konfrontiert werden. Anerkannt ist, dass der Jugendschutz im Internet gesichert sein muss, damit es sich zu dem freien und globalen Informationsmedium entwickeln kann.

5.3.1 Das ICRA-System

Ein transparentes, neutrales und ganzheitliches System zur Filterung von Internet-Inhalten hat die Internet Content Rating Association (Vereinigung zur Klassifizierung von Internet Inhalten - ICRA)[144] entwickelt. Das ICRA-Kennzeichnungs- und Filtersystem zielt auf den globalen, interkulturellen Kontext. Es ist das Produkt eines mehrjährigen Konsultationsprozesses und besteht aus verschiedenen Elementen. Das erste Element ist die Kennzeichnung von Internet-Seiten durch die Betreiber dieser Seiten, den sogenannten Anbietern von Internet-Inhalten, anhand eines im Dezember 2000 vorgestellten Klassifizierungssystems. Als zweites Element werden den Internet-Nutzern Softwarelösungen unentgeltlich zur Verfügung gestellt, die auf dem Rechner des Internet-Nutzers installiert werden und je nach Konfiguration gekennzeichnete Internet-Seiten lesen und verarbeiten, d.h. filtern können. Ein drittes Element bilden die komplementären Positiv- und Negativlisten.

5.3.2 Die Selbstklassifizierung und Kennzeichnung von Internet-Inhalten

Im Rahmen des ICRA-Systems wird den Betreibern von Internet-Seiten die Möglichkeit geboten, auf einem innerhalb der ICRA-Website *http://www.icra.org* aufrufbaren Online-Fragebogen anzugeben, welche Inhalte ihre Internet-Seite enthält oder nicht enthält. Die Klassifizierung der Inhalte erfolgt in jeder der Kategorien, indem der Anbieter des Internet-Inhalts bestimmte „Deskriptoren" anklickt, die den vorhandenen Inhalt wertneutral beschreiben. Nach diesen Beschreibungen erstellt ICRA sodann ein Etikett, computersprachlich ein „html meta tag (PICS)".

(144) ICRA ist eine gemeinnützige Organisation mit Hauptsitz in Großbritannien. ICRA setzt sich für eine verantwortungsvolle Entwicklung und Verbreitung des Internet ein und wird von führenden kommerziellen und nicht-kommerziellen Akteuren der Informationsgesellschaft getragen. Eine aktuelle Übersicht der Mitglieder ist abrufbar unter: http://www.icra.org.

Die Plattform for Internet Content Selection (PICS) ist ein Set von Software-Spezifikationen für Filtersysteme, das vom World Wide Web Consortium (W3C) erstellt worden ist. Auf der Grundlage von PICS lassen sich Etiketten erstellen, die einzelnen Internet-Adressen (Universal Resource Locators, URLs) zugeordnet werden können. Ein PICS-Etikett ist im Wesentlichen eine Angabe darüber, welcher Typ von Daten auf einer Seite unter einer bestimmten Internet-Adresse zu finden ist. Bei ICRA enthält das Etikett die angegebenen „Deskriptoren" der auf der Seite vorhandenen Inhalte in allen Kategorien. Der Anbieter bekommt das Etikett auf seinem Bildschirm angezeigt und kann es dort kopieren. Ferner erhält er Informationen, wie er das Etikett seiner Internet-Seite anheften, d.h. in den HEAD-Abschnitt seines html - Quellcodes einfügen kann. Das eingefügte Etikett ist als solches nicht direkt auf der Internet-Seite sichtbar. Allerdings können die Betreiber folgendes visuelles Kennzeichen anbringen:

Das verwendete PICS-System ermöglicht es, entweder die gesamte Seite oder einzelne Dateiverzeichnisse jeweils gesondert zu kennzeichnen. Der gesamte Vorgang dauert weniger als 10 Minuten und ist einfach zu handhaben. Die verschiedenen Internet-Inhalte können in folgenden Kategorien klassifiziert werden:

Nacktdarstellungen und sexuelle Inhalte
- Erektionen oder detaillierte Darstellungen der weiblichen Genitalien
- Männliche Genitalien
- Weibliche Genitalien
- Weibliche Brüste
- Entblößter Hintern
- Sichtbarer Geschlechtsakt
- Verhüllt dargestellter oder angedeuteter Geschlechtsakt
- Sichtbares Berühren der Geschlechtsorgane
- Leidenschaftliches Küssen
- Kontext: Kunst, Erziehung, Medizin

Gewalt
- Sexualgewalt/Vergewaltigung
- Blut und Blutvergießen, Menschen
- Blut und Blutvergießen, Tiere
- Blut und Blutvergießen, Fantasiefiguren (einschließlich Zeichentrickfilme)
- Tötung von Menschen
- Tötung von Tieren
- Tötung von Menschen Fantasiefiguren (einschließlich Zeichentrickfilme)
- Absichtliche Verletzung von Menschen
- Absichtliche Verletzung von Tieren
- Absichtliche Verletzung von Fantasiefiguren (einschließlich Zeichentrickfilme)
- Absichtliche Sachbeschädigung
- Kontext: Kunst, Erziehung, Medizin, Sport

Sprachgebrauch
- Sexualisierte Sprache
- Derber Sprachgebrauch oder Gotteslästerung
- Gemäßigte Kraftausdrücke

Andere Themenbereiche
- Positive Darstellung von Tabakwaren
- Positive Darstellung von Alkohol
- Positive Darstellung von Drogen
- Glücksspiele
- Positive Darstellung von Waffen
- Aufruf zur Diskriminierung von oder Gewalt gegen Personen
- Inhalte, die jüngeren Kindern ein schlechtes Beispiel setzen können
- Inhalte, die jüngere Kinder beeinträchtigen könnten

Chat
- Chat
- Ausschließlich gemäßigter, für Kinder und Jugendliche geeigneter Chat

Abb. 4: Deskriptoren

5.3.3 Die Filtersoftware

Damit die angehefteten Etiketten beim Aufruf einer Internet-Seite gelesen und interpretiert werden können, bedarf es einer geeigneten Filtersoftware. ICRA bietet einen solchen Filter unentgeltlich zum download an.

a. Die Einstellung der Filter- Software

Damit die Filtersoftware für den Nutzer einsatzfähig ist, muss der Filter konfiguriert werden. Die Filterkonfiguration kann der Nutzer selbst bestimmen oder durch Dritte einstellen lassen. In jedem Fall kann der Nutzer des Filtersystems selbständig entscheiden, was gefiltert wird und was nicht. Jeder Nutzer kann gegen Eingabe eines Passwortes innerhalb der genannten Kategorien genau festlegen, welche der beschriebenen Inhalte von dem Filter zugelassen und welche geblockt werden sollen. Zusätzlich kann eingestellt werden, ob nicht etikettierte Internet-Seiten generell gesperrt oder zugelassen werden.

Inhalte liegen im Internet nicht nur in Form von Websites vor. Auch in Newsgroups, über E-Mail oder in Chat Rooms können Nutzer kommunizieren. Weitere Dienste, die durch das Filtersystem maßgenau gesperrt oder zugelassen werden können, sind sichere Seiten, wie sie etwa bei online-Käufen in der Regel verwendet werden, und FTP, mit dem Dateien im Internet übertragen werden können. Der Nutzer kann auch weitere einzelne Ports sperren, beispielsweise um auf seinem System den Austausch von Dateien über bestimmte peer-to-peer Tauschbörsen zu sperren.

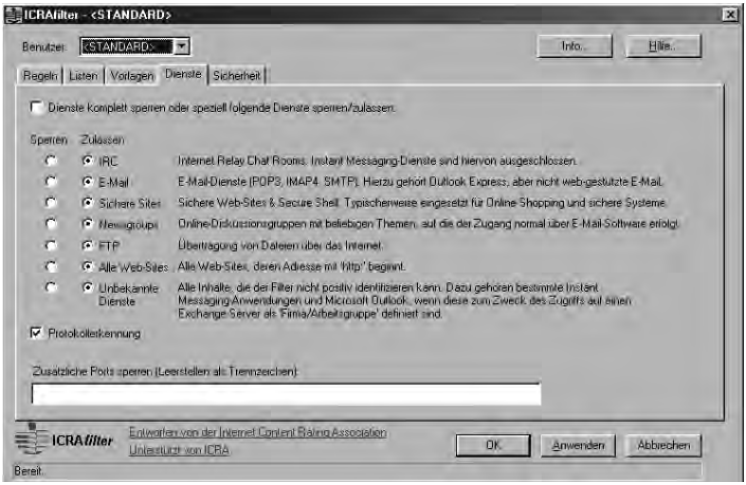


Abb. 5: Einstellung der Filtersoftware: Dienste

Die vielfältigen Möglichkeiten, den ICRA-Filter auf seine eigenen Bedürfnisse anzupassen, ermöglichen es dem Nutzer, auf seinem System einen nach den eigenen Vorstellungen und individuellen Maßgaben sicheren Zugang zum Internet einzurichten.

Eltern, die sich mit der Konfiguration des neuen ICRA-Filters schwer tun, können daneben auch aus einem Angebot von bereits konfigurierten Filterschablonen (templates) auswählen. Diese werden von verschiedensten Institutionen angeboten und erleichtern die Anwendung des ICRA Filters. So konfiguriert eine Organisation beispielsweise einen Filter speziell für die Nutzergruppe der Acht- bis Zehnjährigen, oder ein feststehendes Profil, das bestimmte Werte widerspiegelt. Doch steht es jedem Nutzer frei, die Voreinstellungen in solchen Schablonen nachträglich wieder zu verändern. Je nach Kennzeichnung der Seite und Einstellung des Filters wird der Aufruf einer Internet-Seite erlaubt oder geblockt. Im letzteren Fall wird das ICRA-System dem Nutzer des Filters den Grund für die Sperrung anzeigen. Wurde die Seite gesperrt, weil sie den Einstellungen einer Filterschablone widerspricht, so kann der Nutzer die Sperrung durch Eingabe des Passwortes umgehen und sich die geblockte Seite anzeigen lassen kann.

b. Die Einbindung von Positiv- und Negativlisten

Die dritte Ebene des neuen ICRA-Systems besteht in der Verwendung von URL-Listen, die von unterschiedlichsten Organisationen erstellt werden und mit dem Filtersystem kompatibel sind. ICRA selbst wird allerdings keine Listen zur Verfügung stellen. Denn ICRA enthält sich selbst jeder moralischen Wertung von Internet-Inhalten. Das ICRA-System ist offen, um moralische Wertvorstellungen solcher Institutionen, denen die Nutzer des Filters vertrauen, zum Ausdruck zu bringen (z.B. Jugendschutz- oder Elternverbände).

Positivlisten beinhalten die Wertung, dass die aufgeführten URLs, die nach der individuellen Konfiguration des Filters eigentlich gesperrt sind, ausnahmsweise freigeschaltet sein sollen. Dies kann beispielsweise für Internet-Seiten Sinn machen, auf denen eigentlich als schädlich bewertete Inhalte in Kontexten auftauchen, die eine Freischaltung rechtfertigen; oder für noch nicht nach dem ICRA-System etikettierte Internet-Seiten, wenn der Filter so konfiguriert ist, dass nicht etikettierte Seiten generell geblockt werden. So können Eltern insbesondere sicherstellen, dass eine bestimmte Auswahl von Internet-Seiten für ihr Kind stets zugänglich bleibt.

Negativlisten beinhalten die Wertung, dass die Inhalte der aufgeführten URLs per se schädlichen Charakter haben und unter keinen Umständen aufgerufen werden sollten. Die Sperrung der Internet-Seite wird in diesen Fällen unter Verweis auf die aktivierte Liste angezeigt. Der Nutzer hat in dem neuen ICRA-Filter in jedem Fall das Recht, unter Verwendung seines Passwortes die Sperrung wieder aufzuheben.

Diese Listen lassen sich vom Nutzer jederzeit ergänzen durch individuell eingepflegte URLs, die freigeschaltet oder gesperrt werden sollen. Zu beachten ist allerdings, dass die von unterschiedlichen Organisationen angebotenen Negativlisten nirgendwo im Klartext erscheinen. Die Negativlisten werden von den anbietenden Organisationen in verschlüsselter Form übermittelt. Der Nutzer selbst kann sie nicht auslesen. So wird vermieden, „best-of"-Listen problematischer oder gar illegaler Inhalte im Internet bekannt zu machen.

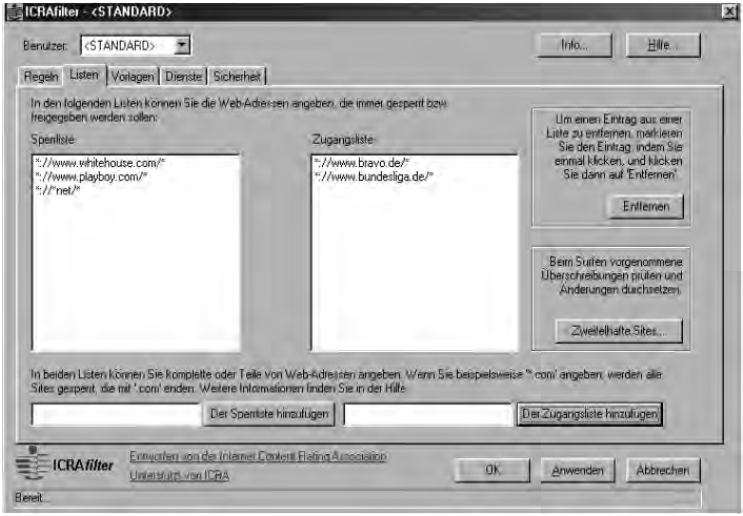


Abb. 6: Einstellung der Filtersoftware: Listen

5.3.4 Warum also ICRA?

Das neue ICRA-Kennzeichnungssystem ist neutral und objektiv, so dass es die wertfreie Klassifizierung aller denkbaren Internet-Inhalte ermöglicht. Der Filter andererseits kann ganz individuell je nach den Bedürfnissen der Nutzer konfiguriert werden. Dadurch ist das ICRA-System in besonderer Weise für die konvergente und globale Welt der Neuen Medien geeignet. Indem das System im wesentlichen auf einer Selbstklassifizierung der Internet-Inhalte durch die Anbieter von Inhalten und Diensten basiert, vermeidet es zudem Zensur von Dritten und gewährleistet damit die Meinungs- und Informationsfreiheit im Internet.

Für den Anbieter von Internet-Inhalten bringt die Kennzeichnung mit dem ICRA-System nur Vorteile: Bei Internet-Seiten für Kinder erzeugt die Etikettierung mehr Aufrufe der Seite. Bei Internet-Seiten für Erwachsene ermöglicht es die Bewerbung der Inhalte

im Internet auf eine Weise, die die größtmögliche Sicherheit vor dem Zugriff von Kindern bietet. Dies verhindert nicht nur hoheitliche regulatorische Maßnahmen zum Schutz der Kinder, sondern gewährleistet auch, dass die Zielgruppe der Erwachsenen effektiver erreicht wird. Schließlich erhöht die Kennzeichnung der Internet-Inhalte die Transparenz im Netz und beugt dadurch generellen Vorurteilen der Eltern gegenüber dem Umgang mit dem Medium Internet vor.

Auch wenn nicht davon ausgegangen werden kann, dass alle Internet-Seiten mit dem ICRA-System gekennzeichnet werden, so sollte dies seine Tauglichkeit nicht beeinträchtigen. Denn die 1000 meist besuchten Internet-Seiten machen etwa 80% der gesamten Internet-Nutzung aus. Das bedeutet, dass mit der Kennzeichnung von nur 1000 Internet-Seiten 80% aller Vorgänge im Internet kinderfreundlich gesichert werden können. Ferner ist ICRA darum bemüht, dass die meisten kinderspezifischen sowie alle auf Erwachsene abzielenden Seiten klassifiziert werden. Wenn es in den nächsten Monaten gelingt, dass alle weltweit gängigen Kinderseiten aufgerufen und die meistbesuchten Erwachsenen-Seiten gesperrt werden können, hätte das ICRA-System eine bisher unbekannte Sicherheit im Netz erzielt und käme einem Standard gleich. Aus Sicht der Eltern ist auch ICRA selbstverständlich kein absolut sicheres Instrument, um ihre Kinder vor schädlichen Inhalten zu bewahren. Kinder werden auch mit dem Filter auf jugendgefährdende Seiten stoßen. Allerdings wird durch die Verwendung des ICRA-Filters die Gefahr zumindest minimiert. ICRA ist ein Hilfsmittel; nicht mehr, aber auch nicht weniger.

5.4 Bekämpfung illegaler und jugendgefährdender Inhalte im Internet – Probleme und Lösungen bei der Rechtsdurchsetzung

eco-Verband

5.4.1 Einleitung

Das Internet ist ein globales, dezentrales Netzwerk. Die technische Struktur des Internet ermöglicht es, Inhalte an beliebig vielen Stellen des dezentralen Netzwerkes einzustellen und von beliebig vielen Punkten über beliebig viele unterschiedliche Verbindungen zu erreichen. Zudem ist das Internet ein dynamisches Medium; Inhalte sind nicht statisch, sondern unterliegen einer permanenten Veränderung und Aktualisierung, inhaltlich wie physikalisch.

Das Internet hat unsere Gesellschaft nachhaltig verändert. Erst das world wide web hat es vielen Menschen ermöglicht, einen einfachen und kostengünstigen Zugang zu Informationen zu erhalten.

Es muss an dieser Stelle darauf hingewiesen werden, dass die positiven Inhalte und Möglichkeiten des Internet die negativen bei weitem überwiegen. Das Internet spiegelt die Vielschichtigkeit der Gesellschaft wie kein anderes Medium wider, deshalb finden sich dort auch negative Entwicklungen, – speziell im Bereich der illegalen und jugendgefährdenden Inhalte. Die Bekämpfung illegaler und jugendgefährdender Inhalte stellte seit Beginn der Massennutzung des Internets staatliche Stellen und die Internetwirtschaft vor neue Herausforderungen.

Das Internet ist kein rechtsfreier Raum. Was offline verboten ist, ist auch online nicht erlaubt. Dies ist unstreitig. Eine von der Bekämpfung illegaler und jugendgefährdender Inhalte strikt zu trennende Frage ist jedoch die der Durchsetzung nationaler Rechtsvorschriften in einem globalen, dezentralen Netzwerk: Wie sollen nationale Rechtsvorschriften in einem internationalen Kontext durchgesetzt werden, wenn sich die illegalen Inhalte im Ausland befinden? In einem globalen Netzwerk wie dem Internet stoßen die bekannten staatlichen Aufsichtsmaßnahmen an ihre Grenzen. Vor diesem Hintergrund kommt der Selbstkontrolle der Internetwirtschaft eine zentrale Bedeutung zu, vgl. unten.

Wichtigste Voraussetzung für eine effektive und nachhaltige Bekämpfung illegaler und jugendgefährdender Inhalte in einem globalen dezentralen Medium wie dem Internet ist es, auf eine internationale Rechtsangleichung (vgl. bspw. die Cyber-Crime Convention des Europarates) hinzuarbeiten und gemeinsam in Abstimmung mit europäischen Staaten und Drittstaaten zu handeln.

5.4.2 Selbstkontrolle der Internetwirtschaft

Illegale Internetinhalte müssen dort bekämpft werden, wo sie zum Abruf über das Internet bereitgestellt werden. Daher muss im Ursprungsland, wo die Inhalte ins Netz gestellt wurden, angesetzt werden. Nur dort besteht die Möglichkeit, die Täter zu fassen oder wenigstens die fraglichen Inhalte dauerhaft von den Servern zu entfernen. Durch nationale Maßnahmen wie bspw. Eingriffe in die Netzwerkintegrität (wie die Sperrung bei Access-Providern) werden illegale Inhalte nicht entfernt, sondern bleiben weiterhin verfügbar. Damit wird das Problem nicht gelöst, sondern höchstens verschleiert.

5.4.3 Aktivitäten der Internetwirtschaft auf nationaler Ebene

Der Verband der deutschen Internetwirtschaft – eco Forum e.V. – setzt bereits seit 1996 auf Selbstkontrolle. In diesem Jahr ist der Arbeitskreis Internet Content Task Force (ICTF) gegründet worden. Im Rahmen dieses Arbeitskreises wird auch die ICTF-Hotline betrieben. Aus der ICTF gingen in Folge die NewsWatch-Hotline (heute ICTF-Hotline) und aus der Zusammenarbeit mit anderen Organisationen die Freiwillige Selbstkontrolle Multimedia e.V. (FSM), die Internet Content Rating Association (ICRA), sowie die Internet Hotline Providers in Europe Association (INHOPE) hervor. Über die ICTF-Beschwerde-Hotline kann jedermann illegale Inhalte im Internet melden, damit unverzüglich entsprechende Maßnahmen eingeleitet werden können. In Frage kommt hier die Löschung des illegalen Materials bei dem Hostprovider und bei Bedarf die Einschaltung und Zusammenarbeit mit den Strafverfolgungsbehörden. Durch dieses Engagement der deutschen Internetwirtschaft ist das Problem illegaler Inhalte bei deutschen Providern beziehungsweise auf deutschen Servern stark zurückgegangen und besteht somit weitestgehend nicht mehr.

5.4.4 Aktivitäten der Internetwirtschaft auf internationaler Ebene

Eco verfolgt auch auf internationaler Ebene im Rahmen von INHOPE den Ansatz einer nachhaltigen und effektiven Bekämpfung illegaler Inhalte. Um eine grenzüberschreitende Arbeit von Hotlines zu ermöglichen, wurde im Jahre 1999 die INHOPE Association ins Leben gerufen. Eines der acht Gründungsmitglieder dieser von der EU im Rahmen des Safer Internet Action Plans finanziell unterstützten Organisation ist eco (neben der FSM und jugendschutz.net). Inzwischen ist das Netzwerk auf 17 Mitglieder in Europa, den USA und Australien gewachsen. Bewerbungen weiterer Hotlines liegen vor. Ziel ist, eine grenzüberschreitende Beschwerdebearbeitung zu gewährleisten, den Austausch von Expertenwissen zu fördern und gemeinsame Standards und Herangehensweisen

– bei Beachtung der jeweils einschlägigen nationalen gesetzlichen Regelungen – zu ermöglichen. Die Hotlines müssen zur Erlangung der Mitgliedschaft nachweisen, dass sie die Unterstützung sowohl der Polizei, der Internetindustrie, wie auch der Nutzer genießen. Auf diese Weise soll eine optimale Wirkung sichergestellt werden. Die Kooperation der Internethotlines hat in der Vergangenheit bereits vielfach zu einer schnellen Löschung und Strafverfolgung der illegalen Inhalte im Ursprungsland des Angebotes geführt. Im Rahmen des „Safer Internet Action Plan" wird INHOPE von der Europäischen Union unterstützt. eco und die FSM stellen jeweils noch ein weiteres Vorstandsmitglied der Organisation. Dies verdeutlicht den Stellenwert, den die Bekämpfung illegaler Inhalte im Internet bei der deutschen Internetwirtschaft einnimmt.

5.4.5 Fazit

In einem globalen Medium wie dem Internet ist es zwingend erforderlich auf eine internationale Rechtsangleichung hinzuarbeiten und gemeinsam in Abstimmung mit europäischen Staaten und Drittstaaten zu handeln, um nationale oder regionale Alleingänge zu vermeiden, die wenig Erfolg versprechend sind. Illegale und jugendgefährdende Inhalte im Internet werden am effektivsten dort bekämpft, wo sie zum Abruf bereitgehalten werden. Nur im Ursprungsland des Angebotes können derartige Inhalte effektiv und nachhaltig durch die Löschung und gegebenenfalls Strafverfolgung der Täter bekämpft werden.

Die Inanspruchnahme in Deutschland ansässiger Access-Provider zur Bekämpfung illegaler, im Ausland gehosteter Inhalte durch die Bezirksregierung ist wenig zielführend. Access-Provider vermitteln lediglich den Zugang zum Internet und haben keinen Einfluss auf die abgerufenen Inhalte, da sich die Angebote außerhalb des Herrschaftsbereiches der Access-Provider befinden. Technisch sind, nach allgemeiner Expertenauffassung, Sperrungen bei Access-Providern nicht dazu geeignet, einen Zugang zu bestimmten Inhalte zu verhindern. Aufgrund der mangelnden Effizienz der Sperrungen bei Access-Providern sind die Angebote trotz ihrer Sperrung weiterhin abrufbar. Darüber hinaus sind Sperrungen nicht zielgerichtet möglich und haben schädliche Nebenwirkungen, da von den Sperrungen ebenfalls nicht nur rechtswidrige, sondern ebenfalls rechtmäßige, nicht zu beanstandende Inhalte betroffen sind. Selbst wenn es juristisch möglich sein sollte, technische Sperrungen von den Providern zu verlangen, so heißt dies noch nicht, dass sie auch ein geeignetes und wirkungsvolles politisches Mittel sind, um gegen die Verbreitung illegaler Inhalte vorzugehen. Auch das Europäische Parlament hält in einer Entschließung vom 11. April 2002 die Sperrung von Websites nicht für eine wirksame europäische Lösung zur Bekämpfung schädigender und illegaler Inhalte im Internet. In dem Bericht zeigt sich das Europäische Parlament

besorgt darüber, 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"*[145].

Die Bezirksregierung möchte mit der Inanspruchnahme der Access-Provider ein Zeichen setzten und eine Vorreiterrolle auch für andere Aufsichtsbehörden übernehmen. Ihr ist sehr wohl bewusst, dass durch die Sperrungen bei den Access-Providern der Abruf lediglich erschwert, aber nicht verhindert werden kann. Das Handeln der Bezirksregierung ist geprägt von der Vorstellung eines „starken Staates". Dabei nimmt sie großen Schaden für die Internetnutzer und die Internetindustrie billigend in Kauf.

Die Bezirksregierung zeigt mit der Inanspruchnahme der Access-Provider auch die Grenzen staatlichen Handels: Die nachhaltige Durchsetzung nationaler Rechtsvorschriften durch ineffektive und leicht zu umgehende Sperrungen bei Access-Providern ist in einem globalen, dezentralen Netzwerk nicht zu gewährleisten. Würden nicht alle Beteiligten verlieren, wenn Sperrverfügungen als ein geeignetes Aufsichtsinstrument angesehen würden? Der Nutzer, weil er vor etwas geschützt wird, was er sich sowieso nicht anschaut. Die Wirtschaft, weil sie technisch ineffektive Maßnahmen vorzunehmen hätte. Die Politik, weil sie an Glaubwürdigkeit verlöre.

(145) Bericht über den Evaluierungsbericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Empfehlung des Rates vom 24. September 1998 in Bezug auf den Jugendschutz und den Schutz der Menschenwürde (KOM(2001) 106 – C5-0191/2001 – 2001/2087(COS)), Nr. 16.

5.5 Aktivitäten der BITKOM

Wolf Osthaus

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) beobachtet die Existenz rassistischer und fremdenfeindlicher Inhalte im Internet mit großer Sorge, begrüßt daher die Auseinandersetzung mit diesem Thema und nimmt hierzu, wie folgt, Stellung:

5.5.1. Ausgangssituation

Das Internet ist ein in dieser Form zuvor nie gekannter Marktplatz der Ideen und Meinungen. Es erlaubt einen wesentlich einfacheren Austausch von Meinungen, erleichtert den Kontakt zu Gleichgesinnten und den Aufbau und die Organisation von Interessengruppen. Der einzelne Nutzer gewinnt Zugang zu einem wesentlich breiteren Meinungsspektrum. Das Internet wird hierdurch zu einem Medium, das die Meinungs- und Informationsfreiheit und darüber auch die Demokratie fördert.

Der Missbrauch dieser neuen Freiheiten zur Verbreitung illegaler, menschenverachtender Botschaften ist eindeutig und mit aller Schärfe zu verurteilen. Alle gesellschaftlichen Kräfte müssen sich solchen Tendenzen klar entgegenstellen. Gerade die von BITKOM vertretenen Wirtschaftsbranchen sind in besonderer Weise von internationaler Zusammenarbeit geprägt und leben von der Mischung und dem Austausch der verschiedenen Kulturen dieser Welt.

5.5.2 Kritik der aktuellen Vorgehensweise

Sperrverfügungen gegen Zugangsvermittler sind kein geeignetes Mittel zum Umgang mit illegalen Inhalten. Ungeachtet der Details der juristischen Diskussionen über die Zulässigkeit von Sperrverfügungen ist festzuhalten, dass die Zugangsvermittler nicht für die von ihnen durchgeleiteten Inhalte verantwortlich sind und eine Inanspruchnahme allein als Nichtstörer in Frage käme. Dann sind jedoch in jedem Fall auch die allgemeinen polizeirechtlichen Grundsätze zur Entschädigung bei der Inanspruchnahme eines Nichtverantwortlichen anzuwenden.

Sperrverfügungen verursachen erhebliche Freiheitsbeschränkungen und Kosten, ohne dass dem tatsächlich ein maßgeblicher Schutzeffekt als Rechtfertigung gegenüberstünde. Durch ein Blocken auf Providerseite werden die Inhalte nicht entfernt, sondern lediglich in begrenztem Umfang und meist nur für begrenzte Zeit unsichtbar gemacht. Die Sperren sind unproblematisch zu umgehen. Schließlich lenkt

die Sperranordnung oft erst das Interesse der Öffentlichkeit, insbesondere von Jugendlichen, auf bestimmte Inhalte.

Für einzelne Sperrungstypen gilt Folgendes:

- Das Sperren von IP-Adressen bedeutet einen eklatanten Eingriff in die Meinungsäußerungsfreiheit, weil nicht einzelne URLs gesperrt und so auch legale Inhalte getroffen werden können, die unter derselben IP erreichbar sind. Durch die Verlagerung der illegalen Inhalte auf andere Server mit anderer IP-Adresse (das sogenannte „Spiegeln") kann der Inhalt in Minutenfrist wieder zugänglich gemacht werden. IP-Sperren können zudem aufgrund der komplexen Routingregeln zu Performanceeinbußen und Stabilitätsproblemen beim Provider führen.
- Die Manipulation der Einträge auf den DNS-Servern hätte zwar den Vorteil, gezielter als IP-Sperren Seiten blockieren zu können, ist aber besonders leicht zu umgehen, weil bereits der Zugriff auf einen anderen DNS-Server zur Umgehung genügt. Die notwendigen Einstellungsänderungen im Browser sind mit im Internet verfügbaren Anleitungen auch für einen Computerlaien ohne weiteres möglich. Dem „Spiegeln" von Seiten kann auch mit DNS-Manipulationen nicht begegnet werden. Das Verfahren bringt überdies hohe Belastungen für die betroffenen Provider für Pflege und allfällige Aktualisierungen der Sperren mit sich; dies gilt insbesondere in großen Backbones mit verteilter DNS-Struktur.
- Die Führung von Internetabfragen über „Zwangs-Proxies", auf denen dann Filter eingesetzt werden können, erfordert erheblichen technischen Aufwand, behindert komplexe, auf schnelle, unterbrechungsfreie Datenübertragung angewiesene Anwendungen und gefährdet bei den zu bewältigenden großen Datenmengen maßgeblich die Leistungsfähigkeit und die Ausfallsicherheit der Internetzugänge.

5.5.3 Alternative Lösungen / Ausblick

Für eine sinnvolle Reaktion auf illegale Meinungsäußerungen ist auf der Empfängerseite zwischen jenen zu differenzieren, die eher zufällig auf diese Botschaften stoßen, hieran aber grundsätzlich nicht interessiert sind, und solchen, die diese Inhalte aus Interesse gezielt suchen.

Die erste Gruppe der Nicht-Interessierten kann am effektivsten durch nutzerautonome Filtersysteme geschützt werden (wie z.B. das internationale Filtersystem ICRA). Gerade die besonders wichtige Aufgabe, Kinder und Jugendliche vor menschenverachtenden Inhalten zu schützen, kann so wirksam wahrgenommen werden. Die nutzerautonomen Filtersysteme bzw. die von solchen Filtern verwandten „Negativlisten" können auch von staatlichen Stellen wie z.B. dem BKA oder unabhängigen gesellschaftlichen

bzw. politischen Organisationen bereitgestellt werden. Die Filtersysteme können auch auf öffentlichen Internet-Zugangstellen in staatlichen Institutionen, also etwa in Schulen, Universitäten oder Büchereien als Schutzmechanismen eingesetzt werden.

Nutzerautonome Filtersysteme bieten keinen Schutz, wenn ein gerade an derartigen Inhalten interessierter Nutzer den Filter an seinem privaten Internetzugang nicht verwendet. Allerdings sind, wie schon dargelegt wurden, auch Sperren bei den Providern technisch ohne großen Aufwand zu umgehen. Solange also solche Inhalte im Netz bereitgestellt sind, wird man den Zugriff hierauf nicht wirksam unterbinden können. Deshalb verspricht letztlich nur der Zugriff auf die eigentlichen Urheber durchgreifenden Erfolg.

Bei den rassistischen und fremdenfeindlichen Inhalten handelt es sich um ein globales Phänomen. Nur ein kleiner Teil der betreffenden Internetseiten wird in Deutschland gehostet oder von hier aus betrieben. Soweit dies der Fall ist, besteht die Möglichkeit straf- und ordnungsrechtlicher Maßnahmen gegen die jeweiligen Urheber. Die Behörden sind aufgerufen, diese auch einzusetzen.

In der großen Mehrzahl werden die betreffenden Seiten im Ausland betrieben. Hieraus folgen nicht nur Durchsetzungsprobleme für die deutschen Rechtsvorgaben. Vielmehr ist zu beobachten, dass viele der aus deutscher Sicht illegalen Seiten in anderen – durchaus zivilisierten – Staaten als Formen zulässiger Meinungsäußerung angesehen werden. Die Globalität des Internets verlangt, sich diesem Aufeinandertreffen verschiedener kultureller Wertvorstellungen zu stellen, diese in gewissem Maße auch zu akzeptieren und mit daraus resultierenden Friktionen zu leben.

Wo immer aber ein Wertekonsens erreicht werden kann, sollten sich die Staaten um internationale Zusammenarbeit bemühen, um so den Zugriff auf die Urheber illegaler Meinungsäußerungen auch über nationale Grenzen hinweg zu ermöglichen. Als erfolgversprechender Ansatz ist insoweit die Cybercrime Convention des Europarates hervorzuheben.

Im Unterschied zu der oft langwierigen und mühsamen internationalen Koordination bei staatlichen Maßnahmen, sind Selbstkontrollansätze der Wirtschaft gerade auch in der internationalen Dimension deutlich erfolgreicher. Selbstkontrollinstanzen können flexibler und schneller reagieren. Bestehende internationale Netzwerke von Selbstkontrolleinrichtungen wie INHOPE gehen bereits mit beachtlichem Erfolg gegen illegale Inhalte im Internet vor.

Daneben ist es erforderlich, dass die Gesellschaft den Urhebern und den potenziell empfänglichen Adressaten rassistischer oder fremdenfeindlicher Inhalte mit intensiver Aufklärungs- und Überzeugungsarbeit begegnet. Parallel muss über die in diesen Botschaften liegenden Gefahren und Irrtümer informiert und vor ihnen gewarnt werden. Ziel sollte letztlich nicht das Blockieren von Meinungsäußerungen, sondern das Bemühen sein, die dahinter stehenden Ideologien und Irrtümer durch Aufklärung zu bekämpfen. Hierzu kann am besten eine offene, freie und von gelebter Toleranz geprägte Gesellschaft beitragen. Alle Kräfte in dieser Gesellschaft sollten dabei den bewussten und verantwortlichen Umgang mit Freiheit – gerade auch mit der Meinungsfreiheit und damit auch mit den Möglichkeiten der neuen Medien – fördern und fordern. Auch die Internet-Wirtschaft steht bereit, hierzu ihren Beitrag zu leisten.

5.6 Effektive Ko-Regulierung von Internetinhalten, ein Diskussionsvorschlag

Dr. Thomas Hart, Carsten Welp

5.6.1 Einleitung

Das Internet erlaubt den weltweiten Informations- und Datenaustausch. Dabei werden auch illegale und legale, aber potenziell jugendgefährdende Inhalte weltweit angeboten und verbreitet. Um Jugendschutz online zu realisieren, sind neue Regulierungsansätze notwendig, da klassische Instrumente der Medienaufsicht in vielen Fällen ein effektives Erreichen der Regulierungsziele nicht mehr erlauben.

Kern des hier vorgeschlagenen Modells ist ein wirksames Zusammenspiel der Akteure der Informationsgesellschaft: Nutzer, Anbieter und Medienaufsicht kooperieren auf dem Weg zu sicherer Internet-Nutzung und verantwortlichem Umgang mit den Netz-Inhalten. Es beruht deshalb auf Anreizen und Freiwilligkeit und verbindet die Instrumente „Verhaltenskodexe", „Internet-Hotline" und „Internet-Filter" auf möglichst zielführende und anreizorientierte Weise. Das Modell sollte in Form eines Abkommens zwischen Regulierern und Industrieverbänden implementiert werden. Es will die bestehenden Bestimmungen aus Mediendienste-Staatsvertrag und Jugendmedienschutz-Staatsvertrag ergänzen und konkretisieren und damit den Schutz der Nutzer auf ein breiteres und solideres Fundament stellen.

Das hier vorgeschlagene Ko-Regulierungsmodell bezieht sich auf nach deutschem Recht legale Internet-Inhalte, die aber potenziell jugendgefährdend sind. Illegale Inhalte hingegen können in der derzeitigen deutschen Aufsichtsstruktur nur am Rande in ein solches Konzept integriert werden.

5.6.2 Koregulierung von Internetinhalten

a. Notwendige Voraussetzungen

aa. Abkommen zwischen Regulierungsbehörde (KJM) und Internet Service-Providern

Den Ordnungsrahmen für das Ko-Regulierungsmodell setzen Regulierer und ISPs-Verbände in Form eines freiwilligen Ko-Regulierungs-Abkommens. Mögliche Inhalte der Selbstverpflichtung sind im Anhang genannt. Die zentralen Aspekte eines solchen Abkommens werden im Folgenden geschildert.

Ein solches Abkommen wird nur wirksam sein, wenn beide Seiten sich daraus Vorteile bei der Verfolgung ihrer Ziele versprechen:

- Der Anreiz für die Provider besteht v.a. darin, dass sie, sofern sie sich dem Abkommen anschließen, von der KJM ein Qualitätssiegel erhalten. Ein solches Qualitätssiegel sollte von der KJM gegenüber Nutzern und Industrie aktiv beworben und als Zeichen verantwortlichen Handelns im Internet kommuniziert werden.
- Der Anreiz für die Medienaufsicht besteht darin, dass sie die Industrie als Kooperationspartner bei der Erreichung des Regulierungsziels „Jugendschutz im Internet" gewinnen kann.

bb. Abkommen zwischen Regulierungsbehörde (KJM) und Filteranbietern:

Dieses Abkommen umfasst insbesondere die Selbstverpflichtung von Anbietern von Internet-Filtersystemen, die an sie übermittelten Internet-Adressen unverzüglich in ihre Filter-Listen einzupflegen. Empfohlen werden sollten ausschließlich solche Filter, deren Installation, Aktivierung und Konfigurierung in der Entscheidung des Nutzers steht (also: keine Empfehlung server-basierter Filter).

Die KJM erstellt (ggf. auf Empfehlung von jugendschutz.net) eine Liste von Internet-Filtern, die aus ihrer Sicht geeignet sind, nutzerautonomen Schutz zu gewährleisten. Diese Filter werden von der KJM „als geeignet empfohlen".

Zudem sollte die KJM selbst eine Negativ-Liste pflegen. Diese Liste bietet sie denjenigen Filter-Anbietern an, die selbst keine eigenen Negativ-Listen erstellen, die derartige Listen aber integrieren können (z.B. ICRAfilter). Ein solches Abkommen kann Gegenstand des allgemeinen Zertifizierungsprozesses im Rahmen des Jugendmedienschutz-Staatsvertrages sein.

b. Vorgehensweise bei Meldung jugendgefährdender Inhalte

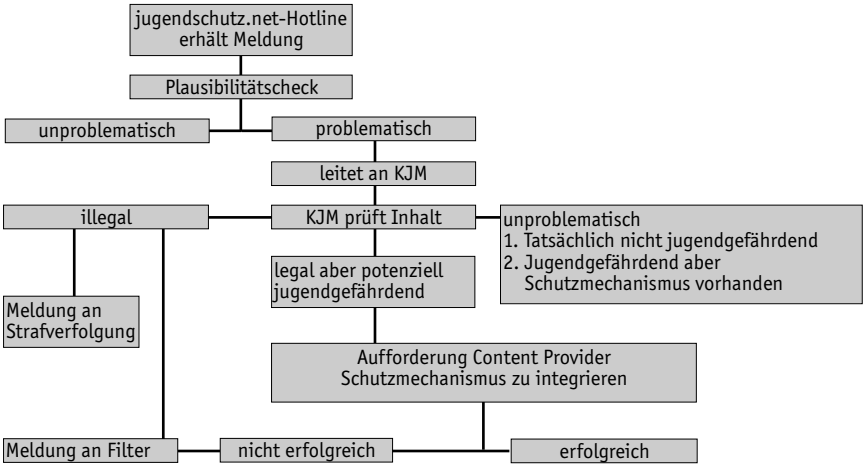


Abb. 7: Ausgangspunkt: Meldung jugendgefährdender Inhalte

Eine Internet-Hotline, unterhalten von *jugendschutz.net* im Auftrag der Bundesländer, nimmt Nutzerbeschwerden über problematische Internetinhalte entgegen. Die Mitarbeiter der Hotline prüfen die Beschwerde (Plausibilitäts-Check). Besteht der begründete Verdacht, dass es sich um jugendgefährdende oder illegale Inhalte handelt, so wird die Adresse zur verbindlichen Prüfung an die KJM weitergeleitet.

Nachdem es in Deutschland verschiedene Internet-Hotlines gibt, wäre eine effektive Kooperation dieser Hotlines wünschenswert. So könnten sich bspw. alle Hotlines verpflichten, alle gemeldeten Seiten in jedem Falle auch an *jugendschutz.net* weiter zu leiten. Eine diesbezügliche Selbstverpflichtung könnte Bestandteil des Ko-Regulierungs-Abkommens sein.

- Illegale Inhalte: Bei begründetem Verdacht auf Illegalität des Materials wird die entsprechende Adresse an die Strafverfolgungsbehörden weitergeleitet. Bestätigt sich der Verdacht, so wird unabhängig vom weiteren Vorgehen innerhalb der Strafverfolgung die Adresse an die am Ko-Regulierungsmodell beteiligten Filteranbieter weitergeleitet.
- Legale, jugendgefährdende Inhalte ohne Schutzmechanismen: Kommt die Prüfung zu dem Ergebnis, dass es sich bei den Inhalten um legales, aber potenziell jugendgefährdendes Material handelt, das nicht mit entsprechenden Jugendschutzmechanismen (insbes. Altersverifikation) ausgestattet ist, so erfolgt zunächst

eine Aufforderung an den Content Provider, solche Schutzmechanismen in sein Angebot zu integrieren. Dies kann durch Klassifizierung der Inhalte gemäss einem anerkannten Selbstklassifizierungssystems (z.B. PICS) geschehen sowie durch Integrierung von Zugangssicherungen auf der Website.

Bleibt die Aufforderung binnen einer festgelegten Frist ohne Erfolg, so wird die entsprechende Adresse an alle am Abkommen beteiligten Filter-Anbieter weitergeleitet. Diese nehmen die Adresse unverzüglich in ihre Negativ-Listen auf. Zudem wird die Adresse in die von der KJM gepflegte Negativ-Liste aufgenommen.

- Nicht jugendgefährdende Inhalte oder legale, potenziell jugendgefährdende Inhalte mit von der KJM anerkannten Jugendschutzprogrammen

In diesen Fällen ist keine weitere Aktivität der Medienaufsicht notwendig.

Die am Abkommen beteiligten Anbieter von Internet-Filtern nehmen die ihnen auf diesem Wege übermittelten Adressen unverzüglich in ihre Negativ- (oder Blocking-) Listen auf und stellen diese ihren Nutzern als Update zur Verfügung. Sobald die Grundlage für die Meldung durch die KJM entfallen ist (z.B. durch ein Gerichtsurteil) entfernen sie die Adressen umgehend wieder aus ihren Listen. Mit den Filter-Anbietern sollte eine Übereinkunft geschlossen werden, in welcher Regelmäßigkeit den Nutzern Aktualisierungen der Negativ-Listen angeboten werden. Dies sollte mindestens einmal pro Monat geschehen.

5.6.3 Schlussbemerkung

Über das vorgeschlagene Modell hinaus lassen sich sicher weitere Aspekte finden, die dem Schutz der Nutzer dienen könnten: etwa die Frage, inwieweit eine Anwendung von Qualitätssiegeln auch auf Content Provider oder Suchmaschinenbetreiber sinnvoll sein könnte bzw. wie die Institutionen der Freiwilligen Selbstkontrolle in ein solches Modell integriert werden könnten. All diese denkbaren Erweiterungen sind geeignet, Nutzer- und vor allem Jugendschutz auf eine breitere Basis des Konsenses und der Kooperation zu stellen.

Derzeit scheint es nicht möglich zu sein, illegale Inhalte systematisch in ein solches Ko-Regulierungs-Abkommen zu integrieren. Das Aufsichtssystem hat zwei scharf getrennte Betrachtungsgegenstände: illegal einerseits; legal, aber aufgrund anderer Überlegungen „problematisch“ andererseits. Dennoch lässt sich vielleicht ein Gesamtziel der Aufsicht über elektronische Medien formulieren: es lautet „Schutz der Nutzer“. Auch strafrechtliche Vorschriften sind oft an diesem Ziel orientiert: Während das

Verbot von Kinderpornographie vor allem den Schaden, der durch die Produktion der Inhalte entsteht, unterbinden will, ist es im Falle extremistischer Inhalte in erster Linie der Nutzer, der vor weltanschaulicher Manipulation geschützt werden soll. Dieser Schutz kann aber nicht nur durch staatliche Regulierung erfolgen, sondern – vielleicht effektiver? – auch durch das Setzen geeigneter Anreize für Industrie und die Nutzer selbst.

Durch den Verzicht auf Intervention auf der einen Seite des Spektrums (etwa hinsichtlich im Ausland legaler, nach deutschem Recht jedoch illegaler Inhalte) kann möglicherweise in der Summe das Ziel "Nutzerschutz" besser erreicht werden. Durch einen glaubwürdigen Interventions-Verzicht könnten Anreize für die Akteure der Provider-Industrie gesetzt werden, sich sehr viel umfassender als verantwortungsvolle Akteure einzubringen. Derzeit ist eine solche Abwägung zwischen den in den verschiedenen Rechts-Domänen eingesetzten Mitteln und der Effektivität des gesamten Regulierungssystems offenbar noch nicht möglich. Es braucht hier noch eine sehr viel grundsätzlichere gesellschaftliche Diskussion, als es im Rahmen unseres Vorschlages hier möglich ist.

Für alle Ko- und Selbstregulierungs-Bemühungen gilt: soll ihnen Erfolg beschieden sein, so müssen sich alle beteiligten Akteure als glaubwürdige Partner positionieren. Glaubwürdigkeit kann man nicht allein durch das Schließen eines Abkommens erreichen, sondern wird erst in der Praxis eines solchen Abkommens aufgebaut.

Es scheint, als seien Medienaufsicht und Industrie mehr als je zuvor bereit, dieses Experiment einzugehen.

5.6.4 Anhang: Mögliche Komponenten einer Selbstverpflichtungs-Erklärung von ISPs[146]

ISPs verpflichten sich:

- Informationen und Hilfestellungen darüber anzubieten, wie der Zugang von Kindern zum Internet kontrolliert werden kann (z.B. Filtersoftware, Altersverifizierungs-Systeme);
- ihren Kunden Informationen über die Verfügbarkeit, Installation und Anwendung verschiedener Internet-Filterlösungen zu geben;
- Hilfestellung bei der Entwicklung und Implementierung von Internet-Filter-Technologien zu geben;

(146) Angelehnt an den "Code of Practice" der australischen Internet Industry Association, Version 7.2, Mai 2002, abrufbar unter: http://www.iia.net.au/.

- sicherzustellen, dass sie, sobald sie Kenntnis erlangen, dass ein inländischer Host-Provider einen illegalen Inhalt bereithält, diesen Host-Provider darüber informieren;
- illegale Inhalte nach entsprechender Benachrichtigung vom Server zu löschen (Host-Provider);
- ihre Kunden über die Möglichkeit aufzuklären, problematische Inhalte über eine Hotline zu melden und den Kunden bei einer solchen Meldung Hilfestellung zu geben;
- sofern eine eigene Internet-Hotline unterhalten wird, eingehende Beschwerden immer auch an die Hotline von jugendschutz.net weiter zu leiten;
- Anbieter von Internet-Inhalten (Content Provider) über die Haftung für ihre Inhalte aufzuklären;
- Anbieter von Internet-Inhalten zu ermutigen, potenziell jugendgefährdende Inhalte als solche zu kennzeichnen;
- ihren Kunden Hilfestellung beim Umgang mit unerwünschter E-Mail-Werbung zu geben;
- keine Accounts an Personen unter 18 Jahren ohne die Einwilligung eines Erziehungsberechtigten oder anderen verantwortlichen Erwachsenen zu vergeben.

6. Anhang

6.1 Entscheidung des OVG Münster: Internet-Zugangsanbieter können zur Sperrung rechtswidriger Websites verpflichtet werden

Beschluss v. 19.3.2003 - 8 B 2567/02- (LG Arnsberg)

6.1.1 Leitsätze

- Die Anwendbarkeit des Mediendienste-Staatsvertrages (MDStV) bestimmt sich in Abgrenzung zum Teledienstegesetz (TDG) nach dem konkreten Inhalt des Internetangebotes im Einzelfall.
- Von einem Mediendienst ist auszugehen, wenn der Dienst der allgemeinen Meinungsbildung dienen soll, also die redaktionelle Gestaltung im Vordergrund steht.
- Entscheidend für die Abgrenzung zwischen der Anwendbarkeit des MDStV und des TDG ist, ob bei einer Gesamtschau der Dienst an die Allgemeinheit gerichtet ist oder ob der individualkommunikative Charakter im Vordergrund steht.
- §§ 12, 22 Abs. 2 und 3 MDStV stellen Vorschriften im Sinne des Art. 5 Abs. 2 GG dar und können die Meinungsfreiheit daher rechtmäßig einschränken.
- Internetsperrungen stellen keine Vor- oder Präventivzensur dar. Das Zensurverbot des Art. 5 Abs. 1 Satz 3 GG ist daher nicht einschlägig.
- Eine Verfügung ist bereits hinreichend bestimmt, wenn die Behörde das zu erreichende Ziel festlegt und dem Ordnungspflichtigen die Wahl überlässt, auf welchem Wege er seine Pflicht erfüllt.
- § 22 Abs. 3 MDStV räumt der Behörde ein Entschließungsermessen ein
- Eine ordnungsrechtliche Maßnahme ist bereits dann geeignet, wenn durch sie eine Förderung des gewünschten Erfolgs möglich ist bzw. sie einen Beitrag zu dessen Erreichen leistet. Eine vollständige Gefahrenbeseitigung ist nicht erforderlich.
- Jeder Träger öffentlicher Gewalt kann den Gleichheitssatz des Art. 3 Abs. 1 GG nur innerhalb seiner eigenen Zuständigkeit beachten.

6.1.2 Sachverhalt

Die Antragstellerin ist ein Internet-Service-Provider und bietet ihren Kunden u.a. den Zugang zum Internet an (Zugangsanbieter oder „Access-Provider"). Bei den Kunden der Antragstellerin handelt es sich nach ihren Angaben zu einem großen Teil um Privatkunden, aber auch um Geschäftskunden, die die Dienstleistungen der Antragstellerin für den E-Mail-Verkehr und den Internet-Zugang in ihren Betrieben nutzen.

Über den von der Antragstellerin angebotenen Zugang ist auch der Zugriff auf die Webseiten „www.nazi-lauck-nsdapao.com“ und „www.stormfront.org“ möglich. Mit Verfügungen vom 6. Februar 2002 an die I. GmbH und vom 8. Februar 2002 gab die Antragsgegnerin diesen Gesellschaften auf, den Zugang zur Nutzung zu den beiden Webseiten wegen Verstößen gegen den MDStV im Rahmen des von ihnen vermittelten Nutzungsangebotes zu sperren.

Die Antragstellerin erhob mit Schreiben vom 22. Februar 2002 Widerspruch gegen den Bescheid vom 6. Februar 2002. ... Den Widerspruch wies die Antragsgegnerin mit einem an die Antragstellerin gerichteten Bescheid vom 12. Juli 2002 zurück. Am 14. August 2002 hat die Klägerin Klage erhoben (VG Arnsberg 13 K 3173/02). Nachdem die Antragsgegnerin mit Schreiben vom 6. September 2002 die sofortige Vollziehung der Sperrverfügung vom 6. Februar 2002 angeordnet und den Antrag der Antragstellerin auf Aussetzung der Vollziehung unter dem 10. Oktober 2002 abgelehnt hatte, hat die Antragstellerin am 22. Oktober 2002 um vorläufigen Rechtsschutz nachgesucht.

Die Antragstellerin hat beantragt, die aufschiebende Wirkung ihrer Klage gegen die Verfügung der Antragsgegnerin vom 6. Februar 2002 in der Gestalt des Widerspruchsbescheids vom 12. Juli 2002 wiederherzustellen, hilfsweise, die Anordnung der sofortigen Vollziehung vom 6. September 2002 in der Gestalt des Ablehnungsbescheids vom 10. Oktober 2002 aufzuheben. Die Antragsgegnerin hat beantragt, den Antrag abzulehnen. Sie hat im Wesentlichen auf die angefochtenen Bescheide sowie die Anordnung der sofortigen Vollziehung vom 6. September 2002 Bezug genommen.

Das Verwaltungsgericht hat den Antrag auf Anordnung der aufschiebenden Wirkung der Klage mit Beschluss vom 6. Dezember 2002 abgelehnt. Hiergegen hat die Antragstellerin am 23. Dezember 2002 Beschwerde eingelegt. Sie beantragt, den Beschluss des Verwaltungsgerichts Arnsberg vom 6. Dezember 2002 abzuändern und die aufschiebende Wirkung ihrer Klage gegen die Verfügung der Antragsgegnerin vom 6. Februar 2002 in der Gestalt des Widerspruchsbescheids vom 12. Juli 2002 wiederherzustellen. Die Antragsgegnerin beantragt, die Beschwerde zurückzuweisen.

6.1.3 Entscheidungsgründe

Die Beschwerde der Antragsgegnerin gegen den Beschluss des Verwaltungsgerichts Arnsberg vom 6. Dezember 2002 hat keinen Erfolg. Das Verwaltungsgericht hat den Antrag auf Gewährung vorläufigen Rechtsschutzes nach § 80 Abs. 5 VwGO zu Recht abgelehnt. Der Antrag ist unter Berücksichtigung des Beschwerdevorbringens, auf dessen Prüfung der Senat gemäß § 146 Abs. 4 Satz 6 VwGO beschränkt ist, unbegründet.

Das öffentliche Interesse am Vollzug der Sperrverfügung überwiegt das Interesse der Antragstellerin an der Wiederherstellung der aufschiebenden Wirkung ihrer Klage. Gemäß § 80 Abs. 5 Satz 1 VwGO kann das Gericht auf Antrag die aufschiebende Wirkung des Widerspruchs oder der Klage wiederherstellen bzw. anordnen. Dabei ist im Rahmen einer Interessenabwägung zu prüfen, ob das öffentliche Interesse an der sofortigen Vollziehung oder das private Interesse an der aufschiebenden Wirkung des Rechtsbehelfs überwiegt. An der Vollziehung einer offensichtlich rechtswidrigen Maßnahme kann kein öffentliches Interesse bestehen; ist die zu vollziehende Maßnahme offensichtlich rechtmäßig, kann das private Interesse am Aufschub der Vollziehung regelmäßig als gering veranschlagt werden, so dass jedenfalls bei Hinzutreten einer der Sache nach gegebenen Dringlichkeit das öffentliche Interesse an der sofortigen Vollziehung überwiegt. Lassen sich die Erfolgsaussichten des Rechtsbehelfs in der Hauptsache bei der im Verfahren nach § 80 Abs. 5 Satz 1 VwGO allein möglichen summarischen Prüfung nicht abschließend abschätzen, bedarf es einer Abwägung aller relevanten Umstände, insbesondere der Vollzugsfolgen, um zu ermitteln, wessen Interesse für die Dauer des Hauptsacheverfahrens Vorrang gebührt.

Es ist weder von der offensichtlichen Rechtmäßigkeit noch der offensichtlichen Rechtswidrigkeit des angegriffenen Bescheids auszugehen. Bei summarischer Prüfung spricht einiges für die Rechtmäßigkeit der in der Hauptsache angefochtenen Sperrverfügung. Eine weitere Sachverhaltsermittlung und eine abschließende Beurteilung der Rechtsfragen müssen aber dem Hauptsacheverfahren vorbehalten bleiben. Die von den Parteien aufgeworfenen Rechtsfragen, auch verfassungsrechtlicher Art, können und müssen nicht im Verfahren des vorläufigen Rechtsschutzes geklärt werden.

Ermächtigungsgrundlage ist § 22 Abs. 3 i.V.m. Abs. 2 des Mediendienste-Staatsvertrages vom 27. Juni 1997 (GV NRW S. 158) in der Fassung des Art. 3 des Sechsten Rundfunkänderungsstaatsvertrages vom 7. Juni 2002 (GV NRW S. 178) –MDStV –. Der MDStV findet auf die beiden in Rede stehenden Webseiten Anwendung, weil es sich bei ihnen um Mediendienste und nicht um Teledienste handelt.

Die Anwendbarkeit des MDStV bestimmt sich – in Abgrenzung zum Teledienstegesetz (TDG) - nach dem konkreten Inhalt des Internetangebotes im Einzelfall[147]. Der Begriff der Mediendienste umfasst nach der Legaldefinition des § 2 Abs. 1 Satz 1 MDStV das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbrei-

(147) Vgl. VG Gelsenkirchen, Beschl. v. 18.12.2002 - 1 L 2528/02-, 4; VG Düsseldorf, Beschl. v. 19.12.2002 - 15 L 4148/02-, 17 ; VG Aachen, Beschl. v. 5.2.2003 - 8 L 1284/02-, 5; VG Köln, Beschl. v. 7.2.2003 - 6 L 2495/02-, 15; Spindler/Volkmann, K & R 2002, 399 f.; Zimmermann, NJW 1999, 3145 (3146); Hoeren, Stellungnahme zur geplanten Sperrverfügung der Bezirksregierung Düsseldorf v. 8.11.2001, 2.

tet werden. Dazu gehören nach Abs. 2 Nr. 4 dieser Bestimmung insbesondere Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden, mit Ausnahme von solchen Diensten, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht[148]. Von einem Mediendienst ist danach auszugehen, wenn der Dienst der allgemeinen Meinungsbildung dienen soll, also die redaktionelle Gestaltung im Vordergrund steht. Unter redaktioneller Gestaltung ist das Sammeln und Aufbereiten von verschiedenen Informationen oder Meinungen mit Blick auf den potenziellen Empfänger zu verstehen. Die inhaltliche, sprachliche, graphische oder akustische Bearbeitung eines Angebotes muss zur Einwirkung auf die öffentliche Meinungsbildung oder der Information zu dienen bestimmt sein[149].

Demgegenüber gelten nach § 2 Abs. 1 TDG die Bestimmungen dieses Gesetzes für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. In diesem Fall sind die elektronisch erbrachten Leistungen auf ein konkretes Individualverhältnis zwischen dem Nutzer und dem Anbieter – z.B. Telebanking nach § 2 Abs. 2 Nr. 1 TDG – bezogen oder haben die reine Informationsvermittlung - z.B. Datendienst nach § 2 Abs. 2 Nr. 2 TDG - zum Ziel[150]. Entscheidend für die Abgrenzung ist danach, ob bei einer Gesamtschau der Dienst an die Allgemeinheit gerichtet ist oder ob der individualkommunikative Charakter im Vordergrund steht.

Nach diesen Grundsätzen sind beide in Rede stehenden Webseiten Mediendienste. Es handelt sich nicht nur um reine Informationsangebote i.S.d. § 2 Abs. 2 Nr. 2 TDG. Beide Seiten zielen auf Meinungsbildung ab. Sie weisen hinreichend publizistische Elemente auf und sind erkennbar auf Propaganda ausgerichtet.

Die Webseite *www.stormfront.org* eröffnet mit dem Schriftzug Whitepride/Worldwide. Die Verfasser stellen sich als eine Organisation für die „mutigen Männer und Frauen" vor, die die weiße westliche Kultur, die Ideale und die Meinungsfreiheit verteidigten sowie politische und soziale Gruppen bildeten, um „den Sieg sicherzustellen". Die nachfolgenden Artikel, so z.B. „Schafft befreite Zonen!", „Zentrale Thesen des dritten Weges" mit ihren jeweiligen Untertiteln und die dargestellten Hakenkreuz-Symbole sind auf die Meinungsbildung eines nicht bestimmten Nutzerkreises gerichtet.

Auch die Webseite *www.nazi-lauck-nsdapao.com* ist redaktionell ausgestaltet. Auf der Eingangsseite findet sich ein Foto von Gary Lauck mit Hitlerfrisur und Schnurrbart, bekleidet mit khaki-braunem Uniformhemd und Hakenkreuzbinde um den Arm,

(148) Zu "Internet-(Online-)Diensten" vgl. Meier, in: Rossnagel, Recht der Multimedia-Dienste, § 2 MDStV, Rn. 66.
(149) Vgl. Gounalakis/Rhode, CR 1998, 487 (490); Spindler, in: Rossnagel (a.a.O.), § 2 TDG Rn. 31.
(150) Vgl. Gounalakis/Rhode (a.a.O.), 489 ff.; Spindler, in: Rossnagel, (a.a.O.), § 2 TDG Rn. 31, 33 f.

der vor einer Hakenkreuzfahne am Schreibtisch sitzt. Es wird ausgeführt, dass die NSDAP/AO Zeitschriften in zwölf Sprachen sowie diverses Propagandamaterial wie z.B. Hakenkreuzaufkleber und Bücher über den Nationalsozialismus herausgebe. Auf den nachfolgenden Seiten werden Politiker und Persönlichkeiten verunglimpft, indem ihnen rechtsradikale Lieder und Gedankengut in den Mund gelegt werden. Im Folgenden können diverse Naziartikel bestellt werden. Des Weiteren finden sich Aufrufe zur Unterstützung des nationalsozialistischen Gedankenguts sowie zum Verschicken von Solidaritätsschreiben an „inhaftierte Kameraden". Darüber hinaus werden Anleitungen gegeben, wie das Internet zur nationalsozialistischen Propaganda genutzt werden kann. Dass unter anderem auch Nazi-Artikel bestellt werden können, steht der Zuordnung als Mediendienst nicht entgegen. Die Angebote sind eingebettet in entsprechende nationalsozialistische Propaganda und werden mit entsprechenden Begleittexten versehen[151]. Nach dem gesamten Erscheinungsbild der Webseite steht die „journalistische" Ausgestaltung zur Verbreitung nationalsozialistischen Gedankenguts für die Allgemeinheit im Vordergrund[152].

Die Antragsgegnerin ist nach § 22 Abs. 3 MDStV für den Erlass der Verfügung zuständig, vgl. §§ 1 und 2 der Verordnung über Zuständigkeiten nach dem Mediendienste-Staatsvertrag vom 1. Juli 1997 (GV NRW S. 184). Die von der Antragstellerin aufgeworfene Frage, ob die Antragsgegnerin für den Erlass der Verfügung etwa im Hinblick auf das völkerrechtliche Nichteinmischungsgebot international zuständig ist, dürfte sich nicht stellen. Gegenstand des Verfahrens ist die Sperrung des Zugangs, den die Antragstellerin – mit Sitz in Nordrhein-Westfalen – ihren Kunden vermittelt.

Offenkundige Zweifel an der Verfassungsmäßigkeit der Ermächtigungsgrundlage bestehen nicht. Die Gesetzgebungszuständigkeit der Länder dürfte sich aus einer Annexkompetenz zur anerkannten Gesetzgebungskompetenz der Länder für den Rundfunk nach Art. 70 Abs. 1 GG ergeben[153].

Sofern – wofür wenig spricht – die Materie Presserecht einschlägig sein sollte, stünde dem Bund eine Rahmengesetzgebungskompetenz gemäß Art. 75 Abs. 1 Nr. 2 GG zu. Gleichwohl wäre auch für dieses Gebiet die Gesetzgebungszuständigkeit der Länder gegeben, da der Bund für den hier in Rede stehenden Regelungskomplex seine Rahmenkompetenz nicht in Anspruch genommen hat[154].

(151) Vgl. z.B. zum Film "Der Ewige Jude".
(152) Vgl. VG Düsseldorf (a.a.O.), 17; VG Gelsenkirchen (a.a.O.); 5 f.; VG Köln (a.a.O.), 16 f.; VG Aachen (a.a.O.), 5 f.; Greiner, CR 2002, 620.
(153) Vgl. Vesting, in: Rossnagel (a.a.O.), § 18 MDStV, Rn. 11; a.A.: Koenig/Loetz, C & R 1999, 438.
(154) Vgl. zur landesrechtlichen Regelung der Verjährung von Pressedelikten: BVerfGE 7, 29 (42 f.).

Offensichtliche Bedenken im Hinblick auf eine verfassungswidrige Einschränkung der Rundfunk- oder der Pressefreiheit der Anbieter (Art. 5 Abs. 1 Satz 2 GG) bzw. der Meinungs- oder Informationsfreiheit der Anbieter und Nutzer (Art. 5 Abs. 1 Satz 1 GG)[155], sind nicht gegeben. Unabhängig davon, ob die Freiheit der Übermittlung von Informationen aus dem Internet durch die Rundfunkfreiheit (Art. 5 Abs. 1 Satz 2 GG) oder durch die Meinungsäußerungs- und -verbreitungsfreiheit (Art. 5 Abs. 1 Satz 1 GG) gewährleistet ist[156], kommt ein Eingriff in diese Freiheiten auf der Grundlage des Art. 5 Abs. 2 GG in Betracht. Danach finden die Rechte des Art. 5 Abs. 1 GG ihre Schranken in den Vorschriften der allgemeinen Gesetze, in den Bestimmungen zum Schutz der Jugend und in dem Recht der persönlichen Ehre. Das Zensurverbot des Art. 5 Abs. 1 Satz 3 GG dürfte nicht einschlägig sein. Hierunter wird allein die sog. Vor- oder Präventivzensur verstanden, d.h. ein Verfahren, vor dessen Abschluss ein Werk nicht veröffentlicht werden darf[157].

Offensichtliche Bedenken gegen die Verfassungsmäßigkeit des § 22 Abs. 2 und 3 MDStV ergeben sich auch nicht aus dem Grundsatz der „Polizeifestigkeit der Presse“[158]. Dieser in § 1 Abs. 2 LPresseG NRW normierte Grundsatz schließt zwar in dem vom Landespressegesetz erfassten Bereich ein präventives Einschreiben auf der Grundlage der allgemeinen polizei- bzw. ordnungsrechtlichen Generalklausel aus.

Soweit ihm darüber hinaus über Art. 5 GG ein verfassungsrechtlicher Gehalt zukommen sollte, steht er einer spezialgesetzlichen Ermächtigungsgrundlage, die – wie § 22 MDStV – zu einem Einschreiten wegen Verstoßes gegen konkrete, spezifizierte gesetzliche Verbote ermächtigt, nicht entgegen, soweit den Anforderungen des Art. 5 Abs. 2 GG genügt wird[159]. Soweit durch die Regelung die Berufsausübung (Art. 12 GG) und unter Umständen das Eigentumsrecht (Art. 14 Abs. 1 GG) der Zugangsvermittler im Einzelfall beeinträchtigt sein könnten, bietet schon das Tatbestandsmerkmal der Zumutbarkeit in § 22 Abs. 3 MDStV eine hinreichende Möglichkeit zur Berücksichtigung etwaiger Grundrechtspositionen.

Die Voraussetzungen für den Erlass der Sperrverfügung gegenüber der Antragstellerin nach § 22 Abs. 3 i.V.m. Abs 2 Satz 1 MDStV liegen bei summarischer Prüfung vor. Gemäß § 22 Abs. 2 MDStV hat die Aufsichtsbehörde bei im einzelnen bezeichneten Verstößen gegen den MDStV die erforderlichen Maßnahmen gegenüber dem Diensteanbieter zu treffen. Nach § 22 Abs. 3 MDStV können Maßnahmen zur Sperrung von Angeboten nach Abs. 2 auch gegen den Diensteanbieter von fremden Inhalten nach

(155) Siehe aber Vesting, in: Rossnagel (a.a.O.), § 18 MDStV, Rn. 6 ff.; Stadler, MMR 2002, 343.
(156) Vgl. Starck, in: von Mangoldt/Klein/Starck, Grundgesetz, Band 1, 1999, Art. 5 Abs. 1, 2, Rn. 97 m.w.N.
(157) Vgl. Stark (a.a.O.), Rn. 156; Spindler/Volkmann, K&R 2002, 398 (407).
(158) Vgl. Vesting, in: Rossnagel (a.a.O.), § 18 Rn. 8; Stadler (a.a.O.), 343 f.
(159) Vgl. zur Polizeifestigkeit der Meinungsfreiheit: Degenhart, in: Bonner Kommentar, Art. 5 Abs. 1 und 2, Rn. 260 ff. und zur Pressefreiheit: Rn. 572; Götz, Allgemeines Polizei- und Ordnungsrecht, 13. Auflage, Rn. 331; Löffler, Handbuch des Presserechts, 4. Auflage, Rn. 4.

den §§ 7 bis 9 MDStV gerichtet werden, sofern Maßnahmen gegenüber dem Verantwortlichen sich als nicht durchführbar oder nicht Erfolg versprechend erweisen und eine Sperrung technisch möglich und zumutbar ist.

Ein Verstoß gegen die Bestimmungen des Staatsvertrages im Sinne des § 22 Abs. 2 Satz 1 MDStV liegt vor. Die Webseiten enthalten offenkundig unzulässige Inhalte im Sinne des § 12 MDStV. Die Webseite "stormfront" verstößt gegen strafrechtliche Bestimmungen (§ 12 Abs. 1 Nr. 1 MDStV). Der Tatbestand des § 86 a Abs. 1 Nr. 1 StGB wird auf mehreren Seiten durch die Verwendung von Kennzeichen verfassungswidriger Organisationen (Hakenkreuzdarstellungen etc.) verwirklicht. Auch dürfte voraussichtlich der Tatbestand der Volksverhetzung nach § 130 Abs. 1 Nr. 1 StGB erfüllt sein. In dem gesamten Internetangebot wird rechtsextremes Gedankengut verbreitet. Insbesondere mit dem Text: "Schafft befreite Zonen" wird zum Hass gegen Teile der Bevölkerung aufgestachelt bzw. zu Gewalt und Willkürmaßnahmen aufgefordert. Nach der maßgeblichen Rechtsprechung des Bundesgerichtshofs in vergleichbaren Fallkonstellationen tritt der zum Tatbestand gehörende Erfolg bei der Verbreitung im Internet auch im Inland (§ 9 Abs. 1 Alt. 3 StGB) ein[160].

Zudem ist das Angebot offensichtlich geeignet, Kinder und Jugendliche sittlich schwer zu gefährden (§ 12 Abs. 1 Nr. 3 MDStV). Auf den Seiten von *www.nazi-lauck-nsdapao.com* werden die Juden auf zynische Weise verunglimpft. Es wird zum Hass und zur Vernichtung von Juden und anderen "Volksfeinden" aufgerufen, wodurch zumindest der Tatbestand der Volksverhetzung nach § 130 Abs. 1 Nr. 1 StGB erfüllt ist. Ferner wird die Judenvernichtung gebilligt, wodurch der qualifizierte Tatbestand des § 130 Abs. 3 StGB verwirklicht ist. Auf dem gesamten Seitenangebot werden Kennzeichen verfassungswidriger Organisationen verwendet, § 86 a Abs. 1 Nr. 1 StGB. Darüber hinaus wird mit dem Gesamtangebot der Webseite auch der Krieg verherrlicht (§ 12 Abs. 1 Nr. 2 MDStV). Insgesamt besteht offensichtlich die Eignung, Kinder und Jugendliche sittlich schwer zu gefährden (§ 12 Abs. 1 Nr. 3 MDStV).

Maßnahmen gegenüber dem bzw. den Verantwortlichen nach § 6 Abs. 1 MDStV sind nicht durchführbar bzw. nicht Erfolg versprechend. Es kann dahinstehen, ob an die Unmöglichkeit oder Aussichtslosigkeit von Maßnahmen gegen Content- und Host-Provider insoweit strenge Anforderungen zu stellen sind, um dem Regel-/ Ausnahmeprinzip der §§ 22 Abs. 2 und 3 MDStV gerecht zu werden[161]. Denn die Antragsgegnerin hat in der Sperrverfügung, im Widerspruchsbescheid und in der Antragserwiderung im Einzelnen ihre Bemühungen zur Heranziehung der Verantwortlichen im Ausland dargelegt. Es ist nicht erkennbar, dass die Antragsgegnerin weitere Möglichkeiten hat, gegenüber den Verantwortlichen im Ausland einzuschreiten oder ein Einschreiten zu veranlassen.

(160) Vgl. BGH, NJW 2001, 624 ff.
(161) So: Spindler/Volkmann (a.a.O.), 405.

Nach § 22 Abs. 3 MDStV können Maßnahmen zur Sperrung auch gegen einen Diensteanbieter von fremden Inhalten nach den §§ 7 bis 9 MDStV gerichtet werden. Die Antragstellerin ist als Zugangsvermittlerin Diensteanbieterin im Sinne des § 7 MDStV. Diese Bestimmung gilt nach ihrem Wortlaut für Diensteanbieter, die fremde Informationen in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang vermitteln. Die Antragstellerin stellt unstreitig den Zugang zu fremden Informationen im Internet her. Auch die amtliche Überschrift des § 7 MDStV: „Durchleitung von Informationen" macht deutlich, dass die bloße Zugangsvermittlung von der (haftungsprivilegierenden) Bestimmung erfasst sein soll. Zudem ist bereits nach der allgemeinen Begriffsbestimmung des § 3 Nr. 1 MDStV (auch) Diensteanbieter im Sinne des MDStV, wer fremde Mediendienste zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt.

Die Entstehungsgeschichte stützt dieses Normverständnis. § 7 MDStV geht zurück auf Art. 12 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Rechtsverkehr" - ABl. L 178 vom 17. Juli 2000, S. 1 ff-). Art. 12 der Richtlinie regelt die Verantwortlichkeit von Zugangsvermittlern und lässt nach Abs. 3 insbesondere die Möglichkeit einer Sperrverfügung gegen einen Diensteanbieter, der lediglich den Zugang vermittelt, ausdrücklich zu. Die §§ 7 bis 9 des MDStV setzen die Art. 12 bis 15 der Richtlinie über den elektronischen Rechtsverkehr um[162]; Begründung der Bayerischen Staatsregierung zum Sechsten Staatsvertrag zur Änderung des Rundfunkstaatsvertrages, des Rundfunkfinanzierungsstaatsvertrages und des MDStV (Sechster Rundfunkänderungsstaatsvertrag), Bayerischer Landtag, Drs. 14/8628, S. 11 (21)).

Soweit zu § 18 Abs. 3 MDStV a.F. die Auffassung vertreten wurde, dass eine Sperrverfügung nicht an einen Zugangsvermittler gerichtet werden könne, weil „Anbieter von fremden Inhalten nach § 5 Abs. 3" nur Anbieter von Navigationshilfen, Hyperlinks bzw. Suchmaschinen seien[163], besteht jedenfalls nunmehr angesichts des Wortlauts und der dargestellten Entstehungsgeschichte des § 22 Abs. 3 bzw. des § 7 MDStV kein Zweifel daran, dass auch Access-Provider als Nichtverantwortliche im Sinne des § 7 MDStV Adressaten einer Sperrverfügung gemäß § 22 MDStV sein können.

(162) Vgl. dazu: Greiner, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001, 181 f.; Bornemann, K&R 2002, 301 (304 f.).

(163) Vgl. zum Streitstand: Greiner, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, 73 ff.; zu § 3 TDG: Sieber, Verantwortlichkeit im Internet, München 1999, Rn. 262.

Auch der Einwand, die Tätigkeit eines Access-Providers falle grundsätzlich in den Anwendungsbereich des Telekommunikationsgesetzes, führt zu keinem anderen Ergebnis. Die Vermittlung des Zugangs und damit der Kenntnisnahme von Inhalten im Internet ist zwar grundsätzlich als Telekommunikationsdienstleistung einzuordnen. Dies schließt es nach dem eindeutigen Wortlaut des § 22 Abs. 3 MDStV und des § 7 MDStV aber nicht aus, ihn zugleich auch als Diensteanbieter von fremden Inhalten im Sinne des MDStV zu verstehen[164].

Die Verfügung ist auch hinreichend bestimmt, § 37 Abs. 1 VwVfG NRW. Hinreichende Bestimmtheit bedeutet, dass die getroffene Anordnung so vollständig, klar und unzweideutig erkennbar sein muss, dass die Beteiligten ihr Verhalten danach richten können. Insoweit ist im vorliegenden Fall ausreichend, dass die Behörde das zu erreichende Ziel festlegt und dem Ordnungspflichtigen die Wahl überlässt, auf welchem Wege er seine Pflicht erfüllt[165]. Die Sperrverfügung bestimmt die Sperrung der streitigen Seiten eindeutig als Ziel. Dass sie mehrere technische Möglichkeiten zur Sperrung der beiden Seiten aufzeigt, ist nicht zu beanstanden.

Die Anordnung der Sperrung ist bei summarischer Prüfung auch ermessensfehlerfrei erfolgt. Ein Einschreiten nach § 22 Abs. 3 MDStV steht entgegen der Auffassung der Antragsgegnerin im Ermessen der Aufsichtsbehörde. Zwar besteht für Maßnahmen nach § 22 Abs. 2 MDStV kein Entschließungsermessen. Gemäß Satz 1 dieser Vorschrift trifft die zuständige Aufsichtsbehörde die zur Beseitigung der bezeichneten Verstöße gegen die Bestimmungen des MDStV erforderlichen Maßnahmen gegenüber dem Diensteanbieter. Sie kann nach Satz 2 insbesondere Angebote untersagen und deren Sperrung anordnen. Die Sätze 3 bis 5 schränken die Befugnis zur Untersagung insbesondere unter dem Gesichtspunkt der Verhältnismäßigkeit ein. Die zuständige Behörde ist demnach zum Handeln nach § 22 Abs. 2 MDStV verpflichtet, sofern sie von Verstößen Kenntnis erlangt[166].

Eine vergleichbare Pflicht zum Einschreiten besteht jedoch nicht auf der Grundlage des § 22 Abs. 3 MDStV. Nach dieser Bestimmung "können" Aufsichtsmaßnahmen auch gegen den Diensteanbieter von fremden Inhalten nach den §§ 7 bis 9 MDStV gerichtet werden, wenn sich Maßnahmen nach § 22 Abs. 2 MDStV gegenüber dem Verantwortlichen nach § 6 Abs. 1 MDStV als nicht durchführbar oder Erfolg versprechend erweisen. Der Wortlaut des § 22 Abs. 3 MDStV räumt der Aufsichtsbehörde ein Ermessen auch in Bezug auf das "Ob" der Inanspruchnahme des dort genannten Adressatenkreises ein.

(164) Vgl. Meier, in: Rossnagel (a.a.O.), § 3 MDStV, Rn. 18; Vesting, in: Rossnagel (a.a.O.), § 18 MDStV Rn. 38 ff.; Spindler/Volkmann (a.a.O.), 399; Zimmermann (a.a.O.), 3149; Holznagel/Kussel, MMR 2001, 347 (351); a.A.: Hoeren (a.a.O.), S. 2.; Koenig/Loetz (a.a.O.).

(165) Vgl. Kopp/Ramsauer, VwVfG, 7. Aufl., § 37 Rn. 16; BVerwGE 84, 354 (358).

(166) Vgl. dazu: Vesting, in: Rossnagel (a.a.O.), § 18 MDStV, Rn. 32.; Greiner, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, 135.

Die Antragsgegnerin hat dieses Ermessen zumindest der Sache nach ausgeübt. Zwar führt sie im Widerspruchsbescheid auf S. 12. f. aus, es bestehe kein Entschließungsermessen zum Einschreiten bei Verstößen gegen die Bestimmungen des MDStV. Jedenfalls aber die weiteren (Hilfs-)Erwägungen der Antragsgegnerin zur "unverzichtbaren" Inanspruchnahme der Antragstellerin auf der Grundlage der § 14 OBG NRW sowie zur Verhältnismäßigkeit der Verfügung begründen ausreichend, weshalb die Antragsgegnerin eingeschritten ist und sich für die Heranziehung der Antragstellerin entschieden hat. Diese Überlegungen tragen auch ein ermessensfehlerfreies Einschreiten auf der Grundlage des § 22 Abs. 3 MDStV.

Ob im vorliegenden Verfahren überhaupt Raum für eine Ermessensabwägung verblieben ist, weil der Staat einen - hier gegebenen - Verstoß gegen die Menschenwürde (Art. 1 Abs. 1 GG) allenfalls unter besonderen Umständen hinnehmen kann, ihn vielmehr im Regelfall unterbinden muss[167], kann daher im vorliegenden Verfahren dahinstehen.

Sonstige Ermessensfehler sind nicht ersichtlich. Gegen die Verhältnismäßigkeit der Verfügung bestehen keine offenkundigen Bedenken, insbesondere ist die Sperrung bei summarischer Prüfung für die Antragstellerin technisch möglich und ihr zumutbar im Sinne des § 22 Abs. 3 MDStV. Hiervon ist auch dann auszugehen, wenn § 22 Abs. 3 MDStV dahin auszulegen sein sollte, dass in Anlehnung an das allgemeine Ordnungsrecht und die Qualifizierung eines Access-Providers als Nichtstörer dieser nur ausnahmsweise bei einer erheblichen gegenwärtigen Gefahr in Anspruch genommen werden könnte[168]. Die unter anderem von der Antragsgegnerin aufgezeigte Möglichkeit der sog. DNS-Sperrung ist offenkundig gegeben. Dies ergibt sich bereits daraus, dass die Antragstellerin selbst so (vorläufig bis zur Entscheidung über den vorliegenden Antrag) mit Erfolg verfahren ist. Zahlreiche andere Provider sind der Sperrverpflichtung nach den Angaben der Antragsgegnerin ebenfalls auf diesem, aber auch auf anderem technischen Wege nachgekommen.

Ernsthafte Zweifel an der Geeignetheit der Maßnahme bestehen auch im Übrigen nicht. Eine Maßnahme ist bereits dann geeignet, wenn durch sie eine Förderung des gewünschten Erfolgs möglich ist bzw. sie einen Beitrag zu dessen Erreichen leistet. Eine vollständige Gefahrenabwehr ist nicht Voraussetzung. Es muss sich um einen „Schritt in die richtige Richtung“ handeln[169]. Da es auf die Eignung zur Sperrung der beiden Webseiten ankommt, ist es unerheblich, dass eine steigende Anzahl rechtswidriger Inhalte im Internet zu verzeichnen ist[170]. Die Sperrung durch Access-Provider betrifft ein weites Publikum. Die Verfügung wird einer Vielzahl geschäftlicher oder privater

(167) Vgl. BVerwGE 115, 189 (202).
(168) Vgl. Spindler/Volkmann (a.a.O.), 404.
(169) Zutreffend: VG Gelsenkirchen (a.a.O.), 8 f.; VG Düsseldorf (a.a.O.), 21; Spindler/Volkmann (a.a.O.), 496; Greiner, CR 2002, 620 (621).
(170) so aber Hoeren (a.a.O.), 3.

Nutzer den unmittelbaren Zugriff auf die Webseiten zumindest in zeitlicher und technischer Hinsicht erschweren. Dass es dennoch – mit aus der Sicht vieler Nutzer einfachen Mitteln – möglich ist, die Seiten zu erreichen, dürfte im Ergebnis unschädlich sein. Gleichwohl werden viele Nutzer die vorhandenen Möglichkeiten zur Umgehung der Sperrung nicht kennen oder als zu aufwendig nicht nutzen. Eine vollständige Ausschaltung der Gefahr durch Sperrungen ist ohnehin praktisch unmöglich, da im Internet mannigfaltige Möglichkeiten zur Umgehung bestehen[171].

Die Sperrverfügung ist auch erforderlich. Erforderlich ist eine Maßnahme, wenn sie von mehreren möglichen und voraussichtlich gleich wirksamen Maßnahmen diejenige trifft, die den Einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt. Es ist - wie dargelegt - nicht ersichtlich, dass die Antragsgegnerin mit Erfolg gegenüber den für die Seiten Verantwortlichen vorgehen oder ein Einschreiten veranlassen kann. Die Möglichkeit des Einsatzes der von der Antragstellerin angeführten Filtersoftware ist - wie die Antragsgegnerin vorgetragen hat - abhängig von der Mitwirkung der Content-Provider, die ihre Seiten freiwillig selbst bewerten und indizieren müssten. Von einer Bereitschaft hierzu kann im vorliegenden Verfahren nicht ausgegangen werden. Zudem müsste hierfür jeder einzelne Nutzer Software installieren. Die Bereitschaft dazu dürfte gering sein. Es entspricht auch nicht Sinn und Zweck der Regelungen des MDStV, dass der einzelne Nutzer selbst aktiv werden muss, um vor unzulässigen Inhalten geschützt zu werden. Es geht der Antragsgegnerin zu Recht nicht darum, lediglich einen Schutz vor ungewollter Konfrontation mit den beiden Webseiten zu gewährleisten. Vielmehr soll gegen die Verbreitung strafrechtlich relevanter Inhalte vorgegangen werden. Auch die von der Antragstellerin angesprochene Förderung des kritischen Umgangs mit rechtsradikalen Seiten ist nicht geeignet, das von der Antragsgegnerin verfolgte Ziel, den Zugang zu den beiden Seiten zu verhindern, zu erreichen.

Die Sperrverfügung ist auch zumutbar bzw. angemessen. Hierbei sind die gegenteiligen Interessen der Betroffenen zu berücksichtigen, die um so schützenswerter erscheinen, je stärker der Schutzbereich eines Grundrechts betroffen ist. Ein Verstoß gegen Art. 3 Abs. 1 GG, den die Antragstellerin im Hinblick auf das (bisherige) Nichtvorgehen gegen Access-Provider in anderen Bundesländern rügt, scheidet bereits deshalb aus, weil jeder Träger öffentlicher Gewalt den allgemeinen Gleichheitssatz nur innerhalb seiner eigenen Zuständigkeit beachten kann[172]. Innerhalb ihres Zuständigkeitsbereichs ist die Antragsgegnerin gegen alle Access-Provider vorgegangen, wie sie im Beschwerdeverfahren nochmals dargelegt hat.

(171) Vgl. Spindler/Volkmann (a.a.O.), 405 f.; Zimmermann (a.a.O.), 3150; Greiner (a.a.O.), 621 f.; Mankowski, MMR 2002, 277.
(172) Vgl. BVerfGE 79, 127 (158); Osterloh, in: Sachs, Grundgesetz, 1999, Art. 3 Rn. 81 f., m.w.N.

Die Sperrverfügung greift auch nicht unverhältnismäßig in die Berufsausübungsfreiheit (Art. 12 GG) oder das durch Art. 14 Abs. 1 Satz 1 GG gewährleistete Recht am eingerichteten und ausgeübten Gewerbebetrieb der Antragstellerin ein. Der von ihr geschilderte – relativ geringe – Aufwand für die bereits erfolgte Sperrung steht ersichtlich nicht außer Verhältnis zu dem angestrebten Erfolg, den Zugang zu den unzulässigen Inhalten der Webseiten zu verhindern bzw. zu erschweren. Die Antragstellerin hat ausgeführt, dass für die Sperrung von nur zwei Domain-Namen die Anschaffung neuer Hardware nicht erforderlich gewesen sei. Sie habe zur Umsetzung der Sperrung die Einträge in den Konfigurationsdateien ihrer drei Domain-Name-Server jeweils editieren müssen, wofür zwei Arbeitsstunden erforderlich gewesen seien. Auch der weiterhin geschilderte Aufwand für den Entscheidungsfindungsprozess, die Erstellung und Hinterlegung einer Informationsseite, den Neustart der Systeme, eine Browserkontrollanfrage und die Beantwortung von Kundenanfragen lässt keine erhebliche Belastung erkennen. Diesem relativ geringen Aufwand stehen schwerwiegende Rechtsgutsbeeinträchtigungen, denen entgegen getreten werden soll, gegenüber. Die beiden zu sperrenden Seiten erfüllen wie dargelegt Straftatbestände, verletzen die Menschenwürde, stören den öffentlichen Frieden und sind jugendgefährdend[173].

Ob auch die weiteren von der Antragsgegnerin aufgezeigten Sperrungsmöglichkeiten verhältnismäßig sind, bedarf unter den hier gegebenen Umständen keiner Entscheidung. Die Antragsgegnerin hat ausdrücklich hervorgehoben, dass sie insbesondere eine Sperrung durch Ausschluss von Domains im Domain-Name-Server für ausreichend erachte. Diese Methode ist nach Auffassung der Beteiligten offenbar mit dem geringsten Aufwand verbunden. Die Antragstellerin hat von dieser Möglichkeit – wie dargelegt – auch bereits Gebrauch gemacht. Auf die Verhältnismäßigkeit der übrigen Mittel kommt es daher im vorliegenden Verfahren nicht an.

Soweit die Antragstellerin geltend macht, es sei ihr unklar, wie sichergestellt werden solle, dass die Sperrungen nicht länger als nötig eingesetzt blieben, damit nicht der Zugriff auf völlig harmlose Seiten gesperrt würde, sind keine schutzwürdigen Interessen der Antragstellerin ersichtlich. Sie kann sich vielmehr gegenüber Dritten auf die durch die angefochtene Verfügung ausgesprochene Verpflichtung zur Sperrung berufen. Es ist insoweit unter Umständen Sache der Antragsgegnerin, auf eine geänderte Sachlage zu reagieren.

Bei summarischer Prüfung ist auch nicht ersichtlich, aus welchen Gründen die Antragsgegnerin – wie die Antragstellerin meint – durch die vorgelegte Entschließung des Europäischen Parlaments in Bezug auf den Jugendschutz und den Schutz der Menschenwürde oder durch das am 23.11.2001 zur Unterschrift ausgelegte Übereinkommen

(173) Vgl. Greiner (a.a.O.), 623.

des Europarates zur Datennetzkriminalität (Cybercrime-Konvention) gebunden ist oder inwieweit diese der Sperrverfügung entgegenstehen könnten. Die Einschätzung der Antragstellerin, dass auf internationaler Ebene der Verbreitung rechtswidriger Inhalte im Internet am effektivsten begegnet werden könnte, mag zutreffen, schließt aber ein nationales Vorgehen nicht aus, zumal nicht absehbar ist, wann und in welchem Umfang der Verbreitung unzulässiger Inhalte im Internet auf internationalem Wege entgegen getreten werden wird. Der Umstand, dass es sich nach Auffassung der Antragstellerin um einen Präzedenz- oder Musterfall handele, führt zu keiner anderen Bewertung der angegriffenen Verfügung. Entgegen ihrer Annahme ist im vorliegenden Verfahren nicht zu berücksichtigen, wie sich eine Vielzahl von Sperrverfügungen gleicher Art auf ihre Betriebsabläufe auswirken würde. Abgesehen davon, dass für eine weitere Inanspruchnahme der Antragstellerin derzeit keine konkreten Anhaltspunkte bestehen, ist hier nur über die Verhältnismäßigkeit der konkret im Streit befindlichen Maßnahmen zu befinden. Es wird Sache der Antragsgegnerin sein, die Zumutbarkeit weiterer Sperrverfügungen zu prüfen. Erst in künftigen Verfahren werden sich die Fragen stellen, ob die Praxis der Aufsichtsbehörden zu einer unzulässigen Umkehrung des „Regel-/Ausnahmeprinzips“ bzw. des Subsidiaritätsgrundsatzes des § 22 Abs. 2 und 3 MDStV führt und welche Anforderungen im Einzelnen an die Zumutbarkeit einer Inanspruchnahme eines Access-Providers unter Berücksichtigung ihrer „Gesamtbelastung“ zu stellen sein werden[174].

Sonstige in die Abwägung einzustellende Belange, wie das Allgemeininteresse an einem ungehinderten Datenverkehr, die Einschränkung eines vollwertigen Internetzugriffs, Beeinträchtigungen des Waren- und Dienstleistungsverkehrs sowie eine Hemmung der Entwicklung des e-commerce[175], sind bei der Sperrung der beiden rechtsradikalen Webseiten durch die Veränderung des DNS-Eintrags nicht oder nicht in relevantem Umfang berührt. Schließlich ist die Frage, ob der Antragstellerin ein Entschädigungsanspruch zusteht, im vorliegenden Verfahren ohne Belang.

Zu einem anderen Ergebnis wird entgegen der Auffassung der Antragstellerin auch nicht das Inkrafttreten des Staatsvertrages über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag - JMStV) vom 22. September 2002 (GV NRW 2003, S. 84) zum 1. April 2003 führen. Die Rechtmäßigkeit der Verfügung würde durch einen etwaigen Wechsel der Zuständigkeit schon nicht berührt. Der nach § 20 Abs. 1 JMStV zuständigen Landesmedienanstalt stünden im Übrigen für die vorliegende Fallkonstellation sachlich vergleichbare Eingriffsbefugnisse zu, § 20 Abs. 1 und 4 JMStV, § 4 JMStV, §§ 22 Abs. 2 und 3 MDStV.

(174) Vgl. Spindler/Volkmann (a.a.O.), 404.
(175) Vgl. Stadler (a.a.O.), 346.

Ist nach den vorstehenden Erwägungen die Rechtmäßigkeit oder Rechtswidrigkeit der Verfügung im vorliegenden Verfahren nicht abschließend zu klären, fällt die weitere Abwägung des öffentlichen Interesses an einer sofortigen Vollziehung der Verfügung der Antragsgegnerin gegenüber dem Interesse der Antragstellerin, der an sie gerichteten Anordnung bis zur abschließenden Entscheidung in der Hauptsache nicht nachkommen zu müssen, zuungunsten der Antragstellerin aus. Der Umstand, dass das Verwaltungsverfahren bereits seit über einem Jahr läuft, lässt das öffentliche Interesse an der sofortigen Vollziehung nicht entfallen. Ungeachtet des Hinweises der Antragsgegnerin darauf, dass sie zunächst auf Selbstregulierungsmaßnahmen seitens der Provider gesetzt habe, hat der Senat eine eigenständige Bewertung der widerstreitenden Interessen vorzunehmen. Diese hängt nicht entscheidend davon ab, wie lange und aus welchen Gründen eine Behörde von einer Vollziehungsanordnung abgesehen hat.

Der Antragstellerin ist es zuzumuten, die Sperrung bis auf Weiteres aufrecht zu erhalten. Durch die Webseiten werden Straftatbestände verwirklicht und bedeutende Rechtsgüter beeinträchtigt. Das Gewicht der betroffenen Interessen der Antragstellerin ist – wie dargelegt – demgegenüber derart gering, dass die Klärung der Rechtsfragen im Hauptsacheverfahren nicht abgewartet werden muss. Zur Vermeidung von Wiederholungen kann insoweit auf die Ausführungen zur Zumutbarkeit der Sperrverfügung verwiesen werden. Dass ihr im Zusammenhang mit der Sperrung ein beachtlicher Verlust an Kunden drohen könnte, trägt sie nicht vor und ist auch sonst nicht ersichtlich. Ein Großteil aller Internet-Nutzer in Deutschland mag (noch) über Provider in anderen Bundesländern, insbesondere über die beiden größten Anbieter, weiterhin ungehinderten Zugriff auf die beiden Internetangebote haben. Nach den Erkenntnissen des Senats ist bei U.-P. der Zugriff auf beide Seiten und bei B. der Zugriff auf die Seite „*www.nazi-lauck-nsdapao.com*“ nicht gesperrt. Dies lässt das öffentliche Interesse an einer wenn auch (zunächst nur) geringfügigen Einschränkung des Zugangs zu diesen Seiten für die Nutzer der in Nordrhein-Westfalen ansässigen Access-Provider nicht entfallen.

6.2 Abbildungen im Zusammenhang mit der Sperrverfügung

Pascal Schumacher

Abb. 8: Grafische Gestaltung der Homepage „stormfront"

Abb. 9: Grafische Gestaltung der Homepage „nazi-lauck"

Abb. 10: Homepage von „nazi-lauck"

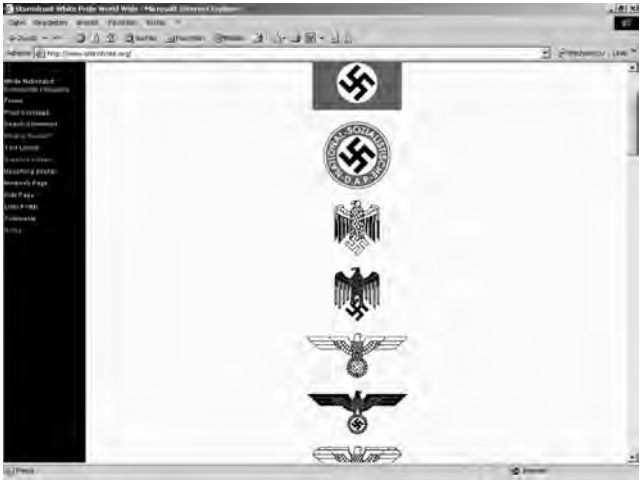


Abb. 11: Verwenden von Kennzeichen verfassungswidriger Organisationen

Anleitung zur Konfiguration der DNS-Einstellungen

für Windows 2000

Wichtige Vorbemerkung:

Windows 2000 ist ein Mehrbenutzer-Betriebssystem, das zwischen 'normalen' Benutzern und Administratoren unterscheidet. Normale Benutzer haben eingeschränkte Rechte bei der Benutzung, während Administratoren uneingeschränkt Einstellungen vornehmen dürfen.

Um die Einstellungen für die Konfiguration von DNS-Servern vornehmen zu können, müssen Sie als Administrator Rechte erlangen! - Das heißt, normalerweise sind Sie dann als *Administrator* beim System angemeldet.

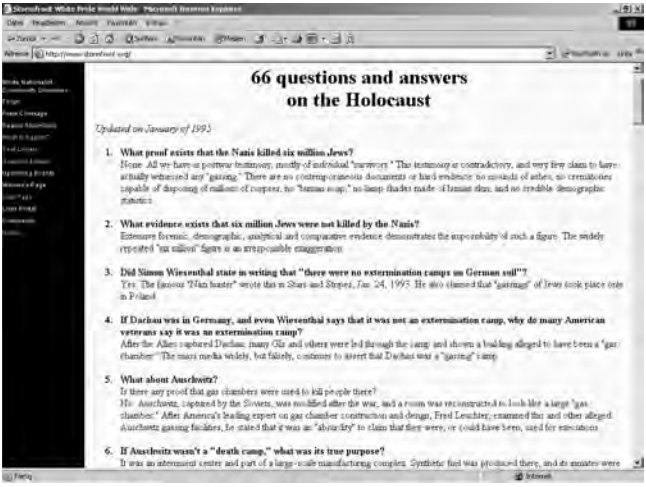
Wenn Sie nicht über Administrator-Rechte verfügen, können Sie in so einem Fall eine Einstellung trotzdem vornehmen. In diesen Fall müssen Sie Ihren Administrator bitten, die Einstellungen für Sie vorzunehmen. **Sorry!** Please blame Microsoft, not us.

Anleitung:

1. Öffnen Sie den *Arbeitsplatz* durch einen Doppelklick mit der linken Maustaste

2. Öffnen Sie die *Systemsteuerung* durch einen Doppelklick mit der linken Maustaste

Abb. 12: Anleitung des Chaos Computer Club zur Konfiguration der DNS-Einstellungen



66 questions and answers on the Holocaust

Updated on January of 1995

1. **What proof exists that the Nazis killed six million Jews?**
None. All we have is postwar testimony, mostly of individual "survivors." The testimony is contradictory, and very few claim to have actually witnessed any "gassing." There are no contemporaneous documents or hard evidence: no records of orders, no cremations capable of disposing of millions of corpses, no "human soap," no lamp shades made of human skin, and no credible demographic statistics.

2. **What evidence exists that six million Jews were not killed by the Nazis?**
Extensive forensic, demographic, analytical and comparative evidence demonstrates the impossibility of such a figure. The widely repeated "six million" figure is an unsupportable exaggeration.

3. **Did Simon Wiesenthal state in writing that "there were no extermination camps on German soil"?**
Yes. The famous "Nazi hunter" wrote this in Stars and Stripes, Jan. 24, 1993. He also claimed that "gassings" of Jews took place only in Poland.

4. **If Dachau was in Germany, and even Wiesenthal says that it was not an extermination camp, why do many American veterans say it was an extermination camp?**
After the Allies captured Dachau, many GIs and others were led through the camp and shown a building alleged to have been a "gas chamber." The mass media widely, but falsely, continues to assert that Dachau was a "gassing" camp.

5. **What about Auschwitz?**
Is there any proof that gas chambers were used to kill people there?
No. Auschwitz, captured by the Soviets, was modified after the war, and a room was reconstructed to look like a large "gas chamber." After America's leading expert on gas chamber construction and design, Fred Leuchter, examined that and other alleged Auschwitz gassing facilities, he stated that it was an "absurdity" to claim that they were, or could have been, used for executions.

6. **If Auschwitz wasn't a "death camp," what was its true purpose?**
It was an internment center and part of a large-scale manufacturing complex. Synthetic fuel was produced there, and its inmates were

Abb. 13: Verbreitung der Auschwitzlüge auf der Homepage „stormfront“

Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Postfach 10 34 43
40025 Düsseldorf

Telefon
› **02 11 / 7 70 07 - 0**
Telefax
› **02 11 / 72 71 70**
E-Mail
› **info@lfm-nrw.de**
Internet
› **http://www.lfm-nrw.de**