Das Internet zwischen Regulierung und Selbstregulierung

Dissertation zur Erlangung des akademischen Grades Dr. iur.

Eingereicht am 04.04.2008
bei der Juristischen Fakultät der Humboldt-Universität zu Berlin

von: Bernhard Georg Kern

Geboren am 30. September 1977 in Berlin

Präsident/ Präsidentin der Humboldt-Universität zu Berlin
Prof. Dr. Christoph Markschies

Dekan/ Dekanin der Juristischen Fakultät der Humboldt-Universität zu Berlin
Prof. Dr. Christoph Paulus

Gutachter/ Gutachterin
1. Prof. Dr. Bernhard Schlink
2. Prof. Dr. Henner Wolter

Tag der mündlichen Prüfung: 13.11.2008

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2008/2009 von der Juristischen Fakultät der Humboldt-Universität zu Berlin als Dissertation angenommen.

Mein Dank gebührt meinem Doktorvater, Herrn Prof. Dr. Bernhard Schlink, der die Arbeit inhaltlich gefördert und mir immer wieder Denkanstöße gegeben hat sowie PD. Dr. Henner Wolter für die schnelle Erstellung des Zweitgutachtens. Des Weiteren gilt er insbesondere dem Leiter Servicezentrums für Informations- und Kommunikationstechnik, Herrn Dipl. Inf. Gerrit Oldenburg sowohl für die geduldige Beantwortung der technischen Fragen, die die Grundlage dieser Arbeit bilden, als auch für zahlreiche sehr anregende inhaltliche Diskussionen. Nicht zuletzt möchte ich mich auf diesem Wege bei meinen Eltern für die andauernde Unterstützung während der Erschaffung dieses Werkes bedanken.

Schließlich gehört mein Danke ebenso Frau Dana Buchzik für die schnelle und gründliche Durchsicht der Arbeit.

Berlin im Herbst 2009

Bernhard Kern

Inhaltsverzeichnis

Literaturverzeichnis

Ahlert, Christian; Marsden, Chris; Yung, Chester: How Liberty Disappeared from Cyberspace http://pcmlp.socleg.ox.ac.uk/liberty.pdf, Oxford 2004

Bachof, Otto: Beurteilungsspielraum, Ermessen und unbestimmter Rechtsbegriff im Verwaltungsrecht, in: JZ 1955, S.97ff.

Balkin, Jack M.; Noveck, Beth Simone; Roosevelt, Kermit: Filtern von Internet-Inhalten – Ein Best-Practices Modell, in: Waltermann/Machill, Verantwortung im Internet, Gütersloh 2000

Baumbach, Adolf; Hefermehl, Wolfgang: Wettbewerbsrecht, 23. Auflage, München 2004

Berger, Christian: Jugendschutz im Internet: "Geschlossene Benutzergruppen" nach § 4 II S.2 JMStV, in: MMR 2003, S.773ff.

Von Bonin, Andreas: Die Kontrolle digitaler Kommunikationsinhalte, Baden-Baden 2000

Bücking, Jens: Liberalisierung im Vergabewesen deutscher Domainadressen?, in: GRUR 2002, S.27ff.

Christiansen, Per: Wahrheitswidrige Tatsachenbehauptungen in einem Internetportal, in: MMR 2004, S.185f.

Conrad, Hermann: Deutsche Rechtsgeschichte, Band I, 2. Auflage, Karlsruhe 1962

Denninger, Erhard; Hoffmann-Riem, Wolfgang; Schneider, Hans-Peter; Stein, Ekkehard: Alternativkommentar zum Grundgesetz, Band I, 3. Auflage, Neuwied 2001, zit. n.: AK-Bearbeiter, Art.

Denninger, Erhard; Hoffmann-Riem, Wolfgang; Schneider, Hans-Peter; Stein, Ekkehard: Alternativkommentar zum Grundgesetz, Band II, 3. Auflage, Neuwied 2001, Zit. n.: AK-Bearbeiter, Art., Rn.

Determann, Lothar: Kommunikationsfreiheit im Internet, Baden-Baden 1999

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
ALAC	At Large Advisory Committee (der ICANN)
AOL	America Online
APNIC	Asian-Pacific NIC
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
AVS	Altersverifikationssystem
BCP	Best Current Practice
BKA	Bundeskriminalamt
BPjM	Bundesprüfstelle für jugendgefährdende Medien
Bundesnetzagentur	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.
CCC	Chaos Computer Club
CD	Compact Disc
CERN	Conseil Européen pour la Recherche Nucléaire
DARPA	Defense Advanced Research Projects Agency
DENIC e.G.	Deutsches Network Information Center
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DoC	Department of Commerce (der US-Regierung)
DVD	Digital Versatile Disc
DSL	Digital Subscriber Line
DTAG	Deutsche Telekom AG
ECRL	E-Commerce Richtlinie, Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs
E-Mail	Electronic Mail
ENUM	Electronic Numbering bzw. Telephonic Number Mapping
EUNet	European ->Unix Network
FDDI	Fiber Distributed Data Interface
FSK	Freiwillige Selbstkontrolle der Filmwirtschaft
FSM	Freiwillige Selbstkontrolle Multimedia
FTP	File Transfer Protocol
GAC	Governmental Advisory Committee (der ICANN)

GB	Gigabyte, Maßeinheit für Speicherplatz
GjSM	Gesetz über die Verbreitung jugendgefährdender Schriften und Medien
HTTP	Hypertext Transfer Protocol
IAB	Internet Activities Board ab 1992 Internet Architecture Board
IANA	Internet Assigned Number Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICCB	Internet Configuration Contol Board
ICRA	Internet Content Rating Association
ID	Identification
IEC	International Electrotechnical Commission
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
InterNIC	Internet Network Information Center
IuKDG	Informations- und Kommunikationsdienste Gesetz
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ISO/OSI	ISO/Open Systems Interconnection (Standard)
ISOC	Internet Society
ITU	International Telecommunication Union
IVNM	Interessenverband Neue Medien
JÖSchG	Gesetz zum Schutz der Jugend in der Öffentlichkeit
JMStV	Jugendmedienschutzstaatsvertrag
JUNet	Japan ->Unix Network
JuSchG	Jugendschutzgesetz
KEK	Kommission zur Ermittlung der Konzentration im Medienbereich
KJM	Kommission für Jugendmedienschutz

KUG	Kunsturhebergesetz
LACNIC	Latin American and Caribbean Internet Addresses Registry
MDStV	Mediendienstestaatsvertrag
MILNET	Military Network
MARID	MTA Authorization Records in DNS
MASS	Message Authentication Standards
MTA	Mail Transfer Agent
NCP	Network Control Protocol
NomCom	Nomination Committee (der IETF)
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NWG	Network Working Group
OECD	Organisation for Economic Co-operation and Development
PIN	Personal Identification Number
RegTP	Regulierungsbehörde für Telekommunikation und Post, seit dem 01.01.2005: Bundesnetzagentur
RfC	Request for Comments
RIPE	Reseaux IP Européens
RIPE	RIPE Network CoordinationCenter
SAC	Stability und Security Advisory Committee (der ICANN)
SLD	Second Level Domain
SMS	Short Message Service
SPAM	Spiced Ham
ssh	Secure Shell
STD	Standard
TCP	Transfer Control Protocol
TDG	Teledienstegesetz
TDDSG	Teledienstedatenschutzgesetz
TMG	Telemediengesetz
TLD	Top Level Domain, sowohl als ccTLD: Country Code TLD als auch als gTLD: generic TLD genutzt
TKG	Telekommunikationsgesetz
UDP	User Datagram Protocol
UDRP	Universal Dispute Resolution Policy
ULD	Unabhängiges Landesdatenschutzzentrum Schleswig-Holstein

UMTS	Universal Mobile Telecommunication Standard
Unix	Ein besonders im Netzwerkbereich beliebtes Betriebssystem
UNO	United Nations Organisation
URL	Uniform Resource Locator
USB	Universal Serial Bus
USENET	User Network
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organisation
WSIS	World Summit on Information Society
WTO	World Trade Organisation
WWW	World Wide Web
XS4ALL	Niederländischer Host-Provider, Abkürzung für Access for All

A. Einführung

Eigentlich geschah Mitte der 60er Jahre nur etwas völlig Normales: Eine neue Kommunikationstechnologie entstand und wurde von einem kleinen Kreis aus Forschern über Jahrzehnte hinweg weiter entwickelt. Nachdem die Möglichkeit, diese Technologie nicht nur für sich, sondern auch für andere nutzbar zu machen, entdeckt und realisiert worden war, veränderten sich die Inhalte: Es tauchten nicht mehr nur rein wissenschaftliche, sondern auch private und kommerzielle Inhalte auf, ebenso wie verbotene. Die Letzteren führten zum Auftreten von Gefahren.

Häufig wird in diesem Zusammenhang die Formulierung „Gefahren des Internets“ gebraucht, die allerdings in der Regel nicht korrekt ist, da nicht Gefahren gemeint sind, die durch das Internet als Kommunikationsnetz entstehen, sondern solche, die durch über das Internet verbreitete Kommunikationsinhalte hervorgerufen werden. Bei gefährlichen Inhalten im „wirklichen Leben“ oder in einem nicht-globalen Kommunikationsnetz gestaltet sich die Bekämpfung relativ einfach: Sie werden verboten oder ihre Nutzung wird auf bestimmte Personenkreise eingeschränkt.

Derartige Vorgehensweisen sind auch bei über das Internet verbreiteten Inhalten möglich; da sich diese jedoch nicht zwangsweise im Zugriffsbereich des Staates befinden, der sie als Gefahr ansieht, treten hier Schwierigkeiten auf. In der Regel wird der Autor verbotener Inhalte zunächst versuchen, seine Person zu anonymisieren und die Inhalte außerhalb des Zugriffsbereichs des betreffenden Staates unterzubringen. Dies macht die herkömmlichen Methoden staatlichen Vorgehens gegen Gefahren durch Kommunikationsinhalte weitestgehend unwirksam.

Allerdings hängt die Rezeption der über das Internet übertragenen Inhalte von der Existenz einer technischen Infrastruktur ab. Ohne deren Mitwirkung können die Inhalte den Empfänger nicht erreichen. Die Betreiber solcher Infrastrukturen stellen daher für Staaten potentielle Ansatzpunkte für Einflussnahmen auf durchgeleitete oder gespeicherte Inhalte dar, welche sich sowohl im Ausland als auch im Inland befinden können.

Dabei ist es aus Sicht des Staates effektiver, die Host- und Access-Provider sowie andere Betreiber der Infrastruktur zu verpflichten, illegale Inhalte selbst zu entfernen oder zu sperren, als auf staatliche Anordnungen zur Entfernung zu setzen. Die eigenständige Kontrolltätigkeit der Host-Provider birgt jedoch Gefahren für die Kommunikationsgrundrechte und die – in allen Staaten erwünschte – wirtschaftliche Betätigung im Internet.

Hinzu kommt bei den Betreibern der Infrastruktur neben der rechtlichen Kontrollebene die der technischen Möglichkeiten hinzu, die die Einflussnahme des Staates begrenzen. Des Weiteren ist das Internet ein Zusammenschluss diverser Netzwerke, so dass auch die Gepflogenheiten des Netzes und seiner Institutionen, die sich in mittlerweile 40 Jahren entwickelt haben, zu beachten sind.

In diesem Geflecht von Zwängen und Begrenzungen, aber auch theoretisch nahezu unbegrenzten Möglichkeiten der Kontrolle, liegt die Besonderheit der Versuche der Regulierung des Internets gegenüber der Regulierung anderer technischer Anlagen.

Die vorliegende Arbeit geht davon aus, dass eine Regulierung des Internets als Kommunikationsnetz mit herkömmlichen Methoden innerhalb des derzeitigen rechtlichen Rahmens entweder die Grenzen des Zulässigen überschreitet oder wirkungslos bleibt. Es wird untersucht, wie eine Regulierung zur Erreichung der gewünschten Ziele gestaltet werden kann, ohne dass dafür die Grenzen des Zulässigen überschritten werden.

Das Ziel dieser Arbeit ist also nicht in erster Linie eine Darstellung der Gefahren, die durch über das Internet verbreitete Kommunikationsinhalte hervorgerufen werden, sondern vielmehr eine Darstellung der technischen Möglichkeiten staatlicher Kontrolle, der gegenwärtig und in der Vergangenheit angewandten Methoden staatlicher Kontrolle sowie eine Analyse der rechtlichen Zulässigkeit dieser Methoden. Der Schwerpunkt liegt dabei auf den Haftungsregeln für Inhalte sowie auf den Jugendschutzregelungen des Jugendmedienschutzstaatsvertrages (JMStV), insofern sie spezifisch die Verantwortlichen für das Internet als Übertragungsmedium betreffen. Dabei liegt der Fokus nicht auf den Regelungen hinsichtlich der Inhalte selbst, sondern auf denen, die auf Verantwortlichkeiten und Verhaltenspflichten der technisch an der Datenübermittlung beteiligten Personen zielen.

Im ersten Teil liegt der Schwerpunkt dementsprechend auf der Betrachtung der Versuche des deutschen Staates, die Gefahren durch Kommunikationsinhalte zu bekämpfen.

In einem zweiten Teil werden die das Internet als Struktur tragenden Organisationen und Gruppen sowie die von ihnen beschlossenen rechtlichen Regelungen und ihre Beratungs- und Entscheidungsprozesse dargestellt. Dabei wird besonderen Wert auf die Möglichkeiten staatlicher Einflussnahme auf die Entscheidungsprozesse_sowie die Anerkennung der Ergebnisse der unabhängigen Organisationen durch den deutschen Staat gelegt.

Die Gesamtbetrachtung wird ergeben, dass eine Regulierung von Inhalten, die sich nicht im Wirkungsbereich des deutschen Gesetzgebers befinden, zwar technisch möglich ist, dass jedoch die Kontrolle nie so vollständig wie bei herkömmlichen Medien sein kann: In vielen Fällen wird sie durch verschiedene Ausweichstrategien der Inhalteanbieter nahezu wirkungslos bleiben oder einen unverhältnismäßig großen Aufwand erfordern, während gleichzeitig ungewollte Nebenwirkungen in Form einer Gefährdung der Kommunikationsgrundrechte auftreten können.

Im Bereich des Jugendschutzes werden die gesetzlichen Regelungen im Bereich der über das Internet übertragenen Inhalte völlig wirkungslos bleiben, solange kein internationaler Konsens besteht. Hier hat der Gesetzgeber die realen Gegebenheiten des Internets zugunsten einer kompletten

Regulierung völlig außer acht gelassen und ein Beispiel dafür geliefert, wie sich eine Regulierung von Inhalten selbst zur Unwirksamkeit verdammt. Dies zeigt, dass völlige Sicherheit vor Gefahren durch Kommunikationsinhalte nicht existieren kann, ja sogar, dass der Versuch der Schaffung völliger Sicherheit durch den Staat zu deren Gegenteil führen kann.

Beispiele wirksamer Regulierung geben hingegen die das Internet technisch beherrschenden Organisationen, die jedoch keinen Einfluss auf die Inhalte ausüben; sie können, wenngleich nicht durch ihre Tätigkeit, jedoch durch die Art ihrer Organisation, als Vorbild für ein überstaatliches Tätigwerden gelten.

B. Grundlagen

Ohne eine Darstellung der historischen und technischen Grundlagen des Internets wäre eine Darstellung der Regulierungs – und Selbstregulierungsmechanismen weder vollständig noch verständlich sowie eine rechtliche Beurteilung nicht möglich.

I. Das Internet

Wie oben erwähnt, ist das Internet kein eigenständiges Netzwerk, sondern die Bezeichnung für sämtliche mit einer einheitlichen Gruppe von Protokollen zusammen geschaltete Netzwerke. Heutzutage ist es weltumspannend; Staaten, die über kein dem Internet angehörendes Computernetzwerk verfügen, sind eher mühsam zu finden - keiner von ihnen gehört zu den bedeutenderen Staaten der Erde[1]. Dieser Zustand wurde jedoch erst in den letzten zehn Jahren erreicht, die einen vergleichsweise kleinen Teil der noch jungen Geschichte des Internets darstellen.

II. Historisches

Die Vorläufer des heutigen Internet entstanden in den 60er Jahren des letzten Jahrtausends unter Anregung und Finanzierung der Advanced Research Projects Agency (ARPA)[2] in den USA. Es handelt sich bei der im Internet genutzten Technologie der Datenübertragung um so genanntes Packet-Switching (Paketvermittlung).

Exkurs: Packet-Switching

Bis zur Entwicklung der Technologie des Packet-Switching wurden Daten in Computernetzen nach demselben Verfahren übertragen, wie es in Telefonnetzen üblich ist.

1. Datenübertragung in Telefonnetzen

Auch Gespräche in Telefonnetzen werden als Daten übertragen: dies ist eine der Folgen der Digitalisierung des Telefonnetzes. Zwischen den Gesprächspartnern wird die Sprache zuerst von

1Dem Autor ist nur Lesotho bekannt.

2Sie wechselte ihren Namen häufiger zwischen ARPA und DARPA.

Tönen in Datensignale „übersetzt“ und anschließend wieder in Töne „zurückübersetzt“. Insofern besteht kein Unterschied zwischen der Übertragung von reinen Daten im Internet und Gesprächen im Telefonnetz, sondern ein Unterschied hinsichtlich der Art der Bereitstellung von Übertragungskapazitäten: In Telefonnetzen werden Daten verbindungsorientiert übertragen; das heißt, dass eine Verbindung vom Anrufer zum Angerufenen hergestellt und die Kapazität dieser Verbindung exklusiv für die Kommunikation zwischen den Gesprächspartnern reserviert wird. Dabei ist irrelevant, ob die Kapazität der Verbindung genutzt wird, also ((ob)) Daten übertragen werden, oder ob die Gesprächspartner schweigen, also kein Datenverkehr zustande kommt. Während der Zeitspanne, in der die Verbindung besteht, kann niemand außer den Gesprächspartnern die zwischen ihnen geschaltete Leitung nutzen. Bricht die Leitung wegen des Ausfalls einer Vermittlungsstelle, über die die Verbindung zustande gekommen ist, zusammen, ist keine Datenübertragung mehr möglich.

2. Packet-Switching

Grundgedanke des Packet-Switching ist es, Informationen in Telekommunikationsleitungen bzw. Computernetzwerken nicht wie bisher in spezifisch einem Nutzer zugewiesenen Verbindungen zu befördern, sondern in Pakete zu verpacken, die jeweils eigenständig und unabhängig voneinander transportiert werden. Es wird also keine den Kommunikationspartnern ausschließlich zugeteilten Verbindung hergestellt, sondern für jedes Paket eine neue Route gesucht. Dadurch muss eine Leitung nicht mehr unabhängig von der tatsächlichen Nutzung für eine bestimmte Zeit einem Nutzer zugewiesen werden. Dies macht die Technik einerseits ausfallsicherer – der Zusammenbruch einer Verbindungsstelle führt nicht zum Abbruch der Verbindung, sondern es wird für das Paket lediglich eine neue Route gesucht – und ermöglicht andererseits eine bessere Auslastung der Leitungen[1].

Ende Exkurs

Das Netz wurde auf Ausfallsicherheit der Gesamtstruktur, nicht einzelner Bestandteile, ausgelegt; man ging also von der Instabilität seiner Komponenten aus[2]. Aus militärischem Blickwinkel – und aus einem solchen heraus wurde das Internet ursprünglich entwickelt – war diese Netzwerkstruktur den bisherigen überlegen, weil es nicht mehr notwendig war, einen zentralen Server zu betreiben, dessen Ausfall das gesamte Netzwerk funktionsuntüchtig gemacht hätte.

1 Grassmuck, S.182, abrufbar unter: http://freie-software.bpb.de/teil2.pdf.

2 Sterling, Short History of the Internet, http://w3.aces.uiuc.edu/AIM/scale/nethistory.html.

1. 1969-1978: Das ARPANET unter der Trägerschaft der ARPA

Im Herbst 1969 startete das erste auf diesen Grundprinzipien beruhende Netzwerk von vier Großrechnern (Knoten) der University of California Los Angeles (UCLA), Santa Barbara (UCSB), der Stanford University und der University of Utah aus, die jeweils untereinander vernetzt waren. 1970 entstand aus dem RFC 1[1] das Network Control Protocol (NCP), der Vorläufer der bis heute angewendeten TCP/IP-Protokolle.

Anfang 1971 bestand das ARPANET aus 14 Knoten und wuchs um einen Knoten pro Monat. Die ersten Anwendungen für Datenübertragungen entstanden, die Standards für E-Mail, ftp und telnet wurden entwickelt. Bei der ersten Konferenz 1972 waren auch Teilnehmer aus europäischen Staaten anwesend; in Europa starteten in den 70er Jahren vielerorts Versuche mit paketvermittelten Computernetzwerken. 1973 kam die erste Version des netzwerkverbindenden TCP-Protokolls auf, welches – wie es bis heute üblich ist – in internationaler Kooperation entwickelt worden war. Bereits Mitte der 70er Jahre wurden Experimente zur paketvermittelten Sprachübertragung durchgeführt. Diese brachten zwar keinen spürbaren Erfolg hinsichtlich des angestrebten Zieles, da die Übertragungskapazitäten noch viel zu gering[2] waren, führten jedoch zur Trennung des TCP-Protokolls in das TCP und IP-Protokoll. Diese Protokolle sind auch heute noch von grundlegender Bedeutung für die Grundstruktur des Internets.

2. 1978-1990: Das ARPANET unter der Trägerschaft des ICCB

Nach der offiziellen Beendigung des ARPANET-Experiments 1978 wurde das Netz von amerikanischen Universitäten unter Führung des am Massachusetts Institute of Technology gegründeten Internet Configuration Control Board (ICCB) weiterhin unter dem Namen „ARPANET“ weitergeführt.

1983 sank die Zahl der angeschlossenen Knoten – zum ersten Mal seit Gründung des ARPANET – rapide, weil das Militär den militärischen Teil (MILNET) vom ARPANET trennte. Es blieben nur 45 von 113 Knoten übrig[3]. Zur gleichen Zeit wurde mit dem Aufkommen der ersten PCs der Grundstein für das enorme Wachstum der anschlussfähigen Rechner gelegt. Der kommerzielle Erfolg blieb dem Internet allerdings vorerst versagt, weil noch keine für weite Teile der Bevölkerung attraktiven Dienste zur Verfügung standen und die Bedienung der notwendigen Programme einen relativ große Fachkenntnis erforderte[4]. 1979 entstand das USENET, auf dem der

1Request for Comment, Standarddokumentation des Internets, zur Bedeutung s.u. S.173ff.

2Ein Hochleistungs-Backbone-Vermittlungsrechner hatte damals eine Datendurchsatzrate von 56 kB/s, dies ist heutzutage die Datentransferrate eines normalen Modems, das als veraltet gilt. Modems sind aber deutlich zu langsam für Sprachtelefonie. Diese ist erst heutzutage sinnvoll nutzbar, da für viele Nutzer Datentransferraten von 2 und mehr MBit/s erschwinglich geworden sind.

3http://w3.aces.uiuc.edu/AIM/scale/nethistory.html.

4An grafische Webseiten war noch nicht zu denken, die Programme erlaubten ausschließlich Kommandozeilen-Eingaben.

bis heute populäre News-Dienst beruht. Zusammen mit E-Mail, ftp und dem Anfang der 90er Jahre entwickelten WWW sind dies die beliebtesten Dienste des Internets.

In Europa bestanden Anfang der 80er Jahre die ersten Netze (EUNet, European Unix Network) mit Verbindungen zum ARPANET in den USA; Deutschland war davon allerdings aus politischen Gründen noch ausgeschlossen[1]. 1984 entstand in Japan das JUNet (Japan Unix Network), und auch die UdSSR erhielt Anschluss an das USENET. 1988 erhielt dann erstmals Deutschland von den Universitäten Dortmund und Karlsruhe aus einen auf TCP/IP basierenden Zugang zum ARPANET.

In Europa wurden schon vor dem Anschluss an das Internet verschiedene Netzwerke betrieben. In Deutschland waren das beispielsweise das HMI-Net I und II des Hahn-Meitner Instituts von 1974-79 sowie das BERNET I und II von 1976-82, in Frankreich das Cyclades-Netzwerk, die jedoch allesamt sehr viel kleiner als das Internet zu dieser Zeit waren[2].

Größere Versuche wurden in Europa mit Netzwerken durchgeführt, die auf dem sog. ISO/OSI Schichtenmodell basierten. Dazu gehörte das Datex-P Netzwerk in Deutschland und das PSS-Netzwerk in Großbritannien.

3. 1988-1995: Das NSFNET

Mitte der 80er Jahre wurde das von der National Science Foundation (NSF) der USA getragene NSFNET errichtet, das 1988 in Betrieb ging. Auch das NSFNET nutzte in Kontinuität zum ARPANET das TCP/IP Protokoll, wodurch dieses eine weitaus stärkere Verbreitung erfuhr als zuvor im ARPANET. Zwei Jahre lang existierten ARPANET und NSFNET parallel, bevor das ARPANET 1990 „abgeschaltet“ und seine Funktion vom moderner strukturierten NSFNET übernommen wurde. Dieses war ursprünglich als reines Backbone-Netz gedacht, das verschiedene Netze miteinander verbinden sollte. Die Rolle der NSF ging jedoch über die reine Finanzierung des NSFNET hinaus: Die von ihr vorgegebenen Nutzungsbedingungen des NSFNET ließen zwar keinen kommerziellen Datenverkehr zu[3], jedoch wurden regionale Netze, die auch kommerziellen Datenverkehr zuließen, sowie die Bildung kommerzieller Backbone-Netze[4] gefördert. In dieser Zeit verbreiteten sich leistungsfähige Computer zunehmend unter Privatpersonen, während das Telefonnetz in den meisten Industriestaaten digitalisiert wurde, so dass der potentielle Teilnehmerkreis für kommerzielle Datennetzwerke stark wuchs. Dies war neben der Ermutigung

1In Deutschland wie in einigen anderen europäischen Staaten wurde das sog. ISO/OSI Protokoll für zukunftsträchtiger gehalten und darum die Entwicklung von darauf basierenden Netzwerken gefördert.

2http://www.baeumle.com/internet/was-ist-das-internet.htm.

3Acceptable Use Policy, General Principle: (1) NSFNET Backbone services are provided to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. (...) Unacceptable Use: (10) Use for profit activities (...) (11) Extensive use for private or personal business. http://www.merit.edu/merit/archive/nsfnet/acceptable.use.policy.

4Géczy-Sparwasser, S.63f.

zum Betrieb gewerblicher Datennetze ein wesentlicher Faktor für den kommerziellen Durchbruch des Internets in der Öffentlichkeit.

4. Seit 1995: Das kommerzielle Internet

Im Jahre 1995 waren die Anzahl und Kapazität kommerzieller Datenübertragungsnetzwerke so weit angewachsen, dass die NSF ein von ihr betriebenes Netzwerk für unnötig erachtete und daher das NSFNET abschaltete. Dessen Funktion wurde weitgehend reibungslos von kommerziellen Providern übernommen, die inzwischen weltweit die wichtigsten Backbone-Netze betreiben.

5. Kurze Gremiengeschichte

Die Ursprünge des Internets lagen zwar in militärischen Forschungsprojekten, jedoch verfügten die am Start des ARPANET im Jahre 1969 beteiligten Universitäten über weit angelegte Freiräume. Obwohl die ARPA das Projekt finanzierte, wurde die Hauptarbeit von Doktoranden und später von Freiwilligen übernommen; eine feste Struktur mit tragenden Institutionen entwickelte sich nicht.

Die erste Organisation, die als Trägerin des ARPANET gegründet wurde, war das ICCB 1978, das 1983 in Internet Activities Board (IAB) und, nach Gründung der Internet Society (ISOC), 1992 in Internet Architecture Board umbenannt wurde. 1986 bildeten sich unter dem Dach des IAB die Internet Engineering Task Force (IETF) und die Internet Research Task Force (IRTF) als Standardisierungs- und Forschungsgremien von Freiwilligen.

Die wesentlichen Entscheidungsgremien des ARPANET blieben auch im NSFNET bzw. nach dessen Einstellung 1995 und beim Übergang auf kommerzielle Backbone-Netze unverändert. Die Entscheidungsfindung der Gremien basiert bis heute auf Diskussion und Konsens; das Motto lautet „rough consensus and running code“[1].

1989 wurde in Amsterdam das RIPE (Réseaux IP Européens) als Koordinierungsstelle der europäischen Netzwerkbetreiber gegründet. 1989 verfügten insgesamt 160 000 Rechner über ARPANET, während 1990 bereits alle Industrienationen angeschlossen wurden, ebenso wie die osteuropäischen Staaten, und die Anzahl der Rechner die Millionenmarke überschritt. Seit 1997 haben alle Staaten eigenständige ccTLDs.

1992 wurden die ISOC und die InterNIC (Network Information Center) gegründet. Letztere schrieb bereits bestimmte Dienste aus ihrem Aufgabenbereich an Dritte aus, wie etwa die Registrierungsdienste[2] an Network Solutions Inc. Damit wurde eine Struktur geschaffen, die in ihren Grundzügen nach wie vor besteht. Diese Kontinuität der Dienste und Gremien unabhängig von der vorhandenen physikalischen Infrastruktur zeigt außerdem erneut, dass „das Internet“ als solches nicht physikalisch existiert, denn es bestand trotz Veränderung der Netze weiter.

---

1 RFC 2031.

2Domainregistrierung und Betrieb von DNS-Servern.

Im Laufe der Jahre wurde TCP/IP zum faktischen Standard im Netz, auch wenn daneben noch verschiedene andere Protokolle verwendet werden; eine offizielle Anerkennung von TCP/IP blieb allerdings stets aus, weil namentlich die deutsche und japanische Regierung den ISO/OSI-Standard[1] für den Zukunftsstandard halten. Dieser ist jedoch nur bedingt mit TCP/IP kompatibel und gilt heute als gescheitert.

Exkurs: Internet und WWW

In der öffentlichen Darstellung wird das Internet häufig synonym mit dem World Wide Web gleichgesetzt. Letzteres ist eine Erfindung des Physikers Tim Berners-Lee, der in den 80er Jahren am Europäischen Kernforschungslabor CERN in Genf arbeitete. Er entwickelte ein Programm, mit dem nicht nur Daten untereinander verknüpft werden konnten (dies geschieht in Printmedien durch Fußnoten und Literaturangaben), sondern dem Leser außerdem ermöglicht wurde, den Verweisen auch außerhalb des Dokuments zu folgen: Die Idee der Links war geboren. Es bedurfte nun einer Sprache, welche die dazu nötigen Informationen aufnehmen konnte, eines Übertragungsprotokolls und schließlich eindeutiger Adressangaben für das Ziel. Der erste Testlauf des WWW erfolgte am 24.12.1990; Berners-Lee machte die Datenstruktur 1991 über das Internet weltweit zugänglich. Allerdings hatten die damaligen Webseiten mit den heutigen – abgesehen vom Konzept der Links – wenig gemeinsam; grafikfähige Browser beispielsweise gab es nicht, die Seiten bestanden aus reinem Text.

Technisch gesehen handelt es sich beim WWW um miteinander verknüpfte Inhalte, die mittels eines speziellen Protokolls über die Strukturen des Internet transportiert werden. Neben dieser inzwischen wohl wichtigsten Anwendung gibt es jedoch ((noch)) viele andere, die ebenfalls das Internet zum Datentransport nutzen. Das Internet ist somit nicht mit dem WWW identisch: Das WWW ist lediglich ein Dienst unter vielen, der die Übertragungsstrukturen des Internets nutzt.

Ein wesentlicher Grund für den Erfolg des Internets und des WWW war, dass das CERN entsprechend dem Wunsch von Berners-Lee keine Lizenzabgaben für die Nutzung und den Code des WWW erhob und sowohl die Browser-Software als auch deren Quellcode jedermann frei zur Verfügung stellte[2]. Dadurch konnte eine Entwicklung beginnen, die häufig als Revolution in der Kommunikationsgeschichte bezeichnet wird.

1Bei der ISO (Internation Organization for Standardisation) handelt es sich um eine internationale Regierungsorganisation mit einem schwerfälligen Standardisierungssystem, bei dem Standards auch noch mit nationalen Standardisierungsorganisationen koordiniert werden müssen. OSI steht für Open Systems Interconnection.

2Vgl. Géczy-Sparwasser, S.69.

III. Technisches

Von überragender Wichtigkeit ist die Kenntnis der Datenweiterleitung und der Rollen der Beteiligten im Internet[1]. Das Internet ist eine Zusammenschaltung verschiedenster Netze und Rechner über Datenleitungen, sei es per Funk, Telefonkabel oder Satellit; außerdem werden Fernsehkabelanlagen oder Stromleitungen für den Datentransport genutzt. Diese Aufzählung zeigt, dass es keine Infrastruktur DES einen Internets gibt und geben kann. Das Internet besteht lediglich aus einer Zusammenschaltung von Rechnern, die miteinander über das gemeinsame TCP/IP Protokoll kommunizieren. Es wäre (theoretisch) möglich, sämtliche Datenleitungen und Verbindungsrechner auszutauschen, ohne dass der Benutzer etwas davon bemerken würde. Das zeigt auch die Kontinuität dessen, was schon seit langem als das Internet bekannt ist, über die verschiedenen Netze – ARPANET, NSFNET und letztendlich das heutige Internet – hinweg. Auch ist die Struktur des Internets keine einheitliche, sondern durch das Gefüge der zusammen geschalteten Netzwerke bestimmt.

1. Digitale Datenübertragung

Computer können nur mit Binärcodes, also mit Nullen und Einsen, umgehen. Daraus ergibt sich, dass eine jede Datei, ob sie Texte, Bilder, Musik, Gespräche, ausführbare Programme oder anderes enthält, als eine Folge von Nullen und Einsen gespeichert sein muss. Dieser Vorgang heißt Digitalisierung. Aus einer Folge von Nullen und Einsen lässt sich aber noch nicht erkennen, welchen Inhalt die jeweilige Ziffernfolge im „Klartext“ hat[2]. Diese Information kann erst durch die sog. Codierungsinformationen einer Datei erkannt werden. Ein anschauliches Beispiel hierfür liefert das Ersetzen der Codierungsinformation eines Bildes (z.B. die Dateiendung) durch die eines Textes und die Öffnung der Datei per Textverarbeitungsprogramm; das Resultat ist in der Regel sinnloser Buchstaben- und Zeichensalat[3], nicht etwa die Anzeige des Bildes, obwohl sich die eigentliche Struktur der Datei nicht geändert hat.

Es existieren also zwei Schwierigkeiten in Bezug auf das Erkennen unbekannter Daten: Zum einen kann aufgrund fehlender Codierungsinformationen nicht sicher herausgefunden werden, was die übertragene Ziffernfolge darstellt, zum anderen sind selbst eindeutig erkannte Informationen nicht zwangsläufig diejenigen, die übertragen werden sollten[4]. Da beim Packet-Switching Dateien auch

---

1Eine sehr anschauliche sowie technisch zutreffende Beschreibung findet sich unter:

http://www.wdrmaus.de/sachgeschichten/internet/, als Video unter:

http://www.wdrmaus.de/service/download/dateien/vid_www.zip.

2Schneider, MMR 2004, 18, 19.

3Schneider, MMR 2004, 18, 19 gibt auch Beispiele, bei denen dieselbe Zeichenfolge unterschiedliche, aber sinnvolle Dateien codieren kann.

4Schneider, MMR 2004, S.8ff.

nicht als ganzes übertragen werden kann auch nicht sichergestellt werden, dass der Kontrolleur zwischen Sender und Empfänger jedes Paket abfangen kann.
Hier ergibt sich das erste Problem für die Kontrolle übertragener Daten auf dem Weg vom Sender zum Empfänger.

2. Datenübertragung im Internet

Die Vorläufer sowie auch das heutige Internet gehören zu den so genannten „Packet Switched Networks“ (paketvermittelnde Netzwerke). In diesen werden die zu übertragenden Daten vom Sender in einzelne „Päckchen“ zerstückelt; jedes „Päckchen“ erhält Angaben über den Absender und den Empfänger sowie einige andere Daten. Da sowohl die Informationen zu Empfänger und Absender als auch die eigentlich übertragenen Inhalte aus Nullen und Einsen bestehen, bestimmen die verwendeten Protokolle, wie viele Zeichen die Codierungsinformationen enthalten.
Da zumeist keine direkte Verbindung zwischen Sender und Empfänger besteht, müssen die Daten über mehrere andere Rechner, sog. Router, weitergereicht werden[1]. Zur Übermittlung dienen verschiedene Protokolle mit unterschiedlichen Funktionen. Es muss dem Sender und allen Übermittlern bekannt sein, wer der Empfänger ist und über welche Wege die Daten weitergeleitet werden müssen. Deshalb werden dem Päckchen zunächst die Empfängerdaten „angehängt“. Der Vergleich mit Briefmarken und Adressaufklebern auf Postpaketen liegt nicht fern.

Beispiel[2]:

01100100101	Das ist ein Beispiel für ein Datenpaket	010010
Header: Informationen über Sender und Empfänger	Inhalt der zu sendenden Informationen	Ende des Pakets

Die vor der eigentlichen Information befindlichen Daten heißen „Kopfdaten“ bzw. „Header“. Auf dem Weg zum Empfänger wird das Datenpaket in der Regel über mehrere Zwischenstationen geleitet, die der ursprünglichen Information eine zweite, Zwischensender und Zwischenempfänger betreffende, Datenschicht hinzufügen. Diese Weiterleitung heißt Routing; die dafür zuständigen Rechner, so genannte Router, sind in der Regel mit mehreren anderen Routern verbunden, deren

1Der Vorgang des Zerstückelns und Weiterleitens heißt Paketvermittlung.

2Zur Veranschaulichung wird für die Daten Klartext verwendet, die Binärinformationen sind fiktiv.

Auslastung und Funktionsfähigkeit sie, ebenso wie die Auslastung der sie verbindenden Datenleitungen, ständig abfragen. Auf diese Weise können Datenpakete stets auf dem schnellsten Weg an ihr Ziel gelangen. Entscheidendes Kriterium für die Weiterleitung ist die Geschwindigkeit, in der das Paket beim Empfänger ankommt; geographische Entfernungen spielen keine Rolle. Für die Adressierung an den Empfänger und das Routing werden keine „Klarnamen" genutzt, sondern weltweit eindeutige Bezeichnungen der Rechner, so genannte IP-Nummern.

a. IP-Nummern

IP-Nummern stellen das Adresssystem des Internets dar. Jeder am Datenaustausch beteiligte Rechner benötigt eine IP-Nummer, die ihn eindeutig identifiziert. Nach dem derzeit noch gültigen Standard IPv4 hat diese aus vier 16 Bit langen Nummernblöcken mit maximal 3 Dezimalzahlen zu bestehen (eine gültige Nummer lautet beispielsweise 141.20.120.67). Dies ermöglicht eine maximale Anzahl von 2^{32}, also knapp vier Milliarden, an das Internet angeschlossenen Computern. Als dieses Adresssystem konzipiert wurde, konnte sich niemand vorstellen, dass eine solche Menge nicht ausreichen würde; mittlerweile aber wird aufgrund der Knappheit an IP-Nummern den meisten Rechnern, die nicht permanent mit dem Internet verbunden sind, bei jeder Anwahl eine neue Identifikation zugewiesen, um keine festen Nummern an sie vergeben zu müssen[1].

Das Problem der Nummernknappheit wird durch eine neue Version des IP-Protokolls, IPv6[2], behoben werden. IP-Nummern, bestehend aus sechs Nummernblöcken, inklusive hexadezimaler Angaben, konzipiert und dadurch insgesamt 2^{128} IP-Nummern ermöglicht. Somit könnten pro Quadratmeter Erdoberfläche 6,5 x 10^{23} IP-Nummern vergeben werden[3]. Die bereits begonnene Umstellung des Domain Name Systems (DNS) auf IPv6 wird allerdings noch einige Jahre in Anspruch nehmen. Bisher werden diese Adressen vor allem in Asien und bei einigen der Root-Server genutzt.

Da sich die Nummern beider IP-Protokolle nur schwer memorieren lassen, wird für die Bezeichnung der Rechner im World Wide Web (WWW) das DNS verwendet.

b. Domain Name System

Das Domain Name System (DNS) wurde 1984 eingeführt, um das Internet, das wegen der stark angestiegenen Zahl der Server unübersichtlich wurde, wieder überschaubarer zu machen. Dieses Ziel kann als erreicht gelten.

1Damit verändert sich die Struktur der Nutzer: während bei festen IP-Nummern jeder sowohl Daten anbieten als auch anfordern kann, ist dies bei wechselnden Nummern nur schwer möglich, da denjenigen, die auf die angebotenen Daten zugreifen möchten, auch die IP-Nummer bekannt sein muss.

2Zusammen mit der Umstellung auf sechs Nummernblöcke, die jeweils vier statt wie vorher drei Zeichen umfassen, können Nummern dann auch aus Hexadezimalzahlen bestehen. Weiteres unter http://de.wikipedia.org/wiki/IPv6.

3http://de.wikipedia.org/wiki/IPv6.

Das DNS ist eine dezentrale Datenbank, die sich auf einer Vielzahl von so genannten Nameservern befindet; das heißt, dass es keinen allein gültigen Server gibt[1], sondern dass ein Zusammenspiel von Servern erfolgt, auf denen jeweils Teile des gesamten DNS gespeichert sind.
Auch mit Verwendung des DNS werden Rechner weiterhin durch IP-Nummern identifiziert und können direkt durch die Eingabe der IP-Nummer im Browser angesprochen werden. Die DNS-Nameserver übersetzen den leichter zu merkenden Domain-Namen (z.B. hu-berlin.de) in die der (jeweiligen) Domain zugeordnete IP-Nummer. Die Adressierung der gesendeten Daten geschieht dann mit den vom Nameserver ermittelten IP-Adressen.

(1.) Vergabe von Domainnamen

Domainnamen werden auf verschiedenen Ebenen vergeben, welche Hierarchiestufen entsprechen, die von hinten nach vorne „sinken"; die unterschiedlichen Ebenen werden durch Punkte voneinander getrennt. Die oberste Hierarchieebene ist die Top-Level-Domain (TLD), die immer am Ende eines Domainnamens steht[2]. TLDs werden wiederum in Generic TLDs (gTLD), die staatenunabhängig sind, und Country Code TLDs (ccTLD), die einem bestimmten Staat zugewiesen sind (.de für Deutschland, .at für Österreich, .fr für Frankreich etc.) unterteilt. Die gTLDs werden von der ICANN verwaltet und zugelassen, die die technische Durchführung der SLD-Vergabe sowie die Verwaltung der Root-Server an Unternehmen weiter gibt.
Die Abkürzungen der ccTLDs richten sich nach den internationalen Festlegungen für länderspezifische Abkürzungen der International Standards Organization (ISO); einzig Großbritannien verwendet .uk anstatt des sonst üblichen GB. Die Vergabe der ccTLDs hat die ICANN bestimmten, für einzelne Staaten zuständigen Organisationen übertragen, in Deutschland der DENIC e.G. Einige Staaten lassen ihre ccTLDs auch von Unternehmen vermarkten; hierbei handelt es sich meist um kleinere Staaten wie Tuvalu (.tv) oder Antigua (.ag), die wirtschaftlich interessante ccTLDs besitzen, die aus nahe liegenden Gründen in der Regel nicht nur von nationalen Unternehmen oder Personen genutzt werden. Aus dem Verkauf ihres Adressraums finanzieren solche Staaten teilweise einen nicht unwesentlichen Bereich ihres Haushalts.
Eine Stufe unterhalb der Top-Level-Domain steht die wirtschaftlich interessante Second Level Domain (SLD); wenn von Domains gesprochen und geschrieben wird, sind gewöhnlich SLDs gemeint. Diese können nach je nach TLD verschiedenen Regeln bei international einheitlichen

1Das wäre technisch möglich, allerdings wäre seine Funktion wegen der Vielzahl der Anfragen erheblich langsamer, als es derzeit der Fall ist.

2Eigentlich ist die oberste Ebene die so genannte Root-Ebene, die durch einen „." gekennzeichnet wird, der aber gewöhnlich ausgelassen wird.

Registraren angemeldet werden, welche die Anmeldung an die Registries weiter reichen, die auch die DNS-Nameserver der Domain betreiben.

(2.) Identifikation von IP-Nummern über das DNS

Technisch gesehen setzt die Ansprechbarkeit eines Rechners über das DNS voraus, dass dessen Domain auf einem DNS-Server bekannt und für einen Rechner mit IP-Nummer registriert ist, mit anderen Worten einen Datenbankeintrag erhalten hat. Ein Rechner stellt eine Anfrage mit einer Domain an einen DNS-Server, der als Antwort die gewünschte IP-Nummer zurück sendet, so dass der anfragende Rechner nun das Ziel durch die IP-Nummer identifizieren und an dieses eine Anfrage richten kann.

Wenn der angesprochene Nameserver die Domain (beispielsweise weil sie unter einer anderen TLD registriert ist) nicht kennt, stellt er seinerseits eine Anfrage an den hierarchisch nächsthöheren Nameserver, der entweder mit der zugehörigen IP-Nummer antwortet oder seinerseits den nächsthöheren Server fragt. Der hierarchisch höchste Server[1] ist der so genannte Root-A Server von VeriSign Inc. Dieser kennt zwar nicht alle weltweit eingetragenen Domains, verweist aber jeweils auf die zu den TLDs gehörigen Nameserver. Weltweit existieren 13 Root-Server (Root-Server A-M)[2], von denen die meisten ihren Standort in den USA haben und die inhaltlich mit dem Root-A-Server identisch sind[3]; ihre genauen Standorte sind aufgrund ihrer wichtigen Funktion geheim[4]. Die ICANN ist vom Handelsministerium der USA (DoC) abhängig und muss jede Änderung am Root-A-Server von ihm genehmigen lassen. Die Vergabestellen der TLDs[5] betreiben eigene Nameserver, denen alle unter „ihrer“ TLD eingetragenen SLDs bekannt sind.

Wenn eine SLD einen eigenen DNS-Server betreibt, kann sie auch unter ihrer Domain Subdomains, auch Third-Level-Domains genannt, vergeben; der Betreiber einer SLD kann somit dieselbe Funktion wie eine Vergabestelle ausüben.

Ein Beispiel hierfür wäre die Humboldt-Universität zu Berlin, welche der Juristischen Fakultät die Third-Level-Domain „rewi“ zugewiesen hat[6]. Vor der letzten Domain ist gewöhnlich der Servername genannt; in der Regel heißt der World-WideWeb-Server einer Domain „www“. Um den

---

1Auch hierbei handelt es sich nicht um ein einen einzelnen Rechner, sondern um eine Vielzahl von zusammenarbeitenden Rechnern.

2http://www.root-servers.org/.

3http://de.wikipedia.org/wiki/Root-Server. Die Anfragen, die eigentlich an den Root-A-Server gerichtet sind, werden je nach Auslastung von den Servern A-M beantwortet; es wäre auch möglich, das Internet nur mit dem Root-A-Server zu betreiben, dies hätte aufgrund der Belastungen jedoch eine deutliche Verlangsamung des Datenverkehrs zur Folge.

4Würde man den Root-A-Server komplett außer Betrieb setzen, wären die Folgen nicht sofort, aber innerhalb von 2-3 Tagen spürbar. Würden alle Root-Server außer Betrieb gesetzt, käme die Datenübermittlung weitestgehend zum Erliegen.

5Für die .de TLD ist dies die DENIC e.G.

6Einige Staaten nutzen auch zweigeteilte Länderkennzeichen, wobei der erste Teil eine bestimmte Nutzung anzeigt, während der zweite Teil ausschließlich auf die geographische Herkunft hinweist. Dies ist z.B. in Großbritannien und Österreich der Fall.

Webserver der Juristischen Fakultät der Humboldt-Universität anzusprechen, muss man also den Rechner www.rewi.hu-berlin.de bzw. (den identischen Rechner) 141.20.120.67 kontaktieren.

c. Protokolle

Damit Rechner miteinander kommunizieren können, müssen sie einheitliche Kommunikationsstandards, so genannte Protokolle, nutzen. Die wichtigsten Protokolle im Internet sind http (für den Abruf von Webseiten), ftp (für die Übertragung von Dateien), mail (zur Übermittlung von E-Mails), die TCP/IP Protokoll-Suite[1] sowie das vor allem im Bereich des DNS genutzte UDP. Einige dieser Protokolle bezeichnen so genannte Anwendungsprotokolle wie mail oder ftp, welche die Funktionen von Anwendungen im Internet beschreiben, andere bilden technische Grundlagen und schaffen die Voraussetzungen für die Datenübermittlung, so zum Beispiel TCP/IP.
Die derzeitigen Protokolle für die Datenübertragung sind technisch auf eine möglichst reibungslose und schnelle Datenübertragung ausgerichtet, die auch durch technische Störungen möglichst wenig beeinflusst werden soll. Sie sehen jedoch keine Beeinflussungen des Inhalts während der Übertragung oder eine Verhinderung des weiteren Transports anhand irgendwelcher Kriterien vor. Dies könnte allerdings geändert werden.

3. Beteiligte an der Datenübermittlung und Eingriffsmöglichkeiten

An einer Datenübermittlung im Internet ist eine größere Anzahl von Akteuren beteiligt, als es zunächst den Anschein hat. Der größte Teil der bei der Datenübermittlung notwendigen Prozesse geschieht allerdings automatisch und von den Nutzern unbemerkt.

a. Nutzer

Der Nutzer initiiert eine Übermittlung von Daten per Anfrage beim jeweiligen Anbieter und empfängt diese am Ende der Übertragung. Auf seinem Rechner entstehen außerdem größere Mengen an Verbindungsdaten; auch finden sich im Zwischenspeicher – der durchaus längere Zeit auf der Festplatte gespeichert sein kann – alle abgerufenen Dateien als Kopie. Der Rechner des Benutzers bietet sich damit als Quelle für Ermittlungen bei Rechtsverstößen an. Zugleich stellt er einen möglichen Ansatzpunkt für den Einsatz von Filterprogrammen dar, welche verhindern, dass Pakete mit unerwünschtem Inhalt angenommen oder angezeigt werden. Die Installation von Filterprogrammen könnte rechtlich erzwungen werden, durchsetzen ließe sich eine derartige Regelung aber nur schwer. Es wäre allerdings möglich, die Hersteller von Rechnern anzuregen oder

1Dabei handelt es sich nicht um ein Protokoll, sondern um eine ganze Gruppe von Protokollen, welche die Datenübermittlung kontrollieren.

zu verpflichten, auf den Rechnern bei Auslieferung Filterprogramme mit bestimmten Voreinstellungen zu installieren.

Präventive rechtliche Regelungen zur Regulierung sind aufgrund der Menge an Rechnern praktisch nicht durchsetzbar. Es gäbe allenfalls die Möglichkeit, die Hersteller von Standardsoftware zu verpflichten, bestimmte Funktionalitäten in ihre Produkte zu integrieren. Auch dies ist jedoch bei freier Software nicht umsetzbar.

b. Access-Provider

Access-Provider beschaffen Nutzern den Zugang zu Angeboten eines Netzwerks. In der Regel erfolgt die Einwahl mit einem Modem, ISDN oder DSL über Telekommunikationsleitungen. Die Access-Provider stellen durch ihre Einwahlrechner die Möglichkeit bereit, über diese Telekommunikationsleitungen Zugang zu einem Netzwerk zu erhalten. Ähnliches gilt für eine Einwahl über DSL und auch bei so genannten Flatrates. Jedes Datenpaket passiert dabei zwangsweise denselben Zugangsrechner (auch Gateway genannt), über den die Nutzer mit dem Netz des Providers verbunden sind: Dies ist der Schnittpunkt zwischen dem Internet und dem Telefonnetz.

Damit die Nutzer Zugang zu Angeboten im Internet erhalten können, erhalten sie von ihrem Access-Provider eine IP-Nummer, die in der Regel bei jeder Einwahl wechselt. Das könnte sich mit der Umstellung auf IPv6 ändern, wenn IP-Nummern auf absehbare Zeit kein knappes Gut mehr darstellen werden. Access-Provider betreiben oft eigene DNS-Server und speichern Datenpakete von häufiger angeforderten Angeboten zwischen (so genanntes Caching), um Leitungskapazitäten und damit Kosten zu sparen, aber auch um Inhalte schneller verfügbar zu machen. Des Weiteren betreiben sie in der Regel eigene Mailserver, FTP-Server und häufig auch Web-Server. Diese Strukturen werden über den so genannten Backbone mit dem jeweiligen Nutzer und dem weltweiten Internet verbunden.

Nutzer benötigen keine Access-Provider, wenn sie direkt an ein Netzwerk, das in Verbindung mit dem Internet steht, angeschlossen sind. Die Betreiber solcher Netzwerke heißen Netzwerk-Provider.

Access-Provider stellen die Schnittstelle zwischen Netzwerk und Nutzer bereit und sind damit möglicher Ansatzpunkt für eine Filterung von Inhalten. Sie können auch durch Manipulationen an den DNS-Servern Inhalte unerreichbar zu machen oder bestimmten Nutzern durch Verweigerung der Zuteilung von IP-Nummern den Zugang zu Inhalten zu verwehren.

Nach der Terminologie von § 8 TMG (vormals § 11 TDG bzw. § 9 MDStV) sind Access-Provider „Diensteanbieter [...] die Informationen in einem Kommunikationsnetz durchleiten“. Diese Definition kann aber noch weitere mögliche Funktionen von Anbietern umfassen. Im Sinne der Rechtssicherheit wäre es – wenn auch ein Verstoß gegen das „Gebot“ der Deutschsprachigkeit –

wünschenswert gewesen, hätte sich der Gesetzgeber der in der Praxis und Literatur üblichen Terminologie bedient.

c. Gateway-Betreiber

Gateways befähigen auf unterschiedlichen Protokollen basierende Netzwerke dazu, miteinander zu kommunizieren. Den Gateways ist dabei alles erlaubt, was zur Konvertierung der Daten notwendig ist, auch das Weglassen von Informationen, wenn diese im Zielnetz auf Grund der dort verwendeten Protokolle nicht transportiert werden können. Gateways sind für die Kommunikation zwischen Netzwerken unbedingt notwendige Bestandteile.

Die häufigste Art von Gateways dürften kleine Internet-Router sein, die Rechnern in einem lokalen Netz den Zugang zum Internet ermöglichen. Meist stellt das Gerät dabei selbstständig die Verbindung zum Internetanbieter her und nimmt verschiedene Adressumsetzungen – so genanntes Masquerading – vor, die notwendig sind, da der Internetanbieter meist nur eine IP-Adresse zur Verfügung stellt und sich die Rechner im lokalen Netz dahinter „verstecken“ müssen[1]. So kann ein Netzwerk mit einer IP-Adresse aus mehreren Rechnern bestehen, die intern andere Kennungen haben, aber nach außen nur als ein einzelner Rechner zu erkennen sind. Gateways müssen zwischen Netzwerken verwendet werden, die mit IPv4 und IPv6 zusammenarbeiten. Dies wird auch auf höheren Netzwerkebenen der Fall sein, solange die Umstellung auf IPv6 nicht abgeschlossen ist.

Daneben gibt es auch Gateways für zahlreiche andere Verwendungszwecke, etwa E-Mail zu SMS, Fax zu E-Mail, E-Mail zu Sprache etc. Auch diese übersetzen Daten in andere Formate und Formatierungen. Durch diese Funktionalität könnten Gateways zwischen größeren Netzen eine Ansatzstelle für Eingriffe bieten; allerdings ist es aufgrund der Struktur des Internets durchaus möglich, dass ein Netz durch mehrere Gateways mit anderen Netzen verbunden ist und deshalb nicht alle Pakete, die für einen Nutzer bestimmt sind, dasselbe Gateway passieren müssen. In Datennetzen von Unternehmen ist es bereits üblich, dass Gateways mit Firewalls zusammenarbeiten und dass der Zugang zu bestimmten Angeboten gesperrt wird.

d. Router-Betreiber

Ein Router ist ein Vermittlungsrechner, der in einem Netzwerk dafür sorgt, dass zu verschickende in einzelne Pakete zerlegte Daten zum vorgesehenen Zielrechner weitergeleitet werden. Der Router bedient sich bei der Wegbestimmung einer Routingtabelle; im Falle von IP und IPX beinhaltet diese sowohl vom Administrator hinzugefügte statische als auch dynamische Einträge, die aus Routing-

1als Überblick: http://de.wikipedia.org/wiki/Gateway, vertiefend: Tanenbaum, S.362ff.

Protokollen resultieren und automatisch generiert werden. Die Wahl der Route durch das Netzwerk nach bestimmten Kriterien wie Entfernung, Kosten oder Sicherheit ist möglich.

Die Hochgeschwindigkeitsrouter im Internet sind heute hochgradig auf das Weiterleiten von Paketen optimierte Geräte mit mehreren Gigabit Durchsatz pro Sekunde.[1] Die Weiterleitung wird dabei nicht durch Software, sondern durch Hardware gesteuert, was einerseits die Geschwindigkeit erhöht, andererseits die Möglichkeiten eines Zugriffs von außen verringert.

Eingriffe durch Filterung scheiden auf der Ebene der Router aus, da sie die Leistung zu sehr verringern und damit praktisch den Datenfluss zum Erliegen bringen würden. Eingriffe in die IP-Tabellen sind aber möglich.

e. DNS-Server Betreiber

DNS-Server werden in zwei Klassen aufgeteilt: Autoritative und nicht-autoritative. Autoritative Nameserver sind auf aktuellem Stand, während nicht-autoritative dies nicht gewährleisten. Dementsprechend sind autoritative Nameserver bei den Registries angesiedelt, während nicht-autoritative von jedermann betrieben werden können.

Die übergeordneten Server werden von den Netzinstitutionen, also Registries und der ICANN, betrieben. Die DNS-Datenbanken werden gewöhnlich automatisch aktualisiert; manuelle Veränderungen sind aber auch möglich. So können Einträge zu bestimmten Domains entweder dahingehend manipuliert werden, dass die Domain dem Nutzer als existent angezeigt wird oder dass die Anfrage auf eine andere IP-Nummer umgeleitet wird[2].

Veränderungen am DNS-Server führen dazu, dass diejenigen Domains, deren Einträge manipuliert wurden, nicht mehr erreichbar sind. Statt des standardmäßig verwendeten DNS-Servers des Providers kann aber auch problemlos ein anderer, beispielsweise in einem anderen Staat befindlicher, DNS-Server genutzt werden, um diese Art des Eingriffs zu umgehen.

f. Host-Provider

Host-Provider stehen technisch gesehen am anderen Ende der Datenübertragungskette. Sie stellen Speicherplatz für Inhalte zur Verfügung und sorgen für deren Erreichbarkeit. Nach § 10 TMG (vormals § 11 TDG / § 9 MDStV) sind sie Diensteanbieter, die fremde Informationen speichern. Daneben sind sie meist Registrare für Domainanmeldungen und stellen somit den idealen Anknüpfungspunkt für eine Beeinflussung von Inhalten dar: sie müssen diese lediglich von ihren Servern löschen oder anderweitig unerreichbar machen. Die größte Schwierigkeit stellt sich allerdings bei Host-Providern im Ausland, die dem deutschen Recht nicht unterliegen und derartige Eingriffe ignorieren, wenn die Inhalte – wie fast immer in derartigen Fällen – nach ihrem nationalen

1Quelle: http://de.wikipedia.org/wiki/Router.

2Beispielsweise werden Anfragen auf „sieg-heil.de“ auf das Angebot von „shoa.de“ umgeleitet.

Recht legal sind. „Jugendschutz.net“ hat allerdings unlängst in Kooperation – nicht durch staatlichen Zwang – mit Providern in den USA erreicht, dass diese auf ihren Servern gespeicherte jugendgefährdende Inhalte gelöscht haben[1].

g. Content-Provider

Content-Provider stellen Inhalte, also die abzurufenden Daten, bereit. Ein Vorgehen gegen sie ist nur dann Erfolg versprechend, wenn die Inhalte auch in dem Staat, in dem sie ihren Sitz haben, unzulässig sind. Ist dies nicht der Fall, ist ein Vorgehen mittels staatlichen Zwangs gegen sie häufig aussichtslos. Darin liegt das mit Abstand größte Problem der Verfolgung rechtswidrigen Verhaltens.

h. Suchmaschinen

Anders als die zuvor beschriebenen Beteiligten haben Suchmaschinen keine Bedeutung für die Datenübermittlung. Sie stellen keine eigenen Informationen zur Verfügung, sondern halten vielmehr einen Katalog abrufbarer Inhalte bereit, der nach Stichworten durchsucht werden kann. Aufgrund der Vielzahl der Inhalte sind Suchmaschinen häufig die einzige Möglichkeit, Inhalte unbekannter Adressen ausfindig zu machen. Wenn bestimmte URLs aus dem Index von Suchmaschinen entfernt werden, können diese praktisch nicht mehr oder nur noch unter sehr großem Aufwand erreicht werden. Somit sind auch Suchmaschinen geeignete Ansatzpunkte, um den Zugang zu Inhalten wesentlich zu erschweren.

IV. Regulierung und Selbstregulierung

So klar die Grundsätze der beiden Konzepte zu sein scheinen, so unscharf sind sie in ihren Grenzbereichen[2]. Zwischen den beiden Polen liegen zwei Formen von hybriden Modellen: Regulierung mit Einbau selbstregulativer Elemente und regulierte Selbstregulierung. Für diese Arbeit_gilt es zunächst die verschiedenen Begriffe zu klären und voneinander abzugrenzen.

1. Staatliche, imperative Regulierung

Regulierung bedeutet jedenfalls das staatliche, hoheitliche Eingreifen in bestimmte Bereiche durch Gesetze und darauf aufbauende administrative Maßnahmen, die das Verhalten der Adressaten, sei es durch Vorschriften oder durch Verbote, lenken. Dies setzt jedoch auf Seiten des Staates das regulierungsrelevante Wissen und natürlich auch die Möglichkeit einer regulativen Steuerung voraus. Im Bereich des Internets kann es sich hierbei etwa um verschiedene Datenschutzgesetze, das

1Meldung von Jugendschutz.net vom 26.07.04.

2 Zu den verschiedenen Methoden, die unter dem Begriff gewöhnlich zusammengefasst werden: Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.300ff.

Strafgesetzbuch, das TMG und den RStV oder die Polizeigesetze der Länder handeln, aber auch um Verträge wie den „ENUM-Vertrag“ zwischen der DENIC e.G. und der RegTP. Darauf aufbauend greift der Staat – entweder durch Verwaltungsentscheidungen auf dem Gebiet des öffentlichen Rechts oder durch Gerichtsentscheidungen im Privatrecht – direkt auf die Akteure zu. Diese Form staatlichen Handelns wird vor allem in der Eingriffsverwaltung verwendet[1].

2. Regulierung mit selbstregulativen Elementen

Hierbei handelt es sich grundsätzlich um staatliche Regulierung. Der Staat nutzt dabei Möglichkeiten, Kenntnisse und Engagement privater Akteure und überträgt ihnen Verantwortung, um staatlich vorgegebene Ziele zu erreichen[2]. In den regulierenden Vorschriften werden die Möglichkeiten einer begrenzten Selbstregulierung geschaffen und in das Regulierungskonzept integriert, wobei die Erfüllungsverantwortung beim Staat verbleibt. Diesem Konzept liegt die Annahme zugrunde, dass die Aufgaben leichter zu erfüllen seien, wenn die Regulierten Spielraum für eigene Entscheidungen haben[3]. Häufig werden auch die Eigeninteressen der Beteiligten nutzbar gemacht, um das Regulierungsziel zu erreichen[4]. Ein weiterer nützlicher Nebeneffekt dürfte die größere Akzeptanz derartiger Regulierungsinstrumente sein, welche die Durchsetzung der Ziele letztlich beschleunigt.

3. Regulierte Selbstregulierung

Zwischen dem Modell der „Regulierung mit selbstregulativen Elementen“ und der reinen Selbstregulierung liegt die Regulierte Selbstregulierung. Hierbei überlässt der Staat Privaten – auch unter Einschluss privatautonomer Zielsetzung – die Regulierung[5]. Regulierte Selbstregulierung liegt vor, wenn Selbstregulierungsanliegen mit Regulierungsanliegen verbunden und aufeinander bezogen werden und sich ergänzen[6]. Auf der Aufgabenebene wird sie als „das Scharnier des Übergangs von der Erfüllungs- zur Gewährleistungsverantwortung“[7] bezeichnet, welches vor allem, aber nicht ausschließlich, zum Einsatz komme, wenn der Staat die gewünschten Ergebnisse durch Ge- und Verbote nicht oder nur unter erheblichem Aufwand selbst erreichen könne[8]. Dies sei insbesondere dann der Fall, wenn das für eine Regulierung erforderliche Wissen auf Seiten des Staates nicht oder zu spät verfügbar sei[9]. Durch Regulierte Selbstregulierung würden nicht nur die Möglich-

1Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.300.

2Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.300.

3Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.300f.

4Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.301.

5Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.301.

6Schmidt-Aßmann, S.255.

7Schmidt-Aßmann, S.257.

8Rossen-Stadtfeld, AfP 2004, 1, 2.

9Rossen-Stadtfeld, AfP 2004, 1, 3.

keiten gesellschaftlicher Selbstregulierung abgesichert und erweitert, sondern auch den gesellschaftlichen Akteuren diverse Entfaltungsspielräume und Optionen angeboten[1], wodurch die Leistungsfähigkeit verschiedener Teile der Gesellschaft zu einem Maximum gebracht werden könne, ohne dass andere mehr als nötig an der Entfaltung ihrer Leistungsfähigkeit gehindert würden[2]. Die Erfüllungsverantwortung liege nicht mehr beim Staat, sondern gehe auf die Selbstregulierungsgremien über[3]; der Staat beschränke sich darauf, einen regulativen Rahmen für die Selbstregulierung zu setzen, der den Spielraum der Akteure begrenze und ihre Optionen konkretisiere[4]. Um eine Nutzung der Privatautonomie zu einem Machteinsatz zum Schaden Dritter zu vermeiden, seien die Regeln häufig auf die Vermeidung bzw. den Ausgleich von Machtungleichgewichten ausgerichtet, damit die Interessen aller Beteiligten möglichst gut ausbalanciert werden könnten[5]. Je homogener die betroffenen Interessen seien und je weniger Machtungleichgewichte existierten, desto geringer sei die Notwendigkeit eines engen regulativen Rahmens[6]. Voraussetzung für ein Gelingen sei aber eine möglichst breite Beteiligung aller Betroffenen und damit eine große Interessenvielfalt zur Erhaltung und Förderung der Dynamik in den Selbstregulierungsgremien[7].

Beispiele für vorhandene Regulierte Selbstregulierung sind die Rundfunk- und Fernsehräte im öffentlich-rechtlichen Rundfunk, Rundfunkkommissionen der Landesmedienanstalten und spezieller die Kommissionen zur Ermittlung der Konzentration im Medienbereich (KEK).

Ein etwas anders strukturiertes Modell ist das der primären privaten Aufgabenübernahme, wobei der Staat nicht nur Zielvorgaben setzt, sondern auch ein „Auffangnetz“ bereithält, dessen bloße Existenz als vorbeugend gegen ungewollte, aber mögliche Entwicklungen wirken soll[8]. Es beinhaltet zudem die Statuierung einer (Handlungs-) Pflicht, die allerdings durch den Einsatz anderer Mittel abgewendet werden kann und zu einem solchen auch motivieren soll[9]; ein Beispiel hierfür wäre die Bestellung eines Jugendschutzbeauftragten nach § 7 JMStV, die durch den Anschluss an eine Selbstkontrollorganisation vermieden werden kann.

Die staatliche Tätigkeit verlagert sich beim Einsatz des Steuerungsmittels der Regulierten Selbstregulierung vom Eingriff in die private Tätigkeit hin zur ihrer Anregung und Überwachung,

1Rossen-Stadtfeld, AfP 2004, 1, 1.

2Rossen-Stadtfeld, AfP 2004, 1, 4; Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.302.

3Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.301.

4Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.302.

5Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.302.

6Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.302.

7Ladeur, Regulierung von Selbstregulierung, S.74.

8Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.302.

9Ladeur, Regulierung von Selbstregulierung, S.62.

von der Aufgabenerfüllung zur Gewährleistung der Aufgabenerfüllung; die Normsetzung rückt von direkter Steuerung ab und verlegt sich auf die Festsetzung von Zielen[1], die von den Selbstregulierungsgremien eigenverantwortlich umgesetzt werden sollen, wobei eine zumindest partielle Übereinstimmung ihrer Interessen mit den staatlichen Zielen gegeben sein muss. Diese Entwicklung lässt sich als Übergang vom „Eingriffsstaat“ zum „Gewährleistungsstaat“ beschreiben[2].

Die Selbstregulierungsgremien sind aufgrund beschränkter Umsetzungskompetenzen hinsichtlich der Durchsetzung ihrer Entscheidungen vom Staat abhängig[3]; andererseits besteht von Seiten des Staates eine freiwillige Bindung an die Entscheidungen der Selbstkontrolleinrichtungen, da diese über eine höhere Sachkunde und einen näheren praktischen Bezug zu den Problemen verfügen.

Die Entscheidungen der Freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) etwa, einem der ältesten Selbstregulierungsgremien, wurden vom Staat praktisch nie desavouiert, obgleich sie keinerlei Bindungswirkung haben konnten; eine verweigerte Freigabe kam geradezu einer an staatliche Stellen gerichteten Einladung zum Eingreifen gleich[4]. Ist die freiwillige staatliche Bindung an Entscheidungen der Privaten nicht vorhanden, droht die Regulierte Selbstregulierung zu scheitern[5]; eine funktionierende Regulierte Selbstregulierung wird also in der Regel nicht in Konflikte mit der Rechtsprechung geraten beziehungsweise darauf abzielen, derlei Konflikte zu vermeiden.

Dies kann dazu führen, dass Selbstregulierungsgremien gegenüber schwächeren Beteiligten tendenziell strenger vorgehen, als es von Seiten eines staatlichen Aufsichtsgremiums der Fall wäre, um Eingriffen nationaler Aufsicht vorzubeugen. Daher benötigen sie einen gewissen Spielraum gegenüber den staatlichen Regulierern, der auch gerichtlichen Überprüfungen standhalten muss, da andernfalls die Gefahr besteht, dass die Regulierten sich nicht dazu veranlasst sehen, sich einem Selbstregulierungsgremium zu unterwerfen, das für sie bei negativen Kostenfolgen letztlich keinen Vorteil gegenüber einer staatlichen Aufsicht bietet.

1Die Vorteile konditionaler gegenüber finaler Programmierung, wie sie im Übergang zur regulierten Selbstregulierung gesehen werden, beschreibt Luhmann, S.220f.

2Rossen-Stadtfeld, AfP 2004, 1, 2.

3Ladeur, Regulierung von Selbstregulierung, S.66.

4Ladeur, Regulierung von Selbstregulierung, S.65f.

5Ladeur, Regulierung von Selbstregulierung, S.65f.

4. Selbstregulierung

Im Unterschied zu den zuvor genannten Regulierungsmöglichkeiten ist die „rein private“ Selbstregulierung keinen anderen Regelungen als denen der allgemeinen Rechtsordnung unterworfen[1], wobei staatliche Interventionen dennoch im Bereich des Möglichen liegen[2].

Im Bereich des Internets sind es vor allem informelle Gremien, die nicht auf der Basis staatlich festgesetzter Vorgaben aktiv werden, beispielsweise die Standardisierungsorganisationen IAB und W3C oder auch einzelne private Verbände, welche die Einhaltung allgemein anerkannter Regeln (etwa die so genannte „Netiquette“) überwachen und deren Missachtung sanktionieren.

Die Ahndung von Verstößen kann durch die Einschaltung staatlicher Gerichte – auf Grund von Unterwerfungserklärungen – oder durch private Schiedsgerichte geschehen; davon abgesehen existieren diverse nicht-rechtsförmige Sanktionsmechanismen.

C. Inhaltliche Regulierung

Für den Nutzer des Internets haben inhaltliche Beschränkungen den eingreifendsten Charakter: Der Zugriff auf gewünschte Inhalte wird ihm verwehrt. Wegen ihrer Offensichtlichkeit erzielen sie häufig eine große Öffentlichkeitswirkung, was von Behörden und dem Gesetzgeber wohl auch geschätzt wird[3]. Allerdings sind sie, wie noch zu zeigen sein wird[4], technisch schwierig umzusetzen und können in vielen Fällen ohne großen technischen Aufwand umgangen werden. Das Verhältnis zwischen Aufwand und Ertrag ist also eher ungünstig. Inhaltliche Regulierungsmaßnahmen können – anders als Eingriffe in die technische Struktur des Internets – von nationalen Behörden angeordnet und für deren Staatsgebiet, soweit es die Struktur des Internets erlaubt, auch repressiv geahndet werden. Dabei ist es nicht nur möglich, gegen den Urheber der Inhalte vorzugehen, sondern auch gegen diejenigen, die für deren Übertragung oder Zugänglichkeit verantwortlich sind. Letztere sind in der Regel sowohl für den Staat als auch für private Schadensersatzforderungen die „besseren Verantwortlichen“, da durch einen Zugriff auf sie bereits weiteren Verletzungen vorgebeugt werden kann – in der Regel werden sie selbst versuchen, weiteren Eingriffen zu entgehen, indem sie die betreffenden Inhalte entfernen.

Ein Vorgehen gegen andere Verantwortliche als den Anbieter verbotener Inhalte ist häufig die einzige Erfolg versprechende Option, da der Anbieter sich nicht selten im Ausland befindet und der

---

1Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.303.

2Hoffmann-Riem, Öffentliches Recht und Privatrecht, S.303.

3Einigen Teilen des IuKDG wurde 1997 vorgeworfen, es handele sich um symbolische Gesetzgebung, die nur zeigen sollte, dass das Internet kein rechtsfreier Raum sei, den Regelungszweck aber nicht erreichen könne, so z.B. MdB Tauss, BT/PlPr. 13/170, S.15400.

4S.u. S.76ff.

Empfänger nicht immer zu finden ist[1]. Es verbleiben also diejenigen im staatlichen Einflussbereich, die technisch für die Verbreitung von Inhalten zuständig sind. Die Eingriffsmöglichkeiten der technisch Beteiligten werden jedoch durch die eingesetzte Technik der Datenübermittlung begrenzt, was wiederum die Mittel des Staates im Vergleich zu herkömmlichen Medien einschränkt. Generell unterscheiden sich die Möglichkeiten der Einflussnahme des Staates sowie der Verbreiter der Inhalte im Internet erheblich von jenen der Verleger und Rundfunkveranstalter: Ohne deren aktive Tätigkeit – und somit ohne Überprüfung der Inhalte – ist keine Veröffentlichung möglich. Im Internet üben Host- und Access-Provider die Rolle der Verbreiter von Inhalten aus; eine Kontrolle dieser Inhalte ist aufgrund der Struktur und Technik des Internets sehr schwierig und – wenn überhaupt – nur unter hohen Kosten zu realisieren. Dies ergibt sich bereits aus dem unterschiedlichen Ansatz hinsichtlich der Nutzung der Inhalte: Während beim Rundfunk und in der Presse die produzierten Inhalte vom Verleger verteilt bzw. vom Rundfunksender zentral ausgestrahlt werden, stellen Internet-Provider lediglich ihren Speicherplatz Dritten zur Verfügung. Dort werden Inhalte von diesen eigenständig gespeichert und können unmittelbar von Nutzern abgerufen werden. Eine Vorabkontrolle ist rein praktisch nicht möglich: Internet-Provider haben keine Kenntnis der von ihnen transportierten und von Nutzern abgerufenen Inhalte. Allein die riesige Datenmenge, die gespeichert wird, bringt es mit sich, dass eine Kontrolle durch Menschen undurchführbar und eine Kontrolle durch Maschinen zwar möglich, aber bestenfalls sehr fehleranfällig ist. Bei der Durchleitung von Daten kann die Kontrolle ebenfalls nur maschinell erfolgen; dies ist derzeit technisch nicht zuverlässig praktikabel und würde außerdem zu einer spürbaren Verlangsamung des Datenverkehrs führen. Sollten Daten zudem verschlüsselt sein, ist eine Kontrolle technisch ausgeschlossen[2].

Relevant geworden sind Eingriffe gegenüber radikalen Inhalten und im Bereich des Jugendschutzes. Eine Steuerungswirkung für Inhalte kann entweder durch spezialgesetzliche Verbote bzw. Beschränkungen oder durch die Regelung und Modifizierung allgemein bestehender Verantwortlichkeiten für Angebot, zugänglich Machen und Transport von Informationen erreicht werden. Spezialgesetzliche Regelungen existieren im Bereich des Jugendschutzes; dort sind allerdings nicht nur spezialgesetzliche Verbote von Inhalten, sondern auch kooperative Modelle der Rechtsdurchsetzung zu finden.

1Mit Ausnahme von kinder- und jugendpornografischen Inhalten ist der Konsum rechtswidriger Informationen in der Regel nicht verboten.

2Eine Verschlüsselung gilt als sicher, wenn sie nicht mit vertretbarem Zeitaufwand zu brechen ist; eine absolute Sicherheit kann es nicht geben. Wenn dieser unangemessene Zeitaufwand auch noch für eine Vielzahl von Dateien benötigt wird, ist eine Kontrolle unmöglich.

Aufgrund der technischen Gegebenheiten und um dem damals aufkeimenden E-Commerce eine solide rechtliche Grundlage zu geben[1], beschlossen 1997 der Bundestag das IuKDG[2] und die Länder den MDStV, welche am 18.01.2007 von Telemediengesetz (TMG) und RStV abgelöst wurden. Das TMG trat zum 01.03.2007 in Kraft[3].

I. Systematik der Haftungsregeln

Das TMG enthält, ebenso wie zuvor TDG und MDStV, keine Verantwortung begründenden Normen, sondern setzt eine Verantwortlichkeit nach anderen Vorschriften voraus, wobei nicht unterschieden wird, ob sich diese aus zivilrechtlichen, strafrechtlichen oder öffentlich-rechtlichen Normen ergibt. Sie gilt gleichermaßen für alle Rechtsgebiete. Die Regelungen des TMG schränken die nach den allgemeinen Vorschriften bestehende Verantwortlichkeit grundsätzlich ein, lassen allerdings unter bestimmten Voraussetzungen Ausnahmen gelten.

Haftungsbegründung

a. Haftung nach allgemeinen Gesetzen für eigene Informationen

Die Haftung für Inhalte folgt den allgemeinen Gesetzen des öffentlichen Rechts, des Zivil- und des Strafrechts: Wer rechtswidrige Informationen anbietet oder verbreitet, ist dafür auch verantwortlich. Diese Selbstverständlichkeit drückt § 7 I TMG aus. Allerdings kann auch derjenige nach denselben Normen verantwortlich sein, der sich Informationen Dritter zu eigen macht[4]. Ein Zu eigen Machen kann auch dann vorliegen, wenn der Anbieter die Inhalte als fremde kennzeichnet[5]: So gilt auch eine von einem Anbieter eröffnete und moderierte „Online-Community“, deren Eröffnung eine grobe Beschreibung von Themenbereichen voraussetzt, als eigenes Angebot des Anbieters[6]. Folge des Zu eigen Machens ist eine unbeschränkte Haftung nach § 7 I TMG.

b. Haftung nach allgemeinen Gesetzen für fremde Informationen

Wer an der Verbreitung fremder Informationen beteiligt ist, kann nach allgemeinen Gesetzen grundsätzlich zur Verantwortung gezogen werden[7]. Allerdings würde durch eine derartige Haftung insbesondere von Host- und Access-Providern Unmögliches, nämlich die präventive Überwachung aller gespeicherten Inhalte bzw. des Datenstroms, gefordert.

1BT Drs. 13/7385, S.16.

2BT Drs. 13/7385, S.16.

3BGBl. I 2007, S.251.

4BT-Drucksache 13/7385, S.19.

5OLG Köln, Urteil vom 28.5.2002, Az.: 15 U 221/01.

6OLG Köln, Urteil vom 28.5.2002, Az.: 15 U 221/01.

7 Vassilaki, MMR 1998, 634.

Dieser Ausgangslage hat der Gesetzgeber durch die Verantwortlichkeitsregelungen der §§ 7 ff. TMG Rechnung getragen. Das Ziel der Befreiung der Provider von der Verantwortlichkeit für das Handeln Dritter ist zumindest in Grundzügen eindeutig erkennbar. Die Haftungsbefreiungen decken tatbestandlich nahezu jede Möglichkeit des Umgangs mit rechtswidrigen fremden Informationen ab. In jedem Fall wird die Haftung für fremde Informationen akzessorisch zu einer Haftung des Erstellers der Informationen, sowohl hinsichtlich zivil- und strafrechtlicher als auch öffentlich-rechtlicher Normen.

c. Medienrechtliche Haftung

Auch für das Medienrecht gelten die grundsätzlichen Verantwortungsregeln[1]. Bei diesen ist allerdings zu beachten, dass eventuelle Verstöße üblicherweise einen Presse-, Kunst- oder Meinungsbezug haben und die allgemeinen Haftungsregeln deshalb im Lichte des Art. 5 GG zu lesen sind, was zu einer im Vergleich zu telemedienrechtlichen Regelungen weiter gehenden Einschränkung der Verantwortung führt. Da aber Sachverhalte, in denen neben den telemedienrechtlichen auch die medienrechtlichen Regelungen einschlägig sind, nach den letzteren behandelt werden, werden diese hier als Ausnahmen nicht berücksichtigt.

Einschränkung der Haftung

a. Telemediengesetz

Die Regelungen des TMG zur Verantwortlichkeit differenzieren jeweils danach, ob es sich bei den rechtswidrigen Informationen um eigene Inhalte desjenigen handelt, der sie bereithält, oder ob es sich um fremde Inhalte handelt. Unter bestimmten Voraussetzungen stuft die Rechtsprechung auch eigentlich fremde – also von anderen stammende – Inhalte als eigene ein, nämlich wenn derjenige sie sich zu eigen macht.

Neben den Verantwortlichkeitsregelungen enthält das TMG noch Direktiven zum Datenschutz in den §§ 11-15, welche die Datenschutzregelungen des MDStV und TDDSG zusammenführen.

Die Definitionen in den Vorschriften zur Verantwortlichkeit sind so konzipiert, dass sie alle Möglichkeiten der Tätigkeit im Zusammenhang mit der Datenübermittlung – d.h. Erstellen, Speichern und Durchleiten von Informationen – im Internet erfassen.

Die dogmatische Einordnung der Verantwortlichkeitsregelungen ist umstritten[2]. Ob diese als „Filter“ vor die eigentliche Normprüfung gesetzt werden[3], die einschlägigen Haftungsnormen auf der Tatbestandsebene modifizieren[4,] oder sie nach einer festgestellten Verantwortlichkeit

1Baumbach/Hefermehl, UWG, Einl. UWG Rn. 331.

2Der Streit und die Literatur dazu stammen noch aus der Zeit des TDG und MDStV. Da deren Wortlaut aber unverändert im TMG übernommen wurde, dürfte sich an den Standpunkten nichts geändert haben.

3 Reg. Beg. zu § 5 TDG a.F., BTDrs. 13/7385, S.14; Eberle/Rudolf/Wasserburg-Gersdorf, III. Rn. 249.

4 Spindler, MMR 1998, 639, 643.

ausschließen[1], kann hier dahingestellt bleiben; der Gesetzgeber wollte diesbezüglich keine Aussage treffen[2]. Relevant wird die Frage der Einordnung lediglich in strafrechtlichen Fällen der Beteiligung, wenn Beteiligten bestimmte Privilegierungsmerkmale nicht zugute kommen.

b. Rundfunkstaatsvertrag

Parallel zum TMG wurde der RStV geändert. In seinem sechsten Abschnitt finden sich Vorschriften für journalistisch-redaktionell gestaltete Inhalte. Außerdem enthält er in § 59 IV die aus dem MDStV übernommene Möglichkeit, gegenüber Providern die Sperrung fremder Inhalte, orientiert am Vorbild der Inanspruchnahme Nichtverantwortlicher aus den Polizeigesetzen der Länder, anzuordnen. Inhaltliche Anforderungen an Telemedien ergeben sich auf Grund des Verweises in § 1 IV TMG aus den §§ 54 ff RStV[3].

c. Jugendmedienschutzstaatsvertrag

Der Jugendmedienschutzstaatsvertrag (JMStV) ist im Bereich des Jugendmedienschutzes am 1. April 2003 in Kraft getreten und statuiert Pflichten für Provider. Nach dem JMStV ist zwischen verschiedenen Formen von jugendgefährdenden oder menschenverachtenden Angeboten zu unterscheiden. Je nach Art der Angebote sind diese entweder

- gänzlich unzulässig
- entwicklungsbeeinträchtigend oder
- unbedenklich.

Je nach Einordnung der Inhalte legt der JMStV verschiedene Verpflichtungen fest[4]. Des Weiteren enthält er, unabhängig von der konkreten Einstufung, in § 7 eine Pflicht zur Bestellung eines Jugendschutzbeauftragten.

Haftung und Verantwortung

Terminologisch fällt auf, dass die §§ 7-10 TMG von einer „Verantwortlichkeit“ der Anbieter sprechen, während die Literatur die gesetzlichen Regelungen in der Regel als „Haftungsnormen“ qualifiziert[5]. Mitunter werden die Begrifflichkeiten auch vermischt genutzt, ohne dass eine Differenzierung erkennbar wird.

---

1 Mayer, Öffentliches Recht, S.197.

2Sonst enthielte die Begründung eine andere als die mehr als vage Formulierung, dass die Regelungen „untechnisch als Filter zu verstehen“ seien.

3Rundfunkstaatsvertrag vom 31.08.1991, Gbl. BW 2007, S.111.

4Zu den einzelnen Pflichten: s.u. S.87ff.

5Z.B. Köhler/Arndt, S. 230; Hoeren, Internetrecht, S. 273, noch zum TDG und MDStV, diese Regelungen wurden aber in ihrem Wortlaut nicht verändert.

Es wäre denkbar, dass der Gesetzgeber mit der gewählten Terminologie lediglich eine Freistellung von öffentlich-rechtlichen sowie strafrechtlichen Verantwortlichkeitsregelungen erreichen, die zivilrechtlichen Haftungsnormen aber unberührt lassen wollte. Dem steht entgegen, dass die Verantwortlichkeitsregelungen des TMG als „Querschnittsnormen" fungieren sollen, die sowohl die zivilrechtlichen Haftungsnormen als auch die straf- und öffentlich-rechtliche[1] Verantwortlichkeit modifizieren[2] - anders ließe sich das Ziel der Rechtssicherheit für Anbieter nicht erreichen. Verantwortlichkeit und Haftung werden dementsprechend weitgehend gleichbedeutend verwendet. Für die Anwendbarkeit der Haftungsregeln des TMG muss aber zunächst eine Verantwortlichkeit nach generellen Regeln bestehen.

II. Verantwortlichkeit für Inhalte

Grundsätzlich spielt es für die Publikation von Inhalten rechtlich keine Rolle, ob diese im Internet, auf Papier oder per Rundfunk verbreitet werden. Diesem Grundsatz folgen auch die Verantwortlichkeitsregelungen. Die volle Verantwortlichkeit trägt derjenige, der die Inhalte erstellt hat. Andere Beteiligte haften nur unter bestimmten Umständen.

1. Entwicklung der Inhaltsregulierung

Der oben beschriebene zweite Ansatz – das Vorgehen gegen illegale Inhalte aufgrund bestehender Vorschriften – war 1996 die erste Reaktion deutscher Behörden. Radikale Inhalte waren dabei, zusammen mit pornographischen Inhalten, als erste von der gewachsenen Aufmerksamkeit der Öffentlichkeit und Behörden gegenüber dem Internet betroffen. Dies führte 1996 zu der Auszahlungsverfügung des BKA gegen den niederländischen Provider XS4ALL, auf dessen Server sich die Seiten der in Deutschland verbotenen, linksextremistischen Zeitschrift „Radikal" befanden, darunter auch eine Ausgabe mit wohl strafbarem Inhalt. Den deutschen Access-Providern wurde vom BKA aufgegeben, den Zugang zu den Servern von XS4ALL zu sperren[3].

Im Jahre 2002 wurde vom Regierungspräsidenten Düsseldorf eine Sperrungsanordnung gegenüber den nordrhein-westfälischen Access-Providern für die Seiten „http://www.neonazi-lauck.nsdapao.com" und http://www.stormfront.org" erlassen. Die Sperrungsverfügung sollte nicht nur die betroffenen Seiten unerreichbar machen, sondern auch an die Provider appellieren, eigenständig gegen rechtswidrige Inhalte vorzugehen, um weiteren behördlichen Eingriffen zuvorzukommen.

1Zimmermann, NJW 1999, 3145, 3148 hält die Regelungen von TDG und MDStV für nicht auf das Polizeirecht anwendbar.

2BT Drs. 13/7385, S.14.

3Zu den Vorgängen: Schulzki-Haddouti, abrufbar unter:
http://www.heise.de/tp/r4/artikel/1/1388/1.html.

Inzwischen liegt der Schwerpunkt des Vorgehens, wie zahlreiche Urteile zeigen, im Bereich der privaten Rechtsdurchsetzung hauptsächlich bei urheberrechtswidrigen und Markenrechte verletzenden Inhalten.

2. Persönlicher Anwendungsbereich

Für Rechtsverletzungen durch Kommunikationsinhalte sind in der Regel, abgesehen vom für die rechtsverletzenden Inhalte Verantwortlichen, andere Beteiligte notwendig[1]. In der Presse sind dies Verleger und Händler, im Rundfunk die Sender und die Betreiber der Sendeinfrastruktur (Kabelnetz, Satelliten, terrestrische Sendeanlagen). Im Bereich des Internets handelt es sich um Host-Provider, Access-Provider sowie andere Betreiber der Netzwerkinfrastruktur. Während in der Regel Content- und Host-Provider als „Sender" fungieren, stehen ihnen Access-Provider und Nutzer als Empfänger der Inhalte gegenüber.

Voraussetzung für die Anwendung der Verantwortlichkeitsregelungen des TMG ist, dass die Betroffenen einen Tele- oder Mediendienst anbieten. Die Definition eines Tele- bzw. Mediendienstes richtet sich nach § 1 TMG. Ausdrücklich nicht anwendbar ist das TMG nach § 1 IV auf Telekommunikationsvorgänge; für diese besteht nach dem TKG keine Privilegierung für die Verantwortlichkeit für Rechtsverletzungen durch Dritte. Allerdings ist eine Verantwortlichkeit wohl wegen Unzumutbarkeit bzw. Unmöglichkeit einer Kontrolle ausgeschlossen.

a. Geltung für Host - und Content-Provider

Content- und Host-Provider gehören nach § 1 I TMG unstrittig zu den Telemedienanbietern; das Regelwerk ist somit auf sie anwendbar[2].

b. Geltung für Access-Provider

Fraglich ist die Geltung des TMG in Hinsicht auf Access-Provider, deren Tätigkeit sich auf die Durchleitung von Informationen in Telekommunikationsnetzen beschränkt, was nach § 3 Nr. 24, 25 TKG eine Telekommunikationsdienstleistung darstellt. Das Angebot von Telekommunikationsdienstleistungen unterliegt jedoch nach § 1 III TMG nicht den Regelungen des TMG, sondern lediglich den Regelungen des TKG.

1In seltenen Ausnahmefällen ist der für die Inhalte Verantwortliche auch Host-Provider, dann sind keine weiteren Beteiligten für Verletzungen notwendig.

2Determann, S.522, hält das TDG a.F. auch nicht für auf „Service-Provider" anwendbar, ohne aber diese ansonsten ungebräuchliche Kategorie näher zu erläutern. Damit könnten auch Host-Provider gemeint sein.

(1.) Meinungsstand vor der Novellierung 2002

(a.) Access-Provider als Telekommunikationsanbieter

Nach einer Meinung gelten Access-Provider als bloße Telekommunikationsanbieter, da sie letztendlich nur Daten transportieren und keinerlei Einsicht in diese haben. Um von ihnen als von Telediensten sprechen zu können, müsse Nutzern durch die Tätigkeit der Access-Provider ein Kommunikationsmehrwert bleiben[1]. Den Zugangsvermittlern sei es allenfalls möglich, bestimmte Zugänge zu sperren, dies stelle an sich aber noch keinen Mehrwert dar. Daher seien nach der Definition des § 2 IV TDG a.F. handele es sich nicht um Teledienste[2]. Als Telekommunikationsdienstleistung habe nicht nur eine Durchleitung von Daten, sondern auch der Betrieb von Gateways, „Servern" und Routern zu gelten[3]. Nach dieser Ansicht stellen Teledienste nur Angebote zur Nutzung von einzelnen Diensten und nicht Angebote zur Nutzung des gesamten Netzes dar[4].

Auch das AG München ging in dem zu Recht viel kritisierten „Compuserve"- Urteil[5] davon aus, dass es sich beim Angebot der Compuserve GmbH nicht um einen Teledienst handele, allerdings nur da diese „keine eigenen Kunden" habe und nur indirekt den „Zugang zum Netz" über die amerikanische Muttergesellschaft verschaffe. Diese Ansicht ließ sich jedoch nicht in Übereinstimmung mit § 5 TDG a.F. bringen und wurde deshalb abgelehnt[6].

(b.) Access-Provider als Teledienstanbieter

Nach einer zweiten Ansicht werden Access-Provider entweder pauschal für ihre gesamte Tätigkeit als Teledienstanbieter gewertet[7] oder es wird zwischen Telekommunikationsdienstleistungen und Telediensten differenziert[8]; beides führt zu einer Anwendung des TDG.

Zwar böten Access- Provider auch Telekommunikationsdienstleistungen an, da nach § 2 I TDG Telediensten die Übermittlung der Daten mittels Telekommunikation zugrunde liegt; der nach außen hin einheitliche Vorgang der Zugangsvermittlung lasse sich aber in einen Telekommunikationsteil – den Transport der Daten vom Endnutzer zum Zugangsserver des Providers – und einen Teledienstteil – die Verarbeitung der Daten auf dem Zugangsserver und die Weiterleitung an einen Router bzw. DNS-Server – aufspalten[9]. Die Anwendung des TKG für die bloße Datenübermittlung

1 U.a. Popp, Strafrechtliche Verantwortlichkeit von Internet-Providern, S.58.

2Germann, Gefahrenabwehr und Strafverfolgung im Internet, S. 167f., Determann, S.522.

3Determann, S.522.

4Determann, S.522.

5AG München, MMR 1998, S.429ff.

6 Statt **V**ieler: Sieber, Beilage zu MMR 2/99 (Nachweise in Rn.167).

7Kröger/Moos AfP 1997, 675, 678f.; Hoeren, Internetrecht, S.279.

8Engel-Flechsig/Maennel/Tettenborn, § 2 TDG Rn. 77, so wohl auch Dietz/Richter, CR 1998, 528, 530.

9Engel-Flechsig/Maennel/Tettenborn, § 2 TDG Rn. 77, so wohl auch Dietz/Richter, CR 1998, 528, 530, die sich aber in erster Linie mit telekommunikationsrechtlichen Fragen befassen.

und des TDG für den Teledienstteil sei durchaus möglich. Dafür spreche der Begriff der „Zugangsvermittlung zu fremden Telediensten“. Auch die Gesetzesbegründung[1] lasse erkennen, dass Access-Providern das Haftungsprivileg des § 5 III TDG a.F. zu gute kommen solle. Die Gesetzesbegründung spreche statt von „Zugangsvermittlung“ von „Durchleitung von Informationen“, was die Tätigkeit eines Access-Providers beschreibe und nicht das von der ersten Ansicht als „Zugangsvermittlung“ beschriebene Setzen von Links. Auch § 18 III MDStV a.F.[2] hätte wenig Sinn, wenn nicht auch Access-Provider vom Anwendungsbereich des TDG umfasst wären und nicht als reine Telekommunikationsdienstleister gälten

(2.) Meinungsstand nach der Novellierung

Durch die Novellierung des TDG und des MDStV hatten sich die ursprünglich weitgehend inhaltsgleich formulierten Gesetze auseinander entwickelt. Es wurde aber auch in den den jeweiligen § 5 ersetzenden §§ 8-11 TDG bzw. §§ 6-9 MDStV die Verantwortlichkeit detaillierter geregelt. Diese sind inhaltlich identisch als §§ 7-10 in das TMG übernommen worden.

Bei der Novellierung von TDG und MDStV wurde entsprechend der E-Commerce-Richtlinie (ECRL)[3] der Begriff des „Zugang Vermittelns“ durch den des „Übermittelns von Informationen“ ergänzt, so dass nunmehr eindeutig erkennbar ist, dass der Gesetzgeber Access-Provider als Teledienst-Anbieter einstuft.

Dennoch führt die Wertung der Access-Provider zu einem Problem im Zusammenhang mit dem

Datenschutz. Im TMG wurden in den §§ 12 ff**.** die Datenschutzregelungen des TDDSG und des MDStV eingearbeitet; diese sind allerdings nicht identisch mit denen des Telekommunikationsrechts.

Werden Access-Provider nun für einen Teil ihrer Tätigkeit als Telekommunikationsdienstleister, für einen anderen Teil als Teledienstanbieter gesehen, unterliegen sie beiden Regelungen. Das ist zum einen unnötig kompliziert, zum anderen müssen dieselben Daten nach unterschiedlichen Vorgaben gehandhabt werden, was datenschutzrechtlich sicher nicht optimal ist. Dennoch steht der Wortlaut des § 1 TMG einer anderen Beurteilung im Wege.

---

1 BT Drs. 13/7385, S.14.

2Heute § 59 IV RStV. Danach können Teledienstanbieter verpflichtet werden, den Zugang zu bestimmten Angeboten quasi als Nicht-Störer zu sperren. Wenn aber Access-Provider keine Teledienste anbieten würden, könnte niemand verpflichtet werden, der Anwendungsbereich wäre allenfalls minimal.

3Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABlEG Nr. L 178 v. 17.07.2000.

3. Haftung der Beteiligten nach TMG

Nach § 7 I TMG trifft die volle Verantwortlichkeit denjenigen, der eigene rechtswidrige Informationen bereit stellt. Verantwortlichkeit meint das Einstehen müssen für eigenes Verschulden[1].

Diese Selbstverständlichkeit ist rein deklaratorisch und bedarf keiner näheren Erläuterung. Die Regelung des § 7 I TMG betrifft ausschließlich Content-Provider.

Informationen gelten als eigene, wenn der Anbieter sie selbst hergestellt oder sich fremde Informationen zu eigen gemacht hat[2]. Andere Beteiligte an der Datenübertragung können auch an fremden Rechtsverletzungen beteiligt sein, profitieren allerdings von weitreichenden Haftungsfreistellungen.

Die Haftung für fremde Inhalte ist privilegiert gegenüber herkömmlichen Gesetzen. Der Umfang der Privilegierung knüpft an die jeweilige Tätigkeit des Beteiligten an.

a. Haftungsfreistellung für Access-Provider

Nach § 8 I TMG ist derjenige, der Informationen ausschließlich durchleitet, für diese grundsätzlich nicht verantwortlich. Der durch die Neufassung des TDG und MDStV in das Gesetz gekommene und in das TMG übernommene Tatbestand des „Durchleitens“ ersetzt den des „Zugang Vermittelns“ des § 5 III TDG a.F. Damit ist geklärt, dass Access-Provider in den Anwendungsbereich des TMG fallen.

Eine Ausnahme von der Privilegierung besteht nach § 8 I TMG, wenn der Access-Provider die Informationen verändert oder auswählt, die Adressaten aussucht oder die Übermittlung veranlasst hat; letzteres dürfte nur für so genannte Push-Dienste gelten, bei denen die Anbieter den Nutzer wie im Rundfunk mit eigens ausgewählten Angeboten beliefern[3]. Diese Ausnahmen sind insofern zwingend, als der Anbieter in diesen Fällen zumindest Kenntnis von den Inhalten haben und deren Übermittlung ohne größeren Aufwand unterbinden könnte. Eine Privilegierung ist daher in derartigen Fällen nicht geboten.

Des Weiteren ist fraglich, ob Anbieter von Suchmaschinen sowie Content-Provider, deren eigene Angebote Links auf fremde Angebote enthalten, ebenfalls nach § 8 TMG privilegiert sind[4].

Im Übrigen sind Access-Provider nach § 8 II TMG auch für notwendigerweise während der Datenübermittlung entstehende Kopien von der Verantwortlichkeit für Inhalte befreit, soweit diese nur kurzfristig gespeichert werden und nicht für andere zugänglich sind. Für diese Kopien kann der

---

1 Amtl. Begr. zu § 5 I TDG a.F. BTDrs 13/7385, S.14.

2 Eberle/Rudolf/Wasserburg-Gersdorf, III. Rn. 256.

3 A.A. Spindler, NJW 2002, 921, 923 mit dem Argument, dass der Nutzer generell in die Zusendung eingewilligt und ein Profil erstellt habe. Es kann aber bei der Frage der Haftungsbefreiung des Providers nur um die konkreten Informationen und deren Rechtswidrigkeit gehen, und die konkreten Informationen hat nicht der Nutzer ausgewählt, sondern der Provider.

4 S.u. S.58ff.

Access-Provider nicht verantwortlich sein, da sie – anders als beim Caching – bei einer Datenübertragung notwendigerweise[1] und unabhängig von seinem Willen entstehen. Die Speicherung darf „nicht länger, als für die Übertragung üblicherweise erforderlich ist“ andauern; diese sehr auslegungsfähige Zeitdauer dürfte sich in der Praxis auf den Millisekundenbereich beziehen.

b. Haftungsfreistellung für Betreiber von Cache-Servern

Noch weitergehender ist der Ausschluss, wenn die Speicherung nur zwischenzeitlich erfolgt. Dies ist bei den Zwischenkopien während einer Übermittlung sowie beim so genannten Caching der Fall. Caching bedeutet das Zwischenspeichern von häufig nachgefragten Informationen auf einem speziellen Server des Access-Providers oder an anderen Stellen[2]. Die Informationen werden dabei nur eine bestimmte Zeit vorgehalten. Es wird von allen Access-Providern betrieben, um einerseits ökonomischer mit der knappen Ressource „Bandbreite“ zu wirtschaften[3] und andererseits die eigenen Kosten zu reduzieren, da nicht jeder Seitenaufruf zu einer (in der Regel für den Provider kostenpflichtigen) Inanspruchnahme von zusätzlichen Leitungskapazitäten führt. Dabei kann es dazu kommen, dass, wenn Nutzer rechtswidrige Inhalte aufrufen, diese auch im Cache gespeichert werden und der Access-Provider – ohne es im konkreten Fall zu wollen – zum Host-Provider unzulässiger Inhalte wird. So können durch das Caching auch längst vom ursprünglichen Speicherort gelöschte Inhalte noch zugänglich bleiben. In diesen Fällen ist der Anbieter nach § 9 TMG nicht verantwortlich.

Die Privilegierung gilt nach § 9 TMG nur, wenn der Provider nicht absichtlich bestimmte Informationen speichert und die Aktualisierungszeit sich im Rahmen von „weithin anerkannten Industriestandards“ hält. Eine Präzisierung dieser zeitlichen Angabe wäre durchaus möglich und auch wünschenswert gewesen[4]. Die gewöhnliche Zeit des Cachings beträgt einige Stunden; eine Steuerung der Speicherdauer durch Webseiten ist technisch möglich. Daher dürfte es keinen Industriestandard geben.

Der Provider muss des Weiteren „die Bedingungen für den Zugang zu den Informationen beachten“ und darf „die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen“.

1Der Router muss die ankommenden Pakete zunächst in seinem Arbeitsspeicher speichern, bevor er sie an die vorgesehene Adresse weiterleiten kann.

2Google etwa funktioniert im Prinzip wie ein großer Cache-Speicher, bietet als Suchmaschine allerdings weit über die üblichen Funktionen hinausgehende Möglichkeiten.

3 Pankoke, S.194.

4So auch Wenzel, S.639.

c. Haftungsfreistellung für Gateway- und Router-Betreiber

Bei jedem Datentransfer von einem Netzwerk in ein anderes entstehen auf dem jeweiligen Gateway Kopien der übertragenen Daten. Eine Datenübertragung – und damit eine mögliche Rechtsverletzung – wäre ohne die kurzfristige Zwischenspeicherung der Daten auf Gateways und Routern nicht möglich, so dass sich hier eine andere Möglichkeit der akzessorischen Haftung für eine rechtswidrige Tätigkeit Dritter böte.

Für derlei Fälle der Zwischenspeicherung enthält § 8 II TMG eine Privilegierung: Diese gilt für notwendigerweise während der Datenübertragung entstehende Kopien von Inhalten, soweit diese nur kurzfristig abgespeichert und nicht für andere zugänglich sind. Der Server-Betreiber kann für sie nicht verantwortlich sein, da sie technisch erforderlich sind und unabhängig von seinem Willen entstehen.

Ohne diese Zwischenspeicherung wäre eine Datenübertragung mit Routern nicht möglich[1]. Zeitlich darf die Speicherung „nicht länger als für die Übertragung üblicherweise erforderlich ist“ erfolgen. Diese Zeit dürfte sich in der Praxis auf den Millisekundenbereich beschränken.

d. Haftungsfreistellung für die Speicherung von Informationen

Derjenige, der Dritten Speicherplatz für Informationen zur Verfügung stellt, sorgt technisch dafür, dass diese Informationen abgerufen und verbreitet werden können und leistet somit einen kausalen Beitrag zu Rechtsverletzungen. Hieraus ergibt sich ein Anknüpfungspunkt für eine mögliche zivil- oder strafrechtliche Haftung, auch eine Verantwortlichkeit als Handlungs- oder Zustandsstörer ist denkbar.

(1.) Grundsätzliche Privilegierung

Da eine Überwachung fremder Informationen aufgrund der Menge und der häufigen Änderungen derselben technisch unmöglich ist[2], besteht für Host-Provider eine weitgehende Privilegierung: Sie sind nach § 7 II TMG von einer Pflicht zur Überwachung der auf ihren Servern gespeicherten Informationen beziehungsweise nach § 10 TMG grundsätzlich von der Verantwortung für fremde Informationen, die sich auf ihrem Speicherplatz befinden, befreit. Allerdings existieren zahlreiche Ausnahmen von dieser prinzipiell weit reichenden Regel.

(2.) Ausnahmen von der Privilegierung

Host-Provider haften für rechtswidrige fremde Informationen, die sich auf ihren Servern befinden, nach § 10 TMG nur, wenn sie positive Kenntnis[3] von rechtswidrigen Handlungen Dritter haben.

1Der Router muss die ankommenden Pakete zunächst in seinem Arbeitsspeicher speichern, um feststellen zu können, an welche Adresse er die Pakete weiterzuleiten hat, bevor er sie an die vorgesehene Adresse weiterleiten kann.

2Eine derartige Überwachung wäre angesichts der großen Mengen allenfalls durch den Einsatz von Software möglich, diese könnte aber nicht zu 100% zuverlässig arbeiten; eine Überwachung durch Menschen würde zwangsläufig an unvertretbaren Kosten scheitern.

3Hoeren, Access-Provider, S.646, insoweit besteht noch Einigkeit.

Eine andere Regelung gilt bei Schadensersatzansprüchen nach § 10 Nr. 1 2. Hs. TMG. Danach genügt „Kenntnis von den Umständen [...], aus denen die rechtswidrige Information oder Handlung offensichtlich wird“ (Nr.1) für die Begründung von Schadensersatzansprüchen. Deshalb ist im Folgenden zwischen Voraussetzungen für die Privilegierung bei Schadensersatzansprüchen und für andere Ansprüche zu differenzieren.

Damit gilt auch in Deutschland das so genannte „Notice-and-take-down“-Verfahren[1], das allerdings nur eine unklare gesetzliche Ausformung erhalten hat. Strittig ist insbesondere,

- ob der Provider positive Kenntnis des Inhalts oder Kenntnis der Rechtswidrigkeit haben muss und
- ob positive Kenntnis der Rechtswidrigkeit oder eine bloße Behauptung der Rechtswidrigkeit vorliegen muss.

Im Falle von Schadensersatzansprüchen ist fraglich, welcher Grad der Kenntnis vorliegen muss. Ferner ergeben sich insbesondere bei Links Fragen der Abgrenzung von fremden und eigenen Inhalten.

(a.) Weitgehende Privilegierung

Zweck des IuKDG – und damit auch des TDG und MDStV – war die Schaffung von Rechtssicherheit für das sich 1997 langsam entwickelnde Geschäftsfeld des e-Commerce in Deutschland[2]. Neben diesen kommerziellen Gesichtspunkten sind grundrechtliche Aspekte, namentlich die Kommunikationsfreiheiten, zu beachten. Eine weitgehende Privilegierung der technischen Beteiligten an der Datenübertragung dient diesen Zielen am besten. Demnach besteht eine Haftung für Host-Provider nur, wenn sie durch ein Anerkenntnis ihres Kunden oder ein Urteil bzw. eine einstweilige Verfügung positive Kenntnis der Rechtswidrigkeit haben. Es kann auch nicht sein, dass diejenigen, die lediglich Speicherplatz anbieten, zu privaten Schiedsrichtern werden und auf Grund unklar vorgetragener Behauptungen entscheiden müssen, ob Inhalte rechtmäßig oder rechtswidrig sind. Für Entscheidungen von Privaten können keine geringeren Anforderungen an die vorzutragenden Tatsachen gestellt werden als es für den gerichtlichen Vortrag der Fall, vielmehr müssen die Anforderungen höher sein, da der Provider ansonsten bei unrechtmäßigen Sperrungen von Inhalten einen Vertragsverstoß gegenüber seinem Kunden begehen würde. Die Sperrung beim Provider kann daher nur ultima ratio sein oder nur in sehr klaren Fällen gefordert werden, ansonsten muss sich der Verletzte an den Eigentümer der rechtswidrigen Inhalte halten.

1Holznagel, Selbstregulierung, S.97.

2So auch weiterhin die Begründung zur TDG-Novelle 2002, BTDrs. 14/6098, S.11.

Im Falle von Schadensersatzansprüchen muss positive Kenntnis der Rechtswidrigkeit und nicht nur bloße Kenntnis der Inhalte oder eine reine Behauptung der Rechtswidrigkeit der Inhalte vorliegen. Andernfalls würde das Risiko der Bereitstellung rechtswidriger Inhalte bzw. der falschen Behauptung der Rechtswidrigkeit von Inhalten von den Schädigern und Geschädigten auf den eigentlich unbeteiligten Provider verlagert.

Mit dem Ziel der Förderung des elektronischen Geschäftsverkehrs sowie innovativer Geschäftsmodelle ist es nicht zu vereinbaren, diejenigen, die bloß Speicherplatz auf Servern bereitstellen bzw. Datenverkehr zwischen Dritten auf ihren Leitungen und Gateways durchleiten, für die Rechtsverletzungen Dritter haften zu lassen, sofern sie die Rechtsverletzungen nicht in besonderer Art und Weise gefördert haben. Eine derartige Haftung würde dazu führen, dass angesichts hoher Streitwerte die Provider eine größere Neigung zeigen dürften, behauptet rechtswidrige Angebote „vom Netz zu nehmen“, als sie erreichbar zu belassen. Hieraus würde ein erheblicher Schaden für das Image des jeweiligen Betroffenen, wenn nicht gar das Scheiterns seines – womöglich rechtmäßigen – Geschäftsmodells resultieren, was für die Ausschaltung unliebsamer Konkurrenten im Internet ausgenutzt werden werden könnte[1]. Die Provider befänden sich bei einer weitgehenden Haftung also in der misslichen Lage, entweder mit Schadensersatzansprüchen ihrer Kunden oder der Verletzten konfrontiert zu werden. Bei geringen Anforderungen an die Kenntnis von Rechtsverstößen müssten sie sich aus wirtschaftlichen Gründen nahezu zwangsläufig gegen die Interessen ihrer Kunden und für die Interessen der Verletzten entscheiden. Eine Beurteilung der Rechtslage ist, insbesondere bei urheber- und markenrechtlichen Streitigkeiten, für Außenstehende nur selten möglich. Der Provider würde sozusagen zum unbezahlten Hilfsrichter mit persönlicher Haftung.

Des Weiteren ist zu beachten, dass eine Haftung der Provider nicht nur der effektiven Rechtsdurchsetzung dient, sondern auch vom Gedanken der Schaffung zahlungsfähiger Haftender geleitet sein kann[2]. Letzteres kann jedoch kein schützenswertes Interesse darstellen. Der Interessenausgleich und die Frage der Klärung der Rechtswidrigkeit würden letztendlich auf das Verhältnis zwischen dem Provider und seinem Kunden in einem möglicherweise nachfolgenden zivilrechtlichen Verfahren abgewälzt. Auch dies liegt keinesfalls im Interesse der Schaffung von Rechtssicherheit für alle Beteiligten.

(b.) Strittige Fragen

Unklar bleibt auch nach der Gesetzesbegründung, ob

- einfache Kenntnis der Inhalte

1Die internationalen Regelungen über Domainstreitigkeiten sehen differenziertere Lösungsansätze vor, s.u. S.191ff. Auch das deutsche Recht erlaubt nicht die einfache Entziehung von rechtswidrigen Domains, s.u. S.182ff.

2So möglicherweise der Fall biedenkopf.de, bei dem nicht der Inhaber der Domain, sondern die DENIC e.G. verklagt wurde.

- substantiierte Behauptung der Rechtswidrigkeit durch den Verletzten oder
- positive Kenntnis der Rechtswidrigkeit

gefordert ist. Diese Frage ist insbesondere für die Funktion des Internets als freies Kommunikationsmedium wichtig.

Die erste Auslegung würde den Host-Providern die Überprüfung der Rechtswidrigkeit auferlegen, die zweite sie mit einem Haftungsrisiko zurücklassen, während die dritte dem Verletzten unter Umständen einen großen Aufwand abverlangen würde, um die Rechtsverletzung zu beenden, falls der Urheber nicht auffindbar sein sollte.

(c.) Kenntnis des Inhalts

Nach einer vor allem von der Rechtsprechung zu § 5 TDG a.F. vertretenen Auffassung genügt die bloße Kenntnis, dass sich bestimmtes Material auf den Servern des Providers befand.

Zwei Entscheidungen des LG München I zu § 5 II TDG a.F. hielten eine solche Kenntnis des Host-Providers für ausreichend[1]. Zu einer identischen Ansicht gelangt das LG Köln[2] in einem Urteil über die Haftung eines Forenbetreibers. Dieser veröffentlichte Kleinanzeigen und machte sie erst nach einer Freischaltung zugänglich. Dem LG Köln genügte für die Haftung, dass er damit Kenntnis von der Existenz einer Anzeige hatte, die sich als rechtswidrig herausstellte[3]. Auch der BGH hat in einer der ersten Entscheidungen zu § 5 II TDG a.F. auf die Kenntnis des Inhalts abgestellt[4].

Der Wortlaut des vormaligen § 5 II TDG a.F. wurde jedoch geändert, so dass § 10 TMG nunmehr „Kenntnis der rechtswidrigen Handlung oder der Information“ fordert. Trotzdem wird teilweise davon ausgegangen, dass ebenso wie bei § 5 TDG a.F. die Kenntnis der Information ohne Kenntnis über deren Rechtswidrigkeit genügen soll[5]. Nach einer anderen Meinung soll nur noch Kenntnis der Rechtswidrigkeit der Handlung und Information zu einer Haftung führen[6].

Die erste Auffassung verdient in Anbetracht des Hintergrundes und Zweckes des luKDG Kritik: Das luKDG sollte die Entwicklung und die Nutzung des Internets zu kommerziellen Zwecken in Deutschland fördern. Diesem Ziel ist nicht gedient, wenn sekundär Verantwortlichen, die eine wesentliche Rolle für die Entwicklung des E-Commerce spielen, eine Haftung auferlegt wird, wenn ihre Vertragspartner illegale Inhalte auf ihren Servern ablegen. Zwar sind die sekundär Verantwortlichen für diejenigen, in deren Rechte eingegriffen wurde, leichter zu erreichen, jedoch

1 LG München I, Az.: 7 O 3625/98; LG München I, Urteil vom 30.03.2000 7 O 3625/98.

2LG Köln MMR 2004, 183, 183.

3LG Köln MMR 2004, 183, 184.

4BGH MMR 2004, 166, 167.

5Kröger/Gimmy-Müller-Terpitz, S.573; Härting CR 2001, 271, 276.

6Spindler, NJW 2002, 921, 924; Wenzel, S.636f.

sind im Bereich des Internetrechts noch so viele Fragen ungeklärt und auch in der Rechtsprechung umstritten, dass einem Provider nicht zugemutet werden kann, die häufig mehrere Terabyte umfassenden Datenspeicher rechtlich zu bewerten, auch wenn nur ein Promillebereich der Angebote rechtlich bedenklich ist. § 7 II TMG stellt gerade aufgrund der Unmöglichkeit der Überwachung klar, dass keine Überwachungspflicht besteht.

Allerdings wird für die Kenntniserlangung bereits die Kenntnis eines „Wissensvertreters“ nach § 166 BGB für ausreichend gehalten[1]. Solange es sich bei diesem ausschließlich um eine Person mit einer gewissen rechtlichen Schulung, wie sie etwa Jugendschutzbeauftragte besitzen sollten, handelt, ist dies noch akzeptabel. Wenn jedoch die Kenntnis von „Scouts“ für ausreichend gehalten wird, dürfte eine schnell vorzunehmende Bewertung angesichts der Komplexität der Materie und der nicht immer eindeutigen Rechtsprechung nicht nur oberflächlich geschultes Personal, sondern auch die Mehrzahl der Juristen überfordern. Eindeutig rechtswidrige Informationen gibt es eigentlich nur bei Verletzungen der Menschenwürde, Schmähkritik, Formalbeleidigungen und rechtsradikaler Propaganda. Des Weiteren ist – besonders im Urheberrecht, auf das ein großer Teil der Fälle der zurückgeht – für den Provider in der Regel nicht zu klären, ob die angebotenen Inhalte lizensiert sind oder der Anbieter sie sonst berechtigt nutzt. Im Sinne der Rechtseinheit wäre es jedenfalls nicht, wenn sich die Maßstäbe verschiedener Rechtsgebiete auseinander entwickelten: Eine Folge dieser Auffassung wäre eine „willful blindness“, durch die sich der Provider nach der Rechtsprechung einiger Gerichte neuen Haftungsrisiken ausgesetzt sähe[2], und die auch für die Verletzten abträglich wäre: Eindeutigen Rechtsverletzungen könnte nicht mehr ohne Beschwerde abgeholfen werden, da der Provider voraussichtlich keine Anstrengungen mehr unternehmen wird, seinen Datenbestand auch nur oberflächlich zu kontrollieren. Der beabsichtigte Schutz der Betroffenen führte somit zu einem Ansteigen der Rechtsverletzungen, weil einer Kontrolle das Risiko der Haftung innewohnt[3]. Das Resultat bestünde nicht in gewonnener Rechtssicherheit oder Förderung des E-Commerce, sondern nur im Löschen auf Verdacht von möglicherweise rechtlich bedenklichen aber nicht zwangsläufig illegalen Inhalten[4]. Es liegt außerdem eine gewisse Missbrauchsgefahr vor, wenn der für eine Sperrung erforderliche Aufwand gering, der durch ein Unterlassen drohende Schaden aber hoch ist[5]. Dass diese Gefahr durchaus real ist, hat eine Studie in

1LG München I, NJW 2000, 2214, 2216; Kröger/Gimmy-Müller-Terpitz, S.568.

2Christiansen, MMR 2004, 185, 185. Wenig hilfreich ist auch der Hinweis von Hoeren, Access-Provider, dass der Host-Provider vorsichtshalber fragliche Inhalte einfach sperren sollte. Das TMG und seine Vorläufer TDG und MDStV sollten genau diese Rechtsunklarheit beseitigen.

3Christiansen, MMR 2004, 185, 185.

4So auch Mayer, Öffentliches Recht, S.210.

5Gerade im Bereich kommerzieller Inhalte könnte die Versuchung bestehen, um Mitbewerbern zu schaden oder kritische Informationen zu unterdrücken.

England belegt[1]. Auch in Deutschland wurde ein Access-Provider durch eine einstweilige Verfügung unter Hinweis auf eine angebliche Rechtsverletzung dazu verpflichtet, den Zugang zu bestimmten Angeboten zu unterbinden[2]. Dabei darf auch nicht aus den Augen verloren werden, dass die primäre Verantwortlichkeit den Content-Provider trifft und dass ein Rückgriff auf den Host-Provider häufig nicht der Rechtssicherung, sondern eher der effektiven Durchsetzung von Schadensersatzansprüchen dient. Es besteht aber kaum ein Zweifel, dass es – auch rechtspolitisch – wünschenswerter ist, Rechtsverletzungen und damit Schadensersatzansprüche zu vermeiden, statt zusätzlich Haftende für geschehene Rechtsverletzungen zu schaffen. Die Folgen des Löschens auf Verdacht sind zudem unter dem Blickwinkel der durch die Folgen betroffenen Grundrechte, unter anderem aus Art. 5 GG, mehr als bedenklich.

Auch der Wortlaut der Richtlinie spricht für die strengere Auslegung. Die französische Fassung[3] der – mit den §§ 7-10 TMG nahezu wortgleichen – ECRL[4] geht sowohl von einer Kenntnis der Rechtswidrigkeit der Handlung als auch der Information aus; somit gilt eine bloße Mitteilung hinsichtlich des Inhalts nicht als ausreichend. Es stellt sich die Frage, ob der Provider positive Kenntnis der Rechtswidrigkeit haben muss oder ob bereits deren Behauptung genügt.

(d.) „Notice-and-take-down“

Die Haftungsprivilegierung für Host-Provider entfällt, wenn sie einer Aufforderung, eine Information zu entfernen oder den Zugang zu ihr zu sperren, nach Kenntnis ihrer Rechtswidrigkeit nicht nachgekommen sind (§ 10 Nr. 2 TMG). Diese Methode ist als „Notice-and-take-down“- Verfahren inzwischen international üblich[5]. Dabei informiert der Geschädigte den Provider über die Inhalte und fordert ihn zu deren Beseitigung auf. Die konkrete Prozedur hat bislang nur in den USA eine gesetzliche Ausformung erhalten; die Anforderungen an die Begründung sind international unterschiedlich.

Auch hier ist fraglich, ob der Host-Provider schon auf die bloße Aufforderung der Behörde oder eines Privaten handeln muss oder ob positive Kenntnis der Rechtswidrigkeit – beispielsweise durch ein gerichtliches Urteil – vorhanden sein muss. Die erste Auslegung lässt dem Provider nur die

1Ahlert/Marsden/Yung, S.27. Dabei handelte es sich um offensichtlich legale Inhalte, die ausschließlich zum Zweck der Studie erstellt worden waren. Nachdem deren Rechtswidrigkeit behauptet wurde, löschte in einem Fall der Provider die Inhalte sofort, in einem anderen gab er detaillierte Auskunft, wie die Beschwerde zu formulieren sei, damit die Inhalte gelöscht werden könnten. Nach Meinung der Autoren hätte dies nur wenig kriminelle Energie erfordert.

2http://www.heise.de/newsticker/meldung/95758.

3Art. 14 I Nr. 1: „le prestataire n´ait pas effectivement connaissance de l´activité ou de

l´information illicites“.Wichtig ist, dass sich „illicites“ sowohl auf „activité“ als auch auf „information“ bezieht.

4Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABlEG Nr. L 178 v. 17.07.2000, S.1.

5Ahlert/Marsden/Yung, S.8.

Wahl, in die Gefahr zu geraten, entweder einen Vertragsverstoß gegenüber einem Kunden zu begehen oder in die Haftung nach allgemeinen Normen gegenüber demjenigen zu geraten, dessen Recht verletzt ist. Die zweite Auslegung, die eine positive Kenntnis des Providers von der Rechtsverletzung, verlangt, gibt ihm mehr Rechtssicherheit und erfüllt somit den Zweck des TMG. Noch dazu schadet sie dem Verletzen nicht wesentlich, da es ihm möglich sein dürfte, zeitnah zu belegen, dass die Inhalte wirklich rechtswidrig sind.

Nach § 10 Nr. 1 2. Alt. TMG genügt die „Kenntnis von Umständen, aus denen die Rechtswidrigkeit offensichtlich“ wird, für die Begründung von Schadensersatzansprüchen gegen den Host-Provider; auch hier muss also mehr als eine bloße Behauptung der Rechtswidrigkeit vorliegen. Wenn aber schon der Gesetzgeber für Schadensersatzansprüche von einem geringeren Kenntnisgrad ausgeht als für andere Ansprüche und dieser Grad an Kenntnis immer noch höher ist, als eine bloße Kenntnis der Inhalte, muss auch im Fall von § 10 Nr. 1. 1. Alt. TMG mehr als eine bloße Kenntnis der Inhalte vorliegen. Daher ist von demjenigen, der eine Verletzung unterstellt, zu fordern, dass – sollte der Urheber der möglicherweise rechtswidrigen Inhalte nicht erreichbar sein – seine Angaben eine Rechtsverletzung zumindest wahrscheinlich erscheinen lassen. In allen anderen Fällen muss z.B. ein gerichtliches Urteil, Vergleich oder Anerkenntnis vorhanden sein: Der Provider muss also positive Kenntnis der Rechtswidrigkeit erhalten[1], was für den Verletzen angesichts der Möglichkeit, einstweiligen Rechtsschutz in Anspruch zu nehmen, auch zumutbar ist.

(e.) Haftung bei Schadensersatzansprüchen

Die Haftung für Schadensersatzansprüche nach § 10 Nr. 1 2. Alt. TMG setzt eine Kenntnis der „Umstände, aus denen sich die Rechtswidrigkeit [...] ergibt“ voraus. Fraglich ist dabei, ob auch positive Kenntnis der Inhalte vorliegen muss[2] oder ob die bloße Kenntnis von Umständen genügt, die rechtswidrige Informationen wahrscheinlich erscheinen lassen, nach denen der Provider dann zu forschen hat[3]. Nachforschungen diesbezüglich müssen allerdings in jedem Fall erst unternommen werden, wenn konkrete Hinweise dafür vorliegen[4]; alles andere liefe auf eine Kontrollpflicht hinaus, die aber nach § 7 II TMG nicht besteht.

Eine Haftung, für die die Kenntnis von Umständen für das Vorliegen rechtswidriger Informationen genügt, läuft jedoch der hier zu der grundsätzlichen Privilegierung vertretenen Auffassung zuwider: Es wäre widersprüchlich, für Unterlassungsansprüche eine positive Kenntnis der Rechtswidrigkeit zu fordern und für Schadensersatzansprüche bloße Hinweise auf Umstände, aus denen das Vorliegen von rechtswidrigen Informationen hervorgeht, genügen zu lassen. Daher ist ebenso wie für

1So auch Hoeren, Access-Provider, S. 273.

2Freytag, CR 2000, 600, 608 zu § 5 TDG a.F.

3Spindler, NJW 2002, 921, 924.

4Spindler, NJW 2002, 921, 924.

die Haftung nach § 10 Nr. 1 2. Alt. TMG eine Kenntnis der Inhalte verbunden mit der Kenntnis der Umstände, aus denen die Rechtswidrigkeit offensichtlich wird, Voraussetzung für die Begründung von Schadensersatzansprüchen. Hierfür ist mehr als eine bloße Behauptung des Vorliegens der Umstände notwendig: Der Geschädigte muss beispielsweise substantiiert darlegen, dass er überhaupt Inhaber der verletzten Rechte ist[1]. Nur so ist es dem Provider möglich, eine eigene Beurteilung vorzunehmen und gleichzeitig die Gefahr des Missbrauchs mit drohenden Beschränkungen der Kommunikationsgrundrechte einzudämmen.

(f.) Zu eigen Machen

Wie oben schon beschrieben, können Anbieter für fremde Informationen ebenso wie für eigene zur Verantwortung gezogen werden, wenn sie sich diese zu eigen machen. Dies kommt vor allem in Foren und Gästebüchern, aber auch bei anderen Formen von seitens Dritter generierten Inhalten in Frage[2]. Technisch gesehen besteht zwischen Foren und Gästebüchern kein Unterschied: Beide beruhen auf Datenbanken auf einem Server, für die der Betreiber einem beschränkten Personenkreis oder der Öffentlichkeit Lese- und Schreibzugriff gewährt[3]. Daraus folgt, dass der Anbieter von Informationen[4] für den Bereich des Forums vom Content- zum Host-Provider wird, er mithin nur Speicherplatz für fremde Informationen – die Eingaben beliebiger Dritter – zur Verfügung stellt. Damit profitiert der Anbieter eines Forums grundsätzlich von der Haftungsprivilegierung des § 10 TMG. Etwas anderes gilt jedoch, wenn der Host-Provider sich die Inhalte Dritter zu eigen macht: In diesem Fall haftet er ebenso wie für eigene Inhalte. Ein Zu eigen Machen liegt vor, wenn der Anbieter aus Nutzersicht zu erkennen gibt, dass er sich mit den fremden Inhalten identifiziert[5]. In der Rechtsprechung scheint sich eine Vermutung heraus zu bilden, dass der Anbieter von Inhalten sich diese zu eigen macht, wenn er sich nicht von ihnen distanziert. Um sich von fremden Inhalten zu distanzieren, muss der Anbieter deutlich zum Ausdruck bringen, dass er sich ausdrücklich nicht mit den Inhalten identifiziert[6]. Eine pauschale Distanzierung von Inhalten Dritter oder ein Verweis auf die Verantwortung der Urheber ist nicht ausreichend.[7]. Gerade bei Foren kann man aber angesichts der dort vertretenen, häufig kontroversen Meinungen daran zweifeln, dass überhaupt ein Benutzer davon ausgeht, dass sich der Anbieter mit allen vertretenen Meinungen identifiziert, da

1So auch Wenzel, S. 638.

2In jüngster Zeit haben vor allem Webseiten wie www.YouTube.com und www.Flickr.com von ihren Usern erstellte Inhalte als Geschäftsmodell erkannt und damit Erfolg gehabt.

3Anders bei herkömmlichen Inhalten, wo der Anbieter in der Regel alleinigen Lese- und Schreibzugriff hat.

4Gewöhnlich werden Foren und Gästebücher in Verbindung mit anderen, eigenen Inhalten angeboten.

5Hoeren, Access-Provider, S. 275.

6BGH GRUR 1975, 89, 91.

7OLG Köln, MMR 2002, 548; OLG München, MMR 2002, 611, 613.

dies der Annahme einer multiplen Schizophrenie gleichkommen würde. Es ist zweifelhaft, ob in diesem Bereich die Übernahme der Grundsätze des Presserechts[1] angebracht ist.

Obwohl das Kriterium des Zu eigen Machens inzwischen nicht mehr auftaucht, greift die Rechtsprechung immer noch darauf zurück[2] und stellt darauf ab, ob beim Betrachter der Anschein erweckt wird, dass die Inhalte vom scheinbaren Anbieter stammten. Angemessener erscheint es, eine Haftung nur dann anzunehmen, wenn sich der Anbieter die fremden Informationen explizit zu eigen macht, also durch einen willentlichen Akt seine Zustimmung kundtut. Das einfache Angebot eines Forums oder Gästebuchs kann hierfür noch nicht genügen[3], ebenso wenig wie die Ausgabe von Suchergebnissen einer Suchmaschine[4]. Ansonsten gilt auch für Foren die Privilegierung des § 10 TMG[5], da andernfalls eine Haftung für falsch formulierte so genannte Disclaimer[6] entstünde, die von den Nutzern der Erfahrung nach generell ignoriert werden. Diese Abweichung von presserechtlichen Grundsätzen ist auch deshalb geboten, weil die Betreiber von Foren, anders als Presseorgane, keine Auswahl hinsichtlich der Inhalte Dritter treffen. Eine Haftung würde also nur auf dem Angebot der Äußerungsmöglichkeit für Dritte, ohne irgendeinen Akt der Zustimmung zu deren Äußerungen, aufbauen. Der wesentliche Grund für eine presserechtliche Haftung besteht aber in der willentlichen Veröffentlichung der Inhalte Dritter, welche beim Leser zumindest den Anschein der Zustimmung hervorruft. Dieser liegt im Internet allerdings für den verständigen Nutzer nicht ohne Weiteres vor, wie auch das OLG Hamburg in Bezug auf Suchmaschinen klarstellte[7].

e. Haftung für Hyperlinks

Hyperlinks sind Teile der Inhalte eines Angebots und technisch wesentliche Bestandteile des WWW. Hyperlinks können sowohl auf eigene Inhalte desjenigen verweisen, der sie setzt – in diesem Fall sind sie unproblematisch – als auch auf fremde Angebote[8]. Da diese unter Umständen wechseln, kann es vorkommen, dass sich ein Verweis auf einen ursprünglich legalen Inhalt ohne Zutun des Linksetzenden in einen Link auf einen illegalen Inhalt verwandelt. Aber auch die Verlinkung auf einen bereits ursprünglich illegalen Inhalt, dessen Rechtswidrigkeit dem Linksetzenden nicht bekannt war, kann für diesen eine Haftung auslösen. Allerdings sind nach dem Ideal des

1So OLG Köln, MMR 2002, 548.

2So anscheinend LG Hamburg, Urteil vom 28.04.2006, Az.: 324 O 993/05.

3So auch Spindler/Schmitz/Geis-Spindler, § 8 TDG Rn. 8.

4So aber LG Hamburg, Urteil vom 28.04.2006, Az.: 324 O 993/05, aufgehoben durch OLG Hamburg, CR 2007, 330f.

5LG Köln, Urteil vom 4.12.2002, Az.: 28 O 627/02, abrufbar unter: http://www.jurpc.de/rechtspr/20030140.htm.

6Erklärung, dass der Urheber der Seite nicht verantwortlich für die Inhalte der verlinkten Seiten ist.

7OLG Hamburg, CR 2007, 330, 330.

8Hier interessiert nur die Frage nach der Rechtswidrigkeit des verlinkten Inhalts. Zur Frage der Rechtswidrigkeit des Verlinkens siehe z.B. Stadler, http://www.jurpc.de/aufsatz/20030002.htm.

WWW alle Inhalte weltweit miteinander verknüpft, so dass jeder, der Links auf andere Seiten setzt, indirekt auch rechtswidrige Inhalte verlinken wird, solange solche existieren. Eine Abgrenzung, ab welchem Grad der indirekten Verlinkung eine Haftung ausgeschlossen ist, ist nur durch das unscharfe Kriterium der Zumutbarkeit einer Kontrolle möglich.

In eine Haftungsfalle drohte vor dem „Paperboy"-Urteil[1] zu geraten, wer einen Link setzen wollte. Wer pauschal auf ein Angebot verwies, das in Teilen rechtswidrig war, wobei sich der Link auf einen rechtmäßigen Inhalt bezog, hätte sich nach der Rechtsprechung einiger Gerichte die Inhalte aller Seiten des Anbieters zu eigen gemacht und damit wie für eigene Inhalte gehaftet. Wäre der Link direkt auf den Inhalt gesetzt worden, wäre bei der damals unklaren Rechtslage wegen Verletzungen von Urheberrechten bzw. wettbewerbswidrigem Verhalten eine Verurteilung zu Unterlassung und Schadensersatz denkbar gewesen. Der BGH hat jedoch klar gestellt, dass auch ein direkter Link auf den gewünschten Inhalt unter Umgehung der Eingangsseite rechtmäßig ist[2].

Grundsätzlich haftet derjenige, der einen Link setzt, für die Inhalte der fremden Seiten, wenn er sich deren Inhalt zu eigen macht. Durch das Zu eigen Machen wird der ursprünglich fremde Inhalt wie ein eigener Inhalt behandelt, was eine Haftungsprivilegierung ausschließt[3]. Wann dieser Tatbestand jedoch vorliegt, ist in der deutschen Rechtsprechung bisher unklar.

Für Links wird eine Haftungsprivilegierung nach § 8 I TMG oder § 10 TMG diskutiert[4], wenn nicht schon eine Haftung nach § 7 I TMG gegeben ist.

(1.) Einordnung von Links

Durch Links werden fremde Angebote mit eigenen verbunden, wobei der Status der Fremdheit grundsätzlich unberührt bleibt. Wenn allerdings die fremden Inhalte durch die Gestaltung der Links ausdrücklich zum Inhalt des eigenen Angebots gemacht werden, bestehen keine Bedenken gegen eine Haftung. Es dürfte sich in derartigen Fällen nicht mehr um fremde Inhalte handeln, da sich der Linksetzende diese zu eigen gemacht hat. Vergleichbare Fallgestaltungen finden sich bei eindeutig fremden Inhalten im Presserecht, wo grundsätzlich ebenfalls keine Haftung besteht. Es ist kein Grund ersichtlich, wieso diese Grundsätze nicht auch im Bereich des Internets – ungeachtet der Meinungsrelevanz der Angebote – gelten sollten, nicht zuletzt angesichts der im Internet existenten Möglichkeit der „Mutation" von Inhalten von rechtmäßigen zu rechtswidrigen, ohne Zutun und

1BGH AfP 2003, 545ff. – Paperboy.

2BGH AfP 2003, 545ff. – Paperboy.

3Durch ein Zu eigen Machen werden fremde Inhalte wie eigene Inhalte nach § 7 I TMG behandelt.

4Die Diskussion wurde zu § 9 TDG/§ 7 MDStV bzw. zu § 11 TDG / § 9 MDStV geführt. Da der Wortlaut der Vorschriften nicht geändert wurde, bestehen die Meinungen jedoch fort. Im Folgenden werden lediglich die geltenden Vorschriften des TMG zitiert.

Kenntnis des Verlinkenden[1]. Es gibt keine Kontrollpflicht für Links[2], obgleich diese ein zentrales Element des WWW und damit der wichtigsten Anwendung des Internets überhaupt darstellen.

Ungeklärt ist, ob Links eine Zugangsvermittlung nach § 8 I TMG (§ 5 III TDG a.F.)[3] oder ein Bereithalten von Inhalten nach § 10 TMG darstellen. Der Wortlaut scheint zunächst für eine Einstufung als Zugangsvermittlung im Sinne des § 8 I TMG zu sprechen. In der Gesetzesbegründung des weitgehend ähnlichen § 5 III TDG a.F. wird davon ausgegangen, dass „Zugänglich- machen" für „den Weg öffnen" steht[4]; hier taucht auch die im jetzigen § 8 TMG verwendete Variante des „Durchleitens" auf[5]. Damit ist klar, dass von § 5 III TDG a.F. bzw. seinem Nachfolger § 8 TMG in erster Linie der technische Vorgang der Zugangsermöglichung gemeint war und nicht der willentliche Hinweis auf fremde Inhalte.

Allerdings ist das Setzen eines Links nach § 10 TMG auch kein Bereithalten von Inhalten[6]: Der Linksetzende hat – anders als Host-Provider – keine Möglichkeit der Kontrolle über die fremden Inhalte. Damit sind die Haftungsprivilegierungen des TMG nicht direkt anwendbar.

In der Konsequenz befände sich der Ersteller eines Angebots in der misslichen Lage, dass er von keinerlei Haftungsbeschränkung für die gesetzten Links profitieren würde, auch nicht für die Links der Angebote, die er verlinkt hat. Jemand, der Links auf andere Inhalte setzt, wird jedoch zumeist mittelbar auf irgendwelche rechtswidrigen Inhalte irgendwo im Internet verweisen; eine Einschränkung wäre nur auf der Ebene der Zumutbarkeit einer Kontrolle möglich. Dieses Kriterium ist aber ebenso flexibel handhabbar wie unscharf; eine Einschränkung der Verantwortlichkeit einzig über die Zumutbarkeit käme geradezu einer Einladung zur Prozessführung gleich und wäre zur Erreichung von Rechtssicherheit sicherlich nicht förderlich.

Die Folge der Nicht-Privilegierung von Links steht nicht im Einklang mit dem Zweck des IuKDG; es liegt eine Lücke vor. Der Gesetzgeber lässt auch nicht erkennen, dass er die Folge der Nichtprivilegierung für Links billige: Die Gesetzesbegründung zu den §§ 7-10 TMG erklärt in Bezug auf Links lediglich, dass eine Reform nötig sein könnte, dafür aber noch auf Vorschläge auf EU-Ebene gewartet werden müsse[7]. Das spricht nicht dafür, dass der Gesetzgeber mit der vollen Haftung für Links einverstanden ist, die Begründung lässt nur erkennen, dass der Gesetzgeber die zur Zeit der Novellierung von TDG und MDStV geltende Rechtslage nicht verändern, sondern nur die damals geltenden TDG und den MDStV terminologisch an die ECRL anpassen wollte. Genau

1AG Tiergarten, Az.: 260 DS 857/96, Entscheidung vom 30. Juni 1997, abrufbar unter: http://www.netlaw.de/urteile/agb_01.htm.

2AG Tiergarten, Az.: 260 DS 857/96, Entscheidung vom 30. Juni 1997, abrufbar unter: http://www.netlaw.de/urteile/agb_01.htm.

3So z.B. Hoeren, Internetrecht, S. 282; Koch CR 1997, 193, 200.

4BT Drs. 13/7385, S. 20.

5BT Drs. 13/7385, S. 20.

6S.o. S.49.

7BT Drs. 16/3078, S.11.

das ist in der Folge nicht geschehen, vielmehr änderte sich die Rechtsprechung, was zu den Ausführungen über die Notwendigkeit einer Reform in der Begründung des TMG führte. Weitgehende inhaltliche Änderungen finden sich nicht, auch der ursprüngliche Zweck von TDG und MDStV – die Schaffung von sicheren Rahmenbedingungen[1] – lässt nicht den Schluss der Bejahung einer vollen Haftung für das Setzen von Links zu: Allein aus dem Schweigen zu einer bekannten Kontroverse kann nicht gefolgert werden, dass Nebenfolgen der Novellierung von Gesetzen gebilligt würden, insbesondere, wenn diese die Änderung einer sich festigenden Rechtsprechung zur Folge haben[2]. Es erscheint vielmehr plausibel, dass der Gesetzgeber die Frage der Privilegierung von Links weiterhin der Rechtsprechung überlassen und zu diesem Zeitpunkt nicht entscheiden wollte[3]. Insbesondere ist nicht erkennbar, dass der Gesetzgeber die sich festigende Rechtsprechung missbilligt hätte.

Die volle Haftung für das Setzen von Links hätte außerdem die – vom Gesetzgeber sicher nicht gewünschte – Folge, dass die durch die Einführung des TMG eigentlich beseitigte Unterscheidung von Tele- und Mediendiensten, welche bereits vor Schaffung des TMG als „dogmatischer Irrgarten“[4] bezeichnet wurde, wieder aufleben würde. Während Anbieter von meinungsrelevanten Mediendiensten dann nur unter den Haftungsregelungen des Medienrechts – die zu ähnlichen Privilegierungen wie das TMG kommen – für Links Verantwortung trügen, wären Anbieter von nicht-meinungsrelevanten Telediensten überhaupt nicht privilegiert und voll verantwortlich für Inhalte, die letztlich unter der Kontrolle Anderer stehen.

Die Unterscheidung zwischen Medien- und Telediensten sollte aber nach den Vorstellungen des Gesetzgebers bereits bei der Schaffung von TDG und MDStV und erst recht nach Inkrafttreten des TMG wegen der identischen Haftungsregelungen sowie der schwierigen und bis zum Schluss in den Details unklaren Abgrenzung keine praktische Relevanz erlangen[5].

Als Problemlösung bietet sich aufgrund der großen Bedeutung der Links für inhaltliche Angebote sowie der Unmöglichkeit der Kontrolle aller Links und womöglich noch der Folgelinks[6] eine analoge Anwendung des § 10 TMG an[7]. Dies liegt sowohl durch eine ähnliche Interessenlage als auch durch die ideal passenden Rechtsfolgen der abgestuften Haftung nach § 10 TMG nahe. Ebenso wie für diejenigen, die fremde Inhalte anbieten, ist eine Haftung für Linksetzende auch dann

1BT Drs. 13/7385, S.16.

2Das bekannteste Beispiel des Schweigens des Gesetzgebers zu einem bekannten Problem, das trotzdem durch (weitgehende) Analogien gelöst wurde, sind die Entwicklungen von pVV und cic.

3So auch Neumann, CR 2005, 70, 72.

4Engel, MMR Beilage 4/2003, S.13.

5BT Drs. 14/1191; Engel-Flechsig/Maennel/Tettenborn, Einl. IuKDG, Rn. 16.

6Dazu führt in konsequenter Anwendung die Entscheidung AG Stuttgart, CR 2005, 69f.

7So z.B. Waldenberger MMR 1998, 124, 128f.

zumutbar, wenn sie Kenntnis von der Rechtswidrigkeit der Angebote haben. Somit haftet der Ersteller von Links nur unter den Voraussetzungen des § 10 TMG[1].

Die Rechtsprechung nahm jedoch eine andere Entwicklung.

(2.) LG Hamburg 1998

Nach einer Entscheidung des LG Hamburg[2] liegt ein Zu eigen Machen bereits in der Linksetzung ohne ausreichende Distanzierung vor; demnach hafte der Linksetzende für den Inhalt der verlinkten Seiten wie für eigene Inhalte. Ein ähnliches Verständnis liegt wohl auch der „FTP-Explorer"-Entscheidung[3] des LG München I zugrunde: Eine Privilegierung nach § 5 II TDG a.F. (jetzt in § 10 TMG enthalten) komme nicht in Frage, da es sich um eigene Inhalte im Sinne des § 5 I TDG a.F. (jetzt in § 7 I TMG enthalten) handele[4].

Diese Auffassung würde jedem Betreiber einer Homepage vorschreiben, eine Rechtmäßigkeitsprüfung aller verlinkten Inhalte durchzuführen, was Laien angesichts der nach wie vor unklaren Rechtslage nicht zumutbar und unter Umständen aus tatsächlichen Gründen unmöglich ist[5].

(3.) LG Lübeck 1998

Das LG Lübeck[6] schließt zwar ebenfalls auf eine Haftung des Linksetzenden, hält aber die Linksetzung an sich nicht für ausreichend für ein Zu eigen Machen; dazu bedürfe es noch des zusätzlichen Umstandes, dass sich der Anbieter die Inhalte „geistig zu eigen macht"[7]. Zu einer Annahme der Haftung gelangte das Gericht, weil der Beklagte die verlinkten Inhalte zum notwendigen Bestandteil seines eigenen Angebots gemacht und sie sich damit „geistig zu eigen gemacht" hatte[8].

Diese Entscheidung stimmt mit der oben vertretenen Auffassung überein; allerdings ist das Kriterium des geistig Zu eigen Machens konkretisierungsbedürftig.

(4.) OLG Braunschweig 2001

In einem mit dem „FTP-Explorer"-Fall des LG München[9] identischen Fall desselben Klägers kam das OLG Braunschweig zu dem Ergebnis, dass mit dem Setzen eines Links auf die Eingangsseite

---

1Siehe dazu S.49. So wohl auch Geiseler-Bonse, allerdings unter falscher Bezugnahme auf § 9 I TDG.

2Entscheidung vom 12.5.1998, Az.: 312 O 85/98.

3LG München I, Urteil vom 25.01.01, Az: 4HK 0 2l648/00.

4LG München I, Urteil vom 25.01.01, Az: 4HK 0 2l648/00.

5Dazu die identische Lage bei Host-Providern, S.51ff.

6LG Lübeck, Urteil vom 24.11.1998, Az.: 11 S 4/98.

7LG Lübeck, Urteil vom 24.11.1998, Az.: 11 S 4/98.

8LG Lübeck, Urteil vom 24.11.1998, Az.: 11 S 4/98.

9LG München I, Urteil vom 25.01.01, Az: 4HK 0 2l648/00.

eines Angebots noch kein Zu eigen Machen der Inhalte des Angebots vorliege[1]. Derartige Links seien nach § 5 II TDG a.F. (jetzt § 10 TMG) privilegiert, so dass eine Haftung ausscheide. Auch Links, die direkt auf das rechtswidrige Angebot führten, seien nicht notwendigerweise „zu eigen gemacht", wenn deutlich werde, dass es sich nicht um eigene Inhalte handele[2]; diese seien als fremde Inhalte nach § 5 II TDG a.F. (jetzt in § 10 TMG enthalten) zu beurteilen[3]. Maßgeblich für die Beurteilung des Zu eigen Machens sei die Verkehrsauffassung[4].

Die Entscheidung des OLG Braunschweig markierte den Beginn einer Vielzahl von Entscheidungen der OLGe zu vergleichbaren Fallgestaltungen; sie brachte außerdem zum ersten Mal die sich fortan verfestigende Rechtsprechung zur Rechtswidrigkeit der Linksetzung zum Ausdruck. Für die in diesem Urteil vertretene Auffassung spricht einerseits die Bezugnahme auf die Privilegierung nach § 5 II TDG a.F., andererseits die ausgewogene Entscheidung über das Zu eigen Machen, die nicht mehr nur auf rein technische Fragen, sondern im Wesentlichen auf die Verkehrsauffassung abstellt.

(5.) BGH 2004 – Schöner Wetten[5]

In einer presserechtlichen Entscheidung hat der BGH quasi im Vorübergehen – letztlich kam es auf die Frage nicht entscheidend an – konstatiert, dass das Setzen von Hyperlinks nicht vom Anwendungsbereich der Privilegierungen der §§ 6 - 9 MDStV (jetzt §§ 7 - 10 TMG) umfasst sei. Hierbei berief er sich auf Teile der Literatur und den angeblichen Willen des Gesetzgebers, der gegen eine Privilegierung des Setzens von Links gerichtet sei.

(6.) AG Stuttgart 2004[6]

In einer strafrechtlichen Entscheidung hatte sich das AG Stuttgart mit der Frage zu befassen, ob es strafbar sei, Links auf eine Seite zu setzen, über die verbotene Inhalte erreichbar waren[7]. Es handelte sich also nicht um eine direkte Verlinkung, jedoch war sich der Urheber des Links der Gesetzwidrigkeit der indirekt verlinkten Seiten bewusst[8]. Die Strafbarkeit wurde bejaht, ohne eine eventuelle Haftungsbefreiung oder Argumente für eine Nichtanwendung zu thematisieren; nach den Ausführungen des AG Stuttgart gilt es nunmehr auch als Straftat, indirekt auf rechtswidrige Inhalte

1OLG Braunschweig, Urteil vom 28.6.2001, Az.: 2 U 141/00.

2OLG Braunschweig, Urteil vom 28.6.2001, Az.: 2 U 141/00.

3OLG Braunschweig, Urteil vom 28.6.2001, Az.: 2 U 141/00.

4OLG Braunschweig, Urteil vom 28.6.2001, Az.: 2 U 141/00; OLG Brandenburg, Urteil vom 16.12.2003 Az.: 6 U 161/02.

5BGH MMR 2004, 529ff.

6AG Stuttgart, CR 2005, 69f.

7Dieser Sachverhalt ergibt sich nicht aus dem Urteil selbst, sondern der Anmerkung von Neumann, CR 2005, 70ff.

8Es handelte sich um die von der Sperrungsverfügung des Düsseldorfer Regierungspräsidenten betroffenen Seiten. Der Angeklagte wollte durch das gesamte Angebot gegen Sperrungsverfügungen und für Meinungsfreiheit eintreten, ohne mit den verlinkten Inhalten zu sympathisieren.

zu verweisen. Als Anknüpfungspunkt dieser neuen dogmatischen Linie ist lediglich zu nennen, dass es „ein leichtes sei, die strafbaren Inhalte zu erreichen“[1] – diese so bisher nicht vertretene Ansicht wird nicht durch die Bezugnahme auf irgendwelche Normen unterstützt und hat, unter anderem aus diesem Grund, heftige Kritik in der Literatur erfahren[2].

(7.) OLG Stuttgart 2006[3]

In einer strafrechtlichen Entscheidung vom 24. April 2006 hat das OLG Stuttgart den Betreiber einer Seite, der vorsätzlich Links auf verbotene Inhalte in den USA gesetzt hatte, die Gegenstand der bereits erwähnten Sperrungsverfügungen waren, freigesprochen, jedoch unter Verweis auf die Rechtsprechung des BGH[4] entschieden, dass die Links nicht unter die Privilegierungen des TDG bzw. MDStV fielen, da sie dort nicht explizit geregelt seien – auch eine analoge Anwendung sei nicht möglich. Dieselbe Begründung diente für zwei Entscheidungen des KG zu Suchmaschinen[5].

(8.) Kritik der Rechtsprechung

Die Rechtsprechung zur Abgrenzung eigener und fremder Inhalte ist sehr unübersichtlich geworden. Dabei wird in den seltensten Fällen beachtet, dass es zwar nicht die „Natur“ des Internets, jedoch einen großen Reiz seiner Inhalte ausmacht, dass problemlos auf fremde Inhalte Bezug genommen werden kann. Links sind vergleichbar mit Fußnoten, jedoch können durch erstere die verknüpften Inhalte sofort auf den Bildschirm gerufen werden. Sofern eine Haftung für Urheberrechtsverletzungen begründet werden soll, ist eine Haftung des Linksetzenden wohl im allgemeinen Interesse, da es zumindest möglich ist, die Rechtswidrigkeit urheberrechtlich geschützter Inhalte zu erkennen. Bei Meinungsäußerungen in verlinkten Inhalten stellt sich die Lage anders dar. Der verständige Durchschnittsnutzer wird bei verlinkten Inhalten nicht davon ausgehen, dass diese auch die Meinung des Linksetzenden wiedergeben: Bei Anbietern von Foren etwa wird, angesichts der Vielzahl der dort vertretenen, kontroversen Meinungen, kaum jemand annehmen, dass diese sich, selbst wenn sie sich nicht eindeutig distanzieren, mit allen Inhalten identifizieren[6] – angesichts der Vielzahl kontroverser Meinungen in einem Forum müsste hierfür eine ausgeprägte multiple Schizophrenie gegeben sein[7].

Die neuere Rechtsprechung umgeht das Problem des Zu eigen Machens von Links der Einfachheit halber, indem sie mit Verweis auf Teile der Literatur[8] und ohne weitere Begründung dem Gesetzgeber eine Ablehnung der Privilegierung von Links unterstellt. Diese Annahme ist allerdings

---

1AG Stuttgart, CR 2005, 69, 70.

2Neumann, CR 2005, 70ff, Kaufmann/Köcher, MMR 2005, 334f.

3OLG Stuttgart, MMR 2006, 387ff.

4BGH NJW 2004, 2158, 2159.

5KG, MMR 2006, 392; KG, MMR 2006, 393.

6So auch im Ergebnis OLG Düsseldorf MMR 2006, 618ff.

7Zweck eines Forums ist schließlich der kontroverse Meinungsaustausch.

8BGH MMR 2004, 529ff, OLG Stuttgart MMR 2006, 387ff.

nicht zwangsläufig korrekt: Der Gesetzgeber hat sich in den Materialien zur Novellierung des TDG und im Gesetzgebungsverfahren zum TMG mit dieser Thematik zwar nicht auseinander gesetzt, jedoch kann daraus noch nicht geschlossen werden, dass er angesichts der eine Privilegierung annehmenden und sich festigenden Rechtsprechung zur Zeit der Novellierung von TMG und MDStV diese nicht gewollt habe.

(9.) Keine Haftungsbefreiung

Nach in der Literatur vertretenen Standpunkten soll sowohl nach dem TDG a.F. als auch nach dem geltenden TMG keine Haftungsbefreiung für das Setzen von Links gelten, die Linksetzenden seien vielmehr nach den allgemeinen Vorschriften verantwortlich[1]. Dies wird damit begründet, dass derjenige, der einen Link setze, mehr tue, als „nur“ den Zugang zur Nutzung eines Angebots bereitzustellen[2]: Er wähle ein spezielles Angebot aus und schaffe somit ein spezifisches Risiko. Dies sei weder ein Bereithalten von Inhalten anderer noch ein bloßes neutrales Zugänglich machen. Eine Analogie zu den Regelungen des TMG scheide wegen der der Novellierung von TDG und MDStV sowie der Verabschiedung des TMG vorausgegangenen Diskussionen um die Haftung für Hyperlinks aus, da diese dem Gesetzgeber bekannt gewesen seien und somit keine unbewusste Regelungslücke mehr bestehe[3]. Im Einzelfall solle dennoch eine Haftungsbefreiung nach den Grundsätzen des TMG gelten[4].

Diese Auffassung verdient in verschiedener Hinsicht grundsätzliche Kritik: Sie führt in der Haftungsfrage direkt zu einer Differenzierung zwischen Mediendiensten, für welche die mit denen des TMG vergleichbaren Regeln des Medienrechts zu gelten hätten, und Telediensten.

Für letztere wäre eine Haftungsbefreiung im Wesentlichen nach dem Kriterium der Zumutbarkeit möglich, was allerdings aller Wahrscheinlichkeit nach zu einer umfangreichen und unübersichtlichen Kasuistik führen würde. Noch unklarer dürfte die Rechtslage werden, wenn wie vorgeschlagen[5] die Regelungen des TMG im Einzelfall Anwendung fänden – die Einzelfälle, in denen dennoch eine Privilegierung stattfinden soll, sind nicht ansatzweise erkennbar. Da auch keine dogmatischen Gründe vorliegen, die eine Anwendung im Einzelfall ermöglichen würden, wäre die Entscheidung letztendlich von Willkür und Inkonsequenz geprägt und würde zudem dem mit der Verabschiedung des IuKDG verfolgten Ziel der Rechtssicherheit für den e-Commerce

1Kröger/Gimmy-Müller-Terpitz, S.583ff.

2Kröger/Gimmy-Müller-Terpitz, S.584.

3Statt Vieler: Stadler, http://www.jurpc.de/aufsatz/20030002.htm, Spindler, NJW 2002, 921, 924.

4Spindler, NJW 2002, 921, 924.

5Spindler, NJW 2002, 921, 924.

entgegenlaufen[1]. Um einer undurchdringlichen Kasuistik und Unsicherheit der Anbieter bezüglich des Bestehens einer Haftung entgegen zu wirken, wird im Einzelfall die sicherlich zu begrüßende Anwendung der Regeln des TMG vorgeschlagen[2].

f. Privilegierung der Störerhaftung

Nach mittlerweile gefestigter Rechtsprechung[3] sowie Teilen der Literatur[4] sind Host- und Accessprovider nicht von der zivilrechtlichen Störerhaftung befreit. Dabei ist jedoch schon strittig, ob bei diesen Providern überhaupt die Voraussetzungen einer Störerhaftung gegeben sein können und ob – wenn die Voraussetzungen vorliegen – die Haftungsregelungen des TMG zugunsten der Provider eingreifen.

(1.) Voraussetzungen der Störerhaftung

Die Provider verletzen nicht durch eigene Handlungen fremde Rechte, ermöglichen durch ihre Dienstleistungen allerdings die rechtsverletzenden Handlungen Dritter. Gemäß § 830 BGB müsste für diesen Tatbestand eine willentliche und adäquat kausale Teilnahme an der Herbeiführung einer Rechtsverletzung erfolgen[5]; dies ist aber in der Regel nicht der Fall[6].

Ein anderer Anknüpfungspunkt besteht in einer Haftung analog § 1004 BGB: Als haftungsbegründende Handlung kommt das Anbieten von Speicherplatz bzw. Übertragungskapazitäten, deren bestimmungsgemäßer Gebrauch durch den Schädiger zur Verletzung der Rechte Dritter führt, in Frage[7]. Allerdings setzt eine Störerhaftung nach der neueren Rechtsprechung des BGH eine Verletzung von Prüfpflichten voraus[8], die nach dem eindeutigen Wortlaut des § 7 II 1 TMG aber nicht gegeben ist. Auch anhand § 7 II 2 TMG kann eine Überwachungspflicht weder direkt begründet noch über eine Analogie konstruiert werden[9]. Anderes gilt, wenn dem Provider die gespeicherten oder durchgeleiteten Daten bekannt sind[10], was jedoch lediglich in Ausnahmefällen vorliegen dürfte.

(2.) Haftungsprivilegierungen

Nähme man entgegen der hier vertretenen Meinung eine Störerhaftung an oder handelte es sich um einen der seltenen Ausnahmefälle, stünden einer Haftung von Host- und Accessprovidern noch die

---

1BT Drs. 13/7385, S.16.

2Spindler, NJW 2002, 921, 924.

3LG Hamburg, Urteil vom 07.07.2004, Az.: 308 O 264/04; LG Köln, Urteil vom 28.07.2004, Az.: 28 O 301/04; BGHZ 158, 236, 246 ff.

4Volkmann, S. 101; Stadler CR 2004, 521, 525.

5Sieber/Höfinger, MMR 2004, 575, 578.

6Sieber/Höfinger, MMR 2004, 575, 578.

7Sieber/Höfinger, MMR 2004, 575, 578.

8Sieber/Höfinger, MMR 2004, 575, 578; BGH GRUR 1999, 418, 420; GRUR 1997, 313, 316. A.A. Volkmann, S.61ff.

9Sieber/Höfinger, MMR 2004, 575, 580.

10Sieber/Höfinger, MMR 2004, 575, 578f.

Regelungen der Verantwortlichkeit der §§ 7-10 TMG entgegen. Diese schließen für Access-Provider nahezu jegliche Haftung für die transportierten Daten aus; für Hostprovider besteht eine Haftung nur bei Kenntnis der Rechtsverstöße[1]. Allerdings soll nach Urteilen der LGe Hamburg und Köln[2] die Privilegierung des § 8 TMG nicht auf die verschuldensunabhängige Störerhaftung anwendbar sein, was sich aus § 7 II 2 TMG ergebe[3] – aus der Begründung des EGG[4] wird aber gerade nicht ersichtlich, dass eine verschuldensunabhängige Haftung von den Haftungsprivilegierungen ausgenommen sein solle. Zuzugeben ist dem BGH[5] die Möglichkeit von Providern, eine Perpetuierung der Rechtsverletzung zu verhindern; dies gilt allerdings nur für die erstmalige Veröffentlichung von Inhalten durch Dritte und kann nicht zu Unterlassungsverpflichtungen führen. Der BGH hat diese auch für technisch vergleichbare Live-Sendungen im Fernsehen nicht aufgestellt[6]. Nach § 7 II 2 TMG sind Provider nur gegenüber Ansprüchen auf Unterlassung nicht privilegiert[7], was sich aber auch aus den §§ 8 ff TMG ergibt, nach denen für Host-Provider bei Kenntnis von Rechtsverletzungen eine Privilegierung nicht besteht[8], sie mithin nach Kenntnis der Rechtswidrigkeit zur Entfernung von Inhalten verpflichtet sind. Insofern geht die Auffassung fehl, dass die Störerhaftung nicht privilegiert sei: Es besteht lediglich eine Ausnahme von der Privilegierung, wenn oben[9] genannte Voraussetzungen – und somit Kenntnis von Inhalten – vorliegen.

(3.) Unterlassungsanspruch aufgrund der Störerhaftung?

Grundsätzlich ergibt sich aus einem Anspruch aus Störerhaftung analog § 1004 I 1 BGB nur ein Anspruch auf Beendigung der Störung[10]. Im Fall von Abs. I 2 richtet er sich bei Wiederholungsgefahr auch auf Unterlassung zukünftiger Störungen. Wiederholungsgefahr wird regelmäßig angenommen, wenn eine Störung schon einmal eingetreten ist[11]; dies tritt fast zwangsläufig bei allen Fällen der Störerhaftung gegenüber Providern auf. Host- und Accessprovider haften nur nach Kenntnis der Störung, der Eintritt der Störung ist somit denklogisch notwendig. Mit einem Anspruch auf Beseitigung der Störung wäre auch ein Anspruch auf Unterlassung weiterer

1S.o. S.49ff.

2LG Hamburg, Urteil vom 07.07.2004, Az.: 308 O 264/04; LG Köln, Urteil vom 28.07.2004, Az.: 28 O 301/04.

3LG Hamburg, Urteil vom 07.07.2004, Az.: 308 O 264/04, das auf die Begründung des EGG, BT-Drucks. 14/6098, S.23 verweist.

4BT Drs. 14/6098. Auch für das TDG a.F. ergibt sich keine andere Rechtslage.

5BGH, Urteil vom 27.03.2007, Az. VI ZR 101/06.

6BGHZ 66, 182, 188. Auf dieses Urteil bezieht sich BGH VI ZR 101/06 ausdrücklich.

7Stadler, Providerauskunft, abrufbar unter: http://www.afs-rechtsanwaelte.de/Pages/providerauskunft.html.

8S.o., S.49ff.

9S.o. S.50f.

10Prütting/Wegen/Weinreich, § 1004, Rn. 6.

11Herberger/Martinek/Rümann/Weth, § 1004, Rn. 14.

Störungen verbunden, der nach der vorherrschenden Rechtsprechung nicht von der Privilegierung umfasst ist.

Problematisch ist dieser Anspruch, weil § 7 II 1 TMG festlegt, dass keinerlei Prüfungs- und Überwachungspflichten bestehen; ein Anspruch auf Verhinderung künftiger Störungen setzt aber voraus, dass ein Provider sein Angebot in irgendeiner Weise überwacht, um eingetretene Störungen sofort beseitigen zu können, da im Internet eine Verhinderung der Störungen vor Eintritt in der Regel unmöglich oder zumindest unzumutbar sein dürfte. Gleichwohl existiert nach einem Urteil des BGH ein vorbeugender Unterlassungsanspruch[1].

(4.) Stellungnahme

Die noch auf dem alten § 5 TDG bzw. MDStV beruhende Auffassung, dass keine Privilegierung für verschuldensunabhängige Haftungstatbestände bestehe, findet weder im Wortlaut des Gesetzes noch in der vom LG Hamburg zitierten Begründung des EGG eine Grundlage[2]. Sie widerspricht vielmehr der Intention des Gesetzgebers, für die Provider Rechtssicherheit durch weitestgehende Haftungsprivilegierungen zu schaffen, und ist daher abzulehnen. Zwar existiert keine Privilegierung, wenn ein Provider Kenntnis des Inhalts und dessen Rechtswidrigkeit hatte und es entsteht eine Verpflichtung zur Entfernung der Inhalte, jedoch lässt sich daraus nicht ableiten, dass auch eine Pflicht zur Verhinderung weiterer, in der Zukunft liegender Rechtsverletzungen vorliege. Ein solcher Anspruch setzt eine Kontrolle der Inhalte, ob die von einer Unterlassungsverfügung betroffenen Inhalte enthalten sind, voraus. Eine Kontrollpflicht für fremde Inhalte besteht jedoch nach § 7 II TMG nicht.

(5.) Kritik der Rechtsprechung

Die Rechtsprechung hat den mit dem IuKDG im Jahre 1997 verfolgten Zweck im Laufe der Zeit durch eine undurchdringliche Vielfalt von Entscheidungen in sein Gegenteil verkehrt. Es fehlt den Urteilen an Systematik, und es wird keine Entwicklung in Richtung einer bestimmten, einheitlich gehandhabten Rechtsprechung ersichtlich. Einige Beschlüsse, auch aus der jüngeren Vergangenheit, scheinen eher die sekundäre Haftung ausdehnen zu wollen, was dem Ziel des IuKDG und TMG, Host- und Access-Provider von einer Haftung weitestgehend zu befreien, zuwider läuft. Die Tatsache, dass diese Freistellung nicht einer willkürlichen Laune des Gesetzgebers entsprang, sondern technisch bedingt ist, wird nicht beachtet bzw. ihr wird in einigen Urteilen, ohne sie konkret zu erwähnen, nur dadurch Rechnung getragen, dass die Beklagten allein bei Kenntnis der rechtswidrigen Inhalte verurteilt wurden. Diese Haftung ließe sich teilweise durch einen völligen Kontrollverzicht vermeiden, was jedoch nicht Ziel der Rechtsprechung sein kann. Dem entgegen

1BGH, Urteil vom 19.04.2007, Az: I ZR 35/04.

2BT Drs. 14/6098.

steht die Gesetzesbegründung zu dem damaligen § 5 TDG a.F., dass eine Haftung nur bei Kenntnis der Rechtswidrigkeit gegeben sei sowie der Neuformulierung in § 10 Nr. 1 2. Alt. TMG, nach dem die Rechtswidrigkeit offenkundig sein müsse. Dies kann logisch nur bei Kenntnis aller die Rechtswidrigkeit begründenden Umstände der Fall sein[1].
Unnötig verkompliziert wurde die Rechtslage vor der Novelle von TDG und MDStV im Jahr 2002 durch Versuche, deren Anwendungsbereich auf bestimmte Inhalte zu beschränken und die urheberrechtliche Verantwortung von der Privilegierung auszunehmen[2]; diese Ansätze haben durch

die Ersetzung von „Inhalten“ durch „Informationen“ in den §§ 7 ff**.** TMG ein Ende gefunden.
Die Rechtsprechung schien daher häufig weniger auf Wortlaut und Sinn des IuKDG, sondern mehr auf die Schaffung von zahlungsfähigen Haftenden fokussiert zu sein, da die primär Verantwortlichen auf Grund der möglichen Anonymität in der Regel nicht zu finden sind oder, speziell im Bereich des Urheberrechts, die hohen Schadensersatzsummen nur selten aufbringen können. Diese Unauffindbarkeit war allerdings auch Intention des Gesetzgebers, der als Teil des IuKDG das TDDSG mit sehr restriktiven Datenschutzvorschriften verabschiedet hat, die jetzt in den §§ 11-15 TMG enthalten sind. Sie schließen eine Speicherung von Daten zur Identifikation der Nutzer aus; eine Speicherung von Nutzerdaten, auch zum Zweck der Aufklärung von Eingriffen in die Rechtssphäre Dritter, ist demnach nicht zulässig, und ein genereller Auskunftsanspruch liegt bisher nicht vor.
Insgesamt scheint die Rechtsprechung von dem Gedanken geleitet, dass insbesondere Host-Provider – zu denen nach der hier vertretenen Ansicht sowohl Anbieter von Internet-Versteigerungen als auch Forenanbieter zählen – allein aus dem Grund für eine künftige Unterlassung zu haften hätten, dass diese Dritten die Möglichkeit geben, Rechtsverletzungen zu begehen. Sie beachtet hierbei aber nicht, dass eine adäquate Überwachung kaum zu leisten ist. Auf den Offline-Bereich übertragen, käme dies einer Rechtsprechung gleich, dass Eigentümer öffentlich zugänglicher Räume dafür zu haften hätten, dass zukünftig in ihren Räumen keine Rechtsverletzungen mehr geschähen. Außerhalb des Internets gibt es eine derartige, schlicht als absurd zu bezeichnende, Unterlassungshaftung nicht.

g. Haftung von Suchmaschinenbetreibern

Das Problem beim Auffinden von Informationen im Internet besteht heutzutage nicht mehr in der Verfügbarkeit von Informationen, sondern darin, diese Informationen auch zu finden. Dies ist

1Christiansen, MMR 2004, 185, 186.
2OLG München MMR 2001, 375ff.

entweder durch die Kenntnis der genauen URL oder durch eine gezielte Suche nach bestimmten Stichworten möglich. Für Letzteres werden Suchmaschinen benötigt. Ohne sie gilt eine „sinnvolle Nutzung der unübersehbaren Informationsvielfalt im WWW als praktisch ausgeschlossen“[1].

Suchmaschinen stellen innerhalb von Sekundenbruchteilen zu vom Nutzer eingegebenen Suchbegriffen Listen mit Links von Angeboten zusammen, in denen die gesuchten Stichworte enthalten sind, und gewichten diese nach ihrer Relevanz. Sie generieren derlei Listen aus einem Verzeichnis, das sie automatisch beim Durchsuchen von Angeboten mit spezialisierten Programmen[2] erhalten und auf darin vorkommende Stichworte und Querverbindungen auswerten. Somit bieten Suchmaschinen technisch gesehen nichts anderes als Links, die sie allerdings – anders als Inhalteanbieter – notwendigerweise automatisch erstellt haben. Daher ist fraglich, ob sie denselben Haftungsregeln wie Inhalteanbieter für Links unterstehen. Auf der anderen Seite ist auch die Bedeutung von Suchmaschinen für das Auffinden von Inhalten – und damit die Funktionsfähigkeit des Internets für den Nutzer – sowie die Möglichkeit der Verantwortlichkeit von Suchmaschinenbetreibern für eigene Rechtsverstöße zu beachten.

(1.) Haftung für eigene Rechtsverstöße

Durch das Durchsuchen von Informationen und das Setzen von Links auf diese Informationen können Suchmaschinen vor allem gegen Urheberrechte verstoßen. Ein Rechtsverstoß scheidet allerdings, selbst bei Deep-Links[3], aus, weil durch das Veröffentlichen der Inhalte eine Einwilligung in die Verlinkung vermutet wird[4], wenn der Anbieter keine technischen Vorkehrungen gegen das Durchsuchen trifft[5]. Es scheint auch denkbar, dass Suchmaschinen in Zukunft zumindest für die Entfernung rechtsverletzender Textausschnitte, so genannte Snippets, in den Suchergebnissen haftbar werden[6]. Schuster schlägt dazu vor, eine Haftung nur dann zuzulassen, wenn Snippets mehr beinhalten als die reine Wiederholung des Inhalts des Suchergebnisses[7].

1BGH AfP 2003, 545ff. – Paperboy.

2So genannte Robots.

3Links, die nicht auf die Eingangsseite eines Angebots verweisen, sondern nur auf die konkret gesuchte Information. Das ist für den Suchenden angenehmer, schafft für den Anbieter aber Probleme, weil dadurch Werbung, die auf den Eingangsseiten vorhanden ist, nicht angezeigt wird und so die Einnahmen geschmälert werden.

4BGH AfP 2003, 545ff. – Paperboy.

5BGH AfP 2003, 545ff. – Paperboy. Für Suchmaschinen wird eine Datei „robots.txt“ angelegt, in der beschrieben werden kann, welche Teile durchsucht werden dürfen. Diese Praxis wird allgemein von Suchmaschinen akzeptiert.

6OLG Hamburg, CR 2007, 330 hat dies zwar abgelehnt, allerdings lässt die Ablehnung noch genügend Spielraum für zukünftige Klagen. Die Haftung für rechtsverletzende Snippets ist dadurch jedenfalls noch nicht ausgeschlossen.

7Schuster, CR 2007, 443, 446.

(2.) Haftung für fremde Rechtsverstöße

Bei von Suchmaschinen gelisteten, fremden Informationen handelt es sich entweder um Werbung, die je nach eingegebenem Suchbegriff angezeigt wird (z.B. Google AdWords) oder um Inhalte, die verlinkt werden, wenn sich der gesuchte Begriff in den Inhalten befindet.

Der Unterschied zwischen beiden Arten der Information besteht darin, dass der Betreiber der Suchmaschine notwendigerweise Kenntnis von den Inhalten der Werbung haben muss, während dies bei Antworten auf Suchanfragen nicht notwendigerweise der Fall ist. In der Regel wird der Betreiber einer Suchmaschine den größten Teil seiner Links inhaltlich nicht kennen.

Die Haftung für Rechtsverstöße in Anzeigen ist derzeit noch in Rechtsprechung und Literatur strittig: Teilweise wird sie bejaht[1], teilweise unter Berufung auf die Unzumutbarkeit der Kontrolle abgelehnt[2]. Die Diskussion dreht sich in der Regel darum, ob überhaupt ein Tatbestand der Störerhaftung in Betracht kommt und ob in diesem Falle die geforderte Handlung – in der Regel die Entfernung der rechtswidrigen Inhalte aus dem Katalog – für eine Suchmaschine zumutbar wäre; die Frage nach dem Bestehen einer Haftungsfreistellung nach TMG ist bisher unberührt geblieben.

Für die Haftungsbefreiung wird das TMG – wie auch hier vertreten – analog herangezogen. Überraschenderweise und wenig konsequent ist die Rechtsprechung bisher nicht regelmäßig zu einer Haftung von Suchmaschinen gekommen[3]. Die Ablehnung einer Haftung geschieht allerdings unter Verweis auf die Unzumutbarkeit der Prüfung der Suchergebnisse[4], was insofern begrüßenswert ist, als Suchmaschinen selbst nicht zu der Rechtsverletzung beitragen und auf Grund des Umfangs der Suchkataloge keine rechtliche Bewertung vornehmen können. Allerdings müssen die Suchmaschinen, auch wenn eine Prüfung unzumutbar ist, die beanstandeten Inhalte aus dem Suchkatalog entfernen. Das kann es praktisch unmöglich machen, die Inhalte zu erreichen, wenn die URL nicht bekannt ist.

Für eine Haftungsbefreiung für Anzeigen spricht die Rechtsprechung zum Pressehaftungsrecht, nach der Zeitschriften für rechtswidrige Anzeigen Dritter nur haften, soweit die Rechtswidrigkeit offensichtlich ist[5]. Dies ist allerdings – entgegen Teilen der Rechtsprechung[6] – dahingehend zu erweitern, dass eine Haftung nur bei Kenntnis der illegitimen Inhalte – die anders als bei Anzeigen in der

---

1LG Hamburg, Beschluss vom 14.11.2003, Az.: 312 O 887/03.

2LG München I, MMR 2004, 261, 262.

3Zuletzt OLG Hamburg, Urteil vom 20.02.2007, Az.: 7 U 126/06.

4OLG Hamburg, Urteil vom 20.02.2007, Az.:_7 U 126/06, KG Berlin, Urteil vom 10.02.2006, Az.: 9 U 55/05; LG Hamburg Urteil vom 16.09.2004, Az.: 315 O 755/03.

5BGH NJW 1972, 2302; NJW RR 1990, 1184, 1185.

6LG München I, CR 2001, 46, 47; LG Hamburg, Urteil vom 16.09.2004 Az.: 315 O 755/03.

Presse nicht zwangsläufig ist[1] – und bei offensichtlicher Rechtswidrigkeit gegeben ist[2]. Alles andere würde zu einer – nach § 7 II TMG nicht bestehenden – Kontrollpflicht führen, die außerdem als solche aufgrund der Menge der Anzeigen unzumutbar ist. Somit entspricht die Haftung der Suchmaschinen derjenigen von Inhaltsanbietern für Links analog § 10 TMG – ein auch aus technischer Sicht zutreffendes Ergebnis, da Suchmaschinen letztendlich nichts anderes als Links anbieten.

Die Versuche, eine Haftung für die Antwort auf Suchanfragen zu konstruieren, stellen sich in zweifacher Hinsicht als problematisch dar: Zum einen unterfallen die Suchmaschinen dem TMG und sind daher auch für die Verlinkung privilegiert, zum anderen ist die Zumutbarkeit einer Prüfungspflicht, die Voraussetzung für eine Haftung ist, mehr als fraglich, sie wird von der Rechtsprechung allerdings auch nicht kategorisch verneint. Im Wesentlichen nimmt diese eine Störerhaftung von normalen und von Metasuchmaschinen an, wenn die Zumutbarkeit der Entfernung der Suchergebnisse nicht verneint wird[3]. Eine einheitliche Aussage dahingehend, wann dies der Fall sein solle, ist bislang nicht erkennbar[4]. Der generelle Unterschied der Begründung der Ergebnisse liegt darin, dass Teile der Rechtsprechung sich auf die Zumutbarkeit einer Kontrolle im Einzelfall berufen und so zu einer Haftung gelangen[5], während andere eher auf die umfassende Kontrolle des gesamten Datenbestandes abstellen und daher in der Regel von einer Unzumutbarkeit ausgehen[6].

h. Medienrechtliche Verantwortlichkeit

Für mit herkömmlichen Medien vergleichbare Telemedien kommt ebenfalls eine Haftungsprivilegierung nach medienrechtlichen Regeln in Frage. Hierbei sind insbesondere presserechtliche Regelungen von Interesse, da über das Internet übertragene Inhalte diesen in der Regel am nächsten kommen.

Unter Presse sind neben den herkömmlichen Druckwerken wie Zeitschriften und Büchern auch Ton- und Bildträger und Disketten zu verstehen[7]. Der Pressebegriff ist entwicklungsoffen[8]; von zentraler

---

1Anzeigen werden bei Suchmaschinen nicht durch eine Anzeigenredaktion entgegengenommen und gesetzt, sondern online direkt vom Kunden eingegeben und bei entsprechendem Kontext der Suchanfrage eingeblendet.

2So auch OLG Hamburg, Urteil vom 20.02.2007, Az.: 7 U 126/06, allerdings nicht für Anzeigen und LG München, Urteil vom 02.12.2003, Az.: 33 O 21461/03 .

3So auch OLG Hamburg, CR 2007, 330, 331. Anders noch vorgehend LG Hamburg, Urteil vom 28.04.2006, Az.: 324 O 993/05.

4OLG Hamburg, Urteil vom 20.02.2007, Az.: 7 U 126/06: kein Unterlassungsanspruch; LG Berlin, Urteil vom 01.06.2006, Az.: 27 O 146/06: Störerhaftung der Suchmaschine; LG Frankenthal, Urteil vom 16.05.2006, Az.: 6 O 541/05: Keine Haftung wegen Unzumutbarkeit.

5Unter anderem: LG Berlin, Urteil vom 01.06.2006, Az.: 27 O 146/06; KG Berlin, Urteil vom 10.02.2006, Az.: 9 U 55/05; LG Regensburg, Urteil_vom 15.02.2005, Az.: 2 S 340/01 (1), 2 S 340/01.

6LG Frankenthal, Urteil vom 16.05.2006, Az.: 6 O 541/05; LG Hamburg, Urteil vom 16.09.2004 Az.: 315 O 755/03.

7Fechner, Rn. 448; Jarass/Pieroth-Jarass, Art. 5 Rn. 25.

8Jarass/Pieroth-Jarass, Art. 5 Rn. 25.

Bedeutung ist die Eignung und Bestimmung der Druckwerke zur Verbreitung[1], nicht die Art der Vervielfältigung[2]. Auch andere Kriterien wie Auflagenstärke oder Verbreitungsgrad sind nicht zulässig[3]. Daher fallen elektronische Medien – sofern sie diese Voraussetzungen erfüllen und der herkömmlichen Presse funktionell entsprechen – ebenfalls unter den Begriff der Presse[4], selbst wenn sie keine Druckwerke sind. Dies entspricht der Abgrenzung zwischen Medien- und Telediensten[5] anhand des Kriteriums der „redaktionellen Bearbeitung zur Meinungsbildung“[6]. Die genannten Faktoren sowie die zunehmende Konvergenz der Medien und die damit verbundenen Abgrenzungsschwierigkeiten sprechen für eine funktionelle Gleichstellung von Neuen Medien und Presse und damit für die Einordnung aller Mediendienste als „Presse“ im Sinne des Art. 5 GG.
Sofern andere „herkömmliche“ Medien nur über das Internet übertragen werden, gelten die spezifischen Regelungen dieser Medien[7]; sofern – beispielsweise in Homepages oder Blogs – „lediglich“ individuelle Meinungen geäußert werden, ist allein die Meinungsfreiheit nach Art. 5 I GG einschlägig, da es sich bei Eingriffen gegen bestimmte Inhalte in der Regel nicht um Eingriffe gegen das gesamte Blog bzw. die gesamte Homepage handelt.

(1.) Anwendbarkeit im Internet

Die allgemeineren medienrechtlichen Regelungen könnten durch spezielle Regelungen des TMG verdrängt werden; diese modifizieren zwar nur die allgemein geltenden Haftungsregeln im Hinblick auf bestimmte Personenkreise, anstatt selbst Regelungen festzulegen, jedoch gilt Selbiges auch für die – größtenteils von der Rechtsprechung entwickelten – Regelungen des Medienrechts. Eine Haftung im Bereich des Medienrechts setzt zunächst eine generell bestehende Haftung voraus, die auch durch die allgemeineren Haftungsmaßstäbe des Medienrechts beeinflusst wird.
Zunächst ist zu klären, welche Arten von Internetangeboten unter welche speziellen medienrechtlichen Haftungsregeln fallen.
Per Internet verbreitete Angebote anderer Medien unterliegen den für den ursprünglichen Verbreitungsweg bestimmten Regeln; die Art der Verbreitung stellt hinsichtlich der Haftung keinen Unterschied dar. Wichtig hierbei ist allerdings, dass für eine Verbreitung im Internet gleichzeitig die internetspezifischen Verantwortungsregelungen gelten; die Besonderheiten dieses Mediums müssen beachtet werden.

1Jarass/Pieroth-Jarass, Art. 5 Rn. 25.
2Jarass/Pieroth-Jarass, Art. 5 Rn. 25.
3Sachs-Bethge, Art. 5 Rn. 68.
4Von Bonin, S. 94ff., a.A. Umbach/Clemens-Clemens, Art. 5 Rn. 69b, der auf die technische Art der Verbreitung abstellt.
5Statt Vieler: Hoeren, Recht der Access-Provider, Rn. 605.
6Statt Vieler: Hoeren, Recht der Access-Provider, Rn. 605.
7Fechner, Rn. 775.

Weniger eindeutig ist die Lage bei ausschließlich über das Internet verbreiteten Angeboten, die keine Entsprechung in anderen Medien haben, beispielsweise Homepages, Foren, Blogs und Newsgroups. Diese sind in der Regel wegen ihrer zumindest potentiell meinungsgestaltenden Funktion als Mediendienste zu werten[1], also nicht wie herkömmliche Medien zu behandeln. Aus Gründen der Rechtssicherheit werden Einzelfälle von Seiten der Betreiber zugunsten der generellen Anwendbarkeit kaum Relevanz erlangen, eher ist an Ausnahmen im Einzelfall zu denken.

(2.) Haftungsmaßstab

Der Haftungsmaßstab unterscheidet sich ebenfalls danach, ob es sich um eigene Informationen des Presseorgans oder um fremde Informationen handelt. Für eigene Informationen trifft den Verantwortlichen eine Störerhaftung. Deliktisch Haftende sind alle mit den rechtswidrigen Inhalten inhaltlich befassten Personen sowie andere mit der Verbreitung der Erzeugnisse befasste Personen; die strafrechtliche Haftung nach §§ 185ff. StGB trifft nur den für den Wortlaut direkt Verantwortlichen. Andere Normen, insbesondere §§ 86, 130 II, 130a, 131, 184 StGB, welche die Verteilung von Informationen regeln, treffen auch andere als die direkt für die Inhalte Verantwortlichen, beispielsweise Herausgeber und Verleger.

Im Internet dürfte dies aber aufgrund der Haftungsprivilegierungen relativ selten eintreten; die medienrechtliche Haftung für fremde Informationen ist grundsätzlich eine Haftung für unterlassene Kontrolle, woraus sich unterschiedliche Haftungsmaßstäbe ergeben.

(a.) Haftung für eigene Informationen

Im Bereich des Medienrechts existieren keine spezifischen Haftungsnormen, allerdings allgemeine Vorschriften, die vorwiegend an Medien gerichtet sind; außerdem sind grundsätzlich die Normen des Straf- und Zivilrechts anwendbar, insbesondere das nach § 823 I BGB in Verbindung mit Art. 2 I, 1 I GG geschützte Allgemeine Persönlichkeitsrecht (APR) und das Recht der informationellen Selbstbestimmung aus Art. 2 I GG, das in § 22 KUG verankerte Recht am eigenen Bild als Unterfall des APR, § 1004 BGB sowie Delikte, die in Verbindung mit der Verbreitung von Informationen stehen.

Diesen gegenüber steht an wichtigster Stelle Art. 5 GG, der für das Recht am gesprochenen Wort von der Rechtsprechung gebildete Rechtfertigungsgrund der überwiegenden Interessen der Allgemeinheit[2] sowie die Rechtfertigungsgründe der Wahrnehmung berechtigter Interessen des § 193 StGB. Dieser ist im Bereich der Presse ebenfalls anwendbar, wenn die Presseorgane allgemeine öffentliche Interessen verfolgen[3] und die Interessenabwägung ein Überwiegen öffentlichen Interesses ergibt. § 23 KUG kennt die Unterscheidung zwischen absoluten und

1Hoeren, Recht der Access-Provider, Rn. 605.

2Fechner, Rn. 162; BVerfGE 34, 238, 245f. für die Verwertung in Strafverfahren.

3Groß, Rn. 44; BVerfGE 12, 113, 125f.; BGHZ 31, 308, 312.

relativen Personen der Zeitgeschichte: Erstere müssen die Publikation von im öffentlichen Raum entstandenen Bildern grundsätzlich dulden, wenn die Aufnahme im Zusammenhang mit bedeutenden Ereignissen steht, während letztere eine Veröffentlichung von Abbildungen nur im Zusammenhang mit den Ereignissen und Personen dulden müssen, die sie zu Personen der Zeitgeschichte machen[1].

Des Weiteren können Vorschriften des Urheberrechts und des Wettbewerbsrechts anwendbar sein, wobei dort das so genannte Presseprivileg des§ 13 VI Nr. 1 S.2 UWG die Haftung für die Verbreitung irreführender Angaben auf vorsätzliches Handeln beschränkt.

(b.) Haftung für fremde Informationen

Fremde Informationen können in Presseorganen entweder als übernommene Berichte, Anzeigen oder Beilagen erscheinen. Im ersten Fall haftet das Presseorgan wie für eigene Informationen, wenn es sich diese zu eigen gemacht hat, was regelmäßig der Fall sein dürfte, wenn keine eindeutige Distanzierung vorliegt. Für den Anzeigenteil, auf den Presseorgane inhaltlich nur wenig Einfluss nehmen, besteht ebenfalls eine Haftung[2], die sich allerdings auf die Wahrung von Sorgfaltspflichten beschränkt[3], welche nicht so weitgehend sind wie jene für Verbreitung eigener Informationen, sondern lediglich eine Nachforschungspflicht bei Anzeichen für mögliche Rechtswidrigkeit der Informationen beinhalten[4].

i. Inanspruchnahme als Nichtverantwortlicher

Nach § 59 IV RStV können Access-Provider als Nichtverantwortliche nach dem Vorbild der Polizeigesetze der Länder in Anspruch genommen werden[5]. Unter den Voraussetzungen des § 59 IV RStV können die zuständigen Behörden Access-Provider verpflichten, den Zugang zu Inhalten zu sperren[6]. Eine Anwendung des RStV auf Access-Provider ist hierfür weder notwendig[7] noch – nach den Abgrenzungsregelungen des § 1 TMG und § 2 RStV – möglich.

§ 59 IV RStV entstand vor dem Hintergrund, dass Anbieter von (nach deutschem Recht) rechtswidrigen Inhalten diese vorzugsweise auf dänischen, niederländischen oder US-amerikanischen Servern lagern und ein Vorgehen deutscher Behörden gegen derartige Inhalte technisch

1Fechner, Rn. 171ff.; ein Urteil des EGMR lässt diese Unterscheidung für die Zukunft zweifelhaft werden.

2Groß, Rn. 56; BGH NJW 1972, 1658f.

3BGH NJW 1972, 1658f.

4BGH NJW 1972, 1658f.; Baumbach/Hefermehl, UWG, UWG Einl. Rn. 332.

5 Vgl. nur § 16 ASOG.

6Selbstverständlich benennt auch § 59 IV RStV nicht konkret Access-Provider, ist aber aufgrund seiner Zielsetzung kaum auf Andere anwendbar.

7So aber Matthies, S.43.

nur per Sperrung bei Access-Providern möglich ist. Er ist sehr weit gefasst und gibt die Möglichkeit, gegen jede Art von – nach deutschem Recht – rechtswidrigen Inhalten vorzugehen. Eine Beschränkung durch das Verhältnismäßigkeitsprinzip ist nach § 59 IV RStV nur insoweit gegeben, als die Anordnung für den Provider zumutbar sein muss, nicht jedoch hinsichtlich der Menge der Anordnungen und des Anlasses[1]. Ein solches Korrektiv könnte allerdings eine nicht im RStV geregelte Kostenerstattungspflicht mit sich bringen.

Einzelfragen

Nach der Regelung des § 59 IV RStV ist eine Sperrungsverfügung gegenüber Access-Providern zwar zulässig, darf jedoch nur Telemedien betreffen, die eine journalistisch-redaktionelle Gestaltung haben, da die §§ 54 ff. RStV nur auf derartige Telemedien anwendbar sind und sich § 59 IV RStV seinem Wortlaut nach nur auf Verstöße gegen die Vorschriften des sechsten Abschnitts des RStV bezieht. Eine Differenzierung gestaltet sich danach zwar einfacher als bei der Frage der Unterscheidung von Tele- und Mediendiensten nach TDG und MDStV, ist aber auch nicht immer trennscharf möglich. Dies hätte hinsichtlich der Frage der Entschädigung indessen keine praktische Bedeutung, wenn für Sperrungsverfügungen nach § 59 IV RStV die Entschädigungsregelungen der Polizeigesetze analog anzuwenden wären, da für die übrigen Telemedien mangels spezieller Regelung im TMG die Ordnungsgesetze der Länder eine Eingriffsmöglichkeit gegen Provider als Nichtverantwortliche geben: Damit bestünden identische Regelungen mit identischen Rechtsfolgen.

Die Sperrungsanordnung gegen XS4ALL

Die erste Sperrungsanordnung wurde 1996 gegen deutsche Provider mit dem Ziel erlassen, die auf dem Server des niederländischen Providers „XS4ALL“ befindlichen Seiten der Zeitschrift „Radikal“ zu sperren. Auf diesen Seiten befand sich eine Anleitung zum Bau von so genannten Hakenkrallen, die, wenn sie auf Oberleitungen im Bahnnetz geworfen und von Zügen erfasst werden, zur Zerstörung der Oberleitung und zur Unterbrechung des Bahnbetriebs führen. Dies ist strafbar nach § 315 StGB. Es wurde eine Anordnung erlassen, dass der Server, auf dem sich die Seiten von „Radikal“ befanden, durch Entfernung der IP-Adresse aus der DNS-Datenbank der deutschen Access-Provider zu sperren sei. Der Erfolg war zweifelhaft: Die Seiten von „Radikal“ wurden auf anderen Servern gespiegelt, während tausende legale Angebote auf dem betroffenen Server nicht erreichbar waren.

Die „Düsseldorfer Sperrungsverfügung“

Nach dem Gesetzeswortlaut ist eine Sperrungsanordnung nur zulässig, soweit sie dem Provider zumutbar ist. Dies bezieht sich sowohl auf die Frage, ob überhaupt eine Sperrungsanordnung

1Schätzungen des Regierungspräsidiums Düsseldorf gingen zur Zeit der Sperrungsanordnung davon aus, dass ca. 6000 Seiten, die rechtsradikale Inhalte enthielten, abrufbar seien.

erlassen werden darf, als auch auf die Mittel zu ihrer Umsetzung; eine präzise Beschreibung der zu wählenden Mittel fand sich in § 22 III MDStV (und im wortgleichen § 59 IV RStV) nicht.
In dem bisher einzigen Fall nach Inkrafttreten des IuKDG wurden den Providern das zu erreichende Ziel sowie drei Möglichkeiten der technischen Umsetzung vorgegeben; die Vorgehensweisen der Provider – und dementsprechend der erzielte Erfolg – variierten.

(a.) Sperrung der IP-Adresse

Wie bereits beim Fall der Sperrungsanordnung gegen XS4ALL konnten die Provider dem Beschluss durch die für sie kostengünstigste Vorgehensweise, nämlich die Sperrung der IP-Adresse der Server, nachkommen. Es zeigten sich jedoch dieselben Nachteile: Der Einsatz eines Anonymizers, durch den die Inhalte von einem anderen Server als dem tatsächlichen Absender zu kommen scheinen, ermöglicht, diese Sperrungsmethode ohne besondere technische Kenntnisse zu umgehen.

(b.) DNS-Manipulation

Eine andere, ebenfalls sehr kostengünstige Sperrungsmethode besteht in der Manipulation des DNS-Servers des Providers, so dass Anfragen zu den betreffenden Domains entweder mit einer Fehlermeldung beantwortet oder zu einer anderen Adresse umgeleitet werden. Diese Methode ist durch die Benutzung eines anderen – bevorzugt im Ausland befindlichen – DNS-Servers zu umgehen.

(c.) Einsatz von Filtersystemen

Es ist auch möglich, den Zugang zu Inhalten zwar zu erlauben, diese aber auf dem Server des Access-Providers zu filtern: Hierfür werden alle von dem Server, auf dem sich die zu sperrenden Inhalte befinden, gesendeten Datenpakete zunächst an einen Proxy-Server weitergeleitet und dort auf bestimmte Kriterien, also konkrete Worte oder Zeichen, untersucht. Werden diese nicht gefunden, werden die Pakete an den Empfänger ausgeliefert, andernfalls erscheint eine Fehlermeldung oder ein Hinweis auf die Sperrung. Zwar kann auch diese Methode umgangen werden, jedoch stellt sich dies deutlich komplizierter dar als die Umgehung einer IP-Sperrung. Andererseits ist die Einrichtung der für diese Filterung notwendigen Proxy-Server wesentlich teurer als die Sperrung von IP-Adressen oder die Manipulation des DNS-Servers; die mit den Sperrungen verbundenen Kosten werfen die Frage nach Kostenerstattungsansprüchen der Provider auf.

(d.) Kostenerstattung

Hinsichtlich der Frage der Kostenerstattung ergab sich zunächst ein widersprüchliches Bild. Für die Sperrung von (in der Regel ausländischen) Telediensten galten mangels Spezialregelung im TMG die Polizeigesetze, die für die Inanspruchnahme Nichtverantwortlicher Kostenerstattungsansprüche vorsahen.

Für die Sperrung von Mediendiensten durch Nichtstörer ist hingegen die landesrechtliche Norm des § 59 IV RStV einschlägig, da es nicht auf die Einordnung des Providers ankommt, dem gegenüber die Anordnung ausgesprochen wird, sondern auf die Einordnung des zu sperrenden Angebotes.

Nach der Nassauskiesungsrechtsprechung des BVerfG[1] ist die Auferlegung von Sonderopfern grundsätzlich zulässig, jedoch nur, wenn sie mit einer Entschädigungsregelung verbunden ist. Ein Sonderopfer liegt in der Durchführung der Sperrungsanordnung zweifellos vor[2]. Eine Entschädigungsregelung enthält der RStV jedoch ebenso wenig wie zuvor der MDStV, was angesichts der deutlichen Anlehnung an die Regelungen zur Inanspruchnahme Nichtverantwortlicher in den Ordnungsgesetzen der Länder und die der Verabschiedung des TMG vorausgegangene Diskussion mehr als verwunderlich ist. Dies hätte nach der Nassauskiesungsrechtsprechung des BVerfG die Verfassungswidrigkeit des § 59 IV RStV zur Folge. Auch die Begründung lässt eine Auseinandersetzung mit der Problematik vermissen. Um eine Verfassungswidrigkeit der Vorschrift zu vermeiden, sind daher die Entschädigungsregelungen des Ordnungsrechts des jeweiligen Landes anzuwenden[3]. In diesem Zusammenhang entsteht jedenfalls in der vom Regierungspräsidium Düsseldorf gewählten Form der Sperrungsverfügung[4] ein Problem durch die Auswahl der Sperrungsmethode. Wegen der Unbestimmtheit der Mittel könnte das Regierungspräsidium den Schadensersatzforderungen entgegenhalten, dass die Provider eine unnötig aufwändige und kostenintensive Methode gewählt hätten. Dies stünde jedoch im Widerspruch zu dem Ziel der möglichst effektiven Zugangsverhinderung und führte auch die Wahlmöglichkeit ad absurdum. Daher muss das Regierungspräsidium die konkret durch eine der vorgeschlagenen Maßnahmen entstandenen Kosten ersetzen.

Einerseits entsteht durch die Entschädigungsansprüche der in Anspruch genommenen Provider ein Korrektiv der Anwendung der Vorschriften durch die zu erwartenden Kosten, so dass die Inanspruchnahme Nichtverantwortlicher die Ausnahme bleiben und wohl nur bei schwerwiegenden

1BVerfGE 58, 300ff.

2So auch Volkmann, S.223.

3So auch Volkmann, S.222. Alternativ könnte man auch auf den gewohnheitsrechtlichen Aufopferungsanspruch zurückgreifen. Sähe man die Vorschrift deshalb als verfassungswidrig an, wäre die Rechtsgrundlage für eine Sperrungsverfügung die Generalklausel des jeweiligen Polizeirechts, so dass die Entschädigungsregelungen Anwendung fänden. So auch Engel, MMR Beilage I/2003.

4Das Regierungspräsidium hat den Access-Providern mehrere, unterschiedlich kostenintensive und wirksame Wege der Zugangsverhinderung zur Auswahl gegeben. S.u. S.76f.

Verstößen in Frage kommen wird, andererseits sind die – nach der Einrichtung von Filter-Proxies – entstehenden Kosten zu vernachlässigen, so dass sich die zuständigen Behörden angeregt sehen könnten, die in den Aufbau der Filterstruktur getätigten „Investitionen“ auch effektiv zu nutzen und auch andere Seiten ähnlichen Inhalts mittels Sperrverfügungen unerreichbar zu machen. Dies ist bislang jedoch nicht geschehen.

Suchmaschinen als Adressaten von Sperrungsverfügungen?

Aufgrund der Vielzahl der über das Internet erreichbaren Angebote sind Suchmaschinen für den Nutzer notwendige Dienste für eine effektive Nutzung des Internets geworden[1]; die Entfernung eines Angebots aus den Datenbanken einer Suchmaschine käme der Entfernung des Angebots nahezu gleich. Somit stellen Suchmaschinen einen möglichen Ansatzpunkt für regulierende Eingriffe des Staates dar; denkbar wäre etwa, diese – wie bereits bei Access-Providern üblich – nach § 59 IV RStV zur Sperrung von Angeboten durch deren Entfernung aus ihren Verzeichnissen zu verpflichten. Dieses Vorgehen könnte bezüglich der Zielsetzung der Sperrungsverfügung, Interessenten von rechtswidrigen Inhalten abzuhalten, größere Erfolge zeitigen als eine bloße Sperrung der Inhalte beim Access-Provider.

Selbst wenn man die Anwendbarkeit von § 59 IV RStV auf Suchmaschinen für gegeben hielte, müsste eine Sperrung den Suchmaschinen jedoch auch möglich und zumutbar sein; nach nach einem Urteil des LG Frankfurt[2] gilt dies allerdings wegen der wichtigen Funktion der Suchmaschinen, dem hohen öffentlichen Interesse an ihrer Funktionstüchtigkeit und dem zu erwartenden hohen Aufwand im Regelfall als ausgeschlossen. Es handelt sich hierbei um eines der seltenen Urteile, in denen explizit die wichtige Funktion eines Akteurs für die Nutzung des Netzes genannt wird und daraus rechtliche Konsequenzen gezogen werden.

Sperrungsverfügungen gegen Rundfunk im Internet?

Sperrungsverfügungen nach § 59 IV RStV können nach dessen Wortlaut wegen Verstößen gegen „die Vorschriften“ gegenüber Providern ausgesprochen werden, wenn Maßnahmen gegen die Verantwortlichen nicht erfolgversprechend sind. Da sich § 59 IV RStV im sechsten Abschnitt befindet, der sich ausschließlich mit inhaltlichen Anforderungen an Telemedien befasst, kann sich auch die Vorschrift des § 59 IV RStV nur auf die Sperrung von Telemedien wegen Verstößen gegen die Regelungen des sechsten Abschnitts beziehen.

1LG Frankfurt, CR 2002, 219, 221.

2LG Frankfurt CR 2002, 220, 221.

Nach den übereinstimmenden Regelungen von § 1 I TMG und § 2 I 3 RStV sind Telemedien als elektronische Informations- und Kommunikationsdienste definiert, die nicht Rundfunk sind; daher kann Rundfunk nicht gleichzeitig unter den Begriff der Telemedien fallen. Bei Rundfunk ist es nach der Definition von § 2 I RStV aber nicht ausgeschlossen, dass er über das Internet verteilt wird[1]. Somit ist eine Sperrung von über das Internet übertragenem Rundfunk nach § 59 IV RStV nicht möglich, da es sich nicht um Telemedien handelt. Maßgebliches Unterscheidungsmerkmal zwischen Rundfunk und Telemedien ist nicht der Verbreitungsweg, sondern das Merkmal der individuellen Abrufbarkeit (Telemedien) bzw. der universellen Aussendung (Rundfunk). Ein Streamingverfahren, bei dem die Daten kontinuierlich übertragen werden, wie es bei Internetradios die Regel ist, ist auch als Rundfunk zu qualifizieren.

Denkbar wäre allenfalls eine Sperrung nach den Vorschriften über die Inanspruchnahme Nichtverantwortlicher nach den Polizeigesetzen der Länder; es stellt sich aber die Frage, ob diese überhaupt auf per Internet verteilten Rundfunk anwendbar sind oder ob der RStV, insbesondere § 59 IV RStV, eine abschließende Regelung darstellt.

Zunächst ist ein Eingriff aufgrund der Polizeigesetze der Länder nicht schon deshalb ausgeschlossen, weil ein Verstoß gegen ein allgemeines Gesetz im Sinne des Art. 5 I 2 GG vorliegen muss: Zwar ist eine ordnungsrechtliche Sperrungsverfügung kein Gesetz im Sinne des Art. 5 I 2 GG, der Grund für den Erlass einer Sperrungsverfügung wird jedoch in der Regel ein Verstoß des Rundfunkveranstalters gegen ein allgemeines Gesetz sein. Eine Intervention auf Grund der Vorschriften zur Inanspruchnahme Nichverantwortlicher ist allerdings ausgeschlossen, weil es sich bei den Direktiven des RStV um eine abschließende Regelung handelt. Anläßlich des neunten Rundfunkänderungsstaatsvertrags wurde die bisherige Regelung des § 22 III MDStV als § 59 IV in den RStV übernommen und gleichzeitig die nach § 2 I MDStV noch bestehende Anwendbarkeit der Regelungen von Telemedien auf Rundfunk, der ebenfalls unter die Definition von Mediendiensten nach § 2 I MDStV fiel, ausgeschlossen, indem Rundfunk vom Begriff der Telemedien in § 1 I TMG und § 2 I 3 RStV ausgenommen wurde. Für Telemedien wurde die Regelung des § 59 IV RStV geschaffen, im Bereich des Rundfunks gab es kein entsprechendes Reglement; es bestand hierfür allerdings auch keine Notwendigkeit[2]. Ob diese Lücke dem Gesetzgeber bewusst war, lässt sich anhand der Begründung nicht erkennen. Ein Lückenschluss per Analogie zu § 59 IV RStV ist jedenfalls nicht möglich, da dieser nur für Telemedien gelten soll. Eine Anwendung auf Rundfunk ist ausdrücklich ausgeschlossen. Gleiches gilt für eine Anwendung des Ordnungsrechts, da der RStV eine in sich abgeschlossene Sonderregelung bildet. Dies wird allein daraus ersichtlich, dass

1So auch die Begründung zum TMG, BT Drs. 16/3078, S.13.

2Grenzüberschreitender Rundfunk kann entweder nicht wie Telemedien durch eine Sperrungsverfügung an der Übertragung gehindert werden oder es ist möglich, dem Veranstalter in Deutschland bei schweren Verstößen die Lizenz zu entziehen.

mit den Landesmedienanstalten für die Rundfunkaufsicht spezielle, staatsferne Gremien geschaffen wurden: Diese Gestaltung ist von Art. 5 GG vorgegeben und würde untergraben, wenn zusätzlich die Ordnungsbehörden der Länder eingreifen könnten. Auch § 59 IV RStV wäre in diesem Falle unnötig.

Zusammenfassung

Der Gedanke, der bei der Haftung im Internet leitend sein sollte, ist der, dass es keinen Unterschied machen darf, ob Inhalte über das Internet veröffentlicht und verbreitet werden oder ob dies auf herkömmlichem Wege geschieht. Dieser Grundgedanke ist auch richtig, eine Differenzierung wäre nur sinnvoll erklärbar, wenn die Eigenarten des gewählten Mediums dazu zwingen.

Eine einheitliche Bewertung ist für den Inhalt selbst recht unproblematisch. Schwierig wird es bei der Bewertung der Tätigkeit derjenigen, die nicht selbst die Inhalte bereitstellen, sondern lediglich anderen Speicherplatz für Inhalte bieten oder den Transport dieser Inhalte übernehmen. Dabei ist zunächst das TMG Richtschnur für die Regelungen der Verwantwortlichkeit. Dazu muss die Tätigkeit des jeweiligen Beteiligten unter die Regelungen des TMG subsumiert werden. Dies geschieht schon häufig nicht bzw falsch.

Ist eine Tätigkeit nicht im TMG erwähnt böte es sich an, nach parallelen Tätigkeiten bei der Veröffentlichung herkömmlicher Medien zu suchen und deren Verantwortlichkeit auf die Provider zu übertragen.

Voraussetzung für eine einheitliche Bewertung dieser Tätigkeiten ist, dass den Tätigkeit der Provider entsprechende Tätigkeiten bei herkömmlichen Inhalten zugeordnet werden. Wird weder sauber unter die Tätigkeiten nach dem TMG subsumiert noch nach vergleichbaren Tätigkeiten in herkömmlichen Medien gesucht entsteht ein Sonderrecht, nicht für Inhalte, sondern für Provider. Mit dem Grundgedanken der einheitlichen Rechtslage hätte dieses Ergebnis aber nicht mehr viel gemeinsam.

Eine einheitliche, widerspruchsfreie Rechtslage ließe sich auf dieser Grundlage im Einklang mit den geltenden Gesetzen herstellen. Der Ausgangspunkt muss die Betrachtung der Tätigkeit der Beteiligten sein. Für die nicht im TMG geregelten Fälle bietet sich ein Vergleich mit den entsprechenden Tätigkeiten bei vergleichbaren herkömmlichen Medien an.

Das Ergebnis wäre, dass die rein technischen Beteiligten an der Datenübermittlung nur unter sehr eingeschränkten Voraussetzungen – in der Regel bei positiver Kenntnis der Rechtswidrigkeit der Handlungen und der Inhalte – verantwortlich wären. Eine Störerhaftung mit Überwachungspflichten wäre dann ausgeschlossen. Das entspricht auch der Regelung des § 7 II TMG, nach der es keine Überwachungspflichten für fremde Inhalte gibt, dies verhindert jeglichen Unterlassungsanspruch für

die Zukunft. Genau das gleiche gilt für Telekommunikationsgesellschaften, die auch nur gezwungen werden können, missbräuchlich genutzte Telefonanschlüsse abzuschalten während die Betreiber von Fernsehsendern überhaupt keiner Haftung für Inhalte unterliegen, obwohl sowohl die Tätigkeiten von Senderbetreibern als auch von Telekommunikationsgesellschaften durchaus den Tätigkeiten von Access-Providern gut vergleichbar sind.

Für die Tätigkeit von Host-Providern fehlt eine Entsprechung bei herkömmlichen Medien. Nach § 10 TMG ist eine sie sind aber Anzeigenabteilungen bei Zeitschriften am ähnlichsten, da auch diese in der Regel nur eine Plattform für fremde Inhalte bieten. Dabei wäre aber zu beachten, dass das Aufkommen an Daten bei Host-Providern um ein vielfaches größer ist und dass deshalb eine Überwachung des Datenbestandes auch auf Grund der Störerhaftung aus Gründen der Unmöglichkeit der Überwachung ausscheidet.

Daraus resultiert, dass Forenbetreiber, die selbst nur eine Plattform für die Äußerung fremder Meinungen bieten, nur unter den genannten Voraussetzungen für diese haftbar sind oder wenn sie sich diese zu eigen und damit fremde Meinungen zu ihren eigenen machen. Das letztere dürfte praktisch aber die absolute Ausnahme sein. Das bloße Angebot eines Forums kann jedenfalls noch nicht zu einer Haftung führen. Bei Sachverhalten, die keinen Internetbezug aufweisen, ist eine Haftung nur wegen der Möglichkeit, dass Dritte rechtswidrige Aktivitäten entfalten, jedenfalls unbekannt.

Auch die Haftung für Links und von Suchmaschinen ergibt sich damit quasi von selbst. Auch Suchmaschinen und Linksetzer sind nur unter den Voraussetzungen von § 10 TMG für fremde Inhalte verantwortlich, für eine Differenzierung zwischen ihnen gäbe es auch keinen in den Regelungen des TMG liegenden Grund. Eine Ausnahme gilt lediglich auf Grund von § 7 I TMG, wenn sich der Anbieter die Inhalte zu eigen macht und damit die Fremdheit aufhebt.

Schon an der grundlegenden Voraussetzung der Subsumtion unter die im TMG geregelten Sachverhalten scheitert die Rechtsprechung mitunter. Anders ist es nicht zu erklären, wieso in Urteilen zur Haftung von Forenbetreibern keinerlei Ausführungen zu den Privilegierungen des TMG enthalten sind.

Auch bei der Suche nach vergleichbaren Sachverhalten bei herkömmlichen Medien scheitert die Rechtsprechung, es wird in der Regel überhaupt nicht nach vergleichbaren Tätigkeiten gesucht, obwohl sie sehr wohl vorhanden sind.

Nach den Vorschriften des TMG und deren Auslegung durch die Rechtsprechung sind technische Beteiligte an der Datenübermittlung nur in Ausnahmefällen für Rechtsverletzungen durch die übermittelten oder angebotenen Daten verantwortlich. Dieser im Gesetz so klar dargelegte Grundsatz erfuhr im Laufe der Zeit einige Aufweichungen durch die Rechtsprechung.

Nachdem die Rechtsprechung anfänglich keinerlei Verantwortlichkeit der Host-Provider für Daten Dritter angenommen hat, gilt nach mittlerweile gefestigter Rechtsprechung eine Haftung über den Umweg der zivilrechtlichen Störerhaftung. Diese wird damit zu einem unkalkulierbaren Risiko für Host-Provider, da eine Überwachung des Inhalts auf rechtswidrige Inhalte nahezu unmöglich und in jedem Fall unzumutbar ist. Ungeklärt ist bisher nur das Verhältnis zwischen dem Anspruch auf Unterlassung zukünftiger Störungen, der nur durch eine Überwachung von Inhalten zu realisieren ist und § 7 II TMG, der explizit feststellt, dass keine Überwachungspflicht für fremde Inhalte existiert. Nach der hier vertretenen Meinung besteht demnach kein Anspruch auf eine selbständige Entfernung von rechtswidrigen Inhalten durch Provider. Es ist aber zu befürchten, dass die Rechtsprechung wieder dem allgemeinen Zivilrecht den Vorzug vor den Regelungen des TMG gibt. Damit besteht die Gefahr, dass die Provider aus Angst vor wirtschaftlichen Risiken durch Klagen und Unterlassungsverfügungen die Meinungsfreiheit durch vorauseilenden Gehorsam zu einer Karikatur schrumpfen lassen, wenn schon die bloße Behauptung von Rechtsverletzungen dazu führt, dass Inhalte gelöscht werden, die bei denen lediglich die Möglichkeit besteht, dass sie rechtswidrig sind.

Eine Korrektur der Ergebnisse dieser Rechtsprechung ist nur durch das Merkmal der Zumutbarkeit möglich. Die Zumutbarkeit einer Überwachung bezieht die vorherrschende Rechtsprechung jedoch nur auf den jeweiligen Einzelfall. Unbeachtet bleibt dabei aber, dass die Überwachung von einzelnen Fällen zwar für sich jeweils keinen unzumutbaren Aufwand bedeutet, die Gesamtsumme der zu überwachenden Inhalte aber immer weiter steigt und die Überwachung dadurch unzumutbar wird. Im Ergebnis wird eine Überwachung im Einzelfall nur in seltenen Ausnahmefällen unzumutbar sein.

Die direkte Haftung nach den Ausnahmen von der Privilegierung des § 10 TMG steht noch vor vielen offenen Fragen, die aber angesichts des Vorherrschens der Störerhaftung praktisch nur geringe Relevanz haben. Nach der hier vertretenen Auffassung ist eine Haftung von Host-Providern für die Inhalte Dritter nur möglich, wenn sie sowohl positive Kenntnis der Inhalte als auch von deren Rechtswidrigkeit hatten. Für Schadensersatzansprüche sind nach § 10 I 2.Alt TMG lediglich die positive Kenntnis der Inhalte sowie die positive Kenntnis der Umstände, aus denen die Rechtswidrigkeit erkennbar wird, erforderlich.

Bei der Haftung für Forenbetreiber wird eine Privilegierung nach dem TMG inzwischen gar nicht mehr erwähnt, es gilt scheinbar die Regel, dass derjenige, der Dritten die Möglichkeit bietet, rechtswidrige Äußerungen zu tätigen, auch für deren Äußerungen haftet, unabhängig davon, ob er sie kennt oder teilt. Ein Grundsatz, der beispielsweise auf Gastronomen angewendet, für großes

Erstaunen und Kopfschütteln sorgen würde, wird im Internet ohne jeden Normbezug etabliert. Auch hier wird ein Sonderrecht geschaffen.

Nachdem die Rechtsprechung bis zur Novellierung im Jahre 2002 zumindest teilweise eine Privilegierung für das Setzen von Links angenommen hat, hat sich die herrschende Meinung komplett gewandelt, obwohl sich der Gesetzestext nicht verändert hat und auch die Begründung nicht erkennen lässt, dass eine Haftung vom Gesetzgeber gewollt war und ist. Die flexible Lösung, die auf der Grundlage der Haftung von Zugangsvermittlern danach differenziert hat, ob der Anbieter sich die verlinkten Inhalte zu eigen gemacht hat oder nicht, ist gegenüber der generellen Haftung vorzugswürdig, da eine Überwachung und rechtliche Bewertung fremder Inhalte wohl unmöglich, in jedem Fall aber unzumutbar ist.Dies entspräche auch der Rechtsprechung im Presserecht, wo in der Regel auch keine Haftung für Rechtsverstöße, erst recht nicht durch Dritte, besteht. Die Fortführung der früheren Rechtsprechung ist jedenfalls auch mit dem geltenden Wortlaut des TMG möglich, allerdings kaum gewollt. Die einzige Lösung kann eine Novellierung des TMG bringen, die auch im Rahmen der Überarbeitung von EU-Richtlinien erfolgen wird.

Problematisch wird in Zukunft wohl auch die Haftung von Suchmaschinen werden, die anfangs weitestgehend privilegiert wurden, inzwischen aber immer häufiger auch unter der Störerhaftung zur Entfernung von Links aus ihrem Angebot verpflichtet. Auch das ist bedenklich, weil es einerseits die Rechtswidrigkeit nicht beseitigt, andererseits aber den Zugang zu den Inhalten wesentlich beeinträchtigt. Um dies zu erreichen wird inzwischen auch versucht, das Wettbewerbsrecht einzusetzen, was insofern gefährlich ist, als dass dabei in der Regel hohe Streitwerte anfallen, die es wirtschaftlich erscheinen lassen können, auch wahrscheinlich rechtmäßige Inhalte zu entfernen, da die Anbieter entfernter Inhalte kaum eine Möglichkeit haben, Rechtschutz gegen die Suchmaschinen zu erlangen.

Die öffentlich-rechtliche Haftung als Nichtstörer, zunächst auf Grund von § 22 III MDStV, der jetzt in § 59 IV RStV übernommen wurde, hat anfangs für große Aufregung gesorgt, die sich inzwischen als unberechtigt herausgestellt hat. Obwohl die meisten durch die Sperrungsverfügungen des Regierungspräsidiums Düsseldorf aufgeworfenen Fragen inzwischen gerichtlich geklärt sind ist es bei diesem Einzelfall geblieben, die Relevanz ist gegenüber der zivilrechtlichen Störerhaftung verschwindend gering. Dies dürfte ein Resultat der Kostenerstattungspflich analog der Polizeigesetze der Länder sein. Als neues Randproblem ist durch die Übernahme von § 22 III MDStV in den RStV aufgetreten, dass Radiostationen, die nach deutschem Recht unzulässige Inhalte über das Internet verbreiten, nicht mehr Gegenstand von Sperrungsverfügungen sein können.

III. Jugendschutz

Der Jugendschutz stellt bereits seit Beginn der rechtlichen Beschäftigung mit dem Internet ein zentrales Thema im Bereich der staatlichen Einflussnahme auf Inhalte, die über das Internet zugänglich sind, dar. Dem scheint vielfach die alte Annahme des „Rimm-Reports“[1] zugrunde zu liegen, dass die über das Internet zugänglichen Inhalte voller „Schmutz“ seien und Jugendliche allenthalben auf „harte Pornographie“, Pädophile, Nazis und Gewaltdarstellungen träfen. Diese Inhalte existieren zwar, werden aber wohl in der öffentlichen Berichterstattung übertrieben dargestellt. Vieles ist nicht ohne intensivere Suche auffindbar oder wenig anziehend gestaltet[2]. Dennoch nimmt der Jugendschutz, gerade aufgrund des öffentlichen Interesses und seiner fundamentalen Bedeutung, eine zentrale Stellung bei der gesetzgeberischen Aktivität im Bereich der Inhalte ein, einhergehend mit seiner traditionell wichtigen Rolle im Gefüge der Verfassung[3]. Verankert im elterlichen Erziehungsrecht in Art. 6 Abs. II Satz 1 GG und in der Menschenwürde in Art. 1 Abs. I in Verbindung mit Art. 2 Abs. 1 GG, verpflichtet der Jugendschutz den Staat, eine äußere Umgebung zu gewährleisten, die für eine dem Menschenbild des Grundgesetzes entsprechende geistige Entwicklung notwendig ist[4]. Dies gilt auch für den Bereich der Neuen Medien und den Bereich des Internets[5]. Jedoch gestaltet sich hier die Kontrolle, anders als bei Zeitschriften, Videos oder Computerspielen (sofern die beiden letzteren nicht über das Internet vertrieben werden), ungleich schwieriger, da der Konsument dem Anbieter nicht als Person gegenübersteht, sondern lediglich Daten abruft und seine Identität sowie sein Alter nicht ohne zusätzliche Maßnahmen überprüft werden können. Um die in diesem Kontext vorhandenen Probleme, vor allem hinsichtlich divergierender Regelungen, der schwierigen Abgrenzung von Tele- und Mediendiensten und den daraus resultierenden unterschiedlichen Kompetenzen[6], zu lösen, wurden die zuvor im JÖSchG und GjSM bestehenden Regelungen des Jugendschutzes am 1.4.2003 vom Jugendmedienschutzstaatsvertrag (JMStV) und Jugendschutzgesetz abgelöst, was auch eine Anpassung des Rundfunkstaatsvertrages mit sich brachte.

Im Bereich der Beleidigungsdelikte, der Pornographie – insbesondere § 184 c StGB – und der rechtsradikalen Propaganda hat auch das StGB Einflüsse auf das Internet.

1Eine Kopie des Reports (das Original ist nicht mehr online verfügbar): http://www.sics.se/~psm/kr9512-001.html, unter: http://www.eff.org/Censorship/Rimm_CMU_Time/time_cyberporn.articleshttp://www.eff.org/Censorship/Rimm_CMU_Time/time_cyberporn.articles befindet sich eine frei zugängliche Kopie des auf dem Rimm-Report basierenden Artikel des Time-Magazine.

2Wer beispielsweise die auf Betreiben des Regierungspräsidiums Düsseldorf gesperrten Internet-Seiten betrachtet hat, wurde davon – schon aufgrund der wenig gelungenen graphischen Gestaltung – wohl eher abgeschreckt als angezogen.

3 Eberle/Rudolf/Wasserburg-Landmann, VI, Rn.1.

4 BVerfG NJW 1987, 1429,1430.

5 Eberle/Rudolf/Wasserburg-Landmann VI, Rn.1.

6 Eberle/Rudolf/Wasserburg-Landmann VI, Rn.3.

Dessen Regelungen sind gegen Ersteller und Bezieher gerichtet; Eingriffe bei anderen Beteiligten wären wirkungslos, da die Betroffenen ja aufgrund der Kriminalisierung Inhalte und Urheber der Kommunikation verbergen.

Da das Internet lediglich einen anderen Verbreitungsweg verbotener Inhalte darstellt, unterscheiden sich die Regelungen nicht von den Wirkungen auf herkömmliche Medien und sind insofern kein Untersuchungsgegenstand.

1. Geltung des JMStV

Nach § 2 I JMStV gilt der JMStV für Rundfunk und für Telemedien. Diese gesetzgeberische Neuschöpfung umfasst sowohl Tele- als auch Mediendienste[1], für die im nahezu zeitgleich novellierten TDG und MDStV noch unterschiedliche Gesetze bei weitgehender inhaltlicher Übereinstimmung für nötig gehalten wurden. Die Neuschöpfung des JMStV wurde mittlerweile im Telemediengesetz berücksichtigt; die (Neu-)Schöpfung des Begriffs und die Zusammenfassung von Tele- und Mediendienstregelungen werfen allerdings die Frage auf, warum für den Tele- und Mediendienstbereich statt der noch im Jahre 2002 novellierten TDG und MDStV nicht schon eine gemeinsame Regelung möglich war[2].

2. Persönlicher Anwendungsbereich

Nach § 2 I JMStV gilt dieser für Anbieter von Rundfunk und Telemedien. Der Terminus der Telemedien ist zwar – anders als noch die Begriffe der Teledienste und Mediendienste im TDG bzw. MDStV – nicht genauer bestimmt, jedoch kann davon ausgegangen werden, dass die zuvor definierten Tele- und Mediendienste unverändert als Telemedien gelten. Eine Ausnahme bilden, wie auch im TMG, Anbieter von Telekommunikation. Durch die Weite des Begriffs „Telemedien“ sind allerdings nicht nur Inhaltsanbieter, sondern potentiell auch alle anderen Anbieter, insbesondere von Telediensten, umfasst, also auch reine Host- und Access-Provider. Dies kann einerseits zu einer Kollision mit den Verantwortlichkeitsregelungen des TMG, andererseits zu Problemen bei der Umsetzung der Verpflichtungen des JMStV führen. Um derlei Problemen entgegen zu wirken, gilt es zunächst, den persönlichen Anwendungsbereich des JMStV zu umreißen.

Internet-Cafés werden vereinzelt vom Anwendungsbereich ausgenommen[3]. Soweit sie aber Zugang zum Internet anbieten, sind sie Anbieter von Telemedien und somit gleichermaßen vom persönlichen Geltungsbereich des § 1 I TMG als auch des JMStV umfasst; auch eine vorherrschende andere Geschäftstätigkeit wie etwa das Angebot von Computerspielen spricht nicht gegen eine Anwendung des JMStV.

---

1 Grapentin, CR 2003, 458, 458.

2Die ECRL, auf der die Neufassung von TDG und MDStV beruhten, differenziert nicht zwischen Tele- und Mediendiensten.

3Nikles/Roll/Spürck/Umbach, § 3 JMStV Rn. 6, etwas unklar.

a. Geltung für Inhaltsanbieter

Inhalteanbieter sind nach § 7 I TMG für ihre eigenen Inhalte voll verantwortlich, so dass keine Probleme hinsichtlich des Verhältnisses zwischen TMG und JMStV bestehen.

b. Geltung für Host- und Access- Provider

Der JMStV gilt für alle Anbieter von Telemedien und somit auch für Host- und Access-Provider. Für diese sehen die §§ 8-10 TMG eine gestufte Verantwortlichkeit vor. Nach § 2 III JMStV jedoch bleiben die Regelungen des TMG „im Übrigen“ unberührt.

Der JMStV sollte eine Modernisierung der jugendschutzrechtlichen Bestimmungen des MDStV und der weiteren Jugendschutzgesetze leisten[1]; sie wurden mit seinem Inkrafttreten aufgehoben. Nach den Vorstellungen des Gesetzgebers stehen die Regelungen von TMG und JMStV mithin nicht in einem Konkurrenzverhältnis. Fraglich ist jedoch – wie noch zu zeigen sein wird –, ob das Verhältnis zwischen den Pflichten nach JMStV und den Verantwortlichkeitsregeln des TMG auch für die von §§ 4 II 2, 5 I JMStV normierten Pflichten gelten kann.

3. Pflichten nach dem JMStV

Der JMStV ist seiner Konzeption nach auf Inhalteanbieter zugeschnitten. Diese dürfen die in §§ 4, 5 JMStV aufgezählten Angebote weder in Telemedien noch im Rundfunk verbreiten oder zugänglich machen.

Die Aufzählung des § 4 I JMStV entspricht weitestgehend den bereits nach dem StGB verbotenen Inhalten. Nach § 4 II 2 JMStV gelten die in Satz 1 genannten Angebote in Telemedien als zulässig, wenn sie in geschlossenen Benutzergruppen verfügbar sind. In § 5 JMStV werden Angebote aufgelistet, die Jugendlichen nicht zugänglich gemacht werden dürfen, im Übrigen aber keinen Beschränkungen unterliegen.

Durch die Weite des Begriffs „Telemedien“ sind jedoch neben den Inhaltsanbietern auch Host- und Access- Provider umfasst[2], die nach dem Wortlaut der §§ 4, 5 JMStV ebenfalls verpflichtet wären, Jugendlichen den Zugriff auf entwicklungsbeeinträchtigende Angebote unmöglich zu machen oder wenigstens deutlich zu erschweren. Bevor auf die den verschiedenen Anbietern obliegenden Pflichten eingegangen werden kann, ist zunächst die Terminologie zu klären.

---

1 Begründung zu § 2 III JMStV.

2 Grapentin, CR 2003, S. 458, 461.

a. Zugänglich Machen und Verbreiten

Voraussetzung für die Anwendung des § 5 JMStV ist, dass Anbieter Telemedien „zugänglich machen“ oder „verbreiten“. Dabei ist der Begriff des zugänglich Machens anhand der in § 3 TDG a.F. bzw. § 3 MDStV a.F. verwendeten Definition, also als ein „den Weg öffnen“ zu verstehen[1]. Allerdings wird nicht deutlich, weshalb der Gesetzgeber nicht auf die Begrifflichkeit der gleichzeitig novellierten Fassungen von TDG und MDStV, die unverändert in das TMG übergegangen ist, zurückgegriffen hat.

Generell – aber nicht ausschließlich – bestimmt sich die Abgrenzung zwischen Telemedien einerseits und Rundfunk andererseits nach der Form der technischen Verbreitung, also danach, ob es sich ihrer Art nach um Individual- oder Massenkommunikation handelt. Diese Differenzierung folgt aus den unterschiedlichen Gesetzgebungszuständigkeiten der Art. 70ff. GG, wonach die Verantwortlichkeit für Individualkommunikation (Telekommunikation, Art. 70 GG) beim Bund und diejenige für Massenkommunikation bei den Ländern liegt. Die Abgrenzung von Telemedien und Rundfunk ergibt sich aus § 1 TMG bzw. § 2 RStV.

Bei den Diensten des Internets ist insbesondere bei der Bereitstellung von Daten zum Abruf durch den Nutzer fraglich, ob es sich um Rundfunkdienste oder Tele- bzw. Mediendienste handelt. Auf dieser Unterscheidung bauen die Termini des „Verbreitens“ und „zugänglich Machens“ auf. Dabei sollen anscheinend nach dem Willen des Gesetzgebers Tätigkeiten aus dem Bereich des Rundfunks dem Begriff des „Verbreitens“ zuzuordnen sein und Telemedien dem Terminus des „zugänglich Machens“. Dies lässt allerdings den Status bestimmter Einzelanwendungen wie Push-Dienste oder E-Mail-Newsletter, die über das Internet verbreitet werden können, im Unklaren. Sowohl in den §§ 2 II Nr. 5 TDG, 2 II Nr. 4 MDStV als auch in § 47a RStV waren der Abruf von Inhalten von den jeweiligen Regelungen umfasst[2]. Die Regelfälle in TDG und MDStV sind jedoch im Zuge der Verabschiedung des TMG gestrichen worden, was die Abgrenzung zwischen Telemedien und Rundfunk im Zeitalter konvergierender Medien nicht unbedingt klarer gestaltet hat.

Allerdings bedarf die Qualifikation eines Mediendienstes als Rundfunk gemäß § 20 II RStV der Zustimmung aller Landesmedienanstalten. Damit steht fest, dass Mediendienste in der Regel nicht als Rundfunk zu werten sind, wenn sie nicht (schon) die Definition des Rundfunks erfüllen. Dies ergibt sich allerdings nicht aus den verwendeten Begriffen, sondern vor allem aus dem Zusammenhang des RStV und der Tatsache, dass Mediendienste in der Regel keine Meinungsmacht erreichen können, die der des Rundfunks gleichkommt[3] und daher auch keine Notwendigkeit einer strengen Regelung besteht. Diese inhaltlichen Kriterien haben indes keine Aussagekraft für die technischen Begriffe

1BT Drs. 13/7385, S.20.

2 Kröger/Gimmy-Moos, S.275ff.

3 Kröger/Gimmy-Moos, S.277.

des „zugänglich Machens“ und „Verbreitens“. Daher ist noch nicht sicher, ob Telemedienanbieter nicht auch Inhalte verbreiten, statt sie lediglich zugänglich zu machen.

(1.) Verbreiten

Nach §§ 74 d, 86 I StGB sowie §184 a.F. StGB ist ((das)) „Verbreiten“ das zugänglich Machen von Schriften nach § 11 StGB in körperlicher Form, so dass ein größerer Personenkreis vom Inhalt Kenntnis erlangen kann[1]. Für das Kriterium der Körperlichkeit genügen elektronische Datenspeicher[2]. Auch das Ausstrahlen von Rundfunksignalen, deren Inhalt körperlich gespeichert war, erfüllt den Tatbestand des Verbreitens[3]. Die von dem Kenntnis Nehmenden geforderte Handlung erfordert hier kein aktives Tun, nicht einmal tatsächliche Kenntnisnahme[4].

Diese Tatbestandsvariante ist offensichtlich auf den Rundfunk bzw. auf Verteildienste in Datennetzen zugeschnitten, bei denen der Nutzer, ähnlich wie beim Rundfunk, die Daten nicht anfordern muss, um eine Übertragung zu veranlassen. Im Internet gilt eine Verbreitung als erfolgt, wenn die entsprechende Datei auf dem Rechner des Nutzers gespeichert ist und dieser somit die Möglichkeit hat, Kopien anzufertigen[5]. Bei E-Mails hingegen ist es angebracht, die Verbreitung schon bei Speicherung auf dem Mailserver des Empfängers anzunehmen, da sich die E-Mail ab diesem Zeitpunkt in dessen alleinigem Zugriffsbereich befindet und für ihn die Möglichkeit des Herstellens von Kopien besteht; es existiert kein Grund einer Differenzierung zwischen der Speicherung auf einem Mailserver oder auf einer Festplatte.

Eine etwas andere Auslegung des „Verbreitens“ findet sich in § 186 StGB: Hier genügt die Weitergabe an eine einzelne Person. Aufgrund der durch das IuKDG erfolgten Änderung des § 86 I StGB, der an den Begriff des § 74 d StGB anknüpft[6], sowie der anders gearteten Schutzrichtung des § 186 StGB ist dessen Lesart des Begriffes „Verbreiten“ für den JMStV nicht anzuwenden.

Im Presserecht wird zwischen intellektuellem und technischem Verbreiten unterschieden. Ersteres liegt vor, wenn der Verbreitende eine eigene inhaltliche Beziehung zu der Äußerung von Dritten hat, es sich also um ein Zitat handelt, letzteres setzt keine gedankliche Verbindung voraus und umfasst den bloßen technischen Vorgang[7]. Für den JMStV ist diese Differenzierung nicht relevant, da

1Lackner/Kühl-Lackner, § 74d, Rn. 5; BGHSt 45, 325.

2Lackner/Kühl-Lackner, § 74d, Rn. 5.

3Lackner/Kühl-Kühl, § 184 Rn. 7; Tröndle/Fischer § 184 Rn. 22.

4Lackner/Kühl, § 74 d Rn. 5.

5BGHSt 47, 55, 60.

6Lackner/Kühl, § 86 Rn. 6.

7Wenzel, Rn. 100f.

sowohl Anbieter von Inhalten als auch technische Provider Adressaten sind; eine Verbreitung im Sinne des JMStV setzt mithin voraus, dass Inhalte in den Verfügungsbereich mehrerer Personen gelangt sind.

(2.) Zugänglich Machen

„Zugänglich Machen" umfasste nach § 184 I a.F. StGB die Möglichkeit der Kenntnisnahme ohne Verletzung von Rechtsnormen[1]. Diese liegt vor, wenn Materialien – etwa pornographische Darstellungen – in den Verfügungs- oder Wahrnehmungsbereich eines Jugendlichen geraten, so dass die konkrete und nahe liegende Option der unmittelbaren Kenntnisnahme besteht[2]; diese muss nicht am Ort des zugänglichen Schriftstücks erfolgen[3]. Nach dem KG ist eine solche Sachlage gegeben, „wenn eine Datei zum Lesezugriff ins Internet gestellt" worden ist[4]. Diese Definition ist nicht ganz exakt; gemeint ist wohl eher das Speichern und Freigeben der Datei auf einem Server mit Verbindung zum Internet. Diese Tatbestandsalternative ist erkennbar auf Angebote zugeschnitten, bei denen eine aktive Tätigkeit des Empfängers zur Kenntnisnahme erforderlich ist.

Nicht nur die Tätigkeit der Inhaltsanbieter, sondern auch die der

Access- und Hostprovider fallen unter den Begriff des Zugänglich Machens, da diese gleichsam dafür sorgen, dass Nutzer Kenntnis von Inhalten erlangen können. Ob Suchmaschinen Inhalte zugänglich machen, ist hingegen fraglich.

Die Abgrenzung zwischen zugänglich Machen und Verbreiten verläuft also nach dem zur Kenntnisnahme der Inhalte notwendigen Verhalten der Nutzer: Während beim Verbreiten die Haupttätigkeit bei dem Anbieter bzw. dem – nicht notwendig identischen – Verbreiter liegt und der Nutzer weitgehend passiv bleibt, erfordert das zugänglich Machen ein über das Anschalten des Empfangsgerätes hinausgehendes aktives Verhalten des Nutzers.

b. Verpflichtung zum Jugendschutz

Die von den Anbietern von Telemedien zu erfüllenden Anforderungen zum Schutz von Jugendlichen unterscheiden sich nach den verschiedenen Schutzstufen der §§ 4, 5 JMStV.

(1.) Schutzverpflichtung nach § 4 JMStV

In § 4 JMStV werden sowohl das vollständige Verbot von strafrechtlich unzulässigen oder in der Regel die Menschenwürde verletzenden Inhalten (Abs. I) als auch die beschränkte Zulässigkeit pornographischer Inhalte, von der BPjM indizierter Inhalte sowie von – terminologisch durchaus der

1Tröndle/Fischer § 184 Rn. 11.

2OLG Karlsruhe, NJW 1984, 1975, 1976; KG, Urteil vom 26.4.2004, abrufbar unter:
http://www.kammergericht.de/entscheidungen/5_Ss4_04.pdf, S.6f.

3Tröndle/Fischer § 184 Rn. 11.

4KG, Urteil vom 26.4.2004, abrufbar unter:
http://www.kammergericht.de/entscheidungen/5_Ss4_04.pdf.

Konkretisierung bedürftigen – sonstiger entwicklungsbeeinträchtigender Inhalte in Telemedien (Abs. II S. 1) geregelt. Letztere dürfen nicht über herkömmliche Medien verbreitet werden. Der Zugang in geschlossenen Benutzergruppen nach § 4 II 2 JMStV ist jedoch erlaubt und von strafrechtlicher Verantwortlichkeit ausgenommen.

Geschlossene Benutzergruppen zeichnen sich dadurch aus, dass – anders als bei gewöhnlichen Internet-Seiten – nur ein begrenzter Personenkreis Zugriff auf (die) Informationen hat. Dies wird in der Regel per Vergabe von Passwörtern und Benutzernamen sichergestellt, wie es beispielsweise E-Mail-Anbieter tun. Anders als bei diesen erhält allerdings nicht jeder Nutzer einen eigenen Bereich, sondern eine Nutzergruppe erhält gemeinsam Zugriff auf bestimmte gespeicherte Inhalte. Im Bereich des Jugendschutzes nach dem JMStV muss sichergestellt sein, dass nur Erwachsene Zugriff auf die Inhalte nehmen können. Nach den Vorstellungen des Gesetzgebers muss ein verlässliches System gegeben sein, das die Kenntnisnahme durch Jugendliche verhindert. Anders als im Offline-Bereich, für den die weitgehend parallele Regelung des § 1 IV in Verbindung mit §§ 12, 15 JuSchG existiert, kann die Kenntnisnahme durch Jugendliche nur durch technische Mittel, so genannte Altersverifikationssysteme, verhindert werden. Es sind technisch verschiedene Systeme mit unterschiedlichem Wirkungsgrad vorstellbar.

Exkurs: Sicherungssysteme für geschlossene Benutzergruppen

Auf dem Markt befinden sich derzeit verschiedene Arten von Sicherungssystemen, die garantieren sollen, dass nur berechtigte Nutzer Zugang zu den an geschlossene Benutzergruppen gerichteten Inhalten finden. In der Literatur werden unterschiedliche Kombinationen der genannten Sicherungssysteme vorgeschlagen.

1. Personalausweis- / Kreditkartennummergestützte Systeme

Derartige Systeme setzen die Eingabe der Nummer einer Kreditkarte – die gewöhnlich erst mit Volljährigkeit erlangt werden kann – oder einer Personalausweisnummer, aus der sich das Geburtsdatum berechnen lässt, voraus, bevor der Zugriff auf altersbeschränkte Inhalte freigegeben wird. Vor Inkrafttreten des JMStV wurden Systeme, die eine Altersverifikation durch Eingabe von Personalausweisnummern ermöglichten, teilweise als taugliche Möglichkeit zur Gewährleistung des Jugendschutzes gesehen[1]; in der Rechtsprechung wurden sie jedoch überwiegend abgelehnt[2]. Derlei Systeme haben den Nachteil, dass sie durch Eingabe von Nummern Dritter umgangen werden können; allerdings ist es möglich, Personalausweisnummern so zu speichern, dass sie nur von einer Person genutzt werden können – somit kann zumindest die Mehrfachnutzung von Nummern

1LG Düsseldorf, MMR 03, 418, 418; Berger MMR 03, 773ff.

2OLG Düsseldorf Urteil vom 17. Februar 2004 – III-5 Ss 143/03 – 50/03 I; KG Berlin, Urteil vom 26.4.2004, Az.: (5) 1 Ss 436/03 (4/04) – (571) 75 Js 46/02 Ns (134/03).

verhindert werden. Die Annahme, dass Jugendliche diese Überprüfung durch Nutzung einer aus dem Internet bezogenen oder von ihren Eltern stammenden Nummer nicht umgehen würden, weil dies verboten ist[1], kann eher naiv genannt werden, zumal die Strafbarkeit der Umgehung strittig ist[2]. Eine Strafandrohung, die gegenüber nicht strafmündigen Jugendlichen in jedem Fall versagt, dürfte allenfalls dazu führen, dass Jugendliche sich inhaltlich identischen, jedoch kostenfreien Angeboten zuwenden.[3].

Nach einem Urteil des BGH[4] sind derartige Systeme nicht als für den Jugendschutz geeignet anzusehen.

2. X-Check / Vodafone

Basierend auf dem Post-Ident-Verfahren, verlangt dieses Sicherungssystem vom potentiellen Kunden, sein Alter bei der Deutschen Post überprüfen lassen. Daraufhin erhält er einen Zugangscode, mit dem er sich, in Verbindung mit einer Chipkarte, bei altersbeschränkten Angeboten identifizieren kann[5]. Hierbei ist ein Lesegerät für die Chipkarte notwendig. Das Vodafone-Verfahren beruht darauf, dass das Alter des Kunden bei Abschluss eines Mobilfunkvertrages überprüft wird und dieser sich auch über die Website von bspw. X-Check anmeldet und sich mittels Personalausweisnummer identifiziert. Seine Daten werden mit denen im Zentralrechner von Vodafone gespeicherten verglichen; bei einer Übereinstimmung erhält er eine PIN auf sein Handy, und die Abrechnung erfolgt später über die Mobilfunkrechnung.

Andere, ähnliche Systeme sind ebenfalls denkbar. Aufgrund der Natur von Telediensten scheidet aber eine Identifikation durch den Diensteanbieter selbst in der Regel aus rein praktischen Erwägungen aus. Es können nur Systeme zum Einsatz kommen, welche die Identifikation mit Hilfe eines Dritten vornehmen.

Das Problem dieser und ähnlicher Methoden liegt nicht auf der technischen Seite – sie dürften nur schwer zu umgehen sein –, sondern auf der tatsächlichen Ebene beim Schamgefühl der Nutzer, da bei diesen Vorgehensweisen die seitens der Nutzer gewünschte Anonymität bei der Nutzung von Telediensten wieder aufgehoben wird.

Ende Exkurs

1Berger, MMR 03, 773, 777.

2Liesching, MMR 2/04, VII, VIII; gegen Strafbarkeit KG Berlin Urteil vom 26.4.2004, Az.: (5) 1 Ss 436/03 (4/04) – (571) 75 Js 46/02 Ns (134/03).

3Spoerr/Sellmann, KR 2004, 367, 373.

4BGH, Urteil vom 18. Oktober 2007, Az: I ZR 102/05 – ueber18.de.

5MMR 12/2003, XVII, XVIII, www.x-check.de.

Die Voraussetzungen für die Anerkennung eines Altersverifikationssystems sind stark umstritten, auch die Rechtsprechung ist nicht immer einheitlich. Ungeklärt ist insbesondere, wie das Merkmal des „Sicherstellens“ in verschiedenen jugendschutzrechtlichen Regelungen zu verstehen ist und welche Anforderungen es an ein Altersverfikationssystem stellt.

(a.) Weite Anforderungen

Bei der Frage nach dem durch technische Lösungen zu fordernden Sicherheitsgrad sind nicht nur die Optionen der Fernhaltung Jugendlicher von gefährlichen Inhalten, sondern auch die Interessen der Anbieter zu beachten. Andernfalls werden die Anbieter in Staaten mit niedrigeren Standards ausweichen, wodurch die Verfügbarkeit der Inhalte aufgrund der globalen Natur des Internets unverändert bliebe. Das Resultat bestünde in einem theoretisch hohen Schutzniveau, das wegen der territorialen Grenzen des Rechts aber praktisch keinen Anwendungsbereich hätte. Es ist außerdem zu beachten, dass es keinerlei Erkenntnisse gibt, wie der „Genuss“ von pornographischem Material auf Jugendliche wirkt[1]; auch die Möglichkeit zur Erlangung wissenschaftlich tragfähiger Erkenntnisse dürfte durch die Natur der durchzuführenden Experimente ausgeschlossen sein[2]. Hieraus folgt eine Einschätzungsprärogative des Gesetzgebers[3]; ein Risiko der Beeinflussung ist jedenfalls nicht auszuschließen. Die Möglichkeit, potentiell jugendgefährdende Angebote aus dem Ausland abzurufen, darf vor diesem Hintergrund auch nicht zu einer Kapitulation des nationalen Gesetzgebers führen[4]. Für die Eignung der gesetzgeberischen Maßnahmen genügt es, wenn sie zu einer Verringerung der Gefährdung führen[5]. Die Forderung nach völlig zuverlässigen Systemen, wie sie in der Begründung zu § 4 II 2 JMStV und im Gutachten von Sieber anklingt, ist jedenfalls nicht zu realisieren; auch bei Verfahren mit einmaliger face-to-face Identifikation besteht die Möglichkeit der Umgehung oder des Fremdzugriffs durch technisch versierte Nutzer. Eine völlige Sicherheit wird daher zu Recht auch nicht gefordert. Wenn allerdings hohe Hürden zu einer effektiven Minderung des Jugendschutzniveaus führen, ist zwar dem Wortlaut des Gesetzes Genüge getan, erreicht wird aber ein dem Zweck des Gesetzes entgegengesetzter Effekt[6]. Dies gilt auch, wenn, wie behauptet, die Altersverifikationsmaßnahmen zu einem drastischen Umsatzrückgang der Anbieter führen, so dass die Anbieter sich gezwungen sehen, ins Ausland abzuwandern[7]. Die Annahme, dass

1Erdemir MMR 2/2004, I, VI; Spoerr/Sellmann, K&R 2004, 367, 375.

2Erdemir MMR 2/2004, I, VI. Jugendliche müssten genau den Materialien ausgesetzt werden, vor denen sie eigentlich geschützt werden sollen. Die Rechtswidrigkeit derartiger Studien ist offensichtlich.

3BVerfGE 83, 130, 140ff.

4Erdemir MMR 2/2004, I, VI.

5Erdemir MMR 2/2004, I, VI.

6So auch Spoerr/Sellmann, K&R 2004, 367, 374.

7http://www.heise.de/newsticker/meldung/41187

allein schon die Einführung von auf Personalausweisnummern basierenden Systemen einen Umsatzrückgang und die Abwanderung der Anbieter herbeiführe, ist indes nur schwer nachzuvollziehen, da derartige Systeme bereits vor dem Inkrafttreten des JMStV zur Anwendung kamen[1].

In jedem Fall kann sie, angesichts des aus Art. 6 II GG folgenden Auftrags zum Schutz der Jugend, nicht zu einem völligen Verzicht auf Jugendschutzmaßnahmen führen. Es bietet sich aber eine pragmatische Lösung an, auf deren Basis das deutsche Jugendschutzrecht seine Wirksamkeit behält und dennoch dem Wortlaut des JMStV genüge getan wird. Zu berücksichtigen ist auch, dass es in erster Linie die Entscheidung der Eltern ist, den Jugendlichen den Zugang zu Inhalten zu ermöglichen, die nicht für diese geschaffen sind. Daher ist eine Sicherung gegen die Weitergabe von Zugangsdaten wegen häuslicher Defizite nicht geboten. Die durch eine derartige gesellschaftliche Entwicklung drohenden Gefahren sind auf anderen Gebieten deutlich größer als im Internet. Es kann nicht Aufgabe des Staates sein, die fehlende Erziehung durch das Jugendschutzrecht zu ersetzen; er muss den Eltern aber ermöglichen, ihre Erziehungsbefugnisse auszuüben. Dazu bedarf es keines Schutzes gegen die Weitergabe von Zugangsdaten von kostenpflichtigen Diensten.

Bemerkenswert in diesem Zusammenhang ist die von Nikles verwendete Definition der Medienkompetenz[2], deren Grundannahme wohl weit verbreitet ist: Medienkompetenz wird als „Bewusstsein für die Gefährdungslagen und Fähigkeiten sowie Bereitschaft, durch pädagogische und technische Maßnahmen derartige Gefährdungen zu bekämpfen“ bezeichnet – hier scheint sich noch das vom Rimm-Report[3] geprägte Bild des Internets als ein hauptsächlich von Pornographie durchdrungenes Medium fortzusetzen. Notwendigkeit besteht indes hinsichtlich des Erwerbs von Fähigkeiten zum Umgang mit dem Medium Internet, nicht allein bezüglich der Fähigkeit zur Gefahrenerkennung. Ein nur auf Gefahren fokussiertes Verständnis von Medienkompetenz droht den Blick auf die durch die Technologie des Internets eröffneten Möglichkeiten der Kommunikation zu versperren – eine Gefahr, die für die Zukunft der Jugend wahrscheinlich schwerer wiegt als die Konfrontation mit pornographischen Inhalten auf deutschen Servern.

Eine Lösung einer vergleichbaren Konfrontationslage wurde vom Bundesverfassungsgericht im Bereich der Seeschifffahrt für das deutsche Tarifrecht in der Zweitregisterentscheidung[4] angewendet: Das BVerfG billigte eine Regelung, welche die Einschränkung des Tarifrechts auf deutschen Schiffen im sogenannten Zweitregister gewährt hatte, weil die Alternative in einer Abwanderung nahezu aller Reedereien aus Deutschland bestanden hätte. Entscheidungserheblich

1Auf einem derartigen System basiert der Fall des LG Düsseldorf, MMR 03, 418, 418.

2Nikles/Roll/Spürck/Umbach, § 4 JMStV, Rn. 34.

3S.o. S.85.

4BverfGE 92, 26ff.

war hierbei der Gedanke, dass das Interesse an einer schwächeren Wirkung der Grundrechte einem theoretisch hohen Schutz vorzuziehen sei, der aber zu der faktischen Unanwendbarkeit des Grundrechts führen würde.

Auch wenn das Interesse an einer deutschen Pornoindustrie nicht mit dem am Erhalt einer deutschen Handelsflotte gleichgesetzt werden kann, ist der Grundgedanke der Zweitregisterentscheidung dennoch auch für den Jugendschutz im Internet anwendbar. So bestünde die Möglichkeit, die Interessen aller Beteiligten zu berücksichtigen, so dass die deutsche Jugendschutzgesetzgebung Anwendung finden könnte, wenn die bereits vor dem JMStV bekannten, auf der Personalausweisnummer basierenden Systeme zusammen mit einer zweiten Verifizierungsstufe von der KJM anerkannt würden. Es wäre allerdings zu fordern, dass die Inhalte neben dem bloßen Abgleich der Personalausweisnummer zusätzliche Sicherheitsmechanismen anbieten, also kostenpflichtig sind[1], was in der Regel sowieso der Fall sein dürfte. Diese Systeme böten zwar nur einen vergleichsweise leicht zu umgehenden Schutz, allerdings hätte diese offensichtliche Lücke auch den positiven Effekt, Eltern deutlich zu machen, dass allein technische Schutzmaßnahmen den Schutz von Jugendlichen nicht gewährleisten können und dass der Schwerpunkt auf elterlichen und schulischen Maßnahmen zur Förderung der wohlverstandenen, nicht nur auf Gefahren fokussierten Medienkompetenz liegen muss. Ein lang andauernder, von den Erziehungsberechtigten unerwünschter Konsum von pornographischem Material wäre aufgrund der Kostenpflichtigkeit nicht zu befürchten. Damit wäre sowohl den Interessen der Anbieter als auch den aus dem Grundgesetz folgenden Anforderungen Genüge getan.

(b.) Stellungnahmen der Rechtsprechung

Aufgrund des kurzen Zeitraums, in dem der JMStV in Kraft ist, gibt es bisher – soweit ersichtlich – keine Urteile hinsichtlich der Frage der Sicherstellung des Zugriffs durch Erwachsene. Der BGH hat allerdings entschieden, dass das System von ueber18.de den Anforderungen des JMStV nicht genügt[2]. Es existiert ein Urteil des BVerwG zur Gewährleistung des alleinigen Zugriffs durch Erwachsene beim Pay-TV[3], das häufig als Grundlage für die Auslegung des § 4 II 2 JMStV verwendet wird und auf das sich auch die KJM beruft. Danach muss sich der Anbieter zunächst der Volljährigkeit des Kunden versichern und es muss ein zusätzlicher, im System angelegter Schutzmechanismus vorhanden sein[4]. Es soll nicht genügen, dass zusätzlich zu einer Personalausweiskontrolle noch ein Benutzername und eine PIN vergeben werden, da aufgrund von

1So wohl auch Spoerr/Sellmann, K&R 2004, 367, 373.

2BGH, Urteil vom 18. Oktober 2007, Az: I ZR 102/05 – ueber18.de.

3BVerwG NJW 2002, 2966ff.

4BVerwG NJW 2002, 2966ff.

potentiellen Defiziten im häuslichen Bereich nicht sichergestellt wäre, dass Jugendliche die betreffenden Inhalte nur in Anwesenheit verantwortungsvoller Erwachsener zur Kenntnis nähmen[1].
Des Weiteren existieren Urteile[2] zu § 184 StGB a.F. in Verbindung mit § 3 GjS, der allerdings nur Vorsorge für die Möglichkeit der Beschränkung auf Erwachsene fordert und insofern weniger restriktiv formuliert ist als § 4II 2 JMStV. Daher sind die letzteren Urteile nicht direkt auf die Auslegung von § 4 II 2 JMStV zu übertragen.

(c.) Vorschläge der Literatur

Ansatzpunkt für die Beurteilung der Tauglichkeit eines Jugendschutzsystems ist die Frage der Sicherstellung des Ausschlusses Jugendlicher. Wann diese Sicherstellung allerdings vorliegen soll, ist in der Literatur umstritten. Fest steht, dass keine absolute Zugangsverhinderung gemeint sein kann[3], da diese schon rein technisch unmöglich ist[4]. Es genügt, wenn die Schutzmaßnahmen den Zugriff Jugendlicher regelmäßig verhindern[5]. In der Literatur wird zumeist dem Pay-TV Urteil des BVerwG[6] gefolgt.
Auf diesem Urteil aufbauend, vertritt Ukrow, dass für die zweite Stufe der Zugangsverhinderung Kostenpflichtigkeit und Abrechnung per Konto-, Scheck-, oder Kreditkarte gegeben sein müssten[7].
Nikles fordert für die persönliche Überprüfung bei der Anmeldung die Vorlage eines Personalausweises, Kostenpflichtigkeit des Systems und Vorlage einer auf denselben Namen wie auf dem Personalausweis lautenden Scheck- oder Kreditkarte. Bei der Nutzung verlangt er eine Authentifizierung, die sicherstellt, dass der Nutzer auch wirklich die Person ist, die er vorgibt zu sein, beispielsweise per Hardware oder an Hardware gekoppelte Software[8], so dass eine Umgehung der Schutzmaßnahmen, abgesehen von einer technischen Überwindung, als ausgeschlossen gelten könne. Ein einfaches Passwort solle nicht ausreichen[9]. Man kann sich unschwer vorstellen, dass die meisten Nutzer derartige Systeme nicht akzeptieren und andere Angebote nutzen würden.
Liesching hingegen setzt für die Überprüfung, ob der angemeldete Nutzer auch mit dem tatsächlichen Nutzer identisch ist, auf eine zusätzliche Hardwarekomponente, die z.B. ein USB-Stick

1BVerwG NJW 2002, 2966, 2969.

2LG Düsseldorf, MMR 2003, 418ff, aufgehoben in der Revision durch OLG Düsseldorf, III-5 Ss 143/03 - 50/03 I, Urteil vom 17.02.04; BGH Az.: 1 StR 70/03, Urteil vom 22.05.03; KG Az.: Ss 436/03, Urteile vom 15./26.04.04; alle abrufbar unter http://www.jugendschutz.net.

3Nikles/Roll/Spürck/Umbach, § 4 JMStV Rn. 34, Schumann, Gutachten, S.13.

4Schumann, Gutachten, S.13.

5BVerwG NJW 2002, 2966, 2968; Nikles/Roll/Spürck/Umbach, § 4 JMStV Rn. 34.

6BVerwG NJW 2002, 2966ff.

7Ukrow, Jugendschutzrecht, Rn. 427ff.

8Nikles/Roll/Spürck/Umbach, § 4 JMStV, Rn. 35.

9Nikles/Roll/Spürck/Umbach, § 4 JMStV, Rn. 35.

oder ein sogenannter Dongle[1] sein könne[2] und nur für jugendgefährdende Angebote im Sinne des § 4 JMStV genutzt werden dürfe. Dies würde einem Urteil des OLG München zum Versand jugendgefährdender DVDs entsprechen, das eine Sicherstellung fordert, dass nur der Besteller auch tatsächlich die Waren erhält[3].

Sieber[4] und die KJM[5] vertreten die Ansicht, dass jegliche Umgehungsmöglichkeit zu einer nicht-mehr-geschlossenen Benutzergruppe führe. Der Anbieter müsse auch eine Weitergabe der Zugangsdaten durch seine Kunden an Dritte ausschließen. Dies ergebe sich aus der gegenüber dem Offline-Bereich gesteigerten Gefährlichkeit (der Angebote) wegen der Eröffnung einer Vielzahl von Angeboten. Nach Meinung der KJM ist damit ausgeschlossen, dass eine Kombination aus Passwort und PIN ausreiche.

Allein Schumann[6] und Spoerr/Sellmann[7] weichen von dem Leitbild der Pay-TV Entscheidung ab: Schumann hält es für ausreichend, wenn ein Angebot kostenpflichtig und dadurch – spätestens bei der Abrechnung – eine dauerhafte Nutzung durch Jugendliche ausgeschlossen sei[8]. Spoerr und Sellmann erachten außerdem eine einmalige Kostenpflicht zur Authentifizierung bei dem Anbieter des Altersverifikationssystems als ausreichend[9]. Diese Voraussetzungen sind auch schon bei dem – von einer sich festigenden Rechtsprechung[10] als nicht ausreichend bewerteten – auf Personalausweisnummern basierenden System von „ueber18.de“ erfüllt.

(2.) Schutzverpflichtung nach § 5 JMStV

Nach § 5 I JMStV sind die Anbieter von Telemedien verpflichtet, Jugendlichen den Zugang zu jugendgefährdenden Angeboten, die (aber) nicht die Gefährdungsschwelle des § 4 JMStV erreichen, mindestens wesentlich zu erschweren. Nach § 5 III JMStV kann dieser Pflicht entweder durch technische Maßnahmen oder durch eine zeitliche Verbreitungsbeschränkung genügt werden. Die wesentlich höheren Anforderungen des § 4 JMStV resultieren aus der Einschätzung des

---

1Eine eindeutig identifizierbare Hardwarekomponente, die sicherstellt, dass nur ein Nutzer an einem Rechner eine bestimmte Software nutzen kann.

2Scholz/Liesching, S. 209, Rn. 36ff.

3OLG München, Urteil vom 29.7.2004, Az.: 29 U 2745/04.

4Unveröffentlichtes Gutachten für Coolspot Germany, berichtet bei Schumann, Gutachten, S.9ff.

5Beschluss vom 18.6.2003.

6Schumann, Gutachten, abrufbar unter http://www.ueber18.de/gutachten.pdf.

7Spoerr/Sellmann, K&R 2004, 367, 373.

8Ukrow, Rn. 430.

9Spoerr/Sellmann, K&R 2004, 367, 373.

10BGH Az. 1 StR 70/03, Urteil vom 22.05.03; OLG Düsseldorf, III-5 Ss 143/03 - 50/03 I, Urteil vom 17.02.04; KG Az. Ss 436/03, Urteile vom 15./26.04.04.

Gesetzgebers, dass die dort genannten Inhalte ein wesentlich höheres Gefahrenpotential haben als die in § 5 JMStV genannten.

Die technischen Maßnahmen nach § 5 III JMStV werden in § 11 I JMStV konkretisiert. Danach genügt auch eine Programmierung der Angebote für anerkannte Jugendschutzprogramme. Die Anerkennung eines Jugendschutzprogrammes schließt das Risiko der Verwendung ungeeigneter Programme aus[1], eine Verwendung geeigneter, aber nicht anerkannter Programme dürfte jedoch ebenfalls zur Erfüllung der Pflicht aus § 5 I JMStV genügen, da dieser nur verlangt, dass die Jugendlichen die Inhalte üblicherweise nicht zur Kenntnis nehmen. Als überzogen kann daher die Auffassung gewertet werden, dass ausschließlich anerkannte Programme genutzt werden dürften[2]: Wesentlich ist nicht die Anerkennung, sondern die Eignung des Programms, da § 5 III Nr.1 JMStV nicht von einer Anerkennung, sondern nur von dem herbeizuführenden Erfolg spricht. Es ist allerdings anzunehmen, dass die Hersteller der geeigneten Programme sich um eine Anerkennung bemühen werden.

Jugendgefährdende Inhalte nach § 5 I JMStV müssen entweder für Jugendschutzprogramme programmiert werden, d.h., dass beim Nutzer installierte Jugendschutzprogramme eine Filterung vornehmen können, oder ihnen müssen vom Anbieter Jugendschutzprogramme vorgeschaltet werden. Anders als bei geschlossenen Benutzergruppen nach § 4 II 2 JMStV ist kein doppelseitiger Schutzmechanismus auf Anbieter- und Nutzerseite notwendig.

Neben praktischen Schwierigkeiten, welche die verschiedenen Ansätze mit sich bringen, bestehen auch rechtliche Bedenken gegen den flächendeckenden Einsatz von Jugendschutzprogrammen.

(3.) Anforderungen an Jugendschutzprogramme

Die Anforderungen für die Anerkennung von Jugendschutzprogrammen sind in § 11 III JMStV niedergelegt: Danach müssen diese einen nach Altersstufen differenzierten Zugang zu Inhalten ermöglichen oder „vergleichbar geeignet“ sein.

Exkurs: Jugendschutzsysteme

1. PICS

PICS ist ein vom W3C entwickelter Standard, der es unter anderem ermöglicht, Inhalte für Jugendschutzprogramme zu kennzeichnen. Diese Kennzeichnung wird in einem vorher festgelegten Format in die Datei geschrieben[3] oder auf einem externen Server abgelegt. Dadurch wird es dem Browser oder einem dem Browser vorgeschalteten Programm auf dem Rechner des Anwenders möglich, Dateien nach vorher definierten Kriterien zu filtern. Die heraus gefilterten Daten werden dann zwar

1 Grapentin, CR 03, 458, 460.

2So aber Nikles/Roll/Spürck/Umbach, § 5 JMStV, Rn. 9.

3In den so genannten Header, der nicht angezeigt wird und Angaben über die Datei enthält.

auf den Rechner übertragen, jedoch nicht auf dem Bildschirm angezeigt. Mit diesem Verfahren wird es möglich, Inhalte abstrakt zu beschreiben, was nicht nur für Zwecke des Jugendschutzes nutzbar ist. Diese abstrakten Beschreibungen können automatisch von Computerprogrammen ausgewertet werden, was wesentlich weniger Schwierigkeiten bereitet und weniger fehlerbehaftet ist als eine Suche nach im Text vorkommenden Worten. Damit wird es auch möglich, Datenpakete bereits auf ihrem Weg durch das Netz, z.B. in Gateways, heraus zu filtern, ohne eine relativ rechen- und damit zeitintensive Analyse des Inhalts auf Stichworte durchführen zu müssen; gleichsam ermöglicht diese Methode auch eine Kennzeichnung zu anderen Zwecken als zum Jugendschutz, beispielsweise um den Zugriff auf politisch missliebige Inhalte zu verhindern.

Technisch unterstützt wird ein derartiges Verfahren derzeit nur vom Internet-Explorer (den, mit abnehmender Tendenz, ca. 80 % der Nutzer verwenden); alle anderen Browser wären, um Informationen filtern zu können, auf zusätzliche Programme angewiesen. Eine Strategie zur technischen Umsetzung der Kennzeichnung wurde von der Internet Content Rating Association (ICRA)[1] entwickelt und deren Anerkennung bei der KJM beantragt: Hierbei beantwortet der Webmaster Fragen aus einem – (nur) auf Jugendschutzfragen abgestimmten – Katalog und erhält ein Label bzw. kann die Angaben des Labels in den Header der Seite eingeben. Die konkreten Werte des Labels sind für den Inhalteanbieter nicht sichtbar; sie werden auf dem ICRA-Server gespeichert.

Mit anderen Fragenkatalogen und Filtern ist es möglich, bestimmte oder nicht gekennzeichnete Inhalte zu blockieren. Als Schutz gegen eine Falschkategorisierung fungiert ausschließlich ein Entzug des Labels bei Eingang von Beschwerden beim Labelaussteller. Um sinnvoll funktionieren zu können, müssen von den Filterprogrammen des Nutzers nicht nur Webseiten mit bestimmten Kategorisierungen, sondern auch Webseiten ohne Kategorisierungen gefiltert werden, da andernfalls der Zugriff auf jugendgefährdende Inhalte aus dem Ausland unbegrenzt möglich und das System damit weitgehend sinnlos wäre.

Es geht hier also um aus zwei Komponenten bestehenden Systeme, nämlich einer Kennzeichnung der Inhalte von Anbietern sowie einer Filtersoftware, die nach vorgegebenen Kriterien anhand der Kennzeichnung eine Filterung vornimmt.

2. Filterprogramme

Anders als PICS-basierte Kontrollprogramme existieren auf dem Markt bereits eine Reihe von – vornehmlich dem amerikanischen Raum entstammenden – Jugendschutzprogrammen. Ihnen ist in der Regel gemein, dass sie auf einer Kombination aus Blacklists[2] und Whitelists[3] beruhen. Letztere

1Http://www.icra.org.

2 Listen, die verbotene Domains und Zeichenfolgen enthalten, die daraufhin für den Rechner nicht abrufbar sind.

3 Whitelists beinhalten Seiten, die trotz unzulässiger Stichwörter angezeigt werden dürfen, z.B. AIDS-Aufklärungsseiten, auf denen

sind in der Regel vom Erziehungsberechtigten veränderbar, während Blacklists gemeinhin dem „Know-how“ der Hersteller zugehörig sind und von diesen geheim gehalten werden. Eine eher erheiternde Art von Fehlfunktion zeigte das von British Telecom verwendete Programm „Cleanfeed“, durch das man relativ unproblematisch gezielt nach den gesperrten Seiten suchen konnte.

Listenbasierte Filterprogramme werden im Allgemeinen für ungeeignet gehalten[1], da sie einerseits keinen, für eine Anerkennung notwendigen, nach Altersgruppen gestuften Zugang erlauben und andererseits – was gravierender ist – von zweifelhafter Effizienz und Zuverlässigkeit sind. Untersuchungen haben ergeben, dass – mit wechselnden prozentualen Anteilen – ein größerer Teil der bedenklichen Inhalte nicht gefiltert wird, während ein bedeutender Anteil der gefilterten Inhalte eigentlich unbedenklich ist[2]. Vor diesem Hintergrund kann bezweifelt werden, ob derartige Programme überhaupt in der Lage sind, einen wirksamen Beitrag zum Jugendschutz zu leisten [3]. Eine Besserung ist wohl nicht in Sicht.

Ende Exkurs

(a.) Technische Umsetzung

Technisch erfordert ein effektives Jugendschutzprogramm, das den Anforderungen des § 11 JMStV genügt, zwei Komponenten, eine auf Anbieterseite, eine auf Nutzerseite. Auf der Anbieterseite ist eine Bewertung der Inhalte, entweder durch neutrale dritte Bewertungsstellen oder die Anbieter selbst, notwendig. Auf der Nutzerseite ist ein Programm erforderlich, das die Bewertungsinformationen erkennen und dementsprechend Jugendlichen den Zugriff auf Inhalte verwehren kann. Dieses Programm muss einfach installier- und handhabbar sein, damit auch technisch unerfahrene Erziehungsberechtigte die notwendigen Einstellungen eigenständig vornehmen können, sowie vor dem Zugriff Jugendlicher geschützt sein. Es muss Zugriffe auf jugendgefährdende und nicht bewertete Seiten unterbinden und die Möglichkeit einer „Whitelist“ enthalten, in der unbewertete Angebote aufgeführt sind, die aufrufbar bleiben sollen.

(b.) Praktische Kritik

Bei der Bewertung von Angeboten ist mit Problemen zu rechnen. Die moralischen Vorstellungen neutraler Bewertungsstellen werden nicht zwangsläufig mit denen der Erziehungsberechtigten übereinstimmen. Eine Alternative bildet die Bewertung durch mehrere Stellen – in der Diskussion waren Kirchen, Jugendschutzverbände, Branchenverbände etc. –, jedoch bleibt zu beachten, dass nicht nur jede potentiell jugendgefährdende Seite, sondern auch jede wesentliche Abänderung der

---

mit Sicherheit die Worte „Homosexualität“ und „Sex“ verwendet werden.

1Siehe die Zusammenstellung unter http://www.jugendschutz.net/filtering/list-filter-studien.html.

2U.a. Möller/Amouroux-Akdeniz, S.106ff.

3So auch Möller/Amouroux-Akdeniz, S.113f.

Inhalte bewertet werden müsste, was angesichts der schnellen Änderung von Informationen als eines der charakteristischen Merkmale des Internets zu einer Überlastung der Bewertungsstellen führen würde. Eine Bewertung durch den Ersteller der Inhalte selbst birgt die Gefahr, dass dieser aus Eigeninteresse den Kreis der potentiellen Besucher so groß wie möglich halten will. Des Weiteren sind die Vorstellungen bezüglich dessen, was Jugendlichen „zugemutet" werden kann, in der Gesellschaft nicht einheitlich. Daher werden häufig zu niedrige Einstufungen vorgenommen werden. Eine effektive Kontrolle dürfte aufgrund der Vielzahl der Seiten und Anbieter und der geringen personellen Mittel der KJM ausgeschlossen sein. Auch ist von Seiten der Erziehungsberechtigten keine große Hilfe zu erwarten: Sie werden in der Regel nicht bemerken, wenn die Jugendlichen unzulässige Angebote aufrufen[1]; der Idealzustand des begleiteten Surfens dürfte eine Utopie sein und bleiben. Filtertechniken, die eine nicht zu realisierende Sicherheit vorspiegeln, bergen indes die Gefahr, dass Eltern ihre Erziehungsverantwortung auf die Technik verlagern.

Eine generelle Sperrung nicht bewerteter Seiten wäre ein schwerer Eingriff in die Informationsfreiheit, da derzeit nur ein kleiner Teil der veröffentlichten Seiten gekennzeichnet ist, die Übrigen aber überwiegend nicht jugendgefährdenden Inhalts sind. Von der eigentlich gewünschten Förderung der Medienkompetenz von Jugendlichen könnte nicht mehr die Rede sein. Auch würde ein Fernhalten von ungefährlichen Inhalten die Jugendlichen dazu anstacheln, die Jugendschutzprogramme zu umgehen. In Familien ist ein derartiger Einsatz von Filterprogrammen zwar rechtlich möglich, aber wohl verfehlt. In Schulen oder anderen öffentlich zugänglichen Gebäuden stellt sich die Frage nach der Verfassungsmäßigkeit einer derartigen Filterpraxis.

Derzeit[2] gibt es allerdings kein von der KJM anerkanntes Programm; die existenten Produkte, speziell aus Amerika stammende Software, sehen sich scharfer Kritik ausgesetzt[3], weil sie unter anderem mit den europäischen Vorstellungen von Jugendschutz inkompatible amerikanische Werte transportieren[4], keine Transparenz der Filterkriterien bieten und teilweise ihre Macht missbrauchen. Des Weiteren erlauben sie keinen nach Altersstufen differenzierten Zugang, dieser jedoch bildet die unabdingbare Voraussetzung für eine potentielle Anerkennung.

1Andernfalls wären alle Diskussionen über Jugendschutz mehr oder weniger hinfällig, da die Eltern den Jugendlichen immer den Konsum von jugendgefährdendem Material erlauben können.

2Juli 2007, mehrere Jahre nach Inkrafttreten des JMStV. Es wurden lediglich Modellversuche durchgeführt:

http://www.kjm-online.de/public/kjm/index.php?show_1=87,56. Diese sind mittlerweile ohne Anerkennung ausgelaufen.

3Möller/Amouroux-Akdeniz, S.106ff.

4In den USA wird sehr viel mehr Wert auf die Vermeidung von Pornographie jeglicher Form gelegt, während Gewaltdarstellungen für unbedenklicher gehalten werden.

(c.) Rechtliche Zulässigkeit

Problematisch erscheint in erster Linie eine Verletzung der Informationsfreiheit der Jugendlichen. Im familiären Bereich steht der Informationsfreiheit das elterliche Erziehungsrecht entgegen, welches überwiegt. In der öffentlichen Diskussion wird außerdem – häufig zu Unrecht – der Vorwurf der Zensur erhoben.

Im öffentlichen Bereich, beispielsweise in Schulen oder Internet – Cafés, kollidiert dagegen der Jugendschutz mit der Informationsfreiheit der Jugendlichen und der Berufsfreiheit der Betreiber. Hier ist fraglich, ob der Jugendschutz gegenüber den Rechten der Jugendlichen überwiegen kann.

(aa.) Jugendschutz und Zensurverbot

Das Zensurverbot gilt im Verhältnis des Staates mit den auf der Verbreiterseite stehenden Personen. Dogmatisch handelt es sich um eine zusätzliche Schranken-Schranke der Pressefreiheit[1], die auch durch Schrankengesetze im Sinne des Art. 5 II GG nicht eingegrenzt werden kann[2], wobei unklar bleibt, ob sie auch den Bürger in seinem Recht auf Informationszugang schützt[3].

Das Zensurverbot des Art. 5 I 2 GG gilt absolut, allerdings nur für die Vorzensur, also für Eingriffe vor (der) Veröffentlichung. Ein Eingriff in die Publikation nach dem Erscheinen, die so genannte Nachzensur, ist nach herkömmlichem Verständnis grundsätzlich unter den Eingriffsschranken des Art. 5 II GG zulässig[4]. Problematisch ist hierbei, dass sich die Rechtsprechung und die Literatur auf Zensur bei Druckschriften und Filmen beziehen. Um diese für eine Anwendung auf Telemedien fruchtbar zu machen, müssen zunächst die Druckschriften und Filmen entsprechenden Veröffentlichungsschritte bei Telemedien ausfindig gemacht werden. Erst danach kann beurteilt werden, ob eine unzulässige Vorzensur oder eine zulässige Nachzensur stattfindet.

(aaa..)Vorzensur und Nachzensur in Telemedien

Nach dem BVerfG handelt es sich um Vorzensur, wenn vor Erscheinen eines Werkes Maßnahmen getroffen werden, die dessen Herstellung oder Verbreitung beschränken, beispielsweise wenn das Erscheinen eines Werkes von einer Genehmigung abhängig gemacht wird[5]. Das Zensurverbot wirkt damit einer zu befürchtenden Lähmung des geistigen Lebens durch Genehmigungsverfahren entgegen. Verboten sind daher alle Maßnahmen, die einsetzen, bevor die Inhalte eines Werkes überhaupt ihre Wirkungsmacht entfalten können. Dies ist bei Druckschriften gewöhnlich der Zeitpunkt der Auslieferung, ab dem der Zugriff potentieller Käufer möglich ist. Übertragen auf Telemedien können Inhalte Effekte zeitigen, sobald sie der Öffentlichkeit zugänglich sind, also auf

1 Jarass/Pieroth-Jarass, Art. 5 Rn. 63, Sachs-Bethge, Art. Rn. 129. Dreier/Schultze-Fielitz, Art. 5 I, II Rn. 170 sieht es als verfassungsrechtliche Festlegung der Unverhältnismäßigkeit. J/P Rn. 63.

2Jarass/Pieroth-Jarass, Art. 5 Rn. 63; Umbach/Clemens-Clemens, Art. 5, Rn. 145.

3 Bejahend: Jarass/Pieroth-Jarass, Art. 5 Rn. 63; Sachs-Bethge Rn. 129. Verneinend: BVerfGE 27, 88, 102; E 33, 52, 72.

4 Sachs, Art. 5 Rn. 123; Degenhart BK Art. 5 I, II Rn. 743.

5 BVerfGE 33, 52, 72.

einen Server in ein für die Öffentlichkeit freigegebenes Verzeichnis kopiert oder auf andere Weise verbreitet werden.

(bbb.) Herkömmliches Verständnis

Die Einrichtung von Jugendschutzfiltern verhindert die Verbreitung eines Werkes nicht. Eine Intervention vor der Publikation wäre nur zu bejahen, wenn ein Abrufen von Seiten des Nutzers der Veröffentlichung bei Druckwerken entspräche. Das ist zwar insofern der Fall, als beim Nutzer eine Kopie des Inhalts entsteht, jedoch dürfte dies eher mit der Verbreitung nach der Erstpublikation vergleichbar sein, da die Inhalte bereits öffentlich zugänglich gemacht wurden. In die Produktion von Inhalten wird durch Jugendschutzfilter jedenfalls nicht eingegriffen. Es genügt, wenn die Verbreitung faktisch abgewendet wird[1]. Die Kenntnisnahme wird allerdings nur für Jugendliche verhindert, nicht für alle Bürger; es findet somit kein Eingriff in der Vor-Publikationsphase statt, da die Inhalte in Deutschland generell abrufbar bleiben. Nach einem engen Verständnis liegt keine Zensur vor. Zensur im Sinne des traditionellen Zensurbegriffs läge aber vor, wenn das traditionelle Zensurverbot auch die Informationsfreiheit umfassen würde.

(ccc.) Erweiterter Zensurbegriff

Hoffmann-Riem spricht sich speziell vor dem Hintergrund einer effektiveren Nachzensur in elektronischen Medien für einen erweiterten Zensurbegriff aus[2]. Danach zielt das Zensurverbot nicht nur auf die Verhütung des Aufbaus staatlicher Genehmigungseinrichtungen, um die Verbreitung von Kommunikationsinhalten völlig zu unterbinden, sondern auch auf die Verhinderung staatlicher, planmäßiger und präventiver Suche nach erstmaliger Verbreitung von Inhalten[3]. Ebenso unterfällt der Zensur nach dieser Anschauung eine Förderung der Zensuraktivitäten Privater oder eine diesbezügliche Verpflichtung[4]. Auch eine vorbeugende Kontrolle förderndes Haftungsrecht wäre, selbst bei missbilligten oder strafbaren Kommunikationsinhalten[5], wegen Verstoßes gegen das Zensurverbot verfassungswidrig[6].

Nach Hoffmann-Riems Verständnis ist auch eine technisch vollständige Verhinderung des Zugangs zu Inhalten nach deren Veröffentlichung dem Zensurverbot zuzurechnen, wenn dafür ein vom Anlass unabhängiges Suchsystem eingerichtet worden ist. Dies trifft auf den JMStV nicht zu, da

1 Sachs-Bethge, Art. 5 Rn.135b.

2Hoffmann-Riem, Kommunikationsfreiheiten, S.143.

3Hoffmann-Riem, Kommunikationsfreiheiten, S.143.

4Hoffmann-Riem, Kommunikationsfreiheiten, S.144.

5Hoffmann-Riem, Kommunikationsfreiheiten, S.144.

6Hoffmann-Riem, Kommunikationsfreiheiten, S.144.

weder die KJM noch die Selbstkontrolleinrichtungen Inhalte durchsuchen; sie sind entweder auf Meldungen zum Zweck der Freigabe oder auf Beschwerden von Nutzern angewiesen.

Des Weiteren würde eine konsequente Verfolgung dieses Verständnisses des Zensurverbotes zu der Auffassung führen, dass es dem Staat untersagt sein müsste, Private zu einer Anlass-unabhängigen Suche anzuregen. Dies ist weder in der Tätigkeit der KJM noch im JMStV angelegt, auch die Einrichtung von Hotlines für jugendgefährdende Inhalte ist diesbezüglich unbedenklich, da sie nur Meldungen über Inhalte annehmen und gegebenenfalls den Verantwortlichen zur Beseitigung auffordern.

Die Situation würde sich anders darstellen, wenn das Zensurverbot auch die Informationsfreiheit erfasste. Hierzu müsste allerdings einerseits das Abrufen eines Inhalts mit dessen Publikation gleichgesetzt werden und andererseits die Informationsfreiheit vom Zensurverbot umfasst sein.

(ddd.) Informationsfreiheit und Zensurverbot

Die Informationsfreiheit vervollkommnet den Schutz der Kommunikationsfreiheiten gegenüber dem Staat, indem dem Einzelnen das Recht auf Zugang zu Informationen gegeben wird. Damit ist sie das Gegenstück zu den Äußerungsfreiheiten. Ob allerdings auch das Zensurverbot des Art. 5 I 3 GG von der Informationsfreiheit umfasst ist, wird aus der Verfassung nicht deutlich. Allerdings kann die Informationsfreiheit schon aufgrund ihrer andersartigen Zielrichtung nicht vom Zensurverbot eingeschlossen sein[1]. Dies würde bedeuten, dass die Verhinderung des Zugriffs auf bestimmte Inhalte als Akt der Zensur gälte. Anders wäre das Zensurverbot, das im Gegensatz zu den übrigen Freiheiten des Art. 5 I GG nicht für die Veröffentlichung von Kommunikation, sondern für den Zugang zu Informationen auf Empfängerseite gilt, nicht auf die Informationsfreiheit anwendbar[2]. Eine derartige Anwendung aber ließe Abs. II ins Leere laufen: Ein Fernhalten von Personen von bestimmten Informationen wäre zugleich ein Verstoß gegen das Zensurverbot in der Informationsfreiheit; es könnte nicht zwischen zulässiger Nachzensur und unzulässiger Vorzensur differenziert werden, da ansonsten stets ein einmaliger Zugriff für jeden Empfänger möglich sein müsste – somit erübrigte sich eine Nachzensur generell.

Vorstellbar wäre eine Erweiterung des Zensurverbots auf die Verhältnismäßigkeit der Anwendung der Schranken des Abs. II[3]. Ob dies allerdings andere Ergebnisse zeitigen würde als eine Verhältnismäßigkeitsprüfung, ist zweifelhaft[4].

1Dreier-Schultze-Fielitz, Art. 5 Rn. 173; BVerfGE 27, 88, 102; MD-Herzog, Art. 5 Rn. 297; Umbach/Clemens-Clemens, Art. 5 Rn. 144; Gucht, S.79f.

A.A.: HdbStR-Schmidt-Jortzig, § 141 Rn. 45; Jarass-Pieroth-Jarass, Art. 5 Rn. 63; Sachs-Bethge, Art. 5 Rn. 129.

2 So wohl auch BK-Degenhardt, Art. 5 Rn. 929.

3 BK-Degenhardt, Art. 5, Rn. 929.

4So auch Gucht, S.81.

(bb.) Jugendschutz und Informationsfreiheit in öffentlichen Einrichtungen

Die Informationsfreiheit des Art. 5 I 1 GG kann durch die Schranken des Abs. II begrenzt werden. Die über das Internet erreichbaren Inhalte sind auch allgemein zugängliche Informationsquellen. Eine Filterung nicht gekennzeichneter Inhalte, egal welcher technischen Art, stellt somit einen Eingriff in die Informationsfreiheit dar, der durch die Schranken des Abs. II gerechtfertigt sein müsste. Diese wiederum sind aber durch das Verhältnismäßigkeitsprinzip beschränkt. Es ist fraglich, ob Jugendschutzfilter überhaupt zum Jugendschutz geeignet sind. Sogar unter ihren Befürwortern ist unbestritten, dass Jugendschutzprogramme als einzige Maßnahme zum Schutz Jugendlicher nicht ausreichen, sondern vielmehr auch erzieherische Maßnahmen notwendig sind. Ebenso besteht Einigkeit dahingehend, dass ein vollkommener Schutz nicht möglich ist[1].

Jugendschutzprogramme sind zwar dazu geeignet, Erziehungsberechtigte bei der Überwachung ihrer Kinder und damit der Wahrnehmung ihrer Aufgaben zu unterstützen; jedoch wird die Einführung von PICS-basierten Jugendschutzprogrammen selbst im Idealfall dazu führen, dass ein Großteil der über das Internet erreichbaren Inhalte nicht abrufbar ist, da eine Ausrichtung deutscher privater – und erst recht ausländischer – Anbieter an deutschen Jugendschutzvorschriften nicht zu erwarten ist. Dies gilt sowohl für bedenkliche als auch für völlig unbedenkliche Inhalte wie beispielsweise auf amerikanischen oder britischen Nachrichtenseiten. Des Weiteren ist die oben erwähnte enorme Fehlerrate bei auf Wortlisten basierenden Programmen zu beachten, die derartige Software eher als schädlich denn als nützlich erscheinen lässt. Angesichts der Realität in Schulen und erst recht in öffentlichen Bibliotheken – sofern diese überhaupt über Internet-Arbeitsplätze verfügen – ist es als ausgeschlossen zu betrachten, dass diese Institutionen zusätzlich zu Jugendschutzprogrammen genügend und vor allem qualifiziertes Personal zur Erziehung im Sinne einer umfassenden Medienkompetenz bereitstellen können. Es wird also bei dem allgemein als unbefriedigend empfundenen Zustand bleiben, dass der Schutz der Jugendlichen allein durch Jugendschutzprogramme realisiert wird.

Angesichts dieser Umstände kann der Einsatz von Jugendschutzprogrammen hinsichtlich des Ziels der Medienkompetenz bei Jugendlichen als ungeeignet und bezüglich der zu schützenden Informationsfreiheit als unverhältnismäßig betrachtet werden.

1 So auch die Begründung zu § 5 III Nr. 1 JMStV.

(cc.) Jugendschutz gegen Berufsfreiheit und Informationsfreiheit an privaten Plätzen

Prinzipiell kann der Staat auch Privaten den Einsatz von Jugendschutzfiltern vorschreiben. Dies würde aber nichts an der Tatsache ändern, dass es sich hierbei – ebenso wie im öffentlichen Raum – um einen unverhältnismäßigen Eingriff in die Grundrechte der Jugendlichen handelt.

(d.) Weitere Probleme

Ein einmal eingeführtes Filtersystem lässt nicht nur auf der Ebene der Nutzer, die wenigstens in der Theorie autonom über den Einsatz der Filter entscheiden können, sondern auch auf verschiedenen Netzwerkebenen eine Filterung zu. Denkbar ist nicht nur eine Kennzeichnung nach Jugendschutz-Gesichtspunkten, sondern auch nach politischen oder kommerziellen Kategorien. Ein Einsatz auf Providerebene bleibt jedoch von den Betroffenen unbemerkt – in einigen Staaten erscheinen Fehlermeldungen, die gerade die Filterung nicht erkennen lassen – und steht damit im Widerspruch zu dem Ziel der Förderung der Medienkompetenz und der Förderung der Autonomie der Individuen[1]. Der relativ große Widerstand von „Netzaktivisten“ gegen die Einführung von Jugendschutz-Labels erklärt sich somit nicht aus einer breiten Unterstützung von pornographischen Inhalten, deren einzige Verteidiger in der Regel ihre Anbieter sind, sondern aus grundsätzlichen Erwägungen und den weitergehenden Nutzungsmöglichkeiten des Labeling.

Nach Vorstellungen der Bertelsmann-Stiftung, die ein dem JMStV ähnliches Regulierungsmodell entworfen hat, sollen Filterprogramme in jedem Computer vorinstalliert sein[2]. Was zunächst wie eine sinnvolle, für Erziehungsberechtigte hilfreiche Idee klingt, birgt die Gefahr einer privat und staatlich geförderten Selbstzensur. Die Erfahrung zeigt, dass allen Widrigkeiten zum Trotz vorinstallierte Programme trotz aller Fehler von den meisten Nutzern genau so verwendet werden, wie sie vorkonfiguriert sind, da die Hemmschwelle[3] hinsichtlich einer Veränderung relativ hoch ist[4]. Hier wird der mögliche positive Effekt für den Jugendschutz jedoch durch den Schaden für die Kommunikationsfreiheiten deutlich überdeckt.

(e.) Abhilfen

Die weit verbreitete Annahme, es könne eine totale, durch Technik oder Software vermittelte Sicherheit geben, die praktisch ohne Beschäftigung mit der zugrunde liegenden Technik erworben werden kann[5], ist in hohem Maße kontraproduktiv. Dementsprechend sollten staatliche Maßnahmen nicht die Entwicklung von Filtertechniken unterstützen, sondern durch – um in der Sprache des

1Hausmanninger, S.186.

2Waltermann/Machill-Balkin/Noveck/Roosevelt, S.211, 279.

3Hervorgerufen entweder durch Unkenntnis oder Trägheit.

4Anders lassen sich wohl die zahllosen Virenepidemien der Jahre 2003 und 2004, hervorgerufen durch Sicherheitslücken des Betriebssystems Microsoft Windows XP sowie des Internet Explorers und von Outlook Express nicht erklären. Die Abhilfe wäre verhältnismäßig einfach und mit wenig Aufwand durchzuführen gewesen.

5So auch Möller/Amouroux-Akdeniz, S.120.

Gesetzgebers zu bleiben – aktives Verbreiten den Erziehungsberechtigten Informationen zu Risiken und Chancen technischer Maßnahmen nahe bringen[1]. Der Schwerpunkt sollte nicht auf Verboten und dem Aufbau eines aus staatlichen Aufsichtsgremien und privaten Hotlines bestehenden Überwachungsapparats, sondern auf der Förderung der Medienkompetenz, auch und gerade der Erziehungsberechtigten, liegen. Statt nur mit einfach zu umgehenden oder zu weit greifenden Verboten konfrontiert zu werden, würden Jugendliche über die unbestreitbaren Gefahren und deren Ursachen aufgeklärt und gleichermaßen die Kompetenzen der Eltern erweitert: Dies würde nicht nur einen deutlich verbesserten Jugendschutz, sondern auch einen Gewinn für die gesamte Gesellschaft mit sich bringen.

(4.) Zeitliche Beschränkungen

Nach § 5 III Nr. 2 JMStV ist es ausreichend, wenn Anbieter ihre Inhalte nur in den von § 5 IV JMStV festgelegten Zeiträumen zugänglich machen; dies dürfte im Internet eine nur schwierig zu erfüllende Voraussetzung sein. Zwar ist es technisch möglich, Inhalte nur zu bestimmten Zeiten zugänglich zu machen, jedoch würde dies eine Ablehnung von Anfragen zu bestimmten Uhrzeiten von Seiten des Servers des Anbieters bedeuten und somit einerseits der „Natur“ des Internets als einem internationalen Medium zuwiderlaufen und andererseits für kommerzielle Angebote äußerst unattraktiv sein: Eine Länderkennung durch IP-Adressen ist – wenn überhaupt – nicht mit großer Sicherheit möglich. Derart beschränkte Seiten wären dementsprechend nur für rein nationale Angebote interessant. Zweifelhaft ist außerdem, ob die Wirkung zeitlicher Beschränkungen nicht durch das bei allen Access-Providern vorgenommene Caching oder auch durch beispielsweise von Google offerierte Angebote der kompletten Speicherung von Inhalten, die längst offline sind, zunichte gemacht würde. Daher erscheinen diese Begrenzungen eher im Bereich des Rundfunks als sinnvoll, auch wenn sie in der Gesetzesbegründung als Alternative für Telemedien genannt werden.

c. Bestellung von Jugendschutzbeauftragten

§ 7 JMStV beinhaltet die Verpflichtung zur Bestellung eines Jugendschutzbeauftragten, dessen Aufgabe nach § 7 III JMStV darin besteht, als Ansprechpartner für Nutzer und Berater des Anbieters in allen Fragen des Jugendschutzes zu fungieren. Anbieter, die weniger als 50 Mitarbeiter beschäftigen oder deren Inhalte im Monatsdurchschnitt weniger als 10 Millionen Mal aufgerufen werden, können nach § 7 II JMStV die Verpflichtung zur Bestellung eines Jugend-

1So auch Möller/Amouroux-Akdeniz, S.120.

schutzbeauftragten durch einen Anschluss an eine von der KJM anerkannte Einrichtung der Selbstkontrolle ersetzen.

Nach dem weiten Anbieterbegriff des § 3 II Nr. 2 JMStV sind auch Inhaltsanbieter sowie Host- und Access-Provider zur Bestellung von Jugendschutzbeauftragten verpflichtet, sofern sie jugendgefährdende Inhalte oder den Zugang zu solchen anbieten. Diese Bestellung ist weder eine Regelung der Verantwortlichkeit für Inhalte, so dass kein Konflikt mit der Regelung des § 2 III JMStV mit den §§ 7 ff. TMG entstehen kann[1], noch eine Überwachungspflicht, die der Regelung des § 7 II TMG zuwiderlaufen könnte.

Es stellt sich die Frage, inwieweit Jugendschutzbeauftragte bei bloß technischen Providern eine Funktion haben können.

(1.) Jugendschutzbeauftragte bei Content-Providern

Nach § 7 I 2 JMStV besteht für Content-Provider, die jugendgefährdende Inhalte anbieten, die Pflicht, einen Jugendschutzbeauftragten zu bestellen; dieser können sie allerdings nach § 7 II JMStV durch Anschluss an eine Einrichtung der Freiwilligen Selbstkontrolle entgehen, wenn sie weniger als 50 Mitarbeiter oder monatlich weniger als zehn Millionen Zugriffe haben.

Außerdem gilt die Verpflichtung zur Einsetzung eines Jugendschutzbeauftragten nicht, wenn auf Grund technischer Vorrichtungen die Erreichbarkeit für Jugendliche wenigstens erheblich erschwert wurde[2]. Durch die Struktur der Inhalteanbieter im Internet könnten die Kosten hierfür aber zu einer rechtlich abweichenden Einordnung führen, wenn sie faktisch den Unternehmern so hohe Kosten auferlegen, dass sie erdrosselnd wirken.

(2.) Jugendschutzbeauftragte bei Host-Providern

Jugendschutzbeauftragte müssten bei Host-Providern nur eingesetzt werden, wenn sie die vom JMStV angedachten Kontrollfunktionen überhaupt wahrnehmen können; andernfalls wäre der Anbieterbegriff des § 7 I 2 JMStV in seinem Anwendungsbereich einzugrenzen. Nach § 7 II TMG besteht keine aktive Überwachungspflicht für Host-Provider, was auch für die Kontrolle hinsichtlich einer Bereithaltung jugendgefährdender Inhalte gelten muss. Damit ist nicht klar, inwieweit Jugendschutzbeauftragte überhaupt eine sinnvolle Funktion wahrnehmen können. Bei der Gestaltung des Angebots, also der Strukturierung der Server, können Jugendschutzbeauftragte wohl keinen Einfluss ausüben, da die Gestaltung der Server keinen Einfluss auf die Inhalte hat.

Denkbar wäre eine Beratung der Provider hinsichtlich der Beurteilung der Rechtmäßigkeit eventuell jugendgefährdender Angebote von Seiten der Jugenschutzbeauftragten; diese allerdings liegt bereits im Eigeninteresse der Provider, da ihnen andernfalls die Haftung wegen Kenntnis rechtswidriger

1 S.u. S.109ff.

2 Begründung zu § 7 I 2 JMStV, Landtag von Baden-Württemberg, Drs. 13/1551.

Inhalte droht: Somit besteht keine Veranlassung einer Verpflichtung für Host-Provider zur Bestellung eines Jugendschutzbeauftragten auf Grund von § 7 JMStV.

(3.) Jugendschutzbeauftragte bei Access-Providern

Der Einsatz von Jugendschutzbeauftragten bei Access-Providern wäre nur von Nutzen, wenn diese die vom JMStV angedachten Kontrollfunktionen überhaupt wahrnehmen können; andernfalls wäre der Anbieterbegriff des § 7 I 2 JMStV in ihrem Anwendungsbereich einzugrenzen.
Eine Überwachung der transportierten Inhalte ist Access-Providern technisch nicht möglich; es existiert zudem keine Verpflichtung zur Suche und Sperrung von jugendgefährdenden Inhalten, da nach § 2 III JMStV die Regelungen des TMG durch den JMStV unberührt bleiben. Folglich können Jugendschutzbeauftragte bei Access-Providern keine sinnvollen Aufgaben wahrnehmen; eine Verpflichtung zur Bestellung von Jugendschutzbeauftragten besteht – ebenso wie bei Telekommunikationsanbietern – nicht.

(4.) Jugendschutzbeauftragte bei Suchmaschinen

Nach § 7 I JMStV sind auch Suchmaschinen zur Bestellung von Jugendschutzbeauftragten verpflichtet. Deren Funktion ist allerdings angesichts der Tatsache, dass Suchmaschinen nach der hier vertretenen Auffassung nicht zur Durchführung irgendwelcher aktiven Jugendschutzmaßnahmen verpflichtet sind, unklar und wird auch aus der Gesetzesbegründung nicht ersichtlich.

4. Verhältnis der Regelungen von JMStV und TMG

Es fällt auf, dass der JMStV Handlungspflichten für Anbieter von Telemedien statuiert, die Regelungen des TMG jedoch Verantwortlichkeitsregelungen für eigene und fremde Inhalte enthalten, während nach § 2 III JMStV die Regelungen des TMG durch den JMStV „im Übrigen“ unberührt bleiben sollen. Hier stellt sich die Frage nach dem Verhältnis der Pflichten.

a. Keine Anwendung der §§ 4 II, 5 I JMStV

Nach § 2 III JMStV sollen das TMG und die „für Telemedien anwendbaren Bestimmungen“ vom JMStV unberührt bleiben und ausschließlich die jugendschutzrechtlichen Bestimmungen der beiden Vorschriften ersetzt werden[1], während die gestuften Verantwortlichkeiten der §§ 7-10 TMG im vollen Umfang erhalten bleiben sollen[2]. Die Regeln des JMStV wären nur unter den Voraussetzungen einer bestehenden Verantwortlichkeit anwendbar, was dem Zweck der gestuften Verantwortlichkeit

1 Eberle/Rudolf/Wasserburg-Landmann, VI Rn. 13; Grapentin, S.462.

2 Eberle/Rudolf/Wasserburg-Landmann, VI Rn. 13; Grapentin, S.462.

entspräche, die geschaffen wurde, da eine Kontrolle technisch nahezu unmöglich ist und welche die nahe liegende und – ausweislich der amtlichen Begründung – auch die vom Gesetzgeber gewünschte Regelung darstellt.

(1.) §§ 4 II, 5 I JMStV als Erweiterung

Der JMStV könnte eine Spezialregelung darstellen, die im Bereich des Jugendschutzes neben die Regelungen des TMG tritt und eine neue Verantwortlichkeit schafft. Host- und Access-Provider sorgen durch ihre Tätigkeit dafür, dass andere Personen Zugriff auf fremde Inhalte erhalten. Sie machen diese also sowohl im Sinne des § 5 I JMStV als auch der § 8 I TMG zugänglich. Es gibt keinerlei Anhaltspunkte dafür, dass der Begriff des zugänglich Machens im JMStV anders zu verstehen sei als in TDG a.F. und MDStV a.F.

Die im TMG enthaltenen Privilegierungen betreffen die Verantwortung für fremde Rechtsverstöße[1]; § 5 I JMStV normiert allerdings eine eigene Handlungspflicht der Anbieter. Anbieter sind nach der gesetzlichen Definition des § 3 II Nr.3 JMStV auch Anbieter von Telemedien. Somit gehören auch Host- und Access-Provider zu den Adressaten des JMStV. Die sich aus dem JMStV ergebende Pflicht zum Schutz der Jugend haben Telemedienanbieter, unabhängig von fremden Rechtsverstößen, zu erfüllen, wenn sie jugendgefährdende Angebote zugänglich machen. Aus dem JMStV ist keine Beschränkung auf eigene oder zu-eigen-gemachte Inhalte erkennbar. Nach § 5 I JMStV machen Host- und Access-Provider diese fremden Inhalte zugänglich und unterliegen aufgrund dessen einer eigenen Verpflichtung. §§ 4 II, 5 I JMStV regeln somit andere Sachverhalte als das TMG und können nicht mit dessen Verantwortlichkeitsregelung in Konflikt geraten. Es kann gefolgert werden, dass nicht nur für Inhalte-, sondern auch für andere Telemedienanbieter die Pflicht zur Einrichtung von geschlossenen Benutzergruppen nach § 4 II 2 JMStV und zum Einsatz von technischen oder sonstigen Mitteln nach § 5 III Nr.1 JMStV besteht.

(2.) Teleologische Reduktion

Nach ihrem Wortlaut sind die §§ 4 II, 5 I JMStV auch auf Host- und Access-Provider anwendbar; die dadurch ausgehebelten Privilegierungen sind allerdings keine Geschenke des Gesetzgebers, sondern beruhen auf technischen Notwendigkeiten. Die Provider können allein technisch nicht feststellen, welcher Art die von ihnen gespeicherten oder durch geleiteten Daten sind und somit auch nicht erkennen, ob diese rechtswidrig oder jugendgefährdenden Inhalts sind. Eine Überwachungspflicht besteht nach § 7 II TMG nicht und kann und soll auch nicht durch §§ 4 II, 5 I JMStV begründet werden; dies widerspräche § 7 II TMG, der aber durch den JMStV nicht berührt werden soll. Daraus folgt, dass §§ 4 II, 5 I JMStV teleologisch auf Inhaltsanbieter zu

1 Nach der Systematik der Verantwortlichkeit besteht, wie § 7 I TMG deklaratorisch feststellt, die nach den herkömmlichen Gesetzen bestehende Verantwortlichkeit grundsätzlich auch im Internet; demnach wären Host- und Access- Provider vor allem wegen Beihilfe zu fremden Rechtsverstößen bzw. als Mitstörer verantwortlich. Diese Verantwortlichkeit wird durch das TMG allerdings wesentlich eingeschränkt, so dass sie die Ausnahme bleibt. So auch Sieber, Beilage zu MMR 2/99, 2.

reduzieren sind. Eine Verpflichtung zur Einhaltung des JMStV besteht für andere Provider nur, wenn sie ausschließlich den Zugang zu jugendgefährdenden – auch ausländischen – Angeboten eröffnen[1]. Dafür spricht auch, dass Host- und Access-Provider nach § 7 II TMG nicht dazu verpflichtet sind, fremde Inhalte zu überwachen; dies wäre allerdings die Grundvoraussetzung dafür, in Erfahrung bringen zu können, welche Inhalte der Jugendschutzvorrichtungen bedürfen.

b. Geltung für Suchmaschinen

Da Suchmaschinen Telemedien sind, ist der JMStV auf sie anwendbar. Durch ihre Suchfunktion und die Auflistung der Ergebnisse sorgen sie häufig erst für die Auffindbarkeit von Angeboten. Eine Löschung jugendgefährdender Angebote aus den Verzeichnissen von Suchmaschinen würde deren Auffindbarkeit erheblich erschweren. Insofern stellen Suchmaschinen auch geeignete Ansatzpunkte dar, um den Zugang von Jugendlichen zu ausländischen jugendgefährdenden Angeboten zu erschweren. Allerdings sind sie nach der hier vertretenen Auffassung[2] wie Zugangsvermittler nach § 8 I TMG zu behandeln und somit nicht von der Pflicht zum Einsatz von Jugendschutzprogrammen nach § 5 I JMStV oder zur Einrichtung geschlossener Benutzergruppen umfasst, solange sie nicht speziell für jugendgefährdende Angebote betrieben werden.

Es bestünden die Möglichkeiten, Suchmaschinen als Nichtverantwortliche nach § 59 IV RStV zur Sperrung von Angeboten bzw. zur Entfernung von bestimmten Seiten zu verpflichten[3] oder die Suche nach bestimmten Themen zu verbieten, was eine Kostenerstattungspflicht analog nationaler Polizeigesetze mit sich brächte. Die Motivation der KJM und anderer Behörden, derlei Maßnahmen von fragwürdiger Wirksamkeit zu ergreifen, wird voraussichtlich sehr gering ausfallen.

c. Geltung für Links

Auch eine Person, die Links setzt, gilt nach dem JMStV als Anbieter von Telemedien. Für das Setzen von Links sind allerdings die §§ 4, 5 JMStV teleologisch zu reduzieren, so dass hier zwar eine gegenüber Suchmaschinen erweiterte Verpflichtung entsteht – da ein Link ja zwangsweise nur auf einen bestimmten Inhalt verweisen kann –, diese aber lediglich für die direkt verlinkten Angebote und nicht für Folgelinks gilt, die von dem verlinkten Inhalt auf jugendgefährdende Angebote führen.

1Interessant könnte eine solche Zugangseröffnung vor allem dann sein, wenn Anbieter den Einsatz gefälschter oder gestohlener Kreditkarten verhindern wollen. Bei Einschaltung eines Providers, der nur Zugang zu jugendgefährdenden Angeboten gewährt, könnte die Abrechnung über die Telefonrechnung erfolgen.

2S.ff.

3So auch die Bezirksregierung Düsseldorf, siehe: http://www.heise.de/newsticker/meldung/41237.

5. Indizierung von Inhalten

Nach § 18 JuSchG können Telemedien „indiziert", also in eine Liste jugendgefährdender Medien aufgenommen werden. Hierbei gelten für Telemedien und andere Trägermedien dieselben inhaltlichen Maßstäbe. Die so genannte Indizierungsliste wird von der Bundesprüfstelle für jugendgefährdende Medien (BpjM) geführt. Sie ist nach § 18 II JuSchG in vier Teile zu gliedern, wobei sich die Aufteilung nach der Art der Inhalte richtet. Ob der BPjM bei der Beurteilung der Voraussetzung für die Aufnahme ein Beurteilungsspielraum zusteht, ist umstritten. Eine Verpflichtung zur Aufnahme in die Liste besteht nach § 18 V JuSchG bei rechtskräftigen Entscheidungen von Gerichten.

Für Telemedien gilt die Spezialregelung des § 18 VI JuSchG, wonach bei einem Antrag auf Aufnahme in die Liste durch die „zentrale Aufsichtsstelle der Länder", also die KJM, die betroffenen Inhalte aufzunehmen sind. Eine Ausnahme ist nur möglich, wenn die Entscheidung der KJM „offensichtlich unbegründet" oder mit der Spruchpraxis der BPjM unvereinbar ist. Nach § 18 VIII JuSchG ist die BPjM in jedem Fall an die Entscheidung der KJM hinsichtlich einer Nichtaufnahme gebunden. Nach § 18 VII 3 JuSchG besteht außerdem eine Bindung an die Entscheidungen anerkannter Selbstkontrolleinrichtungen, sofern die KJM die Voraussetzungen für eine Aufnahme in die Liste nicht als gegeben ansieht. Die letztere Regelung wirft allerdings die Frage nach dem Verhältnis zwischen Selbstkontrolleinrichtungen, KJM und BPjM auf.

a. Verhältnis der BPjM zur KJM und Selbstkontrolleinrichtungen

Die Formulierung von § 18 VIII 3 JuSchG legt nahe, dass die BPjM zwar an die Entscheidungen der KJM, nicht aber an jene der Selbstkontrolleinrichtungen gebunden sei. Dies würde bedeuten, dass die KJM, sollte sie wegen des gesetzlich beschriebenen „Beurteilungsspielraums" keine Mittel zum Vorgehen gegen von Selbstkontrolleinrichtungen geprüfte Inhalte haben, per Stellungnahme gegenüber der BPjM dennoch deren Indizierung bewirken kann[1]. Infolgedessen wäre auch ein Vorgehen der KJM gegen indizierte Inhalte nach § 4 I, II JMStV denkbar[2]; diese – sehr paradox erscheinende – Möglichkeit widerspricht allerdings der abschließenden Prüfungskompetenz der KJM nach § 16 JMStV und bedarf dementsprechend der Korrektur. Am ehesten entspräche dem Wortlaut des § 16 JMStV und dem Ziel der Stärkung der Selbstkontrolleinrichtungen eine ähnliche Bindung der BPjM an die Entscheidungen der Selbstkontrolleinrichtungen, wie sie auch für die KJM gilt, bzw. eine Bindung der BPjM an nicht aufhebbare Entscheidungen der Selbstkontrolleinrichtungen gegenüber der KJM.

1So wohl auch Nikles/Roll/Umbach/Spürck, § 18 JuSchG, Rn. 20.

2So wohl auch Nikles/Roll/Umbach/Spürck, § 18 JuSchG, Rn. 20.

b. Indizierung von Telemedien

Die Indizierung bei Telemedien wirft verschiedene und anders geartete Probleme als bei Druckwerken oder anderen Trägermedien auf. Die erste sich stellende Frage bezieht sich auf den genauen Inhalt der Indizierung: Während ein Film nur schwer und der Inhalt eines Buches nicht verändert werden kann, liegen Telemedien zwangsläufig in Form verschiedener, miteinander verknüpfter Dateien vor, die sich auf einem bestimmten oder auch mehreren Servern befinden.
Wenn sich die Indizierung auf das gesamte Angebot eines Anbieters bezieht, gestaltet sie sich unproblematisch. Schwierig wird es jedoch, wenn nur Teile eines Angebots unzulässig oder jugendgefährdend sind und daher indiziert werden sollen. Es muss geklärt werden, was genau indiziert worden ist und welche Teile des Angebots weiterhin verbreitet und zugänglich gemacht werden dürfen. Da Dateien ihren Namen unter Beibehaltung des Inhalts oder unter Beibehaltung ihres Namens den Inhalt oder Server wechseln können und somit ein komplettes Angebot unter neuem Namen auf einem anderen Server auftauchen kann, stellen die Bestimmtheit der Indizierung einerseits und die mit steigender Bestimmtheit erleichterten Umgehungsmöglichkeiten andererseits nicht zu unterschätzende Probleme dar.

(1.) Indizierung des gesamten Angebots

Der Problematik der Bestimmung eines zu indizierenden Inhalts könnte entgegengewirkt werden, indem Verbreitung und zugänglich Machen eines gesamten Angebots verboten werden, auch wenn es nur partiell indizierungsfähig ist. Ein derartiges Vorgehen ist jedoch in der Regel unverhältnismäßig. Eine andere Wertung ist wohl wohl nur dann möglich, wenn lediglich unerhebliche Teile wie die Eingangsseite, aber keine eigentlichen Inhalte, nicht jugendgefährdend sind.

(2.) Indizierung der Dateien

Vorstellbar wäre es auch, ausschließlich die betroffenen Dateien mit ihrem Inhalt zu indizieren. Dies widerspräche der Begründung, wonach nur das Werk als solches indiziert werden solle; eine Indizierung der bloßen Inhalte scheint indes nur schwer möglich. Es wäre sichergestellt, dass die entsprechenden Inhalte nicht nur unter dem vorliegenden Dateinamen nicht mehr publiziert werden könnten, sondern – da auch die Inhalte selbst von der Indizierung betroffen wären – ebenso nicht mehr unter anderem Namen. Durch § 4 III JMStV würde des Weiteren sichergestellt, dass die Indizierung bei Veränderungen weiter wirkt. Allerdings gestaltet sich gerade bei Telemedien die Abgrenzung zwischen einer wesentlichen Veränderung, so genannten Schnitten, und einer

Neugestaltung mit Übernahme von Teilen des Angebots als zumindest schwierig. Ein Verbot der Übernahme von Teilen ohne vorherige Genehmigung würde aber dem Zensurverbot des Art. 5 I 3 GG widersprechen.

(3.) Fortwirkung der Indizierung

Nach § 4 III JMStV wirkt eine Aufnahme in die Liste jugendgefährdender Medien auch bei Schnitten, also dem Herausnehmen bestimmter Teile eines Angebots, bis zu einer Entscheidung der BPjM über die veränderten indizierten Inhalte

fort. Vor der Genehmigung durch die BPjM darf das indizierte Angebot nicht veröffentlicht werden. Nach der Gesetzesbegründung soll sichergestellt werden, dass auch veränderte Angebote nicht ohne weiteres zugänglich gemacht werden können[1]. Ziel dieser Regelung ist, dass auch häufig wechselnde Angebote, deren jugendgefährdender Gehalt jedoch gleich bleibt, erst nach einer Prüfung durch die BPjM wieder erreichbar gemacht oder verbreitet werden. Obgleich sie für den Jugendschutz sehr lobenswert sein mag, stellt sich die Frage nach ihrer Kompatibilität mit dem Zensurverbot, das kategorisch verbietet, die Ausübung einer der Freiheiten des Art. 5 GG einer vorherigen behördlichen Erlaubnis zu unterwerfen[2]. Genau dies muss jedoch bei der Genehmigung der Wiederveröffentlichung eines indizierten Angebots geschehen: Die Regelung des § 4 III JMStV verstößt somit gegen das Zensurverbot[3]. Anders als bei Filmen oder herkömmlichen Medien ist es bei Telemedien möglich, dass statt des indizierten Angebots unter demselben Namen ein völlig anderes Werk veröffentlicht wird; dieses unterliegt allerdings ebenso der Fortwirkung der Indizierung.

6. Überwachung der Vorschriften

Der JMStV ist nach dem Modell der Regulierten Selbstregulierung ausgestaltet, wonach in erster Linie Private die Überwachung der Vorschriften gewährleisten sollen; der Staat soll lediglich die Privaten selbst beaufsichtigen.

a. Struktur der Aufsicht

Die Überwachung der Einhaltung der Jugendschutzvorschriften obliegt nach § 14 I JMStV den Landesmedienanstalten, die zu diesem Zweck die KJM bilden. Diese ist als Organ aller Landesmedienanstalten konstituiert und wird als Organ der jeweils zuständigen Landesmedienanstalt tätig. Zur Erfüllung der Aufgaben der KJM nach § 16 JMStV werden nach § 14 V JMStV Prüfausschüsse gebildet. Organisatorisch an die KJM angebunden ist die von den obersten Landesjugendschutzbehörden eingerichtete Stelle jugendschutz.net, welche die KJM und die Landesmedienanstalten im Bereich der Telemedien nach § 18 JMStV unterstützt.

1Amtliche Begründung, Landtag von Baden-Württemberg, Drs. 13/1551, S.26.

2Statt Vieler: Dreier-Schutze-Fielitz, Art. 5 I, II, Rn. 173.

3Schumann, ZUM 2004, 697, 703; vorsichtiger Nikles/Roll/Spürck/Umbach, § 4 JMStV, Rn. 39.

Nach § 19 JMStV sind Einrichtungen der Freiwilligen Selbstkontrolle anzuerkennen, wenn sie dies beantragen und die Voraussetzungen des § 19 III JMStV – vor allem Unabhängigkeit und Sachkunde der Prüfer, Beteiligung gesellschaftlicher Gruppen, die sich mit dem Jugendschutz befassen und Gewährleistung der Anhörung der betroffenen Anbieter – erfüllt sind. Zuständig für die Anerkennung ist die örtlich zuständige Landesmedienanstalt. Sie trifft ihre Entscheidung durch die KJM.

Folge des Anschlusses eines Anbieters an eine anerkannte Einrichtung der Freiwilligen Selbstkontrolle ist, dass nach § 20 V JMStV eine Entscheidung der KJM über behauptete Verstöße gegen Jugendschutzvorschriften nur bei einer Zuwiderhandlung gegen § 4 I JMStV oder Überschreitung des Beurteilungsspielraumes der Freiwilligen Selbstkontrolle möglich ist. Dieses Regelungskonzept verdient einen näheren Blick aus der Sicht des Modells der „Regulierten Selbstregulierung".

b. Einrichtungen der Freiwilligen Selbstkontrolle

Einrichtungen der Freiwilligen Selbstkontrolle können nach § 19 I JMStV gebildet werden und nach § 19 III JMStV einen Antrag auf Anerkennung durch die KJM stellen. Diesem Antrag hat die KJM nach § 19 III JMStV stattzugeben, wenn dessen Voraussetzungen_erfüllt sind. Bisher[1] haben die seit 1997 bestehende Freiwillige Selbstkontrolle Multimedia sowie die Freiwillige Selbstkontrolle Fernsehen (FSF) erfolgreich Anträge auf Anerkennung gestellt[2].

(1.) Voraussetzungen der Anerkennung

Die Voraussetzungen der Anerkennung sind in § 19 III JMStV abschließend genannt: Prüfer einer Selbstkontrolleinrichtung müssen, entsprechend den Ernennungsvorschriften für Mitglieder der KJM nach § 14 III, V JMStV, unabhängig und sachkundig sein (Nr. 1), die Einrichtung muss sachgerecht ausgestattet sein (Nr. 2), den Prüfern Vorgaben für ihre Entscheidungen geben (Nr. 3), eine Verfahrensordnung besitzen, die eine Vorlagepflicht für die angeschlossenen Veranstalter und Sanktionsmechanismen regelt sowie eine Antragsbefugnis von Trägern der Jugendhilfe vorsieht (Nr. 4), den Anbietern vor der Entscheidung die Möglichkeit einer Anhörung bieten (Nr. 5) und eine Beschwerdestelle eingerichtet haben (Nr. 6).

Auffällig sind eine gewisse Ähnlichkeit mit Verwaltungsverfahren sowie die Möglichkeit der Selbstkontrolleinrichtungen, einen eigenen, gerichtlich nicht nachprüfbaren Beurteilungsspielraum

---

1Stand: 25.10.2007.

2Pressemitteilungen der KJM vom 01.12.2004 und 24.06.2003, abrufbar unter: http://www.alm.de/gem_stellen/presse_kjm/pm/011204.htm und www.kjm-online.de.

wahrzunehmen, da sie nach der vorliegenden Konzeption die von der Rechtsprechung aufgestellten Voraussetzungen für unabhängige, pluralistisch zusammengesetzte Expertengremien erfüllen.

Zur Steigerung der Transparenz wäre eine Pflicht zur öffentlichen Dokumentation der Entscheidungen wünschenswert. Einer Meldepflicht für schwere Verstöße[1] bedarf es nicht unbedingt, da anzunehmen ist, dass *v*iele Beschwerden erst über die KJM an die Selbstkontrolleinrichtungen gelangen oder im Falle evidenter schwerer Verstöße unmittelbar eine Anzeige erfolgen wird. Des Weiteren würde sie dazu führen, dass sich Anbieter im Zweifelsfall nicht an die Selbstkontrolleinrichtungen anschließen, wenn sie eine Meldung von Verstößen befürchten müssen.

Bei nicht kooperierenden Anbietern kann indessen keine Meldepflicht bestehen, da Selbstkontrolleinrichtungen gegen diese keine Maßnahmen ergreifen können.

(2.) Rechtsfolgen der Anerkennung

Nach § 19 II JMStV überprüfen anerkannte Einrichtungen im Rahmen ihrer Satzungen die Einhaltung der Vorschriften des JMStV sowie der von der KJM erlassenen Richtlinien und Satzungen. Anders als beim Rundfunk, besteht für Telemedien keine Vorlagepflicht des Anbieters, bevor er diese zugänglich macht. Die KJM kann daher bei behaupteten Verstößen nicht direkt gegen den Anbieter vorgehen, sondern es muss sich nach § 20 V JMStV zunächst die Einrichtung der freiwilligen Selbstkontrolle mit dem Sachverhalt befassen. Ein Einschreiten nach § 20 I JMStV gegen den Anbieter ist nur möglich, wenn die Entscheidung der Einrichtung der Freiwilligen Selbstkontrolle „den Beurteilungsspielraum überschreitet“. Dies soll insbesondere dann der Fall sein, wenn Rechtsbegriffe falsch ausgelegt werden oder eine unzutreffende Tatsachenermittlung vorliegt[2]. Der Gesetzgeber erwähnt also – dies hat einen gewissen Seltenheitswert – einen Beurteilungsspielraum der Selbstkontrolleinrichtungen[3]. Inwieweit dieser vorliegt und welche Folgen er hat, ist allerdings nicht so klar, wie es im JMStV erscheinen mag.

(a.) Beurteilungsspielraum der Selbstkontrolleinrichtungen

Nach § 20 III, V JMStV kann die KJM nur gegen von anerkannten Selbstkontrolleinrichtungen überprüfte Inhalte vorgehen, wenn deren Entscheidung „die Grenzen des Beurteilungsspielraums“ überschreitet. Daraus kann geschlossen werden, dass den Selbstkontrolleinrichtungen ein Beurteilungsspielraum bei ihren Entscheidungen zustehen soll.

Das Konzept des Beurteilungsspielraums wurde Mitte der 50er Jahre von Bachof[4] und Ule[5] als Möglichkeit der Differenzierung vom gerichtlich nur eingeschränkt nachprüfbaren Ermessen auf der

1So aber Nikles/Roll/Umbach/Spürck, § 19 JMStV, Rn. 6.

2Begründung zu § 20 III JMStV, Landtag von Baden-Württemberg, Drs. 13/1551.

3So auch die Begründung zu § 20 III JMStV, z.B. Landtag von Baden-Württemberg, Drs. 13/1551.

4Bachof, JZ 1955, 97ff.

5Ule, S. 309ff.

Rechtsfolgenseite entwickelt. Anfangs wurden unbestimmte Rechtsbegriffe nur auf ihre Auslegung, nicht aber auf die Anwendung im Einzelfall hin überprüft[1]. Inzwischen hat sich die umfassende gerichtliche Kontrolle unbestimmter Rechtsbegriffe durchgesetzt. Dies gilt jedoch nicht für bestimmte – seltene – Fälle, in denen der Verwaltung ein gerichtlich nicht nachprüfbarer Beurteilungsspielraum zugestanden wird. Ein solcher könnte in § 20 III, V JMStV durch die Bezugnahme auf den „Beurteilungsspielraum" begründet worden sein. Zu den Fallgruppen[2], bei denen Beurteilungsspielräume von der Rechtsprechung unabhängig von einer gesetzlichen Zuweisung angenommen werden, zählen auch Wertentscheidungen von pluralistisch zusammengesetzten Expertengremien, die moralische oder künstlerische Werturteile zu treffen haben und, um einen eigenen Beurteilungsspielraum auch in grundrechtlich relevanten Bereichen annehmen zu können, weisungsfrei und unabhängig sein müssen. Des Weiteren bedürfen sie einer gesetzlichen Einrichtung und müssen entscheidungsadäquat zusammengesetzt sein[3]. In derlei Fällen kann ein Gericht jedenfalls nicht sachgerechter entscheiden als ein entsprechend zusammengesetztes Gremium. Der Entscheidung des letzteren kommt außerdem der Mehrwert einer unabhängigen Entscheidung zu[4].

Die Zulassungsvoraussetzungen des JMStV für anerkannte Einrichtungen der Freiwilligen Selbstkontrolle nehmen auf all diese Elemente für die Anerkennung eines unabhängigen Entscheidungsspielraums Bezug. Allerdings greift der JMStV in zwei Punkten zu kurz: Zum einen handelt es sich genau genommen nicht um einen herkömmlich verstandenen Beurteilungsspielraum, weil der Spielraum der Selbstkonkontrolleinrichtungen nur gegenüber der KJM gilt und es sich nicht um eine Letztentscheidungsbefugnis, sondern lediglich um eine Überprüfungsbefugnis handelt, was der Auffassung eines nicht überprüfbaren Beurteilungsspielraumes entgegen steht[5]: Wenn schon gegenüber der KJM kein Beurteilungsspielraum gegeben ist, kann man diesen erst recht nicht gegenüber Gerichten annehmen. Andernfalls käme es zu der paradoxen Situation, dass die Selbstkontrolleinrichtungen oder die Regulierten sich gerichtlich gegen Entscheidungen der KJM wenden würden, diese zwar nicht an die Einschätzung der Selbstkontrolleinrichtungen gebunden wäre, wohl aber bei einem angenommenen Beurteilungsspielraum das erkennende Gericht.

1Erichsen/Ehlers-Ossenbühl, § 10 Rn. 32.

2Übersicht u.a. bei Erichsen/Ehlers-Ossenbühl, § 10, Rn. 35ff.

3BVerfGE 83, 130, 149ff.

4Erichsen/Ehlers-Ossenbühl § 10 Rn. 37.

5Rossen-Stadtfeld, AfP 2004, 1, 8.

Auch für die KJM – deren Zusammensetzung sich eher an Sachkenntnis als an gesellschaftlicher Pluralität orientiert, wie man aus § 14 III JMStV erkennen kann – lässt der JMStV keinen Beurteilungsspielraum erkennen,

Gegen die Annahme eines Beurteilungsspielraums spricht ferner die Art der von den Selbstkontrolleinrichtungen bzw. der KJM geleisteten Prüfungsarbeit: Anders als häufig bei Expertengremien, besteht ihre Hauptaufgabe in der Konkretisierung der – notwendigerweise – unbestimmten Begriffe der §§ 4, 5 JMStV, in denen unzulässige, jugendgefährdende und entwicklungsbeeinträchtigende Angebote verboten oder Restriktionen unterworfen werden, wobei die absolut unzulässigen Inhalte in § 4 I JMStV relativ detailliert, aber teilweise in unbestimmte Begriffe („verharmlosen", „Pornographie") gefasst, abschließend aufgezählt werden. In § 4 II JMStV sind im Rundfunk und in „offenen" Telemedien unzulässige Angebote aufgelistet. Anders als in § 4 I JMStV steigt der Gehalt an unbestimmten Rechtsbegriffen in Abs. II („offensichtlich entwicklungsgefährdend", „in sonstiger Weise pornographisch") – mit Ausnahme von Nr. 2 – verhältnismäßig stark an.

Der Begriff der Pornographie ist auch nach 30-jähriger Verwendung in der Gesetzgebung nicht annähernd scharf definiert. Gleiches gilt für den Terminus „entwicklungsbeeinträchtigendes Angebot": Es liegen weder gesetzliche Definitionen noch wissenschaftliche Erkenntnisse vor; mit letzteren ist auch nicht zu rechnen[1]. Diese Erkenntnislücke lässt zwar dem Gesetzgeber eine Einschätzungsprärogvoative, führt auf der Ebene der Selbstregulierung aber dazu, dass die Selbstregulierungseinrichtungen ihren Beurteilungsspielraum in erster Linie auf der Ebene der Gesetzesauslegung ausüben: Sie müssen zunächst die Norm auslegen, bevor sie fragwürdige Inhalte bewerten können. Anders als bei hinlänglich bekannten Begriffen wie „Stand der Technik" ist inhaltlich nicht klar, was genau „Pornographie" ist. Die Einschätzung, was genau unter den unbestimmten Rechtsbegriffen zu verstehen ist, kann die KJM durch Satzungen und Richtlinien steuern[2]. Die Aufgabe der KJM bzw. der Selbstregulierungseinrichtungen besteht folglich nicht in der Feststellung einer Tatsachengrundlage, sondern in einer juristischen Definition: Steht diese fest, ergibt sich die Bewertung als simple Subsumption quasi von selbst. Genau genommen handelt es sich also nicht um einen Beurteilungsspielraum, sondern der Gesetzgeber überlässt den Selbstkontrolleinrichtungen schlicht die grundlegende Normkonkretisierung. Wenn die KJM durch ihre Satzungen und Richtlinien allerdings in diese eingreift, verschwindet auch dieser Auslegungsspielraum.

1Wissenschaftliche Erkenntnisse sind auch durch die Natur der durchzuführenden Experimente, die notwendigerweise gegen den Jugendschutz und wohl auch gegen die Menschenwürde verstoßen müssten, ausgeschlossen. Man müsste für aussagekräftige Ergebnisse Jugendliche kontrolliert dem Einfluss der unzulässigen Inhalte aussetzen.

2So ausdrücklich die amtliche Begründung zu § 20 III JMStV, Landtag von Baden-Württemberg, Drs. 13/1551. Eine Ermächtigung zum Erlass von Satzungen für die KJM findet sich im JMStV nicht.

Es besteht indes auch sachlich kein Grund, für die Definition unbestimmter Rechtsbegriffe einen Interpretationsspielraum zu schaffen, der frei von behördlicher und gerichtlicher Überprüfung bleiben soll. Im Strafrecht ist den Richtern die Auslegung und Anwendung derselben Begriffe möglich. Es liegt mithin auch von der Grundlage der Lehre vom Beurteilungsspielraum her keine Notwendigkeit eines Freiraums der Selbstkontrolleinrichtungen oder der KJM vor. Damit soll nicht gesagt sein, dass Selbstkontrolleinrichtungen auf diesem Gebiet keine Beurteilungsspielräume zukommen können. Es soll keine generelle Verschiebung von deren Kontrollfunktionen[1] auf die Verwaltungsgerichtsbarkeit stattfinden. Um dem entgegen zu wirken, müsste allerdings die Art der von den Selbstkontrolleinrichtungen zu treffenden Entscheidungen verändert werden.

(b.) Beurteilungsspielraum der KJM

Noch weniger als im Fall der Selbstkontrolleinrichtungen kann man von einem Beurteilungsspielraum der KJM ausgehen. Ein solcher ist weder im JMStV erwähnt noch steht ihr einer nach den Kriterien der Rechtsprechung zu. Die KJM ist zwar nach ihrer Zusammensetzung laut JMStV ein unabhängiges Expertengremium, jedoch im erheblichen Maße staatlich steuerbar, da die Hälfte ihrer Mitglieder aus staatlichen Stellen entsandt werden[2]. Die restlichen Mitglieder entstammen dem Kreis der Direktoren der Landesmedienanstalten.

Die Besetzung der KJM durch staatliche Stellen richtet sich, wie in § 19 III Nr. 1 JMStV für die Selbstkontrolleinrichtungen vorgesehen, nicht nach gesellschaftlicher Pluralität, sondern gemäß § 14 III JMStV nach ihrer Sachkunde. Eine Möglichkeit breiter gesellschaftlicher Beteiligung fehlt. Ein Beurteilungsspielraum wäre angesichts der straf- und ordnungsrechtlichen Konsequenzen in §§ 23f. JMStV wohl nicht möglich. Folglich fehlen hier bereits die wesentlichen Voraussetzungen zur Annahme eines Beurteilungsspielraumes.

c. Regulierung der anerkannten Selbstkontrolleinrichtungen

Angesichts des im Widerspruch zu der Theorie der Regulierten Selbstregulierung stehenden relativ geringen Erfolges der FSM und ihrer nur zögerlichen Bemühungen um Anerkennung drängt sich die Frage nach der Umsetzung des Konzepts der Regulierten Selbstregulierung im JMStV auf.

1Schuppert, Verwaltungswissenschaft, S.536.

2Rossen-Stadtfeld, AfP 2004, 1, 8.

(1.) Umsetzung des Konzepts

Das Konzept der regulierten Selbstregulierung sieht vor, dass eine staatliche Regulierungsinstanz zwar vorhanden ist, in der Regel aber nicht eingreifen muss, weil private Selbstregulierungsgremien die eigentliche Regulierung übernehmen.

Die KJM als Aufsichtsbehörde ist Organ der Landesmedienanstalten. Sie ist zwar staatsfern[1], aber immer noch ein staatliches Organ der Regulierung und somit – nach ihrer Besetzung – deutlich staatsnäher als die Landesmedienanstalten. Sie nimmt in der Konzeption die Funktion der staatlichen Regulierungsstelle wahr. Die Selbstregulierung soll durch anerkannte Selbstkontrolleinrichtungen gewährleistet werden, zu deren Überwachung die KJM Richtlinien und Satzungen erlassen kann und wird, sobald deren Vorgehen beim Erlass eigenständiger materieller Regelungen ersichtlich wird[2]. Die KJM überprüft also nicht nur anhand von Beschwerden die Entscheidungen der Selbstkontrolleinrichtungen, sondern überwacht auch deren ständige Spruchpraxis. Verstöße gegen geltendes Recht können zu einem Widerruf der Anerkennung führen.

Die KJM nimmt in Bereichen, in denen Selbstregulierungseinrichtungen nicht existieren oder nicht anerkannt sind und gegenüber Anbietern, die keiner Selbstkontrolleinrichtung angeschlossen sind, auch die Funktion der Selbstkontrolleinrichtungen wahr und überwacht das Verhalten der Anbieter. Die Verhinderung eines Eingreifens von Seiten der KJM ist den Anbietern durch Anschluss an anerkannte Selbstkontrolleinrichtungen möglich.

(2.) Gesetzliche Vorgaben und Bewertungsspielräume

Regulierte Selbstregulierung bedarf einerseits gesetzlicher Vorgaben, um die Ziele des Gesetzgebers verwirklichen zu können und andererseits ausreichender Freiheiten für die Ausfüllung von Bewertungsspielräumen[3]: Zu starre Vorgaben verhindern die Entwicklung der angestrebten gesellschaftlichen Dynamik und würden lediglich zu einer Delegation der Verantwortung vom Staat auf Private führen, die angesichts der mit der Tätigkeit der Privaten einhergehenden Grundrechtseinschränkungen als bedenklich zu bewerten wäre.

(3.) Gelingen der Regulierten Selbstregulierung

Wie oben ausgeführt[4], ist das Steuerungskonzept der Regulierten Selbstregulierung von einer breiten Beteiligung der Betroffenen abhängig. Davon scheint der Gesetzgeber stillschweigend auszugehen,

1Ring, AfP 2004, 9, 13.

2Ring, AfP 2004, 9, 13.

3Rossen-Stadtfeld, AfP 2004, 1, 4.

4S.o. S.36.

wenn er in § 19 JMStV gerade dies nicht zur Voraussetzung für die Anerkennung einer Einrichtung der Freiwilligen Selbstkontrolle macht. Ob aber in der FSM die Interessen der im Interessenverband Neue Medien e.V. (IVNM) organisierten so genannten „Adult-Industrie“ gewahrt bleiben, ist nicht sicher, da eine Deckung aller Interessen in der vielgestaltigen Gruppe der Anbieter von Online-Services schwer bis nicht realisierbar erscheint[1]. Es besteht die Notwendigkeit gesetzlicher Regelungen, die zumindest versuchen, Machtungleichgewichte zwischen den in den Einrichtungen der Regulierten Selbstregulierung zusammengeschlossenen Privaten zu kompensieren[2], wie sie etwa bei AOL Deutschland, der Deutschen Telekom oder der erodata GmbH[3] und dem IVNM vorliegen. Jedoch ist diesem Erfordernis bisher nicht nachgekommen worden, und Äußerungen des Vorsitzenden der KJM, Prof. Dr. Ring, legen zudem nahe, dass die KJM ihre Aufmerksamkeit diesem Problem nur bei einer Gefährdung des Jugendschutzes widmen wird[4].

Da die verhältnismäßig kleine „Adult-Industrie“ nicht über hinreichende Mittel zum Aufbau einer der FSM vergleichbaren Organisation verfügen dürfte, scheinen eine Regulierung durch den Markt bzw. das Konzept der Regulierten Selbstregulierung hier nicht umsetzbar[5].

Angesichts der Äußerungen ihres Vorsitzenden, etwa bezüglich eines nicht bestehenden Interesses an an einer deutschen Porno-Industrie[6] oder der von der „seriösen Industrie“ intendierten, sachgerechten Beseitigung der Probleme[7], kann davon ausgegangen werden, dass das Ziel der KJM in der Vertreibung deutscher Porno-Anbieter aus dem Internet besteht. Für den Jugendschutz stellt dies allerdings keinen Gewinn dar, da die Angebote, anders als beim Rundfunk, problemlos auch aus dem Ausland den Weg nach Deutschland finden und Filter diesbezüglich wenig bis nichts ausrichten können.

Ein weiteres Problem für das Verhalten der anerkannten Selbstkontrolleinrichtungen bilden die Richtlinien und Satzungen der KJM, die den „Beurteilungsspielraum“, der, wie gezeigt, auf der Ebene der Normauslegung liegt, praktisch komplett beseitigen können[8]. Des Weiteren schwebt die Möglichkeit der Länder, den JMStV nach drei Jahren ganz oder teilweise zu kündigen, wie ein Damoklesschwert über den Selbstkontrolleinrichtungen, die, selbst wenn sie sich innerhalb des

1Anders ist dies häufig bei so genannten Netzaktivisten oder der technischen Ebene, wo sich die Interessen eher decken.

2Schmidt-Aßmann, S.263.

3Hersteller von Altersverifikationssystemen.

4Vgl. Ring, AfP 2004, 9ff.

5Betrachtet man freilich das Gelingen Regulierter Selbstregulierung in einer weitgehenden Freiheit von jugendgefährdenden Angeboten auf deutschen Servern, ist ein Erfolg wahrscheinlich. Wünschenswerter wären allerdings eine Verbesserung des Jugendschutzes und ein Ausgleich der widerstreitenden Interessen.

6Ring, AfP 2004, 9, 12.

7Ring, AfP 2004, 9, 12.

8Kreile/Diesbach, ZUM 2002, 849, 855.

Beurteilungsspielraums befinden, über den Umweg dieser Kündigung ihre Aufgabe verlieren können, und lässt eine gewisse strengere Tendenz bei der Ausübung der Befugnisse befürchten[1].
Erstaunlich ist hingegen, dass die Entwicklung und Beurteilung von Jugendschutzprogrammen nicht zum Aufgabenbereich der Selbstkontrolleinrichtungen gehört. Speziell erstere ist angesichts der einerseits notwendigen ständigen Anpassung an sich ändernde technische Möglichkeiten und dem andererseits anzunehmenden Wissensmangel auf Seiten des Staates von selbigem nicht zu erwarten. Obgleich der PICS-Standard bereits seit 1997 definiert ist, haben sich private Softwareanbieter dem Bereich des Jugendschutzes kaum angenommen, sodass weder darauf aufbauende noch sonstige, nach § 11 JMStV anerkennungsfähige, Programme existieren. Daher könnte eine diesbezügliche Aktivierung gesellschaftlicher Dynamik sicher als unschädlich und auch weniger bedenklich als im Bereich der Inhaltskontrolle gewertet werden. Die behördliche Anerkennung nach § 11 II 2 JMStV könnte problemlos durch eine Zertifizierung durch die Selbstkontrolleinrichtungen ersetzt werden.

(4.) Verfassungsmäßigkeit der Aufsicht durch die KJM und die Selbstkontrolleinrichtungen

Ziel des Jugendmedienschutzes und somit auch des JMStV ist der Schutz der Jugend vor möglichen Gefahren durch Medieninhalte. Allein aus der Zielsetzung in § 1 JMStV ergibt sich dessen präventive Zielrichtung. Die Gefahrenabwehr gehört jedoch zum Kernbereich der Staatsaufgaben[2] und ist als Hoheitsaufgabe nach Art. 33 IV GG in der Regel unmittelbar durch staatliche Organe durchzuführen[3] und nur ausnahmsweise durch Beliehene[4]. Der genaue Umfang des Begriffs „hoheitsrechtliche Befugnisse“ ist unklar[5], die Eingriffsverwaltung ist ihm allerdings in jedem Falle zugehörig[6]. Von Art. 33 IV GG genannte Ausnahmen vom Funktionsvorbehalt liegen vor, wenn die Ausübung der Hoheitsbefugnisse nicht ständig geschieht oder wenn die Verrichtung durch Nicht-Beamte den Ausnahmefall darstellt. Von einer ständigen Ausübung ist zu sprechen, wenn diese kontinuierlich und auf unabsehbare Dauer geschieht[7], nicht aber, wenn die Aufgabe selbst oder ihre Verrichtung vorübergehend sind[8]. Ob eine ausnahmsweise erfolgte Übernahme als zulässig gilt, hängt von sachlichen Kriterien ab[9]; Hilfs- und Vorbereitungsdienste fallen nicht unter den Funktionsvorbehalt des Art. 33 IV GG[10].

1Kreile/Diesbach, ZUM 2002, 849, 855.

2Schoch in: Schmidt-Aßmann, S.126f.

3Schoch in: Schmidt-Aßmann, S.130.

4Schoch in: Schmidt-Aßmann, S.130.

5Sachs-Battis, Art. 33 Rn. 55, HdbStR-Lecheler, § 72 Rn. 26.

6HdbStR-Lecheler, § 72 Rn. 27; Sachs-Battis, § 33 Rn. 55; AK-Schuppert, § 33 IV, V Rn. 25; Dreier/ Lübbe-Wolff, Art. 33 Rn. 57.

7Jarass/Pieroth-Pieroth, Art. 33 Rn. 30 f.

8Wächter, NJW 1997, 329, 330.

9Wächter, NJW 1997, 329, 330.

10Umbach/Clemens-Dollinger/Umbach, Art. 33 Rn. 79.

Im Zuge der veränderten Aufgabenwahrnehmung des Staates verändern sich auch die Pflichten der Beamten[1]: Je mehr sich der Staat auf die Überwachung beschränkt, desto mehr muss die Durchführung durch Beamte geschehen. Traditionelle Aufgaben staatlichen Handelns wie etwa die Sicherheitsgewährung können allerdings nicht delegiert werden, hier trägt der Staat die Vollzugsverantwortung[2]. Eine ausnahmsweise erfolgende Abgabe von Kompetenzen ist aber verfassungsrechtlich nicht zu kritisieren, wenn deren neuen Trägern ausreichende demokratische Legitimation vermittelt wird, die hoheitlichen Aufgaben nicht dauerhaft wahrgenommen werden und andere gewichtige sachliche Punkte für eine Vergabe an nicht in Dienst- und Treueverhältnissen stehende Personen sprechen[3]. Dies kann der Fall sein, wenn eine gewisse Staatsferne angestrebt wird und zu diesem Zweck gesellschaftliche Gruppen eingebunden werden sollen[4]. Die besonderen

Fähigkeiten[5], die pluralistisch zusammengesetzte Gremien dem Staat voraus haben[6], sind speziell bei Entscheidungen mit einem gewissen Presse- oder Kunstbezug von Belang[7]. Vor diesem Hintergrund ist die Einschaltung von Selbstkontrolleinrichtungen ohne Entscheidungskompetenz unproblematisch[8], die Konstruktion der KJM hingegen erscheint kritisch. Hier soll sich, anders als bei der Bundesprüfstelle für jugendgefährdende Medien (BPjM), der Nachfolgerin der

Bundesprüfstelle für jugendgefährdende Schriften (BjS), mit der sich BVerfGE 83, 130ff. befasst hatte, die Auswahl der Mitglieder trotz Staatsferne nach Sachkunde und nicht nach ausgewogener gesellschaftlicher Repräsentation richten[9].

Eine gewisse Staatsferne ist Bedingung für eine staatlich organisierte Aufsicht über Medien, da diese andernfalls schnell in staatliche Zensur ausarten könnte. Dem soll Genüge dadurch getan werden, dass nach § 14 IV JMStV Beteiligte bestimmter Exekutiv- oder Legislativorgane nicht Mitglieder der KJM werden können. Allerdings sind die Mitglieder zur Hälfte Direktoren der

1Schuppert, AK Art. 33 IV, V, Rn. 31ff.

2Schuppert, AK, Art. 33 IV, V, Rn 32.

3BVerfGE 83, 130, 150.

4BVerfGE 83, 130, 150 zu § 9 GjS.

5Wächter, NJW 1997, 329, 332.

6Für die Beurteilung technischer Fragen müssen Gerichte in der Regel Gutachter herbeiziehen, so dass auch die Gerichtsentscheidungen „fremdgesteuert“ sind. Ebenso wie die Gerichte sind die Expertengremien mit Beurteilungsspielraum unabhängig, daher ist kein sinnvoller Grund für eine Vollkontrolle zu sehen.

7BVerfGE 83, 130, 150.

8Für die BPjM (früher BjS) ist ein Beurteilungsspielraum strittig, dafür: BVerwGE 91, 211, 215; dagegen OVG Münster NvwZ 92, 396f.

9In der BPjM sind gesellschaftliche Gruppen repräsentiert.

Landesmedienanstalten. Die übrigen Beteiligten werden von staatlichen Jugendschutzstellen ernannt und sind nur in Ausnahmefällen Vertreter gesellschaftlicher Gruppen oder Wissenschaftler[1].

Den Mitgliedern der KJM kommt in der Regel keine Einzelentscheidungsbefugnis zu: Die Entscheidungen werden in Prüfausschüssen vorbereitet, denen allerdings stets ein Vertreter der KJM angehören muss und die aufgrund ihrer Funktion in jedem Fall staatsfern zu besetzen sind. Die KJM selbst nimmt aber üblicherweise[2] nur Überwachungs- und Vollzugsaufgaben wahr, für die kein Erfordernis einer Staatsferne, wie sie bei Selbstkontrolleinrichtungen oder Prüfausschüssen gegeben ist, besteht; dies wird auch aus der Besetzung der KJM ersichtlich.

Ein weiteres Problem ergibt sich daraus, dass es gegen die Entscheidungen der KJM keine Beschwerdeinstanz gibt, diese also endgültigen Charakter haben.

Wenn sich aber die Funktion des Staates, wie im Fall der KJM, von der Übernahme von Aufgaben zur Überwachung ihrer Durchführung hin verschiebt, müssen sich auch die Aufgaben von Beamten verändern. In dem Maße, in dem der Staat die Durchführung von hoheitlichen Aufgaben an Private abgibt und deren Ausführung nur noch kontrolliert, ist zu fordern, dass eben diese Beaufsichtigung – die sich in der Regel nur auf die Einhaltung rechtlicher Regelungen bezieht – durch Beamte durchgeführt wird. Da für diese Form der Kontrolltätigkeit keine besondere Sachkenntnis erforderlich ist, entfällt der sachliche Grund für eine Durchführung durch Nicht-Beamte. Somit wird eine Wahrnehmung der Überwachungsaufgaben durch Beamte möglich, die bei einer inhaltlichen Beaufsichtigung aufgrund der zu gewährleistenden Staatsferne nicht zulässig wäre. Die Überwachung wird auf unvorhersehbare Zeit notwendig und damit regelmäßig durch Beamte auszuführen sein[3]. Weder die Selbstkontrolleinrichtungen, die keine Entscheidungskompetenz besitzen, noch die staatsfern zusammengesetzte KJM genügen diesen Anforderungen; die Kontrolle der Selbstkontrolleinrichtungen hat mithin durch Beamte – entweder bei der KJM oder einem eigenständigen Kontrollgremium – zu erfolgen.

(5.) Gerichtliche Kontrolle

Die aufgeworfenen Mängel und Unklarheiten werfen die Frage auf, ob eine abschließende regulierte Selbstregulierung in hinsichtlich des Grundrechts sensiblen Bereichen zulässig ist oder ob zusätzlich die Notwendigkeit einer weitergehenden gerichtlichen Kontrolle besteht. Dabei ist zunächst nicht die Art der Entscheidungsfindung zu kritisieren, jedoch deren staatliche Kontrolle im Falle des

1Von den zwölf Mitgliedern gehören nur ein Mitglied und drei Stellvertreter von „ordentlichen“ Mitgliedern nicht staatlichen Jugendschutzbehörden oder Landesmedienanstalten an. Auch der Präsident der Bundeszentrale für politische Bildung ist wohl nicht „staatsfern“.

2Wenn das Ziel der weitgehenden gesellschaftlichen Selbstregulierung erreicht ist. In diesem Moment ist die Erstentscheidungsbefugnis der KJM auf die Zulassung und Überwachung von Selbstkontrolleinrichtungen und Jugendschutzprogrammen beschränkt, die weniger Probleme bereiten als inhaltliche Entscheidungen.

3Die BPjM übt selbst eine weitgehende Kontrolle aus, sie überwacht nicht, wie die KJM, Selbstkontrolleinrichtungen. Daher bereitet die Staatsferne der BPjM weniger Probleme, zumal sie pluralistisch zusammengesetzt ist.

JMStV. Durch die Einschaltung von Selbstkontrolleinrichtungen, die zwar keine rechtliche, aber eine faktische Entscheidungsbefugnis haben, wird zunächst der Staat entlastet; es bieten sich auch Möglichkeiten kooperativen Vorgehens, das wegen der Einbeziehung der Betroffenen im Vorfeld und bei der Entscheidungsfindung mit einiger Wahrscheinlichkeit eher akzeptiert werden wird als eine staatliche Eingriffsverwaltung. Die Gesetzgebung verwendet allerdings notwendigerweise unbestimmte Rechtsbegriffe, um den Selbstkontrolleinrichtungen einen eigenen Spielraum für deren Ausfüllung und Anwendung zu gewährleisten. Diese verfügen über eigene Entscheidungsbefugnisse[1] oder werden durch Expertengremien mit Letztentscheidungsbefugnis überwacht. Zwar haben, wie gezeigt, weder die Selbstkontrolleinrichtungen noch deren Überwachungsgremien entgegen dem Wortlaut des JMStV einen Beurteilungsspielraum, jedoch benötigen sie diesen im Bereich des Jugendschutzes, im Gegensatz zu anderen Expertengremien, wegen der überwiegend rechtlichen Überprüfung nicht. Gerichte können ebenso gut wie die KJM beurteilen, ob die unbestimmten Rechtsbegriffe korrekt angewandt wurden[2]. Dies widerspricht der ständigen Rechtsprechung zu Beurteilungsspielräumen bei pluralistischen Expertengremien. Eine gerichtliche Überprüfung erscheint hier indes geboten und auch durchführbar, da im Strafrecht von den Richtern dieselben Begriffe angewandt werden. Daher ist auch auf der Seite der Überprüfung der Entscheidungen kein Grund für einen Beurteilungsspielraum ersichtlich. Entscheidungen der KJM und der Selbstkontrolleinrichtungen sind mithin voll überprüfbar.

7. JuSchG

Parallel zum JMStV der Länder wurde das Jugendschutzgesetz des Bundes (JuSchG) beschlossen. Es umfasst die medienrechtlichen Regelungen des bisherigen JÖSchG und GjSM. Ziel war, gemeinsam mit dem JMStV der Länder eine umfassende, vereinheitlichende Neuregelung des Jugendmedienschutzes zu erreichen[3].

a. Anwendungsbereich

Der Anwendungsbereich des JuSchG bei Medien ist im 3. Abschnitt geregelt. Bezüglich des Internets sind insbesondere §§ 12 II, III Nr. 2, IV und 15 JuSchG relevant. Nach seiner generellen Konzeption stellt das JuSchG zwar auf die herkömmlichen jugendgefährdenden Angebote ab, setzt aber in § 1 II 2 JuSchG körperliche Trägermedien mit der elektronischen Verbreitung von auf

1Dies ist gerade nach dem JMStV nicht der Fall; auch deshalb ist die gesetzliche Bezeichnung eines Beurteilungsspielraumes unpassend.

2Anders stellt sich dies bei Beurteilungen von Prüfungsleistungen oder der Frage nach dem aktuellen Stand der Technik dar.

3BT Drs. 14/9013 S.1.

körperlichen Trägermedien gespeicherten Angeboten gleich[1]. Im Sinne des § 2 II JuSchG sind Trägermedien nur solche, die ohne Weiteres zur Weitergabe bestimmt sind[2]. Dies betrifft die Speicherung auf zur Weitergabe bestimmten Medien, die von anderen Rechnern aus abgerufen werden können, nicht aber lokale Festplatten[3]. Voraussetzung für einen Abruf von Inhalten über das Internet ist allerdings eine lokale Speicherung, in der Regel auf einer Festplatte bzw. auf dem Server eines Anbieters. Vom JuSchG umfasst wäre nur eine Speicherung auf beispielsweise per Internet zugänglichen CDs oder DVDs. Diese Regelung lässt das JuSchG für das Angebot von per Internet abrufbaren Informationen praktisch bedeutungslos werden, da diese in der Regel nicht auf Datenträgern gespeichert werden, die zur Weitergabe bestimmt sind. Nach § 1 IV JuSchG wird der elektronische Versandhandel dem herkömmlichen gleichgestellt, so dass das Versenden von Daten als Tele- oder Mediendienst ebenfalls vom JuSchG abgedeckt wird. Allerdings dürfte sich der praktische Nutzen als gering erweisen, da nach §§ 12, 15 JuSchG nur das Versenden von Träger- bzw. Bildmedien nach dem JuSchG unzulässig ist und es sich bei Telemedien nicht um Trägermedien handelt[4].

b. JuSchG und Telemedien

Für Telemedien ist in der Regel nicht das JuSchG**,** sondern der JMStV einschlägig. Das JuSchG ist, wie gezeigt, nur in Ausnahmefällen auf Telemedien anwendbar. Eine Sonderregelung enthält allerdings § 12 II 3 , wonach Anbieter von Telemedien bei der Vorführung von Filmen und Spielprogrammen auf eine vorhandene Kennzeichnung ihres Angebots hinweisen müssen. Diese Kennzeichnungspflicht bezieht sich aber nicht auf den JMStV, sondern auf das JuSchG und bleibt somit deutlich hinter den Anforderungen des JMStV zurück, welche die Programmierung jugendgefährdender Angebote für Jugendschutzprogramme oder den Schutz durch Altersverifikationssysteme beinhalten. Wie dieser Konflikt zu lösen ist, ist bislang unbekannt, es bieten sich jedoch mehrere Möglichkeiten an: Beispielsweise könnte das JuSchG lediglich zusätzlich zum JMStV gelten oder eine Vorrangsregelung zugunsten des JuSchG oder des JMStV geschaffen werden.

(1.) Ausschließliche Anwendung des JMStV

Für eine Anwendung des JMStV könnte die fehlende Gesetzgebungskompetenz des Bundes für Mediendienste sprechen. Zwar steht dem Bund nach Art. 74 I Nr. 7 GG eine konkurrierende Kompetenz für den Bereich des Jugendschutzes zu[5], jedoch liegt die alleinige Zuständigkeit für das

1Gemeint ist die elektronische Verbreitung von Angeboten, die auf körperlichen Trägermedien gespeichert sind.

2Liesching NJW 2002, 3281, 3284.

3Liesching NJW 2002, 3281, 3284.

4Liesching NJW 2002, 3281, 3284.

5BVerfGE 31, 113, 117; Jarass/Pieroth Art. 74 Rn. 17.

Gebiet der Mediendienste bei den Ländern und soll außerdem durch eine „Annexkompetenz“ für den Jugendschutz im Bereich der Online-Medien ergänzt werden[1]. Durch die Aufhebung der auf Telemedien anwendbaren Regelugen von JÖSchG und GjSM hat der Bund den Weg für eine Regelung durch die Länder geebnet. Nach der Gesetzesbegründung wollte der Bund gerade keine eigenen Regelungen für Telemedien im Bereich des Jugendschutzes treffen[2].
Für diese Lösung spricht, dass die Länder nach der Begründung des JuSchG ausschließlich für die Regelung von Telemedien zuständig sein sollen[3]. Allerdings ist nicht davon auszugehen, dass eine – wenn auch vom Sinngehalt her fragliche – Norm existierte, wenn der Gesetzgeber nicht davon ausginge, dass diese auch Anwendung finden solle. Ein sinnvoller Anwendungsbereich im Telemedienbereich ist allerdings angesichts des JMStV kaum erkennbar.

(2.) Ergänzung des JMStV durch das JuSchG

§ 12 II 3 JuSchG lässt sich so auslegen, dass lediglich für Filme zusätzlich zu den Anforderungen des JMStV die Bekanntgabe der Kennzeichnung auf der Seite des Anbieters neben einem Altersverifikationssystem, einer Programmierung für Schutzprogramme oder einer Zeitbeschränkung vorgesehen sei. Eine weitere Kennzeichnung neben einem AVS böte einerseits keine zusätzliche Schutzwirkung, hätte andererseits aber den Vorteil, dass auf diese Weise die Jugendschutzbestimmungen für Filme auf Trägermedien und Telemedien in Übereinstimmung gebracht würden.

(3.) § 12 II 3 JuSchG als Spezialregelung

§ 12 II 3 JuSchG könnte als Spezialregelung interpretiert werden, welche im eng begrenzten Anwendungsbereich der Filmvorführungen über Telemedien die Regeln des JMStV verdrängt. Dies gälte, wenn es sich um eine abschließende Regelung handelte, da den Ländern in diesem Fall aufgrund der Bundeskompetenz aus Art. 74 I Nr. 7 GG keine Regelungskompetenz mehr zustünde. Gegen diese Auslegung sprechen jedoch das Ziel der Verbesserung des Jugendschutzes – von effektiver Zugangsverhinderung kann bei einer bloßen Kennzeichnung kaum die Rede sein – sowie die Einheitlichkeit der Regelungen für Filme, die nur über Telemedien angeboten werden und solche, die auch auf herkömmlichen Trägermedien angeboten werden. Auch ist aus der Gesetzesbegründung erkennbar, dass der Bund keine Gesetzeskompetenz für Telemedien begründen wollte[4].

1So BT Drs. 14/9013, S.13.
2BT Drs. 14/9013, S.13.
3BT Drs. 14/9013, S.13.
4BT Drs. 14/9013, S.13.

8. Zusammenfassung

Die Regelungen des JMStV sind in weiten Teilen mangelhaft und lassen befürchten, dass sie im Bereich des Internets dem eigentlichen Ziel des Gesetzgebers widersprechende Ergebnisse zeitigen. Es besteht die Gefahr, dass sich auch der JMStV in die Reihe der Produkte symbolischer Gesetzgebung einreihen und somit das Ziel des Jugendschutzes nicht gestärkt, sondern vielmehr geschwächt wird.

Der Kreis der potentiell Verpflichteten wird augenscheinlich durch einen Fehler des Gesetzgebers zu weit gezogen, so dass auch die lediglich technisch Beteiligten umfasst sind; die KJM will wohl auch diese zur Mitwirkung am Jugendschutz heranziehen.

Die Umsetzung des Konzepts der Regulierten Selbstregulierung scheitert am mangelnden Vertrauen des Gesetzgebers gegenüber den sich bildenden Selbstkontrolleinrichtungen, die jedoch in anderen Bereichen bisher sehr zufriedenstellende Arbeit geleistet haben. Die eröffneten Bewertungsspielräume könnten durch Richtlinien der KJM fast vollständig beseitigt werden. Gegenüber Gerichten wird den Selbstkontrolleinrichtungen – obwohl der Gesetzgeber einen „Beurteilungsspielraum“ erwähnt, was eine Seltenheit darstellt – gerade kein Freiraum eingeräumt, für den allerdings auch kein Bedarf besteht.

Eine staatsferne Besetzung der KJM ist zwar für ihre eigenen Kontrollaufgaben in der Inhaltskontrolle notwendig, soll allerdings nach der Konzeption der „Regulierten Selbstregulierung“ nur eine Ausnahme darstellen. Für die Überwachung der Selbstkontrolleinrichtungen wäre eine staatliche Besetzung erforderlich. Die Anerkennung von Jugendschutzprogrammen könnte von Selbstkontrolleinrichtungen übernommen werden. Sollte sie Aufgabe der KJM bleiben, böte sich, wie auch hinsichtlich der Kontrolle der Selbstkontrolleinrichtungen, eine Durchführung durch Beamte an – die Notwendigkeit der Staatsferne besteht jedenfalls nicht. Es wäre indes sinnvoll, in der KJM zwei Entscheidungsgremien einzurichten: Eines sollte staatsfern und mit der inhaltlichen Überwachung von Inhalten sowie der Überwachung der Selbstkontrolleinrichtungen beauftragt sein, das andere staatsnah und mit den übrigen Aufgaben der KJM befasst sein.

Zusammenfassend kann festgehalten werden, dass der JMStV die bereits früh befürchtete Gefahr birgt[1], dass er durch ein Auswandern der Regulierten seinen praktischen Anwendungsbereich verlieren und der Funktionsverlust durch den Gesetzgeber noch gefördert wird.

IV. SPAM

Das Wort Spam steht für spiced ham, eine Art gewürztes Dosenfleisch, das 1937 erfunden wurde und im Zweiten Weltkrieg zu zweifelhafter Berühmtheit gelangte. In einem Sketch der britischen

1Trute, VVDStRL 57, 216, 248.

Komikergruppe Monty Python[1] verhindert eine Horde Wikinger in einem Restaurant, in dem alle Gerichte mit Spam zubereitet werden, jegliche Verständigung durch das laute Wiederholen von „Spam, Lovely Spam“. Auf diesen Sketch bezieht sich die übertragene Bedeutung des Wortes heutzutage: unerwünschte Kommunikation, welche die gewollte Kommunikation überlagert und dadurch unmöglich macht. Dies geschieht vor allem durch unerwünscht zugesandte Massen-E-Mails bei individuellen E-Mail-Accounts sowie durch Einsenden großer Mengen sinnloser und themenfremder Beiträge in Newsgroups. Meist handelt es sich bei Spam um Werbung für mehr als zweifelhafte Produkte. Nach Schätzungen sollen ca. 40-80%[2] aller weltweit versandten E-Mails Spam sein. Dieses Volumen wird als Bedrohung für die Benutzbarkeit von E-Mail angesehen[3]. Um gegen diese Bedrohung und Belästigung vorzugehen, wurden in vielen Staaten[4] Gesetze verabschiedet, welche die Zusendung von Werbe-Mails nur bei vorangegangener Bestellung des Empfängers erlauben und ansonsten unter Strafe stellen. In Deutschland existiert noch kein Gesetz gegen Spam; die geltende Rechtslage ähnelt aber derjenigen in Staaten, in denen solche Gesetze bereits in Kraft getreten sind. Neben rechtlichen Maßnahmen gegen Spam gibt es auf der praktischen Ebene rechtlich unproblematische Spamfilter für Mailclients und – sowohl in der Handhabung als auch rechtlich problematischere – Spamfilter für Mailserver. Auf der technischen Ebene existieren noch keine Standards bzw. Erweiterungen geltender Standards, welche die Vermeidung von Spam zum Ziel haben; sie befinden sich jedoch in der Entwicklung.

1. Gesetzliche Regelungen

Gesetzliche Regelungen verbieten gewöhnlich die Zusendung von Spam, es sei denn, die Zusendung von Werbung erfolgte auf Bestellung und mit Zustimmung des Empfängers; in diesem Fall spricht man von einer Double-Opt-In-Lösung. Die Zusendung von nicht verlangter Werbung stellt einen Eingriff in das Allgemeine Persönlichkeitsrecht und gegebenenfalls in den eingerichteten und ausgeübten Gewerbebetrieb des Empfängers dar und verstößt gegen § 1 UWG[5]. Unter Werbung fallen auch E-Mails, die auf einen Newsletter aufmerksam machen sollen. Inwieweit dies schon ohne werbende Inhalte der Fall ist, ist unklar. Das größere Problem – obwohl immer mehr Staaten Anti-Spam-Gesetze erlassen haben, steigt der Anteil von Spam am Gesamtaufkommen von E-Mail

1Den Text des Sketches findet man u.a. unter: http://bau2.uibk.ac.at/sg/python/Scripts/TheSpamSketch.

2An der juristischen Fakultät der Humboldt-Universität hat der Anteil der schon auf dem Server heraus gefilterten Nachrichten (inkl. Viren) inzwischen 90% erreicht; Brightmail geht von einem Spam-Volumen von 65% des gesamten Mailaufkommens aus: http://www.brightmail.com/spamstats.html.

3http://news.bbc.co.uk/1/hi/technology/3465307.stm; http://www.theregister.co.uk/2003/12/10/uk_antispam_law_goes_live/; http://www.heise.de/newsticker/meldung/50670.

4U.a. „Can-Spam-Act“ (USA) sowie basierend auf der EU Datenschutz-Richtlinie 2002/58/EC Großbritannien, Österreich, Dänemark, Irland, Italien und Spanien.

5Ständige Rechtsprechung seit LG Traunstein, Beschluss vom 18.12.1997, 2 HK O 3755/97, letzterer JurPC Web-Dok. 13/1998.

nach wie vor oder geht zumindest nicht zurück – liegt in der rechtlichen Durchsetzung der Regeln. Die Versender wissen sich in der Regel gut zu tarnen: Sie verwenden falsche oder einmalige Mailadressen und nutzen Mailserver, die sich vorwiegend in Russland oder in China befinden, wo zwar schnelle Verbindungen existieren, der Kampf gegen Spam aber noch nicht die Priorität wie in westlichen Staaten hat. Häufig werden so genannte offene Mailserver[1] zur Versendung genutzt, wo sich in der Regel die Spur der Versender verlieren. Die derzeitigen technischen Standards stammen noch aus der Frühzeit des Internets und enthalten keine Sicherung oder Überprüfungsmöglichkeit, um festzustellen, ob der scheinbare Absender auch der tatsächliche ist beziehungsweise wer der Absender wirklich ist. Da die Ziele von Spam-Mails vorwiegend in den USA und in Europa liegen, wird der Verfolgungsdruck auf die Versender in anderen Regionen nicht unbedingt gesteigert, und die gesetzlichen Regelungen werden überwiegend als nur wenig wirksam eingeschätzt[2]. Die deutsche Rechtsprechung dürfte die eher harmlosen Fälle der nur einmaligen Zusendung von Werbung betreffen; eine Wirkung gegen internationale Massenmails zeitigt sie nicht.

Derzeit ist wird ein internationales Abkommen unter Ägide der ITU vorgeschlagen[3], das allerdings erst von den Mitgliedsstaaten ratifiziert und umgesetzt werden muss. Auch die OECD hat eine Task-Force zur besseren Koordinierung der Anstrengungen von Staaten und der Zivilgesellschaft eingerichtet[4]. Eine schnelle Lösung des Problems auf rechtlichem Wege scheint nicht in Sicht.

2. Private Maßnahmen

Spamfilter für Heimrechner sind unproblematisch und auch relativ wirksam, verhindern aber nicht, dass Spam trotzdem auf dem E-Mail-Account ankommt und heruntergeladen werden muss. Dies verursacht Kosten sowohl bei Empfängern als auch Mail-Anbietern; des Weiteren besteht die Gefahr, dass der Account „überläuft“ und erwünschte E-Mails aufgrund dessen nicht empfangen werden können. Auch Unternehmen entstehen, neben der verlorenen Arbeitszeit der Beschäftigten, unter Umständen Kosten durch Spam. Daher gibt es verschiedene Systeme, die versuchen, zu verhindern, dass Spam überhaupt auf den Mailserver gelangt. Am häufigsten werden so genannte Blackhole-Lists verwendet, auf denen Mailserver verzeichnet sind, von denen Spam versandt wird, sowie Programme, die aufgrund inhaltlicher Merkmale von E-Mails feststellen können, ob es sich mit einiger Wahrscheinlichkeit Spam handeln könnte. Der Nachteil solcher Maßnahmen liegt darin, dass eventuell auch erwünschte Nachrichten ausgefiltert werden[5].

1Es ist bei Mailservern möglich, vor dem Versenden der E-Mail zu überprüfen, ob der Versender als autorisierter Nutzer registriert ist. Ist dies nicht der Fall, wird ((schon)) die Annahme der E-Mail verweigert. Mailserver, die diese Technik nicht nutzen, sind „offen“: Jeder kann sie zum Versenden von E-Mails verwenden. Besonders problematisch hierbei ist, dass solche Server häufig ihre IP-Nummern wechseln und daher nicht in Blackhole-Lists erfasst werden können.

2http://news.bbc.co.uk/1/hi/technology/3465307.stm.

3http://www.heise.de/newsticker/meldung/48937.

4http://www.heise.de/newsticker/meldung/5005.

5So z.B. bei AOL, http://www.heise.de/newsticker/meldung/41244.

a. Einsatz von Blackhole-Listen

In Blackhole-Listen werden Server aufgenommen, von denen aus Spam versandt worden ist. Hierfür werden die IP-Nummern der Server in eine DNS-Tabelle eingetragen. Ein Server, der eine E-Mail empfängt, stellt eine DNS-Anfrage mit der IP-Nummer des sendenden Servers an den Betreiber der Blackhole-List. Ist der sendende Server eingetragen, erhält der anfragende Server eine positive, ist er nicht eingetragen, eine negative Antwort; es handelt sich also um eine Art des „Missbrauchs“ von DNS-Anfragen[1]. Ist ein Server in einer Blackhole-Liste enthalten, werden von ihm versendete E-Mails nicht mehr angenommen. Dies soll zum Einen die Nutzer des Empfängerservers vor Spam schützen, zum Anderen den Betreiber des Senderservers dazu motivieren, Maßnahmen gegen die Versendung von Spam zu ergreifen. Die Folge der Aufnahme in eine Blackhole-Liste besteht darin, dass alle Mails von einem dort genannten Server nicht mehr an Empfänger ausgeliefert werden, die einen derartigen Blackhole-Service nutzen, was zu empfindlichen Beeinträchtigungen führen kann.
Da Blackhole-Listen in der Regel mit anderen Maßnahmen eingesetzt (werden) und hierbei Nachrichten nicht an ihren Empfänger weitergeleitet werden, ist die Nutzung eines Blackhole-Services wegen §§ 206 II Nr. 2 und 303a StGB rechtlich bedenklich.

b. Einsatz von Spam-Filtern auf Servern

Spam-Filter auf Servern verhindern zwar nicht die Annahme von Spam-Mails, leiten diese jedoch nicht an die Postfächer der Nutzer weiter, sondern legen sie entweder in einem gesonderten Ordner ab oder löschen sie sofort, wenn sie von bestimmten Viren generiert wurden. Derartige Filter werden bei vielen Mailanbietern und Unternehmen eingesetzt, um die Menge an Spam, die ihre Nutzer erreicht, sowie die Gefahren durch Viren zu verringern.
Die E-Mails werden von dem Spam-Filter einem mehrstufigen Prüfverfahren nach formalen und inhaltlichen Kriterien unterzogen[2] und erst dann an die Nutzer weitergeleitet bzw. gelöscht.
Dies könnte aber – ebenso wie der Einsatz von Blackhole-Listen – nach §§ 206 II Nr. 2 und 303a StGB strafbar sein[3], da der Mailprovider an seine Kunden gerichtete Nachrichten unterdrückt oder verändert. Bei einer Rechtfertigung ist zwischen normalen E-Mails, Spam und automatisch durch Viren generierten E-Mails zu unterscheiden.

1Missbrauch deshalb, weil die Anfrage gerade nicht den Zweck hat, ein Datenpaket zu adressieren. Allerdings haben die DNS-Listen auch nicht das Ziel, eine derartige Adressierung zu ermöglichen.

2Kriterien sind u.a. korrekte DNS-Einträge, benutzte Schriftgröße etc. Die Mails erhalten daraufhin Punkte, die für die Wahrscheinlichkeit des Vorliegens von Spam stehen. Häufig wird innerhalb einer bestimmten Punktegrenze die Punktewertung des Spamfilters in den Header der E-Mail eingefügt, so dass der Mailclient über die weitere Einstufung entscheiden kann.

3Heidrich, MMR 2004, S.75ff.

(1.) Strafbarkeit nach § 206 StGB

Eine Strafbarkeit nach § 206 StGB setzt das geschäftsmäßige Erbringen von Telekommunikationsdienstleistungen voraus. Dieser Begriff ist in § 3 Nr. 5 TKG legal als das „Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen [...]“ definiert. Für eine abweichende Definition im Bereich des Strafrechts gibt es weder Anzeichen noch einen Bedarf. Im Bereich des Internets erbringen allerdings nur Access-Provider – und diese auch nur teilweise – Telekommunikationsdienstleistungen. E-Mail-Anbieter bieten keine Übertragungswege für Dritte nach § 3 Nr. 5 TKG an, sondern nutzen lediglich die Übertragungswege Dritter, um Übertragungsserver, Software und Speicherplatz zur Verfügung zu stellen. Dass darin nach Meinung des Gesetzgebers keine Telekommunikation zu sehen ist, ergibt sich aus § 1 I TMG, der eine Geltung des TMG für Dienste „die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen [und] telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes“ ausschließt. Bei der Zurverfügungstellung von E-Mail-Diensten handelt es sich aber laut dem nicht in das TMG übernommenen § 2 II Nr.2, 3 TDG um Telemedien[1]. Diese Definition dürfte nach wie vor für die Definition von Telediensten als Telemedien anwendbar sein. Lediglich bei der individuellen E-Mail zwischen zwei Nutzern ist nicht von einem Teledienst, sondern von einem Mediendienst zu sprechen[2]; um diese geht es aber bei der Frage nach Strafbarkeit von E-Mail-Anbietern für das Löschen und Verändern von Nachrichten nicht. Eine Strafbarkeit nach § 206 StGB scheidet für E-Mail-Anbieter rein tatbestandlich mangels des Status eines Telekommunikationsdienstes aus[3].

(2.) Strafbarkeit nach § 303a StGB

Eine Strafbarkeit könnte auch nach § 303a StGB vorliegen, der das Verändern, Löschen oder Unterdrücken von Daten auch ohne Vorliegen eines Telekommunikationsdienstes verbietet. Unter den Datenbegriff des StGB fallen elektronisch oder magnetisch gespeicherte Daten, soweit sie nicht unmittelbar wahrnehmbar sind[4]. Dies ist bei E-Mails der Fall, da sie, bevor sie gelöscht werden können, zumindest im Arbeitsspeicher eines Servers gespeichert werden. Allerdings kommt eine Tatbestandsmäßigkeit nicht für den Einsatz von Blackhole-Lists in Frage, da bei diesen der empfangende Server bereits die Annahme der Datenpakete verweigert und diese somit gar nicht erst auf den Server des E-Mail-Anbieters gelangen; sie werden nicht gespeichert und können somit

1Engel-Flechsig/Maennel/Tettenborn-Tettenborn, § 2 TDG Rn. 67. A.A. ohne nähere Begründung: Heidrich/Tschoepe MMR 2004, 75, 76.

2Engel-Flechsig/Maennel/Tettenborn-Tettenborn, § 2 TDG Rn. 67.

3A.A. Heidrich, MMR 2004, 75, 79, der aber eine Rechtfertigung aufgrund von § 87 TKG zulässt.

4Heidrich/Tschoepe MMR 2004, 75, 79; Schönke/Schröder-Stree, § 303a, Rn 2.

weder gelöscht noch unterdrückt werden, da derlei Vorgehensweisen eine Existenz der Daten auf dem Server voraussetzen.

Insoweit sind durch das Filtern der E-Mails auf dem Server die tatbestandlichen Voraussetzungen des § 303a StGB gegeben: Sowohl das Löschen der Mails als auch die Kennzeichnung nach dem Punktesystem erfüllen die Tatbestandsmerkmale des Löschens und Unterdrückens bzw. Veränderns. Allerdings kann ein tatbestandsausschließendes Einverständnis vorliegen. Dieses darf in der Regel bei automatisch generierten Virenmails vermutet werden, da kaum ein Nutzer solche empfangen will[1]. Dies gilt in allen Fällen für die Kennzeichnung von Mails nach Spam-Punkten, der Grundlage für E-Mail-Filter auf den Rechnern der Anwender, jedoch nicht uneingeschränkt für die Aussortierung von wegen Virenbefalls des sendenden Computers virenverseuchten E-Mails, da ihr Inhalt weiterhin erkennbar ist und bei Einsatz eines Virenscanners auch von den Viren befreit werden kann. Eine Rechtfertigung kommt vor allem durch § 34 StGB in Frage, wobei zwischen dem beeinträchtigten Interesse und den drohenden Gefahren abzuwägen ist. Das Interesse am Erhalt aller Mails dürfte gegenüber dem Wunsch nach einem Spam-freien Mailaccount überwiegen[2]. Allerdings wird man hinsichtlich des reibungslosen Funktionieren des Mail-Services, ähnlich wie im Fall der Domainregistrierung, ein großes öffentliches Interesse annehmen dürfen, insbesondere angesichts der zunehmenden Nutzung dieses Mediums durch die öffentliche Verwaltung.

Angesichts der Bedrohung durch Spam, der den Mail-Service unbenutzbar zu machen droht, ist auch das öffentliche Interesse zu berücksichtigen, zumal dieses gleichsam dem eines Mailaccount-Besitzers entspricht. Es ist außerdem zu beachten, dass eine Kennzeichnung nach „Spam-Punkten“ häufig erst die Grundlage für eine Filterung auf dem individuellen Rechner schafft: Demnach wäre eine Spam-Filterung und Kennzeichnung auf dem Mailserver zwar tatbestandsmäßig nach § 303a StGB, aber nicht rechtswidrig[3].

3. Selbstregulierungsmaßnahmen und rechtliche Bewertung

Ob die Lösung des Problems „Spam“ ausschließlich durch technische Mittel erfolgen wird oder ob diese lediglich die Grundlage erfolgreicher Rechtsdurchsetzung bilden werden, ist nicht prognostizierbar. In jedem Fall kann das Problem nur unter Zuhilfenahme technischer Methoden behoben werden. Eine technische Verhinderung der Fälschung von E-Mails würde Spam wahrscheinlich fast völlig versiegen lassen. Technische Ansätze erfordern aber zunächst eine Veränderung oder Ergänzung des E-Mail-Protokolls, da dieses nach dem jetzigen Stand keinerlei

1Manche Nutzer „sammeln“ Viren und haben daher ein Interesse an solchen Mails; sie stellen allerdings die Ausnahme dar.

2Heidrich/Tschoepe MMR 2004, 75, 79.

3A.A. Heidrich/Tschoepe MMR 2004, 75, 79.

Sicherheitsmaßnahmen bietet[1]. Diskutiert werden derzeit mehrere Lösungsansätze, die teilweise von Unternehmen und teilweise von der IETF stammen[2].

a. MARID

Die MARID-Working Group[3] (M(ail Transfer Agent) Authorization Records In DNS) der IETF sucht nach Verfahren, bei denen das Mailauslieferungs-Programm[4] auf der Empfängerseite überprüft, ob die Mail von einem Server stammt, der für die angegebene Domain registriert ist[5]. Hierfür muss die IP-Nummer des Sender-Servers mit den für diese Domain für Server registrierten IP-Nummern verglichen werden. Ist der Sender-Server nicht registriert, können die E-Mails abgewiesen werden. Durch diese Verfahren sind allerdings nicht nur Spam-Mail-Versender betroffen, sondern möglicherweise auch falsch konfigurierte Mailserver von Unternehmen, so dass Mails zu Unrecht abgewiesen werden könnten. Derartige Überprüfungen werden momentan bereits von Mailservern vorgenommen, ohne jedoch standardisiert zu sein. Die rechtliche Bewertung ist identisch mit der für die Strafbarkeit nach § 303a StGB[6].

Allerdings hat sich die MARID-Working Group wegen unüberbrückbarer Differenzen hinsichtlich der Lizenzbedingungen eines Microsoft-Vorschlages, welcher Teil der Technologie werden sollte, aufgelöst, so dass dieses Verfahren keine Aussicht mehr auf eine Standardisierung hat.

b. MASS

In der IETF gibt es außerdem eine Working Group[7], die sich mit Message Authentication Signature Standards (MASS) beschäftigt, welche bestätigen sollen, dass eine E-Mail tatsächlich von dem vorgeblichen Absender kommt. Dadurch werden vor allem sich automatisch versendenden Viren die Verbreitungsmöglichkeiten genommen, da diese in der Regel den Absender fälschen. Anders als MARID, geht MASS nicht von einer Überprüfung der Server, sondern von einer Kennzeichnung der Mails aus. Somit stehen die beiden Ansätze nicht in Konkurrenz zueinander und sind theoretisch gemeinsam anwendbar.

c. Sender-ID

Durch dieses von Microsoft initiierte Verfahren sollen für jede Domain im DNS die für den Mailversand zugelassenen Server registriert werden. Da in jedem Mail-Header angegeben ist, von welchem Server die E-Mail versendet wurde, kann der Empfänger per Anfrage an den für die Do-

---

1Kelm, DuD 1999, 25, 29.

2S.u. S.172.

3http://www.ietf.org/html.charters/marid-charter.html.

4Der so genannte Mail-Transfer-Agent (MTA).

5Im DNS muss eine Domain und deren Server einer IP-Adresse zugeordnet sein. Ist die IP-Adresse nicht der Domain zugeordnet, handelt es sich möglicherweise um eine Fälschung.

6S.o. S.132.

7http://www.ietf.org/ietf/04aug/mass.txt.

main zuständigen DNS-Server prüfen, ob der Sender-Server als für Mailversand zugelassen registriert ist – wenn dies nicht der Fall ist, liegt ein starkes Indiz für Spam vor. Dieses Verfahren benötigt keine Veränderungen im für den Mailversand zuständigen SMTP-Protokoll, erfordert allerdings eine Erweiterung der DNS-Tabellen und wirkt nur gegen Spam mit gefälschten Absenderadressen, der über offene Mailserver verschickt wird. Obwohl die Maßnahme der Sender-ID einigen anderen recht ähnlich ist, steht sie nicht auf der offiziellen Liste der IETF[1].

d. DomainKeys

Das DomainKeys-Verfahren wurde von Yahoo! Inc. entwickelt und bei der IETF als Draft zur Standardisierung eingereicht[2]. Bei diesem auf Kryptographie basierenden Ansatz entwickelt ein Domaininhaber ein Schlüsselpaar aus seiner Domain, wobei der öffentliche Teil des Paares in einer erweiterten DNS-Tabelle abgelegt wird. Jede von einem von der Domain autorisierten Server gesendete Mail enthält im Header eine Signatur, die aus dem Mail-Inhalt und dem privaten Schlüssel erzeugt wird und anhand derer der Empfänger überprüfen kann, ob die E-Mail tatsächlich von dem behaupteten Versender stammt und ob sie verändert worden ist. Durch dieses Verfahren wird sowohl eine gewisse – wenn auch sehr geringe – Sicherheit gegen unbefugtes Mitlesen von E-Mails geschaffen als auch deren Veränderung verhindert. Rechtlich könnte vor allem das Anhängen der Schlüssel an die Mail wegen § 303a StGB problematisch sein. Allerdings wird man wohl eine Einwilligung vermuten können, welche die Provider allerdings in ihren AGB auch explizit einholen sollten. Nach dieser Variante können noch andere, herkömmliche Tests durchgeführt werden, wobei damit zu rechnen ist, dass sich die Spam-Problematik mit der Möglichkeit, die bisher versteckte Identität des Versenders zu ermitteln, erledigen wird.

e. Micropayment

Ein anderer Ansatz plädiert dafür, dass pro abgesandter Mail ein winziger Geldbetrag an den Provider zu zahlen sei: Dadurch würde sich die Nutzung von E-Mail für Endnutzer kaum verteuern, das Verschicken von Spam-Mails für professionelle Versender aber unbezahlbar werden[3]. Dieser Vorschlag setzt allerdings ein funktionierendes, sicheres Micropayment-System voraus, das derzeit nicht existiert.

1http://www.heise.de/newsticker/meldung/44974.

2http://antispam.yahoo.com/domainkeys.

3Die Zahlen schwanken, aber es soll Versender von Spam geben, die mehrere Millionen oder gar Milliarden Mails pro Tag verschicken.

4. Bewertung

Die größte Gefahr beim Einsatz technischer Mittel besteht in der Möglichkeit, dass E-Mails fälschlicherweise als Spam gekennzeichnet und deshalb nicht ausgeliefert werden. Dieses Risiko verringert sich allerdings mit der Weiterentwicklung der Filtermethoden. Eine andere Gefahr liegt in einer falschen Konfiguration der sendenden Mailserver, so dass diese entweder in Blackhole-Listen eingetragen oder von ihnen versandte Mail wegen falscher DNS-Registrierung abgewiesen werden. Allerdings wird eine völlige Sicherheit von E-Mails, ebenso wenig wie die absolute Gewährleistung, dass E-Mails wirklich ihren Empfänger erreichen, wohl nie gegeben sein können.

V. Inhaltliche Selbstregulierung (oder Selbstjustiz)

Neben den Maßnahmen gegen Spam, die sich in der Regel gegen das Phänomen „Spam" als solches und auch dessen Urheber richten, gibt es private Maßnahmen zur Ahndung von Verstößen, sei es gegen Codes of Conduct (Verhaltensrichtlinien), die Netiquette, andere ungeschriebene Verhaltensregeln oder Gesetze, die sich gemeinhin gegen konkrete Inhalte oder Verhaltensweisen Einzelner richten. Diese sind in der Regel nahezu so alt wie das Internet selbst – die früheren Trägerorganisationen haben keine Verhaltensregeln festgeschrieben[1] – und in jedem Fall älter als jedes staatliche Vorgehen gegen Verstöße, gleich welcher Art. Diejenigen, die gegen derlei Übertretungen vorgehen, sind entweder – zumeist selbst ernannte – Einzelne oder Gruppen oder Verwalter von Servern oder Moderatoren von Foren und Newsgroups. Alle Maßnahmen greifen – mit unterschiedlicher Intensität und vielgestaltigen Ergebnissen – in den Rechtskreis der „Sünder" ein; sonst wären sie als Sanktionen wirkungslos. Von Belang ist zunächst die Rechtsverbindlichkeit der Regeln, bevor die Rechtfertigung von Sanktionsmaßnahmen zu untersuchen ist. Die üblicherweise verhängten Sanktionen bewegen sich innerhalb eines Spektrums von einfachen Zurechtweisungen – bei leichten, erstmaligen Verstößen – bis hin zum Ausschluss aus bestimmten Gruppen.

1. Rechtswirksamkeit der Netiquette

Die Netiquette ist ein früh entstandenes Regelwerk für korrektes Verhalten im Internet, insbesondere in Newsgroups und Foren[2], und hat sich mit der Zeit verändert: Es haben sich nicht nur verschiedene Versionen, sondern auch verschiedene Ansätze mit teilweise sehr unterschiedlichen Inhalten entwickelt[3]. Die Netiquette enthält keine Aussagen über Sanktionen, die bei Verstößen drohen, was Anbieter allerdings nicht daran hindert, diese Regeln zum Bestandteil ihrer

1Holznagel, Regulierte Selbstregulierung, S.88.

2http://www.ping.at/guides/netmayer/.

3Beispiel einer deutschen Variante: http://www.ping.at/guides/netmayer/; aber auch RfC 1855, http://www.rfc-editor.org/rfc/rfc1855.txt.

Nutzungsbedingungen zu machen[1]. Soweit Sanktionen für Verstöße gegen die Netiquette von Administratoren verhängt werden, richten sie sich in aller Regel nach der Schwere der Zuwiderhandlungen. In Foren und Newsgroups, die mehrheitlich nicht-kommerzieller Natur sind, spricht daher nichts gegen eine Wirksamkeit der Netiquette, zumal in der Regel schwerere Verstöße auch Gesetze verletzen und leichtere keine rechtlich relevanten Strafmaßnahmen auslösen. Sollten rechtlich relevante Strafmaßnahmen verhängt werden, könnte sich eine Rechtfertigung der Sanktionen ergeben.

2. Rechtmäßigkeit der Sanktionen

Die Sanktionskultur des Internets entspringt den Ursprüngen des Netzes, das rein wissenschaftlich orientiert war[2] und in dem allen Beteiligten bewusst war, dass sie Verantwortung für seine Nutzbarkeit trugen. Diese Ausgangslage spiegelt sich auch in den – heutzutage technisch überholten – Netiquette-Regeln[3] wider, die sich an Neulinge richteten, welche an einer verantwortungsvollen Nutzung und Mitarbeit interessiert waren. Des Weiteren war das Netz noch nicht so anonym wie heute[4]; Verstöße und Sanktionen waren für den Einzelnen spürbarer. Die Wirksamkeit von Sanktionen in Foren war – trotz Anonymität – relativ hoch, da die Akzeptanz der Nutzer von ihren Pseudonymen abhing: Ging ein Pseudonym wegen fortdauernder Verstöße verloren, war auch die damit verbundene fachliche Reputation verschwunden und eine Berufung auf das vorige Pseudonym nicht möglich.

Es wurde allerdings auch schon von anderen Sanktionsmechanismen wie der Anforderung von postalischer Werbung jeglicher bestellbaren Art an die Adresse identifizierter Spammer berichtet. Fragen nach der Rechtmäßigkeit derartiger Maßnahmen stellen sich in der Praxis nicht, da sich zum Einen die Sanktionierten nicht ohne Aufgabe der von ihnen angestrebten Anonymität wehren können und es zum Anderen die Sanktionierenden sehr gut verstehen, ihre eigene Anonymität zu wahren.

Maßnahmen von Administratoren wegen Zuwiderhandlungen gegen die als Nutzungsbedingungen festgeschriebene Netiquette sind rechtlich unproblematisch. Sanktionen jenseits von Ermahnungen und Nutzungsausschluss sind wohl nicht mehr von den Nutzungsbedingungen abgedeckt und daher genauso zu beurteilen wie von Dritten ausgehende Sanktionen.

1Beispielsweise das Servicezentrum für das Recht der Informations- und Kommunikationstechnologie der Juristischen Fakultät der HU Berlin; die Community von Radio Regenbogen, http://ww.regenbogenweb.de/community/club/netiquette.html.

2Holznagel, Selbstregulierung, S. 91.

3Besonders deutlich: http://www.ping.at/guides/netmayer/.

4Jedenfalls konnte das Pseudonym nicht einfach gewechselt werden. Welche reale Person sich hinter einem Pseudonym verbarg, war dagegen häufig unmöglich herauszufinden. Daher hatte das Vertrauen in Pseudonyme eine größere Bedeutung, ebenso wie die Pseudonyme eine größere Bedeutung für die realen Personen hatten, da ihr Geltungsanspruch in der für sie relevanten Gruppe von ihrem Pseudonym abhing.

Sanktionen können nur rechtswidrig sein, wenn die Handlung zu einer Rechtsverletzung beim Sanktionierten führt, was bei einfachen Ermahnungen nicht der Fall ist. Mailbomben[1], Beleidigungen und öffentliches Bloßstellen dürften indes die Rechte des Betroffenen verletzen. Unklar bleibt, ob derartiges Verhalten gerechtfertigt sein könnte, wobei straf- und zivilrechtliche Rechtfertigungsgründe nicht unbedingt in Frage kommen, da keine der Methoden sicherstellen kann, dass sie das rechtswidrige Verhalten beendet[2]. Es bleiben einzig eine mögliche Einwilligung des Störers oder sozial übliches Verhalten als Rechtfertigungsgrund.

a. Einwilligung

Der Ansatzpunkt für eine vorherige Einwilligung des Störers könnte darin bestehen, dass ihm, wie jedem anderen, der sich in Foren oder Newsgroups beteiligt, die Netiquette bekannt ist – spätestens bei Verstößen wird er auf sie aufmerksam gemacht – und er dennoch gegen sie verstößt. Ebenso wie die Netiquette dürften die üblichen Sanktionen bekannt sein, so dass eine Einwilligung zumindest denkbar wäre, vor allem angesichts der Tatsache, dass solche Sanktionsmaßnahmen in einem weitgehend anonymen Medium wie dem Internet die einzig mögliche Art der Bestrafung darstellen. Man wird allerdings (wie im Strafrecht) kaum annehmen können, dass derjenige, der gegen die Netiquette verstößt, seine eigene Bestrafung wünscht. Daher ist eine vorherige Einwilligung auszuschließen.

b. Soziale Üblichkeit

Die Rechtfertigung durch soziale Üblichkeit stellt darauf ab, dass ein Verhalten, das in der Gesellschaft für rechtmäßig gehalten wird, nicht strafbar sein kann. In Newsgroups und Foren sind Sanktionen schon seit der „Kindheit“ des Internets in Gebrauch[3] und werden bis heute im Wesentlichen unverändert genutzt. Man kann also zumindest von einer sektorspezifischen Üblichkeit ausgehen, allerdings nur insofern, als die Kenntnisnahme einer bestimmten Version der Netiquette Bedingung für die Nutzung eines Angebotes ist.

3. Wirksamkeit der Selbstregulierung

Die beschriebenen Mechanismen mögen in der Frühzeit des Internets, als Mailboxen mit 1 GB Speicherplatz und mehr undenkbar und verschiedene Identitäten in Foren nicht üblich waren, wirksame Instrumente gesellschaftlicher Kontrolle gewesen sein. Dies dürfte auch heute noch für Expertenforen gelten. Allgemein kann man aber feststellen, dass für den Umgang unter Menschen im Internet dasselbe gilt wie in der realen Welt: Je mehr Menschen aufeinander treffen und je anonymer diese Zusammenkünfte werden, desto mehr nimmt die Wirksamkeit gesellschaftlicher Selbstkontrolle ab. Dementsprechend werden auch die beschriebenen Mechanismen als wirkungslos

1E-Mails, die so groß sind, dass sie das Postfach des Empfängers füllen.

2Die beschriebenen Maßnahmen sind reaktiv und können allenfalls dazu beitragen, dass in Zukunft keine Verstöße mehr geschehen.

3Wobei die Notwendigkeit in den ersten Jahren nicht bestand.

betrachtet. Die Netiquette hat als „Gebrauchsanweisung des Cyberspace“ einen wichtigen Platz, ist aber nicht als dessen Strafgesetzbuch geeignet und war dazu auch nicht bestimmt.

Eine besondere Stellung nehmen Codes of Conduct ein, da diese zum einen für die unterzeichnenden Anbieter verpflichtend sind und zum anderen in der Regel Strafbestimmungen enthalten. Problematisch sind allerdings international gültige Codes of Conduct, da international agierende Provider in den verschiedenen Ländern unterschiedlichen rechtlichen Regelungen unterliegen[1]. Wie Sieber anmerkt, könnten Codes of Conduct, die eine Lösung für das Problem der grenzüberschreitenden Regelung finden, die Grundlagen für international einheitliche staatliche Regelungen schaffen. Allerdings besteht auch die Gefahr, dass Eingriffe aufgrund privater Regelungen intensiver werden, als es staatliche Regelungen könnten. Des Weiteren scheint zumindest Deutschland nach Inkrafttreten des JMStV kein Vertrauen in derartige Codes of Conduct[2] zu setzen, da deren Einhaltung der Überwachung durch staatliche Stellen unterliegt.

VI. Staat und Internet

Die im Bereich der Regulierung und Selbstregulierung auftretenden Probleme, die das staatliche Vorgehen an den Rand der Verfassungswidrigkeit und darüber hinaus bringen, lassen die Frage nach dem Verhältnis des Staates zu neuen Techniken aufkommen.

Traditionell gilt die Bewältigung neuer Techniken als Staatsaufgabe[3]. Diese ergibt sich aus den Risiken, die den neuen Techniken innewohnen und Gefahren für die Grundrechte verursachen können, für die der Staat Schutzpflichten trägt[4]. Ob es sich beim Internet um eine neue technische Entwicklung handelt – das Internet ist ein Übertragungsmedium für Kommunikation und die möglichen Gefahren gehen nicht von ihm selbst, sondern von den übertragenen Kommunikationsinhalten aus –, und worin die neuen Gefahren durch das Internet liegen sollen, ist unklar. In jedem Fall folgt aus den vorgehenden Überlegungen, dass es sich bei der Gesetzgebung um Gefahrprävention und somit zwingend um eine Staatsaufgabe handelt. Denkbar wäre auch ein Grundrecht auf Zugang zu derartigen Kommunikationsnetzen, dessen Gewährleistung ebenfalls eine Aufgabe des Staates wäre.

1Sieber, Verantwortlichkeit, Rn. 551.

2Wenn man die Richtlinien der Selbstkontrolleinrichtungen als Codes of Conduct betrachtet.

3Ipsen, VVDStRL 48 (1990), 177, 179; Kirchhof, NvwZ 1988, 97, 97.

4Statt Vieler: Ipsen, VVDStRL 48 (1990), 177, 179 m.w.N.

Gefahren „des Internets“

Es ist unbestritten, dass über das Internet Kommunikationsinhalte abrufbar sind, die gegen geltendes deutsches Recht verstoßen, was eine Gefahr darstellt. Diese allerdings entspringt nicht dem Internet selbst, sondern wird durch die Kommunikationsinhalte hervorgerufen. Das Internet ermöglicht keine neuen Arten von Kommunikationsinhalten[1]. Auch können Kommunikationsnetze weder explodieren, mutieren noch die Umwelt verschmutzen[2]. Die von ihnen ausgehenden spezifischen Bedrohungen müssen also anderer Natur sein als die oben beschriebenen und die herkömmlichen, für die Begründung einer Staatsaufgabe im Technikrecht herangezogenen Gefahren.

Die durch eine zunehmende Abhängigkeit von derartigen Kommunikationsnetzen hervorgerufenen Risiken[3] werden gesetzlich nicht mehr beeinflusst, da sich die mit der Nutzung verbundenen Befürchtungen nicht verwirklicht haben[4]. Einzig der Datenschutz[5] verbleibt als staatlich wahrgenommene Aufgabe: Hier wurde auch mit dem in dem TMG aufgegangenen TDDSG eine bereichsspezifische Regelung geschaffen, da aufgrund bislang unbekannter und ohne Zuhilfenahme der Strukturen des Netzes nicht durchführbarer Möglichkeiten der Datensammlung erhebliche Gefahren für den einzelnen Nutzer bestehen. Durch Datenschutzvorschriften wird zwar das Verhalten von Anbietern in herkömmlicher Weise gesteuert, jedoch nicht die zugrunde liegende Technik, welche sich einer staatlichen Steuerung auch weitestgehend entziehen dürfte. Eine Ausnahme besteht in der Regelung des § 4 VI TDDSG, der eine Gestaltung der Angebote vorsieht, dass nur so wenige Daten wie nötig erhoben werden dürfen. Dieser gilt aber nur für Anbieter in Deutschland. Gerade wegen der Internationalität und der schwer beeinflussbaren Technik leidet der Datenschutz im Internet noch an erheblichen Mängeln; die Daten können schließlich genauso von Anbietern in anderen Staaten gesammelt werden.

Ein weiteres Problem des Datenschutzes, das vom Internet unabhängig, jedoch nicht durch Rechtsetzung zu lösen ist, besteht im mangelnden Bewusstsein der Relevanz des Datenschutzes seitens weiter Teile der Bevölkerung. Abhilfe könnten lediglich absolute Datenerhebungsverbote leisten, die allerdings stark in die Freiheiten der Anbieter eingreifen und teilweise auch den e-Commerce, der durch das IuKDG gefördert werden sollte, unmöglich machen würden. Auch Datenerhebungen durch Anbieter im Ausland entzögen sich einer derartigen Regulierung.

1Rechtsradikale Propaganda, Kinderpornographie und jugendgefährdende Inhalte existierten schon vor dem großen Popularitätsschub des Internets und können mit gleichen Inhalten auch ohne Zuhilfenahme des Internets verbreitet werden.

2Schlink, VVDStRL 48 (1990), 235, 238.

3Schlink, VVDStRL 48 (1990), 235, 243.

4Das Internet gilt als weitestgehend ausfallsicher, die zitierten Beispiele der Genehmigungspflicht für die Herstellung von Telekommunikationsanlagen wurde aufgehoben.

5Schlink, VVDStRL48 (1990), 235, 245.

Schließlich ist die Erhebung bestimmter Daten für die Nutzung von Angeboten auch technisch notwendig.

2. „Bewältigung" der Staatsaufgabe

Das traditionelle Mittel der Wahrnehmung von Staatsaufgaben ist Rechtsetzung[1]. Dieses hat der Staat durch die Verabschiedung des TDDSG und die Anpassung bestehender Vorschriften genutzt. Im Bereich der Inhalte, insbesondere im Jugendschutz, wurde mit dem JMStV und dem JuSchG außerdem versucht, netzspezifische Gefahren zu reduzieren. Hierbei handelt es sich genau genommen zwar um eine Staatsaufgabe, jedoch ist diese nicht durch das Auftauchen neuer Technik entstanden.

Zu beklagen sind erhebliche Vollzugsmängel, die sowohl im Datenschutzrecht als auch im Jugendschutzrecht vorhanden waren und sind. Ob sich die Bewahrung der Jugend vor gefährlichen Kommunikationsinhalten oder der Schutz persönlicher Daten durch die gesetzgeberischen Eingriffe wesentlich gebessert hat, darf bezweifelt werden. Wenn allerdings sogar verfassungswidrige Gesetze und weitreichende Eingriffe keinen Erfolg zeitigen, stellt sich die Frage, ob und auf welche Weise dieser herbeigeführt werden kann.

3. Alternativen

Im Bereich des Informationsrechts zeigt sich, dass staatliches Handeln, das direkt auf Kommunikationsinhalte zielt, selten das gewünschte Ziel erreicht. Inhalte können dem Zugriff des Staates entzogen werden, ohne dass sie ihre Verfügbarkeit einbüßen. Dem hat der Gesetzgeber durch die Vorschrift des § 59 IV RStV Rechnung getragen. Sperrungsmaßnahmen durch Provider werden allerdings aufgrund der Belastung Dritter und der damit verbundenen finanziellen Belastung des Staates deutlich weniger effektiv sein, als es direkte Eingriffe sein könnten und sind außerdem relativ leicht zu umgehen. Es liegt hier, ebenso wie bei Teilen des neuen JuSchG und insbesondere des JMStV, anscheinend ein eher symbolisches Handeln vor. Hierfür spricht auch die zeitliche Nähe[2] ihrer Entstehung zum „Erfurter Massaker", auf das in den Beratungen zum JuSchG Bezug genommen wurde[3]. Diese Art der Gesetzgebung hat allerdings bedenklich weitgehende Eingriffe in die Kommunikationsgrundrechte zur Folge.

1Murswiek, VVDStRL 48 (1990), 207, 208.

2Der erste Entwurf des JuSchG wurde am 15.5.2002, etwa einen Monat nach dem „Erfurter Massaker", in den Bundestag eingebracht; der JMStV wurde zur gleichen Zeit bearbeitet.

3Stellungnahme MdB Dörflinger, BT PlProt 14/24527.

Zwischen Internetrecht und herkömmlichen Technikrecht[1] gibt es einen erheblichen Unterschied: Im Technikrecht handelt es sich in der Regel um neu zu errichtende Anlagen, die sich vollständig im Regelungsbereich des nationalen Gesetzgebers befinden. Entspricht eine Anlage nicht den nationalen Vorschriften, kann sie diesen angepasst werden. Lehnt der Betreiber Änderungen ab, kann er die Anlage nicht betreiben oder muss auf eine Änderung der Vorschriften hinwirken. Dies gilt ebenso und besonders für die technische Gestaltung, auch für Telekommunikationsnetze, die, um international verbunden werden zu können, bestimmte Grundanforderungen erfüllen müssen. Das Internet hingegen ist ein schon seiner Konzeption nach internationales Kommunikationsnetz, dessen Entwicklung weitestgehend staatsfern abgelaufen ist. Neben staatlichen Gesetzen existiert eine weitere, mächtige Regelungsebene, nämlich die Architektur[2] des Netzes. Diese ist von Menschen erschaffen worden und somit nicht unabänderlich. Nichtsdestotrotz ist sie bei der Ausübung staatlicher Befugnisse zu beachten. Der einzelne Staat kann keine Änderung erzwingen. Dies gilt ebenso für andere Bereiche: Kein Staat kann bestimmen, wie ein Kernreaktor arbeitet[3], aber er kann festlegen, welche Vorkehrungen bei dem Betrieb zu treffen sind beziehungsweise ob überhaupt Kernreaktoren gebaut werden dürfen. Für das Internet gilt Anderes: Staaten können weder auf die Datenübertragung noch – aufgrund der Internationalität – auf die genauen Modalitäten Einfluss nehmen. Ebenso wenig wie ein Staat oder irgendjemand sonst erkennen kann, ob gerade „Atomstrom“ importiert wird oder nicht, kann er feststellen, ob rechtswidrige Inhalte über seine Grenze kommen. Die Modalitäten werden von der Architektur vorgegeben, und diese liegt nicht im Wirkungsbereich eines Einzelstaates[4]. Eine Änderung wäre nur einheitlich für das gesamte Internet möglich[5]. Für staatliche Einflussmöglichkeiten ergibt dies, dass ein Schutz gegen architekturbedingte Gefahren nicht durch ein Vorgehen gegen die konkreten Gefährdungen[6] möglich ist, sondern – wenn die Inhalte nicht erreichbar sind – letztlich nur durch eine Änderung der Architektur des Internets. Diese können Staaten jedoch nicht durch Gesetzgebung herbeiführen. Insofern ist der Ruf nach dem Gesetzgeber weder erfolgversprechend noch angemessen.

Die Architektur des Internets[7] wird wesentlich durch private Expertengruppen bestimmt, die sich bei ihren Entscheidungen über die Verabschiedung von Standards in erster Linie an deren Zweck-

1Gemeint sind Regelungen des BImschG, GenTG, TKG etc.

2Von Lessig „Code“ genannt.

3Übertragen wäre dies die Architektur des Systems „Kernreaktor“.

4Einzelstaaten können für die unter ihrer Hoheit stehenden Personen und Anlagen eine Abweichung von der Architektur erzwingen, diese kann aber zur Folge haben, dass bei inkompatiblen Strukturen der betreffende Staat vom gesamten Internet „abgekoppelt“ und ein rein nationales Netz entstehen würde, dessen Durchsetzungskraft gering einzustufen ist.

5Staaten können auch versuchen, für ihr Hoheitsgebiet neue, mit anderen kompatible, Architekturen durchzusetzen. Das Eindringen unerwünschter Inhalte von „außen“ wäre allerdings nach wie vor möglich und so durch den Architekturwandel letztendlich nichts gewonnen.

6Wie oben, S.140, erläutert, gehen die Gefahren von den Kommunikationsinhalten und nicht vom Internet aus.

7Dazu unter D, S.149ff.

mäßigkeit orientieren. Innerhalb dieser Gruppen existieren, wie auch bei ICANN und IAB, Gremien, die speziell für die Abstimmung zwischen ((den)) technischen Lenkungsgremien und Vertretern von Regierungen konzipiert sind. Diese Gruppen üben indes keine direkte Wirkung hinsichtlich der Verwirklichung der Standards aus; diese müssen von den Verwaltern der Server und – je nach Art der Standards – von den Softwareherstellern und Nutzern akzeptiert und umgesetzt werden. Die Umsetzung kann nicht gesetzlich erzwungen werden. Eine Einflussnahme über diese Gremien dürfte nur nach internationaler Abstimmung möglich sein und auch nur dann, wenn viele Staaten eine koordinierte Position finden können. Die wahrscheinlich einzige erfolgreiche Handlungsform besteht in einem international abgestimmten, informellen staatlichen Handeln; auch informelle Kooperationen mit Host-Providern in anderen Staaten bieten Chancen für die Bekämpfung von durch Kommunikationsinhalte hervorgerufenen Gefahren[1].

Ein solches Vorgehen birgt allerdings andere und ebenso beachtenswerte Risiken: Zum einen können sich Allianzen bilden, deren kleinster gemeinsamer Nenner die Kontrolle der Kommunikation ist[2], zum anderen werden die für die Umsetzung von Kontrollmaßnahmen notwendigen Umgestaltungen von Privaten vorgenommen, so dass – auch bei einer ursprünglichen Anregung von Seiten des Staates – keine demokratische Kontrolle gegeben ist und somit eine Gefährdung der Kommunikationsgrundrechte nicht ausgeschlossen werden kann[3].

Eine kurzfristig realisierbare Alternative im Bereich des Jugendschutzrechts stellt die Schulung und Aufklärung von Erziehungsberechtigten, die Bereitstellung von Informationsmaterialien sowie die sachliche Darstellung von Gefahren und Möglichkeiten, diesen zu entgehen, dar. Ein Teil dieser Aufgabe besteht auch in der Erziehung zur Medienkompetenz, die aber nicht nur auf die Präsentation von Gefährdungen reduziert sein darf. Die Aufklärung darf sich außerdem nicht auf die Erziehungsberechtigten beschränken, sondern muss auch die Jugendlichen erfassen; Verbote können nur flankierend wirken.

4. Und die demokratische Kontrolle?

Problematisch an der vorgeschlagenen Lösung ist die demokratische Kontrolle des Verfahrens. Den demokratisch gewählten Regierungen fehlt es nicht an Legitimation, jedoch setzen sich die Standardisierungsgremien ausschließlich aus freiwillig mitarbeitenden Experten zusammen, die keiner, gleich wie gearteten, demokratischen Kontrolle unterliegen. Verschärft wird die Problematik durch

1Jugendschutz.net hat durch Kooperation mit amerikanischen Anbietern erreicht, dass nach deutschem Recht rechtswidrige Inhalte von den amerikanischen Servern entfernt wurden. Durch Methoden der Eingriffsverwaltung hätte dieses Ergebnis höchstwahrscheinlich nicht erreicht werden können.

2China, Vietnam und Singapur und andere Staaten mit einem zumindest fragwürdigen Demokratieverständnis würden eine derartige Veränderung der Architektur mit Sicherheit unterstützen. Lessig skizziert eine Möglichkeit, Staaten zu erlauben, auszuwählen, was ihre Bürger wahrnehmen dürfen; dazu müssen Inhalte allerdings mit Labeln versehen werden.

3Trute, VVDStRL 57, 216, 256f; Möller/Amouroux-Einziger, S.143.

die Form des informellen Staatshandelns: Dieses unterliegt zwar auch bei Grundrechtseingriffen einer gerichtlichen Kontrolle, jedoch kommen die Grundrechtseingriffe nicht direkt durch staatliches Handeln, sondern erst mittelbar durch die Umsetzung der Empfehlungen in Standards und deren Umsetzung in funktionierende Technik zustande, wobei letztere rein privat ist und somit kein Rechtsschutz besteht. Die Regulierung geschieht allein durch den Markt. Anders als bei letztlich zur Erfolglosigkeit verdammten Versuchen der Inhaltskontrolle durch Gesetze entstünde hier ein Eingriffsmechanismus, der ungleich effektiver als alles bekannte ist und gleichzeitig keiner irgendwie gearteten Kontrolle unterliegt. Im Endeffekt würde es sich also nicht um die Herstellung von Zuständen, wie sie auch in der „realen Welt" herrschen, sondern um die Schaffung eines nicht überwachten, nicht kontrollierten umfassenden Überwachungs- und Kontrollinstruments handeln.
Zu beachten ist, dass eine solche Umgestaltung nicht nur das Herausfiltern jugendgefährdender Inhalte, sondern gleichsam autoritären Staaten ermöglichen würde, die Kommunikation ihrer Bürger über das Internet, der häufig einzigen unabhängigen Informationsquelle, der quasi-totalen Kontrolle zu unterwerfen.

VII. Regulierung zur Freiheitsgewährleistung?

Die bisherigen Felder der Regulierung wurden als Schranken der Kommunikationsfreiheiten beschrieben. Ebenso wie der Staat aber über die Schrankenregelungen des Art. 5 II GG die Möglichkeit der Einschränkung der Kommunikationsfreiheiten hat, muss er für eine Umgebung sorgen, in der diese effektiv ausgeübt werden können[1]. Dies ergibt sich aus ihrer konstituierenden Rolle für das Funktionieren der Demokratie[2]. Wichtig für die Gewährleistung sind nicht nur Anbieter von Inhalten, sondern auch die für die Kommunikation unersetzlichen Host- und Access-Provider sowie Suchmaschinenbetreiber[3]. Anders als Eingriffe zur Verhinderung von Kommunikation sind Eingriffe zur Herbeiführung erwünschter Kommunikation – beispielsweise zur Qualitätssicherung von Angeboten – nicht von vornherein zum Scheitern aufgrund der technischen Gegebenheiten verurteilt. Auch hier können zwei grundsätzlich verschiedene Ansätze verfolgt werden: Zum einen kann der Staat selbst zum Anbieter von Inhalten werden, zum anderen kann er regulierend auf Private einwirken, durch deren Vorgehen die Kommunikationsfreiheiten in Gefahr zu geraten drohen.
Derartige Regelungen finden sich im Bereich der traditionellen Medien, insbesondere im Rundfunkstaatsvertrag sowie bei der Pressefusionskontrolle. Allerdings ist fraglich, inwieweit

1Hoffmann-Riem, Gesetzliche Gewährleistung, S.59f.

2Hoffmann-Riem, Gesetzliche Gewährleistung, S.59; BVerfGE 7, 198, 208; 20, 162, 174; 62, 230, 247; 71, 206, 220; 76, 196, 208f.

3Hoffmann-Riem, Gesetzliche Gewährleistung, S.65; für Suchmaschinen funktionell ähnliche Navigatoren im digitalen TV: Leopoldt, S.60f.

derartige Regelungen auf den Bereich der über das Internet verbreiteten Medien sinnvoll anwendbar sind.

1. Staatliche Angebote

Staatliche Angebote zur Sicherung der Kommunikationsfreiheiten sollen den Bürger dazu befähigen, sich individuell und kollektiv zu orientieren, an Kommunikationsprozessen teilzunehmen, die eigenen Interessen sowohl im privaten als auch öffentlichen Umfeld zu verfolgen und am politischen Geschehen teilzuhaben[1]. Laut Hoffmann-Riem gilt es nicht nur, für Angebote, sondern auch für deren Aufnahme zu sorgen[2]. Ein Eingreifen des Staates sei allerdings erst dann angezeigt, wenn es zur Erreichung der Ziele erforderlich und geeignet sei[3]. Im Bereich des Internets gewährleistet jedoch der Markt ein ausreichendes, in jede denkbare Richtung diversifiziertes Angebot[4].

Im Bereich des Rundfunks sorgten einerseits die Frenquenzknappheit und andererseits die finanziellen Hürden für den Einstieg in den Markt dafür, dass die Zahl der Anbieter relativ gering blieb[5]. Hieraus resultierte nicht nur die Garantie der Rundfunkfreiheit, sondern auch eine Ausgestaltungspflicht, die auch bei Abwesenheit eines Marktes zu einer Pluralität führen soll[6]. Anders als im relativ übersichtlichen Rundfunkmarkt besteht im Internet das Problem nicht darin, dass der Markt keine ausreichende Informationsvielfalt gewährleisten könnte, sondern darin, dass der Nutzer in der Fülle von Informationen nicht die für ihn relevanten finden kann. Daher ist er auf die Hilfe von Suchmaschinen und Portalen angewiesen, welche nunmehr über einen wesentlich größeren Einfluss auf die Kommunikation als die Anbieter verfügen[7]: Ohne Aufnahme in eine Suchmaschine besteht kaum eine Chance, dass Angebote gefunden und rezipiert werden können. Dies kann bei der Beurteilung der rechtlichen Möglichkeiten und Pflichten des Staates nicht ohne Auswirkungen bleiben.

Anders als in traditionellen Medien ist die Hemmschwelle zum Einstieg in den Markt denkbar gering – es genügt Speicherplatz und eine Domain[8] –, so dass eine unzureichende Bereitstellung der erforderlichen Güter weder zu beobachten noch in näherer Zukunft vorstellbar ist. Daher ist die

1Hoffmann-Riem, Gesetzliche Gewährleistung, S.60.

2Hoffmann-Riem, Gesetzliche Gewährleistung, S.60f.

3Hoffmann-Riem, Gesetzliche Gewährleistung, S.61.

4Holznagel, Regulierte Selbstregulierung, S.88.

5BVerfGE 12, 205, 261. Ob dies angesichts von Satellitenfernsehen, DVB-T und diversen digitalen Sendern heute noch uneingeschränkt gelten kann, darf als zweifelhaft gelten.

6BVerfGE 12, 205, 262 ff.; 57, 295, 320ff.

7Hoffmann-Riem, Gesetzliche Gewährleistung, S.71.

8Holznagel, Regulierte Selbstregulierung, S.88.

Situation im Internet – wegen der hohen Investitionen in konventionellen Medien, für die im kommerziellen Bereich immer ein ausreichendes, zahlendes Publikum vorhanden sein muss – nicht mit der in anderen Sektoren des Medienbereichs vergleichbar. Es gibt derzeit keinen Bedarf für staatliche Angebote und es kann davon ausgegangen werden, dass der Markt auch in Zukunft eine mehr als ausreichende Bandbreite an Informationen zur Verfügung stellt.

2. Eingriffe zur Gewährleistung der Freiheit

Die vorangegangenen Ausführungen haben gezeigt, dass nicht staatliche Aktivitäten zur Erreichung eines die Wahrnehmung der Kommunikationsfreiheiten fördernden Angebots, sondern vielmehr Tätigkeiten zur Verhinderung von privaten, die Kommunikationsfreiheiten einschränkenden, Eingriffen wichtig sind. Anders als die oben beschriebenen Maßnahmen sind diese nicht reaktiv, sondern präventiv.

Wie bereits[1] dargestellt, können verschiedene Akteure, die sich nur nur teilweise innerhalb des Wirkungsbereichs nationaler Regierungen befinden, in den Kommunikationsprozess eingreifen. Des Weiteren ist die Gewährleistungspflicht auch die Grenze staatlicher Regulierung.

a. Regulierung gegenüber nationalen Akteuren

Einflussnahme gegenüber Inhalteanbietern kommt in erster Linie durch Anregung erwünschten Verhaltens in Frage. Denkbar wären mit entsprechenden Kennzeichnungen einhergehende Auszeichnungen für „gute Angebote“, wobei sich die staatliche Tätigkeit wegen der Neutralitätspflicht auf die Ausarbeitung von Kriterien und die Gründung einer die Preisvergabe eigenverantwortlich arrangierenden Organisation zu beschränken hätte. Eine andere Möglichkeit bestünde in der Ausarbeitung von Zertifikaten, für deren Vergabe allerdings die gerade aufgestellten Kriterien – die auch von Suchmaschinen bei der Darstellung von Suchergebnissen berücksichtigt werden könnten – gleichsam zu gelten hätten.

Der Staat muss weiterhin gewährleisten, dass Access-Provider und Suchmaschinen transparente Filtersysteme einsetzen sowie die Verwendung von Filtersystemen ihren Nutzern gegenüber offen legen[2]. Außerdem muss er sicherstellen, dass keine Suchmaschine eine marktbeherrschende Stellung einnimmt bzw. dass bei Erreichen einer marktbeherrschenden Stellung der Anspruch auf Zugang zu der Suchmaschine besteht[3]. Dies gebietet die Rolle jener Akteure für die Wahrnehmung der Kommunikationsfreiheiten[4]. Als problematisch erweist sich in diesem Zusammenhang die zunehmende Verschmelzung von Infrastrukturprovidern mit Anbietern von Inhalten, von der auch

1S.o. S.30ff.

2Das war bei der Beta-Version von MSN-Search nicht der Fall, welche gesuchte Inhalte nach unklaren Kriterien filterte; so führte eine Suche nach „Staatsexamen“ wegen der enthaltenen Buchstabenfolge „sex“ zu keinem Ergebnis.

3Ott, MMR 2006, 195, 196ff.

4Hoffmann-Riem, Gesetzliche Gewährleistung, S.72.

Suchmaschinen betroffen sein können[1]: Kommerzielle Interessen können in solchen Fällen zu einer Bevorzugung eigener Inhalte bzw. derjenigen der Partner bis zur Ausblendung konkurrierender Anbieter führen, was dem Nutzer, da er in der Regel keine Kenntnis mehr von konkurrierenden Angeboten erhalten wird, weitestgehend intransparent bleibt. Ähnlich – wenngleich sie nicht so einschneidende Auswirkungen wie der zuvor beschriebene Fall zeitigt – ist die derzeit übliche, nicht kenntlich gemachte Höherplatzierung bezahlter Links in den meisten Suchmaschinen zu bewerten[2].
Das Interesse am Erhalt der Kommunikationsfreiheit dürfte auch gegenüber den Schranken des Art. 5 II GG, die ihrerseits die Gewährleistungspflichten eingrenzen, überwiegen.

b. Beeinflussung internationaler Akteure

Ebenso wie auf Standardisierungsorganisationen eingewirkt werden kann, damit diese ihre Standards so fassen, dass eine Regulierung der Inhalte möglich wird, können Staaten auf demselben Weg Einfluss darauf nehmen, dass dies die Kommunikationsfreiheit nicht zu stark einschränkt. Diese Pflicht ist Bestandteil der Gewährleistung der Kommunikationsfreiheit und wirkt als Schranke der Möglichkeiten des Staates zur Beeinflussung der Standardisierungsvorgänge.

3. Zulassungspflicht für Anbieter?

Angesichts der Unübersichtlichkeit des Angebots im Internet und der damit einhergehenden Schwierigkeiten, qualitativ hochwertige Angebote zu finden, wäre die Einführung einer Zulassungs- oder Lizenzpflicht, ähnlich wie im Rundfunkbereich, denkbar. So könnte der Staat gewährleisten, dass bestehende Angebote wahrgenommen werden, statt im „Rauschen der Inhalte“ verloren zu gehen, und ebenso, dass ein ausgewogenes Verhältnis zwischen verschiedenartigen Angeboten, die eine gewisse inhaltliche Vielfalt bieten, besteht. Dies entspräche auch der Gewährleistungskomponente des Art. 5 I 2 GG; allerdings sprechen verschiedene Aspekte gegen derartige Regelungen. Zunächst sieht § 4 TMG explizit vor, dass keine Zulassungs- und Anmeldepflicht besteht. Das gilt allerdings nur für Telemedien und nicht für als Rundfunk zu qualifizierende Angebote. Die Verhältnismäßigkeit einer derartigen Regelung wäre auch zu verneinen: Sie wäre aufgrund ihrer notwendigen Beschränkung auf Deutschland weder geeignet, den Informationsüberfluss zu beseitigen[3], noch angemessen, da, anders als im Rundfunksektor, keine Knappheit an Übertragungswegen besteht und daher jeder Anbieter sein Angebot gleichberechtigt verbreiten beziehungsweise zugänglich machen kann. Da gleichzeitig die Kosten, verglichen mit

1Hoffmann-Riem, Gesetzliche Gewährleistung, S.72. AOL besitzt eigene Suchdienste und stellt außerdem Speicherplatz und Zugänge bereit. Auch andere Anbieter, insbesondere Microsoft, versuchen, ähnliche Strukturen zu schaffen.

2Einzig Google listet bezahlte Links – AdWords genannt – getrennt von den Ergebnissen der Suchanfragen und nicht als deren Bestandteil auf.

3Hoffmann-Riem, Gesetzliche Gewährleistung, S.76.

denen der Produktion von Rundfunkinhalten, relativ gering sind, kann der Markt die Regulierung herbeiführen. Auch Angebote, die sich nur an wenige Nutzer richten, können wirtschaftlich betrieben werden, ohne dabei andere Angebote, die für eine größere Öffentlichkeit von Bedeutung sind, einzuschränken.

Die Lösung sollte nicht auf der Ebene des Angebots, sondern bei dessen Auffindbarkeit liegen; der Staat hat daher sein Hauptaugenmerk auf die Tätigkeit der Suchmaschinen zu richten.

VIII. Zwischenergebnis

Technisch an der Datenübertragung beteiligte Provider haften im Grundsatz nicht; eine andere Regelung dürfte rechtlich auch nicht möglich sein. Die Ausnahmen von der grundsätzlichen Privilegierung reichen jedoch nicht weit genug. Access- und Hostprovider sollten nur bei positiver Kenntnis der Rechtswidrigkeit der Inhalte für diese haften. Dies gilt nicht für die Störerhaftung, bei der es aber auch nur_um die Entfernung der Inhalte geht; hierbei muss der Verletzte die Rechtswidrigkeit der Inhalte zumindest substantiiert darlegen, da alles andere lediglich der Schaffung zusätzlicher Haftender dienen würde.

Die Haftung für das Setzen von Links wird von der neueren Rechtsprechung überspannt. Zu fordern wäre eine weitgehende Haftungsfreistellung analog der Vorschriften zur Haftungsfreistellung der Access-Provider, die im Übrigen auch für Suchmaschinen angewandt werden.

Im Bereich des Jugendschutzrechts schießt der Gesetzgeber über das angestrebte Ziel hinaus: Die Regelungen werden letztendlich nicht zu einem wirksamen Jugendschutz im Internet führen, sondern nur zu einem jugendfreien „deutschen“ Internet. Im Widerspruch zu den theoretischen Grundlagen fehlt es den Selbstregulierungsgremien an der notwendigen Freiheit: Ihre Entscheidungen sind weder vor einer Überprüfung durch die KJM geschützt noch können die Regulierten gegen sie vorgehen. Die Ausformung des Konzepts der regulierten Selbstregulierung ist so angelegt, dass es mit einiger Sicherheit scheitern wird. Die bisherigen Ergebnisse sind wenig ermutigend. Um dieses ungenügende Ergebnis zu erreichen, werden die Grenzen des verfassungsrechtlich Zulässigen überschritten.

Im Bereich der Bekämpfung von Spam sind Selbstregulierungsmaßnahmen, besonders technische, derzeit erfolgversprechender als staatliche Maßnahmen. Das Problem von Spam ist eher ein technisches als ein rechtliches. Dementsprechend muss seine Lösung auch eine technische sein.

Es besteht des Weiteren Handlungsbedarf bei der Gewährleistung der Freiheiten, die durch Marktkräfte eingeschränkt zu werden drohen, indem größere und finanzkräftigere Akteure die Möglichkeit haben, kleinere Konkurrenten aus dem Netz zu drängen. Ein guter Ansatz ist in diesem Zusammenhang die Förderung der Entwicklung von neuen Suchmaschinen wie „Quaero“ und „Theseus“, die sich dem entstehenden Google-Monopol bzw. dem Oligopol von Google, Yahoo und

Microsoft entgegenstellen können. Andernfalls besteht, anders als bei herkömmlichen Medien, die Gefahr, dass zwar Angebote vorhanden sind, ihre Auffindbarkeit aber durch nicht transparente Kriterien von Privaten bestimmt wird. Die Folgen wären zensurähnlich. Inhaltlich erscheint aber keine Aktivität notwendig, da die erwünschte Pluralität der Angebote gewährleistet ist.

D. Standards / Organisationen

In Deutschland ist die technische Ebene der Internet-Kommunikation weitgehend staatsfrei. Viele Server, Router und Teilnetze, über die auch ein Teil des kommerziellen Verkehrs fließt, werden zwar von Universitäten und Forschungseinrichtungen bereitgestellt, die Telekommunikations-infrastruktur, also die Kabel, mit denen die verschiedenen Netze verbunden sind, dürfte sich aber überwiegend in der Hand der Deutschen Telekom AG, also im zumindest mittelbaren Einfluss-bereich des Staates, befinden. Andererseits gehören auch nicht unwesentliche Teile des Backbones zum Eigentum verschiedener, großer internationaler Netzwerkbetreiber: Der europaweit wichtigste Knoten zur Verbindung von Netzen, DE-CIX, wird beispielsweise von eco e.V., dessen Mitglieder die Netzwerkbetreiber sind, betrieben. Diese partielle Kontrolle hat staatliche Institutionen aber noch nicht dazu verführt, über ihre Kontrolle über Teile der Infrastruktur auf die Struktur des Netzes einzuwirken. Technisch wäre eine Einflussnahme mit dem Risiko behaftet, die Kompatibilität und damit die Möglichkeit der Kommunikation mit dem Ausland zu verlieren. Die Gestaltungsmöglichkeiten auf den physikalischen Netzwerkebenen sind außerdem eher gering.

Im Gegensatz dazu besteht sowohl auf internationaler als auch auf nationaler Ebene eine zunehmende Diskussion über „Internet Governance“. Der Begriff der „Governance“ ist noch teilweise unklar. In seinem Grundbereich geht es aber um die Kontrolle über die bisherigen Institutionen und die von ihnen ausgeübten Funktionen. Als prominenteste Funktion wäre die Verwaltung des DNS – und damit die Hoheit über die Vergabe von Domainnamen sowie IP-Adressen – zu nennen.

Die Vergabe von Domainnamen wird in Deutschland von der DENIC e.G., also einer Genossenschaft, deren Mitglieder die deutschen Netzwerkbetreiber sind, wahrgenommen. IP-Nummern werden europaweit von der RIPE NCC, einer privatwirtschaftlichen Gesellschaft mit Sitz in Amsterdam, ausgegeben. Die Frage, ob diese Aufgaben nicht von der Bundesnetzagentur, also einer staatlichen Behörde, wahrgenommen werden müssten, ist schon früh entstanden und vor dem Hintergrund der ersten Versuche mit ENUM, einem Protokoll, das die Verbindung von Telefon und Internet unter einer einheitlichen Rufnummer bzw. Adresse erlaubt[1], wieder aktuell geworden. ENUM bildet keine „eigenen“ Nummern, es erlaubt nur eine Übernahme vergebener Nummern und

1 Dabei wird die Rufnummer „umgedreht“ und eine Adresse unter der ENUM-Domain .e164.arpa zugewiesen. Eine internationale Rufnummer +493012345678 wird also zu 8.7.6.5.4.3.2.1.0.3.9.4.e164.arpa.

deren Umwandlung in Domains. Diese Möglichkeit besteht allerdings auch schon heute unter herkömmlichen „.de"-Adressen[1]. Daher ist nicht nur angesichts der ENUM-Einführung fraglich, inwieweit Domainnamen bzw. IP-Adressen der telekommunikationsrechtlichen Regulierung unterfallen[2]. Sind sie von dieser umfasst, besteht eine staatliche Aufgabe in jedem Fall; sind sie es nicht, wäre es möglich, dass sich eine staatliche Aufgabe aus der Verfassung herleitet.

I. Vergabe von Basis-Ressourcen als staatliche Aufgabe

Sowohl IP-Nummern als auch Domainnamen sind für den Zugang zu Inhalten bzw. Diensten des Internets unverzichtbare Bestandteile. Eine IP-Nummer ist notwendig, damit Rechner in einem – auf dem IP-Protokoll basierenden – Netzwerk überhaupt von anderen Rechnern angesprochen werden und mit diesen kommunizieren, also Datenpakete senden und empfangen, können. Domainnamen sind keine technische, aber eine praktische Notwendigkeit: Die Domain „www.rewi.hu-berlin.de" kann man sich ohne Weiteres merken, die Ziffernfolge „141.20.120.67" hingegen nicht, obwohl mit beiden Adressierungsverfahren derselbe Rechner angesprochen wird.

Wenn ein Rechner nun verschiedene Dienste bereitstellt, beispielsweise Mailservice, FTP oder HTTP, werden diese durch so genannte Ports gekennzeichnet, wobei jedem Dienst standardmäßig bestimmte Ports zugeordnet sind: Für HTTP sind das die Ports 80 und 8080, für Mail ist es 25 etc. Die Portkennung wird, getrennt durch einen Doppelpunkt, an die IP-Nummer angehängt, es ergibt sich z.B. 141.20.120.68:8080 – eine Ziffernfolge, die sich wohl niemand, insbesondere angesichts der Vielzahl von Domains, merken kann[3].

Die Einführung des DNS Anfang der 90er Jahre war somit notwendige Voraussetzung für die Ausweitung der Nutzung des Internets durch weite Teile der Bevölkerung. Aus der technischen Unterscheidung zwischen IP-Nummern und Domainnamen ergibt sich zunächst auch eine notwendige rechtliche Differenzierung. Der enge technische Zusammenhang der beiden Adressierungsverfahren könnte allerdings – einer differenzierten rechtlichen Bewertung zum Trotz – zu einer identischen rechtlichen Behandlung führen.

Einfachgesetzliche Regelungen für die Vergabe von IP-Nummern und Domains fehlen. Verfassungsrechtlich sind lediglich Staatsaufgaben der Bundes in der Telekommunikation in Art. 87 f GG geregelt. Ausgangspunkt für eine rechtliche Betrachtung der staatlichen Vergabe von IP-Nummern und Domainnamen kann daher nur Art. 87 f GG sein.

1. Hoheitsaufgaben

Es gibt zwei Arten von Hoheitsaufgaben: Zum einen existiert ein klassischer Kanon von Aufgaben, die der Staat in der Regel selbst und durch Beamte durchzuführen hat, zum anderen können

1Koenig/Neumann, CR 03, 182, 183.

2Koenig/Neumann, CR 03, 182, 183.

3Zumal diese Port-Einstellungen Standardeinstellungen sind, die aber vom Serverbetreiber ohne Weiteres verändert werden können.

Hoheitsverpflichtungen durch gesetzgeberische Zuweisung beliebig vermehrt werden. Zum Kanon der „klassischen Hoheitsaufgaben“ gehört die Vergabe von IP-Nummern sicher nicht; allerdings finden sich in Art. 87 f GG sowie im TKG Regelungen, die auf die Vergabe von IP-Nummern angewandt werden könnten.

2. Regelungsstruktur des Art. 87 f GG

Nach Art. 87 f I GG hat der Bund die flächendeckende Versorgung mit Telekommunikationsdienstleistungen zu gewährleisten. Das bedeutet nicht, dass er diese selbst zu erbringen hat. Vielmehr sieht Art. 87 f II 1 GG vor, dass die Aufgaben des Abs. I durch privatwirtschaftliche Unternehmen erfüllt werden. Damit enthält Abs. II S.1 einen Verfassungsauftrag zur Privatisierung[1] und verbietet gleichzeitig die Erbringung der Dienstleistungen durch die Verwaltung[2]. Die Gewährleistung soll nach Maßgabe eines Bundesgesetzes – des Telekommunikationsgesetzes (TKG) – geschehen.

Nach Art. 87 f II 2 GG sind Hoheitsaufgaben durch bundeseigene Verwaltung auszuführen. Hier findet sich als Gegenstück zur privatwirtschaftlichen Ausgestaltung der Telekommunikationsdienstleistungen die Pflicht des Staates zur eigenen Wahrnehmung von Hoheitsaufgaben; eine Delegation an Private ist nicht zulässig[3]. Nach Abs. III ist eine mittelbare Bundesverwaltung für einzelne Aufgabenbereiche zulässig, postalische Tätigkeiten und Hoheitsaufgaben sind hierbei allerdings ausgeschlossen[4].

Wenn es sich bei der Vergabe von IP-Nummern und Domainnamen um Hoheitsaufgaben handelte, wäre der Bund verpflichtet, diese selbst zu übernehmen; ein Wahlrecht könnte insofern nicht bestehen[5]. Als Bundesbehörde für die Wahrnehmung von Hoheitsaufgaben wurde zum 01.01.1998 die Regulierungsbehörde für Telekommunikation und Post (RegTP) eingerichtet; sie trägt seit dem 13.07.2005 den Namen Bundesnetzagentur.

3. Hoheitsaufgaben auf dem Gebiet der Telekommunikation

Hoheitliche Aufgaben ergeben sich nicht von selbst aus Art. 87 f II 2 GG[6], sondern aus nationaler Gesetzgebung sowie „supranationalen Aussagen“[7]; auch können sie unabhängig von diesen

1 Statt Vieler: M/ D/ H/ S-Lerche, Art. 87f Rn. 54; Jarass/Pieroth-Pieroth, Art. 87f Rn. 3.

2Sachs-Windthorst, Art. 87f, Rn. 22; BT Drs. 12/7269, S. 5.

3 Sachs-Windthorst, Art. 87f, Rn. 33; M/D/H/S-Lerche, Art. 87f Rn. 102; M/K/S-Gersdorf, Art. 87f Rn. 99. Die Übertragung einzelner Aufgaben an Beliehene wird teilweise für zulässig gehalten; dies ist aber schwerlich mit dem Wortlaut des Art. 87 f II 2 GG in Übereinstimmung zu bringen.

4 BT Drs. 12/7269, S. 5, M/ D/ H/ S-Lerche, Art. 87f, Rn. 116f.

5 So aber Trute/Spoerr/Bosch-Spoerr, § 43 Rn. 16.

6 M/D/H/S-Lerche, Art. 87f, Rn. 93.

7 M/D/H/S-Lerche, Art. 87f, Rn. 93.

legislativen Festlegungen bestehen. Ein Gesetz, das Hoheitsaufgaben festschreibt, stellt § 66 TKG dar. Entstehungsgeschichtlich gehören zu Hoheitsaufgaben Fragen der Standardisierung, Normierung, die Frequenzverwaltung[1] und – durch die Erwähnung in § 66 TKG – auch die Nummerierung.

4. IP-Nummern und Domainnamen als Nummern nach § 66 TKG?

Nach § 66 TKG obliegt die Nummerierung der Bundesnetzagentur. Nummern im Sinne des § 66 TKG sind in § 3 Nr. 13 TKG definiert als Zeichenfolgen, die der Adressierung in Telekommunikationsnetzen dienen. Dies trifft auf Rufnummern für den Sprachkommunikationsdienst zu. Ob auch IP-Nummern und Domainnamen unter den Rufnummernbegriff fallen, ist umstritten.

a. IP-Nummern

Jeder Rechner, der am Datenverkehr über das Internet oder ein anderes IP-basiertes (Sub-) Netz teilnimmt, benötigt eine IP-Nummer, damit die gesendeten Informationen ihn erreichen können. Dass diese Nummer, anders als eine Telefonnummer, in der Regel kaum jemandem bekannt ist, spielt für die Einordnung keine Rolle. Damit erfüllen IP-Nummern nach dem Gesetzeswortlaut den Nummernbegriff des § 3 Nr. 13 TKG[2]. Allerdings ist fraglich, ob der Staat praktisch zur Vergabe in der Lage wäre – technische Voraussetzungen können nur selten durch Gesetz geändert werden – oder ob der Nummernbegriff nicht teleologisch so zu reduzieren ist, so dass IP-Nummern ausgenommen sind.

(1.) Derzeitige Vergabepraxis

Die Hoheit über die Vergabe von IP-Nummern weltweit hat die ICANN[3]. Diese delegiert die Vergabe für bestimmte geographische Zonen an fünf regionale Vergabestellen, so genannte Network Coordination Center (NCC). Für Europa und den Mittleren Osten liegt die Zuständigkeit bei der RIPE NCC[4] mit Sitz in Amsterdam[5]. Die RIPE NCC ist, anders als die Trägergesellschaft RIPE, eine rechtsfähige Gesellschaft, die jedoch nicht auf Gewinnerzielung ausgerichtet ist[6].

1 BT Drs. 12/7269, S.5.

2 So auch Holznagel, MMR 03, 182ff.; König/Neumann, CR 03, 182, 183.; dies. K&R 99, 145ff.; Schäfer CR 02, 690ff; Trute/Bosch/Spoerr- Spoerr, § 43 Rn. 16.

3http://www.icann.org/tr/english.html.

4Réseaux IP Européens Network Coordination Center.

5http://www.ripe.net/info/ncc/index.html.

6http://www.ripe.net/info/ncc/index.html.

(a.) Voraussetzungen für die Zuteilung

IP-Nummern werden nach nachzuweisendem Bedarf vergeben. Voraussetzung für die Zuteilung von IP-Nummern von der RIPE NCC ist die Mitgliedschaft in der RIPE[1], die grundsätzlich jeder natürlichen und juristischen Person – nach Zahlung einer Aufnahmegebühr – möglich ist[2].

(b.) Mögliche Veränderungen

Mit der Einführung von IPv6 wird die IP-Nummern-Knappheit zumindest für sehr lange Zeit beendet sein. Auch könnten sich Veränderungen bei der Zuteilung von IP-Nummern einstellen: Höchstwahrscheinlich wird die Bedarfsprüfung wegfallen und eine Regulierung nur noch durch die entstehenden Kosten stattfinden. Es wäre zudem denkbar, Personen oder Geräte mit festen IP-Adressen auszustatten[3]. Allerdings muss diese Möglichkeit auf datenschutzrechtliche Bedenken stoßen, da sie eine totale Überwachung des Kommunikationsverhaltens[4] von Personen ermöglicht und weiter vereinfacht. Hier bestünde von Seiten der EU oder einer Gruppe von Nationalstaaten Handlungsbedarf[5].

(2.) Praktische Unmöglichkeit der staatlichen Vergabe

In der Literatur wird vorgebracht, dass es dem Staat gar nicht möglich sei, IP-Nummern hoheitlich zu vergeben, weil die Zuweisung der IP-Nummernblöcke in Europa von der privatwirtschaftlichen Vereinigung RIPE NCC vorgenommen werde[6], auf die der deutsche Staat nicht zugreifen könne. Die Teilnetze des Internets seien zudem häufig staatenübergreifend, so dass auch aus diesem Grund keine staatliche Vergabe möglich sei[7]. Da sich die Struktur der Zuweisung – die ICANN vergibt Nummernblöcke für Europa an die RIPE NCC – aus privatrechtlichen Verträgen ergebe, würde eine Überführung in staatliche Verwaltung möglicherweise am Widerstand der ICANN bzw. RIPE NCC scheitern[8]. Dies sei allein deswegen zu erwarten, weil letztere sich aus den Zahlungen für die Vergabe finanziere[9].

1http://www.ripe.net/info/resource-admin/index.html

2http://www.ripe.net/rs/ipv4/index.html.

3Dies ließe neue Geschäftsmodelle wie den berühmten „sich selbst nachfüllenden Kühlschrank“ zu. Dieser ist ein oft genanntes Beispiel für neue kommerzielle Anwendungsmöglichkeiten. Die Bewertung einer Innovation, die beispielsweise immer denselben übel schmeckenden Joghurt nachbestellt, darf individuell vorgenommen werden.

4Und nicht nur des Kommunikationsverhaltens!

5Bisher werden IP-Nummern bei jeder Verbindung neu vergeben, so dass dieselbe Person anhand der IP-Nummer nur durch einen Vergleich zwischen IP-Nummer und Anschluss identifiziert werden kann. Dies ist ohne Weiteres nur dem Access-Provider möglich.

6Holznagel, MMR 03, 219, 221.

7Holznagel, MMR 03, 219, 221.

8Holznagel, MMR 03, 219, 221.

9Holznagel, MMR 03, 219, 221.

Diesen Einwänden steht jedoch entgegen, dass die Vergabe von IP-Nummern in China eine staatliche Aufgabe ist, die reibungslos funktioniert[1]. Die Bundesnetzagentur wäre außerdem nicht gehindert, Verträge sowohl mit der RIPE NCC als auch den Providern bzw. Endnutzern abzuschließen, so wie es beispielsweise bereits bei der Vergabe von 0900-Nummernblöcken geschieht. Sie müsste zwar die bei der RIPE NCC entstehenden Gebühren zahlen, könnte diese aber wiederum auf diejenigen umlegen, denen sie IP-Nummern zuweist. Gesetzlich könnte dies so geregelt werden, dass Rechner, die auf deutschem Territorium stehen und IP-Nummern von einem deutschen Provider beziehen, nur von der Bundesnetzagentur zugeteilt werden dürfen.

Eine derartige Regelung wäre auch Voraussetzung für den Vorschlag der ITU[2], die Verwaltung der IPv6-Nummern in die Hände nationaler Behörden zu legen. Aus praktischen Gründen wäre eine Verwaltung der IP-Nummern durch staatliche Behörden nicht ausgeschlossen, jedoch nicht sonderlich effizient.

(3.) Historische Auslegung

Die historische Auslegung soll ergeben, dass der Gesetzgeber bei Schaffung des TKG nicht an eine Einbeziehung von IP-Nummern gedacht, sondern in den Entwürfen den Begriff der Nummer im Sinne des § 3 Nr. 13 TKG und den der Rufnummer synonym gebraucht habe. Dies lasse eher darauf schließen, dass er nicht an IP-Nummern gedacht habe. IP-Nummern könne man aber nicht unter den Begriff der Rufnummer subsumieren, da letzterer auf Sprachtelefonie hindeute.

Das ist sicherlich richtig, allein aus dem Grunde, dass dem Gesetzgeber zu dieser Zeit die Problematik nicht bewusst war[3]; möglicherweise ahnte er überhaupt nicht, wie die Adressierung im Internet funktioniert und dass es durch den Gesetzeswortlaut Probleme mit der möglichen Einbeziehung von IP-Nummern geben könnte. Insofern ist die historische Auslegung unergiebig. Aus der scheinbar eindeutigen Formulierung ist allerdings nicht zwingend ableitbar, dass eine Auslegung nicht zulässig ist[4]. Sie wird gerade dann notwendig, wenn das Gesetz nach seinem Wortlaut für einen Sachverhalt eine Lösung vorsieht, den es möglicherweise nicht erfassen wollte[5]. Der Wortlaut hat nur eine auslegungsbegrenzende Funktion, seine Eindeutigkeit steht aber – innerhalb der Wortlautgrenze – einer Auslegung nicht entgegen[6].

Dies ist hier der Fall.

1http://www.heise.de/newsticker/meldung/53394. China setzt sich dementsprechend auch vehement für eine nationale Vergabe von IPv6-Nummern ein.

2http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf, Nr. 4.2.b.

3Holznagel, MMR 03, 219, 221.

4So aber Schäfer, CR 02, 690, 693.

5Larenz, Methodenlehre S.317.

6Larenz, Methodenlehre, S.322; König/ Neumann, CR 03, 182, 183.

(4.) Teleologische Auslegung

Die Entwicklung von Telekommunikationstechnik und Telekommunikationsrecht schreitet schnell voran, was eine stabile rechtliche Grundlage notwendig macht. Die sich auf die zum Zeitpunkt des Inkrafttretens aktuelle Technik beziehende Fassung des TKG muss nunmehr allgemeiner formuliert werden[1]. Technische Entwicklungen können häufig zu neuen Anwendungsbereichen eines bestehenden Gesetzes führen, die für den Gesetzgeber nicht voraussehbar waren. Diese Regelungsbereiche sollen nach dem Willen des Gesetzgebers nicht allein schon wegen späteren Entwicklungen vom Anwendungsbereich des TKG ausgeschlossen sein[2]. Um zu klären, ob die Hoheitsaufgaben im Bereich der Telefonie auch auch auf IP-Nummern Anwendung finden, bietet es sich an, die Regelungen des § 66 TKG nach ihrem Zweck zu analysieren und anschließend durch einen Vergleich mit IP- Nummern zu klären, ob der für die Vergabe von Rufnummern verfolgte Zweck auch bei IP-Nummern erreicht werden kann.

(a.) Hoheitsaufgaben im Bereich der Telefonie

Die Hoheitsaufgaben im Bereich der Nummerierung ergeben sich aus § 66 TKG. Nach § 66 I 1 TKG übernimmt die Bundesnetzagentur als Bundesverwaltung die Nummerierung. Dies umfasst nach S. 2 insbesondere die Strukturierung und Ausgestaltung des Nummernraumes sowie nach S. 3 die Zuteilung von Nummern. Nach § 67 I TKG legt sie ferner die Bedingungen für die Zuweisung von Nutzungsrechten für Nummern fest.

(aa). Nummernvergabe

Die Notwendigkeit der hoheitlichen Nummernverwaltung ergab sich aus der Monopolstellung der ehemaligen Post, die als einziger öffentlicher Telekommunikationsbetreiber Rufnummern vergab. Im Zuge der Liberalisierung wurde die Post aufgelöst und der Bereich der Telekommunikation auf die Deutsche Telekom AG (DTAG) ausgegliedert. Die DTAG soll aber nach der Vorstellung des TKG im Wettbewerb mit anderen Anbietern stehen, die ebenfalls eigene Anschlüsse bereitstellen. Dieser Ansatz ist nicht vereinbar mit der Möglichkeit eines Wettbewerbers, der anfänglich noch wie ein Monopolist agieren konnte, die Vergabe von Rufnummern an Konkurrenten zu behindern[3]. Eine einheitliche Verteilung von Rufnummern ist aber Grundbedingung für das Funktionieren eines einheitlichen Telefonnetzes[4]. Eine Lösung dieser Problematik kann nur in der staatlichen Vergabe

1Holznagel, MMR 03, 219, 222.

2Holznagel, MMR 03, 219, 222.

3Scheurle/Mayen-Scheurle, § 43, Rn. 1.

4Scheurle/Mayen-Scheurle, § 43, Rn. 1.

liegen. Die Hoheitsaufgabe ergibt sich folglich aus der Garantiefunktion des Staates für die Funktion der Märkte.

(bb). Strukturierung des Nummernraumes

Die Zuweisung von bestimmten Vorwahlen für bestimmte Tarife und Dienstleistungen ist für den Nutzer notwendig, um die entstehenden Kosten vorhersehen zu können; dies gilt gleichsam für Ortsvorwahlen.

Da die Kompatibilität verschiedener Anbieter im nationalen wie internationalen Bereich sichergestellt werden muss, wird auch die Strukturierung des Nummernraumes als staatliche Aufgabe in § 66 I 1 TKG genannt.

(b.) Übertragung auf IP- Nummern

Fraglich ist, ob die für Telefonnummern gewonnenen Erkenntnisse eine Anwendung der Regelungen auf IP-Nummern zulassen: Bei der Anwahl von IP-Nummern ist nicht gewährleistet, dass die Datenpakete den (geographisch) kürzesten Weg nehmen.

Außerdem sind IP-Nummern in der Regel unbekannt und ihre Kenntnis für die Nutzung der meisten Dienste auch nicht erforderlich. Des Weiteren besteht kein Bedarf für eine regionale Strukturierung, da entweder eine dynamische Vergabe der IP-Nummern erfolgt und diese somit Telefonanschlüssen zugeordnet sind oder derjenige bekannt ist, dem die Nummer zugeteilt wurde. Entfernungen spielen ebenso wenig eine Rolle wie – in der Regel – die Kenntnis des Aufenthaltsortes eines Rechners. Abgesehen davon, dass technisch gesehen kein Grund für eine lokale Strukturierung vorliegt, würde diese den ohnehin knappen IPv4- Adressraum zusätzlich einengen. Auch wenn ein Bedürfnis nach einer obersten Instanz besteht, wird deutlich, dass keine Notwendigkeit einer staatlichen Zuweisung vorliegt: Die oberste Vergabestelle funktioniert unproblematisch und kostengünstig. Eine regionale Vergabe von IP-Nummern wäre zwar möglich, ist jedoch nicht erforderlich, da die IP-Nummern, anders als Telefonnummern, in der Regel den meisten Nutzern verborgen bleiben und Entfernungen technisch irrelevant sind. Eine Anwendung der Regelungen des TKG zur Rufnummernzuteilung auf IP-Nummern und deren Vergabe scheint daher nicht von Nutzen.

(c.) Vergabe

Anders als Rufnummern zur Zeit der Zuweisung durch die Telekom wurden und werden IP-Nummern von einer Stelle vergeben, die keine kommerziellen Interessen im Wettbewerb der Provider hat. Sie verfügt zwar über ein Monopol, jedoch ist dies sowohl technisch notwendig, da für das Funktionieren des Internets immer eine „oberste“ Instanz vorhanden sein muss, als auch aus Sicht des TKG unbedenklich, solange die Stelle unparteiisch agiert, keine Wettbewerber diskriminiert und somit keine Gefahr für die privatwirtschaftliche Erbringung von Telekommunikationsdienstleistungen im Wettbewerb darstellt.

Gleiches gilt für die Bundesnetzagentur im Telefonnetz. Deren übrige Aufgaben für die Zuteilung von Rufnummern, insbesondere die regionale Strukturierung, sind für IP-Nummern indes überflüssig, da durch eine derartige Praxis kein Gewinn zu erkennen wäre. Die einzige Alternative zur derzeitigen Regelung bestünde in einer internationalen Behörde. Aber auch bei Teilnahme der Vergabestelle am Markt böte das Wettbewerbsrecht ausreichende Möglichkeiten, die ein direktes staatliches Eingreifen in die Vergabe als nicht notwendig erscheinen lassen.

(d.) Strukturierung und Ausgestaltung des Nummernraumes

Es wäre technisch möglich, IP-Nummern wie Telefonnummern nach Regionen und Diensten zu vergeben. Dies würde allerdings aufgrund der örtlichen Unabhängigkeit der Rechner [1] sowie der rein technischen Bedeutung der IP-Nummern einen gegenüber dem zu erwartenden geringen Gewinn unverhältnismäßigen Aufwand bedeuten. Des Weiteren gibt es keinen einheitlichen, Deutschland zugewiesenen Nummernraum bei IP-Nummern; eine Strukturierung der vorhandenen Nummernräume wäre zwar möglich, würde jedoch den Entzug von IP-Nummern und eine strukturierte Neuverteilung erfordern. Zu beachten wäre außerdem § 66 II TKG, nach dem eine Umgestaltung nur bei internationalen Regelungen, Empfehlungen oder zur besseren Nutzung des Nummernraumes – unter Berücksichtigung der Interessen der Nutzer – zulässig ist.
Da jedoch weder ein Nutzerinteresse noch eine verbesserte Nutzungsmöglichkeit erkennbar sind, die internationalen Gepflogenheiten bei der IP-Nummernvergabe keine geografische Verteilung beinhalten und auch die RfCs, auf denen die Zuweisung beruht, keine lokale Strukturierung vorsehen, kann gefolgert werden, dass die Regelung des § 66 II TKG einer Umgestaltung des IP-Nummernraumes nach dem Vorbild der Rufnummern entgegensteht.

(e.) Ergebnis

Auch die teleologische Auslegung ergibt kein eindeutiges Ergebnis. Das Überwiegen der nicht anwendbaren oder nutzlosen Regelungen lässt aber darauf schließen, dass der Nummernbegriff des § 66 TKG sich nicht auf IP-Nummern bezieht und deren Vergabe somit keine Hoheitsaufgabe aufgrund gesetzlicher Erfassung darstellt.

(5.) Aufgabenzuweisung durch Art. 87 f GG

Es wäre denkbar, dass Art. 87 f GG auch ohne Vorliegen einer gesetzlichen Regelung zur Zuweisung von Hoheitsaufgaben führt, da er neben der Kompetenzzuweisung an den Bund eine

1Es ist möglich, einem Gerät eine feste IP-Nummer zuzuweisen, mit der es an verschiedenen Orten Netzwerkverbindungen aufbauen kann.

materielle Komponente aufweist[1], die sich auf die Konstituierung von Pflichten in Abs. I und Abs. II 1 bezieht[2]. Allerdings kann der Begriff der Hoheitsaufgaben in Art. 87 f II 2 GG nicht auf den traditionellen Kanon und die gesetzliche Übernahme von Aufgaben beschränkt sein: Wären Hoheitsaufgaben nur solche, die entweder dem traditionellen Kanon entstammen oder die der Gesetzgeber durch Gesetz übernommen hat, wäre die Vorschrift des Art. 87 f II 2 GG weitestgehend sinnlos – der Gesetzgeber könnte sich der Pflicht zur Erfüllung dieser Aufgaben durch Gesetzesänderung entziehen. Genau das soll durch eine Regelung in der Verfassung verhindert werden: Der Staat soll die für das Erreichen der Ziele der Postneuordnung notwendigen Aufgaben selbst und durch unmittelbare Bundesverwaltung wahrnehmen[3].

Als weitere, unabhängig von der Gesetzgebung des TKG in Art. 87 f II 2 GG existierende, Hoheitsaufgaben sind auch die Sicherung des Grundrechts aus Art. 10 GG, die Gewährleistung ausreichender Telekommunikationsdienstleistungen für die Allgemeinheit und die Förderung eines funktionierenden Wettbewerbs allgemein akzeptiert[4]. Begrenzt wird die Möglichkeit der Begründung neuer Hoheitspflichten durch Art. 87 f II 1 GG[5]. Wie weit der Kreis der Hoheitsaufgaben zu ziehen ist, steht damit freilich noch nicht fest. Nach Art. 87 f I GG ist indes die Gewährleistung einer ausreichenden Kommunikationsinfrastruktur in jedem Fall inbegriffen[6]. Wenn demnach die für die Kommunikation per Internet notwendige Vergabe von IP-Nummern eine Hoheitsaufgabe darstellt, könnten die zur Erledigung dieses Auftrags notwendigen Eingriffe in Grundrechte Dritter auf § 66 TKG gestützt werden. Eine diesbezügliche Auslegung ist zwar nicht nahe liegend, doch zumindest möglich, da unter § 66 TKG die Aufgaben gefasst werden können, deren Erledigung im öffentlichen Interesse steht, die für einen funktionierenden Wettbewerb notwendig sind und für die eine staatliche Übernahme notwendig ist.

Die Garantie einer funktionsfähigen, diskriminierungsfreien Infrastruktur für das Internet dient zweifellos dem Gemeinwohl und steht im öffentlichen Interesse. Allerdings ist fraglich, ob sie für einen funktionierenden Wettbewerb notwendig ist: Die RIPE NCC als vergebende Stelle ist nie Wettbewerberin im Angebot von Internet-Zugängen oder anderen Diensten gewesen, auch ist bisher kein Machtmissbrauch bei der Verteilung von IP-Nummern bekannt. Da diejenigen, die IP-Nummern erhalten möchten, nicht nur ihren Bedarf nachweisen, sondern auch Mitglieder der RIPE

1 Sachs-Windthorst, Art. 87 f, Rn. 34; Kloepfer, § 3 Rn. 5.

2 Sachs-Windthorst, Art. 87 f, Rn. 34; Kloepfer, § 3 Rn. 5.

3M/D/H/S-Lerche, Art. 87 f, Rn. 10.

4 Sachs-Windthorst, Art. 87 f, Rn. 31; Dreier-Wieland, Art. 87 f, Rn. 18; M/K/S-Gersdorf, Art. 87 f, Rn. 90; Jarass/ Pieroth-Pieroth, Art. 87 f, Rn. 4.

5Sachs-Windthorst, Art. 87 f, Rn. 17.

6Schmidt-Bleibtreu/ Klein-Henneke/ Ruge, Art. 87 f, Rn. 4; M/D/H/S-Lerche, Art. 87f., Rn. 10; Sachs-Windthorst, Art. 87 f, Rn. 34.

NCC werden müssen, steht ihnen folglich auch eine Kontrolle über deren Geschäftspraktiken zu. Aus diesem Grund wäre die Entstehung eines „closed market“ theoretisch denkbar[1]. Diese Überlegung stellt sich allerdings, speziell vor dem Hintergrund der Einführung von IPv6, durch welche die Nummernknappheit endgültig der Vergangenheit angehören wird, als unwahrscheinlich dar. Ein Bedürfnis nach einer staatlichen Vergabe zur Herstellung eines funktionsfähigen Wettbewerbs ist daher nicht gegeben; vielmehr besteht bereits ein intensiver Wettbewerb um Internetzugänge. Bei der Verwaltung aller IP-Nummern hingegen erscheint ein Wettbewerb wenig wahrscheinlich und lässt daher eine, zudem erforderliche, höchste Stelle zu[2]. Somit ist auch hier keine Hoheitsaufgabe erkennbar: Die Vergabe von IP-Nummern fällt nicht in den Aufgabenbereich der Bundesnetzagentur.

(6.) Infrastrukturgewährleistung als Staatsaufgabe

Es war lange Zeit anerkannt, dass die Gewährleistung von bestimmten Infrastrukturen[3] eine staatliche Aufgabe aus dem Bereich der Daseinsvorsorge darstellt[4]. Diese Aufgabe haben Staaten in der Regel durch eigene Verwaltung, geschützte Monopole oder in Form von staatlich reguliertem Wettbewerb erfüllt[5]. Die entstandenen Netze wurden teilweise als natürliche Monopole angesehen, weil die Kosten zur Errichtung eines Konkurrenznetzes prohibitiv waren und die Leistungserbringung durch mehrere Konkurrenten als ineffizienter als durch den Monopolisten galt[6]. Gerade im Bereich der Telekommunikation hat sich aber gezeigt, dass eine Entmonopolisierung möglich ist, indem anderen Anbietern Zugang zu den Einrichtungen des Monopolisten gewährt wird[7]. Eine wichtig gewordene Infrastruktur stellt auch das Internet dar, dessen Aufbau, der – anders als bei Telekommunikationsnetzen oder Stromnetzen – nicht durch Unternehmen erfolgte, durch die USA angestoßen und auch weitestgehend finanziert wurde. Inzwischen ist der Betrieb der Infrastruktur staatsfrei[8] und ein Bedürfnis der Wahrnehmung einer Infrastrukturverantwortung nicht ersichtlich. Soweit eine Grundversorgung mit lebenswichtiger Kommunikationsinfrastruktur zu

---

1Selbst wenn es zu einem abgeschlossen Markt kommen sollte, ist dieser aufgrund der großen Mitgliederzahl der RIPE immer noch relativ groß, so dass die typischen Gefahren einer Kartellbildung kaum bestehen dürften.

2Siehe auch Stellungnahme der RIR zur Übernahme der Ipv6-Verwaltung durch die ITU: http://www.nro.net/documents/pdf/nro17.pdf.

3Zu diesen Infrastrukturen gehören unter anderem Stromnetze, Wasserversorgung, Verkehrsnetze und Telekommunikationsnetze.

4So schon Adam Smith, Wohlstand der Nationen, S.612ff.

5Kutzschbach, S.24.

6Kutzschbach, S.32ff.

7Staatliches Eingreifen war notwendig, da andernfalls aufgrund der Monopolstellung der DTAG kein Wettbewerb hätte zustande kommen können.

8Seit parallel zum NSFNET auch ein kommerzieller Backbone aufgebaut wurde.

gewährleisten ist, wird dies durch die Pflicht zur Erbringung von Standardangeboten in § 23 I TKG sichergestellt.

Die Wahrnehmung staatlicher Infrastrukturverantwortung im Bereich von Computernetzwerken hat in der Vergangenheit in Europa nicht zur Verbesserung der Infrastruktur beigetragen, sondern war vielmehr der Auslöser für die große Verspätung Deutschlands beim Anschluss an das zu dieser Zeit hauptsächlich in den USA bestehende Internet[1].

Es ist anzunehmen, dass das Angebot von Internet-Übertragungswegen in naher Zukunft von der Gewährleistung von

Universaldiensten umfasst sein wird. Da die private Leistungserbringung gemeinhin problemlos verläuft, sind keine Strukturen erkennbar, die einen regulierenden Eingriff des Staates im Sinne der Gewährleistungspflicht erfordern würden.

b. Regelung durch zukünftige Gesetzgebung

Eine Übernahme der Aufgabe der IP-Nummernvergabe von Seiten des Staates könnte, wie gezeigt, durch zukünftige Entwicklungen erforderlich werden oder auch ohne zwingende Notwendigkeit erfolgen. Um letzteres zu ermöglichen, müsste eine Änderung des TKG, des Art. 87 f GG oder der Erlass eines neuen Gesetzes vorgenommen werden, was Folgeprobleme mit sich brächte: Beispielsweise müssten den Nutzern bzw. den Providern die vorhandenen, von der RIPE NCC zugewiesenen Nummern entzogen werden, bevor die Bundesnetzagentur sie neu zuteilen könnte. Dies würde einerseits voraussetzen, dass die RIPE NCC der Bundesnetzagentur Nummernblöcke überließe, was sich allerdings einer Regelung durch den Gesetzgeber entzieht, und andererseits, dass ein solcher Entzug rechtlich zulässig wäre.

(1.) Rechtliche Möglichkeiten der Entziehung von IP-Nummern

(a.) Rechtsnatur von IP-Nummern

IP-Nummern werden von der RIPE NCC an Provider vergeben; diese Zuteilung behält Gültigkeit, soweit die Zahlung der Mitgliedschaftsbeiträge erfolgt[2]. Die Höhe der Beiträge bestimmt sich allerdings nicht nur nach der Zahl der zugeteilten Adressen, sondern auch nach anderen Faktoren[3].

Aufschluss über die Art der Rechte an IP-Nummern kann ein Vergleich mit ähnlichen Ressourcen geben; infrage kommen hier Rufnummern nach dem TKG sowie (Funk-)Frequenzen. Mögliche Rechte wären Nutzungsrechte an fremdem Eigentum, Nutzungsrechte an Allmendegütern oder Eigentum des Besitzers.

---

1 Zu erwähnen ist hier außerdem der Aufbau eines Glasfasernetzwerkes in Ostdeutschland, der ursprünglich auf eine „Datenautobahn“ abzielte und inzwischen aufgrund seiner immensen Kosten den Ausbau von DSL behindert. Derzeit wird angedacht, die Glasfaserinfrastruktur wieder zu entfernen und durch die – zuvor für veraltet erklärten – Kupferkabel zu ersetzen.

2 http://www.ripe.net/ripencc/faq/general/qa1.html#11.

3 Näher dazu: http://www.ripe.net/ripe/docs/billing.html (Stand 23.12.03).

(aa.) Nutzungsrechte analog § 66 TKG

Nach § 66 TKG erwerben Nutzer nur zeitlich begrenzte Nutzungsrechte und kein Eigentum an Nummern. Dies gilt nicht für IP-Nummern, da diese nicht unter den geltenden Nummernbegriff fallen. Auch eine Analogie erscheint ausgeschlossen, da die Regelungen des TKG von ihrer Zweckrichtung her nicht auf IP-Nummern anwendbar sind[1].

(bb.) Eigentum im Sinne des Art. 14 I GG

Sämtliche Arten von Nummern sowie Domains könnten Eigentum im Sinne des Art. 14 GG darstellen. Der Schutzbereich von Art. 14 GG ist nicht abgeschlossen, sondern wird vielmehr durch die von ihm umfassten Objekte beschrieben[2]. _Der Maßstab für die Beurteilung des Eigentumsschutzes besteht in der durch die Verfassung getroffenen Wertentscheidung, wobei auf Zweck und Funktion des Eigentumsschutzes zurückzugreifen ist[3]: Danach soll dem Einzelnen die eigenverantwortliche Gestaltung des Lebens im vermögensrechtlichen Bereich ermöglicht werden[4]. Hieraus ergibt sich die Möglichkeit der Erweiterung des Kreises der vom verfassungsrechtlichen Eigentumsbegriff umfassten Objekte. Was als schutzwürdiges Objekt gilt, wird im Bereich der nicht „natürlich eigentumsfähigen“ Rechte maßgeblich durch den Gesetzgeber bestimmt, der eine Position erst eigentumsfähig machen muss[5]. Das Unterlassen einer Ausformung kann aber verfassungswidrig sein[6].

Unter den Begriff des Eigentums fallen alle ausschließlich dem Berechtigten zustehenden Rechte[7]. Er ist nicht auf dingliche Rechte beschränkt, sondern umfasst alle vermögenswerten Rechte, die dem Berechtigten so zugeordnet sind, dass sie von ihm eigenverantwortlich zu seinem privaten Nutzen gebraucht werden können[8]. Nicht-dingliche Rechte müssen jedoch Funktionen erfüllen, wie sie typischerweise dem Sacheigentum zukommen[9]. Des Weiteren werden Rechtspositionen geschützt, die durch eigene Leistung des Berechtigten erworben wurden[10]. Auch eine zeitlich begrenzbare oder

---

1S.o. S.157.

2Kimminich, BoKo, Art. 14, Rn. 30; Sachs-Wendt, Art. 14, Rn. 44; Dreier-Wieland, Art. 14, Rn. 38.

3BVerfGE 36, 281, 290; 83, 201, 208; Sachs-Wendt Art. 14 Rn. 9f.

4Statt Vieler: BVerfGE 24, 367, 389; 105, 252, 277; Münch/Kunig-Bryde, Art. 14 Rn. 3; Jarass/Pieroth-Jarass Art. 14 Rn. 1.

5HdbStR-Leisner, § 149 Rn. 69ff; Jarass/Pieroth-Jarass, Art. 14, Rn 7.

6HdbStR-Leisner, § 149 Rn. 69ff.

7Sachs-Wendt, Art. 14, Rn. 21.

8BVerfGE 79, 141, 191; 101, 239, 259; Kimminich BK Art. 14, Rn. 30.

9BVerfGE 89, 1, 6.

10BVerfGE 14, 288,293; 58, 81, 112 (st. Rspr.); HdbStr-Leisner, § 149 Rn. 85.

begrenzte Berechtigung führt nicht dazu, dass Rechtspositionen kein Eigentum im Sinne des Art. 14 GG darstellen können[1].

Die RIPE NCC vergibt nach ihren Bedingungen Nutzungsrechte an IP-Nummern. Letztere sind für die Inhaber – ebenso wie Telefonnummern – Eigentum im Sinne des Art. 14 GG, da insbesondere Domains dafür geeignet sind, zusammen mit den unter ihnen betriebenen Angeboten vom Inhaber eigenverantwortlich genutzt zu werden. Damit ist aber noch nichts über die Rechtsnatur der von der RIPE NCC bzw. der ICANN verwalteten IP-Nummern gesagt.

Für die Einräumung von Nutzungsrechten muss der Vergebende Rechte an diesen Ressourcen haben. Hinsichtlich der bisher ungeklärten Rechtsnatur von IP-Nummern erweist sich ein Vergleich mit den funktionell ähnlichen Rufnummern in Telefonnetz und Funkfrequenzen als aufschlussreich.

(b.) Rechtsnatur von Rufnummern

Rufnummern sind, ebenso wie IP-Nummern, künstlich erschaffene Ressourcen. Anders als Funkfrequenzen sind sie nicht natürlich vorhanden oder begrenzt, sondern können vielmehr – theoretisch auch national – beliebig vermehrt und verändert werden[2]. Sie werden, ebenso wie die unten behandelten Funkfrequenzen, durch die ITU, einer Unterorganisation der UNO, international koordiniert. Innerhalb der ihnen zugeordneten Bereiche verfügen die Staaten – mit wenigen Ausnahmen – über völlige Gestaltungsfreiheit. Auch wenn im Verhältnis des Staats zu den Nutzern kein Zwang zur Beachtung internationaler Normen besteht, entsteht doch ein faktischer Zwang zu deren Einhaltung, da andernfalls keine internationale Telekommunikation möglich wäre.

Nach Art. 14 GG ist das Eigentum wesentlich durch seine gesetzliche Ausgestaltung definiert. Rufnummern in Telefonnetzen werden in §§ 66, 67 TKG geregelt. Danach teilt die Bundesnetzagentur den Nutzern Rufnummern zu. Geschaffen wurden Rufnummern durch Festlegungen der ehemaligen Deutschen Post bzw. ihrer Vorgänger; jetziger Inhaber aller Rufnummernbestände ist nach §§ 66, 67 TKG der Staat, vertreten durch die Bundesnetzagentur. Diese erteilt zeitlich grundsätzlich nicht beschränkte Nutzungsrechte. Die Nutzer erhalten nach § 67 I TKG nur Nutzungsrechte an den Rufnummern, die allerdings nicht von dem zuweisenden Netzbetreiber abhängen; sie sind Eigentümer des Nutzungsrechts im Sinne des Art. 14 GG, da die Nummern einerseits durch das Gesetz einem Nutzer als alleinigem Verfügungsberechtigten zugewiesen und gemäß § 67 II TKG nicht ohne weiteres entziehbar sind, andererseits aber auch von dessen Eigenleistungen – beispielsweise der Bezahlung des Anschlusses bei dem Netzbetreiber, in dessen Kosten die Kosten für die Bearbeitung des Antrags auf Zuteilung der Rufnummer enthalten sind – abhängen. Damit ist aber noch nicht die Frage des Status der bei der Bundesnetzagentur

1Konsequenz aus BVerfGE 89, 1ff.

2Allerdings mit der möglichen Folge, dass sie nicht mehr international genutzt werden können.

verfügbaren freien Rufnummern geklärt. Es könnte sich bei diesen um Allmende oder um staatliches Eigentum handeln.

(aa). Rufnummern als Allmende?

Allmende in ihrem ursprünglichen Sinn steht, vereinfacht ausgedrückt, für gemeinschaftlich genutztes „Eigentum“[1] von Gemeinschaften. Dabei handelte es sich nicht um immaterielle Güter, sondern um Felder, Wiesen und Wälder und teilweise auch deren Erträge[2], also um ausnahmslos natürlich vorhandene, knappe Güter, deren Nutzung einer Regelung zum Zweck einer möglichst gerechten Verteilung unterworfen wurde: Ein Kreis von Berechtigten war zu Nutzungsbestimmung und-änderungen berufen[3]. Der Begriff der Allmende wird heute zunehmend für nicht-sächliche Ressourcen verwendet[4], auf die seine ursprüngliche, auf das Mittelalter bezogene, Definition nur noch sehr bedingt anwendbar ist. Ein alleiniges Nutzungsrecht eines Berechtigten schloss zwar schon im Mittelalter nicht die Eigenschaft als Allmende aus[5], generell aber hat die heutige Bedeutung mit dem ursprünglichen Begriff nur noch gemeinsam, dass es für eine Ressource keinen Eigentümer gibt und sie von allen Interessierten bzw. Berechtigten genutzt werden kann. Beliebig vermehrbare Ressourcen benötigen – anders als Grundstücke und ihre Früchte – in der Regel keine allzu scharfen Nutzungsregelungen, da ein Mangel bzw. die so genannte „Tragödie der Allmende[6]“ kaum auftreten kann.

Die Allmende grenzt sich von den ähnlichen öffentlichen Sachen dadurch ab, dass sie keinem Gebrauch gewidmet ist und auch grundsätzlich keinen Nutzungsbeschränkungen unterliegt[7]. Für eine Allmende im Sinne eines von der Allgemeinheit nutzbaren, durch den Staat lediglich verwalteten Gutes spricht, dass jeder zur Nutzung berechtigt ist und es keinerlei inhaltliche Einschränkungen der Nutzung gibt. Auch die Nutzungsregelungen des § 67 TKG, die einen Entzug

---

1Wie so häufig ist der heutige Begriff des Eigentums in Anwendung auf das Mittelalter nicht ganz zutreffend; ein anderer steht aber nicht zur Verfügung.

2Dies ist stark verkürzt, die Allmende unterschied sich nach Region und Zeit teilweise sehr stark. Nach dem Sachwörterbuch der Mediävistik handelt es sich um das „nach germanisch-deutschem Recht (...) gemeinschaftlich genutzte und verwaltete Gemeinschaftseigentum (Wald, Weide, Ackerland, Ödland) der Gemeindemitglieder, besonders des Grundherren und der Dorfgenossen, später auch einer Stadt. Die Nutzungen sind ausnahmslos Naturalnutzungen zum Privatgebrauch der Berechtigten. Aus einem persönlichen Allmende-Recht wurde im Lauf der Zeit ein an Haus oder Liegenschaft gebundenes dingliches Recht; Neuzugezogene waren meist von der Allmende-Nutzung ausgeschlossen. [...] Im ausgehenden Mittelalter wurde sie oft widerrechtlich vom verarmten Niederadel bzw. von der Landesherrschaft beansprucht.“

3Conrad, S.200; in bestimmtem Maße konnte dies auch der Einzelne.

4Das häufigste Schlagwort in diesem Zusammenhang dürfte die Wissens-Allmende sein, z.B. Grassmuck:http://mikro.org/Events/OS/interface5/wissens-allmende.html; http://de.wikipedia.org/wiki/Wissensalmende.

Allmende im herkömmlichen Sinn existiert in Deutschland inzwischen nicht mehr.

5Vgl.: http://de.wikipedia.org/wiki/Allmende.

6Die Tragödie der Allmende bezeichnet nach Garret Hardin (Die Tragik der Allmende, 1968) die Übernutzung der Allmende aus egoistischen Motiven, so dass die Allmende als Ganze für alle unbenutzbar wird.

7Es existieren logische Nutzungsbeschränkungen; ein Wald kann beispielsweise nicht zum Getreideanbau verwendet werden.

nach §§ 66 II, 67 I TKG nur vorsehen, wenn dies zur Umsetzung einer Umstrukturierung des Nummernraumes oder zur Umsetzung internationaler Regelungen notwendig ist oder der Inhaber die Nummer zu rechtswidrigen Zwecken gebraucht, lassen den Nummernraum als eine Allmende erscheinen. Die staatliche Aufsicht durch die Bundesnetzagentur kann als bloße Erhaltung und Überwachung der Nutzung der Allmende gelten. Die internationalen Abkommen stecken den für die Staaten verfügbaren „Allmende-Raum" ab. Die Kosten waren nach § 43 III 3 TKG a.F. nicht Nutzungskosten, sondern Bearbeitungsgebühren des Antrags auf Zuteilung einer Nummer.

(bb).Rufnummern als Eigentum des Staates

Gegen den Status der Allmende spricht in erster Linie, dass Rufnummern von der Post erschaffen wurden und dieser allein zustanden. Dieser Zustand der Ausschließlichkeit besteht weiterhin: Mit der Privatisierung der Deutschen Post ist die alleinige Verfügungsbefugnis durch das TKG auf die Bundesnetzagentur übertragen worden ist. Zwar können Allmenden auch durch den Willen der Inhaber vormaliger Eigentumsrechte entstehen, wenn diese ihr Eigentum zur allgemeinen Nutzung freigeben – dies geschieht regelmäßig bei freier Software bzw. Open Source Software –, jedoch dürfte der Fall der Rufnummern anders liegen: Das TKG zeigt, dass der Staat nach wie vor die Hoheit über die Vergabe der Rufnummern haben will und sich dementsprechend nicht aus seiner Verantwortung für die Vergabe von Rufnummern zurückzieht. Die Regelungen zum Entzug der Rufnummern zeichnen ein ähnliches Bild. Im Ergebnis ist daher die Gesamtheit der Rufnummern als Eigentum des Staates zu sehen.

(c.) Rechtsnatur von Funkfrequenzen

Funkfrequenzen sind natürlich begrenzte, nicht verbrauchbare Ressourcen, die auf Grund physikalischer Zwänge nicht von mehr als einem Sender gleichzeitig genutzt werden können[1]. Dies gilt auch für die von Mobilfunkanlagen genutzten Frequenzbereiche. Wegen dieser Eigenschaften sind bestimmte Frequenzbereiche international einheitlich bestimmten Anwendungen zugewiesen. Zentrales Dokument für die internationale Frequenzvergabe ist Art. 44 II der Konstitution der ITU. In Deutschland werden die Frequenzen innerhalb der internationalen Verwendungsdefinitionen im Rahmen der Rundfunkstaatsverträge oder anderweitig – wie beispielsweise in den Versteigerungen der UMTS-Lizenzen erfolgt – vergeben. Bestimmte Frequenzbereiche sind auch ohne Zuteilung von Nutzungsrechten für verschiedene Anwendungen[2] freigegeben.

Es herrscht die Auffassung, dass etwas so wenig Beherrschbares wie Funkwellen nicht von der Luftraumsouveränität der Staaten erfasst sei. Daher besteht das Prinzip der Sendefreiheit im

1 Mehrere Sender auf der gleichen oder einer benachbarten Frequenz, die sich in ihrem Sendebereich überschneiden, verursachen Interferenzen. Im Endeffekt wäre im Extremfall keiner der Sender empfangbar. Vgl. Kruhl, Die Versteigerung knapper Frequenzen, S. 31.

2Z.B. die Türöffnung von Autos oder Fernöffnung von Garagentoren.

Funkverkehr, das allerdings durch die Souveränität eines jeden Staates, diesen in seinem Bestand gefährdende Aktivitäten zu unterbinden, sowie durch das von der internationalen Fernmeldeunion weiterentwickelte Funkrecht beschränkt ist[1]. Demnach hat der Staat kein – wie auch immer geartetes – Eigentum an Frequenzen.

Die Vergabe von bestimmten Frequenzbereichen und die völlige Freigabe anderer Bereiche stellt indessen ein starkes Indiz für das Vorliegen einer Allmende dar. Aus der Notwendigkeit der Nutzungsregelung ergibt sich auch die staatliche Regelungsbefugnis im Falle der Frequenzen. Grundlage der internationalen Frequenzordnung ist die Vollzugsordnung für den Funkdienst (VO Funk), eine Anlage zu Art. 43 Internationaler Fernmeldevertrag. Danach kann weder von einer Form staatlichen noch privaten Eigentums ausgegangen werden; Funkfrequenzen gehören somit zum Bereich des Gemeineigentums, der Allmende. Die Vornahme von Versteigerungen der Nutzungsrechte von Frequenzbereichen läuft dieser Tatsache nicht zuwider, da sie nicht in erster Linie der Einnahmeerzielung des Staates, sondern der Sicherstellung der Vergabe an Bewerber dienen, die in der Lage dazu sein werden, die in begrenzter Anzahl vorliegenden Frequenzen im Sinne der Allgemeinheit bestmöglich zu nutzen.

(d.) Folgen für IP-Nummern

IP-Nummern sind, genauso wie Telefonnummern, künstlich geschaffene Ressourcen. Anders als bei Funkfrequenzen ist die Mehrfachnutzung einer IP-Nummer nicht störend für den rechtmäßigen Inhaber: Ein anderer hat zwar dieselbe Nummer, jedoch kann diese nicht angesprochen werden und die angeforderten Pakete finden nicht den Weg zum Empfänger, da die Nummer nicht in DNS-Tabellen eingetragen werden kann[2]. Eine Nutzung der IP-Nummer durch denjenigen, dem sie zugeteilt wurde, wird aber – anders als bei Funkfrequenzen – nicht verhindert. IP-Nummern sind, im Gegensatz zu Telefonnummern, nicht durch staatliche Institutionen entstanden und werden außerdem durch eine privatwirtschaftliche Vereinigungen, die ICANN auf der globalen Ebene und die RIPE NCC in Europa, verwaltet. Insofern handelt es sich bei IP-Nummern nicht um öffentliche Sachen; der Begriff der Allmende wird allerdings häufig auch im Zusammenhang mit IP-Nummern verwendet. Fraglich ist nun, ob es sich wirklich um Allmende oder um Privateigentum handelt.

1Eberle/Rudolf/Wasserburg-Rudolf, Kap. II, Rn. 50.

2Das Problem ist sehr theoretisch, da IP-Nummern eines bestimmten Bereichs einem Provider zugeteilt werden und dieser sie vergibt. Technisch ist sichergestellt, dass die Nummern nicht zweimal vergeben werden können; sollte jemand die Nummer fest einstellen, wäre sie nicht auf dem DNS-Server registriert und Pakete würden nicht weitergeleitet werden.

(aa.) IP-Nummern als Allmende

IP-Nummern sind von Menschen erschaffen, künstlich und prinzipiell beliebig vermehrbar, wie der Umstieg auf IPv6 zeigt. Niemand wird daran gehindert, ein alternatives IP-Nummernsystem zu erschaffen. Daher sind bereits die tatsächlichen Voraussetzungen der Allmende ebenso wenig wie die Folge, dass der Kreis der Berechtigten, nämlich die gesamte Menschheit, über die Verwendung bestimmen kann, gegeben; letztere wäre zudem höchst unzweckmäßig und nicht mit der Realität der IP-Nummernverwaltung übereinstimmend. Es wäre außerdem nicht einzusehen, wieso Telefonnummern als Eigentum und IP-Nummern als Allmende zu gelten hätten.

(bb.) IP-Nummern als Eigentum

Die Voraussetzungen für Zuweisung von IP-Nummern, die in einer Mitgliedschaft in der RIPE NCC und der Zahlung einer jährlichen Gebühr bestehen, lassen den Vergleich mit dem Besitz einer Mietwohnung zu. Um aber ebenso wie der Besitz an einer Mietwohnung eigentumsfähig im Sinne des Art. 14 GG zu sein, müssten auch IP-Nummern die Voraussetzungen von Eigentum nach Art. 14 GG erfüllen.

IP-Nummern sind Grundbedingung für eine Kommunikation jedweder Inhalte über das Internet und somit von fundamentaler Wichtigkeit für die kommunikative und wirtschaftliche Betätigung des Individuums oder von Unternehmen. Auch die Möglichkeit, sie bei Nichtzahlung oder einer Umstellung wieder zu entziehen, hindert die Eigentumsfähigkeit nicht. Somit stellen sie Eigentum im Sinne des Art. 14 GG der ICANN dar: Zugeteilte IP-Nummern stehen im Eigentum der jeweils Berechtigten.

(e.) Internationale Voraussetzungen

Wahrscheinlicher als eine auf Deutschland oder die Europäische Union beschränkte Übernahme der Verwaltung der IP-Nummern ist eine Verwaltung durch eine Internationale Organisation. Erste Vorstöße in dieser Richtung werden von Seiten der ITU unternommen[1]. Ihr Vorschlag läuft auf ein Nebeneinander der bisher bestehenden RIR[2] und der ITU hinaus, die zwar gemeinsam, aber gleichsam im Wettbewerb miteinander, den Adressraum verwalten würden[3]. Die Rolle der ITU auf nationaler Ebene würde von den Regierungen übernommen[4].

Bereits die Vorstellung zweier Wettbewerber, die neben- und miteinander eine Ressource verwalten, ist keine unkomplizierte[5]. Es kann erst recht davon ausgegangen werden, dass der Wettbewerb einer von Mitgliedsstaaten subventionierten und möglicherweise auch rechtlich unterstützten in-

1http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf.

2Regional Internet Registries, z.B. die RIPE NCC.

3http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov01.pdf.

4http://www.heise.de/newsticker/meldung/53394.

5http://www.nro.net/documents/pdf/nro17.pdf.

ternationalen Organisation mit einer rein privatwirtschaftlichen, nicht auf Gewinn ausgerichteten Organisation nur schwerlich fair verlaufen wird. Des Weiteren ist der intendierte positive Effekt der dadurch entfachten Konkurrenz unklar[1]. Voraussetzung eines derartigen Wettbewerbs wäre in jedem Fall die Übertragung eines Teils der Ressourcen an die ITU und somit – nach den derzeitigen Regelungen – von einer Zustimmung der USA abhängig.

5. Domains

Domains bilden nach Einführung des Domain Name System (DNS) die Grundlage für den enormen Aufschwung von Internet-basierten Anwendungen. Durch die Verwendung von Domain-Namen wurde es erst möglich, „über" die IP-Nummern ein anderes Adressierungsverfahren zu legen, durch das die Ressourcen mit leichter handhabbaren Zeichenfolgen, als es IP-Nummern sind, angesprochen werden.

a. Domains als Nummern

Teilweise wurde behauptet, Domains seien Nummern im Sinne des TKG, da auch sie der Adressierung in Telekommunikationsnetzen dienten. Durch die Beschreibung der Funktionsweise wird allerdings deutlich, dass nicht die Domain-Namen, sondern vielmehr die IP-Nummern für die Adressierung in der Datenkommunikation zuständig sind. Daran vermag auch die Tatsache, dass vom Anwender eigentlich nur die Domain-Namen genutzt werden, nichts zu ändern: Domain-Namen adressieren keine Datenpakete, sondern werden ausschließlich zum einmaligen Auffinden von IP-Nummern genutzt, was wiederum lediglich der Adressierung der Datenpakete dient. Daher sind Domain-Namen keine Nummern im Sinne des § 3 Nr. 13 TKG. Des Weiteren stellt § 66 I 4 TKG klar, dass die Vergabe von Domains (in der Sprache des Gesetzes: Domänen) der obersten und der nachgeordneten Stufe nicht Aufgabe der Bundesnetzagentur ist.

b. Domainvergabe als Hoheitsaufgabe

Eine Hoheitsaufgabe könnte auch die staatliche Vergabe von Domains zwingend werden lassen[2]. Letztere stellen zwar ein noch knapperes Gut dar als IP-Nummern und können wie diese beliebig vermehrt werden, nämlich durch die Einführung von SLDs[3] und neuen TLDs. Außerdem besteht für Domainnamen noch weniger die Notwendigkeit einer staatlichen Zuweisung zwecks Sicherung des Wettbewerbs, als es bei IP-Nummern der Fall ist. Einem potentiell erforderlichen Eingriff zur

1http://www.nro.net/documents/pdf/nro17.pdf.

2Vergleich oben S.158.

3Durch zweistufige SLDs, wie sie beispielsweise in Österreich und Großbritannien verwendet werden.

Verhinderung von Domain-Missbrauch kann durch Gesetzgebung und gerichtliche Kontrolle durch die ordentliche Gerichtsbarkeit genügt werden; eine Hoheitsaufgabe besteht somit nicht.

c. Kartellrechtliche Notwendigkeit?

Bei der Vergabe von Domain-Namen handelt es sich um einen wirtschaftlich relevanten Markt, auf welchem die DENIC e.G. eine beherrschende Tätigkeit ausübt[1]. Da es sich bei Domains nicht um staatliche Ressourcen handelt, käme eine kartellrechtliche Regulierung nur unter dem Gesichtspunkt der „essential facilities"-Doktrin in Frage, um den Monopolisten[2] zu zwingen, Wettbewerbern Zugang zu seinen Einrichtungen zu gewähren[3]. Die „essential facilities"-Doktrin wurde zwar für den Zugang zu Netzwerken entworfen, ist aber auch auf zentrale Infrastruktureinrichtungen wie etwa Rootserver anwendbar. Bei der Aktivität der DENIC e.G. handelt es sich genau genommen um zwei Tätigkeiten, die eine Betrachtung verdienen.

Zum einen verwaltet die DENIC e.G. den Nameserver der .de-TLD. Dies beinhaltet, dass sie bestimmt, ob Domains eingetragen werden und ob unterhalb der .de-Hierarchie eine zusätzliche Zwischenhierarchie eingeführt wird, wie es beispielsweise in Österreich, Großbritannien oder Australien der Fall ist[4]. Die DENIC e.G. handelt hierbei monopolistisch. Eine zweite, vergleichbare Institution müsste entweder gemeinschaftlich mit der DENIC e.G. den Server verwalten oder durch die ICANN anerkannt sein, damit von ihr vergebene Domains überhaupt angesprochen werden können. Allerdings ist die Verwaltung des Nameservers notwendigerweise eine nur von einem Akteur wahrzunehmende Aufgabe, da andernfalls auf dem für den Bereich der .de-TLD unentbehrlichen Server Chaos entstehen und die .de-TLD völlig zusammenbrechen könnte. Somit scheidet dieser Markt nach § 19 IV Nr. 4 GWB für eine Verpflichtung zur Zugangsgewährung zum .de-Nameserver aus. Auch ist fraglich, ob die reine Nameserver-Verwaltung als wirtschaftlich relevanter Markt zu gelten hat; angesichts der Tatsache, dass sie nur sinnvoll im Zusammenhang mit anderen Dienstleistungen wie der Registrierung von Domains erbracht werden kann, ist dies wohl eher zu verneinen. Ökonomisch bedeutungsvoll ist allerdings der der Verwaltung vorgelagerte Markt der Domainregistrierung. Auch hier ist die DENIC e.G. als Anbieter tätig. Eine wirtschaftliche und marktdominierende Tätigkeit wird auch von einer Eigenschaft als Genossenschaft und einem besonderen Förderzweck nicht ausgeschlossen[5]. Voraussetzung für die Anwendung des § 19 IV Nr. 4 GWB ist, dass der über eine zentrale Infrastruktureinrichtung herrschende Wettbewerber auch eine dominierende Stellung auf einem vor- oder nachgelagerten

1Bücking, GRUR 2002, 27, 28.

2In diesem Fall die DENIC e.G. als alleinige Registry für .de-Domains.

3 Bücking, GRUR 2002, 27, 29.

4Diese hätte dann beispielsweise das Format .com.de oder .edu.de und davor erst die eigentliche Domain (hu-berlin.edu.de).

5EuGH Slg. 1994, I-43 (S.60ff.) = NJW 1994, 2344 (Eurocontrol); EuGH Slg. 1995, I-4520 (S.4525ff.- Rn. 11ff.) – DPF; BGH NJW-RR 1986, 1298; Bücking, GRUR 2002, 27, 27.

Markt innehat und Mitbewerber benachteiligt. Eine Marktbeherrschung im Bereich der Domainvergabe wird indessen angesichts der Vielzahl anderer Anbieter auf dem deutschen Markt schwerlich anzunehmen sein. Die DENIC e.G. selbst hat über ihre eigene Registrierungsannahme einen Marktanteil von unter 1%[1]. Andere Anbieter müssen aufgrund der technischen Struktur notwendigerweise mit der DENIC e.G. zusammenarbeiten, da andernfalls die von ihnen registrierten Domains nicht aufrufbar wären. Eine Lösung nach dem Vorbild der ICANN-Reform, bei der Subdomains eingerichtet und dann von eigenständigen Registraturen verwaltet werden[2], würde lediglich zu einer Verschiebung der Problematik auf die Ebene der SLDs führen.

Der derzeitige internationale Trend geht zu einer gesteigerten Klarheit durch die Zuweisung von aufgabenspezifischen Domains wie etwa .aero, .pro oder .museum[3], nicht jedoch in Richtung der Einführung von Subdomains. Aufgrund der technischen Struktur wäre notwendigerweise jede Registry für Subdomains ebenso marktbeherrschend für ihre SLD wie derzeit die DENIC e.G. für die .de-TLD. Wettbewerb würde demnach nicht entstehen, da einem Kunden im Regelfall nur die Nutzung einer SLD möglich sein sollte. Eine Lösung für das Problem der Monopolstellung der DENIC e.G. wäre allenfalls möglich, wenn die DENIC e.G. sich von der Vergabetätigkeit zurück zöge und diese nur durch ihre Genossen erledigen ließe. Für große Kunden, welche die Dienstleistungen eines Providers nicht benötigen, wäre dies allerdings nicht effizienter, während für kleine Kunden eine Registrierung durch die DENIC e.G. derzeit und voraussichtlich auch zukünftig preislich unattraktiv ist[4].

Aus kartellrechtlicher Sicht besteht zwar ein Monopol der DENIC e.G., jedoch gebraucht sie dieses nicht zum Schaden von möglichen Konkurrenten. Eine derartige Betätigung ist auch aufgrund der Struktur der DENIC e.G. – die „Konkurrenten“ sind ihre Genossen – nicht zu befürchten. Es erscheint also weder ein staatlicher Eingriff notwendig noch die Herstellung eines staatlichen Monopols gerechtfertigt.

6. ENUM

ENUM bezeichnet ein noch in der Testphase befindliches Protokoll, mit dem Rufnummern im DNS abgebildet werden können. Dies geschieht unter der Domain e164.arpa: „.arpa“ ist eine Domain aus der Frühzeit des Internets (es hieß bis zur Abspaltung des militärischen Teils 1983 Arpanet), die nur

1LG Wiesbaden, Az.: 10 0 116/01, Urteil vom 13.6.2001, abrufbar unter: http://www.DENIC.de/media/pdf/urteile/r-e-y-LG-eV.pdf. Auch wenn die Zahlen veraltet sein mögen, dürfte die Größenordnung immer noch zutreffend sein.

2Vorschlag von Bücking, GRUR 2002, 27, 34.

3Vgl. die neuen gTLDs der ICANN. Zwar wären für den .de-Adressraum auch Alternativen möglich, jedoch sorgen die neuen TLDs, anders als prognostiziert, nicht zu einer Vermehrung verfügbarer Domains, da sich bisherige Domaininhaber häufig auch die passenden neuen Domainnamen gesichert haben.

4Die Registrierungskosten belaufen sich auf 116 € und die Pflegekosten auf 58 €/Jahr, während andere Provider nur geringe Registrierungsgebühren erheben und die Jahresgebühren sich auf ca. 12 €/Jahr beschränken.

für Versuchszwecke benutzt wird und E164 bezeichnet den Standard der ITU, nach dem Telefonnummern vergeben werden. Die Verwaltung der Domain „e164.arpa“ wurde der ITU übergeben, welche wiederum die länderspezifischen Subdomains an verschiedene Organisationen in den am Feldversuch teilnehmenden Staaten delegiert hat. In Deutschland ist dies die für die Domainvergabe zuständige DENIC e.G.

Eine ENUM für die fiktive (internationale) Telefonnummer 0049 30 12345678 sähe folgendermaßen aus: 8.7.6.5.4.3.2.1.0.3.9.4.e164.arpa. Sie würde also die Telefonnummer in umgekehrter Reihenfolge beinhalten. Während der „Rang“ bei Telefonnummern nach hinten hin sinkt, steigt er bei Domains.

Allein aus der Tatsache, dass derartige Domains noch schwerer zu handhaben sind als IP-Nummern, wird ersichtlich, dass der mit dem ENUM-Standard verfolgte Zweck nicht darin besteht, solche Seiten über das Internet aufrufbar zu machen. Vielmehr zielt dieser Standard auf eine Vereinheitlichung der Kommunikation ab. Über die Einträge unter einer ENUM-Domain soll es allerdings möglich werden, eine Person über die ihr zugeordnete ENUM mit allen netzbasierten Kommunikationsmitteln zu erreichen. Ein denkbares Anwendungsbeispiel bestünde darin, dass eine Person angerufen wird, die nicht erreichbar ist: Der Anruf würde automatisch auf ein Mobiltelefon weitergeleitet. Wenn auch dieses nicht verfügbar ist, kann eine Sprachnachricht auf die E-Mailbox geschickt werden, ebenso wäre ein Hinweis per E-Mail denkbar. Die Einrichtung entsprechender Domains wäre heutzutage bereits möglich, jedoch könnte der weitergehende Nutzwert der Weiterschaltung nicht erreicht werden.

Aus dem zuvor zu Domains Gesagten wird deutlich, dass ENUMs als Domains nicht unter die Zuständigkeit der Bundesnetzagentur fallen können; dennoch verzögerte sich der Feldversuch, da die Bundesnetzagentur der Meinung war, es handele sich um Nummern im Sinne des TKG und deren Zuweisung sei ihre Aufgabe und nicht die der DENIC e.G. Dieser Meinung dürfte aber durch den neuen § 66 I 4 TKG endgültig der Boden entzogen sein.

7. Zusammenfassung

Aus der bisherigen Rechtslage ergibt sich, dass im Bereich der Ressourcenverwaltung derzeit keine staatliche Aufgabe vorliegt. Eine solche könnte sich lediglich durch eher unwahrscheinliche Entwicklungen oder durch ein Eingreifen des Gesetzgebers ergeben; letzterem stehen allerdings verschiedene Bedenken entgegen. Außerdem bestehen bei der derzeitigen Struktur der Ressourcenverwaltung auch verfassungsrechtlich keine Bedenken gegen eine rein private Aufgabenerfüllung.

II. Standards

Die Standards des Internets werden durch private Organisationen definiert. Dies stellt keine Besonderheit dar: Standards wurden auch schon vor der Zeit des Internets selten durch staatliche Akte festgesetzt.

Die bekannteste deutsche Standardisierungsorganisation, der DIN e.V. und sein Vorgänger, der 1917 gegründete Normenausschuss der deutschen Industrie (NADI), sind seit ihrer Gründung rein privatrechtliche Vereinigungen, deren Mitglieder vorwiegend aus Wirtschaftsunternehmen bestehen. Daneben existieren weitere, ebenfalls privatrechtlich organisierte Normungsorganisationen[1]. Die Tätigkeit des DIN e.V. wurde 1975 in einem Vertrag mit der Bundesrepublik Deutschland anerkannt, in welchem der DIN e.V. sich verpflichtet, das öffentliche Interesse zu berücksichtigen, die betroffenen hoheitlichen Stellen zu beteiligen sowie staatliche Normungsanträge bevorzugt zu behandeln. Die Bundesrepublik verpflichtet sich hingegen, keine Normen zu erlassen, die denjenigen des DIN e.V. entsprechen, sowie bei der Normsetzung auf DIN-Normen Bezug zu nehmen[2].

Im Bereich des Informationsrechts befassen sich auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und die Initiative Digitaler Rundfunk (IDR) der Bundesregierung mit nationalen und internationalen Normen. Sie setzen allerdings keine solchen fest, sondern nutzen bereits bestehende bei ihren Aufgaben[3]. Die EU bedient sich bei der Formulierung von Rechtstexten der anerkannten Normungsinstitutionen und beschränkt sich auf die Formulierung grundlegender Anforderungen[4]. Auch die europäischen Normungsinstitutionen sind privatrechtlich organisiert, wobei sich ihre Mitglieder zumeist aus den nationalen Normungsorganisationen zusammensetzen. Auch die international tätige ISO und die 1906 gegründete International Electrotechnical Commission (IEC) sind privatwirtschaftliche Vereinigungen, deren Rolle durch die WTO anerkannt ist[5]. Dies soll die gleichmäßige Umsetzung der Normen zwecks Verringerung von Handelshindernissen gewährleisten.

1. Standardisierung im Internet

Es haben sich in relativ kurzer Zeit verschiedene Organisationen herausgebildet, die sich spezifisch mit der Entwicklung von Standards für den Bereich der Kommunikation im Internet befassen. Diese

1Z.B. VDE (Verband der Elektroindustrie), DKE (Deutsche Elektrotechnische Kommission), NI (Normenausschuss Informationstechnik).

2Kloepfer, § 4 Rn. 100.

3Vertrag zwischen der Bundesrepublik Deutschland vom 5.6.1975 (Beilage zum Bundesanzeiger Nr. 114 vom 27.6.1975).

4Kloepfer, § 4 Rn. 104.

5Kloepfer, § 4 Rn. 128.

Organisationen, die anfänglich ohne eine Struktur bestanden, waren notwendig, um die Bemühungen des Aufbaus des Internets zu koordinieren.

a. ISOC

Die für die Standardisierung wichtigste Organisation ist die 1992 gegründete Internet Society (ISOC), unter deren Dach Gruppen wie das Internet Architecture Board (IAB) sowie die Internet Engineering Task Force (IETF) tätig sind. Deren informelle Vorläufer, wie auch die Network Working Group (NWG), reichen ebenso wie der Standardisierungsprozess, bis in die ersten Tage des Internets zurück.

Die ISOC wurde 1992 gegründet, um den Aktivitäten des älteren IAB und der IETF einen rechtlichen Rahmen zu geben, diese vor eventueller Haftung zu schützen[1] und um eine Dachorganisation für die verschiedenen technischen Gremien zu schaffen; letzteres Ziel scheiterte zunächst an Widerständen vor allem von Seiten der IETF[2].

Die ISOC nimmt auch Aufgaben der Fortbildung für Unternehmen und Staaten, insbesondere Entwicklungsstaaten, wahr[3]. Sie ist die einzige Organisation mit formeller, indes kostenloser, Mitgliedschaft[4]. Ihre Leitung wird von einem Präsidenten übernommen, der von einem Vorstand gewählt wird, welcher wiederum von einem so genannten Board of Trustees, einer Vertretung der Mitglieder, bestimmt wird. Die Beteiligung im Board of Trustees ist auf drei Jahre befristet, wobei eine Wiederwahl möglich ist[5]. Der Präsident ist kraft seines Amtes nicht stimmberechtigtes Mitglied[6]. Die Mitglieder sollen eine Anzahl von 20 Personen nicht überschreiten sowie Repräsentanten der Industrie, Bildungseinrichtungen, Non-Profit Organisationen und Regierungen umfassen[7].

Obwohl die ISOC formell die beherrschende Organisation und das Dach der nachfolgend zu erläuternden Institutionen ist, stellt die IETF die mit Abstand wichtigste und einflussreichste Organisation dar.

(1.) IETF

Die IETF entstand in der Anfangszeit des ARPANET aus der NWG und wurde unter ihrem jetzigen Namen 1986 gegründet. Sie ist für die Erarbeitung von Standards und deren technische Umsetzung zuständig und erfüllt außerdem, hauptsächlich im Bereich der Ernennung von Mitgliedern in anderen Gruppen, weitere wichtige Funktionen. Die Arbeit geschieht in Working Groups (WG), die

1Leib, S.119.

2Leib, S.121.

3http://www.isoc.org/isoc/mission/.

4http://www.isoc.org/members/indiv_app.php.

5ISOC By-Laws Art. II Section 2, abrufbar unter: http://www.isoc.org/isoc/general/trustees/bylaws.shtml.

6ISOC By-Laws Art. II Section 2.

7ISOC By-Laws Art. II Section 2.

sich nach den anstehenden Aufgaben zusammenfinden und sich über öffentlich zugängliche Mailinglisten koordinieren.

(a.) Mitglieder

Die IETF kennt keine formelle Mitgliedschaft. Sie ist offen für alle Interessierten. Für eine „Mitgliedschaft“ genügt es, eine oder mehrere der offiziellen Mailinglisten zu abonnieren, über die auch die Tätigkeiten der Working Groups koordiniert werden[1].

(b.) Struktur

Jede Working Group gehört zu einer Area, die von einem vom IAB eingesetzten Director geleitet und in der IESG vertreten wird[2]. Der Vorsitzende der IETF wird vom IAB auf Vorschlag des Nomination Commitee der IETF ernannt[3].

(c.) Mitwirkung

Die IETF wirkt maßgeblich bei der Besetzung des IAB, der IESG und über diese auch der ISOC mit. Der Vorsitzende der IETF ist zugleich Vertreter der IETF im IAB und Vorsitzender der IESG[4]. Das Nomination Commitee (NomCom) der IETF wählt die Kandidaten für das IAB und die IESG aus, deren Plätze frei werden oder für die eine Revision der Besetzung des Postens vorgeschlagen wurde[5]. Die Benennung der Posten erfolgt durch den Vorsitzenden der IETF[6]. Des Weiteren schlägt das NomCom dem IAB den Kandidaten für den Vorsitz der IETF vor. Die Kandidaten für die IESG werden vom IAB aus den Vorschlägen des NomCom ausgewählt. Die Kandidaten für die Posten im IAB werden vom Board of Trustees ausgewählt[7].

Das NomCom setzt sich aus zehn Freiwilligen, einem nicht stimmberechtigten Vorsitzenden und drei nicht stimmberechtigten Verbindungsleuten zusammen[8]. Die Freiwilligen werden per Zufallsprinzip aus dem Pool der gemeldeten Kandidaten ausgewählt und müssen wenigstens zwei der letzten drei Meetings der IETF besucht haben[9]. Dadurch soll einerseits sichergestellt werden, dass die Freiwilligen genügend Einblick in die Tätigkeit der IETF und der Kandidaten haben, und

1http://www.ietf.org/join.html.

2http://www.ietf.org/overview.html.

3http://www.iab.org/about/overview.html.

4RfC 2850.

5RfC 2727.

6RfC 2727.

7RfC 2727.

8RfC 2727.

9RfC 2727.

andererseits eine die Offenheit der IETF respektierende demokratische Auswahl unter den Kandidaten ermöglicht werden.

(d.) Standardisierungsprozess

Der Standardisierungsprozess (Standards Track) ist darauf ausgerichtet, von allen Beteiligten tragbare und dabei funktionsfähige Ergebnisse zu erzielen. Das Ergebnis heißt weiterhin Request for Comments (RfC), wenn es als Standard beschlossen wird. Der Standards Track wird in RfC 2026 beschrieben. Das Ergebnis wird darin als stabile, in mehreren Anwendungen erprobte Spezifikation beschrieben, die bedeutende öffentliche Unterstützung genießt und zumindest in einigen Teilen des Internets nützlich ist[1]. Diese Kriterien müssen nicht zwangsweise erfüllt werden, wie Standards wie beispielsweise das Carrier Pigeon Internet Protocol (CPIP)[2] beweisen; dessen Anwendbarkeit wurde allerdings in einem Versuch bestätigt[3].

(aa.) RfC

Die Standards des Internets heißen RfC. In dieser elektronischen Publikationsserie sind sowohl die gesamte technische Dokumentation der Standards des Internets als auch die Beschreibungen von Abläufen und Satzungen der Organisationen enthalten. Der für einen Standard ungewöhnliche Name stammt aus der Frühzeit des ARPANET, als die Entwickler Doktoranden waren, die weder über Autorität verfügten noch jemandem etwas aufzwingen wollten, aber eine Form der Publikation ihrer Vorschläge finden mussten, die einerseits eine Diskussionsgrundlage darstellte und durch die sich andererseits niemand verletzt fühlte. Ihre Aufgaben sind bis heute nicht von anderen Personen übernommen wurden. Ebenso wie die Pioniere des Internets immer noch wichtige Positionen innehaben, sind Name und Verfahren der Standardisierung erhalten geblieben.

Es gibt drei verschiedene Gruppen endgültiger RfCs: Internet Standards Track RfCs, Best Current Practice (BCP) und RfCs mit dem Status „Experimental“ und „Informational“. Des Weiteren können Dokumente als Internet Drafts zur Diskussion gestellt werden.

(aaa.) Standards Track

Standards Track RfCs bezeichnen von der IESG beschlossene Standards. Sie werden in eine Serie mit eigener Zählung (STD) aufgenommen, behalten aber ihre Nummer als RfC. Standards Track RfCs müssen als ASCII Dokumente verfügbar sein. Eine zusätzliche Veröffentlichung in anderen Formaten ist möglich, stellt aber keine gültige Version dar[4].

1RfC 2026.

2RfC 1149. Es handelt sich hier um die nicht besonders innovative Möglichkeit, Datenpakete auszudrucken und mittels Brieftauben zu transportieren. Der RfC ist zwar durchaus lesenswert, jedoch nie als Internet Standard verabschiedet worden.

3http://www.pro-linux.de/news/2001/3007.html.

4RfC 2026.

Ein Vorschlag wird zunächst als Proposed Standard von der IETF veröffentlicht und in ihren Mailinglisten diskutiert, wobei versucht wird, ihn zu implementieren und in Anwendungen zu nutzen. Wenn die Überzeugung vorliegt, dass ein Draft Standard einen hinreichenden Grad an technischer Reife erreicht hat und von signifikantem Nutzen sein wird, wird er als Internet Standard (STD) beschlossen und erhält eine entsprechende Nummer.

(bbb.) Non Standards Track

Als Non Standards Tracks werden RfCs bezeichnet, die nicht als Internet Standards bestimmt sind oder deren Technik entweder überholt oder nicht weit genug fortgeschritten ist, um als solche vorgeschlagen zu werden. RfCs werden als „Experimental“, „Informational“ oder „Historic“ eingeordnet: „Experimental“ kennzeichnet RfCs, die Ergebnis einer Forschung sind und zur Information Anderer veröffentlicht werden. „Informational“ beschreibt RfCs, die für die Kenntnisnahme einer breiteren Öffentlichkeit bestimmt sind, aber weder einen Konsens noch eine Empfehlung darstellen; sie werden typischerweise von Working Groups konzipiert, können bei Erlaubnis des RfC-Editors aber auch von Einzelpersonen erstellt werden. Als „Historic“ gekennzeichnete RfCs gelten als überholt.

(ccc.) Best Current Practice (BCP)

Es können nicht nur technische Dokumentationen, sondern auch andere Dokumente als RfC publiziert werden. Für diese existiert eine Unterkategorie namens BCP, welche die Standardisierung von Vorgehensweisen beschreibt. Als Beispiel kann hier RfC 2026 angeführt werden, der die Erstellung von RfCs zum Thema hat. Auch diese müssen einem Konsens entspringen; für dessen Erzielung hat sich die Erstellung von RfCs als geeignet erwiesen. Der Weg eines BCP vom Vorschlag zur Verabschiedung ist allerdings deutlich kürzer als derjenige eines RfCs zum Standards Track.

(bb.) Verfahrenseinleitung

Gemäß des offenen Verständnisses darf jeder einen Internet Draft schreiben und veröffentlichen. Der Antrag auf Aufnahme in den Standards Track muss von der zuständigen IETF Working Group an die IESG gestellt werden. Die von einer Frist begrenzte Zeitspanne vor der Entscheidung kann von Interessenten genutzt werden, um den Draft kritisch zu überprüfen. Vor einer Aufnahme in den Standards Track versendet die IESG eine „Last Call“-Mai, welche die Ankündigung der Entscheidung enthält.

(cc.) Verfahren im Standards Track

Nach einer erfolgten Entscheidung über die Aufnahme in den Standards Track wird der RfC-Editor diesbezüglich in Kenntnis gesetzt und der Internet Draft in die Kategorie der Proposed Standards eingeordnet. Der Proposed Standard erhält eine Nummer als RfC. Wenn er sich bewährt und implementiert ist, entscheidet die IESG über einen Status als Draft Standard. Eine Überprüfung erfolgt – allerdings in jeweils unterschiedlichen Zeiträumen – auf jeder einzelnen Stufe. Wenn ein bereits beschlossener Standard durch die technische Entwicklung überholt wird, kennzeichnet ihn die IESG als „Historic".

(dd.) Verfahren für BCPs

Der dreigeteilte Standardisierungsprozess für technische Standards ist für BCPs zu langwierig und zu kompliziert, zumal auf den verschiedenen Stufen keine substantiellen Neuerungen und Erkenntnisse hinzukommen können. Daher ähnelt die Prozedur derjenigen für Proposed Standards, wird aber nach der ersten Stufe beendet und der RfC behält zwar seine Nummer, wird allerdings als BCP bekannt gegeben.

(ee.) Konfliktlösung

Beim Auftreten von Konflikten während des Standardisierungsprozesses in der IETF ist eine Lösung durch den Vorsitzenden der Working Group vorgesehen, die einen Konsens beinhalten muss. Sollte diese Vorgabe nicht erfüllt werden können, wird der Fall an den zuständigen Area Director übertragen. Ist auch hier keine Konfliktlösung möglich, wird diese vor der IESG und in letzter Instanz vor dem IAB zu erreichen versucht.

Jede der involvierten Parteien kann bei einer ihrer Meinung nach ungenügenden Lösung den Schritt vor die nächsthöhere Instanz gehen. Eine Befassung ordentlicher Gerichte ist nicht vorgesehen und eine Verletzung subjektiver Rechte kaum wahrscheinlich.

(e.) Normen und der Staat

Fast alle Normen sind von privaten Organisationen gesetzt und sofern ihre Geltung weder vertraglich vereinbart noch gesetzlich festgelegt ist, liegt zunächst keine rechtliche Bindungswirkung vor.

Allerdings zeitigt ihr Bestehen eine gewisse Indizwirkung[1] oder stellt eine Orientierungshilfe dar[2]. Es besteht zudem ein Vertrag zwischen dem DIN e.V. und dem deutschen Staat[3], nach dem sich der Staat verpflichtet, DIN-Normen, soweit möglich, immer anzuwenden und keine eigenen DIN-Normen entsprechenden Regelungen zu entwickeln. Eine derartige Anerkennung ist bei den Standards der IETF allerdings nicht gegeben. Das OLG Dresden weist zwar darauf hin, dass die Standards des

1BVerwGE 79, 254, 264.

2BVerwGE 77, 285, 291.

3Vom 5.6.1975 (Beilage zum Bundesanzeiger Nr. 114 vom 27.6.1975).

IETF keine rechtliche, sondern nur eine faktische Bindungswirkung hätten und bleibt somit auf der allgemeinen Linie der Rechtsprechung, zitiert aber gleichwohl RfC 1591[1] und weist auf die grundsätzliche Billigung des (auf RfC 1591 beruhenden) Verfahrens der DENIC e.G. durch die Bundesregierung hin. Damit wird faktisch die Regelung des RfC 1591 in deutsches Recht übernommen, obwohl ein dem DIN-Vertrag entsprechendes Abkommen nicht einmal ansatzweise existiert.

b. IESG

Die Internet Engineering Steering Group (IESG) besteht aus den Area Directors der IETF sowie einem von der IETF vorgeschlagenen und dem IAB bestätigten Chair. Ihre wichtigste Aufgabe stellt die Beschlussfassung über die Annahme eines RfC als Standard dar. Des Weiteren ist sie höchste Schlichtungsstelle im Konfliktlösungsmechanismus der IETF.

IAB

Das Internet Architecture Board (IAB), unter dessen Dach verschiedene Gremien tätig sind, hat formell die höchste Stellung im Standardisierungsprozess inne; allerdings wird es durch seine Zusammensetzung und die Kandidatenauswahl maßgeblich von der IETF beeinflusst. Es nimmt eine wichtige Rolle in der Besetzung der IESG, des Vorsitzenden der IETF, der Internet Research Task Force (IRTF) und der Internet Research Steering Group (IRSG) ein. Wichtiger noch sind seine Aufgaben in Form der Überwachung des Standardisierungsprozesses und der IANA sowie der Sammlung der RfCs, die von der IANA an eine als RfC-Editor handelnde Organisation delegiert wird[2].

Außerdem übernimmt es die Vertretung der oben genannten Institutionen in der ISOC und gegenüber anderen Organisationen[3].

Das IAB besteht aus zwölf, vom Board of Trustees aus den vom NomCom vorgeschlagenen Kandidaten ausgewählten, Mitgliedern und dem Vorsitzenden der IETF; zusätzlich entsenden der RfC-Editor, die IANA sowie die IESG und IRSG beratende Mitglieder[4].

1OLG Dresden, Urteil vom 28.11.2000, 14 U 2486/00 – kurt-biedenkopf.de (abrufbar unter http://www.jurpc.de/rechtspr/20010098.htm).

2RfC 2727, bis zu seinem Tod 1998 war Jon Postel alleiniger RfC-Editor.

3http://www.iab.org/liaisons/index.html.

4RfC 2727.

d. IANA / ICANN

Die Bezeichnung „Internet Assigned Number Authority“ (IANA) steht nicht für eine Organisation mit einer bestimmten Struktur, sondern für eine bestimmte Aufgabe[1]. Die diese Aufgabe wahrnehmende Organisation verwaltet unter anderem IP-Nummern und das DNS. Vor der Übernahme durch die ICANN 1998 war die IANA ein rechtlich nicht fassbares Forschungsvorhaben[2], dem die Verwaltung der Ressourcen durch einen Vertrag mit der National Science Foundation (NSF), die den Betrieb der Infrastruktur des Internets bis Mitte der 90er Jahre finanzierte, übertragen worden war. Die IANA ist Teil und Herzstück der ICANN; die Registrierung von gTLDs wurde an verschiedene Unternehmen delegiert[3]. Der Root-A-Server wird im Auftrag der ICANN von VeriSign Inc. betrieben.

Die Funktion als IANA wurde der ICANN vom US-Handelsministerium 1998 durch ein Bündel von Verträgen[4] für zunächst drei Jahre übertragen, 2003 erfolgte eine bis 2006 geltende Erneuerung. Nach der ursprünglichen Planung sollte der Vertrag 2006 endgültig auslaufen und die ICANN organisatorisch eigenständig werden, allerdings wurde er stattdessen nochmals – um bislang unbekannte Zeit – verlängert[5].

Die Verwaltung der für Infrastrukturaufgaben vorgesehenen „.arpa“-Domain erfolgt durch die IANA in Kooperation mit der IETF, während die Verantwortung für die restlichen TLDs bei privatwirtschaftlichen Unternehmen liegt: Die Verwaltung der ccTLDs wurde von der IANA/ICANN an nationale Organisationen wie die DENIC e.G. in Deutschland übertragen. Die Vergabe von IP-Nummern wurde an vier regionale Gesellschaften (Regional Internet Registry, RIR) für Europa und Nordafrika (RIPE NCC), Asien und den Pazifikraum (APNIC), Südamerika und die Karibik (LACNIC) sowie Nordamerika und südliches Afrika (ARIN) delegiert[6].

(1.) Struktur

An der Spitze der ICANN steht das Board of Directors[7], derzeit unter dem Vorsitz von Vinton G. Cerf, Gründungspräsident der ISOC und Mitglied der Gruppe, die Ende der 60er Jahre das ARPANET entwickelte.

Präsident der ICANN ist seit dem 27.03.2003 Paul Twomey.

1http://www.icann.org/general/.

2Leib, S.137.

3http://www.iana.org/gtld/gtld.htm.

4Zu den Vertragsbeziehungen: Leib, S.89ff.

5http://www.icann.org/announcements/announcement-29sep06.htm.

6http://www.iana.org/ipaddress/ip-addresses.htm.

7ICANN Bylaws Art. II Section 1.

Nach Art. VI Section 7 der ICANN – Bylaws sollen die Direktoren im besten Interesse der ICANN handeln und sind dabei nur ihrem Gewissen unterworfen; auch sollen sie die verschiedenen in Art. VI Section 6 der ICANN – Bylaws aufgezählten geografischen Regionen repräsentieren.

Nach einer einmaligen öffentlichen Wahl im Oktober 2000 wurden die Bylaws geändert[1], so dass die Direktoren jetzt durch das Nomination Commitee der ICANN ausgewählt werden[2]. Im Board sind außerdem Vertreter verschiedener Organisationen als nicht stimmberechtigte „Liaison" vertreten. Daneben existieren das Governmental Advisory Commitee (GAC), das Stability and Security Advisory Commitee (SAC), das Root Server System Advisory Commitee (RSSAC) und das At-Large Advisory Commitee (ALAC). Das GAC ist offen für alle Regierungen und internationalen Organisationen auf Einladung durch den Vorsitzenden. Es soll das Board bei Entscheidungen beraten, die das öffentliche Interesse, Gesetze oder internationale Verträge berühren[3]. Das ALAC wurde erst nach Abberufung der At-Large Direktoren im Oktober 2002 geschaffen[4]; seine Aufgabe besteht in der Beratung bei Entscheidungen, die den einzelnen Internetnutzer berühren[5]. Sowohl das SAC als auch das RSSAC haben beratende Funktion bei der Durchführung der technischen Aufgaben der ICANN. Nach Art. XI Section 1 der Bylaws kann das Board nach Bedarf zusätzliche Advisory Commitees einberufen.

(2.) Vorgehen

Die ICANN ist kein Standardisierungsgremium. Sie hat zwar durch die direkte Kontrolle über das Root Server System und die indirekte Kontrolle über die IP-Nummern erheblichen Einfluss auf technische Standards, jedoch korrespondiert dieser Einfluss nicht mit demokratischen Kontrollmöglichkeiten, wie es bei der IETF der Fall ist.

Das Vorgehen der ICANN soll „to the maximum extent feasible" transparent sein[6]. Dies wird unter anderem dadurch erreicht, dass die Direktoren nicht zum Schweigen verpflichtet sind und Protokolle sowie Materialien von Meetings auf der Website der ICANN veröffentlicht werden[7].

1http://www.wired.com/news/politics/0,1283,56122,00.html.

2ICANN Bylaws Art. VII Section 1. Abrufbar unter: http://www.icann.org/general/bylaws.htm#VII.

3ICANN Bylaws Art. XI Section 2.

4http://www.icann.org/committees/alac/.

5ICANN Bylaws Art. XI Section 4.

6ICANN Bylaws Art. III Section 1.

7http://www.icann.org/minutes/.

(3.) Kritik

Die Kritik an der ICANN richtet sich einerseits gegen ihr demokratisch nicht überwachtes Monopol auf die Kontrolle des DNS, andererseits gegen ihren starken amerikanischen Einfluss[1]. Des Weiteren wird die Verlängerung des Vertrages zwischen der ICANN und dem DoC bis zum Oktober 2006, die ohne Ausschreibung erfolgte, beanstandet. Einige Kritiker fordern eine Übertragung der Funktionen der IANA auf die ITU, um diese wichtige Ressourcen unter internationale Kontrolle zu stellen[2]. Eine solche Überwachung wäre aber nur unter Mitwirkung der Netzwerkbetreiber oder der ICANN umsetzbar; andernfalls könnte die Möglichkeit bestehen, dass ein konkurrierendes DNS keinerlei Funktion wahrnimmt oder zwei miteinander konkurrierende, untereinander inkompatible Systeme entstehen.

(4.) Reform der Internetverwaltung

Die (behauptete) Macht der ICANN und die schon seit längerem bekannten Kritikpunkte bieten immer wieder Anlass für Reformbestrebungen. Dabei wird zum einen eine stärkere Beteiligung der Nutzer gefordert, so dass die ICANN nicht nur von Vertretern der Industrie besetzt wird, zum anderen besteht angesichts der wichtigen Rolle der USA ein Bedürfnis nach stärkerer Beteiligungsmöglichkeit von Seiten anderer Staaten. Beide Anliegen haben in der vergleichsweise kurzen Zeitspanne seit Gründung der ICANN bereits zu Reaktionen verschiedenster Art geführt.

(a.) Stärkere Nutzerbeteiligung

Im Zuge der ersten Reform der ICANN wurden im Oktober 2000 fünf zusätzliche Posten im Board of Directors eingeführt; es handelte sich um so genannte At-Large Direktoren, die von den Nutzern bestimmt werden konnten. Die Registrierungsserver für die Wahl brachen mehrmals wegen zu vieler Anfragen zusammen, die Arbeit der At-large-Direktoren hingegen fand scheinbar weniger Anklang: Diese mussten ihre Ämter bereits im Rahmen der nächsten Reform im Dezember 2002 wieder aufgeben. Als Grund wurde unter anderem genannt, dass die Fairness und Kontrollierbarkeit bei Online-Wahlen kaum zu gewährleisten seien. Soweit ersichtlich, ist allerdings kein Vorwurf der Wahlfälschung erhoben worden; dementsprechend kann es sich lediglich um partiell unfaire beziehungsweise unkontrollierbare Wahlen gehandelt haben, die für eine demokratische Kontrolle immer noch besser geeignet scheinen als gar keine Beteiligung. An die Stelle der at-Large-Direktoren trat das at-Large Advisory Commitee (ALAC).

(b.) Stärkere Regierungsbeteiligung

Die Forderung nach einer stärkeren Regierungsbeteiligung hat, im Gegensatz zu jener nach einer ausgeprägteren Nutzerbeteiligung, erst vor relativ kurzer Zeit an Ausdruck gewonnen. In einem

1Z.B.: http://www.heise.de/newsticker/meldung/85281.

2http://www.heise.de/newsticker/meldung/28643.

ersten Schritt wurde durch die ICANN Reform des Jahres 2002 das Government Advisory Commitee eingeführt. Eine neuerliche Diskussion entstand im Vorfeld des ersten World Summit on Information Society (WSIS I) im September 2003 in Genf. Da die dort vertretenen Regierungen weder untereinander noch mit den Vertretern der Zivilgesellschaft zu einer Einigung kamen, wurde das Thema auf den im November 2005 in Tunis stattfindenden Folgekongress WSIS II vertagt. Zur Vorbereitung des Themas wurde die Working Group on Internet Governance (WGIG) gegründet. Der Vorbereitungsprozess begann im Juni 2004 und die ersten Stellungnahmen von Staaten zeigen – sofern sie überhaupt inhaltlicher und nicht nur prozeduraler Natur sind – divergierende Auffassungen[1]. Die USA setzen auf ein weiterhin hauptsächlich von Privaten organisiertes und verwaltetes Internet [2], während Norwegen für eine stärkere internationale Beteiligung plädiert[3], Japans Standpunkt die Mitte zwischen diesen beiden Positionen einnimmt[4] und andere Staaten, insbesondere Entwicklungsländer, eine Kontrolle durch eine internationale Organisation fordern. Des Weiteren liegen diverse weitere Stellungnahmen[5] der „Zivilgesellschaft“ vor, die insgesamt eine stärkere eigene Beteiligung und eine schwächere der Staaten fordern, wobei auch hier Unterschiede feststellbar sind. Einig scheinen sich alle Beteiligten dahingehend zu sein, dass eine Reform der ICANN relativ viel Zeit in Anspruch nehmen wird.

Der WSIS II-Kongress im November 2005 in Tunis führte den stark divergierenden Stellungnahmen entsprechend zu einem Kompromiss: Kurzfristig wird die ICANN in der bisherigen Form ihre Aufgaben behalten und nicht an die ITU oder andere Organisationen abgeben[6], langfristig aber soll nach den Art. 68-74 des Abschlussdokuments eine stärkere Regierungsbeteiligung auf gleichberechtigter Basis erfolgen[7], wobei die Zeitspanne bis zum Erreichen dieses Ziels nicht absehbar ist[8].

(5.) Konfliktlösung bei Domainstreitigkeiten

Die Zuteilung von Domains stellt eines der streitträchtigsten Gebiete überhaupt dar. Die nationale und internationale Rechtsprechung ist kaum mehr zu überblicken. Dies resultiert daraus, dass Markenrechtsinhaber von bekannten Marken auch die auf die Marke passende Domain besitzen

1Mitte Dezember lagen Stellungnahmen von vier Staaten (Kanada, Japan, Norwegen, USA) vor. Abrufbar sind diese unter: http://www.itu.int/wsis/preparatory2/wgig/.

2Stellungnahme der USA, abrufbar unter: http://www.itu.int/wsis/preparatory2/wgig/.

3Stellungnahme Norwegens, abrufbar unter: http://www.itu.int/wsis/preparatory2/wgig/.

4Stellungnahme Japans, abrufbar unter: http://www.itu.int/wsis/preparatory2/wgig/.

5Abrufbar unter: http://www.itu.int/wsis/preparatory2/wgig/.

6Kleinwächter, http://www.heise.de/tp/r4/artikel/21/21418/1.html.

7Tunis Agenda for the Information Society, abrufbar unter: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

8Kleinwächter, http://www.heise.de/tp/r4/artikel/21/21418/1.html.

möchten. Die Zuteilung von Domains richtet sich jedoch ausschließlich nach dem Zeitpunkt der Anmeldung und nicht danach, ob Rechte an dem Domainnamen bestehen oder ob durch die Zuteilung Rechte beeinträchtigt werden. In diesem Kontext hat sich das so genannte Domaingrabbing entwickelt: Privatpersonen ließen Domains auf sich eintragen, um diese später möglichst gewinnbringend an zahlungskräftige Unternehmen zu verkaufen. Derartige Fälle treten allerdings mittlerweile kaum noch auf.

Neben dieser allseits bekannten, unlauteren Vorgehensweise sorgen „normale" Namensstreitigkeiten und vermehrt auch das so genannte „Reverse Domain Hijacking", bei welchem Namensinhaber versuchen, Domains von Anderen zu erlangen, auch wenn diese gleichfalls berechtigte Nutzer sind und Eigeninteresse an der Domain haben, für Probleme.

Eine Lösung dieser Konflikte ist durch ordentliche Gerichte möglich, wobei deren Entscheidungen häufig durch Unklarheiten hinsichtlich des anwendbaren Recht verzögert werden. Daher hat die ICANN die Uniform Domain-Name Dispute Resolution Policy (UDRP) eingeführt, die ein Schiedsgerichtsverfahren durch unabhängige Schiedsstellen, unter anderem die World Intellectual Property Organisation (WIPO), vorsieht.

In einigen Staaten wird diese Maßnahme auch für ccTLDs angewandt. Die DENIC e.G. hat ihre Anwendung jedoch nicht beschlossen, sodass die UDRP im Bereich der .de-TLD keine Gültigkeit hat. Die Registries für sTLDs haben teilweise ergänzende Konfliktlösungsregelungen verabschiedet.

(a.) Deutsche Rechtsprechung

Nach einem anfänglichen Streit[1] ist mittlerweile in der deutschen Rechtsprechung und Literatur anerkannt[2], dass Domains den Schutz des Kennzeichenrechts genießen können[3]. So genannte generische Domains, die bloße Gattungsbegriffe darstellen, sind hiervon allerdings ausgenommen[4].

Bei den auftretenden Domainstreitigkeiten sind zwei Grundfälle erkennbar: Zum einen versuchen Markeninhaber, zu ihrer Marke passende Domains zu registrieren, zum anderen möchten Domaininhaber verhindern, dass verwechslungsfähige Domains betrieben werden.

Grundsätzlich gilt bei internationalen Kollisionen, dass der Inhaber eines national geschützten Namens oder Kennzeichens keinen Anspruch auf internationalen Schutz hat, da einerseits andere international ebenfalls berechtigt sein können den Namen zu benutzen und es andererseits aufgrund der Struktur des Internets derzeit nicht möglich ist, einen Anspruch auf Nutzungsunterlassung auf

1Gegen eine Kennzeichenfähigkeit: LG Köln GRUR 1997, 377; CR 1997, 291, 291f; Kur, CR 1996, 325, 327; Gabel, NJW CoR 1996, 322; Wilmer, CR 1997, 562, 564. Für eine Kennzeichenfähigkeit: LG Mannheim CR 1996, 353; LG München I, 1997, 479, 480; Wiebe, CR 1998, 157ff.

2Nordemann, Rn. 2791; OLG Hamburg GRUR 2001, 838, 839; MMR 1999, 159, 160; OLG München GRUR 2000, 519, 520.

3Nordemann, Rn. 2791.

4Nordemann, Rn. 2825.

einen Staat zu beschränken[1]. Eine Unterscheidung kann daher nur auf der Ebene der second-level-Domains erfolgen[2].

Abschließend ist zu betrachten, wie sich der Schutz von Domains durch die Rechtsprechung auf die Funktionsfähigkeit der Domainverwaltung auswirkt.

(aa.) Schutz von Kennzeichen- und Namensinhabern gegen fremde Domains

Bei Kennzeichen ist zwischen Marken und geschäftlichen Bezeichnungen zu differenzieren. Die Wertungen der zu treffenden Konfliktentscheidungen sind unterschiedlich, die Grundprinzipien jedoch weitgehend identisch, so dass auf die Differenzierung hier verzichtet werden kann.

Marken sind geschützt, wenn sie ins Markenregister des Deutschen Patent- und Markenamtes eingetragen sind (§ 4 Nr. 1 MarkenG) oder „notorische Bekanntheit“ (§ 4 Nr. 2 MarkenG) bzw. „Verkehrsgeltung“ (§ 4 Nr. 3 MarkenG) haben. Nach §§ 9, 14, 15 MarkenG liegt ein Schutz gegen gleiche und verwechslungsfähige Zeichen vor. Beim Zusammentreffen von Domains und anderen Kennzeichen- oder Namensrechten entscheidet der Prioritätsgrundsatz des § 6 MarkenG. Eine Domain kann sich demnach auch gegenüber einer Marke durchsetzen, wenn Verwechslungsgefahr besteht und die Domain länger geschützt ist. Eine Nutzung der Domain ist trotz eines bestehenden Markenschutzes möglich, wenn die Marke für einen anderen Bereich als die Domain angemeldet bzw. genutzt wird. In einem derartigen Fall kann auch die Domain als Marke eingetragen werden. Notorisch bekannte Marken und solche mit Verkehrsgeltung sind allerdings nach § 15 MarkenG auch gegen eine solche „Parallelnutzung“ geschützt. Voraussetzung eines Anspruchs nach §§ 14, 15 MarkenG ist, dass der in Anspruch Genommene das verletzende Kennzeichen auch benutzt[3], da die reine Registrierung weder rechtliche Folgen hat noch Ansprüche nach § 1 UWG oder § 826 BGB begründet[4]. Zusätzliche Umstände können allerdings zu einer derartigen Wertung führen, insbesondere wenn durch eine Registrierung verhindert werden soll, dass ein Kennzeicheninhaber sein Kennzeichen im geschäftlichen Verkehr verwendet[5] oder Domaingrabbing vorliegt, eine Domain also nur registriert wurde, um sie an einen zahlungskräftigen Kennzeicheninhaber weiter zu verkaufen.

Eine Verwechslungsfähigkeit besteht erst, wenn die verwendeten Zeichen ähnlich sind und die Kennzeichen kumulativ für ähnliche Branchen bzw. Waren oder Dienstleistungen der Werke

1Hoeren, Internetrecht, S.40.

2Hoeren, Internetrecht, S.40.

3Ekey/Klippel, I § 14 MarkenG Rn. 73; Gimmy/Kröger-Freitag, S.482.

4Nordemann, Rn. 2823, a.A: Ruff, S.53 für § 12 BGB.

5Ruff, S.130; OLG Frankfurt MMR 2000, 424.

verwendet werden[1]. Es genügt nicht, wenn sich die Ähnlichkeit darauf bezieht, dass die Waren oder Dienstleistungen auf einer ähnlichen Plattform im Netz angeboten werden. Sie muss zwischen den Waren und Dienstleistungen selbst bestehen[2]. Im geschäftlichen Verkehr ist bei überragend bekannten Kennzeichen ein Anspruch auf Unterlassung auch möglich, wenn keine Verwechslungsgefahr besteht[3]. Dies gilt nicht bei der Konkurrenz zwischen Privaten und Unternehmen: Hier müssen die Interessen im Rahmen des § 12 BGB abgewogen werden[4], was die Rechtsprechung dementsprechend schwer überschaubar macht. Bei Unternehmen mit überragender Verkehrsgeltung setzt sich deren Name gegenüber Privatpersonen durch[5]. Es existiert kein Anspruch auf Mitbenutzung einer Domain; allerdings hat es sich bei nicht-kommerziellen beziehungsweise nicht-konkurrierenden Angeboten eingebürgert, dass der Domaininhaber einen Hinweis mit Link auf die möglicherweise verwechslungsfähige Domain setzt[6]. In der Literatur wird daher ein Mitbenutzungsanspruch aus dem Kennzeichenrecht gefordert[7]. Ein gesetzlicher Anspruch auf Übertragung der Domain ist nicht gegeben, ein Geschädigter kann lediglich Unterlassung der Nutzung und Löschung der Domain fordern[8].

Eine Kollision kann auch zwischen den Namen von Privatpersonen oder Unternehmen entstehen: In einem solchen Fall gilt die Regelung des § 12 BGB, nach dem die jeweiligen Namensinhaber grundsätzlich gleichberechtigt sind und der Prioritätsgrundsatz bei der Registrierung anzuwenden ist[9].

Von dieser Regelung sind auch bekannte natürliche Personen betroffen[10]. Im wirtschaftlichen Bereich sind allerdings Ausnahmen möglich, da bei unredlichen Absichten der Gebrauch des eigenen Namens rechtswidrig sein kann[11].

1Kröger/Gimmy-Freitag, S.473.

2Kröger/Gimmy-Freitag, S.473f.

3Kröger/Gimmy-Freitag, S.475.

4U.a. BGH MMR 2002, 382, 384 – shell.de; OLG München , MMR 1998, 668 – freundin.de; LG Hamburg MMR 1998, 448 – eltern.de; MMR 1998, 46 – bike.de; MM R 1998, 485 – emergency.de.

5Ruff, S.96.

6Nordemann, Rn. 2826.

7Nordemann, Rn. 2826.

8Nordemann, Rn. 2827; Kröger/Gimmy-Freitag, S.484f. BGH GRUR 2002, 622, 626.

9OLG Köln, CR 02, 533, 535 - guenther-jauch.de; OLG Dresden, Urteil vom 28.11.2000, 14 U 2486/00 – kurt-biedenkopf.de (abrufbar unter http://www.jurpc.de/rechtspr/20010098.htm); bestätigt durch BGH I ZR 82/01, Urteil vom 19.02.2004.

10OLG Köln, CR 02, 533, 535 – guenther-jauch.de; OLG Dresden, Urteil vom 28.11.2000, 14 U 2486/00 – kurt-biedenkopf.de(abrufbar unter http://www.jurpc.de/rechtspr/20010098.htm); bestätigt durch BGH I ZR 82/01, Urteil vom 19.02.2004.

11Palandt, §12 Rn. 26.

(bb.) Schutz von Domains als Marken

Der Schutz von Domains entsteht, anders als bei Marken, nicht bereits bei Registrierung, sondern erst bei Aufnahme des Betriebs [1]. Auch muss die Nutzung von Domains schneller aufgenommen werden, um deren Entzug aufgrund von Kollisionen mit angemeldeten Marken zu verhindern. Wenn ein Konflikt mit einer älteren Marke besteht, muss der Besitzer der Domain ein Eigeninteresse an der Domain nachweisen, da die Benutzung andernfalls unzulässig sein und Unterlassungs- und Löschungsansprüche nach §§ 823, 826 BGB sowie Ansprüche nach §§ 9, 14, 15 MarkenG nach sich ziehen kann[2]. Dies gilt jedoch nur für Domains der .de-TLD im Rahmen des gerichtlichen Verfahrens, die Registrierungsbedingungen der DENIC e.G. sehen andere Regelungen vor. Für internationale Domains ist in den Allgemeinen Registrierungsbedingungen ein obligatorisches Schiedsgerichtsverfahren, meist nach der UDRP, vorgesehen, was einen Rückgriff auf nationale Gerichte allerdings nicht ausschließt.

(cc.) Ansprüche gegen die Registry

Notwendige Bedingung für die Benutzung einer Domain ist deren Registrierung durch eine Registry wie die DENIC e.G. Aufgrund dessen wurde nicht selten versucht, nicht nur denjenigen, der Kennzeichenrechte durch Nutzung bzw. Anmeldung einer Domain verletzte, sondern auch denjenigen, der diese Domain eingetragen hatte, für die Verletzung haftbar zu machen. Diese Vorgehensweise war insbesondere in den USA verbreitet und wurde durch die Haltung von Network Solutions gefördert, die das Problem des Domaingrabbings anfangs ignorierten. Auch in Deutschland wurde versucht, die DENIC e.G. für Rechtsverletzungen durch Domaininhaber verantwortlich zu machen.

Nach ständiger Rechtsprechung des BGH besteht im Wettbewerbsrecht über eine entsprechende Anwendung von § 1004 BGB eine Haftung desjenigen, der an dem Wettbewerbsverstoß eines Dritten in irgendeiner Weise willentlich und adäquat kausal mitwirkt – wobei dieser Dritte weder schuldhaft noch mit Wettbewerbsförderungabsicht handeln muss[3] – sowie über eine rechtliche Möglichkeit zur Verhinderung der Handlung verfügt hat[4].

Eine Haftung von Registries scheint somit möglich. Sie kommt, sofern diese keine eigene Rechtsverletzung begeht, nur wegen Mitwirkung an einer fremden Rechtsverletzung, also der Nutzung einer Domain, die einem fremden Kennzeichen entspricht, in Frage.

1Nordemann, Rn. 2801.

2Nordemann, Rn. 2823.

3BGH GRUR 1997, 313, 315 mwN.

4BGH GRUR 1997, 313, 315.

Nach der „ambiente.de“-Entscheidung des BGH ist die Registry vor der Registrierung grundsätzlich nicht dazu verpflichtet, zu überprüfen, ob Rechte Dritter an einer einzutragenden Domain bestehen[1]. Dies gilt sogar dann, wenn sie nachträglich auf ein angeblich bestehendes besseres Recht hingewiesen wird. Eine Ausnahme besteht nur, wenn der Rechtsverstoß offenkundig und für die Registry ohne Weiteres festzustellen ist[2]. Eine Haftung ist ferner anzunehmen, wenn die Registry vorsätzlich den Rechtsverstoß eines Dritten fördert[3]. Hierbei ist die positive Kenntnis der Rechtswidrigkeit relevant, die jedoch angesichts des automatischen Registrierungsverfahrens kaum angenommen werden kann. Eine Haftung besteht allerdings bei Bestehen eines rechtskräftigen Urteils oder einer wirksamen Übernahmevereinbarung[4]. Die Registrierung und Verwaltung einer Domain gilt nicht als Benutzung eines Kennzeichens oder Namens, so dass auch daraus keine Ansprüche gegen die Registry folgen können[5]. Ein Anspruch auf Sperrung einer Domain für die Allgemeinheit mit der Folge, dass diese von niemandem als dem Kläger genutzt werden kann, kann nur bestehen, wenn jede denkbare Nutzung eine Rechtsverletzung darstellt[6]; dies ist jedoch nur schwer vorstellbar.

Die Rechtslage erscheint angesichts der wenig übersichtlichen, umfangreichen und komplexen Rechtsprechung angemessen, da das automatisierte Anmeldeverfahren zu einer schnellen Registrierung führt, durch vorherige Prüfungen – angesichts der Menge von Anmeldungen[7] – allerdings unzumutbar verzögert würde[8].

(dd.) Ansprüche gegen Registrare

Nachdem vom BGH in der ambiente.de-Entscheidung eine Haftung der DENIC e.G. als Registry abgelehnt worden war, wurde versucht, die Registrare als notwendig Beteiligte für Verstöße haftbar zu machen und ihnen die Registrierung bestimmter Domains[9] sowie die Kennzeichnung einer streitgegenständlichen Domain als „frei“ (bei so genannten „whois“-Abfrage) zu untersagen[10]. Abgesehen von der technischen Schwierigkeit dieses Unterfangens – bei einer Abfrage der Verfügbarkeit von Domains wird auf die Datenbank der Registry zugegriffen und verglichen, ob die

1BGH NJW 2001, 3265, 3265ff.

2BGH NJW 2001, 3265, 3265ff.; LG Kiel MMR 2002, 64.

3BGH NJW 2001, 3265, 3265.

4BGH NJW 2001, 3265, 3266.

5OLG Dresden 14 U 2486/00, Urteil vom 28.11.2000 (abrufbar unter http://www.jurpc.de/rechtspr/20010098.htm); bestätigt durch BGH I ZR 82/01, Urteil vom 19.2.2004.

6OLG Dresden, CR 2001, 408, 410. Vor diesem Hintergrund verwundert der Vorschlag von Röhrborn, CR 2001, 410, 411, doch einen Anspruch auf generelle Sperrung zuzulassen, auch wenn es möglicherweise berechtigte Nutzungen geben kann, die aber nur im Einzelfall gefunden werden können.

7Durchschnittlich ca. 100.000 Anmeldungen im Monat.

8BGH NJW 2001, 3265, 3267.

9So der Sachverhalt von OLG Köln CR 02, 533ff; Leible/Sosnitza, CR 01, 624, 625.

10So der Sachverhalt von OLG Köln CR 02, 533ff.

Domain verfügbar ist, daher müsste die Datenbank der DENIC e.G. geändert werden – hat das OLG Köln festgestellt, dass in einer reinen „whois"-Abfrage keine Namensverletzung liegen kann[1]. Des Weiteren hat das OLG Köln die Verantwortlichkeit der Registrare nicht prinzipiell abgelehnt und – allerdings in einem obiter dictum – erklärt, dass eine Haftung möglich erscheint, da automatisierte Prüfungsroutinen eingeführt werden könnten[2]. Allerdings wäre es im Sinne der Rechtsprechung des BGH widersprüchlich, eine Prüfungspflicht der DENIC e.G. als Registry abzulehnen, sie jedoch in der Rolle als Registrar, die sie teilweise ausfüllt, aus dem gleichen Grund haften zu lassen. Auch als Registry könnte die DENIC e.G. dieselben nach Ansicht des OLG Köln möglichen Prüfroutinen verwenden, deren Auferlegung für Registrare in der Diskussion stand. In diesem Fall kommt ein Vertrag zwischen Domaininhaber und DENIC e.G. zustande. Das OLG Köln geht – völlig zutreffend – davon aus, dass den für Prüfungen zu verwendenden Programmen ein funktionierendes Filtersystem fehlt[3]; ein solches könnte indessen die Zahl der fraglichen Anmeldungen so weit reduzieren, dass eine manuelle Prüfung zumutbar würde.

Wie die Erfahrung mit Jugendschutzfiltern zeigt, sind diese auch nach jahrelanger Entwicklungsarbeit noch nicht als zuverlässig einzustufen. Allerdings wäre auch bei Vorhandensein verlässlicher Filtersysteme nicht einzusehen, weshalb Registrare über bessere Möglichkeiten zur Überprüfung der Rechtmäßigkeit einer Domain-Anmeldung verfügen sollten als die Registry selbst. Die wirtschaftliche Tätigkeit der ersteren ist als alleiniges Argument nicht ausreichend, da zumindest bisher aufgrund der erheblich niedrigeren Kosten der Anmeldung über Service-Provider gegenüber einer direkten Anmeldung bei DENIC e.G. nicht davon auszugehen ist, dass diese durch Domain-Anmeldungen einen größeren Gewinn erzielen[4]. Auch der nach dem BGH wünschenswerte Effekt der schnellen, unproblematischen Registrierung Prüfung würde verhindert, wenn vom Registrar eine Prüfung durchzuführen wäre, da der Zeit- und Arbeitsaufwand hierdurch steigen würde. Es kann festgehalten werden, dass schwer nachvollziehbare Widersprüche vorliegen würden, wenn die Registry nicht unter denselben Voraussetzungen haftete wie die Registrare.

(ee.) Haftung für Subdomains

Unterhalb einer Second-Level Domain können auch Subdomains (Third-Level-Domains) registriert werden; diese stehen vor der eigentlichen Domain, lauten also „http://subdomain.second-level.de". Dieser Service wird auch kommerziell genutzt. Hierbei stellt sich die Frage, ob und inwieweit

1OLG Köln, CR 02, 533, 534 – guenter-jauch.de II; zustimmend Ernst, CR 02, 535,535; a.A: LG Köln, CR 01, 622f – „guenter-jauch.de" I.

2OLG Köln, CR 02, 533, 534 – guenter-jauch.de II.

3Leible/Sosnitza, MMR 2002, 479, 479.

4Eine Anmeldung über DENICdirekt kostet derzeit 116 € (Stand: 13.1.06), über Service-Provider ist sie bereits ab ca. 10 € möglich.

derjenige, der die Subdomains registriert, für die Handlungen der Inhaber der Subdomains haftet. Technisch gesehen tut der Inhaber von Subdomains nichts anderes als eine Registry. Er muss nur einen eigenen Name-Server für den Bereich seiner Domain betreiben. Eine Haftung dürfte bei Anwendung der Grundsätze der BGH-Rechtsprechung weitestgehend ausgeschlossen sein.

Ein Anbieter von Subdomain-Registrierungen muss nicht zwangsläufig Host- oder Access-Provider sein[1]. Es besteht keine Notwendigkeit, die Daten der Subdomain auf dem Server des Anbieters zu lagern. Fraglich ist nun, inwieweit der Anbieter von Subdomains für deren Bereitstellung von den Privilegierungen der §§ 8-10 TMG profitieren kann.

(aaa.) Haftung als Host-Provider

Als Host-Provider ist ein Anbieter von Subdomains nach § 10 TMG privilegiert[2]. Es stellt sich die Frage, ob der Anbieter zur Erhebung von weiteren Daten verpflichtet ist, damit Dritte im Falle von Rechtsverletzungen ihre Rechte gegenüber dem Inhaber der Domain geltend machen können. Wenn dies nicht der Fall wäre, läge eine „organisierte Verantwortungslosigkeit“ vor: Eine Rechtsverfolgung ist praktisch unmöglich, wenn der Provider aufgrund seines Haftungsprivilegs nicht haftet und der Inhaber die Domain mit falschen Angaben reserviert hat[3]. Im Bereich der Registrierung von SLDs kann dieses Problem kaum auftreten, da für die Abrechnung notwendigerweise Kontaktdaten vorhanden sein müssen.

Nach § 10 TMG haftet ein Host-Provider nur für Rechtsverstöße von Dritten, wenn er positive Kenntnis vom Rechtsverstoß hat oder die Nutzung technisch und auf zumutbare Art verhindern kann; dies dürfte im Vorhinein gemeinhin nicht der Fall sein.

Nach Flechsig[4] soll der Host-Provider analog einem Weisungsbefugten für seine Untergebenen haften, wenn er keine Vorkehrungen trifft, dass Dritte nicht unerkannt Rechtsverletzungen begehen können: Es handele sich hierbei nicht um eine Umgehung der Haftungsprivilegierung der § 7 ff. TMG, sondern um eine Haftung für eine eigene Sorgfaltspflichtverletzung[5]. Eine solche setzt allerdings den Verstoß gegen eine Rechtspflicht zum Handeln, hier der Erhebung von persönlichen Daten des Vertragspartners, voraus. Dass die Feststellung der Daten im eigenen Interesse des Anbieters der Subdomain liegt, bedarf ebenso wenig einer weiteren Erläuterung wie die Feststellung, dass sie für die Rechtsverfolgung notwendig ist. Ob diese Obliegenheit auch eine

1So aber Flechsig, MMR 2002, 347, 348. Das LG Leipzig, CR 2004, 943, 945 verneint jeglichen Unterschied zwischen Host- und Access Providern.

2Diese Thematik klammert LG Leipzig, CR 2004, 943ff. völlig aus und gelangt so mit technisch falschen und rechtlich lückenhaften Ausführungen zu einer Haftung. Allerdings muss der Anbieter von Subdomains nicht zwangsläufig Host-Provider für die Inhalte der Subdomain sein.

3So auch die Sachlage im Urteil des LG Leipzig, CR 2004, 943ff.

4Flechsig, MMR 2002, 347, 349.

5Flechsig, MMR 2002, 347, 349. So wohl auch LG Leipzig, CR 2004, 943ff.; technisch sind dessen Ausführungen allerdings schlicht falsch.

Pflicht gegenüber möglicherweise geschädigten Dritten begründen kann, ist aber vor dem Hintergrund der Datenschutzbestimmungen des TMG fraglich. Hierzu müsste der Anbieter der Subdomains überhaupt diese Daten erheben dürfen. Auch existiert keine generelle Regel, dass ein Anbieter dafür Sorge zu tragen hat, dass Dritte, mit denen er in Verbindung steht, keine Rechtsverletzungen begehen. Eine gesetzliche Haftung wird zwar gefordert, besteht jedoch nicht und würde auch den Haftungsprivilegierungen des TMG widersprechen.

(bbb.) Haftung für die Domainvergabe

Für Rechtsverletzungen durch die Registrierung der Domain ist der Anbieter von Subdomains im selben Maße verantwortlich wie die Registry, da er im Grundsatz nichts anderes tut als diese. Allerdings soll auch hier eine Sorgfaltspflicht bestehen, die sich einerseits aus dem Vorgehen der DENIC e.G. bei Domainregistrierungen, andererseits aus § 242 BGB ergibt. Ob diese auch auf Anbieter mit anderen Geschäftsbedingungen ausgedehnt werden kann, ist fraglich: Schließlich sind die Geschäftsbedingungen der DENIC hauptsächlich im Hinblick darauf entstanden, dass auch sie Vertragspartnerin des Domaininhabers wird und deshalb eventuell Forderungen eintreiben sowie technische Fragen klären muss. Diese Faktoren sind bei einem Anbieter von Subdomains allerdings nicht gegeben.

(ccc.) Kritik

Andere Geschäftsbedingungen, beispielsweise von Free-Mail Anbietern oder dem Anonymisierungsdienst AN.ON[1] des Unabhängigen Landesdatenschutzzentrums Schleswig-Holstein (ULD) und der TU Dresden, sehen keine Erhebung von Daten oder die Kontrolle derer Richtigkeit über die Notwendigkeit für die Vertragsabwicklung hinaus vor, obschon eine rechtswidrige Nutzung beider Dienste möglich ist. Nach einer längeren Auseinandersetzung zwischen AN.ON und dem Bundeskriminalamt wurde vom LG Frankfurt festgestellt, dass für AN.ON nicht einmal die Verpflichtung besteht, Verbindungsdaten zu protokollieren[2]. Des Weiteren gibt es keine gesetzliche Vorschrift, die Anbieter verpflichtet, Daten einzig für die mögliche Rechtsdurchsetzung Dritter zu erheben. Einer derartigen Politik stünde auch das Datenschutzrecht, insbesondere §§ 11-15 TMG entgegen: Danach darf der Anbieter von Telediensten nach dem TMG – wozu das „Hosten“[3] von Internet-Auftritten und die Vergabe von Subdomains eindeutig gehören – nur solche Daten erheben, die er für die Durchführung seiner Verpflichtungen benötigt oder für deren Erhebung eine gesetzliche Erlaubnis besteht. Nach § 15 I TMG dürfen nur die Daten erhoben

1http://anon.inf.tu-dresden.de/.

2Pressemitteilung des ULD vom 27.8.2003, siehe: http://www.datenschutzzentrum.de/material/themen/presse/anonip2.htm.

3Das nicht die Tätigkeit eines Access-Providers umfasst. So aber LG Leipzig, CR 2004, 943ff.

werden, die für die Durchführung eines Vertrags erforderlich sind. Der Begriff der Erforderlichkeit ist eng auszulegen[1].

Eine Erlaubnisvorschrift für die Datenerhebung zum Zwecke der Rechtsverfolgung Dritter existiert nicht, und eine zivilrechtliche Verkehrssicherungspflicht, die aus Billigkeitsgründen konstruiert wird, genügt den Anforderungen der §§ 12 I TMG, die eine gesetzliche Ermächtigung vorsehen, nicht[2]: Diese muss sich, wenn sie nicht im TMG enthalten ist, ausdrücklich auf Telemedien beziehen. Daher ist die Erhebung persönlicher Daten bei einer kostenlosen Überlassung von Subdomains nicht vom Gesetz gedeckt.

Eine Einwilligung darf wegen des Koppelungsverbots des § 12 III TMG, wonach die Erbringung von Telediensten nicht von der Zustimmung zur Erhebung persönlicher Daten abhängig gemacht werden darf, nicht gefordert werden. Somit kollidierte eine Verkehrssicherungspflicht zur Feststellung der Identität des Kunden eines Subdomain-Anbieters mit dem TMG. Der Anbieter würde entweder gegen die geforderte Verkehrssicherungspflicht oder das TMG verstoßen. Die Haftung von Anbietern von Subdomains für Verkehrssicherungspflichtverletzungen ist daher abzulehnen.

(ff.) Rechtsschutz contra funktionsfähiges Vergabesystem

Die zitierten Urteile offenbaren, dass der möglichst effektive Schutz vor Rechtsverstößen Dritter durch die Androhung einer Haftung der Registry bzw. der Registrare nicht selten mit einer möglichst reibungslosen Registrierung von Domains kollidiert. Im Gegensatz zur Anfangszeit der Rechtsprechung über Sachverhalte mit Bezug zum Internet zeigt sich, dass die Gerichte zunehmend ein Problembewusstsein für die technischen Implikationen der zu treffenden Entscheidungen entwickeln. Sämtliche Urteile weisen eine Haftung der Registry zurück und stellen sie – mit Ausnahme vorsätzlichen Handelns – von jeglichen vorherigen Prüfungspflichten und Haftung für Rechtsverstöße Dritter frei. Dies geschieht bewusst, wie die Argumentationen der OLGe Dresden und Köln zeigen. Es wäre auch ein der Anmeldung von Marken ähnliches Verfahren möglich gewesen, das eine Prüfungspflicht des Patent- und Markenamtes beinhaltet hätte; der – auch vom OLG Dresden angeführte – Nachteil bestand allerdings in der langen Wartezeit von sechs bis zwölf Monaten. Im Bereich der Domainvergabe liegt der Schwerpunkt der gerichtlichen Entscheidungen auf dem Schutz der Funktionsfähigkeit des Mediums Internet. Dies scheint nur unter Inkaufnahme der vorübergehenden Verletzung individueller Rechte möglich.

Im Falle der Haftung der Registrare wird nicht ins Feld geführt, dass diese faktisch notwendige Beteiligte bei der Anmeldung von Domains sind. Dies erscheint einigermaßen überraschend, da

1Engel-Flechsig/Maennel/Tettenborn-Engel-Flechsig, § 5 TDDSG Rn. 13.

2Engel-Flechsig/Maennel/Tettenborn-Engel-Flechsig, § 3 TDDSG Rn. 16.

dieselbe Rechtmäßigkeitsprüfung, welche die Registry aufgrund praktischer Unmöglichkeit nicht durchführen kann, den Registraren aufgebürdet werden könnte, wobei die Verzögerungen der Domainanmeldung gegenüber einer Prüfung durch die Registry lediglich vorverlagert würden, da von einem Ansteigen der Gesamtzahl der zu untersuchenden Domains auszugehen ist. Die Begründung, dass Registrare, anders als die DENIC e.G., mit der Absicht der Gewinnerzielung arbeiten, vermag die unterschiedliche Bewertung nicht zu tragen, zumal der Hauptverantwortliche der Rechtsverletzung in der Regel greifbar ist und es nur das Ziel des Klägers ist, einen zusätzlichen, solventen Haftenden zu finden. Dieses Bestreben muss aber, wie auch bei der stark privilegierten Haftung der DENIC e.G. als Registry, gegenüber dem öffentlichen Interesse an einer schnellen, unkomplizierten Abwicklung der Registrierung von Domains zurückstehen. Bisher ist kein Urteil bekannt, in dem Registrare mit einer Haftung belastet wurden.

(b.) Registrierungsbedingungen der DENIC e.G.

Die Registrierungsbedingungen der DENIC e.G enthalten nicht nur gerichtliche, sondern gleichsam weiter gehende Möglichkeiten, gegen eine unzulässige Nutzung eines Domainnamens vorzugehen. Auch wenn die Anmeldung der Domain nicht direkt über die DENIC e.G., sondern über einen Registrar erfolgt, entsteht sowohl ein Vertrag mit dem Registrar als auch mit der DENIC e.G. Wenn eine Domain umstritten ist, hat derjenige, der ihren Besitz erlangen möchte, die Möglichkeit, die Domain nach § 2 III mit einem so genannten Dispute-Eintrag belegen zu lassen, der eine Übertragung der Domain an Dritte, nicht aber die Nutzung ausschließt. Hierfür muss derjenige, der diesen Eintrag wünscht, seine eigene mögliche Berechtigung an der Domain nachweisen und nach § 3 der Registrierungsbedingungen die DENIC e.G. von der Haftung gegenüber Dritten freistellen.
Ein Schiedsgerichtsverfahren hat die DENIC e.G., anders als die ICANN oder die österreichische Registry, nicht vorgesehen, da ein solches den gerichtlichen Rechtsschutz nicht beeinflussen kann und daher nach Meinung der DENIC e.G. keine Auswirkungen auf Domainstreitigkeiten haben würde[1].

(6.) UDRP

Die UDRP wurde als einheitliches Regelwerk für die Schlichtung von Domainkonflikten im Bereich der von der ICANN verwalteten TLDs geschaffen und wird von den für die .com, .net und .org zuständigen Registraren angewandt. Sie zielt nicht darauf ab, ordentliche Gerichtsverfahren ersetzen, sondern soll ein schnelles und effizientes Verfahren zur Lösung von Konflikten bieten und

1Roth, abrufbar unter: http://www.telepolis.de/deutsch/inhalt/te/11616/1.html.

Probleme des Internationalen Privatrechts durch Schaffung eines einheitlichen Rechtsrahmens beseitigen. Für die „sponsored TLDs“ gibt es teilweise ergänzende Konfliktlösungsmechanismen.
Im Bereich der ccTLDs hat die UDRP nur eingeschränkte Wirkung; es steht den NICs aber frei, sie auch für die von ihnen verwalteten Domains anzuwenden. Die DENIC e.G. hat dies nicht getan, da die UDRP weder den Weg vor die ordentlichen Gerichte sperren kann[1] noch dessen Vorteile aufzuwiegen vermag[2]. Allerdings werden 95% der Streitigkeiten nach der UDRP durch ein Schiedsgerichtsverfahren endgültig beendet[3]. Die Konfliktlösungen werden nicht durch die ICANN selbst entschieden, sondern durch von ihr zugelassene Schiedsstellen, so genannte Dispute Resolution Service Provider. Derzeit sind fünf solche Provider, bestehend aus der WIPO (mit Sitz in Genf), dem Asian Domain Name Dispute Resolution Center, zwei US-amerikanischen Schiedsstellen und einer Stelle, die inzwischen keine Verfahren mehr annimmt[4], zugelassen.
Neben der UDRP existieren die UDRP-Rules, die nach Nr.4 UDRP als Verfahrensordnung für Streitigkeiten anzuwenden sind. Sowohl die UDRP als auch die UDRP-Rules wurden am 24.10.1999 durch das ICANN-Board in Kraft gesetzt.

(a.) Voraussetzungen

Nach Nr.1 UDRP gelten diese nur für Streitigkeiten zwischen Domaininhabern und Dritten, nicht für Konflikte mit dem Registrar. Nach Nr. 4a UDRP, Nr. 3b ix UDRP-Rules muss der Antragsteller behaupten und beweisen, dass

1. der Domainname mit einer Marke gleich lautend oder zum Verwechseln ähnlich ist und
2. der Antragsgegner kein legitimes Interesse an der Domain hat und
3. die Domain böswillig vom Inhaber registriert und genutzt wird

In Nummer 4b UDRP sind nicht abschließend Indizien für eine bösgläubige Registrierung und Benutzung aufgezählt; dazu gehören eine Registrierung zum alleinigen Zweck des Weiterverkaufs sowie eine Registrierung, um einen Markeninhaber von der Nutzung abzuhalten oder Nutzer auf eigene Seiten zu locken. Es wird außerdem festgelegt, dass der Antrag eine bestimmte Rechtsfolge enthalten muss.

(b.) Auswahl der Schiedsstelle

Nach Nr. 4d UDRP wählt der Antragsteller die Schiedsstelle aus. Da die UDRP keine Probleme hinsichtlich des internationalen Privatrechts aufwirft, ist diese Regelung unbedenklich.

1Roth, abrufbar unter: http://www.telepolis.de/deutsch/inhalt/te/11616/1.html.

2http://www.DENIC.de/de_1/faqs/recht_dispute/.

3Roth, abrufbar unter: http://www.telepolis.de/deutsch/inhalt/te/11616/1.html.

4http://www.icann.org/udrp/approved-providers.htm.

(c.) Verfahren

Nach Nr.2 UDRP-Rules ist nach erfolgter Zahlung der Gebühren von Seiten des Antragsstellers der Antrag dem Antragsgegner innerhalb von drei Tagen durch die Schiedsstelle auf allen möglichen, bei seinem Provider angegebenen und auf den Websites der Domain erkennbaren Wegen zuzustellen.

Die Erwiderung hat innerhalb von 20 Tagen nach Empfang des Antrags sowohl schriftlich als auch in Textform zu erfolgen und muss auf die Behauptungen des Antragstellers eingehen.

Jede Partei kann eine Entscheidung durch drei Schiedsrichter beantragen und hierfür drei Vorschläge für eine Schiedsrichterstelle aus den bei der Schiedsstelle zugelassenen Richtern einreichen. Diese sind nach Nr.7 UDRP-Rules unabhängig und unparteiisch und sollen die Schiedsstelle von allen Umständen unterrichten, die Zweifel an ihrer Unabhängigkeit begründen können.

(d.) Entscheidung

Grundlage der Entscheidung sind nach Nr. 15a UDRP-Rules die von den Parteien eingereichten Schriftsätze und Beweise. Das Schiedsgericht soll seine Entscheidung sowohl auf der Grundlage der UDRP und UDRP-Rules als auch nach Rechtsregeln und Prinzipien treffen, deren Anwendung es in der Konfliktlage für wünschenswert hält. Wenn die Beschwerde abgewiesen wird, kann das Schiedsgericht auch feststellen, dass der Antrag bösgläubig eingebracht wurde. Die Entscheidung wird der ICANN mitgeteilt, die im Falle einer Stattgabe die Entscheidung nach zehn Tagen umsetzt, wenn sie nicht von der Erhebung einer Klage unterrichtet wird, Nr. 4 k UDRP.

(e.) Kosten

Die Kosten des Verfahrens trägt nach Nr. 6a, 19a UDRP-Rules der Antragsteller. Nach Nr. 5c, 19a UDRP-Rules hat der Antragsgegner aber, wenn er eine Entscheidung durch drei Schiedsrichter beantragt hat, die Hälfte der Kosten für deren Besetzung zu tragen.

(f.) Kritik

Das Streitschlichtungsverfahren der ICANN bzw. die ergänzenden Maßnahmen der Registries stehen seit längerer Zeit in der Kritik[1]. Obwohl das Schlichtungsverfahren, insbesondere bei Länder

1Z.B._http://www.sedo.de/links/showhtml.php3?Id=100&language=d.

überschreitenden Konflikten, erheblich schneller zu einer endgültigen Entscheidung führt als – häufig langjährige – Rechtsstreits[1] und somit zur Rechtssicherheit bei von der ICANN verwalteten Domains beiträgt, werden durch Berichte wie dem von Hoeren[2] Zweifel gesät: Hierbei ging es um einen Schiedsrichter der WIPO, der eine völlig im Einklang mit anerkannten rechtlichen Prinzipien stehende Entscheidung gegen einen bedeutenden Markeninhaber fällte und nach einer informellen Beschwerde dieses Markeninhabers – einem einflussreichen Mitglied der WIPO – in den folgenden Jahren ohne jede Begründung nicht mehr als Schiedsrichter vorgeschlagen wurde. Fraglich ist nun, ob ein solcher Vorfall zu einer Ablehnung des Schiedsverfahrens oder eher zu einer Anregung von Reformen führen sollte.

Ein grundsätzliches Problem des Schiedsverfahrens besteht darin, dass es weitestgehend Sache des Beschwerdeführers ist, eine Schiedsstelle zu suchen. Angesichts statistisch abweichender Erfolgsaussichten[3] liegt es nahe, dass auch materielle Unterschiede im Umgang mit Beschwerden existieren, die von finanzstarken Beschwerdeführern genutzt werden können. Die starke Rolle des Beschwerdeführers bei recht klaren Missbrauchsfällen, bei denen es um sogenanntes Domaingrabbing geht, ist unproblematisch. Hier darf dem Beschwerdegegner im Interesse der Rechtsdurchsetzung des Berechtigten nicht die Möglichkeit offen stehen, die Rechtsdurchsetzung durch Streitigkeiten um die Auswahl der Schiedsstelle zu verzögern oder zu verhindern. Im Falle der ernsthaften und nicht missbräuchlichen Nutzung von Domains verschafft dieses Verfahren allerdings dem Beschwerdeführer einen unangemessenen Vorteil, den andere Schiedsgerichtsverfahren in dieser Form nicht kennen. Hier wäre eine Anpassung an anerkannte Grundsätze des Schiedsgerichtsverfahrens wünschenswert.

Das grundlegende Ziel muss in der Möglichkeit bestehen, den „Anfangsvorteil“ des Beschwerdeführers durch Kompensationsmechanismen auszugleichen. Diese dürfen allerdings im Falle des Domaingrabbings nicht zu einer Einschränkung der Rechtsdurchsetzung führen. Alternativ könnte dem Gegner nach Einlegung der Beschwerde zugestanden werden, in seiner Antwort eine Auswahl der Schiedsrichter vorzunehmen. Sollte er auf die Antwort bzw. die Auswahl der Schiedsrichter verzichten, bliebe das gegebene Verfahren bestehen; sollte der Beschwerdegegner die Auswahl der Schiedsrichter ablehnen, bekäme er die Möglichkeit, entweder neue Schiedsrichter auszuwählen oder eine andere Institution vorzuschlagen. Im zweiten Fall könnte der Beschwerdeführer die Schiedsrichter der vom Beschwerdegegner vorgeschlagenen Schiedsstelle auswählen. Unbenommen

1Dies belegt die weit überwiegende Zahl von endgültig durch die verschiedenen Schiedsstellen erledigten Verfahren.

2Hoeren, MMR 2003, 761.

3Mueller, S. 2; abrufbar unter: http://dcc.syr.edu/miscarticles/roughjustice.pdf. Eine neuere Untersuchung liegt nicht vor. Nach Stubenschrott, S.36, abrufbar unter: http://rechtsprobleme.at/doks/stubenschrott-wipo-udrp-at.pdf haben die von Mueller beschriebenen Unterschiede dazu geführt, dass der Anbieter mit der höchsten Rate an Beschwerdeabweisungen den geringsten Marktanteil hatte und sich inzwischen zurückziehen musste.

bliebe den Parteien eine Einigung über Schiedsstelle und Schiedsrichter. Das beschriebene Verfahren dürfte für eine faire Verteilung sorgen. Wenn es im streitigen Verfahren zu einem – auch vorher möglichen – Ausspruch kommt, dass die Einbringung des Antrags böswillig war, sollte es der Schiedsstelle erlaubt sein, dem Beschwerdeführer die – möglicherweise erheblichen – Kosten des Gegners aufzuerlegen. Diese Vorgehensweise könnte wahrscheinlich das so genannte Reverse-Domain-Hijacking verhindern und auch finanzschwachen Domaininhabern ermöglichen, ihre Rechte angemessen zu verteidigen, ohne in den finanziellen Ruin getrieben zu werden.
Das vorgeschlagene Verfahren wäre im Vergleich zu der bisherigen Methode insofern positiver zu bewerten, als weder eine Partei im Vorteil wäre noch im Alleingang die Rechtsdurchsetzung der anderen Partei verhindern könnte. Für „klassische“ Domaingrabbing-Fälle bestünde die Möglichkeit des schnellen Verfahrens, gegen das in diesen Fällen keine Bedenken vorlägen, nach wie vor.

(g.) Weitere Schiedsgerichtsordnungen

Neben der UDRP haben verschiedene Registrare für die von ihnen verwalteten TLDs ergänzende Schiedsgerichtsordnungen erlassen. Dazu gehören die für .aero, .coop und .museum Domains anwendbare Charter Eligibility Dispute Resolution Policy (CEDRP)[1], die für die .name Domain anwendbare ERDPR[2], die für die .pro -Domain anwendbare Intellectual Property Defensive Registration Challenge Policy (IPDRCP)[3] und die für die .biz-Domain anwendbare Restrictions Dispute Resolution Policy (RDRP)[4].
Gemeinsam ist diesen Domains, dass sie, anders als die meisten ursprünglichen TLDs, nur für bestimmte Zwecke vorgesehen sind. Daher sehen die Schiedsgerichtsordnungen zusätzlich zur UDRP eine Anfechtung wegen einer nicht den Richtlinien entsprechenden Registrierung vor. Derartige Registrierungsbeschränkungen waren auch schon für .com, .net und .org vorgesehen, konnten aber aufgrund des Ansturms bei der erstmaligen Vergabe von Domains nicht durchgesetzt werden.
Auch die zugelassenen Schiedsstellen weichen zum Teil von der UDRP ab.
Neben den materiellen Ordnungen existieren jeweils zugehörige Verfahrensordnungen, die so genannten „Rules“.

1http://www.icann.org/udrp/#cedrp.
2http://www.icann.org/udrp/#erdrp.
3http://www.icann.org/udrp/#ipdrcp.
4http://www.icann.org/udrp/#rdrp.

2. W3C

Eine andere Form der Entwicklung von Standards wird vom W3C angewandt. Das World Wide Web Consortium (W3C) wurde 1994 von dem Erfinder des WWW, Tim Berners-Lee, am Massachusetts Insitute of Technology und dem Europäischen Kernforschungszentrum CERN mit Unterstützung der DARPA und der EU-Kommission gegründet[1]. Geführt wird es von dem Laboratory for Computer Science des MIT, der Keio-University in Japan und dem European Research Consortium in Informatics and Mathematics (ERCIM)[2]. Anders als die IETF ist das W3C eine hauptsächlich von Industrievertretern getragene Organisation[3]; es bezeichnet sich selbst als Industrieverband. Weitere Mitglieder sind Forschungseinrichtungen und Non-Profit-Organisationen.

Anders als die IETF beschäftigt sich das W3C nicht mit den technischen Grundfunktionen der Datenübertragung, sondern mit anwendungsorientierten Standards. Dazu gehören unter anderem die Grundlagen des WWW, Sprachen wie HTML und CSS, aber auch Standards wie PICS oder P3P für den Datenschutz. Die Entscheidung über in den Standardisierungsprozess aufzunehmende Vorschläge fällt der Vorsitzende nach Beratung durch das Advisory Commitee (AC)[4], das aus Repräsentanten der Mitglieder besteht[5], wobei die Diskussionen, anders in der IETF und den anderen ISOC-Gruppen, nicht öffentlicher Natur und die Mitglieder zu Vertraulichkeit verpflichtet sind[6]. Teilnahmeberechtigt zu den Arbeitsgruppen sind nur Vertreter der Mitglieder und geladene externe Fachleute[7]. Zwar kann prinzipiell jede natürliche oder juristische Person Mitglied werden, jedoch ist der Kreis potentieller Mitglieder durch die Mitgliedsgebühr von derzeit 65.000 € bzw. ermäßigt 6.500 € pro Jahr erheblich beschränkt[8]. Nichtmitglieder können an den – in der Regel – öffentlichen Treffen teilnehmen[9] und werden an über 50 öffentlichen Mailinglisten beteiligt. Es ist ihnen allerdings nicht möglich, sich einen Überblick über die internen Diskussionen zu verschaffen oder sich an den Abstimmungen im Advisory Commitee zu beteiligen. Der Weg eines Vorschlags zu einer W3C Empfehlung wird explizit im W3C Recommendation Track beschrieben, welcher gewährleisten soll, dass nur ausgereifte und von einem breiten Konsens getragene Vorschläge zu

1http://www.w3.org/Consortium/#background.

2http://www.w3.org/Consortium/#background.

3Vgl. Mitgliederliste unter: http://www.w3.org/Consortium/Member/List.

4Mayer, Selbstregulierung im Internet, K&R 2000, 13, 18.

5Mayer, Selbstregulierung im Internet, K&R 2000, 13, 19.

6Lohse/Janetzko, CR 01, 55, 56.

7Lohse/Janetzko, CR 01, 55, 56.

8http://www.w3.org/Consortium/Prospectus/, Stand: 25.2.04.

9Lohse/Janetzko, CR 01, 55, 57.

Empfehlungen werden können[1]. Über die Anerkennung als Recommendation entscheidet der Direktor in Abstimmung mit dem Advisory Commitee. Dieser Weg ist allerdings weit weniger formalisiert als das Standardisierungsverfahren der IETF[2]. Wenn ein Standard den Status einer Recommendation erreicht hat, wird dadurch zum Ausdruck gebracht, dass seine Anwendung von Seiten der Industrie befürwortet wird[3]. Das bedeutet jedoch nicht zwangsweise, dass die Industrie, die den Standard als Recommendation im Konsens verabschiedet hat, diesen auch umsetzt. Als Beispiel kann der heftige „Browser-War" Ende der 90er Jahre zwischen Netscape und Microsoft genannt werden: Keines der Produkte der beiden Firmen setzte die Standards des W3C gänzlich um. Die Befehlssätze waren untereinander teilweise nicht kompatibel. Auch heutzutage sind noch nicht alle Recommendations des W3C aus dieser Zeit angewendet, wenngleich die daraus entstehenden Probleme inzwischen weitaus geringer geworden sind.

Der Standardisierungsprozess des W3C erinnert scheinbar stark an den der IETF. Allerdings fehlt Ersterem die Transparenz und damit auch die basisdemokratische Kontrolle der IETF und die freie Mitwirkungsmöglichkeit aller Interessierter. Außerdem muss beachtet werden, dass aufgrund der Zusammensetzung der Mitglieder eine größere Beeinflussung durch Industrieinteressen sowie aufgrund des weniger formalisierten Verfahrens eine stärkere Wirksamkeit der beschlossenen Standards seitens der führenden Köpfe als in der IETF vorliegt[4]. Das W3C hat indessen keine Handhabe, die Recommendations durchzusetzen, sondern ist auf die Kooperation der großen und einflussreichen Firmen angewiesen, wobei sich diese, obschon sie als Mitglieder die Standards beeinflussen konnten, bisher nur selten an von ihren Vorstellungen abweichende W3C-Recommendations angepasst haben.

3. ISO

Die ISO ist zwar kein internetspezifisches Standardisierungsgremium, jedoch beziehen sich einige ihrer Standards auf das Internet .

Allen Organisationen fehlt die Möglichkeit, Empfehlungen bzw. Standards zwangsweise durchsetzen zu können. Sie sind auf Kooperation angewiesen. Um Konflikten entgegen zu wirken, sind die Entscheidungsmechanismen auf den größtmöglichen Konsens ausgerichtet.

1Lohse/Janetzko, CR 01, 55, 57.

2Mayer, Selbstregulierung im Internet, K&R 2000, 13, 18.

3Lohse/Janetzko, CR 01, 55, 57.

4Mayer, Selbstregulierung im Internet, K&R 2000, 13, 18.

4. Zusammenfassung

Bei der Verteilung von Basisressourcen ist ein staatliches Eingreifen weder angebracht, da die derzeitige Verteilung effizient und diskriminierungsfrei funktioniert, noch ohne erhebliche – wenngleich nicht unüberwindliche – Schwierigkeiten durchführbar; zudem existiert derzeit keine Rechtsgrundlage für eine staatliche Intervention.

Die Standardisierung durch die verschiedenen Internetgremien ist bisweilen langwierig, allerdings funktioniert sie recht effizient und die beschlossenen Standards leiden nicht unter mangelnder Akzeptanz oder werden zum Gegenstand von Standardisierungskriegen, die letztlich nur die Nutzer als Verlierer hinterlassen.

Die Verfahren wegen Domainstreitigkeiten der .de-Domain unterliegen keinen speziellen Regelungen, bemerkenswert ist lediglich, dass sich die Rechtsprechung explizit auf RfC 1591 als Standard bezieht. Internationale Domainstreitigkeiten werden in der Regel durch Schiedsgerichtsordnungen gelöst. Diese weisen jedoch Mängel auf, die Verbraucher und kleine Unternehmen im Vergleich zu größeren stark benachteiligen können.

E. Resümee

Die Gesamtbetrachtung ergibt ein differenziertes Bild der Wirksamkeit staatlicher Regulierungsmechanismen, Selbstregulierungsmechanismen und ihrer Zwischenstufen. Sie lässt Schlüsse auf möglicherweise erfolgreichere Handlungsformen des Staates zu, die bisher kaum genutzt werden.

- Auf inhaltlicher Ebene ist eine staatliche Regulierung nur für nationale Angebote möglich; bei grenzüberschreitenden Sachverhalten stellt sich die klassische Eingriffsverwaltung als nahezu wirkungslos dar: Gesetzgebung wird zu rein symbolischer Tätigkeit, deren Scheitern schon im Vorhinein absehbar ist.
- Im Bereich der Haftung für Inhalte herrscht im Gegensatz zur Intention des TMG eine unübersichtliche Rechtsprechung. Die Haftung für Links und dementsprechend die Haftung von Suchmaschinen sind ungeklärt.
- Die Rechtsprechung hinsichtlich der Haftung für Inhalte basiert auf dem Gedanken, dass Provider für Dritte die Möglichkeit schaffen, Rechtsverletzungen zu begehen und dafür haftbar sind – einer Auffassung, die in der „realen“ Welt keine Entsprechung findet und als überzogen eingestuft werden kann. Hierdurch treten in Diskussionsforen erhebliche Gefahren für die Meinungsfreiheit auf. Dies gilt umso mehr, als die Rechtsprechung nicht unterscheidet, ob derjenige, der die Rechtsverletzung begangen hat, bekannt ist oder nicht.

  Das steht im eklatanten Widerspruch zu der eigentlichen Prämisse, dass es keinen Unterschied machen dürfe, ob Inhalte über das Internet oder auf herkömmliche Weise veröffentlicht werden.

Die derzeitige Rechtsprechung führt zu einer wesentlich schärferen Haftung lediglich technisch Beteiligter als es bei herkömmlichen Veröffentlichungen üblich ist.

- Die Rechtsprechung entfernt sich zusehends von dem technologiefreundlichen Ansatz aus dem TMG und grenzt eine Haftung durch schwer vorhersehbare Zumutbarkeitskriterien ein, statt nach den Kriterien des TMG, die sich an den technischen Funktionen der Akteure orientieren. Damit entsteht ein zunehmend schwer durchschaubares Dickicht an Entscheidungen, die das Gegenteil von Rechtssicherheit hervorrufen.
- Die Regelungen des JMStV sind an vielen Stellen bedenklich, der Kreis der Verantwortlichen wird zu weit gezogen. Die Anforderungen an Jugendschutzsysteme sind überzogen, die Vorschriften des JMStV verstoßen an einigen Stellen gegen die Verfassung. Dies ist umso bedenklicher als die mit ihm verfolgten Ziele nicht erreicht werden können; die vollständige Umsetzung würde aber zwangsläufig starke Einschränkungen bei legalen Inhalten mit sich bringen.
- Regulierte Selbstregulierung gilt im Bereich der Inhalte als Königsweg, allerdings bestehen grundsätzliche Bedenken in grundrechtsrelevanten Bereichen, da die Gefahr besteht, dass die Freiheitsbeschränkungen durch die Selbstregulierungsgremien deutlich rigoroser ausfallen, als es bei staatlichen Stellen der Fall wäre.
- Regulierte Selbstregulierung wurde im JMStV nur unvollkommen umgesetzt; in der derzeitigen Form ist der Erfolg fraglich.
- Nicht einmal der Gesetzgeber scheint dem Modell der Regulierten Selbstregulierung zu vertrauen, da zur Gewährung des Jugendschutzes weitgehende, zur Gewährleistung der Freiheiten der Anbieter hingegen keine Vorkehrungen getroffen wurden. Als Konsequenz ist ein Ausweichen der Anbieter in andere Länder mit weniger rigiden oder keinerlei entsprechenden Regelungen anzunehmen, womit dem Jugendschutz nicht gedient wäre.
- Die Sanktionierungsmöglichkeiten von Selbstregulierungsmechanismen auf inhaltlicher Ebene verpuffen in Zeiten eines Überangebots an Speicherplatz für E-Mails, dynamischen IP-Adressen und Anonymisierungsservices; dies könnte sich bei der Einführung fester IP-Adressen und der damit einhergehenden festen Bindung an bestimmte Geräte unter IPv6 ändern.
- Bei der Bekämpfung von Spam zeitigen staatliche Maßnahmen – mit Ausnahme bisher bisher nicht standardisierter technischer Verfahren – keinerlei Erfolg. Wünschenswert wären nicht erwiesenermaßen wirkungslose Verbote von Spam, sondern Maßnahmen, die den Schutz vor Spam legalisieren, statt ihn in einer rechtlichen Grauzone zu belassen.
- Im technischen Bereich haben sich Selbstbestimmungsmechanismen als staatlichen Planungen deutlich überlegen erwiesen. Auch bei kommerziellen Konflikten stellen sie eine gelingende, die

Funktionsfähigkeit des Internets in den Vordergrund stellende Entscheidungsstruktur dar. Dies gilt, wenngleich beschränkt, auch für das W3C. Eine Alternative der Wahrnehmung durch staatliche Stellen ist nicht erkennbar.

- Es fehlt auf allen Ebenen (IETF, IAB, ISOC, ICANN und W3C) an der Möglichkeit demokratischer Teilhabe. Deren Effektivität wäre allerdings angesichts der teilweise hoch spezialisierten Thematik fraglich. Eine gewisse, mittelbare demokratische Teilhabe können die GAC von IAB, ISOC und ICANN vermitteln.
- Die Konfliktlösungsmechanismen für Domainstreitigkeiten scheinen insbesondere in Fällen des Domaingrabbing gut zu funktionieren. Bei Streitigkeiten um den berechtigten Gebrauch von Domains benachteiligen sie allerdings den Beschwerdegegner, was unter Umständen aufgrund mangelnder Sanktionsmöglichkeiten dazu führen kann, dass Institutionen oder Unternehmen versuchen, Domains von Konkurrenten unrechtmäßig zu erlangen. Diese Ungleichheiten können jedoch ohne Nachteile für Verfahren wegen Domaingrabbings ausgeglichen werden.
- Im Bereich der Haftung für Rechtsverletzungen durch Domains hat die Rechtsprechung inzwischen geklärt, dass Registries nur in absoluten Ausnahmefällen für Verstöße ihrer Kunden haften. Die sich andeutende Haftung für Registrare sollte aus denselben Gründen abgelehnt werden.
- Die Unwirksamkeit traditioneller nationaler Handlungsformen kann die Staaten davon überzeugen, statt dieser die traditionellen Handlungsinstrumente des Netzes zu nutzen, bei denen es mehr auf Akzeptanz und Wirksamkeit sowie hinsichtlich einer Ausarbeitung von Vorschläge mehr auf Inhalte als auf verordneten Gehorsam ankommt. Lassen sich die Staaten – womöglich international koordiniert – auf die Regeln des Netzes ein, besteht die Möglichkeit der Einflussnahme.

F. Glossar

ASCII	Abkürzung für die American Standard Code for Information Interchange, den Basis-Zeichensatz für Computer. Hierbei wird jedem Zeichen eine Zahl zwischen 0 und 255 zugeteilt und diese Zahl wiederum in das Binärsystem umgerechnet, so dass Computer mit den Zeichen umgehen können. Es gibt jedoch auch andere Möglichkeiten der Codierung.
Blackhole-List	Ein Mittel zur Abwehr von Spam. Mailserver werden mit ihrer IP-Adresse in ein DNS-Register eingetragen, der empfangende Mailserver fragt diese DNS-Liste ab und nimmt von eingetragenen Servern versandte E-Mails nicht mehr an. Der Name resultiert daraus, dass die E-Mails wie in einem schwarzen Loch verschwinden.
Client	Bedeutet herkömmlich „Kunde“, wird im Computerbereich für Rechner in Netzwerken verwendet, die lediglich Daten empfangen und verarbeiten, jedoch keine Daten oder Dienste für andere Rechner zur Verfügung stellen. Ebenso wird von Client-Programmen gesprochen, wenn diese keine Daten zur Verfügung stellen; zu den wichtigsten gehören Mail- und FTP-Clients. Das Gegenstück eines Clients stellt ein Server dar.
DENIC e.G.	Abkürzung für DE-Network Information Center, die für die .de TLD zuständige Registry. Sie wird als eingetragene Genossenschaft der in Deutschland ansässigen Internet Access Provider betrieben.
IANA	Internet Assigned Number Authority. Sie verwaltet die IP-Nummern und das Domain Name System. Die IANA ist keine Organisation im herkömmlichen Sinne, sondern vielmehr eine Funktion, die von Organisationen wahrgenommen wird. Seit der Gründung der ICANN hat diese die Funktion der IANA übernommen.
ICANN	Abkürzung für Internet Corporation for Assigned Names and Numbers. Sie ist die Registry für gTLDs, hat die Verwaltung aber an je nach TLD unterschiedliche Unternehmen delegiert. Die ICANN ist ebenfalls zuständig für die Anerkennung nationaler Registries und die Verwaltung der IP-Nummern, die sie an vier für bestimmte Regionen zuständige Gesellschaften übertragen hat.

Registry	Die Stelle, welche die Registrierung von Domains durchführt und die Kontrolle über DNS Nameserver der jeweiligen TLD hat. Für die .de-Domain ist dies die DENIC e.G.
Registrar	Die Stelle, die im Kontakt mit dem Nutzer steht und eine Anmeldung an die Registry weiter gibt. Technisch kann es für jede Domain mehrere Registrare, aber nur eine Registry geben. Eine Registry kann auch gleichzeitig Registrar sein (z.B. DENIC e.G.), muss es aber nicht (z.B. ICANN).
RfC	Abkürzung für „Request for Comment“, Namen für Standards im Bereich des Internets. Sie werden zentral vom RfC-Editor gesammelt und veröffentlicht.
Server	Rechner, die Daten oder Dienste für andere Rechner zur Verfügung stellen, beispielsweise Mail-, Web-, oder FTP-Server. Das Gegenstück zu einem Server ist ein Client.
TCP/ IP	Es handelt sich hierbei eigentlich um ein Bündel verschiedener Protokolle, nach denen die Datenübermittlung im Internet durchgeführt wird, die aber einheitlich bezeichnet werden. Das Transport Control Protocol (TCP) ist für die Kontrolle der Datenübermittlung auf dem Weg vom Sender zum Empfänger zuständig. Dabei wird bei jeder Weiterleitung kontrolliert, ob die gesendeten Pakete angekommen sind; wenn dies nicht der Fall ist, fordert der letzte übermittelnde Server sie erneut an. Dadurch wird sichergestellt, dass alle Pakete ihren Weg vom Sender zum Empfänger finden und die Belastung des gesamten Netzes so gering wie möglich gehalten wird. Allerdings führt die Kontrolle auch zu einer langsameren Datenübermittlung.

TLD

Abkürzung für Top Level Domain. Man unterscheidet drei Arten von TLDs:

Generic TLDs (gTLD) sind die ursprünglichen, nicht nationalen TLDs mit den Endungen .com, .net, .org, .int sowie alle „sponsored TLDs“.

Country Code TLDs (ccTLDs) sind bestimmten Staaten zugeordnet; in diesen Staaten wird eine weitgehend nach eigenen Regeln arbeitende Stelle von der ICANN mit der Verwaltung der Domains beauftragt.

Sponsored TLDs (sTLDs) werden von Unternehmen (Sponsoren) vorgeschlagen und gegen die Zahlung einer Gebühr von der ICANN an diese delegiert. Die Registry ist in der Regel eine dritte Stelle. Der Sponsor entscheidet nur über die Nutzungsbedingungen. Es handelt sich in der Regel um stark zugangsbeschränkte Domains, die von Interessengruppen für ihre Mitglieder verwaltet werden.

Eine Zugangsbeschränkung war eigentlich bereits für die ursprünglichen gTLDs vorgesehen, konnte aber wegen des Ansturms auf diese nie effektiv kontrolliert werden und wurde deshalb nicht durchgesetzt.