Aiko Schilling

PRÄVENTIVE STAATLICHE KONTROLLMASSNAHMEN IM INTERNET UND IHRE VEREINBARKEIT MIT DEM EUROPARECHT

Universität Regensburg

Präventive
Staatliche Kontrollmaßnahmen
im Internet
und
ihre Vereinbarkeit
mit dem Europarecht

Dissertation

zur

Erlangung der Doktorwürde

der Rechtswissenschaftlichen Fakultät

der Universität Regensburg

von

Aiko Schilling

Vorwort

Regensburg, im März 2003

Die vorliegende Arbeit lag der juristischen Fakultät der Universität Regensburg im Wintersemester 2002/2003 als Dissertation vor.

Literatur, Rechtsprechung und Gesetzeslage konnten bis Herbst 2002 berücksichtigt werden.

Die Idee, mich mit diesem Thema zu beschäftigen, beruht darauf, dass ich auf dem Gebiet des Europarechts tiefergehende Einblicke gewinnen wollte. Zudem besaß ich ursprünglich von der Materie „Internet“ nur oberflächliche Kenntnisse. Daher schien es mir sinnvoll, sich mit diesem neuen zukunftsträchtigen Medium, insbesondere mit seiner Technik, intensiver auseinanderzusetzen. Für staatliche Kontrollmaßnahmen im Internet, die vorrangig aus präventiven Gründen angeordnet werden, habe ich mich vor allem deshalb interessiert, weil die ersten präventiven behördlichen Kontrollmaßnahmen allein mit der Androhung von Strafverfolgung, also ohne Rechtsgrundlage ergangen sind. Neben diesem nationalen Rechtsproblem gibt es im Zusammenhang mit den staatlichen Kontrollmaßnahmen auch zahlreiche europarechtliche Schwierigkeiten. Denn die behördlichen Kontrollmaßnahmen haben häufig – über die nationalen Grenzen hinweg – internationale Auswirkungen. Somit lag es nahe, ihre Vereinbarkeit mit dem Europarecht zu überprüfen.

Meinem Doktorvater, Herrn Prof. Dr. R. Arnold, möchte ich für seine vielseitige Unterstützung besonders danken. Darüber hinaus danke ich Herrn Prof. Dr. U. Steiner für die schnelle Erstellung des Zweitgutachtens.

Mein persönlicher Dank gebührt schließlich denen, vor allem meinen Eltern, die mir in den vergangenen Jahren in ganz individueller Art und Weise zur Seite gestanden und damit zum Gelingen dieser Arbeit beigetragen haben.

Aiko Schilling

Übersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis:

a.A.	anderer Ansicht
a.E.	am Ende
ABl.	Amtsblatt
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
AfP	Archiv für Presserecht
AG	Amtsgericht
Anm. d. Verf.	Anmerkungen des Verfassers
AOL	America Online
AöR	Archiv des öffentlichen Rechts
ArchivPT	Archiv für Post und Telekommunikation
ARPA	Advanced Research Project Agency
Art.	Artikel
ASCII	American Standard Code for Information Interchange
Az.	Aktenzeichen
BadWürttPolG	Baden-Württembergisches Polizeigesetz
BayGVBl.	Bayerisches Gesetz- und Verordnungsblatt
BayRS	Bayerische Rechtssammlung
BayVBl.	Bayerische Verwaltungsblätter
BayVwZVG	Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz
BB	Betriebs-Berater
BBS	Bulletin Board System
Bd.	Band
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
Bit	Basic Indissoluble Information Unit
BJs	Az. Ermittlungsverfahren des Generalbundesanwalts beim BGH
BR	Bundesrat
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
CR	Computer und Recht
d.h.	das heißt
DFN	Deutsches Forschungsnetz
DR	Decisions and Reports
DRiZ	Deutsche Richterzeitung
Ds	Az. Strafverfahren vor dem Einzelrichter
DVBl.	Deutsche Verwaltungsblätter
DVD	Digital Video Disc
E	Entscheidung der EKMR
EAGV	Vertrag zur Gründung der Europäischen Atomgemeinschaft
ECRL	E-Commerce-Richtlinie
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EGKSV	Vertrag über die Gründung der Europäischen Gemeinschaft für Kohle und Stahl
EGMR	Europäischer Gerichtshof für Menschenrechte
EGMRE	Entscheidung des Europäischen Gerichtshof für Menschenrechte
EGRC	Charta der Grundrechte der Europäischen Union

EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
Einl.	Einleitung
EKMR	Europäische Kommission für Menschenrechte
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten
endg.	endgefasst
engl.	Englisch
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EuGHE	Entscheidung des Gerichtshofs der Europäischen Gemeinschaften
EuGRZ	Europäische Grundrechte Zeitschrift
EuR	Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f./ff.	folgende
FAG	Fernmeldeanlagengesetz
Fn.	Fußnote
Frankfurt/M	Frankfurt am Main
FTP	File Transfer Protocol
GASP	Gemeinsame Außen- und Sicherheitspolitik
Gbit	Gigabit
gem.	gemäß
GG	Grundgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
GVBl.	Gesetz- und Verordnungsblatt
G-WiN	Gigabit-Wissenschaftsnetz
h.M.	herrschende Meinung
Hrsg.	Herausgeber
HS	Halbsatz
HTTP	Hyper Text Transfer Protocol
ICTF	Internet Content Task Force
IP	Internet-Protocol
IRC	Internet Relay Chat
IRCP	Internet Relay Chat Protocol
ISDN	Integrated Services Digital Network
ISO	International Standard Organisation
IT	Information Technologie
IuKDG	Informations- und Kommunikationsdienstegesetz
Js	Az. Ermittlungsverfahren in Strafsachen
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation und Recht
KOM	Dokument der Europäischen Kommission
LAN	Local Area Network
LG	Landgericht
LStVG	Landesstrafrecht- und Verordnungsgesetz
m.w.N.	mit weiteren Nachweisen
MDStV	Mediendienste-Staatsvertrag
MMR	Multimedia und Recht
n.F.	neue Fassung (eines Gesetzes)
NET	Network
NFS	Network File System
NJW	Neue Juristische Wochenschrift
NJW-CoR	Computerreport der Neuen Juristischen Wochenschrift
NNTP	Network News Transfer Protocol
Nr.	Nummer
NSF	Natinal Science Foundation
NStZ	Neue Zeitschrift für Strafrecht

o.V.	ohne Verfasser
OLG	Oberlandesgericht
ONC	Open Network Computing
OSI	Open Systems Interconnection
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PAG	Polizeiaufgabengesetz
PICS	Platform for Internet Content Selection
PJZS	Polizeiliche und justitielle Zusammenarbeit in Strafsachen
PSTN	Public Switched Telephone Network
Rdnr.	Randnummer
REF	Référence
Rs.	Rechtssache
RStV	Rundfunk-Staatsvertrag
RTkomm	Zeitschrift für das Recht der Telekommunikation und das Recht der elektronischen Medien
S.	Seite
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsPRG	Sächsisches Privatrundfunkgesetz
Slg.	Sammlung
SMTP	Simple Mail Transfer Protocol
StGB	Strafgesetzbuch
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
u.a.	und andere
u.U.	unter Umständen
UNTS	United Nations Treaty Series
URL	Uniform Resource Locator
VA	Verwaltungsakt
Vand. J. Transnat. L.	Vanderbilt Journal of Transnational Law
verb.	verbunden
vgl.	vergleiche
VwVfG	Verwaltungsverfahrensgesetz
W3C	World-Wide-Web-Consortium
WBl.	Wirtschaftsrechtliche Blätter
WiN	Wissenschaftsnetz
WRP	Wettbewerb in Recht und Praxis
WWW	World-Wide-Web
Yb	Yearbook of the European Commission and the Court of Human Rights
z.B.	zum Beispiel
z.T.	zum Teil
ZEuP	Zeitschrift für Europäisches Privatrecht
Ziff.	Ziffer
ZUM	Zeitschrift für Urheber und Medienrecht
ZustV-MedStV	Zuständigkeitsverordnung Mediendienste Staatsvertrag

A. Einleitung

Das Internet gewinnt seit Mitte der neunziger Jahre zunehmend an Bedeutung. Der einzigartige Vorteil des Internets besteht darin, dass es wie keine andere Technologie multimediales Arbeiten auf vernetzten Rechnern, überall auf der Welt, zu jeder Zeit und faktisch durch jeden Teilnehmer, der Computer, Modem und Telefonanschluß besitzt, ermöglicht. Durch die massenhafte Verbreitung von Computern und das unaufhaltsame Zusammenwachsen, der sogenannten Konvergenz, von Informationstechnologie, Telekommunikation und Fernsehtechnologie, hat das Internet nicht nur starke Auswirkungen auf die Wirtschaft, sondern auch auf die Gesellschaft. Nicht umsonst wird schon jetzt von der Entstehung einer „Informationsgesellschaft" gesprochen.[1] Denn mittels des Internets wird die weltweite Kommunikation sowie der Informationsaustausch revolutioniert. So ermöglicht das Internet die gezielte Suche nach Informationen. Interessengruppen können sich im Netz treffen und sich austauschen. Hierdurch sind mittlerweile zahlreiche Diskussionsforen entstanden, an denen sich jederzeit die jeweiligen Netzbesucher beteiligen können. Vor allem in den Chat-Foren und Newsgroups[2] findet ein derartiger Meinungsaustausch vermehrt statt.

Auch die wirtschaftliche Bedeutung des Internets ist gewaltig.[3] Dabei liegt der wirtschaftliche Schwerpunkt nicht allein darin, dass das Internet eine völlig neue Art der Kommunikation ermöglicht und die Anbieter dieses Kommunikationsmittels von der zunehmenden Beliebtheit des Internets profitieren. Viel gravierender für die Wirtschaft wirkt sich der indirekte bzw. direkte elektronische Geschäftsverkehr aus.[4] Der elektronische Geschäftsverkehr umfasst zahlreiche unterschiedliche Tätigkeiten wie beispielsweise den elektronischen Handel mit Waren und Dienstleistungen, Online-Lieferungen digitalen Inhalts, elektronische Geldüberweisungen, den elektronischen Aktienhandel, kommerzielle Auktionen sowie Direktmarketing beim Verbraucher.

Neben der Vielzahl von Vorteilen, die das Internet bietet, bereitet es andererseits auch rechtliche Probleme. Gerade weil das Internet umfangreiche Anwendungsmöglichkeiten besitzt und es sich um ein sehr junges Medium handelt, kann es mit einfachen Mitteln missbraucht werden. Dabei sind die einzelnen Missbrauchsformen sehr unterschiedlich: So können in rechtswidriger Weise fremde Daten ausspioniert und manipuliert werden. Auch wettbewerbsrechtliche Probleme stellen sich beim Umgang mit dem Internet. Neben beleidigenden Inhalten beschäftigt vor allem die Verbreitung rechtswidriger Inhalte

---

1 Sieber, „Computerkriminalität und Informationsstrafrecht", CR 1995, 100 ff.

2 Vgl. bezüglich dieser Begriffe die Ausführungen unten unter B. 1. Teil. I. 3. b. und c.

3 So wird für das Jahr 2004 allein beim E-Commerce der Verbraucher ein Umsatz von 425 Milliarden US-Dollar erwartet. Das wäre verglichen mit dem diesjährigen Umsatz eine Vervierfachung. Vgl. insoweit: o.V. „Es wächst und wächst ...", PC Magazin 2/2002 S. 12.

4 Mitteilung der Kommission, „Europäische Initiative für den elektronischen Geschäftsverkehr", KOM(97)157 endg.

in elektronischen Informations- und Kommunikationsdiensten Öffentlichkeit, Justiz und Gesetzgeber in zunehmendem Maße. In Deutschland liegt der Schwerpunkt der rechtshängig gewordenen Fälle sowie der wissenschaftlichen Diskussion auf der Verbreitung von harter Pornographie, nationalsozialistischer Propaganda,[5] radikalen politischen Ansichten und terroristischen Inhalten.[6] Für Aufsehen sorgten beispielsweise im Jahre 1996 die Seiten des in Kanada ansässigen Neonazis Ernst Zündel[7] bzw. die von Holland aus in das Netz eingestellten linksradikalen Texte der Zeitschrift „Radikal", Ausgabe Nr. 154 und deren angeordnete Sperrung.[8] Auch das CompuServe-Urteil des AG München[9], das einen kinderpornographischen Hintergrund besitzt, wurde in Fachkreisen heftig diskutiert. Dagegen betreffen die einschlägigen Gerichtsentscheidungen im Ausland, speziell im angloamerikanischen Bereich, hauptsächlich Urheberrechtsverletzungen und rufschädigende Behauptungen.[10]

Wie sich schon aus der Sperrung der Internet-Seiten von Zündel und der Zeitschrift „Radikal" entnehmen lässt, gibt es technische Mittel und Wege, dem Missbrauch des Internets entgegenzutreten. Als staatliche Gegenmaßnahmen werden häufig die Sperrung und Löschung von strafbaren bzw. rechtswidrigen Inhalten vorgeschlagen. Daneben bestehen auch rechtliche Möglichkeiten, missbräuchliches Handeln im Internet einzudämmen. Hier sind als nationale Vorschriften bzw. Eingriffsbefugnisse die Telekommunikations- und Mediarechte, namentlich das Telekommunikationsgesetz (TKG)[11], das Teledienstegesetz (TDG)[12], der Mediendienste-Staatsvertrag (MDStV)[13] sowie das allgemeine Polizei- und Sicherheitsrecht zu nennen. Bei den einzelnen Sperr- bzw. Löschmaßnahmen ist allerdings problematisch, dass das Internet keine nationalen Grenzen kennt, sondern eine weltumspannende Vernetzung aufweist. Dabei ist jedoch auffällig, dass innerhalb dieses globalen Netzes „Cyber-Inseln" zu erkennen sind, die sich in die einzelnen Wirtschaftsräume USA, Europa, Asien aufspalten lassen. Dies liegt vor allem an den unterschiedlichen Kultur- und Sprachkreisen. Ein weiterer Grund für

---

5 Allein im Jahr 2001 wurden insgesamt ca. 1000 Seiten mit rechtsradikalen Inhalten entdeckt.

6 Wie gefährlich bestimmte Inhalte im Netz sein können, zeigen die Ereignisse in New York am 11. September und der Amoklauf von Erfurt. So wurde das Internet vom Terrornetzwerk „Al Qaida" für die Vorbereitung ihrer Anschläge missbraucht. Auch zum Verbreiten der extremen religiösen Ansichten wird das Internet von dieser Terrororganisation genutzt.
Der Amok-Schütze aus Erfurt hat sich über das Internet äußerst brutale Computerspiele besorgt. Diese Spiele sind zwar in Deutschland verboten, über das Netz kann jedoch problemlos – meist sogar kostenlos – auf diese oft im Ausland befindlichen Daten zugegriffen werden. Es wird vermutet, dass diese sehr realistisch gestalteten Computerspiele mitursächlich für die Tat des Amok-Schützen gewesen sind.

7 Vgl. hierzu die Ausführungen in Fn. 177.

8 Mayer, das Internet im öffentlichen Recht, S. 63; vgl. auch die Ausführungen in Fn. 171.

9 Urteil des AG München vom 28.05.1998 – Az.: 8340 Ds 465 Js 173158/95, NStZ 1998, 518 ff.; vgl. auch die Ausführungen in Fn. 178.

10 Vgl. dazu den Überblick über ausländische Fälle bei Bortloff, GRUR Int. 1997, 387 ff.

11 BGBl. I 1996, 1120.

12 BGBl. I 1997, 1870.

13 BayGVBl 1997, 226.

diese unsichtbaren, virtuellen Grenzen besteht auch darin, dass es sehr schwer fällt, sich auf einheitliche globale Regelungen für das Internet zu einigen. Selbst im vereinten Europa gibt es nur vereinzelt Regelwerke, die das Internet betreffen. Vielmehr wendet jeder Mitgliedstaat – soweit vorhanden – seine eigenen nationalen Vorschriften auf das Internet an. Dies gilt auch für Deutschland.

Wegen der weltweiten Vernetzung und der damit verbundenen globalen Präsenz der einzelnen Netz-Benutzer, der sogenannten „Ubiquität", wird durch nationale Kontrollmaßnahmen häufig in fremde Rechtskreise eingegriffen. Neben der Verletzung fremder Hoheitsrechte einzelner Staaten kann aber auch supranationales Recht von den Sperr- und/oder Löschanordnungen betroffen sein. Insbesondere das Europarecht kommt hierfür in Frage. Da das Europarecht mehr und mehr an Bedeutung gewinnt, ist es von besonderer Wichtigkeit, herauszufinden, wie sich staatliche Kontrollmaßnahmen aufgrund von nationalen Eingriffsermächtigungen europarechtlich auswirken können.

Gegenstand der vorliegenden Arbeit ist es deshalb, dieser Problematik, nämlich die Kollision von nationalem Recht und Europarecht bei der staatlichen Anordnung, Internet-Seiten zu sperren bzw. zu löschen, nachzugehen. Dabei sollen ausschließlich präventiv motivierte staatliche Kontrollmaßnahmen untersucht werden. Gemeint sind damit also Maßnahmen, die nicht aufgrund der Strafverfolgung ergehen, sondern vielmehr die Gefahrenabwehr bezwecken.[14]

Für eine anschauliche Darstellung der angesprochenen Thematik ist es unerläßlich, zunächst die Funktionsweise des Internets in technischer Hinsicht zu erläutern. Anschließend sollen die technischen Möglichkeiten von Sperr- und/oder Löschmaßnahmen bezüglich der jeweiligen Provider vorgestellt werden. Dies ist Voraussetzung, damit die anschließende Behandlung des eigentlichen rechtlichen Problems verständlich wird. Des weiteren geht die Arbeit auf die einzelnen relevanten Telekommunikationsgesetze ein und grenzt sie voneinander ab.[15] Daraus ergeben sich die für die Kontrollmaßnahmen relevanten nationalen Rechtsgrundlagen. Die darauf gestützten staatlich angeordneten Sperrungen und/oder Löschungen werden dann auf die Vereinbarkeit mit dem bestehenden Europarecht, soweit es anwendbar ist, überprüft.

---

[14] Als Beispiel soll hier eine Sperrverfügung der Bezirksregierung Düsseldorf vom 13.02.2002, http://www.bezreg-duesseldorf.nrw.de/cat/pdf/39sperrverf_022002.pdf (zuletzt abgerufen am 21.06.2002), genannt werden. Sie hatte zum Ziel, dass ein in Deutschland ansässiger Provider den Zugang zu rechtsradikalen Seiten in den USA sperrt. Vgl. hierzu auch Greiner, „Sperrungsverfügungen als Mittel der Gefahrenabwehr im Internet", CR 2002, 620 ff.

[15] Während der Erstellung dieser Arbeit kam es zu einer Gesetzesänderung durch die Umsetzung einer EG-Richtlinie. Dies hatte zur Folge, dass sich das TDG geändert hat. Für dieses neue Gesetz gibt es nur vereinzelt Literatur. Deshalb hat sich der Bearbeiter entschieden, sowohl auf das alte TDG als auch auf das neue TDG und ihren Rechtsproblemen einzugehen. Da das neue Gesetz nur in bestimmten Bereichen geändert worden ist, gelten die meisten Aussagen zum ehemaligen TDG fort. Die Unterschiede zwischen den beiden Gesetzen können ebenfalls durch die Bearbeitung des alten TDG besser veranschaulicht werden. Deshalb wird zunächst an geeigneter Stelle auf das alte TDG eingegangen und im Anschluss daran die neue Gesetzeslage aufgezeigt. Des weiteren findet später auch eine Untersuchung der umgesetzten EG-Richtlinie selbst statt.

B. Hauptteil

1. Teil - Einführung

I. Funktionsweise des Internets

Um die rechtliche Problematik einer Kontrolle im Internet vollständig erfassen zu können, ist es wichtig, die Technik des Internets zu verstehen. Denn das Recht des Internets richtet sich sehr stark nach der jeweils vorhandenen Technik. Daneben ist auch der geschichtliche Hintergrund für ein umfassendes Verständnis des Internets von Bedeutung. Aus diesem Grund wird zunächst auf die Geschichte des Internets eingegangen, bevor seine technische Seite behandelt wird.

1. Historische Grundlagen

Ende der 60er Jahre wurde vom amerikanischen Verteidigungsministerium das sogenannte „ARPA-Projekt“ (Advanced Research Project Agency) gegründet.[16] Die Konzeption zu diesem Projekt stammt von dem Amerikaner Paul Baran.[17] Es verfolgte zur damaligen Zeit nur ein wichtiges militärisches Ziel: Die Übermittlung von Abschussinstruktionen des Kontrollzentrums zu den Basen ballistischer Raketen auch – und vor allem – dann zu ermöglichen, nachdem ein gegnerischer atomarer Angriff einen Teil der Kommunikationsnetze zerstört hatte.[18] Dieses Ziel, einen Datenaustausch durchführen zu können, obwohl gewisse Teilbereiche des Kommunikationsnetzes unbrauchbar geworden sind, wurde sehr schnell auf den Zugriff und die Benutzung des gesamten EDV-Potentials der Vereinigten Staaten ausgeweitet. Das neu erschaffene Netz wurde „ARPANET“ (Advanced Research Project Agency Network) genannt.[19] Die wichtigste Neuerung an diesem Netz bestand darin, dass man nicht mehr – wie bis dahin üblich – auf leitungsorientierte Datenübertragung, d.h. auf den Aufbau einer physikalischen Verbindung zwischen Sender und Empfänger einer Nachricht, setzte. Statt dessen wurden Nachrichten in einzelne Datenpakete zerlegt und diese Pakete unabhängig voneinander und je nach Verfügbarkeit einer Verbindung von einem „Knotenrechner“[20] so lange zum nächsten weitergeleitet, bis die Pakete beim Empfänger ankamen.[21] Dadurch konn-

---

16 Griese/Sieber in: Hilty (Hrsg.), Information Highway, S. 43 ff.; o.V. „Es wächst und wächst ...“, PC Magazin 2/2002 S. 12.

17 Köhler/Arndt, Recht des Internet, 2. Auflage, S. 2 Rdnr. 6; Tanenbaum, Computernetzwerke, 3. Auflage, S. 63 ff.

18 Strömer, Online§Recht, 2. Auflage, S. 3; Kyas, Internet, S. 35 ff.

19 Hance, Internet-Business & Internet-Recht, S. 45.

20 Diese werden auch „Router“ genannt. Vgl. hierzu Fn. 64.

21 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 15.

te eine flexible Struktur geschaffen werden, die unabhängig von den benutzten Computern war.

1969 bestand das ARPANET lediglich aus vier Knotenrechnern.[22] Sehr schnell fand dann der Übergang von der rein militärischen hin zu einer auch zivilen Nutzung statt. Bis 1977 wurden insgesamt 111 Knotenrechner installiert. Parallel entstandene Netze – wie das sogenannte „USENET“[23] – sind in die vorhandene Struktur des ARPANET eingearbeitet worden. Als die National Science Foundation (NSF) das TCP/IP-Protokoll[24] bei der Errichtung von fünf großen Rechenzentren auswählte, wurde die Benutzung dieses Protokolls im Jahr 1984 verstärkt.[25] Gleichzeitig mit der Einführung des TCP/IP-Protokolls fand auch die Teilung des Netzes in einen militärischen (MILNET) und in einen der zivilen Forschung vorbehaltenen Teil (ARPANET) statt. [26]

Aus diesem ARPANET entwickelte sich in den folgenden Jahren das Internet. Die zivile Nutzung beschränkte sich dabei bis in die 80er Jahre hauptsächlich auf den Datenaustausch vornehmlich durch „E-Mails“[27] und das gemeinsame Nutzen kostbarer Rechenleistung durch Universitäten und ihre Mitarbeiter.[28] Denn jedes große Universitätszentrum schloss sich dem durch die NSF eingerichteten Netz an, das die Rolle einer Art Wirbelsäule (Backbone)[29] für die Gesamtheit des Verkehrs auf diesen Unternetzen übernahm. Seitdem war es möglich, auf jede Stelle des Netzes von jedem angeschlossenen Universitätsort zuzugreifen.[30]

Eine kommerzielle Nutzung des Internets fand hingegen zunächst nicht statt. Dies war ja auch bei der Schaffung der Netze anfänglich nicht geplant gewesen. Durch die rasante Entwicklung der Computer- und Kommunikationstechnologien wurden allerdings

---

22 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 4.

23 In der ursprünglichen Bedeutung ist das Usenet ein reines NEWS-Netz gewesen, war also nur für öffentliche Nachrichten bestimmt. Mittlerweile wird der Begriff „Usenet“ aber mehr im Sinne eines weltweiten Mail- und Newsnetzes verwendet, dessen administrative Ebenen unter anderem das EU-Net umfassen. Das Usenet ist nicht mit dem Internet gleichzusetzen. Es ist vielmehr eine Art riesiges Bulletin Board (zu diesem Begriff vgl. unten unter Fn. 142), das natürlich auch über das Internet erreichbar ist. Vgl. hierzu Kyas, Internet, S. 36 f.

24 Der Begriff TCP/IP-Protokoll wird später ausführlich unter B. 1. Teil. I. 2. b. cc. behandelt. Allgemein sind Protokolle im Internet nichts anderes als Vereinbarungen, wie man miteinander kommunizieren muss. Wenn ein „normaler“ Brief zu adressieren ist, wird auch vorgeschrieben, welche Angaben notwendig sind, damit er beim Empfänger ankommt. Solche Regeln gelten ebenfalls im Internet. Sie werden lediglich Protokolle genannt. Vgl. hierzu Herbert, Das Internet Praxisbuch, S. 6.

25 Dies ist der Grund, warum das TCP/IP-Protokoll bis heute im Internet fast ausschließlich benutzt wird.

26 Strömer, Online§Recht, 2. Auflage, S. 4.

27 Unter den Begriff „E-Mail“ wird jede Art von elektronischer Post gefasst. Vgl. hierzu ausführlich unten B. 1. Teil. I. 3. a.

28 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 15.

29 Der englische Begriff für die Wirbelsäule lautet „backbone“. Der Begriff „Backbone“ wird deshalb im Fachjargon für den Hauptstrang in einem Netzwerkverbund verwendet. Dabei stellt der Backbone häufig einen Rechner dar, der unter anderem definitiv feststellen kann, ob es sich um eine gültige oder ungültige Netzadresse handelt. Vgl. zu diesem Begriff auch die Fn. 63.

30 Hance, Internet-Business & Internet-Recht, S. 46.

immer leistungsfähigere Rechenzentren und Datenübertragungsleitungen errichtet. Als dann 1995 in den USA die staatlichen Subventionen für den Telekommunikationssektor ausliefen und die Hauptknotenpunkte zum Internet von mehreren amerikanischen Telefongesellschaften übernommen wurden, nahm auch die kommerzielle Nutzung des Internets stetig zu.

Zu einem internationalen Netzwerk wurde das Internet jedoch erst, als auch außerhalb der USA Internet-Zugänge geschaffen worden sind. In Europa fand dies zuerst in Skandinavien zu Beginn der 80er Jahre mit der Errichtung des NORDUnet statt. Das 1982 gegründete EUnet stellte nur einen vom Internet getrennten Ableger des amerikanischen USENET dar.[31] Eine wirkliche Integration Europas in das Internet wurde Anfang der 90er Jahre dadurch ermöglicht, dass die beiden europäischen Backbones[32] EBONE und EuropaNET errichtet worden sind. Ein wichtiger europäischer Meilenstein für das Internet war zudem, dass Ende der 80er Jahre am Europäischen Kernforschungszentrum (CERN) in Genf die technischen Grundlagen für den Internet-Dienst World-Wide-Web (WWW) gelegt wurden.[33] Welche Bedeutung das WWW mittlerweile hat, wird allein durch die Tatsache deutlich, dass das WWW dem Internet oft gleichgesetzt wird. Denn das WWW besitzt den großen Vorteil, sämtliche Internet-Dienste miteinander verknüpfen zu können.[34]

In Deutschland gehen die Anfänge des Internets auf das Jahr 1984 zurück. Durch die Gründung des Vereins zur Förderung eines Deutschen Forschungsnetzes (DFN) und dem Aufbau des sogenannten „WiN-Netzes“[35], das über ein sogenanntes „Gateway“[36] zum Internet verfügte, konnte Deutschland in das Internet eingebunden werden. Zweck dieser Maßnahmen war es, die Internet-Dienste für die Wissenschaft und Forschung nutzbar zu machen.

Seit Beginn der 90er Jahre wird das Internet in zunehmendem Maße auch von der breiten Öffentlichkeit genutzt. Die Zahl der Anbieter von Internet-Dienstleistungen steigt

---

31 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 15.

32 Vgl. Fn. 29.

33 Köhler/Arndt, Recht des Internet, Rdnr. 8; das CERN gründete 1994 das World-Wide-Web-Consortium (W3C), das bestimmte Empfehlungen zur Standardisierung im Netz abgibt, Mayer, „Selbstregulierung im Internet: Institutionen und Verfahren zur Setzung technischer Standards“, K&R 2000, 13, 18.

34 Vgl. hierzu die Ausführungen unten unter B. 1. Teil. I. 3. g.

35 Die Buchstaben WiN sind eine Abkürzung für das Wort „Wissenschaftsnetz“. Das Wissenschaftsnetz ist ein seit Juni 1990 in Deutschland bestehendes Netz mit rund 450 Anschlüssen, das exklusiv Wissenschaft und Forschung zur Verfügung steht. Es wird von der Deutschen Telekom betrieben. Zunächst basierte das WiN-Netz auf X.25-Technik. Im September 1998 wurde das G-WiN (Gigabit-WiN) in München in Betrieb genommen. Es kann mit 2,34 Gbit/s übertragen.

36 Mit einem Gateway können unterschiedliche Rechnersysteme miteinander verbunden werden, die im Prinzip nichts miteinander gemein haben. Es erfüllt die Aufgaben eines Routers (vgl. unten unter Fn. 64) und führt darüber hinaus die Umwandlung von Protokollen und Codes durch. Ein Gateway, für den regelmäßig ein eigener Computer verwendet wird, funktioniert sozusagen als Dolmetscher zwischen den einzelnen Netzwerken, die eine unterschiedliche Sprache verwenden. Vgl. ausführend Eckert/Göbell/Matejka/Zitterbart in: Schneider (Hrsg.), Lexikon Informatik und Datenverarbeitung, 4. Auflage, S. 352.

unaufhörlich an. Dabei reicht das Spektrum von regionalen gemeinnützigen Vereinen bis hin zu großen nationalen und internationalen Online-Diensten. Eigene private Web-Seiten[37] bzw. E-Mail-Adressen[38] sind nunmehr alltäglich geworden. Ein Zugriff auf das Internet ist mittlerweile in den Industrienationen für jeden möglich.
Entgegen der ursprünglich von den Pionieren des Internets verfolgte Linie hat die anfänglich verbotene kommerzielle Nutzung in den letzten Jahren ein stetiges Wachstum verbucht. Dieses Wachstum ist nunmehr exponentiell geworden. Es beinhaltet heute weltweit mehr als 25000 Netze[39] und die Anzahl seiner Benutzer liegt bei momentan geschätzten 200 Millionen[40] gegenüber 40 Millionen im Jahre 1997[41].[42] Diese Zahlen zeigen, dass das Internet kein statisches Etwas ist, sondern nicht aufhört, sich weiterzuentwickeln. Ein Verlauf oder gar das Ende dieser rasanten Entwicklung ist auch in naher Zukunft noch nicht abzusehen.[43]

2. Technische Grundlagen

a. Das Internet

Das „Internet“ selbst ist nicht, wie der Name suggeriert, ein weltumspannendes, einheitliches Computersystem oder gar ein weltweiter Anbieter von Computerdiensten.[44] Auch die gängige Vorstellung, dass das „Internet“ einen Superrechner irgendwo auf der Welt besitzt, in dem alle Daten gespeichert und jederzeit abrufbar sind, muss revidiert werden. Das „Internet“ ist vielmehr die schlagwortartige Bezeichnung für eine Sammlung technischer Standards, die den weltweit vorhandenen Computern jeglicher Bauart die Kommunikation über jede Art von Datenleitung erlauben.[45] Beim „Internet“ handelt es sich also nicht um ein einheitliches Computernetz, sondern lediglich um eine Definition einheitlicher technischer Standards[46] für die Datenübertragung und den Datenaustausch. Vereinfacht ausgedrückt stellt das Internet nichts anderes als eine globale Vernetzung aller Computer und Einzeldienste dar, die in diesem Netz integriert sind.[47] Das Beson-

---

37 Vgl. hierzu die Ausführungen unter B. 1. Teil. I. 3. g.
38 Vgl. insoweit unter B. 1. Teil. I. 3. a.
39 Hance, Internet-Business & Internet-Recht, S. 46.
40 Aufgrund der dezentralen Struktur des Internet kann die wirkliche Zahl nur grob geschätzt werden.
41 Vgl. o.V., DIE ZEIT Nr. 18 vom 25.4.1997, S. 22.
42 Laut der auf Internet-Statistiken spezialisierten Marktforschungsfirma Matrix.Net wurde am 02.11.2000 der 100 Millionste Rechner an das Internet angeschlossen. In über 150 Ländern gibt es bereits Internet-Zugänge. Vgl. auch Klußmann, Lexikon der Kommunikations- und Informationstechnik, 3. Auflage, S. 506.
43 Ein ausführlicher, chronologischer Überblick über die Entstehungsgeschichte des Internets ist bei Klußmann, Lexikon der Kommunikations- und Informationstechnik, 3. Auflage, S. 494 ff. zu finden.
44 Mayer, Das Internet im öffentlichen Recht, S. 31.
45 Mayer, Das Internet im öffentlichen Recht, S. 31.
46 Im Fachjargon spricht man hierbei von sogenannten „Protokolle“. Vgl. dazu Fn. 24.
47 Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 5 f.

dere an dieser Vernetzung ist allerdings, dass entweder dieselbe oder eine ähnliche Computersprache[48] überall auf der Welt gesprochen wird. Dies hat im Ergebnis zur Folge, dass eine unbegrenzte globale Kommunikation zwischen den Computern stattfinden kann. Dabei sind wahlweise einzelne lokale, regionale und auch nationale Netzwerke an den Gesamtverbund „Internet" angeschlossen, um den gewünschten Datenfluss über den gesamten Erdball zu ermöglichen.[49] Deshalb wird nicht umsonst das „Internet" häufig als das „Netzwerk der Netzwerke" bezeichnet.[50] Jedes dieser Einzelnetze hat eigene Regeln, die den Zugang zum Netz und das im Netz Erlaubte betreffen; alle diese Netze unterwerfen sich aber ihrerseits den Regeln des Gesamtnetzes.

Daneben wird das „Internet" auch als eine institutionalisierte Form der Organisation dieses weltweiten Datenaustausches verstanden.[51] Dieser Organisationsbegriff darf aber nicht als ein geordneter hierarchischer Aufbau des Internets interpretiert werden. Vielmehr ist damit gemeint, dass das „Internet" die Funktion hat, die bereits vorhandenen Standards des Datenverkehrs aufrechtzuerhalten und neue Standards auf diesem Gebiet zu schaffen, um die Schnelligkeit des Datenflusses zu verbessern.[52] Damit dies gewährleistet wird, sind verschiedene nationale und internationale Organisationen, Gruppierungen und Vereine dafür gegründet worden. Neben der Standardisierung und Weiterentwicklung der mit dem Internet zusammenhängenden technischen Fragen haben sie zudem zur Aufgabe, das „Internet" in gewisser Weise zu ordnen.[53]

---

48 Dies geschieht häufig in der Form des TCP/IP-Protokolls. Vgl. insoweit unten unter B. 1. Teil. I. 2. b. cc.

49 Vgl. hierzu auch Dern, The Internet Guide For New Users, S. 16:
„The Internet today is a worldwide entity whose nature cannot be easily or simply definied. From a technical definition, the Internet is <<the set of all interconnected IP networks>> - the collection of several thousand local, reginal, and global computer networks interconnected in real time via TCP/IP Internetworking Protocol suite."

50 Hance, Internet-Business & Internet-Recht, S. 46; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 14; Hoeren, Rechtsfragen des Internet: Ein Leitfaden für die Praxis, Rdnr. 1.

51 Mayer, Das Internet im öffentlichen Recht, S. 31.

52 Strömer, Online§Recht, 2. Auflage, S. 5 f.

53 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 19; so regeln sie beispielsweise auch die Vergabe von „domain-Adressen" und „Portnummern".
Der englische Begriff „domain" bezeichnet in Kommunikationsnetzen auf Basis von TCP und IP (hierzu später unter B. 1. Teil. I. 2. b. cc.) einen durch ein spezielles System ermöglichten und einzelnen, streng abgegrenzten adressierbaren Bereich. Mehrere domains können hierarchisch angeordnet werden, so dass gezielt in der Hierarchie unten befindliche domains adressiert werden können, etwa durch eine mit Punkten getrennte Auflistung der domains (und sub-domains), die von der obersten Ebene durchlaufen werden müssen um zur gewünschten untersten zu gelangen. Vgl. ausführlich und mit Nennung der wichtigsten Top-Level-domains in: Klußmann, Lexikon der Kommunikations- und Informationstechnik, 2. Auflage, S. 213 f. Mit Hilfe der Portnummer können Datenpakete bestimmten Servern zugeordnet werden. Vgl. insoweit unten unter B. 1. Teil. I. 2. b. cc. (2).

b. Datentransport im Internet

Das Ziel von Computernetzen besteht in der Übertragung von Daten.[54] Letztendlich ist es Sinn und Zweck des Internets, einen umfassenden Datenaustausch zu ermöglichen. Demnach wird das Internet nur dann im vollen Umfang verständlich, wenn der Vorgang des Datentransports nachvollziehbar ist. Insbesondere die Anwendung des schon vorher mehrmals erwähnten TCP/IP-Protokolls und die Rolle der Provider im Internet sind besonders wichtig, um die rechtlichen Probleme und eine technische Kontrolle des Internets verstehen zu können.

aa. Allgemeines zum Datentransport im Internet

Das Internet verbindet unterschiedliche Rechnersysteme miteinander. Diese werden je nach Funktion als „Server“[55] oder als „Client“[56] bezeichnet, wobei jedes Computersystem im Netz gleichzeitig Server und/oder Client sein kann.[57] Die Begriffe richten sich danach, woher die Daten kommen und wohin sie geschickt werden. Der Server ist regelmäßig der Absender, der Client der Empfänger der Daten.[58]

Damit Computernetze ihre Aufgabe der Datenübertragung zwischen Server und Client erfüllen können, sind – neben den zu verbindenden Computersystemen und der Software – rein physikalische Übertragungswege sowie Verbindungsrechner (die oben bereits erwähnten Knotenrechner) nötig.[59] Das Internet setzt sich somit „hardwaremäßig“[60] – vereinfacht dargestellt – aus Übertragungsleitungen, Knotenrechnern und Endgeräten zusammen. Die Übertragungsleitungen zwischen den Computersystemen sind meist Kupfer- oder Glasfaserkabel. Mittlerweile gibt es aber auch in zunehmendem Maße drahtlose Verbindungsmöglichkeiten. Beispielsweise werden Daten immer häufiger

---

54 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 588.

55 Der Begriff Server bezeichnet kein spezielles Computersystem, sondern bezieht sich auf die jeweilige Anwendersoftware, die bestimmte Dienste, also Daten, zur Verfügung stellt. Weil diese Software regelmäßig auf speziellen, leistungsfähigen Computersystemen läuft, wird die Hardware selbst auch Server genannt.
Wichtig für den Begriff Server ist die Tatsache, dass alle Internet-Dienste nach dem Client-Server-Prinzip funktionieren: Ein Client ist ein Programm, das ein anderes Programm, den Server, um einen Dienst bittet. Mit der Eingabe eines Kommandos aktiviert der Nutzer auf seinem Computer das Client-Programm, das nunmehr vom Server (dem Computer des Content- oder Service-Providers) Informationen abruft. Der Server übermittelt daraufhin diese Information zur Nutzung. Vgl. hierzu auch Kröger/Moos, „Mediendienst oder Teledienst“, AfP 1997, 675, 679.

56 Die Client-Software ist das Gegenstück zur Server-Software. Sie ist für den Empfang und die Verarbeitung der Daten vom Server verantwortlich. Da beim Computersystem des Client meistens nur Client-Software zu finden ist, werden auch dessen Hardwarekomponenten unter den Begriff Client gefasst.

57 Weiterführend hierzu Inmon, Client/Server-Anwendungen, S. 2 ff.

58 Sehr anschaulich bei Köhntopp/Köhntopp in: „Datenspuren im Internet“, CR 2000, 248, 250 ff.

59 Vgl. hierzu Mayer, Das Internet im öffentlichen Recht, S. 44 ff.

60 Mit dem Begriff „Hardware“ werden sämtliche tatsächlich physikalisch vorhandenen Geräte, Bauteile, Maschinen etc. bezeichnet. Das sprachliche Gegenstück hierzu ist die „Software“. Von ihr werden die Programme erfasst, die in einem Computersystem laufen und die sich, im Gegensatz zur Hardware, ohne vergleichsweise großen Aufwand ändern lassen.

via Satellit verschickt.[61] Die Knotenrechner verbinden demgegenüber verschiedene Teil-Netzwerke über die „Backbones“[62] miteinander. Die Backbones bilden mit ihren großen Bandbreiten und schnellen Verbindungsrechnern im wahrsten Sinne des Wortes das Rückgrat des Internets.[63] Die Verbindungsrechner selbst werden oft als sogenannte „Router“[64] betitelt. Sie sind für die Vermittlung des Datenweges im Computersystem verantwortlich. Die Hauptaufgabe eines Routers besteht vor allem darin, die an einer Eingangsleitung ankommenden Daten auf eine bestimmte Ausgangsleitung weiter zu vermitteln.[65] In komplexeren Netzen haben sie außerdem die Funktion, falls keine Ausgangsleitung frei ist, die Daten zunächst in einem Zwischenspeicher zu sammeln. Besteht zwischen zwei Routern keine direkte physikalische Verbindung oder sind unterschiedliche Verbindungsmöglichkeiten vorhanden, so muss der Router zusätzlich noch die günstigste Verbindung nach dem sogenannten „best effort-Prinzip“[66] über weitere zwischengeschaltete Router bestimmen.[67] Wenn Daten über Netze mit unterschiedlichen Übertragungstechniken transportiert werden, sind darüber hinaus gewisse Konvertierungsfunktionen zu erfüllen, die von speziellen Computersystemen durchgeführt werden.[68]

Die Übertragung der Daten selbst erfolgt durch elektrische Impulse. Diese elektronischen Impulse entsprechen der kleinsten Informationseinheit, dem „Bit“[69]. Durch die unterschiedliche Anordnung und Anzahl der einzelnen Impulse ist es möglich, die verschiedenartigsten und komplexesten Daten zu verschicken. Diese Art der Datenübertragung ist ein sehr komplizierter Vorgang. So muss der Übertragungsimpuls exakt definiert werden. Darüber hinaus ist eine genaue Bestimmung der Route im Netz sowie die anwendungsorientierte Präsentation der Daten auf dem Bildschirm eines bestimmten Computersystems erforderlich.[70]

---

61 Tanenbaum, Computernetzwerke, 3. Auflage, S. 13.

62 Vgl. hierzu Fn. 29 und Fn. 63.

63 Wie bereits oben schon erwähnt, kommt der Begriff „backbones“ aus dem Englischen und wird mit „Wirbelsäule“ übersetzt. Vgl. hierzu Mayer, Das Internet im öffentlichen Recht, S. 44 f.

64 Der Begriff „Router“ stammt von dem englischen Wort „route“ ab, das ins Deutsche mit Weg übersetzt wird.

65 Hage/Hitzfeld in: Loewenheim/Koch, Praxis des Online-Rechts, S. 28 f.; Gercke, Rechtswidrige Inhalte im Internet, S. 8 f.

66 Vgl. hierzu Mayer, Das Internet im öffentlichen Recht, S. 45.

67 Diese Datenübertragung des Routers wird als „point-to-point-Übertragung“ nach dem „Store-and-Forward-Prinzip“ bezeichnet. Nach diesem Prinzip werden Daten an alle benachbarten Systeme, mit denen formalisierte Austauschbeziehungen bestehen, verbreitet. Von jedem beteiligten System erfolgt die weitere Verbreitung, indem die Daten auf jedem der beteiligten Systeme für dessen Nutzer zum Abruf gespeichert und bereitgehalten (store) und gleichzeitig an alle benachbarten Systeme weitergeleitet (forward) werden.

68 Diese werden dann als „Gateways“ bezeichnet. Vgl. zu diesem Begriff Fn. 36.

69 In der Informationstheorie wird mit dem Begriff „bit“ häufig die kleinstmögliche Informationsmenge bezeichnet, die bei binären Entscheidungen (entweder/oder) anfällt. Dann leitet sich der Begriff des bits von „Basic Indissoluble Information Unit“ ab.

70 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 591.

Die Probleme, die das Internet hierbei aufwirft, sind offensichtlich: Indem das Internet ein Netz der Netze darstellt, gibt es in dieser Netzansammlung neben den zahlreichen unterschiedlichen Programmen auch völlig verschiedene technische Standards. Dadurch ist es eigentlich unmöglich, leserliche Daten zwischen den jeweiligen Clients und Servern zu versenden. Um dieses Problem zu beseitigen, wurde 1983 eine Systematisierung der Datenübertragung von der „International Standard Organisation“ (ISO) beschlossen. Dies hatte zur Folge, dass das sogenannte „Open Systems Interconnection Reference Model“ („ISO/OSI-Referenzmodell“) ins Leben gerufen wurde:

bb. Das ISO/OSI-Referenzmodell

Um den komplexen Vorgang der Datenübertragung zwischen unterschiedlichen Computersystemen zu verbessern, werden die bei der Datenübertragung anfallenden Aufgaben von der Informatik in unterschiedliche „Schichten“ oder englisch ausgedrückt in sogenannte „Layer“ unterteilt. Hierdurch entstehen verschiedene Ebenen, worauf die jeweiligen Vorgänge der Datenübertragung stattfinden. Die Probleme der Datenverarbeitung erfahren somit eine gewisse Gliederung. Das grundlegende Modell einer derartigen „Portionierung“ der Datenkommunikation ist das „ISO/OSI-Referenzmodell“. Dieses Modell unterteilt den Vorgang der Datenübertragung in sieben separate Schichten bzw. Layers. Wichtig ist in diesem Zusammenhang, dass die einzelnen Schichten aufeinander aufbauen. Jede dieser Schichten kommuniziert dabei nur mit der unmittelbar über oder unter ihr liegenden Schicht.[71]

(1) Die erste Schicht ist die physikalische Schicht (Physical Layer). Sie ist für die Übertragung der Bits zuständig. Sie besteht, wie der Name schon sagt, aus dem physikalischen Aufbau des Netzes, also den Übertragungskabeln, Routern, Gateways etc.

(2) Die zweite Schicht wird als Verbindungsschicht (Data Link Layer) bezeichnet. Hier werden die Daten in einzelne Datenpakete, sogenannte „Frames“, unterteilt. Außerdem werden die Frames gekennzeichnet, um sie zu unterscheiden und wieder richtig zusammensetzen zu können. Des weiteren besteht auf dieser Schicht die Möglichkeit, einen „Fehler- oder Flusskontrolleur“[72] zu installieren.

---

71 Vgl. hierzu auch die Darstellungen bei Kyas, Internet, S. 61 ff., Washburn/Evans, TCP/IP, S. 8 ff., Badach/Hoffmann/Knauer, High Speed Internetworking, S. 41 sowie Sieber, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 591ff.

72 Die „Flusskontrolle“ ist die Bezeichnung für eine Funktion auf der zweiten Schicht des OSI-Referenzmodells. Ziel der Flusskontrolle ist die Anpassung der Übertragungsgeschwindigkeit des Senders an die Aufnahmefähigkeit des Empfängers, wo die eintreffenden Daten u.U. erst weiterverarbeitet werden müssen, bevor neue Daten empfangen werden können. Man unterscheidet hierbei zwei Realisierungsmöglichkeiten: Zum einen nutzt die Softwareflusskontrolle die Steuerung des Datenflusses durch in einem Programm vorgegebene Mechanismen und Signale, die im Datenstrom selbst gesendet werden. Zum anderen nutzt die Hardwareflusskontrolle die Steuerung des Datenflusses durch Signale, die über eigene Steuerdatenleitungen zwischen Sender und Empfänger ausgetauscht werden.

(3) Die dritte Schicht stellt die Netzwerkschicht (Network Layer) dar. In ihr wird die Route festgelegt, die die einzelnen Datenpakete nehmen sollen. Hierbei kann es sich um eine bereits von vornherein vorgegebene Route handeln. Häufig wird jedoch die günstigste Verbindungsstrecke durch den Router berechnet. Diese Berechnung achtet auch darauf, dass innerhalb der verschiedenen Datennetze unterschiedliche Verbindungsschichten und Topologien vorliegen können. Die Netzwerkschicht ist demnach dafür zuständig, dass trotz dem Vorhandensein von verschiedenen ersten und zweiten Schichten im Netz, ein kontrollierter Datenfluss möglich ist.[73]
(4) Die vierte Schicht wird Transportschicht (Transport Layer) genannt. Ihre Aufgabe ist die Zustellung der einzelnen Datenpakete. Wie schon in der dritten Schicht soll der Verbindungsaufbau, die Segmentierung und die Zustellung ermöglicht werden. Dies geschieht in der Transportschicht dadurch, dass für jedes Datenpaket ein als „Port“[74] bezeichneter Verbindungskanal definiert wird. Außerdem regelt die vierte Schicht die maximale Datenpaketgröße. Im übrigen erhält jede Datensequenz eine Nummer, um die einzelnen Pakete später wieder richtig zusammensetzen zu können.[75]
(5) Bei der fünften Schicht handelt es sich um die Sitzungsschicht (Session Layer). Sie besitzt innerhalb einer Verbindung bestimmte Fehler- und Ordnungsfunktionen. So wird in dieser Schicht die ordnungsgemäße Datenübertragung kontrolliert. Sind Daten falsch verarbeitet worden oder gingen bestimmte Daten beim Transport verloren, findet ein erneuter Abruf dieser Daten aufgrund von speziellen Kontrollpunkten innerhalb dieser Schicht statt.
(6) Die sechste Schicht ist die Darstellungsschicht (Presentation Layer). Sie ist für die Semantik und Syntax der übertragenen Daten verantwortlich. Da die in einem Netz verbundenen Computersysteme unter Umständen verschiedene Verfahren zur Darstellung von Daten besitzen[76], ist die Verwendung einer abstrakten Datenstruktur nötig, durch den die Daten konvertiert werden, um die Daten auf jedem angeschlossenen Computersystem – unabhängig vom dort verwendeten Zeichensatz – darstellen zu können.
(7) Die siebte und letzte Schicht wird als Anwendungsschicht (Application Layer) bezeichnet. Diese Schicht stellt den Computernutzern und Nutzerprogrammen im Netz spezielle Dienste zur Verfügung. Hierdurch soll gewährleistet werden, dass Daten innerhalb eines Netzes unabhängig vom verwendeten Betriebssystem oder Benutzerpro-

---

73 Eines der bekanntesten Protokolle auf dieser Schicht ist das X.25-Protokoll.

74 Ein „Port“ ist der allgemeine Oberbegriff für einen Anschluss (Eingang, Ausgang), über den Daten und Steuerinformationen in ein Gerät ein- oder ausgegeben werden. Oft ist in der IT-Welt die Portnummer eines Sockets unter dem Betriebssystem Unix gemeint.

75 Pankoke, Von der Presse- zur Providerhaftung, S. 42.

76 Als Beispiel kann hier der ASCII-Code genannt werden. Der „American Standard Code for Information Interchange“ (ASCII) stellt einen amerikanischen Standard für den Informationsaustausch dar. Er ist ein Code zur Darstellung von Ziffern, Buchstaben und Symbolen.

gramm auf jedem Computersystem in der gleichen Weise dargestellt und bearbeitet werden können.[77]

Das eben vorgestellte ISO/OSI-Referenzmodell ist allerdings lediglich ein theoretisches Denkmodell, das die bei der Datenübertragung anfallenden Vorgänge systematisiert und erklärt. Es sagt nichts darüber aus, wie die jeweiligen Vorgänge konkret zu realisieren sind. Für die Umsetzung der verschiedenen Funktionen des Modells sind deswegen auf jeder einzelnen Schicht präzise Regeln und Konventionen, die jeweiligen Protokolle,[78] erforderlich. Die Liste aller innerhalb einer Kommunikationsverbindung verwendeten Protokolle bezeichnet man als den sogenannten „Protocol-Stack". Der speziell im Internet zum Einsatz kommende Protocol-Stack führt die Kurzbezeichnung „TCP/IP".

cc. Das TCP/IP-Modell

Das TCP/IP-Protokoll ist das Kommunikationsprotokoll im Internet.[79] Das „Transmission Control Protocol" (TCP) stellt in diesem Zusammenhang die vierte Schicht des ISO/OSI-Modells dar. Ferner ist unter dem „Internet-Protocol" (IP) die darunterliegende dritte Schicht des ISO/OSI-Modells zu verstehen. Das TCP/IP bildet gemeinsam mit den auf dem TCP aufbauenden Anwendungsprogrammen sowie mit den für das IP geeigneten Transportmechanismen die Familie der TCP/IP-Kommunikationsprotokolle.[80]

Beim TCP/IP-Modell fehlt im Gegensatz zum ISO/OSI-Modell die fünfte und sechste Schicht des ISO/OSI-Modells. Trotz der geringeren Anzahl von Schichten entspricht die Netzarchitektur des TCP/IP-Modells dem des ISO/OSI-Modells. Die verbleibenden Schichten und Einzelprotokolle übernehmen nämlich die Funktionen der fehlenden Schichten aus dem ISO/OSI-Modell.[81]

Die Verbindungsschicht und die Physikalische Schicht, also die ersten beiden Schichten des ISO/OSI-Modells, werden beim TCP/IP-Modell zu einer Netzschicht zusammengefasst. An den bereits vorgestellten Funktionen ändert sich dadurch allerdings nichts: Die Anwendungsschicht, d.h. die siebte Schicht des ISO/OSI-Modells, gibt es ohne Unterschied auch im TCP/IP-Modell und wird ebenfalls Anwendungsschicht genannt. Wichtig ist hierbei, dass sowohl die Anwendungsschicht, als auch die Netzschicht vom TCP/IP-Protokoll nicht definiert werden. Dadurch ist es möglich, dass diese Schichten von verschiedenen Computersystemen und Netzprotokollen unterschiedlich geregelt

---

77 Eine vertiefende Darstellung des ISO/OSI-Modells, vor allem hinsichtlich der Technik der jeweiligen Schicht, ist bei den Heijer, DFÜ Daten-Fernübertragung, S. 195 ff. zu finden.

78 Protokolle bestimmen beispielsweise die Paketgröße oder die Fehlerkontrolle innerhalb einer Datenkommunikationsverbindung.

79 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 10; darüber hinaus existieren im Internet neben dem TCP/IP-Protokoll noch andere Internet-Protokolle, wie z.B. das X.25-Protokoll.

80 Kyas, Internet, S. 63.

81 Bezüglich der Unterschiede zwischen dem ISO/OSI-Modell und dem TCP/IP-Modell vgl. bei Santifaller, TCP/IP and ONC/NFS, 2. Auflage, S. 14 f.

werden können.[82] Durch diese Unabhängigkeit des TCP/IP-Protokolls von den übrigen Schichten wird erst die Einzigartigkeit des Internets ermöglicht, weil ein Datenaustausch trotz unterschiedlicher Computersysteme und Netzprotokolle vollzogen werden kann.

(1) Das IP

Das IP ist das Basis-Kommunikationsprotokoll im Internet. Da das IP im ISO/OSI-Referenzmodell auf der Netzwerkschicht angesiedelt wäre, ist seine Aufgabe vor allem das Routing, d.h. die Einspeisung der einzelnen Datenpakete in ein beliebiges Netz und die Wegfindung dieser Daten im Hinblick auf einen bestimmten Empfänger.[83]
Die Art und Weise, mit der das IP die Daten überträgt muss als paketorientiert und verbindungslos angesehen werden. Paketorientiert bedeutet in diesem Fall, dass sämtliche zu übertragenden Daten in Datenpakete aufgeteilt werden. Das IP legt damit das Paketformat aller Datenübertragungen im Internet fest. Diese einzelnen Pakete werden dann verbindungslos verschickt, d.h. die Übertragung der Pakete erfolgt für jedes Paket separat, also unabhängig von vorhergehenden oder nachfolgenden Paketen.[84] Die Funktionsweise des IP kann mit der eines Briefumschlags verglichen werden, der eine Absender- und eine Empfängeradresse enthält und in dessen Innern sich das Datenpaket befindet.[85] Diese Adressen des Internets bestehen dabei aus einer Nummernfolge, der sogenannten „IP-Nummer“.[86] Diese Adressinformation befindet sich im Kopf des IP-Pakets, dem sogenannten „Header“.[87,88]
Der Weg der verschiedenen Datenpakete vom Sender über die verschiedenen Router zum Empfänger wird regelmäßig nicht vom Sender, sondern vom IP bestimmt.[89] Das IP berechnet dabei – vor allem unter Berücksichtigung der freien Leitungen – immer nur den Weg des Datenpakets zum nächstgelegenen Router im Hinblick auf die Erreichung des Endziels. Das Datenpaket wird dadurch bei jeder Übermittlung seinem Zielpunkt ein Stück näher gebracht. Dies hat zur Folge, dass die verschiedenen Datenpakete einer

---

82 Tanenbaum, Computernetzwerke, 3.Auflage, S. 11; Stögmüller, „Konvergenz in der Telekommunikation“, CR 1998, 733, 735.

83 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 593.

84 Kyas, Internet, S. 64.

85 Vgl. hierzu Krol, Die Welt des Internet, S. 28.

86 Bremer, Strafbare Internet-Inhalte in internationaler Hinsicht, S. 31.

87 Der Begriff „Header“ stammt von dem englischen Wort „head“, das ins Deutsche mit Kopf übersetzt wird. Mit dem Header wird der Teil eines Datenpakets bezeichnet, in dem keine Nutzdaten, sondern diverse Verwaltungsdaten enthalten sind. Zu den Verwaltungsdaten gehören beispielsweise die Adresse, die Paketnummer, Senderkennung, Paketstatus etc.

88 Gercke, Rechtswidrige Inhalte im Internet, S. 7; zum Aufbau eines IP-Datenpakets vgl. auch: Kyas, Internet, S. 64.

89 Das IP sieht allerdings die Möglichkeit vor, den Datenpaketen ein bestimmtes Routing vorzuschreiben. Diese – über die Optionen „strict source routing“ oder „loose source routing“ im Header steuerbare – Möglichkeit kann z.B. dann sinnvoll sein, wenn der Sender vermeiden will, dass seine Datenpakete über die Verbindungsrechner eines bestimmten Staates geleitet werden.

einzelnen Nachricht auf unterschiedlichen Wegen – und auch in unterschiedlicher Reihenfolge – ihren Bestimmungsort erreichen.
Da das IP aber keine Kontrollfunktion besitzt, können fehlerhafte oder verlorengegangene Pakete nicht wiederholt werden, so dass eine vollständige Datenübertragung mittels des IP allein nicht garantiert ist. Folglich wird für einen reibungslosen und fehlerfreien Datenaustausch ein weiteres Protokoll benötigt: das TCP.

(2) Das TCP

Die Funktion des TCP ist zunächst die der Transportschicht des ISO/OSI-Modells: Da die vom IP übertragenen Nachrichten grundsätzlich länger sind als die maximal zulässige Größe eines IP-Datenpakets und deshalb mehrere unabhängige Datenpakete für diese Nachrichten nötig sind, müssen sie vor ihrer Übertragung beim Sender zunächst in die maximal zulässige Größe eines IP-Datenpakets segmentiert und dann beim Empfänger wieder in den ursprünglichen Zustand zusammengesetzt werden.[90] Die einzelnen Datenpakete erhalten hierfür fortlaufende Nummern. Damit dieser Vorgang verständlicher wird, ist noch einmal vorstehendes Bild mit dem Briefumschlag heranzuziehen: Demnach muss man sich vorstellen, dass das TCP jedes Datenpaket mit einem nummerierten Umschlag versieht. Diese Umschläge werden dann in die Briefumschläge des IP gegeben und dem gewünschten Empfänger zugestellt.[91] Während des Vorgangs der Nummerierung der einzelnen Datenpakete erstellt das TCP zugleich eine Prüfsumme der zu sendenden Daten und vergleicht diese später mit der aus den empfangenen Daten errechneten Prüfsumme. Stimmen diese beiden ermittelten Prüfsummen nicht überein, so werden die Daten – soweit erforderlich – noch einmal übermittelt. Dies ist der wesentliche Unterschied des TCP zum IP. Im Gegensatz zum IP überträgt das TCP die Daten im Rahmen einer virtuellen Verbindung garantiert.[92] Auch wenn empfangene Datenpakete nicht quittiert werden, wird der Absender um erneute Übermittlung gebeten.[93] Das TCP übernimmt somit eine Fehler- und Flusskontrolle.[94]
Darüber hinaus regelt das TCP eine weitere wichtige Aufgabe: Da bei einem Empfänger viele verschiedene Daten ankommen, müssen sie dem jeweils richtigen Dienst[95] der Anwendungsschicht zugeordnet werden. Zu diesem Zweck erhält jedes TCP-Paket eine eigene Identifikationsnummer, die sogenannte „Port-Nummer“. Diese Port-Nummer ist entweder standardisiert oder muss bei einem speziellen Server abgefragt werden. Bei den standardisierten Nummern repräsentiert dabei jede Nummer einen bestimmten Dienst. Die Port-Nummer wird in den dafür vorgesehenen „TCP-Header“ gespeichert.

---

90 Gercke, Rechtswidrige Inhalte im Internet, S. 7.
91 Krol, Die Welt des Internet, S. 31.
92 Kyas, Internet, S. 66.
93 Herbert, Das Internet Praxisbuch, S. 7.
94 Krol, Die Welt des Internet, S. 30 ff.
95 Zu den einzelnen Diensten im Internet vgl. unten unter B. 1. Teil. I. 3.

Erhält der Empfänger ein TCP/IP-Datenpaket mit einer speziellen Port-Nummer, so kann dieses dann auf der Anwendungsschicht dem richtigen Dienst zugeordnet und mit der entsprechenden Software verarbeitet werden. Die Port-Nummer des TCP ordnet demnach den Datenpaketen die richtige Verarbeitung auf der Anwendungsschicht zu.[96]

3. Internet-Dienste

Das TCP/IP-Protokoll definiert nur, wie der Datenaustausch im Internet zu erfolgen hat. Die Form der übermittelten Daten ist hierdurch noch nicht festgelegt, sondern kann – auf der Anwendungsschicht des ISO/OSI-Schichtenmodells – beliebig definiert werden. In den letzten Jahren haben sich dabei einzelne Internet-Dienste mit speziellen Protokollen herausgebildet. Diese Internet-Dienste zeichnen sich dadurch aus, dass sie aufgrund ihrer Protokolle bestimmte Konventionen zur Darstellung der Daten beachten, so dass bei Verwendung der entsprechenden Software eine weltweite Datenübermittlung möglich ist.[97] Gemeint ist damit die Oberfläche, mit deren Hilfe der Nutzer die jeweiligen Daten zur Verfügung gestellt bekommt und weiterverarbeiten kann. Die bekanntesten Internet-Dienste sind E-Mail, Diskussionsgruppen (Newsgroups), Chat Foren, Internet-Relay Chat, Möglichkeiten zum Datentransfer (Telnet und FTP)[98] sowie das World Wide Web (WWW), dem wohl bekanntesten Internet-Dienst.

a. Electronic Mail (E-Mail) und Mailing-Listen

Einer der zentralen Dienste des Internets ist die elektronische Post (E-Mail).[99] Mit der elektronischen Post können sowohl kurze Nachrichten als auch komplette Dateien an andere Teilnehmer versendet werden. Der Vorteil einer E-Mail besteht vor allem darin, dass sie schnell und preiswert ist. Die Zustellung erfolgt regelmäßig innerhalb von Sekunden, wobei die Kosten weit unter den von herkömmlichen Kommunikationsmitteln wie Briefpost und Telefax liegen.[100]

Besonders wichtig ist zudem, dass die Daten bei der elektronischen Post sofort vom Empfänger digital weiterverarbeitet werden können. Es entfällt das oft lästige Medium

---

96 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 594; vgl. weiterführend zum TCP/IP-Modell: Santifaller, TCP/IP and ONC/NFS, 2. Auflage, S. 17 ff., Washburn/Evans, TCP/IP, S. 11 ff., Badach/Hoffmann/Knauer, High Speed Internetworking, S. 153 ff. sowie Kyas, Internet, S. 64 ff.

97 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 595.

98 Daneben existiert noch das ältere Gopher-System, das aber mehr und mehr an Relevanz verliert. Vgl. hierzu ausführlich in: Klußmann, Lexikon der Kommunikations- und Informationstechnik, 2. Auflage, S. 320.

99 Vgl. hierzu auch Funk, „Wettbewerbsrechtliche Grenzen von Werbung per E-Mail“, CR 1998, 411, 412.

100 Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1)“, 429, 431.

„Papier“ und die früher notwendige Postversendung von Disketten.[101] Diesen Vorteil besitzt nur die E-Mail. Bei den Telefaxen wird versucht, durch aufwendige Technik denselben Status wie bei der elektronischen Post zu erreichen. Dies gelingt mittels einer bestimmten Software, welche die Impulse des eingehenden Telefaxes in die Darstellungsform der E-Mail konvertiert, so dass eine sofortige Bearbeitung dieser Daten auch hier möglich ist.

Um die E-Mail zu nutzen, wird eine entsprechende Adresse benötigt. E-Mail-Adressen bestehen aus zwei Komponenten: der Benutzererkennung und dem Namen des benutzten Internetrechners mit einer Nationalitätskennung.[102] Diese beiden Teile werden durch ein spezielles, ansonsten bisher wenig verwendetes Zeichen aus dem ASCII-Code, dem sogenannten „Klammeraffen“ (Symbol: @), miteinander verbunden.[103]

Probleme bei der elektronischen Post ergeben sich allerdings durch die Tatsache, dass das verwendete „Simple Mail Transfer Protocol“ (SMTP) einen sehr geringen Grad an Fälschungssicherheit aufweist. Es besteht demnach ein erhöhtes Risiko des Missbrauchs.[104]

b. Newsgroups

Die Newsgroups oder News-Dienste stellen ein weltweites Diskussionsmedium dar.[105] Bekannt sind vor allem das Newsnet sowie das Usenet.[106] Sowohl das Usenet als auch das auf dem „Network News Tranfer Protocol“ (NNTP) beruhende Newsnet sind Systeme strukturierter Diskussionen, bei denen von jedermann Beiträge eingestellt bzw. „gepostet“[107] werden können. Verbildlicht dargestellt bestehen Newsgroups aus elektronischen schwarzen Brettern und Pinnwänden. Der News-Dienst bietet dabei die Möglichkeit, öffentliche Nachrichten von diesen schwarzen Brettern abzurufen oder an sie zu senden. Den Textbeiträgen können außerdem Bild-, Ton- oder Videodaten beigefügt werden.

Wegen der unübersehbaren Zahl der möglichen Themen gliedern sich diese elektronischen Pinnwände des Internets in Tausende von wissenschaftlichen, geschäftlichen, kulturellen und rein unterhaltenden Themenbereiche, die „Newsgroups“[108]. Täglich ent-

---

101 Hoeren, Rechtsfragen des Internet, Rdnr. 12.

102 Als wichtige Kennungen sind hierbei zu nennen: „de“ für Deutschland, „uk“ für Großbritannien, „edu“ für amerikanische Universitäten, „gov“ für Regierungsstellen, „com“ für kommerzielle Anbieter und „org“ für Organisationen.

103 Hoeren, Rechtsfragen des Internet, Rdnr. 13.

104 Mayer, Das Internet im öffentlichen Recht, S. 41.

105 Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 8 ff.

106 Schneider, Handbuch des EDV-Rechts, 2. Auflage S. 1686 O Rdnr. 78.

107 Der Begriff „post“ kommt aus dem Englischen und bedeutet zu Deutsch: anbringen, anschlagen.

108 Zu deutsch: Nachrichtengruppen.

steht eine Vielzahl von neuen Newsgroups. Jede dieser Newsgroups enthält wiederum eine unübersehbare Anzahl von Einzelbeiträgen.[109]

Die Gründung von neuen Newsgroups erfolgt oft in Absprache mit diversen anderen Teilnehmern im Internet, falls sich Interessenten für ein Thema gefunden haben. Daneben kann jeder Internet-Teilnehmer bei den mit dem Kürzel „alt." beginnenden Newsgroups eine neue Gruppe auf einem „News-Server"[110] ins Leben rufen.

Bei den Newsgroups ist zwischen den moderierten und unmoderierten Newsgroups zu unterscheiden. Die moderierten Newsgroups werden von einem sogenannten Moderator betreut, der auch die inhaltliche Linie innerhalb der Gruppe vorgibt.[111] Wegen des damit verbundenen Aufwands ist der Anteil der moderierten Newsgroups[112] – gemessen am Gesamtanteil der Newsgroups – sehr gering. In der Praxis dominieren eher die unmoderierten Newsgroups, so dass jeder Internet-Teilnehmer die Möglichkeit hat, eigene Beiträge in die Newsgroups einzubringen. Eine Kontrolle dieser Beiträge findet nicht statt. Für den Inhalt der meisten Newsgroups ist also letztlich allein die „Internet-Gemeinde"[113] bestimmend.

Damit der News-Dienst überhaupt betrieben werden kann, speichern und übermitteln die News-Server die einzelnen Nachrichten. Einige dieser Server sind nur für einen berechtigten Personenkreis bestimmt. Das Gros dieser Server ist jedoch für jedermann zugänglich. Theoretisch ist für das Betreiben eines News-Servers jeder internettaugliche Computer geeignet, da die Computerprogramme der News-Server Standard-Programme sind.

Wird auf einem beliebigen Computersystem eine neue Newsgroup eingerichtet oder ein Einzelbeitrag geschrieben, so befinden sich diese Daten zunächst nur auf dem einen News-Server, an den der Autor seine Nachricht schickt. Die Besonderheit des News-Dienstes besteht aber darin, dass die im Internet vorhandenen News-Server in regelmäßigen Abständen ihre Inhalte abgleichen und damit auf andere News-Server verbreiten. Dieser Vorgang wird „Synchronisation" genannt. Die Synchronisation erfolgt durch ein automatisiertes Verfahren, ohne dass es hierzu eines menschlichen Willensentschlusses bedürfte. Dieses automatisierte Verfahren wird als „Store-and-Forward-Prinzip"[114] be-

---

109 Auf den News-Servern (vgl. zu diesem Begriff nachfolgende Fn.) eines größeren Internet-Service-Providers gehen z.B. täglich über 180.000 Beiträge ein. Dies ergibt eine Gesamtgröße von 2.250.307 KB, was umgerechnet einer Datenmenge von 2.250 Büchern mit je 400 Seiten entspricht.

110 Damit der News-Dienst überhaupt betrieben werden kann, sind bestimmte Computersysteme im Internet, die sogenannten „News-Server", erforderlich, welche die Nachricht speichern und übermitteln.

111 Dies geschieht häufig dadurch, dass die moderierten Newsgroups aufgrund einer entsprechenden Einstellung der News-Server-Software alle Artikel zunächst als E-Mail an den Moderator geschickt werden, der dann die Möglichkeit hat, zu entscheiden, was in die Gruppe aufgenommen wird und was nicht.

112 Meistens handelt es sich dabei um Universitäten, Privatfirmen oder spezielle Organisationen.

113 Gemeint ist damit die Gesamtheit der Internet-Nutzer.

114 Das „Store-and-Forward-Prinzip" stellt ein Vermittlungsprinzip der Speichervermittlung dar, bei dem der Datenfluss von der Quelle zur Senke unterbrochen wird, indem die Daten in Vermittlungs-

zeichnet. Mit Hilfe dieses Prinzips kann letztlich jede neu errichtete Newsgroup oder jeder neu verfasste Beitrag auf jeden im Internet verfügbaren News-Server gelangen. Diese praktisch weltweite Verbreitung der einzelnen Nachrichten ist auch Ziel der Newsgroups. Darüber hinaus kann so das Netz entlastet werden, weil bei der Abfrage von bestimmten Nachrichten nicht mehr nur auf einen, meist weit weg befindlichen News-Server zurückgegriffen werden muss, sondern die gewünschte Datei bereits bei einem Server in der Nähe zu finden ist. Diese den globalen Informationsaustausch erlaubende Möglichkeit wird programmtechnisch dadurch realisiert, dass der Nutzer des News-Dienstes in seinem News-Reader-Programm beliebige News-Server angeben kann, auf die zugegriffen werden soll.

c. Chat Foren

Chat Foren sind Angebote im Internet, bei denen eine Kommunikation der Teilnehmer in Echtzeit möglich ist. Hierbei gibt es zwei Arten der Chat Foren: zum einen können geschlossene „Räume“[115] existieren, worin nur eine bestimmte Anzahl von Nutzern gleichzeitig anwesend sein kann, und offene, in denen jeder Nutzer an der virtuellen Unterhaltung teilnehmen kann. Die Kommunikation erfolgt schriftlich. Damit die Schreibarbeit nicht allzu lange dauert, werden sehr viele Abkürzungen und Symbole verwendet.[116] Chat Foren werden mittlerweile überwiegend als Anwendungen auf der Basis des WWW[117] programmiert, um eine leichte Zugänglichkeit zu gewährleisten.[118]

d. Internet-Relay Chat (IRC)

Ähnliche Funktionen wie die Chat Foren hat das „Internet Relay Chat Protocol“ (IRCP). Auch hier werden über einen Server Teilnehmer verbunden, die in Echtzeit in Schriftform kommunizieren. Diese Kommunikation erfolgt in sogenannten „Channels“, das sind logische Kommunikationsräume mit bestimmten Themen. Beim Betreten eines derartigen virtuellen Raumes werden die Teilnehmer mit ihren Systemnamen[119] angezeigt. Eine gewisse Art von Anonymität bleibt somit auf Wunsch erhalten. Durch Eingabe einfacher Befehle können die übrigen Teilnehmer angesprochen oder Daten über sie abgefragt werden. Die schriftliche Unterhaltung erfolgt auf einem geteilten Bildschirm, in dessen einem Teil die Äußerungen des Gegenübers und in dem anderen die eigenen angezeigt werden. Darüber hinaus können parallel dazu auch andere Daten ü-

---

knoten zwischengespeichert werden und später (zu geeigneter Zeit, beispielsweise bei geringerer Netzauslastung oder zu Zeiten geringerer Gebühren) weitergeleitet werden.

115 Hier spricht man häufig auch von sogenannten „Chat-Rooms“.

116 Als Beispiel sind hier die mittlerweile sehr gängigen „Emoticons“ zu nennen, kleine, aus Satzzeichen gebildete Symbole (engl.: icons), die Gefühle (engl.: emotions) ausdrücken. Bekanntester Vertreter dieser Gruppe ist der „smiley“: „:-)“.

117 Vgl. hierzu unten bei B. 1. Teil. I. 3. g.

118 Mayer, Das Internet im öffentlichen Recht, S. 42.

119 Diese Systemnamen werden auch als „nicknames“ oder „nicks“ (zu deutsch: Spitznamen) bezeichnet.

bertragen werden. Deshalb werden häufig illegale Daten mittels IRC ausgetauscht, weil es eine sehr flüchtige und relativ anonyme Form der Datenübertragung ermöglicht.[120]

e. Telnet

Das nicht sehr anwendungsfreundliche, aber leistungsfähige Telnet bietet eine sogenannte „Terminalemulation" über das Netz an.[121] Dies bedeutet eine völlige oder teilweise Kontrollübernahme eines Rechners über einen anderen, entfernteren Rechner. So kann beispielsweise aus Berlin ein in Tokio befindlicher Rechner „gesteuert" werden. Die Terminalemulation wurde in den Anfängen des Internets oft benutzt, um „Fernarbeit" zu erledigen. Mittlerweile wird diese Methode nur in den Fällen eines Informationsdienstes angewandt, der im Internet den Zugriff auf Informationssysteme anbieten will, die unter einem anderen Betriebssystem laufen.[122] Dabei beschränkt sich die Benutzung von Telnet hauptsächlich auf den Informationszugriff in Form von Texten.

f. Dateientransfer (FTP)

Als eingeschränkte Variante des Telnet stellt das „File Transfer Protocol" (FTP) einen Internet-Dienst dar, der die Übertragung von Dateien eines Rechners auf einen anderen erlaubt.[123] Derartige Daten können durch den Nutzer im Internet sowohl von einem fremden FTP-Server heruntergeladen werden, d.h. der Server sendet die gewünschten Daten zum Nutzer,[124] als auch auf einem fremden FTP-Server hochgeladen werden, d.h. dass der Nutzer verschickt bestimmte Daten an den Server[125]. Die Zugangsmöglichkeiten zu einem bestimmten FTP-Server sind dabei unterschiedlich ausgestaltet und werden vom Betreiber festgelegt. In der Regel gestattet der Betreiber einen anonymisierten Datenabruf. Dieser ermöglicht dem Nutzer das Kopieren von allgemein zugänglichen Daten auf sein eigenes Computersystem. Zusätzlich kann das Recht gewährt werden, eigene Daten auf den FTP-Rechner abzulegen.

g. World-Wide-Web (WWW)

Das World-Wide-Web (WWW) ist wohl der bekannteste und wichtigste Internet-Dienst.[126] Es beruht auf dem „Hyper Text Transfer Protocol" (HTTP)[127]. Das WWW koordiniert eine Sammlung von vielen Millionen Einzeldokumenten, den sogenannten „Web-Seiten", die durch WWW-Server auf der ganzen Welt gespeichert sind. Jede die-

---

120 Mayer, Das Internet im öffentlichen Recht, S. 43.

121 Vgl. hierzu auch Lammarsch/Steenweg, Internet & Co, Ziff. 3.4 S. 60 ff.

122 Als Beispiele sind hier die Bibliothek des amerikanischen Kongresses, Reisebüros und Banken zu nennen.

123 Hance, Internet-Business & Internet-Recht, S. 50.

124 Der aus dem Englischen abgeleitete Fachausdruck für diesen Vorgang heißt „Download".

125 Der aus dem Englischen abgeleitete Fachausdruck für diesen Vorgang wird „Upload" genannt.

126 Lent, Rundfunk-, Medien-, Teledienste, S. 151; Kloepfer/Neun, „Rechtsfragen der europäischen Informationsgesellschaft, EuR 2000, 512.

127 Siehe Hage/Hitzfeld in: Loewenheim/Koch, Praxis des Online-Rechts, S. 37 f.

ser Seiten verfügt über eine eigene Web-Adresse, dem sogenannten „Uniform Resource Locator“ (URL)[128], und kann daher direkt abgerufen werden. Nur durch diesen URL ist es möglich, eine Seite sofort aufzurufen. Der URL besteht dabei aus drei Komponenten: Zunächst wird das Anwendungsprotokoll, d.h. der gewünschte Internet-Dienst definiert. Danach folgt der Domain-Name[129] des Servers, der die angeforderten Informationen speichert, der sogenannte „Host“, sowie eventuell die benutzte Portnummer. Daran schließen sich die Bezeichnungen der Verzeichnisse und Unterverzeichnisse an, worin sich die gesuchte WWW-Seite befindet.[130] Mit dem URL wird eine unkomplizierte Nutzung der Adressen gewährleistet. Denn statt eines verwirrenden Zahlencodes gibt der Nutzer seine gewünschten Domainnamen ein, die häufig eine logische Verbindung zu den gewünschten Informationen aufweisen. So gelangt man beispielsweise durch die Eingabe von „www.spiegel.de“ auf die Web-Seite des gleichnamigen Nachrichtenmagazins. Erst im Rechner wird dieser Domainname, der wie im Beispiel meist aus Buchstaben besteht, in eine Zahlenkombination umgewandelt.

Die große Vereinfachung der Informationssuche durch das WWW liegt vor allem darin, dass innerhalb einer Web-Seite Verweise auf andere WWW-Seiten möglich sind.[131] Diese Verweise auf andere Seiten werden „(Hyper-)Links“[132] genannt.[133] Mittels solcher Links gelangt der Nutzer von Seite zu Seite, bis er die gewünschte Information findet, ohne dass er den konkreten Inhalt der Internet-Seite kennt.[134] Auch innerhalb einer Seite können durch das Einstellen von Hyperlinks Verknüpfungen hergestellt werden, die ein mühsames Suchen vermeiden helfen. Oft enthalten bestimmte Adressen, die über eine Top-Level-Domain verfügen, eine Vielzahl an Informationen. Diese Informationen sind in Unterabteilungen der Web-Seite zu finden. Um auf sie direkt zugreifen zu können, werden sie mit Sub-Level-Domains versehen, so dass sie jederzeit unmittelbar abrufbar sind.

---

128 Vgl. hierzu Köhler/Arndt, Recht des Internet, 2. Auflage, S. 4 f. Rdnr. 14 f.

129 Vgl. zu diesem Begriff Fn. 53.

130 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 33.

131 Solche Dokumente werden als „Hypertext-Dokumente“ bezeichnet.

132 Technisch besehen ist ein Hyperlink der Eintrag eines URL einer anderen WWW-Seite im Quellcode einer WWW-Seite, der dort einem Inhalts-Element, beispielsweise einem Wort oder einer Graphik zugeordnet ist. Indem der Abruf einer bestimmten WWW-Seite mit Hilfe der in dem Browser des Nutzers eingegebenen Adresse vorgenommen wird und die Adressierung der Seiten durch den URL erfolgt, genügt der Einbau derartiger URL, um auf völlig andere WWW-Seiten verweisen zu können.
Klickt der Benutzer ein Seitenelement, das ein URL enthält, an, so zeigt der Browser als nächstes die Seite an, deren URL im Quellcode eingetragen ist. Für das Erscheinungsbild und die Benutzung spielt es aus Sicht des Benutzers dabei keine Rolle, ob die gelinkte Seite auf demselben Server gespeichert ist wie der Link oder auf einem anderen Server an einem anderen Ort. Ebenfalls ohne Auswirkung auf das Erscheinungsbild der gelinkten Seite ist der Umstand, dass diese Seite mittels eines Hyperlinks vom Browser aufgebaut wurde. Das gleiche Ergebnis hätte der Nutzer damit erreichen können, wenn er im Quellcode den URL eingegeben hätte. Vgl. hierzu auch Eichler/Helmers/Schneider, „Link(s) – Recht(s)“, K&R-BB-Beilage 18/1997, S. 23.

133 Köhler/Arndt, Recht des Internet, 2. Auflage, S. 122 ff. Rdnr. 398 ff.

134 Zur Funktionsweise der Hyperlinks vgl. Kuner, Internet für Juristen, 2. Auflage, S. 35 ff.

Abgesehen davon verbindet das WWW – wie schon mehrmals angesprochen – einzelne Web-Seiten und andere Internet-Dienste zu einer riesigen weltweit verteilten Datenbank.[135]

h. Abgrenzung zu anderen Netzen und Diensten

Diese soeben dargestellten Dienste des Internets müssen von anderen verwandten und oftmals vom Internet als solchen in der praktischen Anwendung kaum unterscheidbaren Netzen und Diensten abgegrenzt werden. Für alle im folgenden genannten Systeme ist kennzeichnend, dass sie geschlossene Benutzergruppen aufweisen, über Zentralrechner operieren und regelmäßig hierarchisch strukturiert sind. Dagegen ist das Internet ein nicht hierarchisches, nicht zentrales, offenes System zum Austausch von Daten.

Kommerzielle Online-Dienste[136] bieten ihren Kunden zunächst den Zugang über Telefonleitungen zu ihrem eigenen proprietären Dienst und dem dort enthaltenen Informationsangebot an, das teilweise auf entsprechende Kundengruppen zugeschnitten ist.[137] Diese Angebote ähneln ihrem Aussehen nach zum Teil Angeboten aus dem Internet wie E-Mail, IRC, Newsgroups oder WWW, stehen aber ausschließlich den Kunden dieser Dienste zur Verfügung. Mittlerweile offerieren Online-Dienste darüber hinaus auch über Gateways den Zugang zum Internet, während umgekehrt ein Zugriff auf die Angebote der Online-Dienste aus dem Internet nicht oder nur eingeschränkt[138] möglich ist.[139] Wegen ihres umfangreichen Angebots und ihrer weltweiten Verbreitung erfreuen sie sich beim Publikum als Zugangsmedium zum Internet großer Beliebtheit und werden daher oft fälschlicherweise mit dem Internet als solchem gleichgesetzt.[140]

Ähnlich verhält es sich bei den klassischen Mailboxen[141] oder Bulletin Board Systemen (BBS)[142]. Diese ermöglichen grundsätzlich keinen Zugang zum Internet. Im übrigen

---

135 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 597.

136 Hierzu zählen vor allem T-Online, America Online (AOL) und CompuServe.

137 Vgl. Zimmer, „Online-Dienste für ein Massenpublikum?“, Media Perspektiven 1995, 476 ff.; Stock, „Kinder und Internet – eine Bestandsaufnahme“, DRiZ 1997, 431 ff.

138 Beispielsweise kann dies auf der privaten Homepage der Nutzer der Fall sein.
Zu der sehr umstrittenen Frage, ob ein Internet-Service-Provider auf providerspezifische Dienstleistungsangebote oder technische Ressourcen eines anderen, marktbeherrschende Internet-Service-Provider zugreifen kann, vgl. Dietz/Richter, „Netzzugänge unter Internet Service Providern“, CR 1998, 528, 529.

139 Briner in: Hilty (Hrsg.), Information Highway, S. 495 f.

140 Wetzstein/Dahm/ Steinmetz/u.a., Datenreisende, S. 21 ff.

141 Der Begriff „Mailbox“ hat eine doppelte Bedeutung. Zum einen ist eine Mailbox eine feste Adresse (quasi ein elektronischer Briefkasten) in einem Kommunikationssystem und zum anderen gleichzeitig ein Oberbegriff für verschiedene Arten von Mitteilungsdiensten (sogenannte „electronic mail“). Vgl. weiterführend: Palm/Roy, „Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte“, NJW 1996, 1791; Fangmann/Scheurle/Wehner/Schwemmle, Handbuch für Post und Telekommunikation, 2. Auflage, S. 389 f.

142 „Bulletin Board Systeme“ (BBS) sind computergestützte und meist frei zugängliche Nachrichten- und Telefon-Konferenzsysteme. Benutzer können beispielsweise über das Internet eine Verbindung herstellen und dort Nachrichten und Informationen abrufen, die andere hinterlegt haben, oder selbst Mitteilungen hinterlegen. Die BBS sind sozusagen die elektronischen „Schwarzen Bretter“ des In-

muss zu der gewünschten Mailbox bzw. bei mehreren zusammengeschlossenen Mailboxen zu mindestens eine von ihnen eine unmittelbare physikalische Verbindung z.B. über Modem oder Telefonleitung aufgebaut werden. Einige dieser nicht-kommerziellen Mailboxen sind jedoch miteinander vernetzt und ebenfalls teilweise an das Internet angebunden.[143]

Abschließend handelt es sich bei den sogenannten „Intranets“[144] ebenfalls um geschlossene Datenaustauschsysteme, die zwar auf TCP/IP-Basis arbeiten können, aber grundsätzlich für den Zugriff von außen geschlossen sind. Sie finden beispielsweise in größeren Unternehmen mit mehreren Standorten Anwendung.

Bei kommerziellen Online-Datenbanken handelt es sich meist um Datensammlungen, die sich an professionelle Anwender richten und für ihre Benutzung Gebühren berechnen. Zunehmend werden auch derartige Systeme über das Internet zugänglich, wobei die Zugänge meist passwortgeschützt sind und so nur zahlenden Mitglieder offen stehen.[145]

4. Aufgabenverteilung im Internet

Die vorgeschilderten technischen Ausführungen machen deutlich, dass an der Verbreitung von Informationen im Internet verschiedene Personen beteiligt sind: Auf der einen Seite steht der Urheber einer bestimmten Information, etwa der Verfasser einer E-Mail, einer WWW-Seite oder der Teilnehmer, der eine Bilddatei per FTP verschickt. Auf der anderen Seite steht dann der Empfänger oder Adressat, der sogenannte „Nutzer“ bzw. „User“ solcher Informationen. Dazwischen liegt das Internet und seine zahlreichen Einzelnetze, die jeweils von Betreibern eingerichtet und mehr oder weniger überwacht werden. Sie werden häufig verallgemeinernd mit dem Oberbegriff „Provider“ bezeichnet und verschaffen ihren Teilnehmern eine Zugangsmöglichkeit zum Internet sowie seinen Diensten, bieten selbst Dienste an und/oder betreiben regelmäßig Teile des Inter-

---

ternets, vgl. Koch, „Rechtsfragen der Nutzung elektronischer Kommunikationsdienste“, BB 1996, 2049.

143 Hierzu gehören das weltweit verbreitete FidoNet oder das deutsche Mailbox-Netz Z-Netz. Vertiefend zu diesem Thema: Ackermann, Ausgewählte Rechtsprobleme der Mailbox-Kommunikation, S. 3 ff.; Wetzstein/Dahm/Steinmetz/u.a., Datenreisende, S. 28 ff.; Ehrkamp/Mansfeld, Das Telekommunikations Buch, S. 457 ff.; Palm/Roy, „Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte“, NJW 1996, 1791 f.

144 Der Begriff „Intranet“ setzt sich aus dem lateinischen Wort „intra“ = innen oder innerhalb und dem englischen Wort „net“ = Netz zusammen. Unter einem Intranet ist eine Anfang 1996 aufgekommene Bezeichnung für private Datennetze (z.B. LAN) zu verstehen. Mit dem globalen Internet sind Intranets üblicherweise über eine Firewall (zum Abschotten des Intranets vom restlichen Internet und zur Kontrolle des Zugriffs von der Außenwelt) verbunden. Intranets werden überwiegend hausintern benutzt, beispielsweise zur Verbindung zwischen mehreren Abteilungen oder geographisch verteilten Einheiten. Darüber hinaus ist die Anbindung von Geschäftspartnern oder Kunden über spezielle Zugangsverfahren denkbar.

145 Als Beispiele aus dem juristischen Bereich sind das deutsche JURIS-System oder die amerikanische Datenbank WEST-LAW und LEXIS/NEXIS zu nennen.

nets wie die Server und Router.[146] Provider sind oft Online-Dienste, Wirtschaftsunternehmen, Universitäten oder gemeinnützige Vereine, wobei die technische Umsetzung der Zugangsmöglichkeit zum Internet sehr unterschiedlich bewerkstelligt wird. Aber auch natürliche Personen können als Provider tätig werden.[147] Die Provider dürfen demnach nicht pauschal beurteilt werden, denn ihre Funktionen beim Datenaustausch im Internet allgemein und bei den verschiedenen Internet-Diensten im besonderen sind sehr vielfältig. Weil aber die Provider eine Schlüsselrolle für das Internet besitzen und sich hinter ihnen regelmäßig natürliche wie juristische Personen befinden, sind sie auch rechtlich von besonderem Interesse. Es ist somit wie folgt zu unterscheiden:[148]

a. Network-Providing

Wie bereits oben festgestellt, schafft das Routing die technischen Voraussetzungen für den tatsächlichen Datenaustausch im Internet. Zur Gewährleistung dieser Transportfunktion stellen Provider die notwendigen Übertragungswege oder -kapazitäten zur Verfügung, indem sie z.B. Netzknotenrechner sowie Router und „Proxy-Cache-Server“[149] betreiben oder Telefon- und andere Datenleitungen anmieten.[150] In diesen Funktionsbereich, dessen Akteure als „Network-Provider“[151] bezeichnet werden, gehören auch die Betreiber der zur Datenübertragung notwendigen Telekommunikationsnetze.[152]

b. Access-Providing

Ein weiterer, häufig vom Network-Providing nur schwer abgrenzbarer Tätigkeitsbereich ist die Bereitstellung des Zugangs zum Internet und seinen Diensten.[153] Diese Funktion

---

146 Strömer, Online§Recht, S. 9 ff.

147 Zu der Technik im einzelnen: Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen“, JZ 1996, 429, 434; Schwarz in: Schwarz, Recht im Internet, 1-1 S. 11; Koch, „Rechtsfragen der Nutzung elektronischer Kommunikationsdienste“, BB 1996, 2049, 2051; Jäger/Collardin, „Die Inhaltsverantwortlichkeit von Online-Diensten“, CR 1996, 236, 237; Spindler, „Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme“, ZUM 1996, 533 f.; Perritt, Law and the Information Superhighway, S. 151 ff.

148 Später wird erneut auf die unterschiedlichen Provider-Typen, die für das TKG, das TDG und den MDStV relevant sind, eingegangen. Vgl. hierzu unter B. 2. Teil. II. 4. c. cc.

149 Der Begriff des „Proxy-Cache-Servers“ stammt teilweise aus dem Lateinischen wegen des Wortes „proximus“ = nächster, sehr nahe sowie aus dem Englischen wegen des Wortes „cache“ = Versteck, verstecken. Mit dem Proxy-Cache-Server werden Dienste bezeichnet, die an Stelle von anderen Netzelementen ausgeführt werden. Damit ist es möglich, Sicherheitsfeatures zu realisieren. Ein Proxy-Cache-Server ist ein Server, der sich nahe bei dem Client befindet und vertretungshalber die Bereitstellung von Daten, Programmen usw. für weiter entfernte Server übernimmt. Erst wenn die auf dem Proxy-Cache-Server befindlichen Daten nicht die vom Client angeforderten Daten enthalten, ist es nötig, auf den anderen, weit entfernten Server zuzugreifen. Hierdurch kann eine Netzlast auf den Backbones des Internets vermieden sowie mit schnellen Antwortzeiten für die Kunden der Provider zufriedenstellende Dienstqualitäten ermöglicht werden.

150 Strömer, Online§Recht, S. 10; Briner in: Hilty (Hrsg.), Information Highway, S. 516 ff.

151 Der Begriff „Network“ stammt aus dem Englischen und kann mit Netzwerk übersetzt werden.

152 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438.

153 Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte“, ZUM 2000, 1007, 1016.

beinhaltet die technische Realisierung des Internet-Zugangs und wird daher als „Access-Providing“[154] bezeichnet.[155] Der Zugang zum Internet kann auf verschiedenen Wegen erreicht werden. Demzufolge sind die damit verbundenen Serviceleistungen je nach Provider sehr unterschiedlich. So kann der Access-Provider umfangreiche Dienste für den Zugang zum Internet anbieten.[156] Unter Umständen beschränkt sich die Funktion des Access-Providers aber auch nur auf das bloße Zurverfügungstellen eines Modem- oder ISDN-Zugangs[157] zum Netz.

c. Content-Providing

Neben der Technik können insbesondere Inhalte im Internet angeboten werden. Derjenige, der Inhalte selbst erstellt und in das Internet einstellt, wird „Content-Provider“[158] genannt.[159] Unter die Inhalte des Content-Providers fallen alle Angebote, die er entweder selbst entwickelt und in das Internet eingespeist hat oder die zumindest in seinem Namen entstanden sind. Hauptsächlich handelt es sich beim Content-Provider um den Ersteller einer WWW-Seite, den Verfasser einer E-Mail oder ein Unternehmen, das einem spezialisierten Entwickler von Webseiten den Auftrag erteilt, für das Unternehmen eine Präsenz im Internet zu entwickeln. Das fundamental Neue am Internet besteht darin, dass nicht nur wie bisher gewerbliche Anbieter mit mehr oder minder großem Aufwand Informationen an die Öffentlichkeit tragen können. Vielmehr kann jeder Privatmann – z.B. durch eine eigene Webseite – ohne großen technischen und finanziellen Aufwand zum weltweiten Inhaltsanbieter werden, also zum Content-Provider.

d. Service- bzw. Host-Providing

Abgesehen von eigenen Inhalten des Content-Providers können auch fremde Inhalte im Internet angeboten werden. Diese technische Dienstleistung erbringt der sogenannte „Host- oder Service-Provider“[160]. Der Service-Provider dient der Verbreitung fremder

---

154 „Access“ kommt aus dem Englischen und bedeutet zu Deutsch: Zugang.

155 Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 10 f.; Briner in: Hilty (Hrsg.), Information Highway, S. 492 ff.

156 Koenig, „Regulierungsoptionen für die Neuen Medien in Deutschland“, MMR-Beilage 12/1998, 6

157 Ein „Modem“ macht die empfangenen Daten für den jeweiligen Computer leserlich. Bildlich gesprochen stellt es einen Dolmetscher für die unterschiedlichen „Computersprachen“ dar.
„ISDN“ ist die Abkürzung für den Begriff „Integrated Services Digital Network“ und stellt im Grunde ein Telekommunikations-Dienstleistungsangebot dar. Es kann bereits verlegte Telefonleitungen benutzen. Ein wesentlicher Unterschied zwischen ISDN und dem alten Telefonnetz besteht darin, dass es sich bei ISDN ausschließlich um digitale Signale handelt. Sprache wird digitalisiert, Daten können digital übernommen werden. Ein Modem ist somit nicht mehr nötig. Vgl. weitergehend: Rosenbaum, PC/EDV-Lexikon, S. 153.

158 „Content“ kommt aus dem Englischen und bedeutet zu Deutsch: Inhalt.

159 Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 11; Köhntopp/Köhntopp, „Datenspuren im Internet“, CR 2000, 248, 250.

160 Die Begriffe „Host“ und „Service“ stammen aus dem Englischen und bedeuten zu Deutsch: Gastgeber bzw. Dienst. Die Bezeichnungen „Host-Provider“ und „Service-Provider“ werden grundsätzlich

Informationen, indem er dem Content-Provider eigene Serverkapazitäten[161] für die Speicherung dessen fremder Daten zur Verfügung stellt, ohne dass er auf diesen Inhalt vorab irgendwelchen Einfluss nimmt oder sonst über die bisher beschriebenen Funktionen hinausgehende Dienste anbietet.[162] Im Grunde ähnelt der Service-Provider dem Content-Provider, da er ebenfalls (wenn auch fremde) Inhalte für den Nutzer im Internet bereithält.[163]

e. Mischformen

Manchmal lassen sich die einzelnen Internet-Dienste teilweise kaum voneinander unterscheiden. So kann ein Access-Provider zugleich Content-Provider sein, wenn er z.B. bei einem umfangreicheren Serviceangebot im Rahmen der Bereitstellung des Internet-Zugangs zugleich selbst Informationen anbietet. Gleiches gilt, wenn ein Service-Provider nicht nur die Funktion eines Zwischenspeichers erfüllt. Dies kann einmal dadurch geschehen, dass der Service-Provider beispielsweise seinem WWW-Server eine bestimmte „Färbung“ gibt, indem er nur bestimmten Inhalten Serverkapazitäten zur Verfügung stellt.[164] Zum anderen können Verweisungen etwa in Form von Links oder der Anzeige eines Suchergebnisses einer Suchmaschine einen eigenständigen Hinweis auf Angebote Dritter darstellen, der über das bloße (Zwischen)-Speichern und Abrufhalten fremder Daten hinausgeht.[165] Noch weiter geht der Einfluss auf Inhalte, falls der Service-Provider selbst oder ein Dritter in seinem Auftrag die Moderation etwa von Newsgroups und Mailing-Listen übernimmt oder einen FTP-Server betreibt. In diesen Fällen sichtet der Service-Provider den Datenbestand und entscheidet, welche Daten er allgemein zugänglich machen will. Insofern ist allen diesen Mischformen eine im Vergleich zum reinen Service-Providing erhöhte Nähe zum Inhalt eines Internet-Angebots zu eigen.

Es erscheint sinnvoll, diese Mischformen danach zu behandeln, wie der Schwerpunkt ihrer angebotenen Dienste liegt.[166] Des weiteren sollte für den Fall, dass Rechtsprobleme auftreten, darauf abgestellt werden, welcher Dienst hiervon betroffen ist. Dadurch

---

synonym verwendet. Im folgenden soll lediglich der Begriff Service-Provider benützt werden, um Verwirrungen vorzubeugen und eine einheitliche Linie zu gewährleisten. Vgl. hierzu auch Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 10 f.

161 Hierunter fallen hauptsächlich Speicherplätze und Leistungsbandbreiten.

162 Holznagel/Kussel, Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 349; Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte“, ZUM 2000, 1007, 1016.

163 Zur Ausgestaltung von Service-Provider-Verträgen, die das Leistungsbild des Service-Providers wiedergeben, vgl. Schuppert, „Web-Hosting-Verträge“, CR 2000, 227 ff.

164 A. A. Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen“, JZ 1996, 429, 434, der derartige Fälle noch als Service-Providing qualifiziert.

165 Ernst, „Rechtliche Fragen bei der Verwendung von Hyperlinks im Internet“, NJW-CoR 1997, 224 ff.

166 Zu einer zweigliedrigen Differenzierung vgl. Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen“, JZ 1996, 429, 434.

kann eine schwierige Abgrenzung vermieden werden und es treten zu den übrigen Diensteanbietern keine widersprüchlichen Ergebnisse auf.

f. Empfangen von Inhalten

Am anderen Ende der Kommunikationskette steht der Empfänger einer per Internet versendeten Information. Das Verhalten dieser Adressaten, Teilnehmer, Nutzer oder User ist bei den oben genannten Internet-Diensten dadurch gekennzeichnet, dass sie selbst mehr oder weniger umfangreiche Aktivitäten entfalten müssen, um den Informationsversand zu initiieren. Insofern kann man das Internet als „Pull-Medium“[167] bezeichnen, bei dem der Empfänger beispielsweise per Mausklick eine WWW-Seite auf seinen Bildschirm holt und so selbst für den Informationsfluss sorgen muss. Er „zieht“ sich somit die gewünschten Daten aus dem Internet.[168]

5. Zusammenfassung

Die vorausgegangenen Ausführungen zum Datentransport, den einzelnen Diensten und den unterschiedlichen Providern im Internet machen deutlich, wie vielschichtig und komplex das Internet funktioniert. Nur durch ein reibungsloses Zusammenwirken aller genannten Faktoren wird ein Informationsaustausch über das Internet möglich.

Gerade die Komplexität und insbesondere das Mitwirken einer großen Anzahl von in- und ausländischen Providern haben jedoch zur Folge, dass rechtswidrige bzw. strafbare Inhalte sehr leicht und häufig anonym in dieses „Netz der Netze“ eingespeist werden können. Des weiteren bereitet die aufwändige Struktur des Internets dem Gesetzgeber erhebliche Schwierigkeiten, da nationale Regelungen den komplizierten Aufbau des Internets und dessen weltweiten Datentransports nur in einem gewissen Maße erfassen können.[169] Bevor jedoch auf die Gesetzeslage und deren rechtlichen Probleme eingegangen wird, sollen zunächst die verschiedenen Arten rechtswidriger Inhalte und im Anschluss daran die technischen Möglichkeiten einer Kontrolle des Internets aufgezeigt werden.

---

167 „Pull“ kommt aus dem Englischen und bedeutet zu Deutsch: Ziehen. Vgl. hierzu auch Leupold, „>>Push<< und >>Narrowcasting<< im Lichte des Medien- und Urheberrechts“, ZUM 1998, 99 ff.

168 Demgegenüber lässt sich das Internet auch als „Push-Medium“ einsetzen. „Push“ kommt aus dem Englischen und bedeutet zu Deutsch: Drücken. Dabei werden Dienstleistungen angeboten, bei denen – abgesehen von der einmaligen Registrierung – allein der Content-Provider selbst aktiv wird und nach einer Vorauswahl Inhalte, wie z.B. Tickermeldungen, an den Empfänger weitergibt. Die Informationen werden in diesem Fall zum Empfänger „gedrückt“. Vgl. insoweit: Koch, „Neue Rechtsprobleme der Internet-Nutzung“, NJW-CoR 1998, 45; Leupold, „>>Push<< und >>Narrowcasting<< im Lichte des Medien- und Urheberrechts“, ZUM 1998, 99 ff.; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 55 ff.

169 Kröger/Moos, „Regelungsansätze für Multimediadienste“, ZUM 1997, 462, 463.

II. Rechtswidrige Inhalte im Internet

1. Die häufigsten Missbrauchsformen

a. Urheber- und Markenrechtsverletzungen

Zu den häufigsten Missbrauchsformen[170] im Internet gehören zunächst die Verstöße gegen Urheber- und Markenrechte. Ein Verstoß gegen das Urheberrecht geschieht sehr oft dadurch, dass urheberrechtlich geschütztes Bild- und Tonmaterial auf bestimmten Web-Seiten im WWW für jedermann zum Vervielfältigen angeboten wird.[171] Markenrechtliche Konflikte kommen insbesondere dann in Betracht, wenn mit geschützten Zeichen für Produkte geworben wird.

b. Wettbewerbsrechtliche Verstöße

Daneben können auch wettbewerbsrechtliche Verstöße eine Rechtswidrigkeit von Internet-Seiten verursachen. Vor allem wettbewerbswidrige Werbung beschäftigt in zunehmenden Maße die deutsche Gerichtsbarkeit.[172] Aber auch außerhalb der Wirtschaftswerbung sind Wettbewerbsverstöße denkbar. So gibt es vermehrt unlautere Leistungsübernahmen in der Form, dass Texte, Graphiken, Bilder, etc. in unberechtigter Weise auf die eigenen Webseiten übernommen oder gelinkt werden.[173]

c. Beleidigungen/Persönlichkeitsrechtsverletzungen

Auf manchen Internet-Seiten sind darüber hinaus Beleidigungen zu finden. So besitzen gewisse – oft an die Öffentlichkeit gerichtete – Internet-Adressen beleidigende Inhalte, die sich nicht nur gegen Einzelpersonen, sondern auch gegen bestimmte Personengruppen richten können. Zudem besteht die Möglichkeit, dass durch die unbefugte Verwendung von Daten das Persönlichkeitsrecht von Netzbenutzern verletzt wird.[174]

---

170 Umfassende Ausführungen zu den einzelnen (strafbaren) Missbrauchsformen im Internet sind bei Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2)“, JZ 1996, 494, 496 f. und Gercke, Rechtswidrige Inhalte im Internet, S. 14 ff. zu finden. Vgl. auch Strömer, Online§Recht, 2. Auflage, S. 219 ff., Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 59 sowie Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 16 ff.

171 Als Beispiel soll hier die Entscheidung des Tribunal de Grande Instance in Paris (Tribunal de Grande Instance Paris – 14.08.1996 – REF 60138/96) hinsichtlich einer Web-Site auf der im Jahre 1996 Musik und Text von Jacques Brel, ein französischer Chansons-Sänger, im Internet zum weltweiten Abruf angeboten wurde, genannt werden. Vgl. auch: Bortloff, „Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten“, ZUM 1997, 167, 171.

172 Vgl. zum Problem der vergleichenden Werbung: Kröger/Gimmy, Handbuch zum Internet-Recht, S. 391.

173 Freytag, Haftung im Netz, S. 7.

174 Schneider, Handbuch des EDV-Rechts, 2. Auflage S. 118 ff. B Rdnr. 134 ff.

d. Pornographie/Politische Propaganda

Schließlich sind als weitere rechtswidrige Inhaltsformen des Internets pornographische Darstellungen[175] und die Verbreitung von radikaler politischer Propaganda[176] zu nennen.[177] Für Aufsehen sorgt vor allem die große Anzahl an Kinderpornographie im Internet.[178] Daneben kommt es im Internet immer wieder zur Verwendung von Kennzeichen verfassungswidriger Organisationen, zu rassistischer Propaganda, zur Volksverhetzung, zu Aufrufen gewalttätiger Versammlungen sowie zur Anstiftung bestimmter Terroraktionen.[179]

---

175 Ausführlich zu diesem Problem: Edwards/Waelde, Law & the Internet, 2. Auflage, S. 275 ff. (Pornography and the Internet).

176 So wurden im Jahre 2001 mehr als 1000 Internet-Adressen mit rechtsradikalem Inhalt von den zuständigen Polizei- und Sicherheitsbehörden entdeckt (Quelle: Deutschlandfunk am 22.12.2001). Das Simon-Wiesenthal-Center, Los Angeles geht von über 2000 Websites aus, die antisemitisches oder volksverhetzendes Gedankengut verbreiten, Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte", MMR 2001, 347.

177 Stellvertretend für diese Art rechtswidriger Inhalte im Netz können der Fall des Erwin Zündel sowie der Fall der Zeitschrift „Radikal" genannt werden.
So ermittelte die Staatsanwaltschaft Mannheim gegen die beiden großen deutschen Online-Dienste AOL und T-Online wegen dem Tatvorwurf der Mitwirkung an der Verbreitung von nationalsozialistischer Propaganda und volksverhetzendem Material. Hintergrund war hier der Umstand, dass der kanadische Neonazi Ernst Zündel diverse nationalsozialistische Hetze über die Newsgroups der Online-Dienste weltweit verbreitete.
Der Fall der Zeitschrift „Radikal" stellt wohl – neben dem „CompuServe-Urteil" (vgl. nächste Fn. 178) – den wohl spektakulärsten Fall in Deutschland mit weitreichenden Konsequenzen für die Frage der Verantwortlichkeit im Internet dar. In diesem Fall ermittelte die Generalbundesanstalt von September 1996 bis November 1997 wegen des Verdachts der Beihilfe zum Werben für terroristische Vereinigungen, zur Anleitung zu Straftaten sowie zur öffentlichen Billigung von Straftaten gegenüber dem Betreiber des holländischen Servers „xs4all", gegen zahlreiche in Deutschland ansässige Access-Provider und andere Personen. Der Grund hierfür bestand darin, dass die (verbotene und beschlagnahmte) Druckausgabe Nr. 154 der linksgerichteten Zeitschrift „Radikal" unter anderem einen „Kleinen Leitfaden zur Behinderung von Bahntransporten aller Art", der in detaillierter Form die Sabotage sogenannter Achszähler im Gleisnetz der Deutschen Bahn AG beschrieb. Diese Ausgabe wurde von bisher unbekannten Tätern als WWW-Seiten formatiert und auf den niederländischen Server „xs4all" der Allgemeinheit innerhalb eines Verzeichnisses, das mehrere, auch nicht strafbare Ausgaben der „Radikal" in HTML-Format enthielt, zugänglich gemacht. Vgl. insoweit Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 61 f.

178 Als Beispiel für pornographische Inhalte im Internet soll das - sehr umstrittene - „CompuServe"-Urteil des AG-München vom 28.05.1998 – 8340 Ds 465 Js 173158/95 genannt werden. In diesem Fall ging es um die Strafbarkeit der deutschen Tochterfirma CompuServe GmbH der amerikanischen CompuServe Inc. Die CompuServe GmbH betrieb Verbindungsrechner (insbesondere Netzknoten) über welche die deutschen Mitglieder der CompuServe Inc. Zugang zu den Datenspeichern (sogenannten Servern) der amerikanischen CompuServe Inc. erhielten. Die dem Verfahren zugrundeliegenden strafbaren Inhalte, hauptsächlich in Form von kinderpornographischen Darstellungen, waren nicht auf Computersystemen der deutschen CompuServe GmbH. Sie wurden vielmehr nur über die Netzknoten der CompuServe GmbH von den Servern der CompuServe Inc. in den USA abgerufen.

179 Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte", ZUM 2000, 1007; Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet", NJW 1999, 3145, 3145; zahlreiche Beispielsfälle aus der Praxis zu den genannten Missbrauchsformen im Internet sind bei Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 57 ff. abgedruckt.

2. Eingrenzung

Wie vorstehend aufgezeigt, enthält das Internet also verschiedenartige Varianten rechtswidriger bzw. strafbarer Angeboten. Diese sind sowohl im Straf- als auch im Zivilrecht anzusiedeln. Daneben gibt es aber auch Inhalte, die zum Teil in der Form, wie sie dargestellt werden, lediglich als unerwünscht oder schädlich anzusehen sind. Eine rechtliche Einteilung dieser Inhalte gestaltet sich äußerst schwierig. Trotzdem muss der Staat auch bei diesen Inhalten tätig werden, insbesondere um einen ausreichenden Jugendschutz zu gewährleisten.

Die rechtswidrigen Inhalte im Internet, die dem Zivilrecht zuzurechnen sind, weisen allerdings die Besonderheit auf, dass der Staat üblicherweise dagegen mit Sperr- und Löschanordnungen erst auf gerichtliche Veranlassung aktiv werden kann.[180] Folglich ist hierfür zunächst als Zwischenschritt die gerichtliche Überprüfung nötig, ehe die zuständige staatliche Stelle (normalerweise handelt es sich dabei um den Gerichtsvollzieher) rechtswidrige zivilrechtliche Inhalte sperren oder löschen lässt. Aus diesem Grund befasst sich die vorliegende Arbeit primär nicht mit den rechtswidrigen Inhalten, die dem Zivilrecht zuzurechnen sind. Auch die strafrechtlich motivierten Sperr- und/oder Löschanordnungen sollen nicht unmittelbar Gegenstand dieser Untersuchung sein.[181] Denn es besteht keine Rechtsgrundlage für Kontrollmaßnahmen, die einzig und allein unter Hinweis auf eine Strafbarkeit bestimmter Inhalte im Netz ergehen.[182] Derartige Sperr- und/oder Löschanordnungen wären demnach contra legem und somit nicht zulässig.

Im folgenden werden deshalb ausschließlich die staatlichen Kontrollmaßnahmen untersucht, für die bereits eine gesetzliche Rechtsgrundlage existiert und die ohne Anrufung des (Zivil)-Gerichts durch die Bürger erfolgen. Es geht somit um präventive, also polizei- und sicherheitsrechtliche Maßnahmen, die der Staat vornimmt, um sich und seine Bürger zu schützen.[183] Dabei kommt es nicht nur auf die strafrechtliche Relevanz, sondern vielmehr – gemäß dem Grundsatz des Polizei- und Sicherheitsrechts – darauf an, ob eine (konkrete) Gefahr für die öffentliche Sicherheit und Ordnung von dem jeweiligen Inhalt im Internet ausgeht.[184] Denn es kann bereits ein von der Rechtsordnung nicht gewünschter, schädlicher Inhalt als eine Gefahr für die öffentliche Sicherheit und Ordnung angesehen werden, obwohl er sich noch nicht unter einen Straftatbestand subsumieren lässt.[185] Dies bedeutet, dass in dieser Arbeit unter dem Begriff „rechtswidriger

---

180 Das Gleiche gilt für strafrechtliche Antragsdelikte, wie beispielsweise der Beleidigung (vgl. §§ 184 ff. StGB). Auch hier muss regelmäßig erst der Bürger aktiv werden, bevor der Staat agieren kann.

181 Vgl. hierzu die Ausführungen bei Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347 f.

182 Sieber, Verantwortlichkeit im Internet, S. 144 Rdnr. 287.

183 Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 348.

184 Vgl. Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, Art. 11 Ziff. 11.4.

185 Indem er beispielsweise gegen Vorschriften aus dem Jugendschutzgesetz verstößt. Hinsichtlich der Begriffe der öffentlichen Sicherheit und Ordnung vgl. Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, Art. 2 Rdnr. 6 f.

Inhalt“ ein Inhalt im Internet zu verstehen ist, der geeignet ist, den Tatbestand der „konkreten Gefahr für die Sicherheit und Ordnung“ i.S.d. Polizei- und Sicherheitsrechts zu erfüllen. Deshalb sind rechtswidrige Inhalte in der vorliegenden Arbeit offensichtlich unerwünschte Daten in Form von Text-, Ton- und/oder Bilddateien, die als pornographisch, politisch extrem, terroristisch, staats- bzw. demokratiefeindlich, menschenverachtend oder gewaltverherrlichend anzusehen sind. Zweifelhafte Fälle, die noch einer tolerierbaren Grauzone zugerechnet werden können, sollen nicht erfasst werden. Mit dem Begriff „Inhalt“ sind dabei alle erdenklichen Daten bzw. Informationen gemeint, die im Internet für die Nutzer bereitgestellt werden.

3. Zurechnung der rechtswidrigen Inhalte

Neben der Tatsache, dass das Internet rechtswidrige Bereiche enthält, muss weiter geklärt werden, wem diese rechtswidrigen Inhalte zuzurechnen sind. Dieser Gedanke ist dem Sicherheits- und Polizeirecht entnommen, das neben der Feststellung einer rechtswidrigen Maßnahme auch immer noch den Störer ermitteln muss, um gegen diese Maßnahme vorgehen zu können. Denn die Beseitigung bzw. Verhinderung von rechtswidrigen Inhalten im Internet erfordert einen Adressaten, gegen den die staatliche Maßnahme gerichtet werden kann.

Die Ermittlung des Störers im Internet ist allerdings nicht unproblematisch. Denn sehr oft sind die unmittelbar verantwortlichen Täter, die rechtswidrige Inhalte durch aktives Tun selbst verbreiten, nicht zu identifizieren, da diese Personen häufig im Ausland agieren. Deshalb konzentriert sich die Untersuchung zunächst auf die inländischen Betreiber von elektronischen Kommunikationsdiensten und Netzwerken, deren technische Systeme zur Tatbegehung missbraucht werden.[186] Diesen Providern kann zum Teil vorgeworfen werden, dass sie durch ihre – an sich sozial nützliche – Bereitstellung der technischen Infrastruktur Beihilfe zur Verbreitung sowie zum Anbieten von rechtswidrigen Inhalten im Internet leisten würden. Folglich kann bei ihnen ebenfalls eine Störereigenschaft[187], wenn auch häufig nur eine mittelbare, gegeben sein. Staatliche Maßnahmen richten sich deshalb regelmäßig gegen die natürlichen und juristischen Personen, welche die Möglichkeiten für rechtswidrige bzw. strafbare Inhalte schaffen und anbieten. Hierdurch kann viel schneller und effektiver gegen die ungewünschten Inhalte vorgegangen werden.

Demnach stehen die Provider als Zwischenglieder zunehmend in der Verantwortung und müssen unter gewissen rechtlichen Voraussetzungen bestimmte Kontrollmaßnah-

---

186 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581.

187 Ob darin nun eine Handlungs- oder Zustandsstörereigenschaft zu erblicken ist, kann letztendlich dahingestellt bleiben. Vgl. hierzu Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, Art. 7 Rdnr. 1 ff.

men dulden. Allerdings stellt sich in diesem Zusammenhang die Frage, ob diese Kontrollmaßnahmen überhaupt sinnvoll sowie technisch möglich sind und wie sie gestaltet werden können. Denn erst wenn dies geklärt ist, kann auf die rechtliche Problematik eingegangen werden, da sich diese in erster Linie nach den technischen Gegebenheiten richtet.

III. Technische Ansatzpunkte für eine Kontrolle im Internet

Die oben ausführlich dargestellte Funktionsweise des Internets[188] ist nicht nur Voraussetzung für die Beurteilung der einzelnen technischen Kontrollmaßnahmen. Sie macht auch die Entwicklung von Kontrollstrategien im Internet deutlich.

Zum besseren Verständnis soll noch einmal kurz zusammengefasst werden, wie eine Informationsabfrage durch einen Nutzer geschieht: Der User eines Computernetzes erhält über den Einwahlknoten seines Access-Providers sowie gegebenenfalls über ein lokales Teilnetz Zugang zum Internet. Über zahlreiche redundante Verbindungen ist ein Zugriff auf die einzelnen Server möglich, die entweder eigene Informationen (Content-Provider) oder Daten dritter Inhaltsanbieter (Service-Provider) für den Nutzer zum Abruf bereithalten. Aus dieser Grundstruktur moderner Computernetze ergeben sich für Kontrollmöglichkeiten die folgenden allgemeinen Konsequenzen:

Eine Verhinderung rechtswidriger Inhalte ist insbesondere bei den am Anfang und am Ende des Datenübertragungsvorgangs stehenden Personen möglich, d.h. beim abfragenden Nutzer und beim Inhaltsanbieter, dem Content- bzw. Service-Provider, wo die Daten meist unverschlüsselt abgespeichert sind.

Eine Kontrolle durch den Network-Provider außerhalb der Einwahlknoten direkt auf der Datenautobahn im Netz scheidet in der Regel schon von vornherein wegen des dargestellten Routing-Verfahrens aus: Da die einzelnen Datenpakete einer Nachricht über unterschiedliche Netzknoten vermittelt werden können, sind Zugriffskontrollen hier allenfalls in engen Grenzen und an wenigen Stellen möglich. Darüber hinaus werden Kontrollen durch Network-Provider dadurch erschwert, dass die übermittelten Daten hier nur auf der Ebene der Netzwerkschicht und damit nicht in einer ohne weiteres lesbaren Form vorliegen.

Kontrollmöglichkeiten der Datenübertragung zwischen dem Nutzer und dem Inhaltsanbieter sind damit vor allem an den beiden Stellen möglich, wo die Daten des Informationsanbieters und des Users an der „Auf-“ und „Abfahrt“ zur Datenautobahn in das weltweite Netz übertragen werden. Ansatzpunkte für eine effiziente Kontrolle bieten deswegen insbesondere die Rechner der Content- und Service-Provider, worauf die in Frage stehenden Informationen gespeichert sind. Daneben kommen die Datenverarbeitungssysteme der Access-Provider in Betracht, bei denen eine Filterung von Daten des

---

188 Vgl. oben unter B. 1. Teil. I. 2.

Nutzers entweder an dessen Einwahlknoten oder aber – gemeinsam mit den Daten anderer Nutzer – am Übergang eines abgeschotteten Teilnetzes in das weltweite Netz versucht werden kann.

1. Kontrollmöglichkeiten der jeweiligen Provider

Zunächst soll auf die Frage eingegangen werden, welche Möglichkeiten die einzelnen Provider besitzen, rechtswidrige Inhalte im Internet aufzuspüren und anschließend zu beseitigen. Erst wenn dies geklärt ist, kann die Überlegung angestellt werden, in welchem Maße der Staat entweder selbst oder mit Hilfe der Provider technisch auf das Internet kontrollierend einwirken kann.

Es wurde bereits ausgeführt, dass verschiedene Provider mit unterschiedlichen Funktionen Internet-Dienste anbieten.[189] Die Möglichkeiten einer Kontrolle des Internets richten sich dabei nach der Funktion, die ein Provider im Internet besitzt. Es ist deshalb zwischen dem Content- und dem Service-Provider, die bestimmte Inhalte (eigene bzw. fremde) dem Nutzer im Netz bereitstellen und dem Access-Provider zu unterscheiden, der diese angebotenen Inhalte zum Nutzer transportiert.

a. Kontrollmöglichkeiten des Content-Providers

Der Content-Provider, der eigene Inhalte in das Internet einspeist, hat grundsätzlich eine umfassende Kenntnis von seinen Internet-Angeboten. Er besitzt somit ein umfassendes Wissen über seine für den Nutzer im Internet bereitgestellten Inhalte. Eine Inhaltskontrolle ist für ihn in der Regel ohne weiteres möglich. Problematisch sind höchstens die Inhalte, auf die er mittels Hyper-Link verweist.[190] Abgesehen von dieser Grauzone bestimmt allein der Content-Provider, welche Inhalte er anbieten will. Die Beseitigung bestimmter Inhalte ist für ihn jederzeit möglich. Technisch kann er entweder den Zugang zu den rechtswidrigen Angebote für den Nutzer sperren oder den Inhalt löschen.

b. Kontrollmöglichkeiten des Service-Providers

Im Gegensatz zum Content-Provider kennt der Service-Provider regelmäßig die vom Content-Provider erhaltenen Daten nicht, da seine Aufgabe nur darin besteht, diese Daten im Internet bereitzustellen. Fraglich ist jedoch, ob der Service-Provider diese Inhalte, die er für den Content-Provider speichert, überwachen kann. Als Überwachungsmaßnahme kommt eine Inhaltskontrolle des eigenen Servers in Frage. Das Auffinden unbekannter rechtswidriger Inhalte auf dem eigenen Rechner bereitet jedoch dem Service-Provider grundsätzlich erhebliche Probleme:

Bei geschlossenen Nutzergruppen beruhen diese Probleme häufig auf der Verschlüsselung von Daten. Dagegen sind bei öffentlichen Inhalten, auf die sich die folgenden Aus-

---

189 Vgl. oben unter B. 1. Teil. I. 3. und 4.

190 Vgl. zu dieser Problematik unten unter B. 2. Teil. II. 5. b. cc. (6).

führungen konzentrieren,[191] die Schwierigkeiten der Inhaltskontrolle vor allem darin begründet, dass auf den Servern regelmäßig ein großes und sich rasch veränderndes Datenangebot gespeichert ist, das im Hinblick auf rechtswidrige Inhalte mit den heute verfügbaren Möglichkeiten nicht maschinell, sondern nur durch arbeitsintensive Einzelkontrollen geprüft werden kann. Die Möglichkeiten der Identifizierung rechtswidriger Inhalte hängen dabei allerdings stark vom gespeicherten Datenvolumen des Service-Providers ab.[192] Die Service-Provider haben eigentlich nur eine Möglichkeit, rechtswidrige Inhalte in ihren unterschiedlichen Rechnern zu identifizieren. Diese Möglichkeit stellt die Inhaltsfilterung dar.[193] Durch sie können rechtswidrige Internet-Bereiche ausfindig gemacht und im Anschluss daran eliminiert werden. Schwierig ist und bleibt jedoch die Durchführung dieser Inhaltsfilterung.

Zunächst könnte ein computergestütztes Filterprogramm in Frage kommen. Allerdings enthalten die auf dem Markt befindlichen Programme der einzelnen Server derartige Programme noch nicht. Ob solche Filterprogramme überhaupt einmal zur Anwendung kommen, ist ebenfalls fraglich, da bestimmte Probleme nicht ausgeschaltet werden können: So bereitet allein die Tatsache, dass eine Überprüfung der Inhalte mit Hilfe dieser Programme der Speicherung im Internet durch die Server zeitlich nachfolgen würde, erhebliche Schwierigkeiten. Selbst bei einer raschen Überprüfung besteht daher zumindest eine kurze Zeitspanne, in welcher der Kunde ungefilterte Inhalte abrufen kann. Dieses Problem lässt sich allerdings dadurch umgehen, dass der Betreiber des jeweiligen Servers ein zusätzliches Server-System installiert. Auf diesem System können neu eintreffende Daten zur weiteren Filterung für den Kunden bis zur Überprüfung durch das Filtersystem unzugänglich aufbewahrt werden. Eine solche Sicherungseinrichtung würde aber nicht nur zu erheblichen Kosten in den Bereichen der Hardware-Anschaffung, der Installation und des Betriebs führen, sondern vor allem durch den erhöhten Datenverkehr innerhalb des Netzes des Service-Providers die Netzlast auf ein untragbares Maß anheben.

Daneben könnte bereits in die eigentliche Server-Software ein Filterprogramm integriert werden. Hierdurch wird erreicht, dass die Filterung noch vor der eigentlichen Speicherung und Bereitstellung für den Nutzer stattfindet. Diese Methode der Filterung klingt zwar einfach und wäre vielleicht sogar technisch machbar. Allerdings besitzt diese Art der Inhaltsfilterung neben technischen Problemen auch sämtliche andere Schwierigkei-

---

191 Denn die geschlossenen Nutzergruppen machen vergleichsweise wenig Schwierigkeiten, da sie sehr oft spezialisiert sind und von sich aus einen hohen Sicherheitsstandard besitzen. Außerdem stellen sie nur einen kleinen Teil des Internets dar. Sie können deshalb in dieser Arbeit vernachlässigt werden.

192 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 655.

193 Zu den jeweiligen Filtermöglichkeiten siehe Vielhaber, „Neuer Schutz vor neuen Gefahren? – Jugendschutz im Internet“, MMR-Beilage 9/2001, 16, 18 f. sowie Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 350.

ten, die eine Filterung von Inhalten mit sich bringt. So kann mit derartigen Filterprogrammen normalerweise nur ein sehr grobes Raster angelegt werden, das keine befriedigenden Ergebnisse erzielt. Hinzu kommt noch, dass die Informationen im Internet und damit auch die rechtswidrigen Inhalte nicht nur als Textdateien, sondern auch als Bild-, Video- und Tondateien gespeichert sind. Eine Filterung ist zur Zeit aber nur hinsichtlich Textdateien technisch machbar.[194] Vor allem sind die für diese Zwecke benötigten Verfahren zur Mustererkennung von Bildern derart rechenintensiv, dass sie nur von speziellen Großrechnern in einer akzeptablen Geschwindigkeit bewältigt werden können.[195]
Die Inhaltsfilterung von Textdateien ist aber auch nicht frei von Schwierigkeiten. Denn ein Filterprogramm ist bis jetzt jedenfalls nicht mit einem eigenem Beurteilungsvermögen ausgestattet. Folglich kann das Programm nur darauf programmiert sein, irgendwelche Schlüsselbegriffe[196] in den Textdateien zu erkennen. Dies funktioniert aber dann nicht, wenn die Textdateien verschlüsselt oder komprimiert sind, andere „Binärdateien“[197] vorliegen oder kein Textbaustein der Nachricht mit einem Eintrag der Wortfilter-Liste übereinstimmt, der Nachricht aber Bild- oder Tondateien als Binärdateien angehängt wurden. Ein Textfilter bleibt auch dann wirkungslos, sofern die Teilnehmer beim Bekanntwerden entsprechender Filterungen Umschreibungen oder Tarnbegriffe verwenden würden.[198] Die Textfilterprogramme sind auch deswegen wenig zu gebrauchen, weil das Auffinden eines bestimmten Schlüsselwortes noch nichts über einen möglichen rechtswidrigen Inhalt und insbesondere den mitentscheidenden Kontext aussagt.[199] Computergestützte Textfilter können daher allenfalls als Groberkennungsmuster für die Vorprüfung und Alarmierung von individuellen Kontrollen eingesetzt werden. Entspre-

---

194 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 657.

195 Die von der Firma Microtrope Limited im Frühjahr 1997 erstmals vorgestellte Software „ImageCensor“ analysiert beim Öffnen einer Bilddatei durch den Nutzer die Farbanteile und deren Häufigkeit je Bildfläche. Diese Daten werden einer statistischen Bewertung durch das Programm unterzogen. Stimmen die Ergebnisse mit bestimmten Kriterien überein, vermutet das Programm ein Nacktbild und verhindert ein weiteres Laden des Bildes. Diese Art der Inhaltskontrolle von Bilddateien stößt jedoch schnell an ihre Grenzen. So können Schwarz/Weiß-Bilder überhaupt nicht analysiert werden. Darüber hinaus kann die Software nicht zwischen pornografischen Fotos und harmlosen Abbildungen von Kunstwerken unterscheiden.

196 Zu denken ist hier beispielsweise an das Schlüsselwort „Sex“.

197 Unter dem Begriff „Binär“ ist eine Eigenschaft zu verstehen, die ausdrückt, dass ein bestimmter Sachverhalt (ein bestimmtes Zeichen) durch eine Folge von Symbolen beschrieben (codiert) werden kann, die aus einem Symbolvorrat von nur zwei Zeichen besteht. Ein Beispiel für diesen Symbolvorrat sind die Mengen (0, 1), (Low, High) oder (aus, ein).

198 Eine Ersetzung von Begriffen geschieht teilweise bereits heute, wenn insbesondere Silben durch lautmalerische Zahlen ersetzt werden. So wie z.B. die Phrasen „for you“ durch „4u“ und „Access for all“ durch „xs4all“ ersetzt werden, kann beispielsweise das Wort „Sex“ durch die Zahl „6“ oder das neutrale Wort „Verkehr“ umschrieben werden. Einfache Filterprogramme können auch durch das Einfügen von Bindestrichen in den Texten getäuscht und somit wirkungslos gemacht werden.

199 Als Beispiel hierfür ist die Sperrmaßnahme eines amerikanischen News-Server-Providers zu nennen, dessen Filterprogramm alle Nachrichten mit dem Schlüsselwort „Breast(s)“ untersagte. Kurz darauf kam es zu gewaltigen Protesten einer Gruppe von krebskranken Frauen, die sich in einer entsprechenden Newsgroup über ihre Brustkrebserkrankungen austauschen wollten und dies nicht mehr möglich war.

chende kombinierte Systeme, die aufgrund einer computergestützten Vorprüfung eine effektive menschliche Überprüfung ermöglichen sollen, sind zwar sicherlich wirkungsvoll, allerdings sehr aufwändig und kostenintensiv.

Deshalb bleibt im Augenblick nur die Möglichkeit, Filterprogramme dazu einzusetzen, um eine grobe Unterscheidung von Textdateien zu treffen und die auffälligen Texte dann stichprobenartig auf ihre rechtswidrigen Inhalte zu untersuchen. Zudem kann die Identifikation von weiteren rechtswidrigen Inhalten dadurch erfolgen, dass die übrigen Internet-Teilnehmer, die eher zufällig auf fragwürdige Inhalte im Netz stoßen, auf derartiges Material hinweisen und den jeweiligen Provider hiervon in Kenntnis setzen, der dann die entsprechenden Gegenmaßnahmen ergreifen kann.[200] Als solche kommen aus technischer Sicht wieder nur die Löschung sowie die Sperrung der betreffenden Inhalte in Betracht. Sofern bestimmte Daten durch den Service-Provider auf den eigenen Rechensystemen als rechtswidrig identifiziert sind, bereitet allerdings ihre Löschung oder Sperrung regelmäßig keine Probleme. Dies beruht darauf, dass die auf den Servern gespeicherten Daten durch entsprechende Programme gezielt verarbeitet und damit auch gesperrt bzw. gelöscht werden können. Dies gilt im Grundsatz für alle Anwendungsdienste des Internets.[201]

c. Kontrollmöglichkeiten des Access-Providers

Die vorangegangene Strukturanalyse von Computernetzen macht deutlich, dass eine Zugriffskontrolle des Nutzers durch den an der Auffahrt von Datenautobahnen befindlichen Access-Provider theoretisch in zwei möglichen Formen versucht werden kann: einerseits in der individuellen Kontrolle jedes Nutzers unmittelbar hinter seinem Netzzugang, d.h. am Einwahlknoten, andererseits in der globalen Abschottung einer größeren Nutzergruppe eines geschlossenen Teilnetzes, beispielsweise innerhalb eines Onli-

---

200 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 654 f.

201 Im Bereich der Newsgroups ist sowohl eine Löschung einzelner News-Artikel als auch ganzer Newsgroups möglich. Bei Newsgroups mit einem größeren Anteil rechtswidriger Inhalte ist der Aufwand für eine selektive Löschung einzelner News-Artikel für den Service-Provider erhöht. In der Praxis werden in diesen Fällen deswegen grundsätzlich nicht nur die einzelnen News, sondern die vollständigen Newsgroups vom eigenen Server gelöscht. Bei den thematisch nicht zu beanstandenden Newsgroups, die bei weitem in der Überzahl sind, löscht der Provider die Nachrichten dagegen sehr oft einzeln.

Im WWW-Dienst können von dem Betreiber des WWW-Servers sowohl einzelne Seiten als auch die vollständigen Angebote einzelner Content-Provider gelöscht oder auch nur gesperrt werden. Bei der Sperrung ist ein externer Zugriff auf das Angebot nicht mehr möglich, während bei der Löschung der gesamte Datenbestand vom WWW-Server entfernt wird. Die Sperrung erfolgt regelmäßig vorläufig und kann von dem WWW-Server jederzeit wieder freigegeben werden, wenn der rechtswidrige Inhalt beseitigt wurde. Sowohl eine Sperrung als auch eine Löschung sind mit Hilfe der Betriebssystem-Software der WWW-Server unschwer durchführbar.

Bei FTP-Servern sind Daten ebenfalls einfach zu löschen. Zudem können Inhalte für einen Download solange gesperrt bleiben, bis eine explizite Überprüfung erfolgt ist.

Auch im Bereich der E-Mails würden für den Betreiber eines Mail-Servers keine technischen Probleme bestehen, einzelne als rechtswidrig erkannte Mails zu löschen.

ne-Dienstes oder eines Staats, also am Übergangspunkt des jeweiligen Teilnetzes zum weltweiten Netz. Sowohl die Individualkontrollen als auch die Gruppen- oder Teilnetzkontrollen weisen jedoch grundsätzlich Probleme auf:

aa. Individualkontrolle

Das Konzept einer Individualkontrolle des Nutzers unmittelbar an seinem Einwahlknoten setzt – bei geschätzten 100 Millionen Internet-Teilnehmern[202] – eine große Zahl von Kontrollrechnern voraus. Insbesondere würde es aber auch eine Totalüberwachung aller User erfordern, was einen massiven Eingriff in das Fernmeldegeheimnis, in Betriebsgeheimnisse und Persönlichkeitsrechte der Nutzer mit sich bringen würde. Ein solches Konzept der Individualkontrolle aller Nutzer braucht im folgenden wegen technischer und gesellschaftlich-rechtlicher Gesichtspunkte deshalb nicht ernsthaft diskutiert werden.[203] Diese Art der Kontrolle erinnert ohnehin mehr an „1984“ von George Orwell[204] als an das Bemühen eines Rechtsstaates, rechtswidrige Internet-Inhalte zu vermeiden.

bb. Gruppen- oder Teilnetzkontrolle

Das zweite Konzept einer Abschottung geschlossener Nutzergruppen müsste dadurch realisiert werden, dass sämtliche Nutzer dieses Systems nur auf einen kontrollierten (Proxy-Cache)-Server zugreifen könnten, dessen Kommunikation mit dem weltweiten externen Datennetz durch einen sogenannten „Firewall-Rechner“[205] abgeschottet und kontrolliert würde. Dieser Weg einer Kontrolle geschlossener Nutzergruppen hätte gegenüber der Individualkontrolle eines jeden Nutzers den Vorzug, dass die Überwachung des Datenverkehrs zumindest teilweise nutzerunabhängig in anonymisierter Form erfolgen könnte und Mehrfachkontrollen des von verschiedenen Nutzern angeforderten gleichen Datenangebots vermieden würde: Nach einer einmaligen und möglichst nutzerunabhängigen Kontrolle der Daten würden diese auf dem Proxy-Cache-Server für einen freien Zugang aller Nutzer des kontrollierten Teilnetzes zur Verfügung gestellt. Einer solchen Abschottung aller nationalen Nutzer und Service-Provider gegenüber ausländischen Rechnern mit Hilfe des nationalen Proxy-Cache-Servers sowie einer Überwa-

---

202 Diese Zahlengröße geht dabei von der Anzahl der an das Internet angeschlossenen Rechner aus.

203 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 659.

204 Orwell, 1984, 33. Auflage.

205 Hage/Hitzfeld in: Loewenheim/Koch, Praxis des Online-Rechts, S. 49 f.; unter einer „Firewall“ versteht man ein Hardware- und/oder Software-Modul, das zwischen ein internes Netz und das Internet geschaltet wird, um einen unberechtigten Zugriff von außen auf Daten eines internen Netzes, beispielsweise zur Abwehr eines Hacking-Angriffs, zu vermeiden. Eine Firewall soll nach diesem Konzept also nicht verhindern, dass Nutzer eines bestimmten Netzes auf Daten im Internet zugreifen können, sondern dass unberechtigte Zugriffe von außen, vor allem aus dem Internet, auf unternehmensinterne – meist sensible – Daten abgewehrt werden.

chung des gesamten externen Datenverkehrs liegt die Kontrollstrategie der chinesischen Regierung zugrunde.[206]

Diese Konzeption der Abschottung geschlossener Nutzergruppen widerspricht jedoch nicht nur der Idee eines freien weltumspannenden Datennetzes, sondern verstößt auch gegen das Recht auf Informationsfreiheit, das im Grundgesetz[207], in der Europäischen Menschenrechtskonvention[208] sowie in der Charta der Grundrechte der Europäischen Union[209] garantiert ist.[210]

cc. Probleme der Echtzeitkontrolle von Massenkommunikation

Darüber hinaus steht jeder Versuch einer Zugangskontrolle im Internet vor dem Problem einer Kontrolle riesiger Datenmengen. Für die aus dem anfallenden Datenvolumen resultierenden Schwierigkeiten kann dabei auf die obigen Ausführungen zur Inhaltskontrolle des Service-Providers verwiesen werden.[211] Eine Zugriffskontrolle wird allerdings zusätzlich dadurch erschwert, dass die Kontrollmaßnahmen nicht statisch gespeicherte, sondern zu übermittelnde Daten betreffen. Dies hat zur Folge, dass sie in Echtzeit während der Kommunikation erfolgen müssten. Eine entsprechende Filterung, Analyse und Kontrolle des Inhalts der Datenkommunikation in Echtzeit ist aus technischen Gründen zur Zeit nicht möglich.[212] Etwas anderes würde nur gelten, wenn eine Inhaltskontrolle auf einzelne Elemente innerhalb der Datenpakete beschränkt werden könnte. Dies wäre

---

206 China praktiziert die sogenannten „chinesische Lösung". Darunter wird die totale Zensur des Internets verstanden. Bildlich gesprochen kann man sich diese Zensur wie ein sehr kleines Nadelohr vorstellen, das sich an jeder Internet-Schnittstelle zu China befindet. Lediglich regimekonforme Informationen dürfen diese Schnittstellen nach innen und außen passieren. Dadurch wird das Recht auf Information viel zu stark eingeengt und entspricht nicht den Grundsätzen eines modernen Rechtsstaates.

207 BGBl. III/FNA 100-1.

208 UNTS Bd. 213, S. 221.

209 ABl. EG Nr. C 364 vom 18.12.2000 S. 1.

210 Da – wie oben gezeigt – über die gleichen physikalischen Datenleitungen zahlreiche Dienste übertragen werden, würde eine entsprechende Kontrollstrategie den schon oben erwähnten Konflikt mit dem Fernmeldegeheimnis sowie Betriebsgeheimnissen und Persönlichkeitsrechten auch nur in einem sehr begrenzten Umfang vermeiden. Denn eine konsequente Abschottung des Proxy-Cache-Servers könnte sich nicht auf einen einzelnen Dienst des Internet beschränken, sondern müsste die gesamte Kommunikation – einschließlich des Bereichs der E-Mail – erfassen, über die ebenfalls strafbare Inhalte in das abgeschottete Teilnetz eingebracht werden können. Angesichts der weitreichenden und vielfältigen internationalen Kommunikationsmöglichkeiten – beispielsweise über Telefonverbindungen oder Satellitenkommunikation – ist eine entsprechende Abschottung geschlossener Nutzerkreise auch technisch nicht möglich. Sie gelingt selbst der chinesischen Regierung nicht und wäre in einer freiheitlichen Demokratie unvorstellbar. So wählen sich heute viele Bürger der Volksrepublik China mittels eines (insbesondere Satelliten-)Telefons in ausländische Netze ein und erhalten so vollen Zugriff auf das Internet. Dies macht deutlich, dass ein Zugriff auf ausländische Computersysteme durch den Nationalstaat heute nicht mehr verhindert werden kann. Entsprechende Konzepte kommen daher allenfalls für spezielle Teilnetze mit thematisch begrenzten Aufgabenstellungen – zu denken ist hierbei an Firmen- und Universitätsnetze – oder für spezielle Anwendungsdienste in Betracht. Vgl. Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)", CR 1997, 653, 660.

211 Vgl. oben unter B. 1. Teil. III. 1. b.

212 Vgl. hierzu auch Wischmann in: „Rechtsnatur des Access-Providing", MMR 2000, 461.

beispielsweise der Fall, wenn der Header der Datenpakete eine Signatur[213] mit einem Bewertungskriterium enthalten würde. Ein entsprechendes Labeling der Dateninhalte des Internets ist bisher allerdings nur in Ansätzen für vereinzelte Internet-Dienste vorhanden[214] und auch nur – wegen der oben angesprochenen Gründe – für statische Informationsangebote möglich.[215]

Die Probleme einer Echtzeitkontrolle des Datenzugriffs im Internet werden deutlich, wenn die dazu erforderlichen technischen Lösungen näher betrachtet werden. Denn diese technischen Lösungen bestehen insbesondere im Aufbau einer Firewall, gegebenenfalls kombiniert mit einem Proxy-Cache-Server, um den Access-Provider vor der Datenübertragung rechtswidriger Inhalte zu schützen.[216] Entsprechende Firewall-Konzepte wurden ursprünglich zu anderen Zwecken als zur Filterung strafbarer Inhalte entwickelt: Wie oben schon dargestellt,[217] versteht man unter einer Firewall klassischerweise ein Hardware- und/oder Software-Modul, das zwischen ein internes Netz und das Internet geschaltet wird, um einen unberechtigten Zugriff von außen auf Daten eines internen Netzes, beispielsweise zur Abwehr eines Hacking-Angriff, zu vermeiden. Eine Firewall soll nach diesem Konzept also nicht verhindern, dass Nutzer eines bestimmten Netzes

---

213 In der Fachsprache wird von dem sogenannten „Label" gesprochen.

214 Das am weitesten entwickelte System eines derartigen Labelings im Header der Datenpakete ist das Platform for Internet Content Selection (PICS)-System:
Der Gedanke von PICS ist, dass sowohl der Anbieter selbst als auch Dritte Inhalte bestimmter Web-Seiten nach bestimmten Kriterien abstrakt beschreiben. Hierzu werden Internet-Angebote mittels einer (Un)-Bedenklichkeitsskala nach verschiedenen Kategorien (beispielsweise Jugendschutz, politische Brisanz, Gewaltdarstellungen, Pornografie, etc.) eingestuft. Aufgrund dieser Beurteilung erhält der Inhalt eine typische Kennzeichnung, ein sogenanntes „Label". Mit einer entsprechenden Filtersoftware, die die jeweiligen Labels erkennen und auswerten kann, besteht nun die Möglichkeit, nur noch bestimmte Angebote im Internet aufrufen zu können. Das PICS-System ist der Hauptvertreter dieser sogenannten „Rating-Systeme". Gedacht ist dieses System vor allem für Eltern, die mit dem Labeling ihre Kinder vor bestimmten Inhalte schützen können, indem sie z. B. sämtliche gewaltverherrlichenden oder pornografischen Inhalte herausfiltern lassen.
Wichtig ist, dass PICS selbst neutral ist, also für sich keinerlei Maßstäbe definiert, sondern allein zur Erfassung, Darstellung und dem Austausch der Bewertungen dient. Deshalb weist dieses System auch gravierende Schwächen auf. So ist nicht garantiert, dass sich gewisse „Schwarze Schafe" im Netz diese Methode des Labeling zu Nutze machen, um gezielt gerade die indizierten Inhalte aufrufen zu können. Des weiteren gibt es Probleme bei der Bewertung der einzelnen Inhalte. Denn schon allein auf Grund der verschiedenen Kultur- und Religionskreise in Europa bestehen zahlreiche Unterschiede hinsichtlich der Auffassung, welcher Inhalt wie zu beurteilen ist. Zudem gibt es keine Gewähr, dass sämtliche Angebote im Internet mit einem derartigen Label ausgestattet sind und falls ja, ob dieses Label auch dem Inhalt entspricht.
Es lässt sich somit zusammenfassend sagen, dass das PICS-System und die übrigen Rating-Systeme noch in den Kinderschuhen stecken. Zu viele Fragen sind bis jetzt nicht ausreichend geklärt. Eine effektive Inhaltskontrolle ist deswegen im Moment nicht möglich. Vgl. hierzu ausführlich Geis, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen", CR 1999, 772, 776; Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)", CR 1997, 653, 654 Fn. 134; Mayer, Das Internet im öffentlichen Recht, S. 84; Vielhaber, „Neuer Schutz vor neuen Gefahren? – Jugendschutz im Internet", MMR-Beilage 9/2001, 16, 19.

215 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)", CR 1997, 653, 660.

216 Vgl. hierzu ausführlich Riehm, „Die Brandschutzmauer", NJW-CoR 1997, 337 ff.

217 Vgl. oben unter B. 1. Teil. III. 1. c. bb.

auf Daten im Internet zugreifen können, sondern dass unberechtigte Zugriffe von außen, vor allem aus dem Internet, auf interne – meist sensible – Daten abgewehrt werden. Eine „umgekehrte Firewall“ wird allerdings vor allem dann eingesetzt, wenn in einem Computernetz die zu erwartende Netzlast reduziert werden soll, indem beispielsweise Internet-Dienste mit einem traditionell hohen Datenverkehrsvolumen eingeschränkt werden, um den übrigen Datenverkehr ohne zeitliche Verzögerung reibungslos abwickeln zu können. Darüber hinaus haben Firewalls häufig auch „Auditfunktionen“, womit die Aktionen der Nutzer mitprotokolliert werden. Konzept, Technologie und Aufwand für eine solche „umgekehrte“ Firewall unterscheiden sich jedoch wesentlich von der sonst üblichen Firewall. Während die klassische Firewall den Schutz etwa eines Unternehmensnetzes vor unbefugten Zugriffen mit Hilfe eines relativ kleinen Computersystems verwirklichen kann, würde die umgekehrte Firewall eines Access-Providers zur Kontrolle der Zugriffe Tausender deutscher Internet-Nutzer auf bestimmte (ausländische) Rechner eine damit unvergleichbar größere Rechenleistung erfordern und zu erheblichen Performance-Verlusten sowohl im Bereich der Provider als auch der Nutzer führen.[218]

Eine derartige Analyse des gesamten Dateninhalts ist auch nicht Ziel des klassischen und eng begrenzten Firewall-Konzepts zum Schutz von Rechnern gegen die Benutzung unbefugter Personen. Denn Firewall-Konzepte beruhen grundsätzlich nicht darauf, dass der gesamte Inhalt von Nachrichten, sondern nur die im Header der Datenpakete enthaltenen Informationen kontrolliert werden und gegebenenfalls das gesamte Datenpaket blockiert wird (sogenannte Paketfilterung). Eine klassische Firewall des Internets kontrolliert deswegen nur die in den Headern der übertragenen Datenpakete gespeicherten IP-Adressen sowie die genannten Ports, die den jeweils verwendeten Internet-Dienst charakterisieren. Dabei sind in der Regel zwei Blockade-Entscheidungen möglich: Es können entweder bestimmte IP-Adressen oder Ports blockiert werden.[219] Alternativ werden alle Adressen sowie Ports blockiert und nur bestimmte Adressen durchgelassen.[220]

---

218 Die vom Bayerischen Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst eingesetzte Arbeitsgruppe „Hochschulnetze in Bayern“ stellte dazu in ihrem 1997 erschienenen gleichnamigen Schlussbericht (S. 61) fest:
„Es ist klar, dass Firewalls zwei Arten von Einschränkungen nach sich ziehen: Performance-Verluste sowie Nutzungseinschränkungen bei den möglichen Diensten. Die Performance-Verluste sind bedingt durch die (je nach Grad des Firewall-Einsatzes) erforderliche detaillierte Analyse der über die Schnittstellen fließenden Daten. Bei der zu erwartenden weiteren Steigerung der Netzgeschwindigkeit kommt solchen Aspekten erhöhte Bedeutung zu. Die Nutzungseinschränkungen sind unter dem Gesichtspunkt der Offenheit der Netze höchstens für bestimmte Nutzergruppen (beispielsweise im Verwaltungsbereich) möglich, wo sie auch teilweise realisiert sind. Eine weitergehende individualisierte Sperrung bzw. Freigabe von Diensten ist schon aus administrativen Gründen nicht praktikabel (wer entscheidet darüber, wer wo Zugang hat ?). Die im kommerziellen Bereich verbreitete Firewall-Technik ist also nur sehr eingeschränkt auf die Situation an Hochschulen übertragbar.“

219 Dies nennt man auch das Prinzip des „Forward but ...“.

220 Dies nennt man auch das Prinzip des „Block all but ...“.

(1) Sperrung von Internet-Adressen

Adressensperrungen stellen allerdings gravierende Eingriffe in das Datennetz dar, da die IP-Adressen von Servern teilweise die Angebote tausender Einzelanbieter den Nutzern zugänglich machen. Die Sperrung von IP-Adressen trifft deswegen nicht nur den einzelnen zu sperrenden Inhalt, sondern im erheblichen Umfang auch die legale Geschäftstätigkeit und Kommunikation im Internet. Allerdings kann selbst eine solche – den Datenverkehr im Internet wesentlich einschränkende – Adressensperrung die Verbreitung unerwünschter Dateninhalte nur bedingt verhindern. Denn der Betreiber des Servers braucht lediglich seine IP-Nummer zu wechseln, damit er wieder erreichbar ist.[221]
Als Gegenmaßnahme müsste deswegen die Sperrung der Nummernfolge eines ganzen Netzes in Betracht gezogen werden. Dies hätte jedoch zur Konsequenz, dass sämtliche Computersysteme innerhalb eines Netzbereichs nicht mehr erreichbar wären. Dadurch würden beispielsweise Server gesperrt, die für besondere wissenschaftliche Fachdiskussionen oder die geschäftliche Kommunikation von Firmenkunden unverzichtbar sind. Die Sperrung einzelner IP-Adressen oder ganzer Nummernfolgen bedeutet demnach einen nicht unerheblichen Eingriff in die wirtschaftliche und wissenschaftliche Funktion des Internets sowie den grenzüberschreitenden freien Datenaustausch.
Eine Sperrung von Internet-Adressen bliebe jedoch auch deshalb nur begrenzt wirkungsvoll, weil ein durch die Sperrung vermeintlich eingeschränkter Nutzer auf die Inhalte der gesperrten Adresse nicht nur dann zugreifen kann, wenn diese Inhalte auf anderen, ungesperrten Servern vorhanden sind. Er hat auch die Möglichkeit, auf einen Anonymisier-Dienst im Internet zuzugreifen.[222] Der Nutzer gibt die gewünschte Adresse – hier des gesperrten Servers – in ein virtuelles Formular ein und bekommt umgehend die gewünschten Daten. Die Sperre greift in diesem Fall deshalb nicht, weil die angezeigten Daten für die sperrende Stelle nicht die originale Herkunftsadresse aufweisen, sondern die des anonymisierenden Servers. Eine identische Wirkung entfaltet die Nutzung von Proxy-Cache-Server anderer Provider. Auch hier sind die Daten des gesperrten Servers nicht als solche in der Adresse erkennbar. Die Nutzung dieser Server ist mit einigen Einträgen in die Browser-Software durch den Nutzer möglich. Adressen

---

221 Derartige Wechsel der IP-Nummern finden auch unter normalen Umständen statt, z.B. wenn ein Server an seine Kapazitätsgrenzen stößt und entweder durch einen neuen Server ersetzt oder ergänzt wird. Die sich dadurch ergebende Neuorganisation der Serverstruktur hat dann regelmäßig auch eine Änderung der IP-Nummer zur Folge.

222 Hierbei kann es sich z.B. um WWW-Server handeln, die wie Browser für das Internet erscheinen. Ein solcher Server kann etwa unter http://www.anonymizer.com (zuletzt abgerufen am 08.04.2002) genutzt werden.
Der Begriff „Browser“ stammt vom englischen Wort „to browse“ = schmökern, stöbern ab. Ein Browser ist das Gleiche wie ein Navigationsprogramm im Internet. Er stellt ein einfach zu bedienendes und fensterorientiertes Programm mit grafischer Nutzeroberfläche zum bequemen Verschaffen eines Überblicks über große Datenbestände und zur Untersuchung und Bearbeitung einzelner Datensätze im Detail dar. Zu den am weitest verbreiteten Browsern für das WWW gehören die Browser von Netscape und der Microsoft Explorer.

von Proxy-Cache-Servern, die angeforderte Informationen lokal vorrätig halten, anstatt sie über Interkontinentalleitungen immer wieder anzufordern, sind über Such-Server oder spezielle Listen auffindbar.
Darüber hinaus ist es möglich, dass der Nutzer zum Kunden eines ausländischen, nicht sperrenden Providers wird und seine Datenkommunikation über diesen abwickelt.[223] Bei Benutzung eines solchen „Exil-Logins“ registriert der sperrende Provider nur die Kommunikation mit dem ausländischen Provider, nicht jedoch die Kommunikation mit dem gesperrten Server.
Insgesamt lässt sich somit festhalten, dass die Sperrung von IP-Adressen grundsätzlich mit relativ wenig Aufwand umgangen werden kann. Allerdings müsste der Nutzer, der die Sperrung umgehen will, selbst aktiv werden. Viele Nutzer verfügen aber nicht über das Wissen, diese Umgehungsmaßnahmen durchzuführen und sind auch zu bequem, auf derartige Maßnahmen zurückzugreifen, um an den gesperrten rechtswidrigen Inhalt zu gelangen. Deshalb ist eine Sperrung – abgesehen von den ungewünschten Nebeneffekten im Netz – dennoch in manchen Fällen sinnvoll, da das Gros der User durch die Sperrung effektiv an dem Zugriff von rechtswidrigen Inhalten gehindert wird.

(2) Sperrung von Ports

Als weitere Möglichkeit zur Verhinderung des Austausches rechtswidriger Daten im Internet kommt noch die Sperrung von Ports und damit die komplette Sperrung von Internet-Diensten in Betracht. Jeder Dienst im Internet besitzt eine bestimmte Port-Nummer.[224] Der Service-Provider könnte deswegen einen bestimmten Port für seine Nutzer sperren, so dass ein Zugriff auf alle Server des jeweiligen Internet-Dienstes zunächst unmöglich wäre.
Eine solche komplette Sperrung wegen einzelner rechtswidriger Inhalte würde allerdings nicht nur einen wichtigen Teil des Internets lahm legen, sondern wäre auch ineffektiv: Bei Bekanntwerden einer derartigen Sperrung würden die jeweiligen Server nur die Port-Nummer wechseln. Da zahlreiche noch ungenutzte Port-Nummern zur Verfügung stehen, wäre ein solcher Wechsel auch jederzeit möglich. Die für die Sperrung verantwortlichen Personen müssten deswegen permanent überprüfen, ob nicht ein Wechsel der Port-Nummern stattgefunden hat und die Inhalte der gesperrten Server damit wieder zugänglich gemacht würden. Dies wäre praktisch nicht durchführbar.
Darüber hinaus würden derartige Sperrungen von Ports vor allem die geschäftliche Nutzung des Internets stören, da mit der Sperrung der Ports auch die speziellen Dienste der Geschäftsnetze unerreichbar blieben.
Schließlich wäre für die Verhinderung rechtswidriger Inhalte selbst nur kurzfristig etwas gewonnen, weil die Nutzer auf andere Informationsdienste des Internets zurück-

---

223 Entsprechende „Exil-Logins“ werden von verschiedenen Providern angeboten.
224 Beispielsweise besitzt der News-Dienst im Internet die Port-Nummer 119.

greifen könnten. Denn durch die Sperrung eines bestimmten Ports ist nur der dahinterstehende Dienst gesperrt. Alle übrigen Informationsdienste im Internet, die mittlerweile – meistens über das WWW – auch untereinander Verbindungen aufweisen, bleiben somit erreichbar.
Die Sperrung von Ports ist deshalb nicht der richtige Weg, um die Verbreitung von rechtswidrigen Inhalten im Internet zu unterbinden. Denn die Nachteile der Sperrung der Ports überwiegen bei weitem die kaum zu erkennenden Vorteile.

(3) Inhaltsauswertung mit Hilfe eines Application Gateways

Mit Hilfe moderner Firewall-Programme ist es allerdings auch möglich, unter Verwendung eines sogenannten „Application Gateway“[225] Informationen über die in den IP-Paketen enthaltenen Daten auf der Anwendungsschicht auszuwerten. Dabei wird vor allem auf die Header-Informationen in den Anwendungsdiensten abgestellt. Diese Header-Informationen betreffen insbesondere den Dateityp,[226] den Dateinamen oder im Fall von News die Artikelbezeichnung. Identifizierbar sind auch Typ und Name von Binärdateien, die bei E-Mail, News und WWW-Seiten oft beigefügt werden.[227] Es können aber auch die Inhalte der Dateien gefiltert werden. Um die konkreten Inhalte zu interpretieren, muss ein Application Gateway allerdings die Anwendungssoftware des Nutzers erkennen können. Ein Application Gateway müsste deswegen bei einer echten Inhaltskontrolle eine Vielzahl von Anwendungen simulieren. Voraussetzung wäre hierfür zunächst, dass der Betreiber des Application Gateways die Anwendungssoftware

---

225 Ein „Application Gateway“ ist eine zusätzliches Hard- und/oder Softwaremodul, das in die Firewall integriert wird. Der Application Gateway wird somit Bestandteil der Firewall.
Application Gateways sind grundsätzlich die langsamsten Formen von Firewalls und werden deswegen normalerweise nur von Unternehmen eingesetzt, die ein besonders hohes Sicherheitsbedürfnis haben.

226 So können etwa anhand der Dateiendung „.doc“ der Dateityp „MS Word“ und an der Endung „.xls“ der Dateityp „MS Excel“ erkannt werden.

227 Häufig werden Funktionalität oder Erscheinungsbild von WWW-Seiten durch zusätzliche „dynamische“ Programme, z.B. „Java“- oder „ActiveX“-Applikationen, ergänzt. Vor ihrer Verwendung müssen diese jedoch geladen werden und kommen erst dann auf dem Computer des Betrachters zur Ausführung. Weil diese Applikationen potentielle Überträger von „Computer-Viren“ oder sogenannten „trojanischen Pferden“ sein können, werden sie häufig als zu vermeidende Sicherheitsrisiken eingestuft, die durch ein Application Gateway blockiert werden sollen. Ein Application Gateway kann daher so konfiguriert werden, dass bestimmte Dateitypen die Firewall nicht passieren dürfen. Hierdurch wird grundsätzlich eine selektive Verhinderung des Zugriffs auf bestimmte Dateien möglich.
Die Phantasiebezeichnung „Computerviren“ ist abgeleitet von dem medizinischen Virus, welches von innen her krankhafte Störungen am Menschen und Tier verursacht. Bei den Computer-Viren handelt es sich um in den Computerablauf eingebrachte Störkommandos, welche jedes andere Programm verwenden oder zerstören können. Die Abwehr hierfür ist noch in der Forschung. Vgl. hierzu Rutkowsky/Gerhardt, Leitfaden des Computerrechts, S. 42.
Ein „trojanisches Pferd“ kann zum einen selbst ein Virus sein: Kennzeichen hierfür ist, dass sie vorgeben, vom Nutzer gewünschte Zwecke zu erfüllen oder dies auch tatsächlich tun. Nebenher führen sie jedoch – vom ahnungslosen Nutzer unentdeckt – weitere unerwünschte Operationen, wie das Ausspähen von geheimen Daten, durch. Zum anderen kann ein trojanisches Pferd lediglich Trägermedium sein: Diese voll funktionstüchtige Trägersoftware dient dazu, den Virus von einem Rechner zum nächsten zu transportieren.

zunächst, dass der Betreiber des Application Gateways die Anwendungssoftware kennt.[228] Die übermittelten Daten dürften zudem nicht verschlüsselt sein.
Bei dem großen Datenaufkommen im Internet wäre aber bereits der – in Echtzeit vorzunehmende – rechnerische Aufwand einer solchen Firewall zur Transformation der Daten in die Anwendungsschicht technisch nur schwer zu bewältigen. Der Einsatz von Application Firewalls zur Ausfilterung bestimmter Inhalte würde jedoch vor allem deswegen Probleme bereiten, weil die Firewall auch mit einem Mechanismus zur Bewertung der rechtswidrigen Inhalte verknüpft werden müsste. Die obigen Ausführungen zur Inhaltskontrolle machen deutlich, dass eine solche Bewertung in Echtzeit angesichts des im Internet übertragenen Datenvolumens nicht möglich ist.[229] Ein entsprechendes Konzept der Filterung rechtswidriger Inhalte mit Hilfe einer Firewall wäre also nur dann möglich, wenn die zu filternden Inhalte zuvor erfasst, bewertet und in eine von der Firewall genutzten Liste aufgenommen würden. Dies ist allerdings bisher kaum der Fall.[230] Ein entsprechendes Konzept wäre insbesondere auch hinsichtlich der verschiedenen angebotenen Dienste im Internet fraglich: Wird eine über das WWW erhältliche Informationsseite für den WWW-Dienst anhand einer vorhandenen Sperrliste blockiert, bleibt sie weiterhin, z.B. über FTP, aber auch über alle anderen Internet-Dienste erreichbar. Derartige Listen müssten deshalb für jeden Dienst separat erstellt und laufend aktualisiert werden.[231]

dd. Grundsätzliche Probleme bei speziellen Netzwerkprotokollen

Die vorausgegangenen Ausführungen zeigen, dass der Einsatz einer Firewall zur Filterung von Header-Dateien oder Dateninhalten im Internet voraussetzt, dass die zu filternden Daten mit dem TCP/IP-Protokoll übertragen oder entsprechend dargestellt werden. Falls das von einem Access-Provider genutzte oder einem Network-Provider betriebene Netz jedoch auf keinem Teilabschnitt des Verbindungsweges das TCP/IP-Protokoll verwendet wird,[232] wirft der Einsatz einer Firewall zusätzliche Probleme auf. Werden beispielsweise Daten mit einem X.25-Protokoll transportiert, so können die Router und andere Zugangsknoten nur Steuerungsinformationen der X.25-Datenpakete lesen, nicht jedoch den von ihnen transportierten Inhalt. So erkennt z.B. das X.25-

---

228 Schon allein dies wirft einige Schwierigkeiten angesichts der Vielzahl an übermittelten Anwendungsdiensten und Protokollen auf.

229 Gercke, „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks“, ZUM 2001, 34, 36.

230 Zu dem schon oben erwähnten System des PICS siehe Fn. 214.

231 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 660 f.

232 Dies ist beispielsweise dann der Fall, wenn ein Access-Provider über keine eigenen Verbindungen verfügt und gegen Entgelt die – oft international verlaufenden – Leitungswege eines Network-Providers nutzt, um seinen Kunden bestimmte Dienste zu ermöglichen. Die Leitungswege werden hierbei häufig mit dem X.25-Protokoll betrieben. Das X.25-Protokoll hat insoweit die Funktion eines „Datenvehikels“, weil reine – im TCP/IP-Protokoll vorliegende – Internet-Daten, aber auch andere z.B. mit proprietären Protokollen versandte Daten hiermit transportiert werden.

Protokoll nicht, ob es sich bei den transportierten Daten um TCP/IP-Pakete oder um Pakete eines anderen Netzwerkprotokolls handelt. Notwendig wäre deswegen eine Umwandlung der X.25-Daten in TCP/IP-Daten, die dann gegebenenfalls die Kontrolle einer Firewall durchlaufen könnten. Eine derartige Umwandlung würde jedoch schon im Hinblick auf die Konvertierung der Datenpakete hohe Anforderungen an die Technik stellen. Hierdurch ist zwar eine Sperrung von IP-Adressen nicht sehr stark beeinträchtigt, da allenfalls der Header entschlüsselt werden muss. Innerhalb von X.25-Netzen kann allerdings eine solche Lösung an den hohen Datenmengen auf nationalen und internationalen Weitverkehrsverbindungen scheitern.[233]

ee. Verschlüsselung

Die durch spezielle Netzwerkprotokolle und deren unterschiedliche Schichten entstehenden Probleme der Identifizierung des Inhalts der übertragenen Datenpakete steigern sich innerhalb einer Nutzergruppe um ein Vielfaches, wenn die Daten verschlüsselt oder versteckt übertragen werden. Sobald entsprechend starke Verschlüsselungsalgorithmen angewandt werden, können Filterprogramme bestenfalls den Ein- oder Ausgang verschlüsselter Daten feststellen. Eine Entschlüsselung der Daten ist dann nur noch theoretisch, aber nicht mehr praktisch möglich. Verschlüsselungsprogramme werden im Internet zwar noch nicht sehr häufig eingesetzt. Die Verschlüsselung von Daten wird in der Zukunft jedoch vor allem mit der Verbreitung von multimediafähigen Computern in allen Datennetzen stark zunehmen. Vor allem Straftäter werden – innerhalb geschlossener oder quasi-geschlossener Nutzergruppen – die Möglichkeit der Verschlüsselung nutzen.[234]

d. Zwischenergebnis

Ein Content- oder Service-Provider kann rechtswidrige Inhalte auf seinem Rechner mit einfachen Mitteln löschen oder sperren. Problematisch ist jedoch beim Service-Provider das Auffinden solcher Inhalte. Hier erscheint es sinnvoll, dass sich der Service-Provider – anstelle einer aufwändigen Suche – auf bereits bekannte rechtswidrige Bereiche konzentriert und zumindest diese entweder löscht oder sperrt.[235]

Für den Access-Provider stellt die Sperrung des Zugangs zu fremden Servern mit rechtswidrigen Inhalten die einzige Maßnahme dar, um gegen diese Inhalte vorzugehen und ihre Verbreitung zu verhindern. Da sich die rechtswidrigen Inhalte auf fremden Rechnern befinden, können sie nicht von außen – wegen fehlender Verfügungsgewalt –

---

233 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 661 f.

234 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 662.

235 Dies kann auch dadurch geschehen, dass Dritte den Service-Provider auf rechtswidrige Inhalte eines Content-Providers, die er auf seinem Rechner gespeichert hat und für die Nutzer im Netz bereithält, aufmerksam machen.

durch Löschen vernichtet werden. Für den einzelnen Access-Provider bleibt deswegen nur die Möglichkeit, den Zugriff auf fremde Server dadurch zu verhindern, dass er die IP-Adresse des fremden Content- oder Service-Providers sperrt.[236] Eine derartige Kontrolle des Zugriffs auf fremde Rechner stößt aufgrund der oben dargestellten technischen Gegebenheiten allerdings auf erhebliche Probleme.

2. Staatliche Kontrollmöglichkeiten

a. Zugriffskontrolle auf fremde Server

Die Behörden halten in der Regel selbst keine rechtswidrigen, gespeicherten Daten im Internet bereit, worauf sie Einfluss nehmen könnten. Auch bieten sie üblicherweise den Internet-Nutzern keinen Zugang zum Netz an. Dies bedeutet, dass für sie ein direktes Einwirken auf bestimmte Inhalte im Internet nicht möglich ist. Fraglich ist jedoch, ob sie über das Internet mit staatlichen Rechnern auf fremde Server der Content- bzw. Service-Provider kontrollierend einwirken können. Dies wäre dann denkbar, wenn es ihnen technisch machbar ist, auf fremden Servern Inhaltskontrollen und anschließend eine Löschung bzw. Sperrung der darauf befindlichen rechtswidrigen Inhalte durchzuführen. Eine Zugriffskontrolle auf fremde Rechner durch staatliche Behörden scheitert jedoch schon an der Inhaltskontrolle. Dafür fehlt es nämlich noch an den technischen Voraussetzungen.[237] Hinsichtlich dieser technischen Schwierigkeiten bei der Identifizierung rechtswidriger Inhalte auf fremden Rechnern kann zunächst auf die obigen Ausführungen zur Identifizierung rechtswidriger Inhalte beim Server des Service-Provider verwiesen werden.[238] Unter Einbeziehung fremder Computersysteme steigern sich diese Probleme allerdings noch um ein Vielfaches: Die Identifizierung rechtswidriger Inhalte ist nicht nur durch die eingeschränkte Abfragemöglichkeit auf fremden Rechnern, sondern vor allem durch die Masse des weltweit verfügbaren Datenangebotes zusätzlich erschwert.

Dies hat zur Konsequenz, dass der Versuch einer weltweiten Kontrolle der im Internet zugänglichen Inhalte durch staatliche Behörden zur Zeit aussichtslos ist. Aus diesem Grund kann es für die Konzeption eines Kontrollsystems und für die Beurteilung von sinnvollen und vor allem machbaren Kontrollmaßnahmen nur noch um die Frage gehen, ob es wenigstens möglich ist, auf einzelne, bereits als rechtswidrig erkannte Inhalte kontrollierend einzuwirken.

---

[236] Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 659.
Die Sperrung von Ports stellt wegen der genannten gravierenden Auswirkungen auf das Netz keine sinnvolle Kontrollmöglichkeit dar.

[237] Auch der Datenschutz würde derartige Inhaltskontrollen wohl verbieten.

[238] Vgl. oben unter B. 1. Teil. III. 1. b.

b. Staatliche Anordnungen gegenüber den Providern

Da die Behörden aufgrund unzureichender Technik nicht direkt auf rechtswidrige Inhalte Einfluss nehmen können, müssen sie auf die jeweiligen Provider zurückgreifen, um eine Kontrolle des Internets zu ermöglichen. Wie bereits oben dargestellt,[239] kann aus technischen Gründen weder dem Service- noch dem Access-Provider eine Inhaltskontrolle aufgetragen werden. Der Content-Provider kennt zwar seine Inhalte. Wenn er jedoch rechtswidrige Angebote in das Internet eingestellt hat, wird er diese sicherlich nicht freiwillig wieder beseitigen wollen. Letztendlich bleibt dem Staat deshalb nur die Möglichkeit, gegen bereits (ihm) bekannte, unerwünschte Inhalte im Netz vorzugehen.[240] Da er selbst nicht über die Technik verfügt, um diese Daten zu sperren und/oder zu löschen, muss er sich an die Provider wenden. Dies geschieht durch entsprechende Lösch- bzw. Sperrverfügungen gegenüber den Providern. So kann die dafür zuständige Behörde sowohl den Content- als auch den Service-Provider, der rechtswidrige Inhalte für die Nutzer bereithält, auffordern, diese Angebote zu sperren oder zu löschen, falls ersteres nicht ausreicht, um einen umfassenden Schutz zu gewährleisten. Des weiteren besteht die Möglichkeit, falls die Content- bzw. Service-Provider nicht erreichbar sind,[241] gegenüber den Access-Providern anzuordnen, dass sie den Zugriff des Nutzers auf bestimmte Inhalte sperren sollen.[242] Denn auch mit entsprechenden rechtlichen Anordnungen ist eine Löschung nicht durchsetzbar, sofern sich die Server auf fremden Hoheitsgebiet befinden und Instrumente der Amts- oder Rechtshilfe nicht kurzfristig funktionieren. Natürlich sind bei den Sperr-Verfügungen gegen den Access-Provider die technischen Schwierigkeiten und die negativen Auswirkungen im Netz zu berücksichtigen.

c. Zusammenfassung

Obwohl die staatlichen Behörden aus technischen Gründen nicht in der Lage sind, das gesamte Internet gezielt auf rechtswidrige Inhalte zu durchsuchen, besitzt der Staat mit seinen Verfügungen gegen die jeweiligen Provider ein wirksames Mittel, um gegen rechtswidrige Inhalte im Netz vorzugehen. Allerdings setzt dies voraus, dass er Kenntnis von den betroffenen Inhalten hat. Dies ist – abgesehen von Hinweisen durch die Internet-Gemeinde – nur möglich, wenn der Staat ständig durch bestimmte zuständige Stellen das Internet durchsuchen lässt, um neue unerwünschte Seiten zu finden. Dies ist zwar sehr aufwändig, stellt aber zur Zeit das einzige Mittel dar, um gegen die rechtswidrigen Inhalte vorgehen zu können.

---

239 Vgl. oben unter B. 1. Teil. III. 1. b. und c.

240 Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001 S. 27.

241 Beispielsweise befinden sich die Inhaltsanbieter im Ausland.

242 Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 351.

Die Verfügungen gegen die Content- und Service-Providern sind insgesamt unproblematisch, da sie rasch und unkompliziert den betroffenen Inhalt sperren bzw. löschen können. Dagegen ergeben sich wegen der negativen Nebeneffekte bei der Sperrung von Internet-Adressen durch den Access-Provider bei einer solchen Anordnung erhebliche Schwierigkeiten. Gleichwohl erscheint es sinnvoll, diese Sperrungen von rechtswidrigen Inhalten auf fremden Servern durchzuführen. Denn die Wirkung, die von einer – wenn auch aufwändigen – Sperrung ausgeht, darf nicht unterschätzt werden. So findet durch diese Indizierung eine Unterscheidung zwischen legalen und illegalen Internet-Bereichen statt. Hierdurch entsteht eine gewisse Sensibilisierung der Internet-Nutzer. Daneben kann durch eine Sperrung von Internet-Seiten der „normale“ User durchaus davon abgehalten werden, auf den rechtswidrigen Inhalt eines fremden Providers zuzugreifen. Der erzieherische Wert von solchen Maßnahmen ist ebenfalls von einer nicht zu unterschätzenden Bedeutung. Wichtig ist in diesem Zusammenhang auch der Gesichtspunkt, dass der technische Fortschritt gerade auf dem Informations- und Telekommunikationssektor stetig zunimmt.[243] Folglich werden die im Moment noch technisch nicht ganz ausgereiften Kontrollmaßnahmen bald effizienter arbeiten können. So werden die Firewalls mit der großen Datenmenge leichter zurecht kommen. Auch die Sperrung von einzelnen IP-Adressen kann in naher Zukunft so ausgestaltet werden, dass das übrige Netz nicht zu stark beeinträchtigt wird. Es wäre also kurzsichtig, die jetzt technisch noch unausgereiften Kontrollmaßnahmen wegen ihrer oben dargestellten Nachteile ohne weiteres ad acta zu legen.

Entsprechende staatliche Verfügungen dürfen allerdings gegen den durch sie belasteten Provider jedoch nur ergehen, sofern dafür eine gesetzliche Grundlage vorhanden ist.[244] Deshalb ist nach ausführlicher Darstellung der technischen Möglichkeiten für die staatliche Anordnung einer Löschung bzw. Sperrung von rechtswidrigen Inhalten ist es nun zwingend erforderlich nach den Rechtsgrundlagen für die staatlichen Kontrollmaßnahmen im Internet zu fragen.

---

243 Henkel, Tagungsbericht zum VII. Hamburger Datenschutzkolloquium, CR 1999, 536 f.

244 Dies ergibt sich aus dem Rechtsgrundsatz des Gesetzesvorbehalts.

2. Teil - Rechtliche Rahmenbedingungen für eine Kontrolle des Internets

Es gibt verschiedene Rechtsgrundlagen, die für eine Kontrolle des Internets in Frage kommen. So hat die Internet-Gemeinde mittlerweile bestimmte Verhaltenskodizes ins Leben gerufen, die als sogenanntes „Cyberlaw“[245] das Internet in einem gewissen Rahmen regeln sollen. Auch die EU versucht zunehmend auf die Frage einer Kontrolle im Internet durch verschiedene Richtlinien und Absichtserklärungen Einfluss zu nehmen. Schließlich existieren darüber hinaus verschiedene nationale Internet-Regelungen. In Deutschland sind in diesem Zusammenhang vor allem das Teledienstegesetz (TDG), der Mediendienste-Staatsvertrag (MDStV) und das Telekommunikationsgesetz (TKG) als wichtige Normen zu nennen.

I. Cyberlaw

Unter dem Begriff „Cyberlaw“[246] wird die Regelung des Internets in einem eingeschränkten Sinne verstanden. Legislative Regulierungen von außen werden diesem Begriff nicht zugeordnet.[247] Es geht hierbei einzig und allein um interne Normierungen des Internets, welche die Teilnehmer des Internets oder ihre autorisierten Gremien selbst entwickelt haben.[248] Das Cyberlaw ist entwickelt worden, weil ein großer Teil der Internet-Gemeinde der Meinung war, dass ein eklatanter Widerspruch zwischen der Globalität des Internets und dem nationalen Charakter der realen Welt bestehe. Demnach seien die einzelnen nationalen Vorschriften nicht mehr fähig, eine Ordnung in die virtuelle Welt des Internets zu bringen. Das Internet sei als „Cyberspace“[249] unabhängig von staatlichen Regelungs- und Kontrollinstanzen.[250] Auch völkerrechtliche Verträge wären

---

245 Dieser Begriff setzt sich aus den englischen Wörtern „cyperspace“ und „law“ zusammen. Es handelt sich hierbei um einen Phantasiebegriff, der mit „Recht für den virtuellen Raum“ übersetzt werden kann.

246 Vgl. hierzu auch Lehmann in: Lehmann, Internet- und Multimediarecht, S. 34; Mayer, „Recht und Cyberspace“, NJW 1996, 1782 ff.

247 Vgl. zu diesem Thema auch von Hinden, Persönlichkeitsverletzungen im Internet, S. 242 ff.
Problematisch ist an dieser Stelle, dass der Begriff des „Cyberlaw“ nicht immer einheitlich gebraucht wird. So betrachtet Bleisteiner in: Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 72 ff. lediglich die nationalen Vorschriften des TKG, des TDG und des MDStV als Cyberlaw im engeren Sinne. Zwar stellen diese Regelwerke z.T. die Rechtsgrundlage für eine Kontrolle des Internets dar (vgl. unten unter B. 2. Teil. II.). Allerdings wird hier der Begriff anders gebraucht. Nämlich als interne Normierung des Internets durch die im Internet beteiligten Personen und nicht durch Regelungen, die eine außenstehende Staatsmacht entwickelt hat.

248 Osthaus, „Die Renaissance des Privatrechts im Cyberspace“, AfP 2001, 13, 15.

249 Vgl. Fuentes-Camacho, The International Dimensions of Cyberspace Law, Band 1, S. 1. Der Begriff „Cyberspace“ stammt ursprünglich aus der 1984 erschienenen Novelle „Neuromancer“ von William Gibson. Dort heißt es:
“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation.“ Gibson, Neuromancer, S. 51.
In Gibsons Zukunftsvision ist die „consensual hallucination“ noch perfekter als derzeit im Internet, weil das menschliche Bewusstsein unmittelbar an den Computer angeschlossen werden kann.

250 Mayer, „Recht und Cyberspace, NJW 1996, 1782, 1790; Johnson/Post, Stanford Law Review 48 (1996) 1367, 1370, 1378, 1387; Bechtold, „Multimedia und Urheberrecht“, GRUR 1998, 18, 23; vgl.

aufgrund fehlendem Einigungswillen der jeweiligen Nationalstaaten nicht im Stande, eine vernünftige Ordnung des Internets herbeizuführen. Folglich müssten neue, für das Internet taugliche Regeln geschaffen werden. Im Zuge dieser Überlegungen hat sich die sogenannte „Cyberspace-These“[251] herausgebildet, die sich auf das Grundrecht der Informationsfreiheit beruft und den sogenannten „Global Free Flow of Information“[252] propagiert.[253] Nach dieser Theorie stellt der Cyberspace – die virtuelle Welt des Internets – im Vergleich zur realen bzw. physischen Welt eine völlig andere dar. Denn in der Realität gibt es Grenzen und eine territoriale Aufteilung. Jede Nation besitzt ihre Souveränität und regelt alle Lebensbereiche mit den für sie gültigen Gesetzen. Sämtliche Verhaltensweisen der einzelnen Bürger haben ihre Entsprechung in den dafür vorgesehenen Normen. Hierdurch besteht eine gewisse räumliche Nähe zwischen den Bürgern und ihren Organen.[254] Demgegenüber hat der Cyberspace keine geographischen Grenzen. Die Teilnehmer am Internet kennen keine bestimmte enge Beziehung zu speziellen Internet-Bereichen, sondern alle Vorgänge sind für alle global am Internet Teilnehmenden gleich wichtig. Ein territoriales Bewusstsein existiert nicht mehr. Der Cyberspace-These zufolge ist das Internet nicht nur Kommunikationsmittel, das Daten von A nach B bringt und somit zwei Territorien samt ihrer Rechtsbereiche berührt, sondern ein eigener Raum mit eigenständigem Recht. Streitige Vorgänge spielen sich immer nur im Netz ab, wodurch nationales Recht nie betroffen sein kann.[255] Diese Ausschließlichkeit des Ablaufs sämtlicher Vorgänge innerhalb des Cyberspace hat zur Folge, dass auch nur internes Recht diese Vorgänge regeln kann.[256] Aus diesem Grund ist das Cyberlaw entstanden. Hauptmerkmal des Cyberlaw ist eine Regelung des Internets auf niedrigstem Niveau.

---

hierzu auch die „Declaration of the Independence of Cyberspace“, die John Barlow am 8.2.1996 im Internet veröffentlichte, siehe z.B. http://www.eff.org/~barlow/Declaration-Final.html (zuletzt abgerufen am 08.04.2002).

251 Hauptvertreter dieser These sind die US-amerikanischen Autoren Johnson und Post in: „Law and Borders – The Rise of Law in Cyberspace“, Stanford Law Review 48 (1996) 1367 ff.

252 Dieser Ausdruck stammt aus dem Englischen und kann mit „weltweiter freier Informationsfluss“ übersetzt werden.

253 Schneider, Handbuch des EDV-Rechts, O 41 S. 1673.

254 Johnson/Post, Stanford Law Review 48 (1996) 1367, 1369 f.

255 So Jonson/Post in Stanford Law Review 48 (1996) 1367, 1390:
„Governments cannot ... credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations.“
Ähnlich äußert sich Burnstein in: „Conflicts on the Net: Choise of Law in Transnational Cyberspace“, Vand. J. Transnat. L. 29 (1996) 75, 93:
„In transnational cyberspace, however, the place of the wrong might be any of the 145-plus nations that are on-line. More accurately, there is no lex loci delicti. [...] If injury occurs in cyberspace, it can be said that the place of the wrong is cyberspace itself.“

256 Schack, „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet“, MMR 2000, 59 f.

Ziel ist eine Selbstkontrolle der Teilnehmer im Internet.[257] Der wichtigste Vertreter von Regeln zur Selbstkontrolle ist die sogenannte „Netiquette“[258].

Diese liberalen Ansichten werden aber von den Gesetzgebern vieler Staaten nicht geteilt. Vielmehr wollen sie die Regulierung des Cyberspace vorantreiben.[259] Daneben versuchen auch Strafverfolgungs- und Verwaltungsbehörden, Staatsanwälte sowie Privatkläger die Frage zu klären, inwieweit die geltenden (Rechts-)Grundsätze der Realität auf die virtuelle Welt des Internets übertragen werden können. Dabei geht es nicht nur um das Problem der Anwendbarkeit der bis dato geschaffenen Regeln, sondern auch um ihre Durchsetzbarkeit. Denn zwischen der Meinungsfreiheit, dem „Free Flow of Information“ und dem Wert weltweiter Kommunikation einerseits und den Problemen, die eine ungehinderte, ungefilterte sowie nicht moderierte Kommunikation auslösen kann, besteht ersichtlich Spannung:[260]

Zwar stellt schon allein die Tatsache, dass das Internet grenzüberschreitend genutzt wird, die staatlichen Kontrollmaßnahmen in Frage, da derartige Regelungen nur eingeschränkt anwendbar und äußerst schwer durchsetzbar sind. Indes darf nicht übersehen werden, dass täglich neue Missbrauchsfälle im Internet hinzutreten. Vor allem der Staat hat daher ein berechtigtes Interesse daran, die davon betroffenen Personen(gruppen), insbesondere die (jugendlichen) Nutzer, sowie sich selbst davor zu schützen. Dieser Schutz ist jedoch nur mit Hilfe staatlicher Normen möglich.

Des weiteren verkennt die Cyberspace-These, dass das gesamte Internet und somit der Cyberspace nichts anderes als Illusion ist. Deshalb sind die nationalen Rechtsordnungen nicht gezwungen, diese Illusion anzuerkennen, zumal keine Nation jemals zum Ausdruck gebracht hat, ihre Souveränität auf dem Gebiet des Cyberspace aufgeben zu wollen. Ganz im Gegenteil versucht jeder Staat zur Zeit, seine anfänglich verlorengegangene Souveränität auf dem Gebiet des Internets durch nationale Vorschriften zurückzugewinnen. Es gibt auch keinen ersichtlichen Grund, dass eine (fast) perfekte Technik sich über nationale bzw. internationale Rechtsnormen hinwegsetzen kann. Daneben ist fraglich, ob überhaupt eine so strikte Trennung zwischen realer und virtueller Welt möglich ist, wie es die Befürworter der Cyberspace-These behaupten. Denn nur dann könnte eine Legitimation für ein eigenständiges Cyberlaw angedacht werden.

---

257 Vgl. hierzu ausführlich bei von Hinden, Persönlichkeitsverletzungen im Internet, S. 252 ff.

258 Dieses Kunstwort setzt sich zusammen aus dem Wort „net“ (engl.: Netz) und dem englischen Begriff für Etikette (im Sinne von „Umgangsformen“).
Die Netiquette stellt die Summe der als Minimalkonsens von einer wesentlichen Anzahl von Teilnehmern akzeptierten Verhaltensregeln im Internet dar. In einzelnen Netzbereichen wird die Netiquette in Schriftform fixiert. Ausführlich hierzu auch Mayer, Das Internet im öffentlichen Recht, S. 87. Vgl. hierzu die kodifizierte Fassung der Netiquette im Internet unter http://www.albion.com/netiquette/corerules.html (zuletzt abgerufen am 08.04.2002).

259 Mayer, Das Internet im ö-Recht, S. 109.

260 Mayer, Das Internet im öffentlichen Recht, S. 110.

Das Internet stellt jedoch gerade keinen von der Realität abtrennbaren Raum dar. Dies lässt sich leicht mit einer Betrachtung on- und offline[261] belegen: Eine von der realen Welt losgelöste virtuelle Welt ist nur dann gegeben, wenn sich keiner der Vorgänge, die sich im Cyberspace (online) abspielen, auf die reale Welt (offline) auswirken.[262] Eben dies ist aber nicht der Fall. Denn nicht nur sämtliche wirtschaftliche Bereiche des Internets, sondern auch das übrige Internet mit seinen Diensten beeinflussen immer mehr unser tägliches Leben. Folglich wirken sich Handlungen im Cyberspace auch auf die reale Welt aus und demnach sind auch ihre Regeln anwendbar. Denn solange sich das soziale Leben offline abspielt, sind selbstverständlich seine Normen weiter aktuell.[263] Darüber hinaus sind auch bestimmte Inhalte des Internets – entgegen der Meinung der Cyberspace-These – in bestimmten Weltregionen stärker vertreten. Dies lässt sich schon allein mit den unterschiedlichen Sprachen und den einzelnen Kulturkreisen erklären.[264] Zudem müssen die Maßstäbe des Internets der realen Welt angepasst werden, da sonst ein unerklärbarer Widerspruch zwischen den vorgeschriebenen Verhaltensweisen im Cyberspace und der realen Welt entsteht, der vor allem Minderjährige verwirren könnte. Die Gefahr, dass erlaubte Handlungsweisen des Internets auf die Realität übertragen werden, in der sie untersagt sind, besteht in hohem Maße.[265] Schließlich hat auch die Wirtschaft ein großes Interesse daran, dass die üblichen Regeln der Wirtschaftswelt auch im virtuellen Raum Bestand haben, um einen zuverlässigen Wirtschaftsraum im Internet zu etablieren.

Aus diesen Gründen ist der Ansatz der These vom Cyberspace und der mit ihr zusammenhängende „Global Free Flow of Information" abzulehnen. Eine Selbstkontrolle der Internet-Teilnehmer kann daher nicht ausreichen, um dem komplexen Gebilde Internet eine Ordnung zu geben.[266] Vielmehr besteht nicht nur wegen der steigenden Anzahl an jugendlichen Internet-Nutzern ein staatlicher Auftrag, den Einzelnen und sich selbst vor rechtswidrigen bzw. strafbaren Inhalten im Netz zu schützen. Der Staat hat also jetzt

---

261 „Online" bedeutet, dass der Zugang zum Internet hergestellt ist. Dagegen wird mit „offline" der Zustand beschrieben, wenn der Rechner keine Verbindung zum Internet aufweist. Nur wenn der Server online ist, kann die virtuelle Welt des Internets durch den Nutzer betreten werden. Im offlinen Zustand bleibt man dagegen in der Realität.

262 von Hinden, Persönlichkeitsverletzungen im Internet, S. 246.

263 Kaufmann-Kohler in: Boele-Woelki/Kessedjian, Which Court Decides? Which Law Applies?, S. 89, 90, 112.

264 von Hinden, Persönlichkeitsverletzungen im Internet, S. 247 f.

265 Vgl. hierzu auch Lessig in: „The Zones of Cyberspace", Stanford Law Review 48 (1996) 1403, 1410:
„This next generation of cyberspace will provide individuals with the perfect technology of choice; it will empower individuals to select into the world what they want to see, to select out of the world what they don´t. But they who check out also live here; when not in cworld, they must participate in the making, and regulating, of the live that is here. And so the question: Just how will this life in cworld affect their abilitz to connect to this life in the real world?"

266 Mayer, „Recht und Cyberspace", S. 1790.

und künftig durch bestimmte nationale bzw. supranationale Normen dafür zu sorgen,[267] einen rechtlichen Rahmen für eine moderate Kontrolle des Internets zu herbeizuführen.[268] Somit ist nun zu prüfen, welche Normen hierfür in Betracht kommen:

II. Nationale Rechtsnormen

In diesem Abschnitt wird zunächst die einschlägige nationale Rechtsnormung vorgestellt und auf ihren Regelungszweck eingegangen. Im Anschluss daran werden die einzelnen Gesetze technisch und inhaltlich voneinander abgegrenzt sowie die daraus resultierenden Rechtsfolgen aufgezeigt.

1. Überblick

Zu den nationalen Vorschriften, die eine Regelung des Internets erreichen sollen, zählen neben dem Telekommunikationsgesetz (TKG)[269] und anderen Vorschriften aus dem Telekommunikationsrecht insbesondere die Regelungen des Informations- und Kommunikationsdienste-Gesetz (IuKDG)[270] und des Mediendienste-Staatsvertrags (MDStV)[271].[272]

In dieser Normentrias bildet das TKG als Rahmengesetz das rechtliche Fundament, da es grundsätzlich die rechtlichen Voraussetzungen für den technischen Austausch von Informationen regelt.[273] Darauf bauen das IuKDG und der MDStV auf. Das IuKDG stellt ein sogenanntes „Artikelgesetz" dar.[274] Dies bedeutet, dass es Erstregelungen mit Ergänzungen und Änderungen bereits bestehender bundesgesetzlicher Vorschriften in einem Mantelgesetz vereinigt. Der Mantel wird in diesem Fall vom sachlichen Gegenstand des Gesetzgebungsvorhabens „Multimedia"[275] gebildet.[276] Wichtig für die vorlie-

---

267 So auch Schack in: „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet", MMR 2000, 59, 60, der jedoch eine international möglichst konsensfähige Bestimmung des anwendbaren nationalen Rechts propagiert.

268 Schack, „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet", MMR 2000, 59, 60; so auch Schneider, Handbuch des EDV-Rechts, O 42 S. 1674:
„Durch die Verschmelzung von Rechtsordnungen und Wertordnungen entsteht aber kein rechtsfreier Raum, sondern vielmehr ein zu harmonisierender Rechtsraum."

269 BGBl. I S. 1120, BGBl. III/FNA 900-11.

270 BGBl. I S. 1870, BGBl. III/FNA 9020-6.

271 BayGVBl. 1997, 226.

272 Das TDG ist unlängst durch die Umsetzung der E-Commerce-Richtlinie geändert worden. Statt des vorher gültigen § 5 TDG werden die Haftungsprivilegien nun in den neuen §§ 8 ff. TDG zu finden sein. Zunächst wird in dieser Arbeit noch nicht die kommende, sondern die bisherige Gesetzeslage berücksichtigt. Allerdings soll durch einen Zusatz das neue Gesetz vorgestellt und auf die relevanten Änderungen eingegangen werden. Vgl. hierzu unten unter B. 2. Teil. II. 5. ff. Einen Überblick über die zukünftigen Änderungen stellt Säcker in: „Die Haftung von Diensteanbietern nach dem Entwurf des EGG", MMR-Beilage 9/2001, 2 ff. vor.

273 Geppert/Roßnagel, Telekommunikations- und Mediarecht, in der Einleitung S. XVII.

274 Ausführliche Darstellung des gesamten IuKDG bei Engel-Flechsig/Maennel/Tettenborn: „Das neue Informations- und Kommunikationsdienste-Gesetz", NJW 1997, 2981 ff.

275 Zu diesem Begriff und dessen vielfältige Verwendungsarten vgl. Lehmann, Internet- und Multimediarecht, S. 2; Hesse, „Zur aktuellen Entwicklung des Rundfunkrechts", BayVBl. 1997, 132 f.; Leh-

gende Arbeit ist das in Art. 1 des IuKDG enthaltene TDG. Alle übrigen Gesetze, die die Art. 2 bis 7 IuKDG beinhalten[277], spielen hier keine entscheidende Rolle[278] und werden nur dann angesprochen, wenn sie von Bedeutung sein sollten.

Der MDStV ist demgegenüber ein abgeschlossenes Vertragswerk, das in fünf Abschnitte unterteilt ist. Die Regelungen des MDStV entsprechen im wesentlichen Art. 1 und Art. 2 IuKDG.[279] Die ersten beiden Abschnitte, die den Sinn und Zweck des Staatsvertrags, dessen Geltungsbereich und die Zugangsfreiheit sowie besondere Rechte und Pflichten der Anbieter behandeln, enthalten hauptsächlich die im hier interessierenden Zusammenhang relevanten Bestimmungen.

Ziel des TKG, des TDG sowie des MDStV ist es, eine angemessene und abgestufte rechtliche Behandlung inhaltlicher Fragen bei den unterschiedlichsten elektronischen Medien zu gewährleisten.[280]

Zu ergänzen ist, dass diese Gesetze in ihrer jeweiligen Ausgestaltung die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zum ersten Rundfunkurteil teilweise mitberücksichtigt haben. Deshalb ist es für die Anwendung und Auslegung sowie für das Verständnis dieser Gesetze wichtig, zunächst die Grundsätze dieses Urteils nachzuvollziehen.

---

mann, Rechtsgeschäfte im Netz – Electronic Commerce, S. 8; Müller-Using/Lücke, „Neues Recht für Multimedia-Dienste“, ArchivPT 1997, 101; Engel-Flechsig/Maennel/Tettenborn: „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981; hierzu Schneider, Handbuch des EDV-Rechts, O 12:

„Multi-Media meint insoweit das Zusammenführen bisher technisch getrennter Modalitäten in eine Kombination von Ausdrucksformen, möglicherweise aber repräsentiert nur auf einem einheitlichen Datenträger (z.B. auf einer CD-ROM bzw. dem Download einer „Sendung“ über Netz). Diese Integration wird u. a. über die Digitalisierung ermöglicht, die zugleich dadurch für das nächste Phänomen i.V.m. den Netzen sorgt, nämlich die Ubiquität dieser Modalitäten, also weitgehende Unabhängigkeit von Zeit und Raum.“

276 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 233.

277 Mit den Art. 1, 2 und 3 führt das Gesetz erstmalige Regelungen auf, die für die weitere Entwicklung von Informations- und Kommunikationsdiensten von wesentlicher Bedeutung sind. Neben dem schon oben genannten TDG, das in Art. 1 IuKDG geregelt ist, beinhaltet Art. 2 des IuKDG das TDDSG (Teledienstedatenschutzgesetz) und Art. 3 IuKDG das Signaturgesetz.

Die weiteren Artikeln nehmen Ergänzungen und Änderungen bereits bestehender Bundesgesetze vor, die den veränderten tatsächlichen Bedingungen im Straf- und Ordnungswidrigkeitenrecht sowie im Jugendschutz Rechnung tragen. Art. 7 IuKDG setzt schließlich die EG-Datenbankrichtlinie (RL 96/9/EG des Europäischen Parlaments und des Rates vom 11.03.1996 über den rechtlichen Schutz von Datenbanken; ABl. EG Nr. L 77 S. 20) um.

278 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 353.

279 Lehmann, Rechtsgeschäfte im Netz – Electronic Commerce, S. 13.

280 Hesse, „Zur aktuellen Entwicklung des Rundfunkrechts“, BayVBl. 1997, 132, 136; Schrader, „Datenschutz bei Multimediadiensten“, CR 1997, 707, 708.

Exkurs: Das Rundfunkurteil des BVerfG

Im „Ersten Rundfunkurteil“ aus dem Jahre 1961 hatte das BVerfG über das Verhältnis von Telekommunikation und Rundfunk zu entscheiden.[281] Gestritten wurde vor allem, wer für die Regelung des Rundfunks die Gesetzgebungskompetenz besitzt, der Bund oder die Länder.

Unter Hinweis auf die historische, technische und rechtliche Entwicklung des Rundfunks in Deutschland vertrat das BVerfG die Ansicht, die technischen und inhaltlichen Bereiche zu trennen.

Grund für diese strikte Trennung durch das BVerfG war die unterschiedlich vorgegebene Kompetenzverteilung im Grundgesetz (GG). Denn grundsätzlich wird den Ländern die Kompetenz für den Rundfunk gemäß Art. 30 und 70 GG zugeordnet und dem Bund die ausschließliche Zuständigkeit für die Telekommunikation nach Art. 73 Nr. 7 GG sowie die Rahmengesetzgebungskompetenz für Presse und Film gemäß Art. 75 Nr. 2 GG.[282]

Im weiteren Verlauf seiner Entscheidung stellt das BVerfG hierzu Abgrenzungskriterien auf. So soll unter den Begriff Telekommunikation die technische Seite der Verbreitung von Rundfunk gefasst werden, während der Rundfunk seinerseits alle Vorgänge einschließen soll, die mit dem Zustandekommen und der inhaltlichen Ausgestaltung der zu übertragenden Daten zu tun haben. Nach dem BVerfG ist folglich der Telekommunikation die Übertragungstechnik zuzurechnen, unabhängig davon, ob sie terrestrisch, über Breitbandkabel oder Satellit realisiert wird. Zum Rundfunk gehören dagegen die inhaltliche Ausgestaltung des Rundfunks, beispielsweise die Organisation von Rundfunkanstalten sowie die Konzeption und Umsetzung von Programminhalten.[283]

Gerade die unterschiedliche Kompetenzverteilung, die das GG für den Rundfunk enthält, hatte zur Folge, dass auch bei der Gesetzgebung der neueren Mediengesetze, die eine Regelung des Phänomens „Multimedia“[284] zum Ziel haben, heftiger Streit zwischen Bund und Ländern bezüglich der Gesetzgebungskompetenz entbrannt ist.[285] Womöglich hätte hier am Ende wiederum das BVerfG eingreifen müssen, wenn sich Bund und Länder nicht doch noch auf einen gesetzgeberischen Kompromiss geeinigt hätten.[286] Folge dieser Einigung war das Inkrafttreten der drei neuen Gesetzeswerke TKG, MDStV und IuKDG.

Insgesamt sind in der Praxis somit vier multimediale Bereiche zu unterscheiden, die jeweils durch eigene Gesetze bzw. Staatsverträge geregelt werden: So gibt es weiterhin den Bereich der Massenkommunikation mit den klassischen Rundfunkangeboten. Er ist – wie bislang – im Rundfunkstaatsvertrag (RStV) der Länder normiert. Daneben besteht der Bereich der rein technisch zu verstehenden Telekommunikation, der im TKG des Bundes seine Niederschrift gefunden hat. Darüber hinaus existiert die inhaltliche Sparte

---

281 Vgl. hierzu BVerfGE 12, 205 ff.

282 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675.

283 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 78.

284 Vgl. hierzu Fn. 275.

285 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231, 237.

286 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 676.

der Individualkommunikation und der publizistisch nicht relevanten Datendienste. Sie wird durch das TDG des Bundes geregelt. Unter den letzten Bereich fallen die Mediendienste, die im Mediendienste-Staatsvertrag der Länder behandelt werden, der in zentralen Punkten wortgleich mit den bundesrechtlichen Vorschriften des TDG alte Fassung (a.F.)[287] ist.

Bei genauerer Betrachtung der Normen der drei neueren Gesetze TKG, TDG und MDStV fällt auf, dass sie ihren Regelungsgegenstand bzw. den von ihnen geregelten technisch-funktionalen Lebenssachverhalt als Unterfall eines übergeordneten Begriffs des „Dienstes" bezeichnen. Dieser Begriff darf jedoch nicht mit dem oben angesprochenen Begriff des „Internet-Dienstes" verwechselt werden. Vielmehr muss er als normativer und nicht als technischer Begriff verstanden werden.[288]

Das TKG behandelt – wie sich aus seinem Wortlaut ergibt – die Telekommunikationsdienste. Was hierunter zu verstehen ist, enthält § 3 Nr. 5 TKG, der von einem „*nachhaltigem Angebot von Telekommunikation*" spricht. Diese Aussage muss im Zusammenhang mit § 3 Nr. 16 TKG gelesen werden, wonach Telekommunikation der „*technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen*" ist. Aus den §§ 1 TDG und MDStV ergibt sich, dass diese Telekommunikationsdienste von den Informations- und Kommunikationsdiensten abzugrenzen sind, die vom Gesetz gemäß § 2 I TDG bzw. MDStV weiter in Teledienste und Mediendienste aufgespalten werden. Die Differenzierung dieser unterschiedlichen Multimedia-Dienste und somit ihrer Gesetze wird aus technischer und inhaltlicher Sicht vorgenommen:

2. Technische Abgrenzung der Anwendungsbereiche von TKG, TDG und MDStV

Wie eben schon angedeutet worden ist, hat der Gesetzgeber die Absicht gehabt, die Inhalte durch das TDK bzw. den MDStV und die Technik durch das TKG zu regeln.[289] Deshalb erscheint es sinnvoll, zunächst das Verhältnis von TKG zu TDG sowie MDStV zu klären, bevor auf die Unterschiede zwischen dem TDG und dem MDStV eingegangen wird.[290]

---

[287] Da in der vorliegenden Arbeit auf die neue und alte Fassung des TDG eingegangen wird, müssen Gesetzesbezeichnungen, die sich nur auf eine der beiden Fassung beziehen mit a.F. (alte Fassung) oder n.F. (neue Fassung) gekennzeichnet werden. Bei Aussagen, die für beide Regelwerke gleichermaßen Gültigkeit besitzen, wird dagegen ganz allgemein die Gesetzesbezeichnung TDG verwendet.

[288] Vgl. hierzu auch Hochstein, „Teledienste, Mediendienste und Rundfunkbegriff – Anmerkungen zur praktischen Abgrenzung multimedialer Erscheinungsformen", NJW 1997, 2977, 2978 ff.

[289] Müller-Using/Lücke, „Neues Recht für Multimedia-Dienste", ArchivPT 1997, 101, 106.

[290] Da die Regelungen im MDStV im wesentlichen denen des TDG a.F. entsprechen, gelten – soweit nicht etwas anderes angegeben ist – folgende Ausführungen zum TDG auch für den MDStV.

a. Verhältnis von TKG zu TDG und MDStV

Das TDG des Bundes findet gemäß § 2 IV Nr. 1 TDG keine Anwendung auf „*Telekommunikationsdiensleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes*“. Weiter bestimmt § 3 Nr. 18 TKG, dass Telekommunikationsdienstleistungen „*das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte*“ sind. Schließlich stellt § 3 Nr. 16 TKG in seiner Legaldefinition fest, dass Telekommunikation „*der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen*“ ist. Durch diese weiten Begriffsbestimmungen des TKG kann die Ausschlussregel des § 2 IV Nr. 1 TDG missverständlich wirken, weil die Teledienstedefinition des § 2 I TDG die „*Übermittlung mittels Telekommunikation*“ zum wesentlichen Bestandteil eines Teledienstes macht. Dies hätte bei einer allzu wortgetreuen Anwendung der beiden Gesetze TDG und TKG zur Folge, dass das TDG nur einen sehr engen Anwendungsbereich aufweist. Denn die Anwendbarkeit des TDG könnte mit dem Hinweis auf die stets vorhandenen telekommunikativen Grundlagen eines Teledienstes sehr oft verneint werden.

Der Gesetzgeber wollte jedoch eine möglichst eindeutige Abgrenzung der Anwendungsbereiche dieser Gesetze. Dies geht vor allem aus der Entstehungsgeschichte des § 2 IV TDG hervor. So war im Referentenentwurf zum IuKDG vom 28.06.1996 die Abgrenzung des TDG zum TKG in § 3 III TDG am deutlichsten formuliert. Danach sollte das TDG nicht „für die den Telediensten zugrundeliegende Telekommunikation“ i.S.d. TKG gelten.[291] Dies zeigt, dass der Gesetzgeber die Intention hatte, gerade in diesem Bereich klarzustellen, wie die Abgrenzung zwischen dem TDG und dem TKG zu erfolgen hat, nämlich durch eine Trennung der technischen Übertragungsplattform (Telekommunikation) vom Übertragungsinhalt (Teledienst).[292] Deswegen gibt es die unterschiedlichen Regelungen. Eine klare Abgrenzung zwischen dem TKG und dem TDG muss deshalb – gemäß den Gedanken, die schon das BVerfG in seinem ersten Rundfunkurteil entwickelt hat[293] – über die Einteilung in einen technischen und inhaltlichen Bereich erfolgen.[294] Da der Gesetzgeber aber explizit in § 2 IV Nr. 1 TDG darauf hinweist, dass der technische Bereich des TKG nicht unter das TDG fällt, wird auch aufge-

---

[291] Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 109; Der Entwurf vom 07.06.1996 sprach in § 3 III davon, das TDG gelte nicht „für die Telekommunikationsdienstleistungen“ i.S.d. TKG. Der Entwurf vom 14.05.1996 enthielt dagegen den ungenauen Begriff „Transportdienstleistungen“.

[292] Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 438.

[293] Siehe oben unter B. 2. Teil. II. 1. Exkurs.

[294] So auch Wuermeling/Felixberger, „Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz“, CR 1997, 230, 233 f.

zeigt, dass eine Unterscheidung zwischen Technik und Inhalt zeitweise Schwierigkeiten bereiten kann.[295]

b. Verhältnis von TDG zum MDStV

Der technische Unterschied dieser Gesetze ist jeweils in § 2 I TDG bzw. MDStV zu finden. So gilt gemäß § 2 I TDG das TDG „*für alle elektronischen Informations- und Kommunikationsdienste [...], denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste)*". In § 2 I MDStV heißt es dagegen, dass der MDStV „*für das Angebot und die Nutzung von [...] Informations- und Kommunikationsdiensten (Mediendiensten) [...], die ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden*", gelten soll. Diese zur Verbreitung der von dem TDG und MDStV geregelten telekommunikativen Inhalte beschriebene unterschiedliche Technik ist als Differenzierungskriterium nicht geeignet.[296] Denn gemäß § 3 Nr. 16 und 17 TKG ist es irrelevant, welche Technik eingesetzt wird, weil der technische Bereich – wie eben geklärt – vom TKG erfasst wird. Auf die verschiedenartige Technik darf bei der Frage bezüglich des Verhältnisses vom TDG zum MDStV deshalb nicht abgestellt werden. Vielmehr muss eine inhaltliche Abgrenzung durchgeführt werden, um die Unterschiede dieser beiden Gesetze herausarbeiten zu können.

3. Inhaltliche Abgrenzung der Anwendungsbereiche von TKG, TDG und MDStV

a. TKG zu TDG und MDStV

Weil das TKG ausschließlich die technische Seite der Informations- und Kommunikationsdienste regelt, kommt eine inhaltliche Abgrenzung dieses Gesetzes zum TDG und MDStV nicht in Betracht.

b. TDG zu MDStV

Um so mehr ist die Frage nach den inhaltlichen Unterschieden im Hinblick auf das Verhältnis von TDG zu MDStV von Bedeutung:
Das TDG regelt, wie sich aus der Legaldefinition des § 2 I TDG ergibt, alle „Teledienste". Demgegenüber befasst sich der MDStV gemäß § 2 I MDStV mit den „Mediendiensten". Die inhaltliche Einordnung eines Informations- bzw. Kommunikationsdienstes als Teledienst i.S.d. TDG oder Mediendienst i.S.d. MDStV kann zum einen durch Rückgriff auf die abstrakte Grunddefinition von Telediensten in § 2 I TDG bzw. von

---

295 Eine Abgrenzung zwischen dem TDG und dem TKG wird im übrigen für die Zukunft aufgrund der fortschreitenden Konvergenz zwischen Telekommunikation, Neuen Diensten und Rundfunk immer schwieriger. Hierzu vgl. das Grünbuch zur Konvergenz der Kommunikationsbranchen der Europäischen Kommission vom 01.12.1997, KOM (97) 623.

296 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 123.

Mediendiensten in § 2 I MDtV erfolgen.[297] Darüber hinaus kann eine Subsumtion unter eines der Regelbeispiele für die einzelnen Dienste in § 2 II TDG sowie § 2 II MDStV versucht werden.

§ 2 I TDG besagt, dass Teledienste i.S.d. Gesetzes alle solchen Informations- und Kommunikationsdienste sind, „*die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind, und denen eine Übermittlung mittels Telekommunikation zugrunde liegt*". Demgegenüber soll gemäß § 2 I MDStV der MDStV „*für das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (Mediendiensten) in Text, Ton und Bild, die unter Benutzung elektromagnetischer Schwingungen [...] verbreitet werden*" gelten.

Abgesehen von der Erwähnung einer unterschiedlichen Technik der Datenübertragung in den Gesetzestexten von § 2 I TDG bzw. MDStV soll die inhaltliche Unterscheidung von Informations- und Kommunikationsdiensten in solche, die dem TDG und jene, die dem Staatsvertrag unterfallen, anhand von zwei gegenläufigen Merkmalen erfolgen.[298] So macht § 2 I TDG deutlich, dass von ihm alle auf Telekommunikationsbasis betriebenen Informations- und Kommunikationsdienste erfasst werden, die für eine „*individuelle Nutzung*" bestimmt sind. Im Gegensatz dazu sind diejenigen Informations- und Kommunikationsdienste, die sich „*an die Allgemeinheit*" richten, Regelungsgegenstand des MDStV.[299] Der Gesetzgeber gibt somit durch die beiden Regelungswerke TDG und MDStV zwei Perspektiven vor: Die Perspektive des TDG zielt auf die Frage der individuellen Nutzung.[300] Hintergrund hierfür ist der Umstand, dass mit dem TDG kompetenziell der Bereich der individualkommunikationsnahen Telekommunikation i.S.d. Art. 73 Nr. 7 GG betroffen ist.[301] Dagegen ist die Perspektive des Staatsvertrags dahingehend ausgerichtet, inwieweit die Allgemeinheit angesprochen wird.[302] Dahinter steht die grundsätzliche Gesetzgebungskompetenz der Länder bezüglich des Medienrechts. Werden beide Perspektiven gemeinsam betrachtet, so lebt die Unterscheidung in Individual- und Massenkommunikation auf.[303]

---

297 Pichler, „Haftung des Host Providers für Persönlichkeitsverletzungen vor und nach dem TDG", MMR 1998, 79, 80.

298 Kröger/Moos, „Mediendienst oder Teledienst?", AfP 1997, 675, 676.

299 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks", CR 1998, 351, 353.

300 Schrader, „Datenschutz bei Multimediadiensten", CR 1997, 707, 708.

301 Bullinger/Mestmäcker, Multimediadienste – Aufgaben und Zuständigkeit von Bund und Ländern, S. 156.

302 Holznagel/Kussel, Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet", MMR 2001, 347, 348.

303 Als Grundlage für diese Aufteilung der Zuständigkeiten in Individualkommunikation (Bund) und Massenkommunikation (Länder) nennen Kröger und Moos in „Mediendienst oder Teledienst?", AfP 1997, 675, 676 das Ergebnis des Gutachtens von Bullinger/Mestmäcker, Multimediadienste – Aufgaben und Zuständigkeit von Bund und Ländern, wonach der Bund wegen Art. 73 Nr. 7 GG der Telekommunikationskompetenz, nicht nur die Regelung des Transports, sondern auch des Inhalts der Individualkommunikation besitze. Den Ländern verbleibe danach lediglich der Bereich der Massenkommunikation zur inhaltlichen Regelung.

Insgesamt lässt sich deshalb feststellen, dass eine Unterscheidung zwischen Teledienst und Mediendienst – abgesehen von den Regelbeispielen in § 2 II TDG bzw. MDStV – danach zu erfolgen hat, ob die jeweiligen Informations- und Kommunikationsdienste an die Allgemeinheit gerichtet oder für eine individuelle Benutzung bestimmt sind.[304] Zudem besagt § 2 IV Nr. 3 TDG ausdrücklich, dass das TDG nicht für „*inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienste-Staatsvertrag*“ gilt. Umgekehrt sollen nach § 2 I 3 MDStV die Bestimmungen des TDG unberührt bleiben.[305] Die gesetzliche Konzeption geht also von einer eindeutigen Zuordnung der jeweiligen Informations- und Telekommunikationsdienste ohne Überschneidung der Anwendungsbereiche aus.[306] So wird durch § 2 IV Nr. 4 TDG zugleich auch der Anwendungsbereich des MDStV umschrieben. Dies ergibt sich aus dem Wort „*soweit*“ in dieser Norm. Hierdurch wird klargestellt, dass der in § 2 TDG festgelegte Anwendungsbereich maßgeblich für die Bestimmung dessen ist, was unter Mediendiensten i.S.d. MDStV zu verstehen ist. Dies entspricht im übrigen der verfassungsrechtlichen Regel des Art. 31 GG, wonach das Bundesrecht das Landesrecht bricht.[307] Dies hat zur Folge, dass es theoretisch keine Überschneidungsbereiche zwischen den Anwendungsgebieten der beiden Regelungswerke TDG und MDStV gibt.[308]
In der Praxis gelingt allerdings die Abgrenzung zwischen Teledienst und Mediendienst äußerst schwer.[309] Häufig werden deshalb in der Literatur Prüfungsreihenfolgen vorgeschlagen.[310] Diese orientieren sich vor allem am Gesetz. Welche Angebote als Teledienste oder Mediendienste einzuordnen sind, muss demnach zweistufig mittels der abstrakten Beschreibung des Anwendungsbereichs in § 2 I TDG bzw. MDStV und der Liste der Regelbeispiele in § 2 II TDG sowie MDStV bestimmt werden.[311]

---

304 Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3146.

305 Diese Bestimmung ist wegen der Regelung in § 2 IV Nr. 3 TDG auch nicht nach § 23 II MDStV gegenstandslos.

306 Engel-Flechsig/Maennel/Tettenborn: „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984; Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, MMR 1998, 79, 80; a.A. noch Kröger/Moos, „Regelungsansätze für Multimediadienste“, ZUM 1997, 462, 467 ff., die allerdings den erst in der beschlossenen Gesetzesfassung hinzugekommenen § 2 IV Nr. 3 TDG noch nicht berücksichtigt hatten und deshalb zu einer parallelen Anwendbarkeit kommen, die durch die genannte Vorschrift aber gerade ausgeschlossen werden soll.

307 Siehe hierzu auch Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 126.

308 Engel-Flechsig/Maennel/Tettenborn: „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984.

309 Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, MMR 1998, 79, 80; Holznagel/Kussel, Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 348; Strömer, Online§Recht, 2. Auflage, S. 13.

310 So etwa Lehmann, Rechtsgeschäfte im Netz - Electronic Commerce, S. 15.

311 Engel-Flechsig/Maennel/Tettenborn in „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2983 f. schlagen darüber hinaus vor, für die Abgrenzung der Regelungs-

4. Rechtliche Einordnung des Datenverkehrs im Internet anhand des TKG, TDG und MDStV

Nach Darstellung der einschlägigen gesetzlichen Bestimmungen und ihren Abgrenzungen voneinander, soll nun aufgezeigt werden, wie der Datenverkehr im Internet in diese Regelwerke eingeordnet werden kann. Für die vorliegende Arbeit ist insbesondere die Einordnung des Internets in diese verschiedenen „Multimedia-Gesetze" von Bedeutung, weil dadurch – falls vorhanden – die Rechtsgrundlage für einen staatlichen Eingriff in das Internet bestimmt werden kann.

a. Allgemeines

Zur Einordnung des Datenaustausches im Internet empfiehlt es sich, auf die bereits beschriebenen technischen und funktionalen Aspekte des Internets zurückzugreifen. Sie sind die wesentlichen Merkmale des Internets. Folglich kann am besten durch die Anknüpfung an die typischen Eigenschaften, die Dienste und beteiligten Personen eine Zuordnung zu den einzelnen Telekommunikations- und Mediengesetzen gelingen.[312]
Obwohl das Internet in § 2 II Nr. 3 TDG ausdrücklich genannt wird, wäre es falsch, das gesamte Internet unter das TDG zu subsumieren. Denn § 2 II Nr. 3 TDG spricht lediglich in seinem Anwendungsgebiet von „*Angebote zur Nutzung des Internets oder weiterer Netze*". Das Internet als Ganzes kann, dafür ist es zu vielschichtig und komplex, nicht unter den Anwendungsbereich eines der genannten Gesetze gefasst werden.[313] Die Besonderheit des Internets ist gerade die Tatsache, dass die unterschiedlichen Bereiche der technischen Telekommunikation und der meinungsbildenden Mediendienste von ihm zusammengeführt werden.[314] Folglich muss jeder relevante Teilbereiche des Internets gesondert betrachtet und hierzu das jeweils einschlägige Gesetz ermittelt werden.[315] Dabei kann auch hier – gemäß dem Rundfunkurteil des BVerfG – die technische und inhaltliche Seite des Internets (soweit dies möglich ist) getrennt voneinander betrachtet werden. Außerdem ist es wichtig, zwischen den Internet-Diensten und den Diensten der Provider zu unterscheiden.[316]

---

bereiche des TDG sowie des MDStV ergänzend die allgemeinen Grundsätze des Presserechts heranzuziehen.

312 Mayer, Das Internet im Öffentlichen Recht, S. 134.

313 Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG", MMR 1998, 79, 80.

314 Steckler, Grundzüge des EDV-Rechts, S. 8.

315 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer", ZUM 1997, 238; Engel-Flechsig/Maennel/Tettenborn in „Das neue Informations- und Kommunikationsdienste-Gesetz", NJW 1997, 2981, 2982; Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG", MMR 1998, 79, 80. Anders dagegen Waldenberger in „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter", MMR 1998, 124, 125, der für die Einordnung der Dienste im Internet als Tele- oder Mediendienste das Gesamtspektrum der Angebote eines Dienstleisters berücksichtigen will. Er spricht in seinem Aufsatz deshalb von der „Einheit" des Dienstes als Abgrenzungskriterium.

316 Kröger/Moos, „Mediendienst oder Teledienst?", AfP 1997, 679.

b. Das physikalische Netz des Internets

Die in § 3 Nr. 16 und 17 TKG definierten Begriffe der Telekommunikation und der Telekommunikationsanlagen, auf die bereits oben eingegangen wurde, machen deutlich, dass die technischen Anlagen, die zum Datenaustausch über das Internet benutzt werden, Telekommunikationsanlagen sein müssen, damit das TKG auf sie angewendet werden kann. Zumindest die physikalischen Bestandteile des Internets als System zur digitalen Datenübertragung fallen unter den Begriff der Telekommunikationsanlage des § 3 Nr. 17 TKG.[317] Zu nennen sind hierbei vor allem die Netzwerkverbindungen der Internet-Backbones, die Router und Gateways sowie die Einwahlknoten der Provider. Deshalb werden diese Übertragungswege und -kapazitäten des Internets vom TKG geregelt.[318]

c. Die Zuordnung der Dienste im Internet

Zwar sind die Dienste im Internet begrifflich nicht mit den Tele- und Mediendiensten des TDG und des MDStV identisch.[319] Jedoch stellen sie alle Informations- und Kommunikationsdienste dar,[320] so dass sie entweder in den Anwendungsbereich des TDG oder des MDStV fallen. Dabei gilt auch hier, dass die Abgrenzung zwischen dem TDG und dem MDStV häufig recht schwierig und manchmal eine klare Unterscheidung dieser beiden Regelungswerke nicht möglich ist.[321] Deshalb müssen zunächst grundsätzliche Überlegungen zur Abgrenzung des TDG und des MDStV bezüglich der Dienste im Internet angestellt werden, um anschließend auf die jeweiligen Dienste konkret eingehen zu können.

aa. Überlegungen zur Abgrenzung

Es wurde bereits öfter auf die Abgrenzungskriterien des TDG, das gemäß § 2 I TDG auf eine „*individuelle Nutzung*“ abstellt, und des MDStV hingewiesen, der in § 2 I MDStV *von „an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste*" spricht.

Beim Internet ergibt sich nun die Schwierigkeit, dass diese gesetzlich vorgegebenen Maßstäbe nur bedingt geeignet sind, um seine Informations- und Kommunikationsdienste dem jeweiligen Gesetz zuzuordnen. Denn alle, für jeden Nutzer abrufbar in das Internet gestellten Angebote, sei es in Text, Bild oder Ton, sind an die Allgemeinheit

---

317 Wuermeling/Felixberger, „Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz“, CR 1997, 230, 233.

318 In § 3 Nr. 18 TKG, der die Telekommunikationsdienstleistung definiert, wird darüber hinaus das Anbieten dieser Übertragungswege ausdrücklich genannt. Demnach fällt grundsätzlich auch der Network-Provider hierunter. Vgl. insoweit unten unter B. 2. Teil. II. 4. c. cc. (1).

319 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 76.

320 Dies gilt nicht für den Network-Provider, der die Technik für das Internet dem Nutzer anbietet, vgl. unten bei B. 2. Teil. II. 4. c. cc. (1).

321 Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, MMR 1998, 79, 80.

gerichtet, da sie eine nicht begrenzte Empfängerschaft erreichen sollen und damit veröffentlicht sind. Zugleich sind sie jedoch, wie letztendlich auch die klassischen Massenmedien Zeitung und Rundfunk, für die Konsumenten bestimmt, die über die Art ihrer Nutzung selbst entscheiden, also für die individuelle Nutzung.[322] Das Internet nimmt somit eine Sonderstellung bei den Medien ein, da es sowohl an die Allgemeinheit[323] gerichtet als auch individuell abrufbar ist. Folglich können die einzelnen Dienste je nach Betrachtungsweise eher dem TDG oder dem MDStV zugeordnet werden.
Um diesem Dilemma zu entgehen, müssen sämtliche Dienste aus dem gleichen Blickwinkel untersucht werden. Allerdings ist – gerade im Hinblick auf die folgenden Ausführungen – zu bemerken, dass dies nicht immer gelingt und deshalb Abgrenzungsschwierigkeiten unumgänglich sind.

bb. Die Internet-Dienste

Zu den bereits oben angesprochenen Internet-Diensten[324] gehören vor allem die Kommunikationsdienste (E-Mail, Newsgroups, Internet Relay Chat), der Datei- und Programmtransfer (FTP), die Bedienung entfernter Rechnersysteme (Telnet) und das World-Wide-Web (WWW).

(1) Kommunikationsdienste

Wie sich aus dem Wortlaut des TDG und des MDStV ergibt, wird der Oberbegriff „Kommunikationsdienste“ vom MDStV als Mediendienste und vom TDG als Teledienste erfasst. Im Gegensatz zum MDStV, der in seinen Regelbeispielen gemäß § 2 II MDStV nicht mehr explizit auf Kommunikationsdienste eingeht, spricht das TDG im § 2 II Nr. 1 TDG von „*Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch)*“. Deswegen kann hierunter zumindest auch die private E-Mail subsumiert werden. Denn sie stellt einen reinen Austausch an Daten im Rahmen der Individualkommunikation dar.[325]
Zwar könnten aus diesem Grund geschlossene Mailinglisten[326] und der Internet Relay Chat ebenfalls als „Individualkommunikation“ i.S.d. TDG angesehen werden. Aller-

---

322 Heyl, „Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag“, ZUM 1998, 115, 117.

323 Mit Allgemeinheit sind hier die Personen gemeint, die einen Internetzugang besitzen bzw. die die Möglichkeit haben, sich Zugang zum Internet zu verschaffen.

324 Vgl. hierzu unter B. 1. Teil. I. 3.

325 Diese Schlussfolgerung wird auch durch das sächsische Privatrundfunkgesetz (SächsPRG), vgl. SächsGVBl. Nr. 1 vom 31.01.1996, untermauert, das in seinem Anwendungsbereich gemäß § 1a III Nr. 1 SächsPRG die elektronische Post explizit ausnimmt.

326 Eine Kombination aus dem E-mail-Dienst und dem News-Dienst sind die Mailinglisten (englisch: „Mailing Lists“). Dabei handelt es sich ähnlich wie bei den Newsgroups um Diskussionsforen zu bestimmten Themen. Der Teilnehmer abonniert in diesem Fall bei einem List-Server eine oder mehrere der dort vorhandenen Mailinglisten. Dabei ist zwischen offenen und geschlossenen Mailinglisten zu unterscheiden. Bei ersteren erfolgt das Abonnement automatisiert und unterliegt keinen weiteren Beschränkungen. Neue Beiträge werden in diesem Fall ohne weiteres an die persönliche E-mail-Adresse zugestellt. In der Regel werden dann auch die selbstverfassten Beiträge des Teilnehmers au-

dings würde dies dem § 3 I 2 Btx-Staatsvertrag von 1981 widersprechen, der gemäß § 23 III MDStV durch den MDStV abgelöst wurde.[327] Denn nach § 3 I 2 Btx-Staatsvertrag wurden „*geschlossenen Teilnehmergruppen*“ durch die Länder geregelt, so dass diese Dienste jetzt nicht auf einmal durch das Bundesgesetz TDG erfasst werden dürfen.[328] Folglich müssen die Mailinglisten und der Internet Relay Chat unter den MDStV gefasst werden. Dies macht § 2 II Nr. 2 TDG ebenfalls deutlich, der bestimmt, dass unter diese Norm ebenfalls Angebote zur Kommunikation fallen, „*soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht*“.
Mit Hilfe der negativen Abgrenzung des § 2 II Nr. 2 TDG werden deshalb auch die öffentlichen Kommunikationsangebote sowie der Allgemeinheit zugänglichen Newsgroups und offene Mailinglisten vom MDStV erfasst.[329]

(2) Datei- sowie Programmtransfer und Bedienung entfernter Rechnersysteme

Wie bereits weiter oben erläutert wurde, funktionieren alle Internet-Dienste nach dem Client-Server-Prinzip.[330] Nach diesem Prinzip übermittelt der Server Informationen an den jeweiligen Nutzer. In § 2 II Nr. 4 MDStV heißt es, dass insbesondere „*Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden*“, als Mediendienste anzusehen sind.
Alle beiden Dienste – Telnet und FTP – zeichnen sich dadurch aus, dass jeder Nutzer auf deren Host-Computer zugreifen kann. Darüber hinaus besteht beim FTP die Möglichkeit des Downloads. Wird der Begriff „*Abrufdienst*“ in § 2 II Nr. 4 MDStV weit ausgelegt, so dass sämtliche Dienste, auf die zugegriffen werden kann, hierunter subsumiert werden können, wären diese Dienste als Mediendienste i.S.d. MDStV zu qualifizieren. Zumal auch das Merkmal des § 2 I MDStV erfüllt ist, da die Dienste an die Allgemeinheit gerichtet sind. Sie sind frei zugänglich und stehen somit einer breiten Öffentlichkeit zur Verfügung.[331] Diese Dienste könnten jedoch genauso gut von der Ausnahmeklausel des § 2 II Nr. 4 MDStV erfasst werden, nach der Abrufdienste, bei denen „*die reine Übermittlung von Daten im Vordergrund steht*“, nicht in den Anwendungsbereich des MDStV fallen sollen. Zumindest für den FTP-Dienst muss dies bejaht werden,

---

tomatisch an die anderen Mitglieder versandt. Dagegen entscheidet bei geschlossenen Mailinglisten ausschließlich der Betreiber, ob er dem Aufnahmeantrag stattgibt oder den Interessenten ablehnt. Ebenso wie bei den Newsgroups gibt es auch hier moderierte und unmoderierte Listen. Bei moderierten Mailinglisten entscheidet der Moderator, ob ein Beitrag an die anderen Abonnenten weitergeleitet wird. Vgl. Sieber, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen“, JZ 1996, 429, 433.

327 Hochstein, „Teledienste, Mediendienste und Rundfunkbegriff - Anmerkungen zur praktischen Abgrenzung multimedialer Erscheinungsformen“, NJW 1997, 2977, 2978.

328 Ory, “http://www.medienpolizei.de?“, AfP 1996, 105, 107.

329 In der Begründung zum Vorentwurf zu Art. 1 § 2 II Nr. 1 IuKDG vom 28.06.1996, Bundesrat-Drucksache 966/96 S. 20 wird in diesem Zusammenhang von „Meinungsforen“ gesprochen.

330 Vgl. oben unter B. 1. Teil. I. 2. b. aa.

331 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675, 679.

weil hier hauptsächlich die Übermittlung von Daten bezweckt wird. Dieser Dienst erfüllt grundsätzlich ebenfalls das Regelbeispiel in § 2 II Nr. 2 TDG, sofern nicht dessen pressebezogene Ausnahmen greifen.[332]
Dadurch, dass diese Dienste zum einen der Ausnahmeklausel des § 2 II Nr. 4 MDStV unterliegen und zudem unter § 2 II Nr. 2 TDG subsumiert werden können, ist es sinnvoll, sie als Teledienste einzuordnen. Etwas anderes gilt allerdings dann, wenn entweder gemäß § 2 II Nr. 2 TDG „*die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht*“ oder § 2 V TDG einschlägig ist, wonach presserechtliche Vorschriften unberührt bleiben.

(3) World-Wide-Web (WWW)

Auch das WWW funktioniert wiederum nach dem Client-Server-Prinzip. In diesem Fall ist der Client der „Web-Browser“[333], also die Software, mit der im Netz navigiert werden kann. Die Server sind dagegen alle Rechner, auf denen Daten bereitliegen, die mit dem Browser aufgerufen werden können. Hierunter fallen sämtliche Homepages. Wie schon oben ausführlich dargestellt, sind die Hyperlinks, die die einzeln gespeicherten Dokumente verknüpfen, das Besondere am WWW.[334] Homepages enthalten typischerweise Text- , Ton- und Bilddateien, die auf Anforderung aus dem elektronischen Speicher zur Nutzung übermittelt werden. Mit der Einspeisung ins WWW werden sie regelmäßig der Allgemeinheit zugänglich gemacht. Das Erstellen und Anbieten von Homepages lässt sich demnach als Mediendienst i.S.d. § 2 I MDStV qualifizieren. Demgegenüber darf aber nicht vergessen werden, dass charakteristischerweise bei der Homepage häufig das Angebot zum Beginn einer Interaktion durch jeden einzelnen Nutzer im Vordergrund steht. Außerdem müssen die WWW-Seiten vom Nutzer individuell aufgerufen werden.[335] Sie sind deshalb doch wohl eher der Individualkommunikation zuzuordnen und erfüllen folglich auch die Kriterien des § 2 I TDG, der sie zu den Telediensten rechnet. Wird die Homepage aber hauptsächlich dazu benutzt, Informationen, Meinungen und Weltanschauungen zu verbreiten, so dass das interaktive Element in den Hintergrund tritt, muss sie als Mediendienst i.S.d. MDStV angesehen werden.[336]
Die vorstehenden Ausführungen zeigen, dass das öffentliche Anbieten und die individuelle Nutzung im WWW letztendlich verschmelzen.[337] Eine sinnvolle und vor allem klare Abgrenzung nach § 2 I TDG ist daher kaum möglich. Darüber hinaus könnten die Homepages, falls sie „*direkte Angebote an die Öffentlichkeit für den Verkauf, Kauf oder*

---

332 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675, 679.
333 Zu dem Begriff „Browser“ vgl. auch oben Fn. 222.
334 Siehe oben unter B. 1. Teil. I. 3. g.
335 Flechsig/Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 353.
336 Heyl, „Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag“, ZUM 1998, 115, 119.
337 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675, 679.

Miete oder Pacht von Erzeugnissen oder die Erbringung von Dienstleistungen (Fernsehkauf)“ enthalten, unter § 2 II Nr. 1 MDStV subsumiert werden. Dies ist jedoch zu verneinen, da § 2 II Nr. 1 MDStV gemäß seinem Wortlaut nur den Fernsehkauf regeln will. Das macht auch § 2 II Nr. 5 TDG deutlich, der die Spezialfälle des interaktiven Zugriffs auf Angebote von Waren und Dienstleistungen normiert.[338] Ferner kommt es bei den Homepages darauf an, was sie im einzelnen für einen Inhalt besitzen. So ist beispielsweise ein auf der Webseite befindlicher Werbebanner mit Informationen über ein bestimmtes Produkt als Teledienst i.S.d. § 2 Nr. 2 TDG anzusehen.[339] Die oft aufgeführten Hyperlinks auf anderen Webseiten können ebenfalls als „*Angebote zur Information und Kommunikation*“ nach § 2 II Nr. 2 TDG eingestuft werden, wobei § 2 II Nr. 2 TDG jedes Mal von § 2 II Nr. 4 MDStV abzugrenzen ist, da beide Vorschriften Abrufdienste behandeln.[340]

Es wird deutlich, dass eine Einordnung der Webseiten des WWW immer komplizierter wird, je feiner die einzelnen Seiten aufgegliedert und anhand des TDG und des MDStV untersucht werden. Um das zu vermeiden, könnte der Ansicht von Waldenberger[341] gefolgt werden, der in einer „wertenden Gesamtschau das vollständige, unter einer bestimmten Homepage (Eingangsseite) einschließlich der untergeordneten Seiten abrufbare Angebot eines Unternehmens als diejenige „Einheit“ (als den „Dienst“)“ betrachtet, auf die es für eine Abgrenzung zwischen Tele- und Mediendienst ankommt. Diese Überlegung ist jedoch abzulehnen, da manche Homepages über äußerst umfangreiche Inhalte verfügen. Eine klare Abgrenzung und die damit verbundene Bestimmung eines einheitlichen Dienstes ist somit in vielen Fällen nicht möglich.

Insgesamt lässt sich sagen, dass es beim WWW hinsichtlich seiner Einordnung als Tele- oder Mediendienst auf die jeweiligen Inhalte ankommt. Denn obwohl eine Homepage als Angebot an eine unbestimmte Vielzahl von Nutzern und deshalb grundsätzlich an die Allgemeinheit gerichtet ist, steht doch ihre Funktion als Angebot zum Beginn einer Interaktion durch jeden einzelnen Nutzer im Vordergrund. Sie ist deshalb der Individualkommunikation zuzuordnen und genügt demzufolge den Kriterien des TDG. Das WWW ist also in den häufigsten Fällen als Teledienst zu qualifizieren, zumal sich auf den meisten Web-Seiten Werbebanner befinden, so dass hierdurch § 2 II Nr. 2 TDG erfüllt ist.[342] Wird die Homepage aber hauptsächlich dazu benutzt, Informationen, Meinungen und Weltanschauungen zu verbreiten, wodurch das interaktive Element eher als

---

338 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 2 MDStV Rdnr. 3.

339 Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 125.

340 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 2 TDG Rdnr. 5.

341 Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 125.

342 Heyl, „Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag“ ZUM 1998, 115, 120.

zweitrangig anzusehen ist, muss sie als Mediendienst i.S.d. MDStV eingestuft werden.[343]
Letztendlich bleibt es somit eine Frage des Einzelfalls, ob das WWW dem TDG oder dem MDStV zuzuordnen ist.

cc. Die Dienste der Provider

(1) Einordnung des Network-Providings

Wie bereits oben angesprochen, stellt der Network-Provider Übertragungswege oder Übertragungskapazitäten zur Verfügung.[344] Dabei kann es sich zum einen um Telekommunikationsinfrastruktur im herkömmlichen Sinne handeln, beispielsweise ein „Public Switched Telephone Network" (PSTN)[345]. Zum anderen ist damit aber auch die für Datennetze spezifische Infrastruktur gemeint, sprich Rechnersysteme, die über Wahl- oder Standleitungen miteinander verbunden sind, sowie die Router und Backbones.
Gemäß § 3 Nr. 18 i.V.m. § 3 Nr. 16 TKG ist eine Telekommunikationsdienstleistung „*das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte*". Das Anbieten von Übertragungswegen und -kapazitäten ist somit eine Telekommunikationsdienstleistung.[346] Wichtig ist hierbei der Umstand, dass § 3 Nr. 16 TKG weit auszulegen ist, so dass mit ihm nicht nur die herkömmlichen Telefondienste oder ISDN[347] gemeint sind.[348] Vielmehr werden auch die modernen Telefondienste samt Internet unter diese Norm gefasst.[349]
Die Tatsache, dass der Network-Provider teilweise auch den Wortlaut des § 2 I TDG erfüllt, da er die (Daten-) „*Übermittlung mittels Telekommunikation*" anbietet, ist für die Einordnung des Network-Providings als Telekommunikationsdienstleistung irrelevant. Denn der Netzanbieter stellt gerade keinen „*elektronischen Informations- und Kommunikationsdienst*" dar, den § 2 I TDG in seiner Teledienst-Definition verlangt.[350] Der Network-Provider offeriert nur die telekommunikativen Grundlagen für einen Teledienst.[351] Demnach ist auf den Netzanbieter nicht das TDG, sondern allein das TKG anwendbar.

---

343 Heyl, „Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag", ZUM 1998, 115, 119.
344 Vgl. oben unter B. 1. Teil. I. 4. a.
345 Hierunter ist das gewöhnliche Telefonnetz zu verstehen.
346 Schuster in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), Beck´scher TKG Kommentar, § 4 Rdnr. 5.
347 ISDN ist die Abkürzung für "Integrated Services Digital Network".
348 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern", CR 1999, 438, 439.
349 Etling-Ernst, Telekommunikationsgesetz Kommentar, § 3 Rdnr. 22.
350 Koenig/Loetz: „Sperrungsanordnungen gegenüber Network- und Access-Providern", CR 1999, 439; Etling-Ernst, Telekommunikationsgesetz Kommentar, § 3 Rdnr. 22; Schaar, „Datenschutzfreier Raum Internet", CR 1996, 170, 173 f.
351 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 37.

(2) Einordnung des Access-Providings

Im Gegensatz zum Network-Provider bietet der Access-Provider nicht nur die Nutzung von Übertragungskapazitäten an. Spezifisch für den Access-Provider ist das Angebot einer bestimmten Form der Datenübertragung, die den Zugang zu einem Rechner(netz) gestattet.[352] Der Access-Provider bietet demnach alle Funktionen an, die notwendig sind, um den Rechner eines Nutzers Teil des Kommunikationsnetzes werden zu lassen.[353]

Die Einordnung dieser Dienste in die Gesetze TKG, TDG und MDStV erweist sich als schwierig.[354] Denn der Access-Provider bietet nicht nur reine Telekommunikationstechnik an, sondern ermöglicht dem Nutzer auch den Zugriff auf fremde Inhalte im Internet. Dies zeigt, dass der Access-Provider eine Zwitterstellung einnimmt, der sich rechtlich nicht eindeutig vom Network-Provider und somit vom TKG abgrenzen lässt.[355] Es stellt sich somit die Frage, ob der Access-Provider von den Normen des TKG oder des TDG erfasst wird:

Eine direkte Subsumtion unter die abstrakte Definition des § 2 I TDG setzt voraus, dass der Access-Provider einen Informations- und Kommunikationsdienst „*für die individuelle Nutzung*“ anbietet. Problematisch ist hierbei jedoch, dass erst die Dienstleistung des Access-Providers dazu führt, solche Dienste überhaupt nutzbar zu machen. Er bietet also einen Teil der technisch-telekommunikativen Grundlage an, die einen Informations- und Kommunikationsdienst zur individuellen Nutzung erst ermöglicht. Auch die Teledienstedefinition in § 2 I TDG führt beim Access-Provider zu keinem sinnvollen Ergebnis. Denn eine Nutzung „*von kombinierbaren Daten wie Zeichen, Bilder und Töne*“ i.S.d. § 2 I TDG bietet der Access-Provider ebenfalls nicht an, da der Nutzer durch ihn lediglich auf solche von Dritten bereitgestellte Daten zugreifen kann.

Eine konkrete Einordnung des Access-Providings könnte jedoch mit Hilfe der Regelbeispiele des § 2 II TDG erreicht werden. So besteht die Möglichkeit, den Access-Provider unter die Vorschrift des § 2 II Nr. 3 TDG zu fassen.[356] § 2 II Nr. 3 TDG bestimmt, dass als Teledienste die „*Angebote zur Nutzung des Internets oder weiterer Netze*“ anzusehen sind. Wird dieser Wortlaut wörtlich angewendet, kann auch der Access-Provider hierunter subsumiert werden.[357] Diese Zuordnung hätte jedoch zur Folge, dass die Regelung in

---

352 Hoeren, Rechtsfragen des Internet, S. 128 Rdnr. 301; weiterführend: Wischmann, „Rechtsnatur des Access-Providing“, MMR 2000, 461 ff.

353 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 439 f.

354 Manssen in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, C § 3 Rdnr. 37.

355 Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 597.

356 Schuster in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), Beck´scher TKG Kommentar, § 4 Rdnr. 4.

357 So beispielsweise Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 2 TDG Rdnr. 6. Begründet wird diese Meinung mit der amtlichen Begründung zu Art. 1 § 2 IuKDG, vgl. Bundesrat-Drucksache 966/96 S. 20 f. Im Ergebnis wohl auch Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675, 679.

§ 5 III MDStV ins Leere laufen würde, da der adressierte Anbieterkreis bereits dem Geltungsbereich des TDG zugerechnet wäre.[358] Aus diesem Grund und wegen einer anderen Interpretation der Begründung zu Art. 1 § 2 II Nr. 3 IuKDG[359] gibt es aber auch die Meinung, den Access-Provider gerade nicht unter § 2 II Nr. 3 TDG zu fassen. Vielmehr soll diese Norm nur für Suchmaschinen oder Navigationshilfen im Internet gelten.[360] Leider sind die Begründungen zu § 2 II Nr. 3 TDG nicht eindeutig. So sollen einerseits die „Angebote zur Nutzung der neuen Dienste" hiervon erfasst werden.[361] Dann wären – gemäß diesem Wortlaut – gerade die Access-Provider unter diese Vorschrift zu subsumieren. Andererseits werden als Beispiel für diese Angebote „Navigationshilfen" genannt, die mit einem Access-Providing grundsätzlich nicht in unmittelbaren Zusammenhang stehen. Es spricht aber sehr viel dafür, dass der Gesetzgeber mit dem genannten Beispiel eine Interpretationshilfe schaffen wollte. Demzufolge sollen die Angebote zur Nutzung der neuen Dienste so verstanden werden, dass nicht das Angebot zum direkten Internet-Zugang hierunter fällt, sondern lediglich Dienste, die – wenn der Internet-Zugang bereits geschaffen ist – zur Nutzung der einzelnen Dienste im Internet behilflich sind. Dazu zählen vor allem die Suchmaschinen und Navigationshilfen. Der Unterschied im Wortlaut von § 2 II Nr. 3 TDG, der von einem „*Angebot zur Nutzung*" spricht, und den §§ 3 Nr. 1, 5 III TDG a.F. bzw. § 9 TDG n.F., die den „*Zugang zur Nutzung*" enthalten, bestätigt diese Auslegung. Folglich kann der Access-Provider nicht unter § 2 II Nr. 3 TDG subsumiert werden.[362] Auch die übrigen Regelbeispiele des § 2 II TDG greifen hier nicht. Der Access-Provider kann demnach nicht anhand des § 2 TDG als Teledienst qualifiziert werden.[363] Es besteht jedoch darüber hinaus die Möglichkeit, ihn mit Hilfe des TKG rechtlich einzuordnen. Der Access-Provider hat grundsätzlich die Aufgabe, dem Nutzer den Zugang zum Internet zu verschaffen und ihm bestimmte Inhalte im Netz zu übermitteln. Er besitzt gewissermaßen Transportfunktion.[364] Der Dienst des Access-Providers kann somit unter den Wortlaut des § 3 Nr. 16 TKG

---

358 Vgl. hierzu Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen", CR 1997, 193, 194 insbesondere Fn. 4.

359 Bundestag-Drucksache 13/7385 zu Art. 1 § 2 II Nr. 3; zu Nummer 3 werden folgende Ausführungen gemacht:
„Es werden die von den Zugangsvermittlern – insbesondere Online-Anbietern – bereitgestellten Angebote zur Nutzung der neuen Dienste erfasst (z.B. Navigationshilfen). Die Zuordnung der hierdurch vermittelten Angebote richtet sich nach den Nummern 1, 2, 4 und 5."

360 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern", CR 1999, 438, 439 f.; Engel-Flechsig/Maennel/Tettenborn, Neue gesetzliche Rahmenbedingungen für Multimedia, S. 11.

361 Vgl. amtliche Begründung zu Art. 1 § 2 IuKDG in Bundesrat-Drucksache 966/96 S. 20.

362 Schuster in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), Beck´scher TKG Kommentar, § 4 Rdnr. 4 b.

363 So auch: Manssen in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, C § 3 Rdnr. 37; Dietz/Richter, „Netzzugänge unter Internet Service Providern", CR 1998, 528 ff.; a.A. wohl Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 3 MDStV Rdnr. 5, die den Access-Provider als Teledienst ansehen.

364 Schuster in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), Beck´scher TKG Kommentar, § 4 Rdnr. 4 b; Manssen in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, C § 3 Rdnr. 37.

gefasst werden, weil er einen technischen Vorgang zum Aussenden, Übermitteln und Empfangen von Nachrichten mittels Telekommunikationsanlagen darstellt. Dadurch, dass das Access-Providing in der Regel gewerblich erbracht wird, handelt es sich hierbei um eine Telekommunikationsdienstleistung i.S.d. § 3 Nr. 18 TKG. Auf den reinen Access-Provider finden deshalb grundsätzlich die Normen des TKG und nicht die des TDG Anwendung.[365]

Allerdings wirft dieses Ergebnis erhebliche Probleme auf. So wäre bei einer Unanwendbarkeit des TDG auf den Access-Provider § 5 III TDG a.F. bzw. § 9 TDG n.F. sinnlos. Ein Vergleich von § 3 Nr. 1 und § 5 III TDG a.F. bzw. § 9 TDG n.F. ergibt aber, dass auch ein Access-Provider als Zugangsvermittler unter das TDG und insbesondere unter die Vorschrift des § 5 TDG a.F. bzw. § 9 TDG n.F. fallen kann. Denn § 3 Nr. 1 TDG erwähnt als „*Diensteanbieter*“ ebenfalls solche, die „*den Zugang zur Nutzung vermitteln*“.[366] Diese Formulierung des § 3 Nr. 1 TDG bestätigt zwar noch mal, dass die Vermittlung des Zugangs zu Telediensten selbst keinen Teledienst i.S.d. § 2 I TDG darstellt,[367] aber über die Definition des Diensteanbieters in den Anwendungsbereich des Gesetzes einbezogen wird. Andernfalls wäre § 3 Nr. 1 Alt. 2 TDG überflüssig, da für das Access-Providing immer bereits § 3 Nr. 1 Alt. 1 TDG einschlägig wäre. Dies kann jedoch nicht richtig sein. § 3 Nr. 1 Alt. 2 TDG sowie § 5 III TDG a.F. bzw. § 9 TDG n.F. machen also nur dann Sinn, wenn sie auch auf Zugangsvermittler angewendet werden können, die selbst keine Teledienste sind.

Aufgrund der Tatsache, dass § 3 Nr. 1 Alt. 2 TDG im Gegensatz zu § 3 Nr. 1 Alt. 1 TDG gerade nicht von Telediensten, sondern nur von einer Zugangsvermittlung spricht, wird deutlich, dass der Gesetzgeber ausdrücklich keine Teledienst-Eigenschaft für Zugangsvermittler nach § 3 Nr. 1 Alt. 2 TDG voraussetzt. Ebenso verhält es sich bei § 5 III TDG a.F. bzw. § 9 TDG n.F.[368] Die Vorschriften der §§ 3 Nr. 1 Alt. 2 und 5 III TDG a.F. bzw. § 9 TDG n.F. kommen also auf Zugangsvermittler auch dann zur Anwendung, falls sie nicht als Teledienste i.S.d. § 2 I TDG qualifiziert werden können. Dies ergibt sich auch aus § 5 IV TDG a.F. bzw. § 8 II 2 TDG n.F., der mit § 5 III TDG a.F. bzw. § 9 TDG n.F. im Zusammenhang steht und das TDG mit dem TKG verbindet, indem er auf § 85 TKG verweist.[369] Als übertragungstechnisches Bindeglied zwischen Content-Provider und Nutzer fungiert der Access-Provider als Zugangsvermittler.[370] Die Tätigkeit des Access-Providers unterfällt demnach der Zugangsvermittlung nach §§ 3 Nr. 1, 5 III TDG a.F. bzw. § 9 TDG n.F. Dies bedeutet, dass – obwohl der Access-Provider regelmäßig Telekommunikationsdienstleistungen gemäß § 3 Nr. 18 TKG erbringt – auf

---

365 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 112.

366 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 112.

367 Manssen in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, C § 3 Rdnr. 37 m.w.N.

368 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 111 f.

369 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 148 f.

370 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 440.

ihn, neben dem TKG, die §§ 3 Nr. 1 Alt. 2, 5 III sowie 5 IV TDG a.F. bzw. §§ 9 und 8 II 2 TDG n.F. anwendbar sind.[371]

Es wurde bereits angedeutet, dass die Anwendbarkeit des § 5 III sowie IV TDG a.F. bzw. §§ 9 und 8 II 2 TDG n.F. und damit eine Zuordnung des Access-Providers zum TDG den § 5 III i.V.m. § 18 III MDStV obsolet machen würde. Folglich muss noch geklärt werden, wie die Gesetzeskollision zwischen dem TDG und dem MDStV zu behandeln ist:

Eine Meinung in der Literatur verneint die Anwendbarkeit des MDStV beim Access-Provider.[372] Diese Ansicht wird damit begründet, dass es sich bei dieser Art von Zugangsvermittlung um einen Dienst aus der Individualkommunikation handelt, der dem Regelungsbereich des TDG unterliegt. Somit soll eine Anwendbarkeit der §§ 3 Nr. 1 und 5 III MDStV von vornherein ausscheiden.[373] Diese Meinung ist jedoch wenig überzeugend. So wird schon außer Acht gelassen, dass beide Vorschriften in § 5 III TDG a.F. bzw. § 9 TDG n.F. sowie MDStV gleichermaßen die Zugangsvermittlung regeln. Der Gesetzgeber wollte also auch die §§ 3 Nr. 1 Alt. 2, 5 III und § 18 III MDStV auf den Access-Provider anwenden, obwohl er nicht als Mediendienst i.S.d. § 2 I MDStV angesehen werden kann. Es muss deshalb ein Kriterium gefunden werden, wonach wiederum zwischen Tele- und Mediendienst unterschieden werden kann, so dass entweder das TDG oder der MDStV auf den Access-Provider bedingt zur Anwendung kommen können. Da der Access-Provider selbst kein Tele- oder Mediendienst ist, er aber den Zugang zu fremden Tele- oder Mediendiensten vermittelt, kann als sinnvolles Unterscheidungsmerkmal auf den jeweiligen Inhalt abgestellt werden, für den der Access-Provider den Zugang vermittelt. Handelt es sich hierbei um einen Teledienst i.S.d. § 2 I TDG, dann richtet sich seine Verantwortlichkeit nach § 5 III und IV TDG a.F. bzw. §§ 9 und 8 II 2 TDG n.F.. Vermittelt der Access-Provider dagegen den Zugang zu Mediendiensten, dann findet § 5 III MDStV Anwendung.[374] Neben diesen Normen des TDG und des MDStV sind natürlich auch die des TKG für den Access-Provider weiter zu beachten.

Zusammenfassend ergibt sich also folgendes: Auf den Access-Provider, der eine Telekommunikationsdienstleistung i.S.d. § 3 Nr. 18 TKG anbietet, ist grundsätzlich das TKG anwendbar. Allerdings richtet sich seine Verantwortlichkeit, je nachdem, ob er den Zugang zu Tele- oder Mediendiensten vermittelt, darüber hinaus nach § 5 III und IV TDG a.F. bzw. §§ 9 und 8 II 2 TDG n.F. sowie nach § 5 III i.V.m. § 18 III MDStV.

---

371 Manssen in: Manssen (Hrsg.), Telekommunikations- und Multimediarecht, C § 3 Rdnr. 37.

372 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 3 MDStV Rdnr. 5.

373 Zu bemerken ist hierfür, dass diese Meinung bereits das Access-Providing als Teledienst ansieht.

374 So auch Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 112 f.; Sieber, Verantwortlichkeit im Internet, S. 196 f. Rdnr. 393 ff. geht ebenfalls von einer Anwendbarkeit des TDG und MDStV neben dem TKG aus.

(3) Einordnung des Content-Providings

Hauptmerkmal des Content-Providers ist es, dass er eigene Dienste und damit gleichzeitig eigene Inhalte zum Abruf bereithält.[375] Eigene Dienste liegen dann vor, wenn der Diensteanbieter die Dienste produziert bzw. hergestellt hat.[376] Dabei sind eigene Inhalte i.S.d. § 3 Nr. 1 TDG/MDStV auch von Dritten hergestellte Inhalte, die sich der Anbieter zu eigen macht. Dies geht aus der amtlichen Begründung zu § 5 MDStV hervor.[377] Der Anbieter macht sich dann Inhalte von Dritten zu eigen, wenn der Diensteanbieter den Inhalt in seinen Angebotsbereich übernimmt und aus der Sicht des objektiven Nutzers die Verantwortung für diesen Inhalt übernehmen will.[378]
Der Content-Provider ist in § 3 Nr. 1 TDG und in § 3 Nr. 1 MDStV geregelt.[379] Welches Gesetz wann zur Anwendung kommt, richtet sich danach, ob der Content-Provider Tele- oder Mediendienste anbietet. Hinsichtlich der Einordnungsproblematik der einzelnen Internet-Dienste in Tele- oder Mediendienste kann insoweit auf die früheren Ausführungen verwiesen werden.[380]
Im Ergebnis lässt sich sagen, dass der Content-Provider je nach seinen angebotenen Inhalten entweder unter das TDG oder unter den MDStV fällt.

(4) Einordnung des Service-Providings

Der Service-Provider hält im Gegensatz zum Content-Provider keine eigenen, sondern fremde Inhalte gemäß § 3 Nr. 1 TDG bzw. MDStV für die Nutzer bereit.[381] Fremd sind alle Inhalte, die der Anbieter nur bereithält, sie selbst also nicht hergestellt oder beschafft hat.[382]
Welches Gesetz auf den Service-Provider anzuwenden ist, richtet sich wiederum nach der Einstufung seines Inhalts als Tele- oder Mediendienst.

dd. Zusammenfassung

Die Dienste des Internets in die neuen multimedialen Gesetze einzugliedern, d.h. das „Netz der Netze“ und deren Dienste konkret einer Norm zuzuordnen, bereitet sehr große Schwierigkeiten. Als Grund hierfür kann vor allem die momentane Gesetzeslage genannt werden, die leider noch nicht sehr ausgereift wirkt. Eine Einordnung der Dienste des Internets in die jeweiligen einschlägigen Gesetze führt deshalb nicht immer zum gewünschten Erfolg. Allerdings gelingt es recht gut, eine grobe Aufteilung vorzuneh-

375 Eichhorn, Internet-Recht, S. 43.
376 von Bonin/Köster, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821, 823.
377 Vgl. Begründungen in Bundestag-Drucksache 13/7385 zu Art. 1 § 5 IuKDG S. 51 f.
378 Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien“, MMR 1998, 23, 24; Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 197.
379 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 3 MDStV Rdnr. 3.
380 Vgl. oben unter B. 2. Teil. II. 4. c.
381 Spindler in: Rossnagel (Hrsg.), Recht der Multimedia-Dienste, § 2 TDG Rdnr. 52; Eichhorn, Internet-Recht, S. 43.
382 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 3 MDStV Rdnr. 4.

men. So kann zwischen der Telekommunikation, also der Technik des Internets, sowie den Informations- und Kommunikationsdiensten unterschieden werden.[383] Ob nun das TKG oder das TDG bzw. der MDStV auf bestimmte Internet-Bereiche angewendet werden, lässt sich somit oft noch recht einfach klären. Problematischer zu beantworten ist dagegen die Frage, ob ein Tele- oder Mediendienst vorliegt. Dies lässt sich manchmal nicht mehr eindeutig bestimmen. Aufgrund der Tatsache, dass in vielen Bereichen durch den Gesetzgeber bewusst wortgleiche Regelungen in das TDG und den MDStV aufgenommen wurden, ist diese Problematik etwas entschärft worden. Denn unabhängig von der Zuordnung eines Dienstes zu einem dieser Gesetze wird größtenteils dieselbe Rechtsfolge erzielt, so dass den bestehenden Streitigkeiten über die Zuordnung von vornherein die praktische Relevanz genommen wird.[384] Für eine gesetzliche Einordnung der Informations- und Kommunikationsdienste ist es daher vor allem wichtig, nach dem Inhalt zu fragen und dann diesen Inhalt entweder als Tele- oder Mediendienst zu qualifizieren.

Deshalb gibt es bei den Diensten des Internets sehr viele Graubereiche, die den einzelnen Gesetzen nicht exakt zugeordnet werden können. Hier ist zum einen der Gesetzgeber in der Pflicht, seine Regelwerke den aktuellen und künftigen Entwicklungen anzupassen. Aber auch die Literatur ist aufgefordert, die existierenden Gesetze so auszulegen, dass es in der Praxis zu keinen widersprüchlichen Ergebnissen kommt; dies wird derzeit versucht. In Zweifelsfällen ist es mithin angebracht, nach dem Schwerpunkt der angebotenen Dienste zu fragen, um sie entweder dem TDG oder dem MDStV zuordnen zu können.[385]

Für die vorliegende Arbeit ist eine Einordnung bestimmter Internet-Dienste zu diesen Gesetzen deswegen so wichtig, weil sich aus diesen Gesetzen z.T. die Rechtsgrundlage für staatliche Eingriffsmaßnahmen in das Internet ergeben kann.

5. Rechtsgrundlagen für Kontrollmaßnahmen im Internet gemäß dem TKG, TDG und MDStV

Da das Internet auf nationaler Ebene weitgehend von den Gesetzen TKG, TDG und MDStV erfasst wird, ist nun zu prüfen, ob und inwieweit Normen in diesen Gesetzen die Anordnung von Kontrollmaßnahmen rechtfertigen können. Denn allenfalls bei Vorliegen einer Rechtsgrundlage hat der Staat die Möglichkeit, gemäß dem Prinzip des Vorbehalts des Gesetzes[386] im Rahmen dieser Vorschrift tätig zu werden, weil Lösch-

---

383 Dietz/Richter, „Netzzugänge unter Internet Service Providern“, CR 1998, 528, 530.

384 Kröger/Moos, „Mediendienst oder Teledienst?“, AfP 1997, 675, 680.

385 A.A. Schuster in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), Beck´scher TKG Kommentar, § 4 Rdnr. 4 a.

386 Sachs/Battis, GG-Kommentar, 2. Auflage, Art. 20 Rdnr. 113 ff.; Jarass in: Jarass/Pieroth, GG, 5. Auflage, Art. 20 Rdnr. 60.

bzw. Sperrmaßnahmen belastende Eingriffe gegenüber den adressierten Personen darstellen.

a. Telekommunikationsgesetz

Das TKG enthält auf den ersten Blick keine Norm, die es dem Staat oder den Erbringern von Telekommunikationsdiensten erlaubt, auf den Datenverkehr in irgendeiner Form Einfluss zu nehmen.

Dies lässt sich vor allem mit dem in Art. 10 GG fixierten postalischen Fernmeldegeheimnis erklären, das insoweit auch auf die Übertragungswege des Internets anzuwenden ist, weil sein Wesensgehalt in § 85 TKG eingearbeitet worden ist. Nach § 85 I TKG unterliegen dem Fernmeldegeheimnis „*der Inhalt der Telekommunikation und ihrer näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war*". Als Adressat dieser Vorschrift wird in § 85 II TKG bezeichnet, „*wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt*". Demnach müssen sich sämtliche Network-Provider, welche die Kriterien des § 85 II i.V.m. § 3 Nr. 5 TKG erfüllen, an das in § 85 TKG festgeschriebene Fernmeldegeheimnis halten. Eine Kontrolle der Datenautobahnen und der versendeten Informationen ist deshalb bis auf wenige Ausnahmen untersagt. § 85 III TKG macht dies noch einmal deutlich, indem er darauf hinweist, dass es den nach § 85 II TKG Verpflichteten verboten ist, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

Demgegenüber enthält jedoch § 89 TKG gewisse Ausnahmeregelungen, die in Extremfällen einen Eingriff in das Fernmeldegeheimnis zulassen. So können Daten gemäß § 89 II Nr. 1 e und Nr. 3 b TKG von natürlichen und juristischen Personen erhoben, verarbeitet und genutzt werden, wenn „*das Aufklären und das Unterbinden von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes*" bezweckt wird. Ferner gilt diese Norm für das Identifizieren von Anschlüssen, falls ein Nutzer *„das Ziel bedrohender oder belästigender Anrufe*" ist. Diese Befugnis der Datenverarbeitung wird jedoch von § 89 III TKG wieder eingeschränkt, der bestimmt, dass nur die näheren Umstände der Telekommunikation bzw. im Einzelfall Steuersignale erhoben, verarbeitet und genutzt werden dürfen. Die Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten selbst sind gemäß § 89 III 3 TKG unzulässig, es sei denn, dass sie nach § 89 IV TKG notwendig oder im Einzelfall für Maßnahmen nach § 89 V TKG unerlässlich sind.

§ 89 IV und V TKG regeln aber lediglich die zulässige Datenverarbeitung aus verarbeitungstechnischen Gründen sowie zum Erkennen und Eingrenzen von Störungen. Ein Gebrauch der versendeten Daten ist also nur zum Wohle einer reibungslosen Übertragung möglich. Die Tatsache, dass bei einer Übertragung rechtswidrige oder strafbare

Daten verschickt werden, hat demzufolge im Rahmen des TKG kaum eine Bedeutung, da es hier größtenteils nicht um den Inhalt des Datentransports, sondern nur um seinen ordnungsgemäßen technischen Ablauf geht. Wegen Art. 10 GG und somit wegen § 85 TKG darf auch nichts anderes gelten. Wie sich aus dem Wortlaut von § 85 I TKG ergibt, schützt er die Telekommunikation in ihrer Gesamtheit.[387] Eine Kenntnisnahme ist nur im zur Erbringung der Telekommunikationsdienste erforderlichen Maße zulässig. Des weiteren ist eine Weitergabe nur im Rahmen besonderer gesetzlicher Regelungen sowie der Anzeigepflicht nach § 138 StGB erlaubt. Folglich bleibt es bei der Regel, dass jegliche Telekommunikation, selbst wenn sie rechtswidrige Inhalte zum Gegenstand hat, dem Fernmeldegeheimnis unterfällt.[388]
Abschließend ist deshalb festzuhalten, dass sich – abgesehen von den oben beschriebenen, sehr begrenzten Ausnahmefällen – aus dem TKG keine Eingriffsbefugnis ableiten lässt, um im Rahmen des Datenaustausches im Internet auf telekommunikative Vorgänge Einfluss nehmen zu können.

b. Teledienstegesetz und Mediendienste-Staatsvertrag

Die Frage nach einer Rechtsgrundlage für staatliche Kontrollmaßnahmen konzentriert sich beim TDG a.F. und dem MDStV hauptsächlich auf den § 5 dieser Gesetze. Darin ist die Verantwortlichkeit für die sogenannten Diensteanbieter des Internets geregelt.[389] Eine Eingriffsbefugnis stellen diese Vorschriften – außer § 5 III 2 i.V.m. § 18 III MDStV – zunächst nicht dar. Vielmehr regeln sie, inwieweit welcher Diensteanbieter im Internet für gewisse Inhalte „*verantwortlich*“ ist. Regelungsgegenstand des § 5 TDG a.F. und § 5 MDStV ist demnach die „Verantwortlichkeit“ der jeweiligen Diensteanbieter des Internets. Verantwortlichkeit bedeutet im allgemeinen juristischen Sprachgebrauch „Einstehenmüssen“.[390] Sie ist also im Vergleich zur „Haftung“ der neutralere, aber auch weitreichendere Begriff, der sämtliche Anspruchsgrundlagen und Tatbestände umfasst, woraus Rechtsfolgen abgeleitet werden können, für die eine Person einzustehen hat.[391]

---

387 Etling-Ernst, TKG-Kommentar, § 85 Rdnr. 1; Büchner in: Büchner/Ehmer/Geppert/u.a. (Hrsg.), TKG-Kommentar, § 85 Rdnr. 1 ff.

388 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 145; Klesczewski, „Das Ende des Auskunftsersuchens nach § 12 FAG“, JZ 1997, 719, 720 f.

389 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 354.

390 Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links“, CR 1998, 545, 548; vgl. Tilch, Deutsches Rechts-Lexikon, Band 3, 2. Auflage, S. 878, Stichwort „Verantwortlichkeit“; Creifelds/Weber (Hrsg.), Rechtswörterbuch, 15. Auflage, S. 1421.

391 Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien“, NJW 1997, 3193, 3194 f.; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 158; Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 196; Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 9.

aa. Regelungsumfang

Die rechtliche Einordnung der Verantwortlichkeitsregelungen im TDG a.F. und MDStV ist jedoch nicht unumstritten. Es haben sich bereits eine ganze Reihe von Autoren mit der Auslegung und Reichweite des § 5 TDG a.F. bzw. § 5 MDStV beschäftigt.[392] Deutlich erkennbar sind hier stark voneinander abweichende Vorstellungen über die Funktion der Verantwortlichkeitsklauseln:

So wird die Meinung vertreten, dass die im TDG a.F. und MDStV enthaltenen wortgleichen Haftungsprivilegien zwar auf zivil- und strafrechtliche Verantwortlichkeiten, aber nicht auf verwaltungsrechtliche Inpflichtnahmen angewendet werden sollen.[393] Begründet wird diese Ansicht mit der Entstehungsgeschichte dieser Vorschriften. Denn in den Gesetzgebungsmaterialien zum TDG a.F. heißt es, dass § 5 I bis III des TDG a.F. nur die strafrechtliche und deliktische Verantwortlichkeit regeln sollen.[394] Des weiteren wird argumentiert, dass polizeirechtliche Fragen von § 5 I bis III a.F. schon wegen § 5 IV TDG a.F. nicht erfasst werden dürfen. Denn § 5 IV TDG a.F. stellt ausdrücklich klar, dass objektive, verschuldensunabhängige Verpflichtungen, wie Störungen der öffentlichen Sicherheit und Ordnung, zu unterlassen sind und unter den dort im einzelnen genannten Voraussetzungen von § 5 I bis III TDG a.F. unberührt bleiben sollten.[395] Dieser Begründung wird jedoch entgegengehalten, dass § 5 IV TDG a.F. seinerseits keine eigenständige Verpflichtung zur Unterlassung solcher Störungen oder eine damit korrespondierende Eingriffsermächtigung besitzt, sondern die Existenz solcher, bereits nach den allgemeinen Gesetzen bestehenden Verpflichtungen voraussetzt.[396] Nach dieser Meinung soll § 5 TDG a.F. das Einstehenmüssen für die Rechtsfolgen ganz allgemein regeln. Folglich müsste der § 5 I bis III TDG a.F. nicht nur im Straf- und Zivilrecht, sondern auch im Verwaltungsrecht zur Anwendung kommen.[397] Schließlich wird die Ansicht vertreten, dass zwar § 5 TDG a.F. grundsätzlich auf alle denkbaren zivil-, straf- und öffentlich-rechtlichen Tatbestände anwendbar ist, allerdings soll er nicht für das

---

392 Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 126; Gounalakis, „Der Mediendienste-Staatsvertrag der Länder“, NJW 1997, 2993, 2995; Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien“, NJW 1997, 3193 ff.; Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 195 ff.; Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3147 f.

393 So beispielsweise Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3148 und Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 126.

394 Vgl. insoweit die Regierungsbegründung zu Art. I § 5 IuKDG, Bundestag-Drucksache 13/7385 vom 09.04.1997, S. 20: „...Absatz 1 bis 3 die strafrechtliche und deliktische Verantwortlichkeit der Dienstanbieter zum Gegenstand haben...“.

395 Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3148

396 Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984.

397 Ebenso Lehmann, „Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht“, CR 1998, 232, 233, der insoweit auf Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981 ff. verweist.

Urheberrecht gelten, da das UrhG in seinen §§ 97 ff. Urhebergesetz (UrhG)[398] eine detaillierte Regelung der Verantwortlichkeit bei Verletzungen des Urheberrechts bzw. verwandter Schutzrechte enthält.[399]

Obwohl in den amtlichen Begründungen zum § 5 TDG a.F. nur von strafrechtlicher und zivilrechtlicher deliktischer Verantwortlichkeit der Dienstanbieter die Rede ist, erscheint es sinnvoll, die in § 5 II und III TDG a.F. enthaltenen Haftungsfreistellungen auch auf ordnungsbehördliche Maßnahmen auszudehnen.[400] Zunächst besteht kein Grund, das Verwaltungsrecht im Rahmen des § 5 TDG a.F. auszuklammern; zumal es diese Norm selbst nicht tut.[401] Die Vorschrift ist gerade deswegen so allgemein gehalten, damit sie auf sämtliche Gesetzesbereiche angewendet werden kann. Dies wird durch § 5 I und IV TDG a.F. deutlich, die in ihren Tatbeständen von den „*allgemeinen Gesetzen*“ sprechen und nicht nur von den zivil- und strafrechtlichen Regelwerken.[402] Demnach muss schon allein aufgrund des Wortlauts von § 5 TDG a.F. der Schluss gezogen werden, dass er die zivilrechtliche, strafrechtliche und verwaltungsrechtliche Verantwortlichkeit der Betreiber von elektronischen Kommunikationsdiensten in einer knappen und übersichtlichen Norm regeln soll, die eigenständig neben die speziellen Verantwortlichkeitsnormen der verschiedenen Rechtsgebiete tritt.[403] Im übrigen handelt es sich beim Urheberrecht um ein spezialgesetzlich geregeltes besonderes Deliktsrecht. Folglich kommt § 5 TDG a.F. sogar auf das Urheberrecht zur Anwendung, denn er soll insbesondere das Deliktsrecht regeln.[404]

Da § 5 MDStV mit § 5 TDG a.F. weitgehend übereinstimmt[405] und es – wie oben beschrieben – sehr schwer ist, gewisse Dienste im Internet entweder dem TDG oder dem MDStV zuzuordnen, hat dieses Ergebnis auch für § 5 MDStV zu gelten.

---

398 Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 09.09.1965, BGBl. I S. 1273, BGBl. III/FNA 440-1.

399 Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124, 127; Marwitz, „Haftung für Hyperlinks“, K&R 1998, 369; im Ergebnis auch Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 202 f.; vgl. zu diesem Thema auch den ausführlichen Beitrag von Schaefer/Rasch/Braun, „Zur Verantwortlichkeit von Online-Diensten und Zugangsvermittlern für fremde urheberrechtsverletzende Inhalte“, ZUM 1998, 451, 451 ff.; so auch OLG München im Urteil vom 08.03.2001 – Az.: 29 U 3282/00, K&R 2001, 471 ff.

400 So auch Flechsig/Gabel in: „Strafrechtliche Verantwortlichkeit im Netz durch einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 357, falls die Schwelle zur Strafbarkeit noch nicht überschritten sein sollte; Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 12; Maennel in: Engel-Flechsig/Maennel/Tettenborn (Hrsg.), Beck´scher IuKDG Kommentar, § 5 TDG Rdnr. 13 f.

401 Schwerdtfeger in: Schwarz (Hrsg.), Recht im Internet, Ziff. 6-2.2 S. 64a.

402 Vgl. hierzu auch die Ausführungen von Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 151 ff.

403 Engels, „Haftung für Anzeigen in Online-Angeboten“, K&R 2001, 338, 340; Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581, 583.

404 Decker, „Haftung für Urheberrechtsverletzungen im Internet“, MMR 1999, 7, 8; so auch LG München im Urteil vom 30.03.2000 – Az.: 7 O 3625/98, NJW-CoR 2000, 303, 304.

405 Lehmann, „Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht“, CR 1998, 232, 233.

bb. Filterfunktion

Neben der Frage, für welche Rechtsgebiete der § 5 TDG a.F. Wirkung entfalten soll, wird auch darüber diskutiert, wie § 5 TDG a.F. eigentlich anzuwenden ist:
Nach der überwiegenden Meinung in Rechtsprechung und Literatur soll ein möglicher Haftungsfall zunächst den „Filter" des § 5 TDG a.F. passieren,[406] damit dann die Prüfung nach den Maßstäben des jeweils einschlägigen Rechtsgebiets (Zivilrecht, Strafrecht, Polizei- und Ordnungsrecht, etc.) erfolgen kann.[407] Diese Auffassung ist allerdings insofern problematisch, als zwischen dem sogenannten § 5 TDG-Filter und dem jeweils einschlägigen Rechtsgebiet deutliche Überschneidungen existieren.[408] Infolge dessen wird auch eine „Integrationslösung" sowie eine vermittelnde Lösung vertreten, die einen selbständigen Charakter des § 5 TDG a.F. verneinen und den § 5 TDG a.F. in die Tatbestandsmerkmale des anzuwendenden allgemeinen Gesetzes einbauen wollen.[409] Diese Überlegungen zeigen, wie schwer es ist, die Regelungen des § 5 TDG a.F. rechtlich einzuordnen. Denn die Norm selbst zeitigt keine Rechtsfolge. Sie ergänzt vielmehr die allgemeinen Gesetze, indem sie ihren Anwendungsrahmen einschränkt. Wie diese Art von Vorschrift juristisch zu beurteilen ist, bleibt somit fraglich. Ist sie ein Teil der allgemeinen Gesetze (Integrationslösung) oder stellt sie eine unabhängige Norm dar (Filterlösung)?
Letztendlich ist dem Gedanken zu folgen, § 5 TDG a.F. bzw. § 5 MDStV als eine Art „Filter" zu sehen, mit dessen Hilfe eine gewisse Vorentscheidung hinsichtlich der Verantwortlichkeit getroffen werden kann.[410] Zum einen favorisiert der Gesetzgeber ebenfalls diese „Filterlösung". Denn wie sich aus den Begründungen zu § 5 TDG a.F. ergibt, soll die Verantwortlichkeitsprüfung nach § 5 TDG a.F. entsprechend einem Filter „vorgelagert" werden.[411] Zum anderen lässt sich die Anwendung des § 5 TDG a.F. als Filter auch aus seinem Wortlaut entnehmen. Denn nur erst wenn eine Verantwortlichkeit nach § 5 TDG a.F. bejaht werden kann, können die Tatbestände und Rechtsfolgen der allgemeinen Gesetze geprüft werden. Im übrigen erscheint die „Filter"-Lösung auch aus

---

406 Waldenberger, „Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet – ein Fall des LG Hamburg", AfP 1998, 373; Sieber in seinen Anmerkungen zum CompuServe-Urteil des AG-München, MMR 1998, 438, 438; Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 15 ff.; Engels, „Haftung für Anzeigen in Online-Angeboten", K&R 2001, 338, 340.

407 Spindler in: Rossnagel (Hrsg.), Recht der Multimedia-Dienste, § 5 TDG Rdnr. 36 ff.; Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz", NJW 1997, 2981, 2984; Sieber, Verantwortlichkeit im Internet, S. 123 f. Rdnr. 249 f.; Lehmann, „Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht", CR 1998, 232, 233.

408 So ist beispielsweise der in § 5 II TDG a.F. bzw. MDStV verwendete Begriff der „Kenntnis" von einem bestimmten Sachverhalt ein wichtiges Element des subjektiven Tatbestands.

409 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 153 ff.

410 Waldenberger in „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter", MMR 1998, 124, 127 bejaht ebenfalls die Filterwirkung des § 5 TDG a.F.

411 Bundestag-Drucksache 13/7385 vom 09.04.1997, S. 51; Bundestag-Drucksache 13/8153 vom 02.07.1997, S. 8 zu Nr. 14 a.

Gründen der Übersichtlichkeit bei der Subsumtion von Sachverhalten sinnvoll: Es muss zunächst § 5 TDG a.F. betrachtet werden, bevor eine weitere Prüfung der allgemeinen Gesetze erfolgen kann.[412] Im Ergebnis bedeutet dies für die Praxis, dass eine zweistufige Prüfung zu erfolgen hat: Auf der ersten Stufe ist anhand des § 5 TDG a.F. bzw. § 5 MDStV festzustellen, ob der Anbieter für einen bestimmten Inhalt überhaupt verantwortlich sein kann. Sobald dies bejaht wird, ist auf der zweiten Stufe nach Maßgabe des betroffenen Rechtsgebiets zu prüfen, ob die jeweilige Vorschrift aus dem Zivil-, Straf- oder Verwaltungsrecht einschlägig ist.[413] Dies gilt selbstverständlich ebenso für § 5 MDStV.[414]

Daraus folgt, dass bei präventiv motivierten Kontrollmaßnahmen, die auf das jeweilige Polizei- und Sicherheitsrecht gestützt werden sollen, zunächst der Filter des § 5 TDG a.F. bzw. § 5 MDStV rechtlich durchlaufen werden muss. Zudem ist es nötig, dass die polizei- und sicherheitsrechtliche Norm erfüllt ist. Sind beide Voraussetzungen gegeben, besteht eine nationale Rechtsgrundlage für die staatlichen Lösch- bzw. Sperrmaßnahmen.

Damit der Filter des § 5 TDG a.F. sowie des § 5 MDStV richtig angewendet werden kann, sind nun ihre Verantwortlichkeitsvorschriften näher zu untersuchen:[415]

cc. Teledienstegesetz

(1) Überblick

Der § 5 TDG a.F. regelt die Verantwortlichkeit der Diensteanbieter von Telediensten in den § 5 I bis III TDG a.F. funktionsbezogen:[416] Was der jeweilige Diensteanbieter zu verantworten hat, richtet sich nach der Art seiner Funktion im Internet. Somit wird von § 5 TDG a.F. die von der jeweiligen Handlungsform abhängige Einfluss- und Kontrollmöglichkeit des Diensteanbieters berücksichtigt. Dabei zielt die Abstufung auf die Privilegierung desjenigen Diensteanbieters, der eine Rechtsverletzung nur mittelbar begeht: Hält der Anbieter eigene Inhalte zur Nutzung bereit, haftet er gemäß § 5 I TDG a.F. nach den allgemeinen Gesetzen. Handelt es sich bei den zur Nutzung bereitgehaltenen Inhalten dagegen um fremde, haftet der Anbieter gemäß § 5 II TDG a.F. nur, wenn er von diesen Inhalten Kenntnis hat und es ihm technisch möglich sowie zumutbar ist,

---

412 Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984.

413 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 2.

414 Abgesehen von § 5 III 3 i.V.m. § 18 III MDStV, der selbst schon eine Ermächtigungsgrundlage darstellt. Vgl. Maennel in: Engel-Flechsig/Maennel/Tettenborn (Hrsg.), Beck´scher IuKDG Kommentar, § 5 TDG Rdnr. 20.

415 Es wird wiederum vorab darauf hingewiesen, dass das zu § 5 TDG a.F. Gesagte ebenso für § 5 MDStV gilt, sofern beide Normen identisch sind. Die nachstehende Behandlung der §§ 5, 18 MDStV beschränkt sich deshalb nur auf vom TDG a.F. abweichende Rechtsfragen.

416 Vgl. Bundestag-Drucksache 13/7385 zu Art. 1 § 3 bzw. 5 IuKDG, S. 19 f.; das AG-München in seinem CompuServe-Urteil vom 28.05.1998, MMR 1998, 429, 432 spricht insoweit von einer „aufgabenbezogenen“ Abgrenzung im Rahmen des § 5 TDG a.F.

ihre Nutzung zu verhindern. Vermittelt der Anbieter dagegen lediglich den Zugang zu fremden Inhalten, ist seine Verantwortlichkeit nach § 5 III 1 TDG a.F. ausgeschlossen. Dasselbe gilt für den sogenannten Proxy-Cache-Server, § 5 III 2 TDG a.F.[417] § 5 IV TDG a.F. nimmt hingegen – wie der Wortlaut schon zeigt – eine besondere Stellung in dieser Norm ein.[418]

(2) Bereithalten eigener Inhalte gemäß § 5 I TDG a.F.

Gemäß § 5 I TDG a.F. sind Diensteanbieter „*für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich*". Durch diese Norm wird klar gestellt werden, dass der aus der allgemeinen Rechtsordnung folgende Grundsatz der Eigenverantwortlichkeit der Diensteanbieter für die von ihnen angebotenen eigenen Inhalte auch im Rahmen der Teledienste gelten soll.[419] § 5 I TDG a.F. regelt die Verantwortlichkeit für „*eigene Inhalte*". Er bezieht sich somit auf die Content-Provider.

(a) Diensteanbieter

Was unter dem Begriff „*Diensteanbieter*" zu verstehen ist, wird in § 3 Nr. 1 TDG legal definiert. Demnach sind Diensteanbieter natürliche und juristische Personen oder Personenvereinigungen, die eigene Teledienste zur Nutzung bereithalten.[420]

(b) Inhalte

Obwohl es auf den ersten Blick seltsam erscheint, dass § 5 I TDG a.F. von „*Inhalten*", § 3 Nr. 1 TDG dagegen lediglich von „*Telediensten*" spricht, stellt dieser Unterschied kein Problem dar. Denn aufgrund der Definition des Teledienstes in § 2 I TDG sind diese Begriffe weitgehend als synonym anzusehen.[421] Zwar wird der Rechtsbegriff „Inhalte" weder im TDG noch im MDStV oder auch in den Begründungen zum IuKDG näher bestimmt.[422] Allerdings muss er mangels ausdrücklicher Einschränkung in weiter, schutzzweckorientierter Auslegung Informationen jeglicher Art in Schrift, Bild und/oder Ton umfassen.[423] Diese Definition deckt sich im Grunde mit der aus § 2 I TDG.[424]

---

417 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 6.

418 Die Anwendungsbereiche der ersten drei Absätze für die in § 3 Nr. 1 TDG definierten Anbieter schließen dabei lückenlos aneinander an, so dass für eine etwaige Abgrenzung der einzelnen Absätze auf die jeweils anderen zurückgegriffen werden kann. Vgl. Freytag, „Urheberrechtliche Haftung im Netz", ZUM 1999, 185, 191 f.

419 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 7; so auch die amtliche Begründung in Bundestag-Drucksache 13/7385 zu Art. 1 § 5 I IuKDG, S. 19.

420 Hoeren, Rechtsfragen des Internet, S. 127 f. Rdnr. 298.

421 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 163.

422 Waldenberger, „Teledienste, Mediendienste und die „Verantwortlichkeit" ihrer Anbieter", MMR 1998, 124, 126.

423 Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen", CR 1997, 193, 196; a.A. dagegen Waldenberger in „Teledienste, Mediendienste und die „Verantwortlichkeit" ihrer Anbieter", MMR 1998, 124, 126 f. der eine enge Auslegung des Begriffs „Inhalte" befürwortet. Dies ist jedoch schon deshalb abzulehnen, da dieser Ansicht § 2 I TDG entgegensteht. Außerdem sollen von

(c) Bereithalten von eigenen Inhalten

Ein Bereithalten von Telediensten wird zunächst gemäß den Begründungen zum TDG a.F. nach einer tatsächlichen Betrachtungsweise definiert. Als „Bereithalten" wird demnach jedes „Einstellen in das Angebot" des Diensteanbieters verstanden.[425] Damit ist die Speicherung durch den Anbieter auf seinem eigenem Rechner zum Abruf durch Dritte gemeint.[426] Darüber hinaus verlangt die Literatur noch weitere Kriterien, die sie vor allem im Rahmen von § 5 II TDG a.F. für den Begriff „Bereithalten" in Abgrenzung zur „Zugangsvermittlung" aufgestellt hat.[427] Da sowohl § 5 I als auch II TDG a.F. von „*bereithalten*" sprechen und es nicht ersichtlich ist, warum diese Begriffe unterschiedlich behandelt werden sollen, müssen diese Gedanken ebenfalls auf § 5 I TDG a.F. übertragen werden. Deshalb ist für ein Bereithalten zudem notwendig, dass der Diensteanbieter die zur Nutzung bereitgehaltenen Dienste für eine gewisse Dauer auf eigenen Servern so speichert, dass sie eigenständig wirtschaftlich nutzbar sind.[428] Nicht bereitgehalten werden deshalb Daten, die während des Transportvorgangs nur für äußerst kurze Zeit auf Routern oder Gateways zwischengespeichert werden. Gleichfalls wird vom Begriff Bereithalten und somit von § 5 I TDG a.F. – wie ein Blick in § 5 III 2 TDG a.F. zeigt – die Zwischenspeicherung von Inhalten mittels Proxy-Cache-Speicher nicht erfasst. Hier ist § 5 III 2 TDG a.F. als lex specialis vorrangig. Darüber hinaus versteht die Literatur unter Bereithalten nach einer rechtlichen Betrachtungsweise die rechtliche Verfügungsgewalt über einen bestimmten Inhalt. Der Diensteanbieter hält demnach dann Daten i.S.d. § 5 I TDG a.F. bereit, wenn er die Herrschaft über die einzelnen gespeicherten Daten hinsichtlich einer Löschungs- oder Sperrungsmöglichkeit der einzelnen Inhalte besitzt.[429]

Der Diensteanbieter hält also regelmäßig „eigene Inhalte" im Netz bereit, falls er die Inhalte selbst geschaffen hat oder fremd erstellte Inhalte so übernimmt, dass er aus der Sicht eines objektiven Nutzers für sie die Verantwortung übernehmen will.[430] Letzteres

---

diesem Gesetz verschiedene Sachverhalte erfasst werden, das eine restriktive Auslegung der Inhalte vereiteln würde.

424 Freytag, Haftung im Netz, S. 159 f.

425 Bundestag-Drucksache 13/7385 vom 09.04.1997 zu Art. 1 § 5 II IuKDG, S. 20.

426 Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG", MMR 1998, 79, 87.

427 Gercke, „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks", ZUM 2001, 34, 36 ff.; Bergmann, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, S. 64 ff.

428 Sieber, Verantwortlichkeit im Netz, S. 158 Rdnr. 317; Pelz, „Die strafrechtliche Verantwortlichkeit von Internet-Providern", ZUM 1998, 530, 533; Vassilaki, „Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG", MMR 1998, 630, 632 f.

429 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 165; Sieber in seinen Anmerkungen zum CompuServe-Urteil des AG-München, MMR 1998, 438, 441.

430 Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien", NJW 1997, 3193, 3196.

ist dann zu bejahen, wenn sich der Anbieter die fremden Inhalte so zu eigen macht,[431] dass er sich diese Inhalte als seine eigenen i.S.v. § 5 I TDG a.F. zurechnen lassen muss.[432]

(d) Rechtsfolgen

Gemäß § 5 I TDG a.F. haftet der Anbieter eigener Inhalte nach den „*allgemeinen Gesetzen*". Unter diesen Rechtsbegriff sind nicht die allgemeinen Gesetze i.S.d. Art. 5 II GG zu verstehen, sondern die allgemeinen Haftungs- und Verantwortlichkeitsregeln aller Rechtsgebiete.[433] Es wurde oben schon ausführlich darauf hingewiesen, dass es heftigen Streit darüber gibt, ob der Verweis auf die allgemeinen Gesetze eher weit zu verstehen ist, so dass sämtliche Rechtsgebiete hiervon erfasst werden, oder eher eng, so dass er nur für zivil- und strafrechtliche Vorschriften gilt.[434] Da der § 5 I TDG a.F. jedoch keinerlei Unterscheidungen trifft, welche „*allgemeinen Gesetze*" zur Anwendung kommen sollen, sondern gerade zum Ziel hat, sämtliche Rechtsordnungen zu erfassen, muss er weit ausgelegt werden.[435]

(3) Bereithalten fremder Inhalte gemäß § 5 II TDG a.F.

Gemäß § 5 II TDG a.F. sind Diensteanbieter „*für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern*". § 5 II TDG a.F. soll den Fall regeln, dass der Diensteanbieter fremde Inhalte in sein Angebot aufnimmt. Diese Vorschrift bezieht sich somit auf den Service-Provider. Grundsätzlich bleibt es hier ebenfalls bei der Verantwortung des Urhebers für diese Inhalte.[436] Allerdings soll nach § 5 II TDG a.F. den Anbieter, der fremde Inhalte auf seinem Rechner speichert, eine Mitverantwortung für diese Inhalte treffen.[437] Er ist bei Kenntnis des betreffenden Inhalts dazu verpflichtet, Sperr- und Löschungsmaßnahmen zu ergreifen.[438] Diese Verpflichtung wird aber dadurch eingeschränkt, dass sie ihm nur dann auf-

---

431 Der Diensteanbieter macht sich dann fremde Inhalte zu eigen, wenn er diese Inhalte in den von ihm selbst verantworteten Angebotsbereich übernimmt, ohne sie als von Dritten stammend zu kennzeichnen, Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen", CR 1997, 193, 197.

432 Vgl. Bundestag-Drucksache 13/7385 zu Art. 1 § 5 IuKDG, S. 19 f.; AG-München in seinem CompuServe-Urteil vom 28.05.1998, MMR 1998, 429, 435; hierzu auch ausführlich Sieber, Verantwortlichkeit im Internet, S. 145 ff. Rdnr. 290 ff.

433 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks", CR 1998, 351, 354; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 175.

434 Vgl. oben unter B. 2. Teil. II. 5. b. aa.

435 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 9 m. w. N.

436 Gounalakis, „Der Mediendienste-Staatsvertrag der Länder", NJW 1997, 2993, 2995; dabei behandelt Gounalakis zwar den § 5 II MDStV. Da die Wortlaute von § 5 II TDG a.F. sowie MDStV identisch sind, trifft die an dieser Stelle gemachte Aussage auch auf § 5 II TDG a.F. zu.

437 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 15; Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer", ZUM 1997, 231, 235.

438 Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien", NJW 1997, 3193, 3196.

erlegt werden kann, wenn ihm eine Verhinderung der Nutzung bestimmter Inhalte technisch möglich und zumutbar ist.[439]

(a) Fremde Inhalte

Diesbezüglich kann auf die Definition zu den „*eigenen Inhalten*“ i.S.d. § 5 I TDG a.F. verwiesen werden.[440] Alles, was nicht unter die eigenen Inhalte fällt, stellt fremde Inhalte dar. Demnach sind Inhalte fremd, wenn sie – für den Nutzer erkennbar – nicht vom Anbieter stammen.[441] Ebenso sind alle sonstigen Inhalte als fremd anzusehen, die der Anbieter nur bereithält, also selbst weder erstellt noch beschafft.[442]

(b) Kenntnis

„*Kenntnis*“ bedeutet schon allein aufgrund des Wortlauts nicht nur „kennen können“ oder „kennen müssen“.[443] Vielmehr ist hierunter einzig und allein die positive Kenntnis zu verstehen.[444] Ziel und Zweck des Gesetzgebers war es, durch die Haftungsprivilegierung des § 5 II TDG a.F. den Service-Provider von einer aktiven Kontrollpflicht seiner angebotenen fremden Inhalte zu befreien.[445]

Fraglich und umstritten ist allerdings, ob zur Erfüllung des Tatbestandsmerkmals der Kenntnis auch das Bewusstsein der Rechtswidrigkeit erforderlich ist.[446] Dieser Gedanke ist jedoch abzulehnen:[447] Zum einen enthält der Wortlaut des § 5 II TDG a.F. keine Anhaltspunkte für eine derartige Interpretation des Kenntnisbegriffs. Zum anderen würden die Provider zu sehr geschützt werden, so dass eine Verantwortlichkeit nur in den sel-

---

439 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 15.

440 Vgl. hierzu oben unter B. 2. Teil. II. 5. b. cc. (2). (c).

441 von Bonin/Köster, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821, 823.

442 Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 198.

443 Pichler, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, MMR 1998, 79, 87.

444 Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte“, ZUM 2000, 1007; Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien“, NJW 1997, 3193, 3196; dazu ausführlich auch Pankoke, Von der Presse zur Providerhaftung, S. 178.

445 Sieber, Verantwortlichkeit im Internet, S. 167 Rdnr. 336; besonders deutlich ist diese Zielsetzung auch im Evaluierungsbericht der Bundesregierung, vgl. Bundestag-Drucksache 14/1191 vom 18.06.1999, S. 10 formuliert worden:
„Die Vorschriften dienen dazu, dem Gedanken der Unzumutbarkeit einer Providerkontrolle Ausdruck zu verleihen und so Rechtssicherheit für die Anbieter zu schaffen.“
Die E-Commerce-Richtlinie, Richtlinie 2000/31/EG, bringt diesen Ausschluss von Kontrollpflichten der Provider in einem gesonderten Artikel noch klarer zum Ausdruck: Nach Art. 15 ECRL legen die Mitgliedstaaten den Diensteanbietern „keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen“.

446 So andeutungsweise Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 667, der von einer „“Kenntnis“ von rechtswidrigen Inhalten“ spricht. Auch die E-Commerce-Richtlinie verlangt in Art. 14 ECRL positive Kenntnis von der Rechtswidrigkeit.

447 Vgl. Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 349; Wimmer/Kleineidam/Zang, „Die Verantwortlichkeit für die Verletzung von Urheberrechten im Internet“, K&R 2001, 456, 461.

tensten Fällen bejaht werden könnte. Die Frage nach dem Bewusstsein der Rechtswidrigkeit wird damit nicht für die Feststellung der grundsätzlichen Verantwortlichkeit i.S.d. § 5 TDG a.F. relevant, sondern erst für die nachgeschaltete Prüfung der allgemeinen Gesetze.[448]

Des weiteren ist es für § 5 II TDG a.F. irrelevant, wodurch der Diensteanbieter die Kenntnis erlangt hat. So reicht es aus, wenn er durch einen behördlichen Hinweis[449] oder Bericht in einer Fachzeitschrift über einen entsprechenden Inhalt in Kenntnis gesetzt wurde. Voraussetzung für die Kenntnis von Tatsachen hinsichtlich rechtswidriger Inhalte ist aber, dass der Diensteanbieter auf konkrete Inhalte hingewiesen worden ist.[450]

(c) Verhinderung der Nutzung

Im Gegensatz zu § 5 IV TDG a.F., der lediglich von einer Nutzungssperrung spricht, enthält § 5 II TDG a.F. die allgemeinere Version der Nutzungsverhinderung. Da bei § 5 II TDG a.F. der Diensteanbieter nicht nur den Zugang vermittelt, sondern den fremden Inhalt selbst in seinem Speicher bereithält, muss der Begriff der Nutzungsverhinderung weit ausgelegt werden.[451] Gemeint sind demnach alle erdenklichen Maßnahmen, die die Nutzung von rechtswidrigen Inhalten verhindern können. Hauptsächlich kommt das Sperren des Zugriffs auf den betreffenden Inhalt oder das Löschen dieser bereitgehaltenen Daten auf dem Server des Service-Providers in Frage.[452] Aber auch präventive Maßnahmen sind denkbar. So könnte dem Diensteanbieter in naher Zukunft auferlegt werden, sich technisch machbare und zumutbare Filtersysteme anzuschaffen, um rechtswidrige Inhalte von vornherein abzuwehren.

(d) Technische Möglichkeiten und Zumutbarkeit

Diese beiden Begriffe können nicht getrennt von einander betrachtet werden. Denn technisch unmögliche Maßnahmen sind stets unzumutbar. Häufig beinhaltet die Zumutbarkeit auch die technische Möglichkeit.[453] Deshalb ist die Zumutbarkeit der eigentliche Prüfungspunkt,[454] wobei sie ebenfalls in technischer Hinsicht zu betrachten ist. Dies wird durch den Wortlaut des § 5 II TDG a.F. hervorgehoben.

Die Bundesregierung versteht unter dem Begriff „Zumutbarkeit" i.S.d. § 5 II TDG a.F. primär die Verhältnismäßigkeit des zur Sperrung bzw. Löschung von rechtswidrigen

---

448 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 19.

449 Dieses Prinzip wird „notice-and-take-down-Verfahren" genannt. Die Behörde setzt den Service-Provider von rechtswidrigen Inhalten in Kenntnis. Dadurch wird er dazu gezwungen den Inhalt zu löschen.

450 Freytag, Haftung im Netz, S. 182 f.; Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)", CR 1997, 653, 667.

451 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 192.

452 Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 25.

453 Sieber, Verantwortlichkeit im Internet, S. 176 ff. Rdnr. 358 ff.

454 Freytag, Haftung im Netz, S. 187.

Inhalten zu betreibenden technischen Aufwands.[455] Demnach soll eine Abwägung zwischen dem zu erwartenden Umfang der Sperrung, dem damit verbundenen wirtschaftlichen Nachteil für den Teledienst und der Schwere der Rechtsbeeinträchtigung durch den betreffenden Inhalt stattfinden.[456] Der Bundesrat vertritt im Grunde dieselbe Ansicht, was die Auslegung des Zumutbarkeitsbegriffs anbelangt. Allerdings will er von vornherein festgelegt haben, dass an die Zumutbarkeit keine hohen Anforderungen zu stellen sind. Eine Unzumutbarkeit soll deshalb nur in extremen Ausnahmefällen bejaht werden dürfen.[457] Letztendlich muss bei der Frage der Zumutbarkeit eine umfassende Interessenabwägung durchgeführt werden, die nicht abstrakt, sondern lediglich für jeden Fall einzeln erfolgen darf. Dabei müssen sämtliche relevanten Gesichtspunkte berücksichtigt werden, indem die tangierten Rechtsgüter miteinander verglichen werden.[458]
Bei einem Vergleich des § 5 II TDG a.F. mit § 5 IV TDG a.F. fällt auf, dass der Gesetzgeber dem § 5 II TDG a.F. das Wort „*ihnen*“ beigefügt hat. Hierdurch wollte der Gesetzgeber deutlich machen, dass sich die Kriterien der Zumutbarkeit hauptsächlich aus besonderen Umständen in der Person des Diensteanbieters ergeben sollen. Dies muss bei der Interessenabwägung in § 5 II TDG a.F. ebenfalls Berücksichtigung finden.
Da von § 5 II TDG a.F. das Bereithalten fremder Inhalte durch den Anbieter geregelt wird und somit der Service-Provider Herrschaftsgewalt über die von ihm gespeicherten fremden Daten besitzt, kann er ohne großen Aufwand bei Kenntnis rechtswidriger Inhalte diese in der Regel mit Hilfe der vorhandenen Standard-Software sperren oder löschen.[459]
Probleme der Zumutbarkeit stellen sich bei § 5 II TDG a.F. also nicht im Hinblick auf technische, sondern auf rechtliche und organisatorische Aspekte. So bereitet in manchen Fällen bereits die Frage, ob überhaupt ein rechtswidriger Inhalt gegeben ist, erhebliche Probleme.[460] Auch die Situation, dass der Service-Provider mit einer Vielzahl von Meldungen über rechtswidrige Inhalte überhäuft wird, kann zu Schwierigkeiten führen. Dann sollte dem Diensteanbieter eine gewisse Zeit zur Überprüfung eingeräumt werden, bevor eine Löschung oder Sperrung als für ihn zumutbar angesehen werden kann.[461]

---

455 Bundestag-Drucksache 13/7385 vom 09.04.1997 zu Art. 1 § 5 IuKDG, S. 20.

456 Zu Fragen der Zumutbarkeit und den maßgeblichen Abwägungskriterien im Internet vgl. die ausführlichen Darstellungen bei Sieber, Verantwortlichkeit im Internet, S. 199 ff. Rdnr. 399 ff bzw. S. 206 ff. Rdnr. 409 ff.

457 Vgl. hierzu die Stellungnahme des Bundesrats in Bundestag-Drucksache 13/7385 vom 09.04.1997 zu Art. 1 § 5 IuKDG, S. 51; als Beispiel für einen derartigen Extremfall nennt der BR die Situation, dass die Nutzung eines bestimmten Inhalts nur durch die vollständige Einstellung eines (im übrigen unbedenklichen) Teledienstes verhindert werden kann.

458 Sieber, Verantwortlichkeit im Internet, S. 205 Rdnr. 407 f.

459 von Bonin/Köster, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821, 825; Sieber, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653, 655.

460 Zu denken ist hier vor allem an Urheberrechtsverletzungen.

461 Sieber, Verantwortlichkeit im Internet, S. 177 f. Rdnr. 359 ff.

(4) Zugangsvermittlung zu fremden Inhalten gemäß § 5 III TDG a.F.

Gemäß § 5 III TDG a.F. sind Diensteanbieter „*für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung*“.

Ermöglicht ein Diensteanbieter Zugang zu fremden Anbieterleistungen, ohne sie selbst bereitzuhalten, soll er für diese vermittelten Inhalte gemäß § 5 III 1 TDG a.F. grundsätzlich nicht verantwortlich sein. § 5 III 1 TDG a.F. regelt demnach die Verantwortlichkeit des Access-Providers.[462] Der Proxy-Cache-Server[463] wird über § 5 III 2 TDG a.F. dem Access-Provider im Hinblick auf seine Verantwortlichkeit gleichgestellt.

Handelt es sich im konkreten Haftungsfall um eine Zugangsvermittlung i.S.d. § 5 III 1 TDG a.F., ist eine Verantwortlichkeit des Anbieters regelmäßig ausgeschlossen.

(a) Zugangsvermittlung i.S.d. § 5 III 1 TDG a.F.

Die „Zugangsvermittlung“ nach § 5 III 1 TDG a.F. ist von dem „Bereithalten“ des § 5 I und II TDG a.F. abzugrenzen. Dabei kann die Definition des Bereithaltens zur Hilfe genommen werden.[464] Demnach ist unter der Zugangsvermittlung i.S.d. § 5 III 1 TDG a.F. die Übermittlung von Daten zu verstehen, die nicht im eigenen Verfügungsbereich des Diensteanbieters abgespeichert werden.[465] Der Access-Provider hält also keine Inhalte bereit, sondern vermittelt lediglich den Zugang zu diesen. Gerade durch das Wort „*lediglich*“ in § 5 III 1 TDG a.F. macht der Gesetzgeber deutlich, dass alles, was über die Zugangsvermittlung hinausgeht, schon als Bereithalten i.S.d. § 5 I bzw. II TDG a.F. anzusehen ist.[466] Die Zugangsvermittlung erfasst daher einzig und allein die rein technische Telekommunikationsdienstleistung der Datenübertragung. Nur insoweit soll nach dem Willen des Gesetzgebers die Haftungsprivilegierung des § 5 III TDG a.F. gelten.[467]

(b) Proxy-Cache-Server nach § 5 III 2 TDG a.F.

Die Fiktion des § 5 III 2 TDG a.F. bestimmt, dass selbst kurze Zwischenspeicherungen im Rahmen des Proxy-Cache-Verfahrens, die grundsätzlich als Bereithalten i.S.d. § 5 I und II TDG a.F. anzusehen wären, noch der Zugangsvermittlung zuzurechnen sind.

---

462 So die h.M. wie beispielsweise Freytag in: Haftung im Netz, S.171. Manche Meinungen in der Literatur wollen § 5 III 1 TDG a.F. weit auslegen und ihn nicht nur auf den Access-Provider sondern auch auf Suchmaschinen und Hyperlinks anwenden (vgl. hierzu oben bei B. 2. Teil. II. 5. b. cc. (6).).

463 Proxy-Cache-Server sind – wie bereits oben unter B. 1. Teil. I. 4. a. erwähnt – spezielle Anwendungsprogramme, die meist auf einem separaten Computersystem eingesetzt werden, um fremde Inhalte kurzfristig und automatisch zum Zwecke der vereinfachten Weiterleitung zwischenzuspeichern.

464 Vgl. oben unter B. 2. Teil. II. 5. b. cc. (2). (c).

465 Vgl. hierzu die Formulierung des Vorentwurfs des Bundesforschungsministeriums für das IuKDG vom 07.06.1996 nach welcher der entsprechende Access-Provider „die Daten lediglich zur Nutzung übermittelt, ohne sie im eigenen Verfügungsbereich abzuspeichern“.

466 Sieber, Verantwortlichkeit im Internet, S. 180 Rdnr. 366.

467 Freytag, Haftung im Netz, S. 171.

Denn eine Überprüfung dieser Daten auf dem Proxy-Cache-Server ist ebenso wenig möglich wie während der Datenübertragung bei einer Zugangsvermittlung.
Problematisch ist jedoch der unbestimmte Rechtsbegriff der „*kurzzeitigen Vorhaltung*“ von fremden Inhalten i.S.d. § 5 III 2 TDG a.F.. So wird aus dem Gesetzestext nicht deutlich, was mit einer kurzzeitigen Vorhaltung gemeint ist. Die Gesetzesbegründung geht davon aus, dass die gespeicherten fremden Inhalte „mit zunehmender Verweildauer unter den Tatbestand des Absatzes 2 fallen. Wegen der Verbindung zu den Fällen des Absatzes 2 ist hier aber nur ein Zeitraum von wenigen Stunden, nicht von Tagen gemeint.“[468] Diese zeitliche Abgrenzung des Gesetzgebers beinhaltet jedoch aufgrund der dem Proxy-Cache-Server immanenten Technik gewisse Schwierigkeiten. Denn die Speicherdauer von Daten auf Proxy-Cache-Servern wird regelmäßig nicht durch festgelegte Zeitintervalle, sondern von der jeweiligen Speicherkapazität bestimmt. Ist der Speicher des Proxy-Cache-Servers voll, so wird automatisch die älteste Datei durch die jüngere ersetzt. Häufig abgerufene Daten sind in der Regel über längere Zeit im Proxy-Cache-Server gespeichert.[469] Der Begriff der Kurzzeitigkeit muss deshalb in derartigen Fällen flexibel angewendet werden, damit diese Daten auch noch von ihm erfasst werden können.

(5) Verpflichtung zur Sperrung gemäß § 5 IV TDG a.F.

§ 5 IV TDG a.F. besagt, dass „*Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen*“ unberührt bleiben, „*wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist*“.
Es wurde bereits angedeutet, dass der § 5 IV TDG a.F. im Vergleich zu § 5 I bis III TDG a.F. aus dem Rahmen fällt. So regelt § 5 I bis III TDG a.F. in stufenweiser Abfolge, wann ein Diensteanbieter für gewisse Inhalte verantwortlich ist. § 5 IV TDG a.F. spricht dagegen von einer „*Verpflichtung zur Sperrung*“. Es stellt sich somit die Frage, wie der § 5 IV TDG a.F. rechtlich in die Struktur des § 5 TDG a.F. einzuordnen ist. Dies ist nicht unumstritten:[470]

(a) Rechtliche Qualifizierung des § 5 IV TDG a.F.

Hauptstreitpunkt bei § 5 IV TDG a.F. ist die Frage, was mit dem Begriff „*Diensteanbieter*“ gemeint ist und worauf er sich beziehen soll.[471] So kann einerseits die Meinung vertreten werden, dass § 5 IV TDG a.F. auf alle vorangegangenen Absätze des § 5 TDG

---

468 Bundestag-Drucksache 13/7385 vom 09.04.1997 zu Art. 1 § 5 IuKDG, S. 20.
469 Sieber, Verantwortlichkeit im Internet, S. 186 Rdnr. 378.
470 Ein ausführlicher Versuch, den § 5 IV TDG a.F. grammatikalisch sowie nach Sinn und Zweck in die Struktur des § 5 TDG a.F. einzugliedern, findet sich bei Koenig/Loetz in „Sperrungsanordnungen gegenüber Network- und Access-Providern", CR 1997, 438, 440 ff.
471 Müller-Using/Lücke, „Neues Recht für Multimedia-Dienste“, ArchivPT 1997, 101, 107.

a.F. Bezug nimmt, da § 5 IV TDG a.F. keine Unterscheidung trifft.[472] Auch die Tatsache, dass § 5 IV TDG a.F. lediglich von „*rechtswidrigen Inhalten*“ spricht, also nicht zwischen eigenen und fremden Inhalten differenziert, lässt eigentlich den Schluss zu, dass er sich auch auf die Diensteanbieter aus § 5 I und II TDG a.F. beziehen will.[473] Andererseits könnte nach der missverständlichen Gesetzesbegründung[474] ebenfalls angenommen werden, dass § 5 IV TDG a.F. für alle Formen des Bereithaltens und Zugangsvermittelns von Inhalten i.S.d. § 5 I bis III TDG a.F. gelten soll.[475] Diese Ansicht, die einen umfassenden Anwendungsbereich von § 5 IV TDG a.F. bejaht, führt zu unzutreffenden Ergebnissen und zahlreichen Wertungswidersprüchen: Wird beispielsweise die allgemeine Verantwortlichkeitsregelung des § 5 I TDG a.F. durch eine Anwendung des § 5 IV TDG a.F. eingeschränkt, so kommt es zu einer nicht zu begründenden Besserstellung der Anbieter eigener Inhalte, wenn diese ihre Inhalte online und nicht offline verbreiten. Dies kann der Gesetzgeber, wie sich klar aus dem abschließenden Wortlaut des § 5 I TDG a.F. ergibt, so nicht gewollt haben. Folglich muss diese Meinung abgelehnt werden.

Für die richtige Einordnung des § 5 IV TDG a.F. innerhalb der Gesamtregelung von § 5 TDG a.F. ist die Entstehungsgeschichte zu betrachten: Hieraus ergibt sich, dass § 5 IV TDG a.F. erst im Laufe der Beratungen von Bund und Ländern auf Wunsch der Länder ergänzend in den Regierungsentwurf aufgenommen und so auch vom Parlament verabschiedet wurde.[476] Der Grund für die – ursprünglich nicht geplante – Aufnahme des § 5 IV TDG a.F. in § 5 TDG a.F. bestand darin, dass die Länder ohne § 5 IV TDG a.F. den sehr weit gehenden Verantwortlichkeitsausschluss des Zugangsvermittlers nach § 5 III TDG a.F. so nicht akzeptiert hätten. Durch § 5 IV TDG a.F. sollte die Möglichkeit geschaffen werden, trotz der Haftungsfreistellung des Zugangsvermittlers durch § 5 III TDG a.F. in manchen Fällen doch verschuldensunabhängige Unterlassungs- und Beseitigungsansprüche sowie verwaltungsrechtliche Anordnungen gegen den Zugangsvermittler durchsetzen zu können.[477] Vor diesem Hintergrund kam es deshalb zur Einführung von § 5 IV TDG a.F.. Hiermit war einzig und allein beabsichtigt worden, die Verantwortlichkeit der Zugangsvermittlung zu verschärfen. Als weiteres Indiz dafür, dass

---

472 So Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 TDG Rdnr. 38. Sie vertreten die Ansicht, dass § 5 IV TDG a.F. eine verschuldensunabhängige Verantwortlichkeit der Diensteanbieter regelt. Deshalb soll sich nach § 5 IV TDG a.F. auch dann eine Sperrungsverpflichtung der Diensteanbieter ergeben, wenn sie keine Verantwortlichkeit nach den Abs. I bis III ergibt. Vgl. auch: von Bonin/Köster, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821, 826.

473 So Spindler in „Störerhaftung im Internet“, K&R 1998, 177, 177 f.

474 Vgl. Bundestag-Drucksache 13/7385 vom 09.04.1997 zu Art. 1 § 5 IuKDG , S. 20 f. bzw. Bundesrat-Drucksache 966/96 vom 20.12.1996, S. 22 f. Dort wird von „allen Diensteangeboten“ gesprochen.

475 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231, 236.

476 Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984.

477 Sieber, Verantwortlichkeit im Internet, S. 188 Rdnr. 381.

sich § 5 IV a.F. nur auf § 5 III TDG a.F. beziehen soll, ist der Wortlaut des § 5 IV TDG a.F., der von einer „*Verpflichtung zur Sperrung*“ spricht. Eine Sperrung macht aber nur für den Anwendungsfall des § 5 III TDG a.F. Sinn. Denn das einzige Mittel gegen rechtswidrige fremde Inhalte, zu denen der Access-Provider den Zugang vermittelt, stellt die Sperrung dar. Mangels Herrschaftsgewalt seitens des Access-Providers kommt eine Löschung der Inhalte auf fremden Rechnern nicht in Betracht. Folglich kann sich § 5 IV TDG a.F. ausschließlich auf § 5 III TDG a.F. beziehen. Die in § 5 I und II TDG a.F. genannten Diensteanbieter bleiben von § 5 IV TDG a.F. dagegen unberührt.[478] Zwischen § 5 IV und III TDG a.F. besteht somit ein Regel-Ausnahme-Verhältnis.[479]

(b) Umfasste Tatbestände: „Allgemeine Gesetze“

§ 5 IV TDG a.F. enthält wie § 5 I TDG a.F. den Begriff „*allgemeine Gesetze*“. Grundsätzlich muss dieser Begriff gleichermaßen definiert werden, da er in derselben Norm benutzt wird. Allerdings wird er in einem anderen Zusammenhang verwendet. So besagt § 5 IV TDG a.F., dass die „*Verpflichtung zur Sperrung [...] nach den allgemeinen Gesetzen*“ unberührt bleiben soll. Es stellt sich somit die Frage, nach welchen allgemeinen Gesetzen eine Sperrverpflichtung ausgesprochen werden kann:
Allgemein anerkannt ist, dass sich eine Verpflichtung zur Sperrung aus Verwaltungs- und Zivilrecht ergeben kann. Umstritten ist allerdings, ob das Strafrecht ebenfalls eine Sperrungsanordnung begründet. Dies wird nach ganz herrschender Meinung abgelehnt.[480] Denn § 5 IV TDG a.F. regelt grundsätzlich nur verschuldensunabhängige Tatbestände, beispielsweise in Form von zivilrechtlichen Unterlassungsansprüchen oder aus dem Polizei- und Ordnungsrecht. Er will klar machen, dass diese verschuldensunabhängigen Tatbestände weiterbestehen sollen, wenn eine anderweitige Verantwortlichkeit im Zivil- oder Strafrecht wegen § 5 III TDG a.F. gerade nicht vorliegt.[481] Des-

---

478 So auch Bleisteiner in: Rechtliche Verantwortlichkeit im Internet, S. 204 f.; Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981, 2984; Im Ergebnis wohl auch Moritz, „§ 5 TDG im deutschen Recht – die wissenschaftliche Diskussion ist eröffnet“, MMR 1998, 625, 626.
Eine völlig konträre Meinung vertreten im übrigen Koenig/Loetz in „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1997, 438, 442. Sie sind der Ansicht, dass aufgrund einer systematisch-teleologischen Auslegung des § 5 TDG a.F. den Access-Provider keine Sperrverpflichtung nach § 5 IV TDG a.F. treffen kann. Die hierfür vorgebrachte Begründung, dass § 5 IV TDG a.F. nur auf eine „Sperrung der Nutzung“ und nicht auf eine „ Sperrung des Zugangs zur Nutzung“ gerichtet ist, kann nicht überzeugen. Schon allein die Tatsache, dass sich § 5 IV TDG a.F. wegen seiner Position auch auf Art. 5 III TDG a.F. beziehen muss (ansonsten hätte der Gesetzgeber die Abs. IV und III vertauscht), spricht gegen die von Koenig/Loetz angeführte Ansicht.

479 Sieber, Verantwortlichkeit im Internet, S. 189 Rdnr. 382.

480 Eichler, Tagungsberichte zur Bekämpfung der Kriminalität im Internet, CR 1999, 200, 202; Bröhl, „Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste“, CR 1997, 73, 75; Moritz, „§ 5 TDG im deutschen Recht – die wissenschaftliche Diskussion ist eröffnet“, MMR 1998, 625, 626; Freytag, Haftung im Netz, S. 224; Anmerkungen von Hoeren in: Begründungen des Generalbundesanwalt zur Haftung eines Access-Providers für rechtswidrigen Inhalt in der Einstellungsverfügung vom 26.11.1997, Az.: 2 BJs 104/96-4, MMR 1998, 93, 97 f.

481 Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 205.

halb wird hieraus der Schluss gezogen, dass § 5 IV TDG a.F. auf verschuldensabhängige Normen, wie etwa die Strafvorschriften, keine Anwendung finden kann. Abzulehnen ist deshalb die Gegenansicht[482], dass in den Strafnormen[483] – neben der Rechtsfolge der Strafbarkeit – auch eine allgemeine Sperrverpflichtung i.S.d. § 5 IV TDG a.F. zu finden ist.[484] Folglich muss der Verweis auf die „*allgemeinen Gesetze*" in § 5 IV TDG a.F. so verstanden werden, dass eine zivil- oder verwaltungsrechtliche Verfügung nur mit entsprechenden zivil- und verwaltungsrechtlichen Zwangsmitteln, nicht jedoch durch Drohungen im Hinblick auf eine ansonsten bestehende strafrechtliche Verantwortlichkeit durchgesetzt werden kann.[485]

(c) Rechtsfolge: Verpflichtung zur „Sperrung"

Zwar spricht § 5 IV TDG a.F. von einer Verpflichtung zur Sperrung. Durch den Zusatz „*nach den allgemeinen Gesetzen*" wird jedoch deutlich, dass § 5 IV TDG a.F. keine eigenständige Rechtsgrundlage darstellt, die den jeweils zuständigen Behörden eine Eingriffsbefugnis erteilt.[486] Vielmehr besitzt auch § 5 IV TDG a.F. – wie die übrigen Absätze des § 5 TDG a.F. – lediglich eine Filterfunktion.[487] Denn obwohl im Wortlaut von § 5 IV TDG a.F. der Begriff „Verantwortlichkeit" fehlt, regelt auch er das rechtliche Einstehenmüssen in Form einer Verpflichtung zur Sperrung.[488] Folglich muss er gleichermaßen wie die übrigen Absätze des § 5 TDG a.F. angewendet werden. Erst wenn § 5 IV TDG a.F. erfüllt ist, kann die jeweilige Norm, auf die die Sperranordnung gestützt wird, geprüft werden.

Des weiteren ist im Rahmen von § 5 IV TDG a.F. problematisch, ob getreu seinem Wortlaut nur Sperrmaßnahmen oder auch andere Formen der Unterlassung sowie Beseitigung der Störung von ihm erfasst sind. Diese Frage ist eine Folge der vorbeschriebenen unterschiedlichen Anwendung des § 5 IV TDG a.F. auf den Rest der Norm.[489] Denn je nachdem, auf welche Absätze des § 5 TDG a.F. sich der § 5 IV TDG a.F. zu beziehen ist, kommen unterschiedliche Möglichkeiten in Betracht, wie die Sperrung der Nutzung rechtswidriger Inhalte erreicht werden kann.[490] Da sich der § 5 IV TDG a.F. lediglich

---

482 Begründungen des Generalbundesanwalt zur Haftung eines Access-Providers für rechtswidrigen Inhalt in der Einstellungsverfügung vom 26.11.1997, Az.: 2 BJs 104/96-4, mit Anmerkungen von Hoeren, MMR 1998, 93, 95.

483 Zu nennen sind in diesem Zusammenhang vor allem die §§ 86a, 140 und 184 StGB.

484 Freytag, Haftung im Netz, S. 224 Fn. 631.

485 Es ist daher eindeutig rechtswidrig, wenn Ermittlungs- oder Verwaltungsbehörden Zugangssperren unter Hinweis auf eine Strafbarkeit gemäß § 5 IV TDG a.F. mit der Androhung von Strafverfahren durchsetzen wollen (so geschehen beispielsweise im „CompuServe"-Urteil des AG-München vom 28.05.1998, vgl. MMR 1998, 429-438) anstelle entsprechende Verwaltungsverfahren einzuleiten.

486 Bröhl, „Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste", CR 1997, 73, 76.

487 Sieber, Verantwortlichkeit im Internet, S. 192 Rdnr. 389.

488 Freytag, Haftung im Netz, S. 147.

489 Vgl. insoweit oben unter B. 2. Teil. II. 5. b. cc. (5). (a).

490 So behauptet eine Meinung in der Literatur, dass der Gesetzgeber mit § 5 IV TDG a.F. offenbar den gesamten Bereich der verschuldensunabhängigen Störerhaftung erfassen will, wodurch die Begren-

auf § 5 III TDG a.F. bezieht, stellt die Sperrung des Zugangs von rechtswidrigen fremden Inhalten die einzige Eingriffsmöglichkeit dar.[491] Eine Löschung derartiger Inhalte kann der Access-Provider aus technischen Gründen nicht vornehmen, da ihm insoweit die Herrschaftsgewalt über den fremden Rechner fehlt. Eben dies hat der Gesetzgeber erkannt und bewusst den konkreten Wortlaut in § 5 IV TDG a.F. gewählt. Demzufolge kann mit § 5 IV TDG a.F. nur eine Sperrung angeordnet werden. Sonstige Formen der Unterlassung oder Beseitigung der Störung werden dagegen nicht erfasst.[492]

(d) Kenntnis des Inhalts, Möglichkeit und Zumutbarkeit der Sperrung

Ähnlich wie in § 5 II TDG a.F. verlangt § 5 IV TDG a.F., dass der Diensteanbieter von den Inhalten Kenntnis hat und eine Sperrung technisch möglich und zumutbar ist. Deshalb kann zum einen nach oben verwiesen werden.[493] Zum anderen gelten jedoch für § 5 IV TDG a.F. gewisse Besonderheiten:

(aa)Kenntnis des Inhalts

Im Vergleich zu § 5 II TDG a.F. will § 5 IV TDG a.F. dieses Tatbestandsmerkmal enger fassen, indem er bestimmt, dass eine Kenntnisnahme nur unter gleichzeitiger Wahrung des Fernmeldegeheimnisses nach § 85 TKG möglich ist.[494]

(bb)Möglichkeit und Zumutbarkeit der Sperrung

Bei § 5 IV TDG a.F. fehlt im Gegensatz zu § 5 II TDG a.F. das Wort „*ihnen*“. Wie oben bereits erwähnt, wollte der Gesetzgeber mit diesem eingebauten Wort in § 5 II TDG a.F. deutlich machen, dass sich die Kriterien der Zumutbarkeit hauptsächlich aus besonderen Umständen in der Person des Diensteanbieters ergeben sollen.[495] Die Tatsache, dass der Gesetzgeber in § 5 IV TDG a.F. das Wort „ihnen“ bewusst weggelassen hat, legt den

---

zung auf Verpflichtungen zur Sperrung nur als deklaratorischer Verweis auf jegliche verschuldensunabhängige Ansprüche aus Störerhaftung zu begreifen ist, z.B. auch der Löschung von inkriminierten Inhalten, vgl. Spindler, „Störerhaftung im Internet“, K&R 1998, 177, 178. Eine andere Ansicht vertritt den Standpunkt, dass im TDG a.F. keine Legaldefinition des Tatbestandmerkmals „Sperren“ zu finden ist. Dementsprechend muss § 5 IV TDG a.F. auch nicht zwingend einschränkend dahingehend ausgelegt werden, dass er ausschließlich auf Sperrung, d.h. auf Kennzeichnung des Angebots mit dem Ziel einer Einschränkung der weiteren Nutzung, gerichtete Ansprüche nicht aber auch Löschungsansprüche zuließe. Bei diesem Verständnis vom Anwendungsbereich des § 5 IV TDG a.F. soll folglich die Frage, ob im Einzelfall lediglich eine Sperrung durch den Diensteanbieter als rechtmäßige Maßnahme oder darüber hinaus weitergehende Maßnahmen wie die Löschung des fraglichen Inhalts verlangt werden können, von den Rechtsfolgen abhängen, die die anzuwendende allgemeine Vorschrift gewährt, vgl. Bleisteiner, Verantwortlichkeit im Internet, S. 208 f.
Diese eben dargestellten Ansichten sind jedoch abzulehnen. Denn da bereits an vorstehender Stelle der Meinung gefolgt wurde, dass es sich bei § 5 IV TDG a.F. nur um die Ausnahmevorschrift von § 5 III TDG a.F. handelt, besteht keine praktische Notwendigkeit, den Wortlaut des § 5 IV TDG a.F. bezüglich der Verpflichtung zur Sperrung weit auszulegen.

491 Freytag, Haftung im Netz, S. 186.

492 Sieber, Verantwortlichkeit im Internet, S. 191 Rdnr. 386.

493 Vgl. insoweit die Ausführungen unter B. 2. Teil. II. 5. b. cc. (3). (b). und (d).

494 Bleisteiner, Verantwortlichkeit im Internet, S. 209.

495 Vgl. oben unter B. 2. Teil. II. 5. b. cc. (3). (d).

Schluss nahe, dass bei der Interessenabwägung im Rahmen der Zumutbarkeit von § 5 IV TDG a.F. eine objektivierte Beurteilung durchgeführt werden muss, bei der vor allem Allgemeininteressen unmittelbar heranzuziehen sind.[496]

(6) Verantwortlichkeit für Hyperlinks

Im Rahmen von § 5 TDG a.F. ergibt sich aufgrund der für das Internet typischen Eigenschaft, mittels Hyperlinks[497] auf andere Web-Seiten verweisen zu können, eine besondere Problematik.[498] Denn in § 5 TDG a.F. ist die Verantwortlichkeit für Hyperlinks nicht geregelt worden. Deshalb wird zur Zeit heftig darüber gestritten, wie die Verantwortlichkeit bei der Einrichtung von Hyperlinks, die auf rechtswidrige Inhalte verweisen, rechtlich zu beurteilen ist.[499] So stellt sich für die Verantwortlichkeit desjenigen, der einen Link auf eine Seite mit unerwünschtem Inhalt setzt, die Frage, ob dieser die gelinkten Inhalte als eigene Inhalte zur Nutzung bereithält (§ 5 I TDG a.F.), ob er sie als fremde Inhalte zur Nutzung bereithält (§ 5 II TDG a.F.) oder ob er nur den Zugang zu ihrer Nutzung vermittelt (§ 5 III TDG a.F.):

(a) Links als Bereithalten eigener Inhalte (§ 5 I TDG a.F.)

So wird von einem Teil der Literatur und Rechtsprechung die Meinung vertreten, dass lediglich der § 5 I TDG a.F. auf Hyperlinks angewendet werden soll, da Links als Bereithalten eigener Inhalte i.S.d. § 5 I TDG a.F. anzusehen sind.[500] Diese Ansicht wird damit begründet, dass die Entstehung eines Links kein Zufallsprodukt ist. Vielmehr bezieht der Betreiber den Hyperlink willentlich und gezielt in die Home-Page-Gestaltung mit ein. Der Link wird ein Teil des eigenen Angebots, wenn sich der Anbieter den hinter dem Link stehenden Inhalt selbst inhaltlich oder technisch aneignet. Durch Eigenleistung wird also ein direkter und beabsichtigter Bezug zwischen eigener Präsentation und ursprünglich fremden Inhalten hergestellt. Der Diensteanbieter hat diesen gelinkten Inhalt folglich gemäß § 5 I TDG a.F. selbst zu verantworten. Ein Bereithalten fremder Inhalte nach § 5 II TDG a.F. kann deshalb nicht angenommen werden. Auch § 5 III TDG a.F. soll keine Anwendung finden, da sich der Einrichter von

---

496 Sieber, Verantwortlichkeit im Internet, S. 201 f. Rdnr. 404.

497 Vgl. hierzu oben unter B. 1. Teil. I. 3. g.

498 Aufgrund dieser sehr komplexen und umstritten Problematik soll auf die Einordnung der Hyperlinks in einem separaten Abschnitt und nicht im Rahmen von einem Absatz des § 5 TDG a.F. eingegangen werden.

499 Ein Überblick über den derzeitigen Meinungsstand lässt sich bei Marwitz in: „Haftung für Hyperlinks“, K&R 1998, 369 f., Eichler, Tagungsberichte, CR 1999, 200, 202 sowie Kloos, Anmerkungen zum Urteil des LG Frankfurt/M vom 27.05.1998 – Az.: 3/12 O 173/97, CR 1999, 45, 47 finden. Weitergehend: Boese, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, S. 49 ff.

500 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 354; Gabel in einem K&R-Kommentar zum Urteil des LG Düsseldorf vom 29.04.1998 – 12 O 347/97, K&R 1998, 555, 556; LG Frankfurt/M, CR 1999, 45, 46 mit ablehnender Anmerkung von Kloos.

Hyperlinks als Moderator betätigt, der selbst aktiv wird, so dass eine bloße Zugangsvermittlung nicht mehr bejaht werden kann.[501]

Gegen diese Meinung sprechen jedoch gewichtige Argumente: So wird der oben angeführten Ansicht entgegengehalten, dass § 5 I TDG a.F. schon allein deswegen auf Links nicht angewendet werden darf, weil sich beim Anklicken des Hyperlinks die Adressenzeile ändert und somit kein eigener Inhalt i.S.d. § 5 I TDG a.F. gegeben ist.[502] Zudem erfüllt ein Link nicht das Kriterium des Bereithaltens von Inhalten, das von § 5 I TDG a.F. verlangt wird, da der gelinkte Inhalt nicht permanent gespeichert wird und der Link-Einsteller keinen Einfluss auf das weitere Vorhandensein des fremden Inhalts besitzt.[503] Die Ansicht, lediglich den § 5 I TDG a.F. auf Links anzuwenden, ist im übrigen mit dem Sinn und Zweck des § 5 TDG a.F. nur schwer zu vereinbaren. Denn wenn das Setzen eines Links pauschal als ein Zueigenmachen des hinter dem Link stehenden Inhalts angenommen wird, bleibt durch diese weite Auslegung kaum noch Platz für den § 5 II TDG a.F. Falls schon einzig und allein das Setzen des Links genügt, um ein Zueigenmachen und somit einen eigenen Inhalt zu bejahen, fällt es schwer, jemals ein Bereithalten fremder Inhalte i.S.d. § 5 II TDG a.F. anzunehmen. Aufgrund der angeführten Kritikpunkte muss daher dieser Lösungsansatz abgelehnt werden.

(b) Links als Bereithalten fremder Inhalte (§ 5 II TDG a.F.)

Andere Autoren in der Literatur vertreten die Ansicht, dass auf Hyperlinks der § 5 II TDG a.F. Anwendung finden soll.[504] Als Begründung wird angeführt, dass die Privilegierung des § 5 II TDG a.F. bereits die Verbreitung fremder Inhalte erfasst, wenn und obwohl sie im Machtbereich des Anbieters gespeichert sind. Deshalb muss erst recht die Verbreitung fremder Inhalte durch einen Hyperlink von § 5 II TDG a.F. erfasst werden, die außerhalb des Machtbereichs des Anbieters gespeichert sind. Daneben besteht keine Notwendigkeit für § 5 III TDG a.F., da § 5 II TDG a.F. der Interessenlage bereits ausreichend gerecht wird, weil für die Verantwortlichkeit positive Inhaltskenntnis sowie insbesondere die Zumutbarkeit der Nutzungsverhinderung erforderlich sind. Das Unter-

---

501 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351, 354.

502 Waldenberger, „Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer Anbieter“, MMR 1998, 124, 128.

503 Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 202. Vgl. auch die Ausführungen bei B. 2. Teil. II. 5. b. cc. (2). (c).

504 Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links“, CR 1998, 545, 550 f.; von Bonin/Köster, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821, 823 ff. (die jedoch in Ausnahmefällen auch den § 5 I TDG a.F. auf Hyperlinks anwenden wollen, nämlich dann, wenn sich der Anbieter den gelinkten Inhalt zu eigen machen will); Freytag, „Urheberrechtliche Haftung im Netz“, ZUM 1999, 185, 192; Freytag, Haftung im Netz, S. 228 ff.; Waldenberger, „Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer Anbieter“, MMR 1998, 124, 128 f. (er vertritt jedoch die analoge Anwendung des § 5 II TDG a.F.).
Auch die Rechtsprechung prüft teilweise die Verantwortlichkeit für Hyperlinks anhand des § 5 II TDG a.F., vgl. hierzu den Überblick bei Schuster/Ulf, „Entwicklung des Internet- und Multimediarechts von Juli 2000 bis März 2001“, MMR-Beilage 7/2001, 1, 21 f.

halten von Links muss stets als ein Bereithalten von Inhalten zur Nutzung i.S.d. § 5 I und II TDG a.F. angesehen werden.

Infolge dessen wird vereinzelt an dieser Stelle eine weitere Differenzierung dahingehend vorgenommen, dass nun doch wieder danach gefragt wird, ob durch den Link ein eigener oder fremder Inhalt bereitgehalten wird.[505] Es geht also auch hier um die Frage, ob sich der Link-Einsteller den gelinkten Inhalt zu eigen gemacht hat oder nicht. Nach dieser Meinung soll ein Zueigenmachen dann angenommen werden, wenn ein wirtschaftliches oder sonstiges Interesse an der Verbreitung des ursprünglich fremden Inhalts auf Seiten des Einstellenden vorliegt.[506]

Obwohl § 5 II TDG a.F. eine flexible Regelung darstellt, die interessengerecht auf die verschiedenartigen Einzelfälle im Zusammenhang mit den Hyperlinks angewendet werden kann,[507] gibt es allerdings auch Schwachpunkte: So fällt es schwer, die spezielle Eigenart des Links unter den Begriff „Bereithalten" i.S.d. § 5 II TDG a.F. zu subsumieren. Aus der Begründung des Regierungsentwurfs zum IuKDG[508] wird hinreichend deutlich, dass der Begriff des Bereithaltens technisch verstanden werden soll und zwar im Sinne eines Vorhaltens des fremden Inhalts in einem eigenen Speicher.[509] Dies trifft auf den gelinkten Inhalt gerade nicht zu, so dass ein Bereithalten i.S.d. § 5 II TDG a.F. diesbezüglich zu verneinen ist.[510]

Die später vorgenommene Differenzierung in fremde und eigene Inhalte überzeugt ebenfalls nur teilweise. Zwar ist es konsequent, wenn die Links als Bereithalten i.S.v. § 5

---

505 So Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links", CR 1998, 545, 550 f.; Freytag, Haftung im Netz, S. 228 ff.

506 Freytag in: Haftung im Netz, S. 228 ff. nennt noch weitere Kriterien, bei deren Vorliegen ein Sichzueigenmachen gegeben ist. So soll dies insbesondere bei sogenannten „Frames" angenommen werden. Beim „Framing" handelt es sich um eine Programmiertechnik für WWW-Seiten, die deren Unterteilung in mehrere, voneinander unabhängige Rahmen (engl. frames) ermöglicht; vgl. hierzu die Ausführungen von Gabel in seinem Kommentar zum LG Düsseldorf vom 29.04.1998 – Az.: 12 O 347/97, K&R 1998, 553, 555.

507 § 5 II TDG a.F. hat sogar den Vorteil, dass auch der Umstand eines sich später verändernden gelinkten Inhalts geregelt ist, da insoweit dem Einsteller die positive Kenntnis fehlt. Darüber hinaus wird von § 5 II TDG a.F. berücksichtigt, wenn der Link auf eine große Anzahl von fremden Inhalten verweist, so dass der Einsteller hiervon unmöglich positive Kenntnis erlangen konnte.

508 Bundestag-Drucksache 13/7385 zu Art. 1 § 5 IuKDG, S. 20:
„Die Regelung dient der Klarstellung, dass dem Diensteanbieter, der rechtswidrige Inhalte Dritter in sein Diensteangebot, z.B. seinen eigenen News-Server oder in seinen Online-Dienst übernimmt, eine Garantenstellung für die Verhinderung der Übermittlung an Dritte trifft. Diese Verpflichtung soll allerdings nur dann greifen, wenn der Diensteanbieter die fremden rechtswidrigen Inhalte bewusst zum Abruf bereithält."

509 Pilcher, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG", MMR 1998, 79, 87; Waldenberger, „Teledienste, Mediendienste und die „Verantwortlichkeit" ihrer Anbieter", MMR 1998, 124, 128.

510 So auch Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks", CR 1998, 351, 354; Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen", CR 1997, 193, 202.
von Bonin/Köster versuchen dieses Problem in „Internet im Lichte neuer Gesetze", ZUM 1997, 821, 823 ff. zu umgehen, indem sie das „Bereithalten" eines fremden Inhalts im Sinne eines bloßen „Zugänglichmachens" verstehen wollen. Dies entspricht aber gerade nicht dem Willen des Gesetzgebers. Außerdem wäre dann konsequenterweise § 5 III TDG a.F. einschlägig und nicht § 5 II TDG a.F.

I und II TDG a.F. verstanden werden, im Anschluss daran zu fragen, ob nun fremde oder eigene Inhalte in Form von Links bereitgehalten werden. Allerdings ist diese Frage überflüssig, da in den meisten Fällen der Link-Einsteller positive Kenntnis von dem gelinkten Inhalt hat, ansonsten hätte er den Link nicht gesetzt. Denn er hat auch die Möglichkeit, den Link jederzeit mit einfachen Mitteln wieder zu beseitigen, so dass er gleichermaßen nach § 5 II und I TDG a.F. verantwortlich ist. Eine Unterscheidung des Bereithaltens von fremden und eigenen Inhalten besitzt somit ein großes Unsicherheitspotential und hätte Probleme bei der Abgrenzung zur Folge.
Im Ergebnis scheitert die direkte Anwendung des § 5 II TDG a.F. auf Hyperlinks vor allem daran, dass der Begriff des „Bereithaltens“ nicht erfüllt ist.

(c) Links als Zugangsvermittlung (§ 5 III TDG a.F.)

Zudem wird die Meinung vertreten, dass Hyperlinks rechtlich als Zugangsvermittlung i.S.d. § 5 III TDG a.F. zu qualifizieren sind.[511] Diese Ansicht stützt sich auf den Gedanken, dass § 5 III TDG a.F. nicht nur ausschließlich das Access-Providing und vergleichbare Dienste regeln soll, sondern darüber hinaus auch Links unter den Begriff der Zugangsvermittlung fallen sollen. Denn der Anbieter erleichtert durch den Einbau von Links lediglich den Zugriff auf fremde Inhalte, hält diese aber nicht selbst zur Nutzung bereit.[512] Folglich käme nur eine Anwendung des § 5 III TDG a.F. auf Hyperlinks in Betracht.
Diese Haftungsfreistellung nach § 5 III TDG a.F. soll aber dann nicht gelten, wenn ein Nutzer Hyperlinks in seine Homepage aufnimmt, da der Nutzer dies nicht im Rahmen eines Teledienstes i.S.d. § 2 I TDG tut und er als Urheber deshalb uneingeschränkt den allgemeinen Gesetzen nach § 5 I TDG a.F. unterliegt. Für den anbietenden Dienst, der die Homepage speichert, kann in diesen Links zugleich auch ein fremder, von ihm bereitgehaltener Inhalt gesehen werden, so dass für ihn sogar § 5 II TDG a.F. einschlägig ist. Diese Meinung trennt somit bei einer Homepage zwischen der Person, welche die Homepage errichtet hat, und dem Anbieter, der diese Homepage unterhält.
Allein hieraus wird sichtbar, dass diese Ansicht eine klare Abgrenzung vermissen lässt. Darüber hinaus kann nicht geleugnet werden, dass jeder, der Inhalte zur Nutzung bereithält, diese Inhalte zugleich auch zugänglich macht. Durch eine allzu weite Auslegung des Wortlauts von § 5 III TDG a.F., die nicht nur die Access-Provider erfasst, würden die Abs. I und II des § 5 TDG a.F. weitgehend sinnlos werden. Dies kann jedoch nicht

---

511 So Eichler/Helmers/Schneider, „Link(s) – Recht(s)“, K&R-BB-Beilage 18/1997, 23, 25; König/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 440; Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 200; Koch, Internet-Recht, S. 228, 239; Koenig, „Regulierungsoptionen für die Neuen Medien in Deutschland“, MMR-Beilage 12/1998, 1, 7; Spindler, „Die Haftung von Online-Diensteanbieter im Konzern“, CR 1998, 745, 752; Vassilaki, „Mittäterschaft von arbeitsteilig tätigen Teilorganisationen von Diensteanbietern – Fall CompuServe“, NStZ 1998, 518, 521.

512 Koch, „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193, 200.

im Interesse des Gesetzgebers gewesen sein.[513] Demzufolge und wegen der großen Haftungsprivilegierung darf § 5 III TDG a.F. einzig und allein das Access-Providing und vergleichbare Dienste regeln, mehr jedoch nicht.[514] Denn die Haftungsprivilegierung des § 5 III TDG a.F. ist für den Access-Provider nur deshalb eingerichtet worden, weil er zahllose Zugänge zu fremden Inhalten für die Nutzer zur Verfügung stellt, die er unmöglich alle kontrollieren und auf ihre Rechtswidrigkeit überprüfen kann. Bei der Einrichtung von Links fehlt dieser Grund für eine Haftungsprivilegierung, da hier gezielt bestimmte Links installiert werden, so dass eine inhaltliche Kontrolle durchaus im Bereich des Möglichen liegt. Ein weiterer gravierender Unterschied zwischen dem Access-Provider und dem Einstellen von Links besteht darin, dass der Access-Provider mit einem Telekommunikationsdienstleister vergleichbar ist, der keinerlei inhaltliche Auswahl trifft, sondern lediglich für den Datentransport zuständig ist.[515] Demgegenüber trifft der Link-Einsteller bewusst und gewollt eine entsprechende inhaltliche Auswahl an Links.

§ 5 III TDG a.F. und dessen Haftungsprivileg dürfen darum nicht auf die Hyperlinks angewendet werden.[516]

(d) Je nach Sachlage entweder § 5 I oder III TDG a.F.

Eine andere Meinung schlägt einen differenzierten Lösungsansatz vor.[517] Grundlage für diese Ansicht ist die Überlegung, dass Hyperlinks je nach Einzelfall einen unterschiedlichen Charakter aufweisen, der je nach Fallgestaltung zwischen der „technischen" Darstellung einer Abkürzung des Zugangswegs zu anderen Informationsinhalten und einem eigenständigen Informationsinhalt wechseln kann.[518] Welchen Charakter der jeweilige Hyperlink hat, muss deshalb für jeden Einzelnen und anhand des jeweiligen Kontextes

---

513 Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links", CR 1998, 545, 549.

514 So auch Waldenberger in „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter", MMR 1998, 124, 128 der jedoch auch Suchmaschinen dem Access-Providing gleichstellt.
Zum gleichen Ergebnis, dass § 5 III TDG a.F. nicht weit ausgelegt werden darf, kommt Bleisteiner in: Rechtliche Verantwortlichkeit im Internet, S. 171. Er begründet seine Ansicht mit dem Wortlaut des § 5 III TDG a.F. und zwar mit dem Wort „lediglich". Hierdurch wollte der Gesetzgeber klarstellen, dass eine völlige Freistellung von jeglicher Verantwortlichkeit nur dann zu bejahen ist, wenn „lediglich" der Zugang zur Nutzung vermittelt wird. Deshalb lassen sich aus § 5 III TDG a.F. diejenigen Fälle ausscheiden, in denen der Diensteanbieter sich erkennbar durch das Setzen von Links mehr oder weniger stark mit dem dahinterliegenden Inhalt identifiziert und zu eigen macht.

515 Spindler, „Haftungsrechtliche Grundprobleme der neuen Medien", NJW 1997, 3193, 3198.

516 Gercke, „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks", ZUM 2001, 34, 36; Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks", CR 1998, 351, 354.

517 Spindler in: Rossnagel (Hrsg.), Recht der Multimedia-Dienste, § 5 TDG Rdnr. 119; Pelz, „Die strafrechtliche Verantwortlichkeit von Internet-Providern", ZUM 1998, 530, 533; Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz", NJW 2981, 2985; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 174 (er differenziert noch etwas mehr, indem er eine weitere Unterteilung in „Frames" vornimmt, auf die er § 5 I TDG a.F. anwenden will.).

518 Marwitz, „Haftung für Hyperlinks", K&R 1998, 369.

geprüft werden. Kommt man nach dieser Einzelfallprüfung zu dem Ergebnis, dass der Hyperlink lediglich den „kurzen Weg“ bietet, muss eine Verantwortlichkeit des Einstellers für den dahinter liegenden Inhalt nach § 5 III TDG a.F. entfallen; ist demgegenüber der Link in einen Kontext eingebettet, der deutlich macht, dass der Verweisende sich den hinter dem Link liegenden Inhalt zu eigen macht und in sein Angebot einbezieht, muss sich seine Haftung nach § 5 I TDG a.F. richten.[519]

Aufgrund der Vielschichtigkeit und der unterschiedlichen Verwendungsmöglichkeiten von Hyperlinks erscheint es zunächst sinnvoll, eine differenzierte Betrachtung vorzunehmen und § 5 TDG a.F. mit seinen verschiedenen Absätzen je nach Einzelfall anzuwenden. Allerdings gibt es auch bei diesem Lösungsansatz einiges kritisch anzumerken: Er verkennt zum einen, dass ein Link immer den „kurzen Weg“ zu neuen Inhalten ermöglicht.[520] Zum anderen ist eine sichere Abgrenzung, in welchen Fällen nun § 5 I TDG a.F. oder doch § 5 III TDG a.F. angewendet werden soll, äußerst schwierig. Auf die Frage, wann § 5 II TDG a.F. als Zwischenstufe zu bejahen ist, wird überhaupt nicht eingegangen. Es wird diesem differenzierten Lösungsansatz auch vorgeworfen, dass allein die Tatsache, die fremden Inhalte seien bei einer Pauschalverweisung auf eine „Top-Level-Homepage“[521] sehr groß und eine regelmäßige Überprüfung sei für den Link-Einsteller nicht zumutbar, nicht alleiniger Grund für eine Einordnung von Links als Zugangsvermittlung sein kann.[522]

Aus den genannten Gründen muss dieser Lösungsansatz somit ebenfalls abgelehnt werden.

(e) Weiterer differenzierender Lösungsansatz

Schließlich wird von einer Ansicht in der Literatur eine sehr komplexe Lösung vorgeschlagen, wie Hyperlinks in die Gesetzessystematik des § 5 TDG a.F. einzuordnen sind.[523] Sie unterteilt zunächst danach, worauf der Link verweist. Entscheidend sind hierbei verschiedene Kriterien, beispielsweise die Linkebene, die Größe der fremden Inhalte, Weiterverweisungen, Textgröße, etc. Ist der Inhalt aufgrund einer dieser Parameter für den Verweisenden nicht überblickbar, weil sich z.B. der gelinkte Inhalt auf zahlreichen Unterebenen mit diversen anderen Links aufteilt, so liegt ein fremder Inhalt i.S.d. § 5 II und III TDG a.F. vor. Dieser fremde Inhalt wird also – je nach Einzelfall – entweder dem § 5 II TDG a.F. oder § 5 III TDG a.F. zugerechnet. Aber auch § 5 I TDG a.F. soll in gewissen Fällen zur Anwendung kommen, wenn sich der Linksetzer die In-

---

519 Engel-Flechsig/Maennel/Tettenborn, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 2981, 2985

520 Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links“, CR 1998, 545, 550

521 Die „Top-Level-Homepage“ stellt eine Homepage dar, die als Adresse eine Top-Level-Domain besitzt.

522 Bettinger/Freytag, „Privatrechtliche Verantwortlichkeit für Links“, CR 1998, 545, 550; a.A. jedoch Spindler in „Haftungsrechtliche Grundprobleme der neuen Medien“, NJW 1997, 3193, 3198.

523 Sieber, Verantwortlichkeit im Internet, S. 153 ff. Rdnr. 308 ff.

halte fremder Seiten zu eigen macht. Dies soll bei textlicher und technischer Einbindung zu bejahen sein. Eine weitere Unterteilung wird für die nachträgliche Veränderung des gelinkten Inhalts vorgenommen. Insoweit soll § 5 II TDG a.F. einschlägig sein.[524]
Da in diesem Lösungsansatz zwischen verschiedenen Fällen differenziert werden muss, ist eine klare Abgrenzung beinahe unmöglich. Es müssen zu viele Umstände berücksichtigt werden. Doch selbst dann, wenn sämtliche Umstände geprüft wurden, bleibt ein Rest an Unsicherheit zurück, ob überhaupt der richtige Absatz des § 5 TDG a.F. angewendet worden ist. Denn die rechtliche Problematik, welcher Absatz des § 5 TDG a.F. auf Hyperlinks zur Anwendung kommen soll, ist hierdurch noch nicht entschärft worden. Es bestehen bei diesem differenzierten Lösungsansatz dieselben Bedenken, den § 5 TDG a.F. und dessen Absätze I bis III anzuwenden, wie bei den Meinungen, die nur einen Absatz des § 5 TDG a.F. bei Hyperlinks für einschlägig halten. Letztendlich ist dieser Lösungsansatz aufgrund seiner Komplexität unpraktikabel und somit ebenfalls abzulehnen.

(f) Stellungnahme

Jede der vorbeschriebenen Meinungen kann nur zum Teil überzeugen.[525] Zu oft kollidieren die aufgezeigten Ansichten mit dem Wortlaut des § 5 TDG a.F. und den Absichten des Gesetzgebers. Auch die differenzierenden Lösungsansätze besitzen bei näherer Betrachtung einige Schwächen. Zwar wurde von ihnen das Problem der Hyperlinks, dass sie sowohl bewusst und zielgerichtet vom Linksetzer eingebaut werden als auch ein probates Mittel darstellen, um schnell an weitere Informationen zu gelangen, richtig erkannt.[526] Aufgrund der angesprochenen Schwierigkeiten kann ihnen aber auch nicht gefolgt werden. Selbst die EU-Richtlinie zum E-Commerce[527] enthält bedauerlicherweise keine Lösungsansätze zu diesem Thema, da auf die Hyperlinks in dieser Richtlinie nicht eingegangen wird.
Im Endeffekt ist somit die Ansicht, § 5 II TDG a.F. auf Hyperlinks anzuwenden, am ehesten geeignet, die Hyperlinks in die Verantwortlichkeitsregelungen des § 5 TDG a.F. einzuordnen: § 5 TDG a.F. regelt die Verantwortlichkeit von Diensteanbietern, so dass von dieser Gesetzesvorgabe ausgegangen werden muss. Die Frage ist also, wann sich der Einsteller von Links für diese Links wie zu verantworten hat. Das „Wie“ ist nicht in § 5 TDG a.F., sondern in den allgemeinen Gesetzen geregelt. Folglich kommt es nur darauf an, unter welchen Umständen der Linksetzer verantwortlich ist. § 5 II TDG a.F.

---

524 Köhler/Arndt, Recht des Internet, 2. Auflage, S. 134 Rdnr. 431; Sieber, Verantwortlichkeit im Internet, S. 156 Rdnr. 313.

525 Vgl. hierzu die schon oben bei der Darstellung der einzelnen Ansichten angesprochenen Nachteile.

526 Vgl. insoweit oben unter B. 2. Teil. II. 5. b. cc. (6).(d).

527 Richtlinie 2000/31/EG des Europäischen Rates vom 17.07.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), sogenannte „E-Commerce-Richtlinie“.

scheint hier die geeignete Norm zu sein, mit der gerechte und an die jeweilige Sachlage angepasste Ergebnisse erzielt werden können. Denn mit Hilfe von § 5 II TDG a.F. können die Aspekte, ob der Anbieter Kenntnis vom fremden Inhalt hat und ob die Nutzungsverhinderung technisch möglich sowie zumutbar ist, berücksichtigt werden. Dadurch kann § 5 II TDG a.F. flexibel und interessengerecht angewendet werden. So hat derjenige, der sich den fremden Inhalt durch einen Link zu eigen machen will, regelmäßig Kenntnis von dem gelinkten Inhalt. Als actus contrarius ist ein Löschen des Hyperlinks technisch ohne Schwierigkeit möglich und zumutbar.[528] Folglich ist der Linksetzer nach § 5 II TDG a.F. im gleichen Maße wie nach § 5 I TDG a.F. für den gelinkten Inhalt verantwortlich. Wird der Link aber lediglich als „kurzer Weg" zu neuen Informationen genutzt, fehlt dem Einsteller des Links grundsätzlich die Kenntnis vom fremden Inhalt, der hinter dem Link steht. Eine Verantwortlichkeit – vergleichbar mit § 5 III TDG a.F. – muss insofern nach § 5 II TDG a.F. verneint werden. Allerdings kann der Linksetzer vom rechtswidrigen Inhalt in Kenntnis gesetzt werden, so dass er zur Löschung gezwungen wird, da er sonst den Verantwortlichkeitstatbestand des § 5 II TDG a.F. erfüllen würde. Über § 5 II TDG a.F. kann zusätzlich das Problem, dass ein Link, der ursprünglich auf einen rechtmäßigen Inhalt verwiesen hat und plötzlich den Zugang zu rechtswidrigen Inhalten ermöglicht, zufriedenstellend behandelt werden. Denn hat der Linksetzer von diesem Inhaltswechsel keine Kenntnis, kann ihm dies offensichtlich nicht vorgeworfen werden. Genau dies wird durch § 5 II TDG a.F. geregelt.

Eine direkte Anwendung des § 5 II TDG a.F. auf Links ist allerdings – wie bereits oben besprochen wurde – nicht möglich, weil das Setzen von Hyperlinks nicht unter den Begriff des „Bereithaltens" subsumiert werden kann.[529] Denn wie sich aus den Begründungen zum IuKDG ergibt,[530] wird dieser Begriff rein technisch als Vorhalten des fremden Inhalts in einem eigenen Speicher verstanden.[531] Um diesen Widerspruch zum Wortlaut des § 5 II TDG a.F. zu beseitigen, bleibt als einzige Möglichkeit, dass § 5 II TDG a.F. auf Hyperlinks analog angewendet werden darf.[532] Eine Analogie bei § 5 II TDG a.F.

---

528 Flechsig/Gabel, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks", CR 1998, 351, 354.

529 Gercke, „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks", ZUM 2001, 34, 40; vgl. auch oben unter B. 2. Teil. II. 5. b. cc. (6). (b).

530 Bundestags-Drucksache 13/7385 zu Art. 1 § 5 IuKDG, S. 20.

531 Waldenberger, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter, MMR 1998, 124, 128; Bleisteiner, Rechtliche Verantwortlichkeit im Internet, S. 169.

532 So ebenfalls Waldenberger in „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter, MMR 1998, 124, 128 f.; Waldenberger, „Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet – ein Fall des LG Hamburg", AfP 1998, 373, 374; Gercke versucht in: „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks", ZUM 2001, 34, 36 dem Dilemma, dass Hyperlinks grundsätzlich nicht unter den Begriff „Bereithalten" subsumiert werden können, dadurch zu entgehen, dass er bei Hyperlinks von einem „virtuellen Bereithalten" spricht. Dies hat seiner Meinung zur Folge, dass die Hyperlinks doch von dem Begriff des Bereithaltens in § 5 I und II TDG a.F. erfasst werden.

für Hyperlinks zu bejahen, ist nicht nur sinnvoll, sondern auch rechtskonform:[533] Durch eine historische und teleologische Auslegung ergibt sich der zwingende Schluss, dass der Gesetzgeber eine unbewusste Regelungslücke geschaffen hat, da in keinem der Multimediagesetze Hyperlinks behandelt werden.[534] Dass insbesondere eine Regelung für Hyperlinks im Hinblick auf die Verantwortlichkeit in § 5 TDG a.F. nötig ist, wird schon allein durch den aufgezeigten Meinungsstreit deutlich. § 5 TDG a.F. besitzt demnach eine „planwidrige Unvollständigkeit“[535]. Wie bereits oben mehrfach dargelegt, können Hyperlinks nicht unter den Begriff des „Bereithaltens“ i.S.d. § 5 II TDG a.F. subsumiert werden. Daher wird die Grenze des möglichen Wortsinns dieser Vorschrift überschritten. Eine Auslegung ist somit nicht mehr statthaft.[536] Da die ratio und die Rechtsfolgen des § 5 II TDG a.F. auf die Hyperlinks in einer vernünftigen Art und Weise übertragen werden können, erscheint die analoge Anwendung des § 5 II TDG a.F. als das richtige Mittel, um die angesprochene Gesetzeslücke auszufüllen.
Deshalb ist der Auffassung zu folgen, § 5 II TDG a.F. analog auf Hyperlinks anzuwenden,[537]. Denn durch diese Analogie bleiben die Vorzüge der flexiblen Anwendung von § 5 II TDG a.F. auf Hyperlinks erhalten und ein Widerspruch zu den Vorgaben des Gesetzgebers besteht ebenfalls nicht mehr.

(7) Zusammenfassung

Infolge seiner (Vor-)Filterfunktion kann § 5 TDG a.F. unkompliziert angewendet werden. Insoweit hat der Gesetzgeber mit dieser Norm ein gewisses Maß an Rechtssicherheit geschaffen. Für staatliche Sperr- oder Löschanordnungen bedeutet dies, dass sie ebenfalls anhand von § 5 TDG a.F. zu prüfen sind. Denn aufgrund der Filterfunktion dieser Regelung müssen die Voraussetzungen von § 5 TDG a.F. im Verwaltungsrecht neben den die Störereigenschaft begründenden Umständen vorliegen.[538] In gewisser Weise wird hier lediglich der Störerbegriff neu definiert bzw. erweitert. § 5 TDG a.F. stellt klar, wann der Diensteanbieter als Störer anzusehen ist, gegen den dann entsprechende staatliche, d.h. polizeiliche oder sicherheitsrechtliche Maßnahmen gerichtet werden können. Diese besitzen also nur dann eine Rechtsgrundlage, wenn neben den einfachgesetzlichen Eingriffsermächtigungen auch § 5 TDG a.F. erfüllt ist.

---

533 So auch Härting, Internetrecht, S. 169 f. Rdnr. 342; a.A. dagegen Spindler in: Rossnagel (Hrsg.), Recht der Multimedia-Dienste, § 5 TDG Rdnr. 51, der die Möglichkeit einer Analogie verneint, da es sich bei den Regelungen des TDG um Ausnahmeregelungen handelt, die nicht per Analogie ausgedehnt werden dürfen.

534 Larenz, Methodenlehre der Rechtswissenschaft, 6. Auflage, S. 370 ff., insbesondere S. 381 ff.

535 BGH NJW 1981, 1726, 1727 sowie BGH NJW 1988, 2109, 2110.

536 Palandt-Heinrichs, Bürgerliches Gesetzbuch, 60. Auflage, Einleitung Rdnr. 40.

537 Waldenberger in „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter, MMR 1998, 124 ff.; Waldenberger, „Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet – ein Fall des LG Hamburg“, AfP 1998, 373, 374.

538 Sieber, Verantwortlichkeit im Internet, S. 123 f. Rdnr. 249 f.

dd. Mediendienste-Staatsvertrag

Auch § 5 MDStV regelt die Verantwortlichkeit von Anbietern.[539] Was unter dem Begriff „*Anbieter*“ zu verstehen ist, wird in § 3 Nr. 1 MDStV legal definiert. Wie bereits oben festgestellt worden ist,[540] besitzen § 5 TDG a.F. und § 5 MDStV nahezu den gleichen Wortlaut. Wobei der Wortlaut des § 5 I bis III 2 TDG a.F. mit dem des § 5 I bis III 2 MDStV identisch ist. Hinsichtlich dieser Regelungen kann deshalb auf die Ausführungen zu § 5 I bis III 2 TDG a.F. verwiesen werden.[541]
Lediglich der § 5 III 3 MDStV, der eine Verweisung auf § 18 III MDStV enthält, deckt sich nicht mit der Norm des § 5 TDG a.F. und muss deshalb eingehender betrachtet werden:

(1) Regelungsgehalt des § 5 III 3 i.V.m. § 18 III MDStV

Der MDStV hat auf eine Übernahme des § 5 IV TDG a.F. verzichtet und stattdessen den Inhalt dieser Vorschrift – wie sich aus § 18 MDStV ergibt – in § 18 III MDStV im Rahmen der Aufsichtsregelung aufgenommen.[542] Gemäß § 18 I MDStV soll damit der in den §§ 8, 9 MDStV fixierte Jugendschutz überwacht werden. Durch die gesetzgeberische Positionierung des § 18 III MDStV in den Abschnitt der Aufsicht wird deutlich, dass es sich bei dieser Norm um eine öffentlich-rechtlich ausgestaltete Eingriffsermächtigung handelt.[543] Hervorzuheben ist hierbei, dass sie – im Gegensatz zu § 5 IV TDG – a.F. nicht auf die allgemeinen Gesetze verweist, sondern selbst die Rechtsgrundlage für eine Sperrungsanordnung darstellt.[544]
Des weiteren ergibt sich nicht nur durch den Verweis in § 5 III 3 MDStV auf § 18 III MDStV, sondern auch aufgrund des Wortlauts des § 18 III MDStV, dass der von § 5 III MDStV geregelte Access-Provider, der normalerweise für fremde Inhalte nicht verantwortlich ist, dennoch Adressat von Sperrmaßnahmen i.S.d. § 18 III MDStV sein kann.[545] Folglich bezieht sich § 18 III MDStV lediglich auf § 5 III MDStV und bildet

---

539 An dieser Stelle muss erneut darauf hingewiesen werden, dass durch die Umsetzung der E-Commerce-Richtlinie eine Änderung des MDStV zu erwarten ist. Allerdings kann wegen der Parallelität der Regelungen von TDG und MDStV erst mit dem In-Kraft-Treten des neuen TDG eine Ausarbeitung des neuen MDStV begonnen werden. Ein Abschluss des Umlaufverfahrens wird erst gegen Ende 2002 erwartet. Vgl. Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001.

540 Siehe oben unter B. 2. Teil. II. 1.

541 Vgl. oben unter B. 2. Teil. II. 5. b. cc. (1). bis (4)., (6). und (7).

542 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231, 239.

543 Spindler, „Störerhaftung im Internet“, K&R 1998, 177, 179.

544 Maennel in: Engel-Flechsig/Maennel/Tettenborn (Hrsg.), Beck´scher IuKDG Kommentar, § 5 TDG Rdnr. 19 f.

545 Engel-Flechsig, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231, 239.

somit eine eigenständige Ermächtigungsgrundlage für die Inanspruchnahme des Zugangsvermittlers.[546]

Entgegen einer Meinung in der Literatur, die mangels Gesetzgebungskompetenz der Länder den § 18 III MDStV nicht auf den Access-Provider anwenden will[547], besaßen die Länder sehr wohl die Kompetenz zur Normierung des § 18 III MDStV, der sich gerade auf das in § 5 III MDStV geregelte Access-Providing beziehen soll. Denn diese Meinung verkennt, dass § 18 III MDStV den in den §§ 8, 9 MDStV verankerten Jugendschutz gewährleisten soll. Dies ist Aufgabe der Länder, so dass ihnen eine Gesetzgebungskompetenz zustand.[548] Folglich ist eine Berufung der Länder auf die besondere Nähe der Mediendienste zu Art. 5 I 2 GG und der sich daraus ergebenden Normsetzungskompetenz unnötig.[549]

Um den Access-Provider gemäß § 18 III MDStV in Anspruch nehmen zu können, sind folgende Voraussetzungen notwendig: Zunächst müssen sich Maßnahmen gegenüber den Verantwortlichen nach § 5 I und II MDStV als nicht durchführbar oder nicht erfolgversprechend erwiesen haben. Zudem muss der Provider unter Wahrung des Fernmeldegeheimnisses gemäß § 85 TKG von den Inhalten Kenntnis erlangt haben und ihm eine Sperrung technisch möglich und zumutbar sein.[550]

(2) Zusammenfassung

Insgesamt lässt sich festhalten, dass die Verantwortlichkeitsregelungen des MDStV größtenteils mit denen des TDG a.F. vergleichbar sind. Die einzige Ausnahme stellt der § 18 III MDStV dar. Er ist im Gegensatz zum § 5 IV TDG a.F. eine eigenständige Ermächtigungsgrundlage für die Inanspruchnahme des Zugangsvermittlers. Allgemeine Gesetze sind für eine Sperrungsanordnung aufgrund des § 18 III MDStV nicht mehr

---

546 So Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 5 MDStV Rdnr. 11; natürlich werden auch bei der Frage, wie sich § 18 III MDStV zum Rest des § 5 MDStV verhält, diverse Meinungen vertreten. Beispielsweise will Spindler in „Störerhaftung im Internet“, K&R 1998, 177, 179 die Haftungsprivilegierung des § 5 II MDStV mitberücksichtigt wissen. Diese Meinungen sind zum einen aus den gleichen Gründen abzulehnen, die schon bei der Besprechung bezüglich des Verhältnisses des § 5 IV TDG a.F. zu § 5 I bis III TDG a.F. gefallen sind. Außerdem spricht hier der Wortlaut des § 5 III 3 MDStV sowie des § 18 III MDStV eine klare Sprache.

547 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 443; sie begründen ihre Meinung damit, dass sich die Tätigkeit des Access-Providers auf die unteren Ebenen des Datentransports beschränkt. Wie sich bereits aus dem TKG ergibt, besteht keine Normsetzungskompetenz der Länder auf diesem Gebiet. Deshalb soll die Regelung des § 18 III MDStV auf Service- oder Content-Provider beschränkt bleiben.

548 Sieber, Verantwortlichkeit im Internet, S. 196 Rdnr. 393.

549 Vgl. insoweit Engel-Flechsig in „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231, 239.

550 Als weitere Besonderheit gegenüber dem TDG weist der MDStV die Ordnungswidrigkeitenvorschrift des § 20 I Nr. 15 MDStV auf. Demnach kann das Unterlassen von Sperrungen entgegen der Anordnung einer zuständigen Behörde mit einer Geldbuße von bis zu 500.000,00 DM geahndet werden. Eine Sanktionierung gemäß § 20 I Nr. 15 MDStV setzt allerdings für Bayern nach Art. 19 Bayerisches Verwaltungszustellungs- und Vollstreckungsgesetz (BayVwZVG) voraus, dass die entsprechende Verwaltungsanordnung zum Zeitpunkt der unterlassenen Sperrung zumindest vorläufig vollziehbar war.

nötig. Abgesehen von dieser unterschiedlichen Regelung in § 18 III MDStV enthält § 5 MDStV dieselben Tatbestände wie § 5 I bis III TDG a.F..

ee. Zwischenergebnis

Im Endeffekt sind die Regelwerke des TDG a.F. und MDStV in gleicher Weise anwendbar und enthalten identische Rechtsfolgen. Es macht also keinen großen Unterschied, ob ein Dienst im Internet als Mediendienst oder als Teledienst qualifiziert wird. Denn ob der Diensteanbieter für gewisse Inhalte verantwortlich ist, wird sowohl vom TDG a.F. als auch vom MDStV unterschiedslos sowie zufriedenstellend geklärt. Lediglich bei der Frage, nach welcher Rechtsgrundlage eine Sperranordnung gegen den Acces-Provider ausgesprochen werden kann, gibt es Diskrepanzen zwischen dem TDG a.F. und dem MDStV, weil der § 5 III 3 i.V.m. § 18 III MDStV bereits eine eigenständige Rechtsgrundlage darstellt. Dagegen sind sowohl für § 5 I bis IV TDG a.F. als auch für § 5 I bis III 2 MDStV, die lediglich Filterfunktion besitzen, die eigentlichen Eingriffsbefugnisnormen in den allgemeinen Gesetzen zu suchen. Für präventive staatliche Kontrollmaßnahmen heißt dies, dass eine Sperrungs- oder Löschungsanordnung, sofern eine Verantwortlichkeit nach § 5 I bis IV TDG a.F. bzw. § 5 I bis III 2 MDStV zu bejahen ist, nur aufgrund einer Regelung aus dem Polizei- bzw. Sicherheitsrecht des jeweiligen Bundeslandes[551] ergehen darf.[552] Stellvertretend für sämtliche Bundesländer mit ihren verschiedenartig ausgestalteten Polizei- und Sicherheitsrechten soll hier auf das bayerische Polizei- und Sicherheitsrecht eingegangen werden. Dabei ist zu beachten, dass in Bayern im Gegensatz zu vielen anderen Bundesländern eine Trennung von Polizei und Ordnungsverwaltung besteht. Polizei i.S.d. bayerischen Polizeirechtes sind gemäß Art. 1 PAG „*die im Vollzugsdienst tätigen Dienstkräfte der Polizei des Freistaates Bayern*“. Die nichtvollzugspolizeiliche Gefahrenabwehr ist Aufgabe der allgemeinen inneren Verwaltung, die dabei in der Funktion von Sicherheitsbehörden (der Terminus Ordnungsverwaltung wird nicht gebraucht) handelt:
Aufgrund der Trennung von Polizei- und Sicherheitsrecht in Bayern sowie der Subsidiaritätsklausel des Art. 3 PAG ist das bayerische Landesstraf- und Verordnungsgesetz (LStVG) das geeignet Regelwerk als Rechtsgrundlage für präventive, staatliche Kontrollmaßnahmen.[553]

---

551 Für Bayern wäre dies das Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG), GVBl. S. 397, BayRS 2012 – 1 – 1 – I bzw. das Gesetz über das Landesstrafrecht und das Verordnungsrecht auf dem Gebiet der öffentlichen Sicherheit und Ordnung (Landesstrafrecht- und Verordnungsgesetz – LStVG), BayRS 2011 – 2 – I.

552 Vgl. hierzu: Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 59 ff.

553 Es wäre sicherlich auch vertretbar, statt dem LStVG das PAG als Rechtsgrundlage anzusehen. Dies lässt sich vor allem dadurch begründen, dass die Landeskriminalämter bestimmte Stellen eingerichtet haben, die damit beschäftigt sind, das Internet nach unerwünschten Inhalten zu durchforsten. Für Bayern existiert eine solche Behörde beim Landeskriminalamt in München. Fraglich ist dabei nur, ob diese Tätigkeit der Polizeibeamten mehr repressiver (also strafverfolgend) oder mehr präventiver (zur Gefahrenabwehr) Natur ist. Letztendlich verlangen sowohl das LStVG als auch das PAG eine

Mangels spezialgesetzlicher Vorschriften (vgl. Art. 7 I LStVG) ist auf die Generalnorm des Art. 7 II LStVG und hier insbesondere auf Art. 7 II Nr. 1 LStVG zurückzugreifen. Diese Norm stellt i.V.m. § 5 TDG a.F. die Eingriffsermächtigung dar, falls es sich um rechtswidrige Inhalte bei einem Teledienst i.S.d. TDG handelt.[554] Entsprechendes gilt für einen Mediendienst i.V.m. § 5 MDStV. Die staatliche Maßnahme muss sich gemäß Art. 9 LStVG gegen den richtigen Störer richten. Hierfür kommen die jeweiligen Provider als Handlungs-, Zustands- bzw. Nichtstörer nach Art. 9 LStVG in Betracht. Wie bereits oben angesprochen, benötigt § 5 III MDStV i.V.m. § 18 MDStV keine weitere Rechtsgrundlage aus den allgemeinen Gesetzen.[555] Gegen wen die in § 18 MDStV genannten Maßnahmen zu richten sind, regeln wiederum § 5 und § 18 MDStV (insbesondere die Subsidiaritätsklausel des § 18 III MDStV).

Die sachliche und örtliche Zuständigkeit der jeweiligen Behörden wird bei Telediensten nach dem Art. 6 LStVG bzw. Art. 3 I Nr. 4 bzw. Art. 3 IV bayerisches Verwaltungsverfahrensgesetz bestimmt. Falls es sich um Mediendienste handelt, findet sich eine Regelung in § 18 MDStV i.V.m. den Umsetzungsgesetzen der jeweiligen Bundesländer. So ist in Bayern gemäß § 18 I 3 MDStV i.V.m. Art. 1 II des bayerischen Gesetzes zur Ausführung des Staatsvertrags über Mediendienste[556] i.V.m. § 1 der Verordnung über die Zuständigkeit auf Grund des Staatsvertrags über Mediendienste (ZustV-MedStV)[557] die Regierung von Mittelfranken zuständig. Eine Regelung für die örtliche Zuständigkeit enthält § 18 V MDStV. Diese unterschiedlichen Zuständigkeitsvorschriften für die Bekämpfung sicherheitsrechtlicher bzw. polizeilicher Gefahren, die von Mediendiensten sowie von Telediensten ausgehen, können im Einzelfall auch dazu führen, dass für einzelne Anbieter gleichzeitig mehrere Behörden zuständig sind, weil das Gesamtangebot eines solchen Diensteanbieters – wie erwähnt – teilweise als Teledienst und teilweise als Mediendienst zu qualifizieren sind.[558] Trotz dieser Problematik ist im Ergebnis aber festzustellen, dass staatliche Kontrollmaßnahmen gegen rechtswidrige Inhalte im Internet bei Tele- und Mediendiensten dann eine Rechtsgrundlage besitzen, wenn sämtliche materiellen Voraussetzungen gegeben sind. Folglich sind Sperr- oder Löschanordnun-

---

konkrete Gefahr für die öffentliche Sicherheit und Ordnung. Die Voraussetzungen für eine Gefahrenabwehr nach dem LStVG und dem PAG decken sich also im Endeffekt, so dass keine unterschiedlichen Ergebnisse zu erwarten sind, wenn die Kontrollmaßnahmen zum einen auf das LStVG und zum anderen auf das PAG gestützt werden.

554 Nach Umsetzung der E-Commerce-Richtlinie trifft dies allerdings nicht mehr zu. Vgl. insoweit unten unter B. 2. Teil. II. 5. b. ff.

555 Vgl. oben unter B. 2. Teil. II. 5. b. dd. (1).

556 BayGVBl. S. 310, BayRS 2251-11-S.

557 BayGVBl. S. 865, BayRS 2251-11-1-S.

558 Vgl. hierzu auch: Zimmermann. „Polizeiliche Gefahrenabwehr im Internet“, NJW 1999, 3145 ff.; er behandelt jedoch sämtliche auftretenden Fragen mit dem Polizeirecht aus Baden-Württemberg. Dadurch dass in diesem Bundesland die Organisation der Polizei sowohl die Polizeibehörden als auch den Polizeivollzugsdienst umfasst, eine Ordnungsverwaltung neben den Polizeibehörden somit nicht besteht, gibt es zum bayerischen Sicherheitsrecht keine vergleichbaren Normen. Deshalb sind bei ihm stattdessen die Vorschriften des Baden-Württembergischen Polizeigesetzes (BadWürttPolG) einschlägig.

gen, die von den zuständigen Behörden gegen Provider ausgesprochen werden und mit den Eingriffsermächtigungen im Einklang stehen, nach deutschem Recht grundsätzlich zulässig.

ff. Rechtslage nach Umsetzung der E-Commerce-Richtlinie

(1) Einführung

Die am 17.07.2000 im Amtsblatt der Europäischen Gemeinschaften veröffentlichte Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr" bzw. „E-Commerce Richtlinie")[559] (ECRL)[560], wird auf Bundesebene vor allem durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronisches Geschäftsverkehr-Gesetz: EGG) umgesetzt. Wie das IuKDG stellt das EGG ein Artikelgesetz dar. Durch Inkrafttreten des EGG werden einige Regelungen des IuKDG von 1997 geändert. Besonders betroffen ist hiervon Art. 1 IuKDG. Dadurch findet eine Neustrukturierung des TDG statt, worin die für dieses Gesetz wesentlichen Vorschriften aus der E-Commerce-Richtlinie eingearbeitet werden. Da das EGG bereits am 09.11.2001 vom Bundestag verabschiedet worden und mittlerweile in Kraft getreten ist, muss auf seine für diesen Teil der Arbeit relevanten Änderungen eingegangen werden. Im Vordergrund steht dabei die Verantwortlichkeit nach dem TDG bzw. MDStV. Obwohl das TDG a.F. in wesentlichen Punkten Änderungen erfahren hat, gilt dies noch nicht für den MDStV. Denn aufgrund der Parallelität der Regelungen im TDG und MDStV kann mit dem Verfahren zum in Kraft treten des MDStV erst begonnen werden, wenn die Regelungen des EGG feststehen. Dies bedeutet, dass der neue MDStV mit Abschluss des Umlaufverfahrens voraussichtlich erst gegen Ende 2002 in Kraft treten kann.[561] Er soll jedoch dem TDG neue Fassung (n.F.) wie bisher angeglichen werden.[562] Deshalb gelten für ihn die folgenden Ausführungen gleichermaßen.[563]

---

559 Richtlinie 2000/31/EG des Europäischen Rates vom 17.07.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), sogenannte „E-Commerce-Richtlinie"; Richtlinie 2000/31/EG ABl. EG Nr. L 178, 1 ff.

560 Im Folgenden wird die E-Commerce-Richtlinie bei der Nennung von Artikeln mit „ECRL" abgekürzt.

561 Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr", K&R Beilage 1 zu Heft 12/2001, 1, 3.

562 Libertus, „Medienrechtliche Aspekte der Umsetzung der E-Commerce-Richtlinie in Deutschland", RTkom 2001, 79.

563 Bis zu seiner Umsetzung gelten also die zum TDG a.F. und auf den MDStV übertragbaren Ausführungen fort. Allerdings wird wohl bei einer Kollision zwischen dem neuen TDG und dem alten MDStV der Art. 31 GG zur Anwendung kommen. Außerdem ist sicherlich auch der europarechtliche Anwendungsvorrang (vgl. hierzu unten unter B. 3. Teil. 1. Kapitel. II. 2. d.) zu beachten.

Zunächst ist jedoch zu begründen, warum überhaupt noch auf die alte Gesetzeslage ausführlich eingegangen worden ist. Dies lässt sich plausibel beantworten: Es gibt so gut wie keine Literatur und Rechtsprechung zum neuen TDG. Der Meinungsstand zum alten TDG ist deshalb für das Verständnis des TDG n.F. unbedingt erforderlich.[564] Daneben bleiben die Ausführungen zum TDG a.F. sowie MDStV für den noch nicht aktualisierten MDStV (vorerst) gültig. Im übrigen kann das TDG n.F. im Hinblick auf die Verantwortlichkeitsregelungen nur dann umfassend verstanden werden, wenn die ratio und Problempunkte des alten TDG erfasst worden sind.

Da der deutsche Gesetzgeber die Vorschriften zur Verantwortlichkeit aus der E-Commerce-Richtlinie nicht exakt übernommen hat,[565] sind zuerst die Regelungen der Richtlinie aufzuzeigen, bevor auf die nationalen Vorschriften und deren Besonderheiten eingegangen wird. Eine umfassende Kenntnis der einschlägigen Normen der E-Commerce-Richtlinie ist schon allein deshalb notwendig, weil bei Auslegungsproblemen nicht das deutsche, sondern das europäische Recht – hier primär die Richtlinie – entscheidend ist.[566]

(2) Die Verantwortlichkeitsregelungen in der E-Commerce-Richtlinie

Die Art. 12 bis 15 ECRL befassen sich wie § 5 TDG a.F. bzw. § 5 MDStV mit der Verantwortlichkeit der Provider. Obwohl die Art. 12 bis 15 ECRL vom deutschen TDG a.F. inspiriert waren, gibt es zwischen dem ursprünglichen nationalen Gesetz und der E-Commerce-Richtlinie einige Unterschiede.[567] So spricht die Richtlinie von „*Informationen*“ im Gegensatz zu § 5 TDG a.F. bzw. § 5 MDStV, die auf den Begriff der „*Inhalte*“ abstellen.[568] Auch eine Unterscheidung zwischen Tele- und Mediendiensten ist der E-Commerce-Richtlinie fremd, die lediglich die „*Dienste der Informationsgesellschaft*“ regelt.[569] Aber auch in den einzelnen Vorschriften der E-Commerce-Richtlinie gibt es hinsichtlich der Verantwortlichkeit Differenzen zum deutschen § 5 TDG a.F. bzw. § 5 MDStV. Diese werden bei den jeweiligen Regelungen aufgezeigt.

Die Richtlinie kennt zwei Grundfälle für die Verantwortlichkeit: erstens den Fall des Durchleitens und Vermittelns, Art. 12 und 13 ECRL, sowie zweitens den des Hostings,

---

564 Vgl. deshalb die Ausführungen unter B. 2. Teil. II. 5. b. cc.

565 Vgl. hierzu § 8 TDG n.F.

566 Arndt, Europarecht, 5. Auflage, S. 72 ff.; EuGH, Rs. 14/83, vom 10.04.1984, Slg. 1984, 1891, 1910 Rdnr. 26 (Von Colson und Kamann) sowie EuGH, Rs. 79/83, vom 10.04.1984, Slg. 1984, 1921, 1942 Rdnr. 26 (Harz).

567 Der Grund dafür liegt in dem Umstand, dass nicht dem schlanken Regelungsansatz des § 5 TDG a.F., sondern der schwerfälligen und detailversessenen Kasuistik des Digital Millenium Copyright Act of 1998, Public Law No. 105-304, 112 Stat. 2860, der USA gefolgt wurde. Vgl. zur Vertiefung Freytag in: „Digital Millenium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft“, MMR 1999, 207 ff.

568 Vgl. Waldenberger in „Electronic Commerce: Der Richtlinienvorschlag der EG-Kommission“, EuZW, 1999, 296, 301.

569 Freytag, „Providerhaftung im Binnenmarkt“, CR 2000, 600, 601 f.; Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 254.

Art. 14 ECRL. Reine Klarstellungsfunktion besitzt der Art. 15 ECRL, der besagt, dass den Diensteanbietern keine permanente Überwachungspflicht auferlegt werden darf.
In der E-Commerce-Richtlinie fehlt eine vergleichbare Norm, wie sie § 5 I TDG a.F. bzw. § 5 MDStV enthält, also die Verantwortlichkeit des Content-Providers. Dies lässt sich damit begründen, dass die Verantwortlichkeit des Content-Providers als selbstverständlich vorausgesetzt wird und deshalb eine ausdrückliche Vorschrift i.S.d. § 5 I TDG a.F. bzw. § 5 I MDStV in der E-Commerce-Richtlinie für entbehrlich angesehen wurde.[570] Art. 12 ECRL entspricht im Grundsatz § 5 III TDG a.F. bzw. § 5 III MDStV. Er stellt Diensteanbieter bei einem reinen Durchleiten von Inhalten mittels Telekommunikation, einschließlich automatischer und rein technisch bedingter Zwischenspeicherung, frei, wie es etwa bei der Versendung von E-Mails oder im Rahmen des ISDN-Verkehrs im Sinne einer intelligenten Paketvermittlung regelmäßig der Fall ist. Art. 13 ECRL regelt das Caching, das in § 5 III 2 TDG a.F. bzw. § 5 III 2 MDStV schlicht als Zugangsvermittlung fingiert ist. Art. 14 ECRL entspricht im Grundsatz dem § 5 II TDG a.F. bzw. § 5 II MDStV.[571]

(a) Reine Durchleitung (Art. 12 ECRL)

Art. 12 ECRL beschränkt das Haftungsprivileg des Diensteanbieters in Form des Access-Providers auf die vom Nutzer zur Übermittlung eingegebenen Informationen. Vom Diensteanbieter darf weder der Übermittlungsvorgang veranlasst, noch darf eine Auswahl unter den Adressaten getroffen, noch dürfen die Informationen verändert sein. Haftungsprivilegiert sind die Anbieter von Zugängen zum Kommunikationsnetz als Dienst der Informationsgesellschaft nach Art. 12 I ECRL. Die in Art. 12 II ECRL genannte automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen ist dann haftungsprivilegiert, wenn sie geschieht, um die Information zu übermitteln und die Information nicht über die üblicherweise erforderliche Zeitdauer hinaus gespeichert wird.

(b) Caching (Art. 13 ECRL)

Während Art. 12 II ECRL nur die Zwischenspeicherung zu Zwecken der Übermittlung erfasst, regelt Art. 13 ECRL generell das nicht nur kurzzeitige, aber zeitlich begrenzte Zwischenspeichern, um die Kommunikation zwischen den Netzteilnehmern, insbesondere beim Mirror-Verfahren (sogenannte „Spiegelungen“)[572], und Caching zu erleich-

---

570 Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 258.

571 Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 258.

572 Als Spiegelung bezeichnet man das doppelte Vorhalten technischer Ressourcen zur Erhöhung der Verfügbarkeit. Üblicherweise wird die Spiegelung, häufig auch „Mirroring“ (engl. mirror = Spiegel) genannt, im Zusammenhang mit Datenbanken erwähnt, von denen jeweils eine Kopie auf einem Server, der dann „Mirror“ genannt wird, gehalten wird. Beide Server sind dabei permanent online geschaltet. Operationen werden simultan auf beiden Datenbanken auf den Servern durchgeführt. Im

tern. Um Missbräuche zu verhindern, stellt Art. 13 ECRL eine Reihe von Bedingungen auf, die erfüllt werden müssen, damit sich der Anbieter auf das Haftungsprivileg des Art. 13 ECRL berufen kann. So darf der Diensteanbieter unter anderem die Information nicht verändern, er muss die Bedingungen für den Zugang zur Information und nach den Industriestandards die Aktualisierung der Information beachten und er darf die Sammlung von Daten über die Nutzung der Informationen nicht beeinträchtigen. Aus haftungsrechtlicher Sicht besonders bedeutsam ist schließlich das letzte Kriterium, wonach der Diensteanbieter die Information entfernen oder den Zugang zu ihr sperren muss, sobald er Kenntnis davon erhält, dass die Information am Ursprungsort der Übertragung entfernt, der Zugang zu ihr unmöglich gemacht wurde oder eine Behörde die Entfernung oder Sperrung angeordnet hat.[573]
Gemeinschaftsweit wird damit einer Umgehung der Sperrung einer inkriminierten Information durch ihre Spiegelung auf anderen Servern ein Riegel vorgeschoben.[574]

(c) Hosting (Art. 14 ECRL)

Die Speicherung von Informationen eines Nutzers entspricht der Regelung des § 5 II TDG a.F. bzw. § 5 II MDStV hinsichtlich des Bereithaltens fremder Inhalte. Entgegen der nationalen Norm, die lediglich die positive Kenntnis des rechtswidrigen Inhalts fordert (d.h. auf die Kenntnis, dass der Inhalt selbst rechtswidrig ist, kommt es nicht an),[575] verlangt Art. 14 I ECRL nicht nur die Kenntnis vom rechtswidrigen Inhalt, sondern darüber hinaus auch noch die Kenntnis von seiner Rechtswidrigkeit.[576] Für Schadensersatzansprüche soll gemäß Art. 14 I a ECRL die Kenntnis von Tatsachen oder Umständen genügen, woraus „*die rechtswidrige Tätigkeit oder Information offensichtlich wird*“ oder nach Art. 14 I b ECRL der Anbieter nicht unverzüglich tätig wird, sobald er Kenntnis oder dieses Bewusstsein erlangt, um die Information zu entfernen oder den Zugang zu ihr zu sperren.
Ebenso weicht Art. 14 ECRL von § 5 II TDG a.F. bzw. § 5 II MDStV ab, wenn die Zumutbarkeit der Sperrung des Zugangs zu einem Inhalt nicht zu den Voraussetzungen der Haftungsprivilegierung gehört. Die Richtlinie stellt allein auf die unverzügliche Tätigkeit des Diensteanbieters ab, um die Information zu entfernen oder den Zugang zu ihr

---

Fehlerfall, d. h. wenn ein Server ausfällt, geht der Betrieb ausschließlich und ohne jede Unterbrechung auf den zweiten über, Klußmann, Lexikon der Kommunikations- und Informationstechnik, 2. Auflage, S. 490.

573 Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 17.

574 Sowohl für Art. 12 ECRL als auch für Art. 13 ECRL bestimmt Ziff. 44 der Erwägungsgründe der E-Commerce-Richtlinie, dass ein Diensteanbieter, der absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen, mehr leistet als reine Durchleitung und Caching und daher nicht in den Genuss der Haftungsprivilegierung kommt. Kollusives Zusammenwirken verhindert somit die Bejahung einer Haftungsprivilegierung nach Art 12 bzw. 13 ECRL.

575 Vgl. insoweit oben unter B. 2. Teil. II. 5. b. cc. (3). (b).

576 Holznagel/Holznagel, „Zukunft der Haftungsregeln für Internet-Provider“, K&R 1999, 103, 104; Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte“, ZUM 2000, 1007, 1022.

zu sperren. Allerdings ist dieser Verlust nicht sehr gravierend. Denn dieses Verfahren bezeichnet die notwendige Tätigkeit des Diensteanbieters konkreter als das deutsche Recht, da der Zugang zum Internet gerade im Netz kaum verhindert werden kann. Ob daraus gefolgert werden kann, dass es auf die Frage der Zumutbarkeit überhaupt nicht mehr ankommen soll, muss bezweifelt werden. So bietet gerade der Rechtsbegriff der Unverzüglichkeit eine breite Palette an Auslegungsmöglichkeiten. Wenn darin ein verschuldensabhängiger Begriff gesehen wird, dann stellt er auch ein Einfallstor für Zumutbarkeitsfragen dar, die inzident angeprüft werden müssten. Jedenfalls kann angesichts der von Art. 14 I b ECRL gebotenen Alternativen des Entfernens eines Inhalts oder der Sperrung des Zugangs nicht von vornherein davon ausgegangen werden, dass es unzumutbar ist, wegen eines einzelnen Inhalts einen ganzen Dienst zu sperren. Andererseits betont Ziff. 46 der Erwägungsgründe zur E-Commerce-Richtlinie, dass in diesem Zusammenhang dem Grundsatz der freien Meinungsäußerung Gewicht beizumessen ist.[577] Darin kann ein Abwägungsgebot in Form der Verhältnismäßigkeit gesehen werden, das ebenfalls für eine inzidente Zumutbarkeitsprüfung spricht.
Weiterhin macht Art. 14 II ECRL klar, dass die Haftungsfreistellung keine Anwendung findet, wenn der Nutzer des Dienstes dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird. Daraus ist zu schließen, dass das Gefährdungspotential beim Hosting für eigene Mitarbeiter, Angestellte oder sonst in Abhängigkeit befindliche Personen oder Nutzer zu Lasten des Diensteanbieters erheblich gesteigert ist, da in einem solchen Fall die Haftungsprivilegierung nicht eingreift.[578]

(d) Keine Überwachungspflicht (Art. 15 ECRL)

Die Schlussbestimmung des Art. 15 ECRL bezüglich der Regelungen zur Verantwortlichkeit schließt eine aktive, generelle Überwachungspflicht hinsichtlich der übermittelten Inhalte explizit aus. Lediglich Einzelmaßnahmen sollen zulässig bleiben.[579]

(3) Anwendung dieser Vorschriften

(a) Vorfilterfunktion

Fraglich ist nun, wie die Verantwortlichkeitsvorschriften der Art. 12 bis 15 ECRL auf die jeweiligen Sachverhalte in der Praxis anzuwenden sind. Sinnvoll ist der Gedanke, die Haftungsprivilegien der E-Commerce-Richtlinie ebenfalls als „Filter“ anzusehen,[580] wie dies schon beim TDG a.F. und MDStV gehandhabt wird.[581] Durch die Umsetzung

---

577 Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 18.
578 Brisch, „EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr“, CR 1999, 235, 242.
579 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 191.
580 Zu der Filterfunktion des § 5 TDG a.F. und MDStV vgl. insoweit oben unter B. 2. Teil. II. 5. b. bb.
581 Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1, 27.

der Richtlinie erfahren diese Normen bestimmte Änderungen.[582] Allerdings bleibt die Grundstruktur hinsichtlich der Frage nach der Verantwortlichkeit erhalten. Demnach kann sich trotz der Einarbeitung der E-Commerce-Richtlinie in das TDG a.F. an der Handhabung, den § 5 TDG a.F. bzw. § 5 MDStV als Vorfilter zu betrachten,[583] auch beim TDG n.F. nichts ändern. Denn um ein einheitliches rechtliches Verantwortlichkeitssystem mit nationalen und europäischen Normen erfolgreich aufzubauen, ist es angebracht, die Struktur des vorgelagerten Filters beizubehalten und dieses Prinzip auch bei der Umsetzung der Richtlinie zu berücksichtigen.[584]

(b) Keine Anwendung auf behördliche Anordnungen

Sowohl Art. 12 ECRL als auch Art. 13 ECRL enthalten jedoch in ihren letzten Absätzen (Art. 12 III und Art. 13 II ECRL) die Regelung, dass der jeweilige Artikel „*die Möglichkeit unberührt*“ lässt, „*dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern*“. Der gleiche Wortlaut ist ebenfalls in Art. 14 III ECRL zu finden, allerdings ist ihm noch der Zusatz angefügt, „*dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen*“ können.

Im Gegensatz zum ursprünglichen Richtlinienentwurf von 18.11.1998[585], worin bei den Regelungen der Art. 12 bis 14 Ausnahmen für den Fall „*der Unterlassungsklagen*“ vorgesehen waren,[586] hat sich die E-Commerce-Richtlinie insoweit stark geändert.[587] Denn wie sich aus Ziff. 45 der Erwägungsgründe zur E-Commerce-Richtlinie ergibt, lassen die in der E-Commerce-Richtlinie festgelegten Beschränkungen der Verantwortlichkeit von Vermittlern die Möglichkeit von Anordnungen unterschiedlicher Art unberührt. Im Vergleich zu den Vorschlägen für die E-Commerce-Richtlinie sind jetzt nicht nur ge-

---

582 Vgl. hierzu die Ausführungen bei: Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1 ff.

583 Sieber, Verantwortlichkeit im Internet, S. 112 f. Rdnr. 229.

584 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 191.

585 KOM (98) 586 endg.

586 Vgl. hierzu Waldenberger in: „Electronic Commerce: Der Richtlinienvorschlag der EG-Kommission“, EuZW, 1999, 296, 301.

587 In den Vorschlägen der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt heißt es bei den einzelnen Vorschriften zur Verantwortlichkeit der Diensteanbieter lapidar: „– außer im Falle einer Unterlassungsklage –“. Vgl. u.a. den geänderten Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (1999) 427 endg. Zwar wird zum Teil darauf hingewiesen, dass der Begriff der Unterlassungsklage zu eng sei und auf einem Übersetzungsfehler beruhe, so beispielsweise Tettenborn in: „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 258, da die englische Sprachfassung des Richtlinienvorschlags nämlich lediglich von „prohibitory injunction“ spricht. Allerdings können auch mit Hilfe einer weiten Auslegung des Wortes „Unterlassungsklagen“ darunter nur gerichtliche Vorgehensweisen unter Einschluss einstweiliger Verfügungen verstanden werden.

richtliche Anordnungen als Ausnahme zu den Verantwortlichkeitsregelungen anerkannt, sondern insbesondere auch behördliche Anordnungen, welche die Abstellung oder Verhinderung einer Rechtsverletzung einschließlich der Entfernung rechtswidriger Informationen oder ihrer Sperrung, verlangen.
Dies bedeutet nichts anderes, als dass die hier zu untersuchenden staatlichen Kontrollmaßnahmen, die von einer deutschen Behörde erlassen werden und entweder Sperr- und/oder Löschanordnungen zum Gegenstand haben, von den Verantwortlichkeitsbestimmungen der E-Commerce-Richtlinie nicht betroffen sind.[588] Die in der E-Commerce-Richtlinie genannten Haftungsprivilegien haben also grundsätzlich keinen Einfluss auf die zu untersuchenden behördlichen Sperr- und/oder Löschanordnungen.

(4) Die Verantwortlichkeit gemäß den §§ 8 bis 11 TDG n.F.

Nach Aufzeigen der einzelnen Vorschriften zur Verantwortlichkeit i.S.d. E-Commerce-Richtlinie soll nun ihre Umsetzung ins deutsche Recht näher betrachtet werden:

(a) § 8 TDG n.F.

Der Wortlaut des § 8 I TDG n.F. deckt sich im wesentlichen mit dem des alten § 5 I TDG, wonach die Content-Provider grundsätzlich nach den allgemeinen Gesetzen des Zivil-, Straf- und Verwaltungsrechts verantwortlich sind.
§ 8 II 1 TDG n.F. nimmt den Grundsatz des Art. 15 I ECRL auf. Es wird jetzt ausdrücklich bestimmt, dass die Diensteanbieter ihre zu übermittelnden oder gespeicherten Informationen nicht zu überwachen haben.
Etwas verwirrend liest sich § 8 II 2 TDG n.F., der besagt, dass eine Verpflichtung zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 TDG n.F. unberührt bleiben soll. Zunächst wirft diese Vorschrift die Frage nach dem Sinn der Haftungsprivilegierung gemäß den §§ 9 bis 11 TDG n.F. auf, da eine Sperr- bzw. Löschanordnung weiterhin möglich ist. § 8 II 2 TDG n.F. ähnelt auf den ersten Blick dem alten § 5 IV TDG. Allerdings bezieht sich § 5 IV TDG a.F. nur auf den Access-Provider, verlangt zusätzlich die Kenntnis des Access-Providers und die technische Möglichkeit sowie Zumutbarkeit der Sperrung beim Nichtstörer. Ganz anders dagegen die Regelung in § 8 II 2 TDG n.F.: Da hier von Entfernung und Sperrung die Rede ist, bezieht sich diese Vorschrift nicht nur auf den Access-Provider, sondern auch auf den Content- bzw. Service-Provider. Die Inanspruchnahme des Nichtstörers wird zudem nicht von einer technischen Möglichkeit und Zumutbarkeit abhängig gemacht. Sie kann anscheinend jederzeit angeordnet werden. Dies ist ein völliges Novum. Der Filter des TDG wird insoweit aufgehoben. Der Grund für diese gravierende Gesetzesänderung ist in der E-Commerce-Richtlinie zu finden. Wie bereits vorstehend angesprochen, enthal-

---

588 Vgl. hierzu auch Ziff. 45 der Erwägungsgründe zur E-Commerce-Richtlinie.

ten die letzten Absätze der Art. 12 bis 14 ECRL eine Ausnahmeregelung für gerichtliche und behördliche Anordnungen. Danach sollen die Haftungsprivilegierungen bei gerichtlichen und behördlichen Anordnungen, welche die Abstellung oder Verhinderung einer Rechtsverletzung einschließlich der Entfernung rechtswidriger Informationen oder der Sperrung des Zugangs zu ihnen verlangen, gerade nicht eingreifen.[589] Dieser Punkt war bisher im Rahmen des alten § 5 TDG a.F. noch sehr umstritten.[590] Nur ein Teil der Literatur vertrat die Ansicht, den § 5 TDG a.F. nicht auf das Verwaltungsrecht anzuwenden. Der Bearbeiter folgte hingegen der Meinung, dass § 5 TDG a.F. auf sämtliche Rechtsgebiete zur Anwendung kommen muss.[591] Mit der Umsetzung der Richtlinie herrscht nunmehr Klarheit. Da nur die Verwaltungsbehörden und Gerichte Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen aussprechen können, sollen die §§ 9 bis 11 TDG n.F. nun für sie gemäß § 8 II 2 TDG n.F. nicht mehr gelten. Dies bedeutet, dass für sie allein die allgemeinen Gesetze bedeutsam sind. Die staatlichen Behörden müssen sich also bei den Kontrollmaßnahmen lediglich an den allgemeinen Polizei- und Sicherheitsvorschriften der Länder orientieren.[592] Allerdings ist das Fernmeldegeheimnis nach § 85 TKG gemäß § 8 II 3 TDG n.F. zu wahren.
Insgesamt lässt sich somit sagen, dass die Haftungsprivilegien der §§ 9 bis 11 TDG n.F. nicht für staatliche Kontrollmaßnahmen gelten, sondern nur für strafrechtliche und zivilrechtliche Regelungen.

(b) § 9 TDG n.F.

§ 9 TDG n.F. entspricht exakt dem Art. 12 I ECRL. Insoweit kann nach oben verwiesen werden.[593]

(c) § 10 TDG n.F.

Auch § 10 TDG n.F. stellt eine Norm dar, die der Gesetzgeber genau aus der E-Commerce-Richtlinie übernommen hat. § 10 TDG n.F. enthält die Regelungen des Art. 13 I ECRL. Darauf wurde ebenfalls bereits eingegangen.[594]

(d) § 11 TDG n.F.

§ 11 TDG n.F. geht gleichermaßen auf eine Vorschrift aus der E-Commerce-Richtlinie zurück. Er spiegelt Art. 14 I und II ECRL wider. Hinsichtlich seiner Bestimmungen ist erneut ein Verweis nach oben möglich.[595]

---

589 Vgl. Ziff. 45 der Erwägungsgründe zur E-Commerce-Richtlinie.
590 Vgl. oben unter B. 2. Teil. II. 5. b. bb.
591 Vgl. oben unter B. 2. Teil. II. 5. b. bb.
592 Etwas anderes dürfte nur für Maßnahmen nach dem MDStV gelten, der gemäß § 5 III 3 i.V.m. § 18 III MDStV nicht nur einen Vorfilter sondern bereits eine Rechtsgrundlage enthält. Was mit dieser Rechtsvorschrift in Zukunft passieren wird, ist fraglich.
593 Vgl. oben unter B. 2. Teil. II. 5. b. ff. (2). (a).
594 Vgl. oben unter B. 2. Teil. II. 5. b. ff. (2). (b)
595 Vgl. oben unter B. 2. Teil. II. 5. b. ff. (2). (c).

(5) Unterschiede zwischen dem neuen und alten TDG

Zunächst fällt auf, dass im TDG n.F. nicht mehr von „*Inhalten*“ sondern von „*Informationen*“ die Rede ist. Der Begriff der Informationen wurde von der Richtlinie übernommen. Leider ist die klare Struktur des § 5 TDG a.F. nicht beibehalten worden, der eine übersichtliche und nachvollziehbare Stufenfolge bei der Verantwortlichkeit je nach Providertyp enthielt. Stattdessen wird jetzt in § 8 I TDG n.F. der Content-Provider, in § 9 TDG n.F. der Access-Provider, in § 10 TDG n.F. der Proxy-Cache-Server sowie in § 11 TDG n.F. der Service-Provider geregelt. Eine Struktur für die Verantwortlichkeit, die sich nach der jeweiligen Funktion des einzelnen Providers richtet, ist nicht mehr so klar wie bei § 5 TDG a.F. erkennbar. Abgesehen davon fällt eine Abgrenzung zwischen § 9 II TDG n.F. und Art. 10 TDG n.F. sehr schwer. Wann geschieht die kurzzeitige Zwischenspeicherung zur Durchführung der Datenübermittlung und wann, um die Übermittlung effizienter zu gestalten? Wäre hier nicht eine Norm, die generell die Kurzzeitspeicherung regelt, sinnvoller? Auch hätte die von § 5 TDG a.F. vorgegebene Aufzählung der Provider (Content-Provider, Service-Provider und Access-Provider) und die damit verbundene Steigerung der Haftungsprivilegierung durch ein einfaches Umstellen der §§ erhalten bleiben können. Etwas unverständlich ist ferner die Benutzung unterschiedlicher Begriffe für ein und dieselbe Handlung. So spricht § 8 I TDG n.F. von Diensteanbietern, die „*eigene Informationen* [...] *zur Nutzung bereithalten*“. Demgegenüber enthält der Wortlaut des § 11 TDG n.F. folgende Passage: „[...] *Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern* [...]. Einmal ist von Bereithalten, zum anderen von Speichern die Rede. Letztendlich geht es aber um denselben Vorgang, nämlich das Anbieten von Inhalten im Netz. Der § 5 TDG a.F. benutzt in § 5 I und II TDG a.F. sowohl für das Content- als auch für das Service-Providing gleichermaßen den Begriff des Bereithaltens.[596] Um Auslegungsfragen zu vermeiden, wäre es sicherlich sinnvoller gewesen, in beiden Fällen von „Bereithalten“ zu sprechen. Denn da sich an der Funktion des Content-Providers bzw. des Service-Providers durch die Umsetzung der Richtlinie nichts geändert hat, kann mit der Speicherung in § 11 TDG n.F. nur ein Bereithalten i.S.d. § 8 I TDG n.F. gemeint sein. Bezüglich der übrigen Unterschiede bei der Verantwortlichkeit zwischen dem alten und neuen TDG – insbesondere die nötige Kenntnis von der Rechtswidrigkeit in § 11 Nr. 1 TDG n.F. und die Ausnahme in § 8 II 2 TDG n.F. für gerichtliche und behördliche Anordnungen – kann schließlich nach oben verwiesen werden.[597]

(6) Rechtsfolgen

Letztendlich hat die Umsetzung der E-Commerce-Richtlinie und die damit einhergehenden TDG-Änderung auf die gültige Rechtslage im Zivil- und Strafrecht nur geringe

---

596 Vgl. insoweit auch oben unter B. 2. Teil. II. 5. b. cc. (2) und (3).

597 Vgl. oben unter B. 2. Teil. II. 5. b. ff. (2).

Auswirkungen. Das Haftungsprivileg des § 5 TDG a.F. wird mit wenigen Änderungen in den §§ 8 ff. TDG n.F. fortgeführt. Sogar die Vor-Filterfunktion bleibt außer im Fall des § 8 II 2 TDG n.F. erhalten. Da eine Regelung für Hyperlinks im TDG n.F. fehlt, geht die Diskussion über die dafür richtige Verantwortlichkeitsnorm in eine zweite Runde. Der Gedanke, den § 5 II TDG a.F. analog auf Hyperlinks anzuwenden, erscheint auch nach der Gesetzesänderung richtig. So zwingt der Wortlaut des § 11 Nr. 1 TDG n.F. erneut zu einer Analogie, weil das Setzen eines Hyperlinks nicht von dem Wortlaut der „Speicherung von fremden Informationen“ erfasst wird. Die Frage nach der Kenntnis des Diensteanbieters und dem unverzüglichen Handlungsgebots, solche Informationen unschädlich zu machen, muss als die eleganteste Lösung angesehen werden, die Verantwortlichkeit für Hyperlinks flexibel zu behandeln. Deshalb sollte § 11 TDG n.F. analog für Hyperlinks gelten.

Im Gegensatz zum Straf- und Zivilrecht wirkt sich die Gesetzesänderung auf das Verwaltungsrecht erheblich aus. Denn durch § 8 II 2 TDG n.F. spielen die Haftungsprivilegien der §§ 9 bis 11 TDG n.F. für staatliche Kontrollmaßnahmen keine Rolle mehr.[598] Der Verantwortlichkeitsfilter ist insoweit unbeachtlich. Es müssen nur noch die allgemeinen Gesetze beachtet werden. Dies bedeutet für die Polizei- und Sicherheitsbehörden, dass ihre Sperr- und/oder Löschanordnungen gegenüber Telediensten lediglich noch die Voraussetzungen der jeweiligen Polizei- und Sicherheitsvorschriften zu erfüllen haben. Dabei ist allerdings gemäß § 8 II 3 TDG n.F. das Fernmeldegeheimnis des § 85 TKG zu beachten. Der Vorfilter der §§ 9 bis 11 TDG n.F. ist für die Rechtsgrundlage der staatlichen Kontrollmaßnahmen somit ohne Bedeutung. Wenn also durch bestimmte rechtswidrige Inhalte im Internet die Kriterien der allgemeinen Gesetze, also die des Polizei- und Sicherheitsrechts des jeweiligen Landes erfüllt werden, dann sind die darauf basierenden Kontrollmaßnahmen bereits aufgrund des nationalen Rechts als rechtmäßig anzusehen.

Fraglich ist aber weiterhin, ob ihre Rechtmäßigkeit auch gegenüber dem Europarecht Bestand hat.

---

[598] Dies gilt allerdings momentan nur für Teledienste. Für die Mediendienste bleiben § 5 und § 18 MDStV bis zu ihrer Neuregelung beachtlich.

3. Teil - Vereinbarkeit der nationalen Kontrollmaßnahmen mit dem Europarecht

In den vorausgegangenen Ausführungen ist aufgezeigt worden, welche nationalen Gesetze in Deutschland bei den staatlich angeordneten Sperr- und Löschmaßnahmen gegen rechtswidrige Inhalte im Internet zur Anwendung kommen. Im Anschluss daran muss nun untersucht werden, ob diese behördlichen Anordnungen auch gegenüber dem Europarecht als rechtmäßig anzusehen sind. Hierfür sind zunächst noch einmal die technischen und rechtlichen Möglichkeiten einer staatlichen Kontrolle des Internets zusammenfassend in Erinnerung zu rufen, um dann zu prüfen, ob das entsprechende europäische Recht darauf angewendet werden kann.

1. Kapitel: Allgemeine Überlegungen

I. Öffentlich-rechtliche Kontrollmaßnahmen

Rein technisch können staatliche Behörden nur zwei Arten von Kontrollmaßnahmen anordnen: nämlich gewisse rechtswidrige Inhalte sperren oder löschen lassen. Wie bereits bei der Prüfung des § 5 TDG a.F. bzw. § 5 MDStV festgestellt wurde,[599] muss zwischen den einzelnen Arten der Internet-Provider unterschieden werden. So sind sowohl gegenüber dem Content-, als auch gegenüber dem Service-Provider Sperr- und Löschanordnungen denkbar, da diese Provider unmittelbaren Einfluss auf die gespeicherten Daten ausüben können. Hingegen besitzt der Access-Provider keinerlei technische Möglichkeiten, fremde rechtswidrige Daten zu löschen, zu denen er lediglich den Zugang vermittelt. Folglich sind gegen ihn lediglich Sperranordnungen sinn- und wirkungsvoll.
Die Rechtsgrundlagen für derartige staatliche Lösch- und Sperranordnungen ergeben sich aus § 5 TDG a.F. bzw. §§ 5, 18 MDStV i.V.m. dem jeweils einschlägigen Polizei- und Sicherheitsrecht der Länder.[600] Die Anordnung selbst ergeht in Form eines Verwaltungsaktes (VA)[601] i.S.d. § 35 S.1 Verwaltungsverfahrensgesetz (VwVfG)[602] durch die zuständige Behörde. Diese VAe müssen somit auf ihre Vereinbarkeit mit dem Europarecht überprüft werden.

---

599 Vgl. insoweit oben unter B. 2. Teil. II. 5. b. cc.

600 Mittlerweile ist jedoch das TDG n.F. beachtlich. Dies hat zur Folge, dass für Teledienste nur noch die allgemeinen Gesetze des Polizei- und Sicherheitsrechts als Rechtsgrundlagen in Frage kommen. Demgegenüber kommen § 5 und § 18 MDStV vorerst noch zur Anwendung.

601 Gemäß § 35 S.1 VwVfG ist ein VA „jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalles auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist." Weiterführend vgl. Kopp, Kommentar zum VwVfG, 7. Auflage, Art. 35 Rdnr. 4 ff.

602 BGBl. I S. 3050, BGBl. III/FNA 201-6.

II. Betroffenes Europarecht

1. Eingrenzung

Der Begriff des „Europarechts“ wird in der Literatur äußerst unterschiedlich verwendet. Bevor auf die jeweiligen Normen des Europarechts eingegangen werden kann, muss zunächst geklärt werden, welche Rechtsmaterien unter den Begriff des Europarechts zu fassen sind. Hierfür ist es notwendig, den Begriff „Europarecht“, wie er in dieser Arbeit zu verstehen ist, zu definieren. Im Schrifttum wird häufig vom Europarecht im „weiteren“ und „engeren“ Sinne gesprochen.[603] Dabei ist unter dem „Europarecht im weiteren Sinne“ das Recht der europäischen internationalen Organisationen zu verstehen.[604] Im Gegensatz dazu stellt das „Europarecht im engeren Sinne“ das Recht der drei Europäischen Gemeinschaften (Gemeinschaftsrecht)[605] und die Normen über die neuen Formen der Zusammenarbeit[606] im Rahmen der Europäischen Union (EU)[607] dar.[608]

Diese Arbeit befasst sich ausschließlich mit dem Europarecht im engeren Sinne. Die staatlich angeordneten Kontrollmaßnahmen und ihre Vereinbarkeit mit dem Europarecht sind demzufolge anhand des Vertrags von Maastricht (EUV)[609], wo unter anderem die Formen der Zusammenarbeit festgeschrieben wurden, und dem Recht der drei Gemeinschaften, das auf die drei Gründungsverträge (EG-Vertrag[610], EAG-Vertrag[611], EGKS-Vertrag[612]) zurückgeht, zu prüfen. Von diesen Rechtsgebieten kommen jedoch wieder nur bestimmte Teilbereiche in Frage, die für staatlichen Kontrollmaßnahmen

---

603 Koenig/Haratsch, Europarecht, 2. Auflage, S. 8 f.

604 Schweitzer/Hummer, Europarecht, 5. Auflage, S. 2 Rdnr. 7; als Beispiele für die europäischen internationalen Organisationen sind insbesondere zu nennen: Der Europarat mit der Europäischen Menschenrechtskonvention, die Westeuropäische Union und die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) sowie die Europäische Freihandelsassoziation.

605 Zu den drei Europäischen Gemeinschaften zählen:
- die Europäische Gemeinschaft für Kohle und Stahl (Montanunion): EGKS
- die Europäische Gemeinschaft (früher Europäische Wirtschaftsgemeinschaft genannt): EG und
- die Europäische Atomgemeinschaft (Euratom): EAG.

Diese drei Gemeinschaften bilden die erste Säule der Europäischen Union.

606 Unter den neuen Formen der Zusammenarbeit versteht man die durch den Vertrag von Maastricht (EUV) 1992 geschaffenen zwei weiteren Säulen der Europäischen Union:
- die Gemeinsame Außen- und Sicherheitspolitik (GASP) und
- die Zusammenarbeit in den Bereichen Justiz und Inneres, die jedoch mittlerweile im Rahmen des Amsterdamer Vertrags 1997 zur polizeilichen und justitiellen Zusammenarbeit in Strafsachen (PJZS) abgeändert worden ist. Vgl. hierzu Fischer, Europarecht, 3. Auflage, S. 1 Rdnr. 1.

607 Im folgenden bezeichnet der Rechtsbegriff EU die Verbundkonstruktion der institutionellen, materiell- und verfahrensrechtlichen Verklammerung intergouvernementaler Politiken (GASP, ZBJI) mit supranationalen Gemeinschaftspolitiken (EG, EAG, EGKS) nach dem EUV.

608 Herdegen, Europarecht, 2. Auflage, § 1 Rdnr. 2.

609 ABl. EG Nr. C 191 vom 29.07.1992 S. 1.

610 Vertrag zur Gründung der Europäischen Gemeinschaft vom 25.03.1957 (EGV), BGBl. II Nr. 23 vom 19.08.1957 S. 766.

611 Vertrag zur Gründung der Europäischen Atomgemeinschaft (EURATOM) vom 25.03.1957 (EAGV), BGBl. II Nr. 23 vom 19.08.1957 S. 1014.

612 Vertrag über die Gründung der Europäischen Gemeinschaft für Kohle und Stahl vom 18.04.1951 (EGKSV), BGBl. II Nr. 7 vom 06.05.1952 S. 447.

relevant sein können: So entsprechen die Regelungen im EUV den herkömmlichen Formen zwischenstaatlicher Kooperation auf vertraglicher Grundlage. Dies bedeutet, dass durch sie kein dem nationalen Recht vorgehendes Unionsrecht existiert bzw. entsteht. Vielmehr entfaltet der Unionsvertrag lediglich völkervertragsrechtliche Bindungswirkungen, welche die Vertragsstaaten zu einer intergouvernementalen Zusammenarbeit verpflichten.[613] Es handelt sich hierbei also um die rechtliche Ebene einer bloßen Regierungszusammenarbeit,[614] deren Maßnahmen in diesen Bereichen allein die Mitgliedstaaten selbst binden und – sofern sie innerstaatliche Wirksamkeit erlangen sollen – immer der Umsetzung in das nationale Recht der Mitgliedstaaten bedürfen.[615]
Eine nationale Umsetzung von Maßnahmen aufgrund der im EUV festgeschriebenen intergouvernementalen Zusammenarbeit, die sich mit der Kontrolle des Internets befasst, ist bisher noch nicht erfolgt. Aus dem EUV sind auch direkt keine Vorschriften zu entnehmen, die von den staatlichen Kontrollmaßnahmen im Internet tangiert sein können. Deshalb sind die Normen des EUV für die vorliegende Arbeit grundsätzlich nicht Prüfungsgegenstand. Hingegen kann er mittelbar rechtlich sehr wohl bedeutsam sein. Denn er besitzt zum einen ebenfalls europarechtliche Begriffe, so dass er als Auslegungshilfe bei Rechtsfragen im Zusammenhang mit anderen Bereichen des Europarechts herangezogen werden kann. Zum anderen besagt Art. 6 II EUV ausdrücklich, dass die Mitgliedstaaten die Grundrechte, wie sie in der am 04.11.1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK)[616] festgelegt sind, zu achten haben.[617] Dieser Aspekt ist daher bei der Anwendung des übrigen Europarechts im engeren Sinne zu berücksichtigen.
Neben dem EUV und seinen für staatliche Kontrollmaßnahmen indirekten europarechtlichen Auswirkungen sind vor allem die Gründungsverträge der drei Gemeinschaften für vorliegende Arbeit von großer Relevanz. Von diesen drei Europäischen Gemeinschaften spielt jedoch allein die Europäische Gemeinschaft (EG), die auf eine umfassende wirtschaftliche und auch politische Integration angelegt ist, eine zentrale Rolle,[618] während sich die anderen Gemeinschaften auf eine Integration in den durch ihre Bezeichnung gekennzeichneten Teilbereichen beschränken. Aufgrund der Tatsache, dass diese Teilbereiche (Kohle und Stahl bzw. Atomenergie) keinerlei Berührungspunkte zur multimedialen Welt besitzen und somit für die staatlichen Kontrollmaßnahmen im Internet ohne Bedeutung sind, braucht im folgenden auf sie nicht weiter eingegangen werden. Dies bedeutet, dass sich das zur Anwendung in Betracht kommende Europa-

---

613 Pechstein/Koenig, Die Europäische Union, 3. Auflage, S. 7 f. Rdnr. 12.
614 Lecheler, Einführung in das Europarecht, § 2 S. 27.
615 Fischer, Europarecht, 3. Auflage, S. 18 Rdnr. 5.
616 UNTS Bd. 213, S. 221.
617 Fischer, Europarecht, 3. Auflage, S. 23 Rdnr. 23.
618 Vgl. dazu nur Art. 3 EGV.

recht auf den gemeinschaftsrechtlichen EGV konzentriert. Denn nur gegen eine seiner Vorschriften könnten die staatlichen Kontrollmaßnahmen verstoßen.
Die behördlichen Sperr- und/oder Löschanordnungen sind somit hinsichtlich der Frage nach ihrer europarechtlichen Vereinbarkeit hauptsächlich an dem „primären Gemeinschaftsrecht“[619] in Form des EGV sowie dem daraus resultierenden „sekundären Gemeinschaftsrecht“[620] zu messen.

2. Das Gemeinschaftsrecht

Staatliche Kontrollmaßnahmen können aber nur dann gegen gemeinschaftsrechtliche Normen des EGV verstoßen, wenn das Gemeinschaftsrecht überhaupt hierauf angewendet werden kann und die zuständigen Behörden diese Art des Rechts zu beachten haben. Daher ist das Gemeinschaftsrecht generell näher zu betrachten:

a. Überblick

Das für die behördlichen Kontrollmaßnahmen relevante Gemeinschaftsrecht aus dem Primär- und Sekundärrecht. Dabei geht grundsätzlich das Primärrecht dem Sekundärrecht innerhalb des Gemeinschaftsrechts vor.[621] Das Primärrecht nimmt also in der Rechtsordnung des Gemeinschaftsrechts die oberste Rangstufe ein.[622] Allerdings wird häufig durch das Sekundärrecht das Primärrecht ausgestaltet. So wird vor allem zur Regelung spezifischer Einzelprobleme das sekundäre Gemeinschaftsrecht in Ergänzung der Gründungsverträge herangezogen.[623] Die möglichen Erscheinungsformen des Sekundärrechts, die sogenannten „Handlungsformen“, sind insbesondere in Art. 249 EGV (Verordnungen, Richtlinien, Entscheidungen, Empfehlungen und Stellungnahmen)[624] beschrieben.

---

619 Der Begriff „primäres Gemeinschaftsrecht“ umfasst die Gründungsverträge EGKS-, E(W)G- und EAG-Vertrag einschließlich ihrer Anhänge, Protokolle etc. sowie die zu ihrer Änderung und Ergänzung geschlossenen Verträge wie der Einheitlichen Europäischen Akte (EEA), dem Maastrichter und Amsterdamer Vertrag, aber auch die Beitrittsverträge mit neuen Mitgliedstaaten.

620 Das „sekundäre Gemeinschaftsrecht“ ist das Recht, welches die Gemeinschaftsorgane auf der Grundlage der Verträge setzen. Es soll grundsätzlich spezifische Einzelprobleme in Ergänzung der Gründungsverträge regeln. Die Mitgliedstaaten haben in den Gründungsverträgen die Organe ermächtigt, in bestimmten Grenzen eigenständig Recht zu setzen, welches europaweit Geltung erlangen kann. Hauptinstrumente dieser Rechtsetzung sind dabei die Verordnungen und Richtlinien. Aber auch Entscheidungen, Empfehlungen und Stellungnahmen, wie sich aus Art. 249 EGV ergibt, können von den jeweils zuständigen Organen zur Regelung erlassen werden.

621 Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 527; Oppermann, Europarecht, § 6 Rdnr. 429.

622 Herdegen, Europarecht, 2. Auflage, § 9 Rdnr. 161.

623 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrecht, 2. Auflage, S. 62.

624 Vgl. zu diesen Begriffen Herdegen, Europarecht, 2. Auflage, § 9 Rdnr. 175 ff.; Schweitzer/Hummer, Europarecht, 5. Auflage, § 4 Rdnr. 346 ff.; Oppermann, Europarecht, § 6 Rdnr. 444 ff.

b. Das Gemeinschaftsrecht und das Internet

Das Gemeinschaftsrecht kann jedoch nur auf solche Sachverhalte angewendet werden, für die die Gemeinschaft auch die Kompetenz zur Regelung besitzt. Dieses sogenannte „Prinzip der begrenzten Einzelermächtigung“ ist in Art. 5 I EGV ausdrücklich geregelt, wonach die Gemeinschaft nur aufgrund einer in dem Vertrag benannten Ermächtigungsgrundlage tätig werden darf.[625] Folglich ist es wichtig, dass das Gemeinschaftsrecht überhaupt auf das Internet zur Anwendung kommt.

Eine Anwendbarkeit des Gemeinschaftsrechts – speziell des EGV – auf das Internet lässt sich schon allein aus den Grundfreiheiten[626] ableiten.[627] Sie sind unerlässliche Voraussetzungen für einen funktionierenden Binnenmarkt. Staatliche Sperr- und/oder Löschanordnungen können die Warenverkehrsfreiheit, die Niederlassungsfreiheit oder die Dienstleistungsfreiheit tangieren. Das Europarecht gilt deshalb grundsätzlich für den multimedialen Bereich und somit auch für das Internet.[628]

c. Unmittelbare Anwendbarkeit des Gemeinschaftsrechts

Des weiteren stellt sich die Frage, welche Wirkung das Gemeinschaftsrecht auf die nationale Rechtsordnung hat und wie es zur Anwendung kommt. Hierzu hat sich der Europäische Gerichtshof (EuGH) in diversen Urteilen geäußert.[629] Dabei ging es anfangs lediglich darum, inwieweit das Primärrecht des EGV unmittelbar angewendet werden kann.[630] Er hat diesbezüglich entschieden, dass das primäre Gemeinschaftsrecht regelmäßig direkte Anwendung findet. Später übertrug er diesen Grundsatz der unmittelbaren Anwendbarkeit des Primärrechts auch auf das sekundäre Recht des EGV.[631] Die unmittelbare Anwendbarkeit des Gemeinschaftsrechts („effet direct“) bedeutet, dass sich jeder Gemeinschaftsbürger vor einem nationalen Gericht direkt auf die jeweilige

---

625 Hamann, „Der Entwurf einer E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290, 295.

626 Als die vier „Grundfreiheiten“ des EGV (vgl. insoweit Art. 3 I c und 14 II EGV) werden die Gewährleistungen
- des freien Warenverkehrs (Art. 23 ff. EGV),
- des freien Personenverkehrs (Art. 39 ff. bzw. 43 ff. EGV),
- des freien Dienstleistungsverkehrs (Art. 49 ff. EGV) und
- des freien Kapitalverkehrs (56 ff. EGV)

wegen ihrer konstituierenden Bedeutung für die freien Verkehrsströme und insbesondere für den freien Wirtschaftsverkehr bezeichnet. Denn wie sich aus Art. 14 II EGV ergibt, besteht das primäre Ziel des EGV in der Schaffung eines gemeinschaftlichen Binnenmarktes, der durch einen Raum ohne Binnengrenzen mit einem freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gekennzeichnet ist. In enger Verbindung zu den oben genannten vier Grundfreiheiten steht die Sicherung des freien Zahlungsverkehrs, die manchmal auch als fünfte Grundfreiheit angesehen wird. Die Freiheit des Personenverkehrs lässt sich darüber hinaus in die Freizügigkeit der Arbeitnehmer und die unternehmerische Niederlassungsfreiheit untergliedern.

627 Vgl. hierzu auch unten unter B. 3. Teil. 3. Kapitel. II. 1. a.

628 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 189.

629 So zum Beispiel: EuGH, Rs. 2/74, 21.06.1974, Slg. 1974, 631, 649 ff. Rdnr. 1 ff. (Reyners).

630 EuGH, Rs. 26/62, 05.02.1963, Slg. 1963, 3, 8 ff. Rdnr. 1 ff. (Van Gend & Loos).

631 EuGH, Rs. C-6/90 und C-9/90, 19.11.1991, Slg. 1991, I-5357, 5405 ff. Rdnr. 1 ff. (Francovich).

Gemeinschaftsvorschrift berufen kann, ohne dass ein nationaler Transformationsakt notwendig wäre.[632] Denn durch das Gemeinschaftsrecht in Form des EGV, des EAGV sowie des EGKSV ist eine eigenständige Rechtsordnung geschaffen worden, die nicht nur für die Mitgliedstaaten gilt, sondern auch für den Einzelnen unmittelbare Rechte und Pflichten begründet.[633] Entscheidend ist dabei, dass die Mitgliedstaaten den drei Gemeinschaften Hoheitsrechte übertragen haben und dadurch den Gemeinschaftsorganen erlauben, an ihrer Stelle Regelungsgewalt auch gegenüber dem Einzelnen auszuüben.[634] Aufgrund dieser Übertragung von Gesetzgebungskompetenz der jeweiligen Mitgliedstaaten auf die supranationale Organisation EG[635] hat nämlich der EGV – was seine unmittelbare Anwendbarkeit betrifft – die gleiche Qualität wie das nationale Recht.[636] Folglich können unmittelbar anwendbare Bestimmungen auch bestehenden Gesetzen und sonstigen nationalen Rechtsakten entgegengehalten werden.[637]

d. Anwendungsvorrang des Gemeinschaftsrechts

Nachdem der EuGH die unmittelbare Anwendung des Gemeinschaftsrechts bejaht hatte, musste er sich zwangsläufig mit der – früher sehr umstrittenen[638] – Frage beschäftigen, wie das Verhältnis des Europarechts zum nationalen Recht zu verstehen ist.[639] Denn durch die direkte Anwendung des EGV entstand in bestimmten Rechtsgebieten eine Kollision mit den nationalen Vorschriften.[640] Mittlerweile ist dieses Thema weitgehend geklärt: Es hat sich die Meinung des sogenannten „Anwendungsvorrangs“[641] durchgesetzt.[642] Demzufolge beansprucht das Gemeinschaftsrecht für sich den Vorrang vor dem nationalen Recht, wenn und soweit gleiche Regelungsinhalte betroffen sind. So hat der EuGH entschieden, dass das Gemeinschaftsrecht eine eigene Rechtsordnung darstellt, die bewusst von den Mitgliedstaaten unter Aufgabe bestimmter Souveränitätsrechte geschaffen worden ist.[643] Bestehende innerstaatliche Rechtsvorschriften, die dem Ge-

---

632 Kingreen, „Die Gemeinschaftsgrundrechte“, JuS 2000, 857, 858; Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, S. 67.

633 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, S. 67.

634 Herdegen, Europarecht, 2. Auflage, § 1 Rdnr. 4.

635 In Deutschland ist diese Kompetenz-Übertragung in Art. 24 I bzw. 23 I n. F. GG fixiert.

636 Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 533 f. und 1160.

637 Herdegen, Europarecht, 2. Auflage, § 9 Rdnr. 167.

638 Vgl. insoweit die weitergehenden Ausführungen in Bleckmann, Europarecht, 6. Auflage, § 11 Rdnr. 1070 ff.

639 EuGH, Rs. 6/64, 15.07.1964, Slg. 1964, 1251, 1260 ff. Rdnr. 1 ff. (Costa/ENEL); EuGH, Rs. 106/77, 09.03.1978, Slg. 1978, 629, 643 ff. Rdnr. 13 ff. (Simmenthal); EuGH, Rs. 249/85, 21.05.1987, Slg. 1987, 2345, 2355 ff. Rdnr. 1 ff. (Albako).

640 Bleckmann, Europarecht, 6. Auflage, § 11 Rdnr. 1090.

641 Oft wird in diesem Zusammenhang auch der französische Ausdruck: „primauté du droit communautaire“ verwendet.

642 Paulweber, „Europäische Telekommunikationspolitik an der Schwelle zum 21. Jahrhundert“, ZUM 2000, 11, 35; Kingreen, „Die Gemeinschaftsgrundrechte“, JuS 2000, 857, 858; Streinz, Europarecht, 4. Auflage, § 3 Rdnr. 179.

643 EuGH, Rs. 6/64, 15.07.1964, Slg. 1964, 1251, 1269 f. (Costa/ENEL):

meinschaftsrecht widersprechen, dürfen daher in einem konkreten Fall nicht angewendet werden, da das Gemeinschaftsrecht hierfür Vorrang besitzt.[644] Gemeint ist damit allerdings nur ein Anwendungs- und kein – Nichtigkeit bedeutender – normenhierarchischer Geltungsvorrang. Denn dem Primat des Gemeinschaftsrechts wird schon mit einem schlichten Anwendungsvorrang im Einzelfall Genüge getan. Gleichzeitig ist nicht einzusehen, weshalb nationale Regelungen, die allgemein Sachverhalte mit Auslandsbeziehung betreffen, bei einem Verstoß gegen das Gemeinschaftsrecht unwirksam werden, obwohl sie im Hinblick auf Drittstaaten und Drittstaatsangehörige unbedenklich sind.[645] Schließlich kann durch eine Änderung des Gemeinschaftsrechts die ursprüngliche Kollision zwischen dem gemeinschaftlichen und nationalen Recht wegfallen, so dass die nationale Vorschrift ihre regelnde Wirkung wieder entfalten muss.[646]

Der beschriebene Anwendungsvorrang des Gemeinschaftsrechts gilt nach Meinung des EuGH auch gegenüber nationalem Verfassungsrecht.[647] Problematisch ist jedoch, dass das BVerfG in verschiedenen Urteilen unterschiedliche Ansichten zu diesem Thema vertreten hatte und sich bis heute noch nicht gänzlich der Meinung des EuGH angeschlossen hat:

Exkurs: Die Entwicklung der Rechtsprechung des BVerfG zum Verhältnis des deutschen Verfassungsrechts gegenüber dem gemeinschaftlichen Europarecht

Zwar bejahte das BVerfG ursprünglich im Zuge der Costa/ENEL-Entscheidung des EuGH[648] einen generellen Anwendungsvorrang des Gemeinschaftsrechts.[649] Mit seinem berühmten „Solange-I-Beschluss“[650] revidierte es allerdings seine Meinung und stellte klar, dass zwar grundsätzlich von ei-

---

„Zum Unterschied von gewöhnlichen internationalen Verträgen hat der EWG-Vertrag eine eigene Rechtsordnung geschaffen, die bei seinem Inkrafttreten in die Rechtsordnungen der Mitgliedstaaten aufgenommen worden und von ihren Gerichten anzuwenden ist. Denn durch die Gründung einer Gemeinschaft für unbegrenzte Zeit, die mit eigenen Organen, mit der Rechts- und Geschäftsfähigkeit, mit internationaler Handlungsfähigkeit und insbesondere mit echten, aus der Beschränkung der Zuständigkeit der Mitgliedstaaten oder der Übertragung von Hoheitsrechten der Mitgliedstaaten auf die Gemeinschaft herrührenden Hoheitsrechten ausgestattet ist, haben die Mitgliedstaaten, wenn auch auf einem sehr begrenzten Gebiet, ihre Souveränitätsrechte beschränkt und so einen Rechtskörper geschaffen, der für ihre Angehörigen und sie selbst verbindlich ist.

[...]

Der Vorrang des Gemeinschaftsrechts wird auch durch Artikel 189 (mittlerweile Art. 249 n. F. EGV Anm. d. Verf.) bestätigt; ihm zufolge ist die Verordnung „verbindlich“ und „gilt unmittelbar in jedem Mitgliedstaat“. Diese Bestimmung, die durch nichts eingeschränkt wird, wäre ohne Bedeutung, wenn die Mitgliedstaaten sie durch Gesetzgebungsakte, die den gemeinschaftsrechtlichen Normen vorgingen, einseitig ihrer Wirksamkeit berauben könnten.“

644 Schweitzer/Hummer, Europarecht, 5. Auflage, § 10 Rdnr. 849 ff.

645 Streinz, Europarecht, 4. Auflage, § 3 Rdnr. 200.

646 Herdegen, Europarecht, 2. Auflage, § 11 Rdnr. 230.

647 EuGH, Rs. 106/77, 09.03.1978, Slg. 1978, 629, 643 ff. Rdnr. 13 ff. (Simmenthal).

648 EuGH, Rs. 6/64, 15.07.1964, Slg. 1964, 1251, 1260 ff. Rdnr. 1 ff. (Costa/ENEL).

649 BVerfGE 22, 293, 296 f.; BVerfGE 31, 145, 173 f.

650 Leitsatz in BVerfGE 37, 271:

„Solange der Integrationsprozess der Gemeinschaft nicht so weit fortgeschritten ist, dass das Gemeinschaftsrecht auch einen von einem Parlament beschlossenen und in Geltung stehenden formulierten Katalog von Grundrechten enthält, der dem Grundrechtskatalog des Grundgesetzes adäquat

nem Vorrang des Gemeinschaftsrecht auszugehen ist, dieser Vorrang jedoch seine Grenzen in den Grundrechten des Grundgesetzes (GG) finden soll.[651] Denn im Rahmen der Kompetenzübertragung nach Art. 24 I bzw. 23 I n.F. GG sei die Grundstruktur der Verfassung vor der Übertragung geschützt. Zu der Grundstruktur sind gemäß der Ansicht des BVerfG zum einen die in Art. 79 III GG geschützten Bereiche und auch die Grundrechte zu zählen. Insoweit könne deshalb der Grundsatz des Anwendungsvorrangs keine Wirkung entfalten. Erst wenn ein vom Europäischen Parlament beschlossener formeller Grundrechtskatalog existieren würde, besäße das BVerfG keine Entscheidungskompetenz mehr, so dass dann das Gemeinschaftsrecht auch gegenüber der gesamten deutschen Verfassung Vorrang besitzen würde.

Im „Solange-II-Beschluss“[652] vollzog das BVerfG allerdings eine Kehrtwende. In dieser Entscheidung wiederholte zunächst das BVerfG seine Aussage zum Solange-I-Beschluss, dass die Ermächtigung zur Übertragung von Hoheitsrechten gemäß Art. 24 I bzw. 23 I n. F. GG durch die Grundstruktur der Verfassung begrenzt sei. Überraschend war jedoch an diesem Beschluss, dass das BVerfG den Europäischen Gemeinschaften einen mittlerweile generell angemessenen Grundrechtsschutz attestierte. Des weiteren kam es von seiner Forderung nach einer völligen Adäquanz des Grundrechtsschutzes und nach einem kodifizierten Grundrechtskatalog auf Gemeinschaftsebene ab. Ihm genügte jetzt, dass generell ein Mindeststandard an inhaltlichem Grundrechtsschutz gewährleistet sei, der den verfassungsrechtlichen Anforderungen des Grundgesetzes prinzipiell entspreche. Als Konsequenz aus dieser Entwicklung lehnte das BVerfG seine Kompetenz, soweit es das abgeleitete Gemeinschaftsrecht anbelangt, ab. Demzufolge ist indirekt ein Anwendungsvorrang des Gemeinschaftsrechts auch hinsichtlich des Verfassungsrechts vom BVerfG bejaht worden.

Diese Rechtsposition des BVerfG wurde allerdings mit dem „Maastricht-Urteil“[653] wieder relativiert. In dieser Entscheidung nimmt das Gericht erneut seine Zuständigkeit an und zwar hinsichtlich des

---

ist, ist nach Einholung der in Art. 177 des Vertrages (mittlerweile Art. 234 EGV Anm. d. Verf.) geforderten Entscheidung des Europäischen Gerichtshofs die Vorlage eines Gerichts der Bundesrepublik Deutschland an das Bundesverfassungsgericht im Normenkontrollverfahren zulässig und geboten, wenn das Gericht die für es entscheidungserhebliche Vorschrift des Gemeinschaftsrechts in der vom Europäischen Gerichtshof gegebenen Auslegung für unanwendbar hält, weil und soweit es mit einem der Grundrechte des Grundgesetzes kollidiert.“

651 Schweitzer/Hummer, Europarecht, 5. Auflage, § 10 Rdnr. 856.

652 BVerfGE 73, 339, 387:
„Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz unabdingbar gebotenen Grundrechtsschutz im wesentlichen gleichzuachten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleiteten Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte oder Behörden im Hoheitsgebiet der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen; entsprechende Vorlagen nach Art. 100 Abs. 1 GG sind somit unzulässig.“

653 7. Leitsatz in BVerfGE 89, 155, 156:
„Auch Akte einer besonderen, von der Staatsgewalt der Mitgliedstaaten geschiedenen öffentlichen Gewalt einer supranationalen Organisation betreffen die Grundrechtsberechtigten in Deutschland. Sie berühren damit die Gewährleistungen des Grundgesetzes und die Aufgaben des Bundesverfassungsgerichtes, die den Grundrechtsschutz in Deutschland insoweit nicht nur gegenüber deutschen Staatsorganen zum Gegenstand haben (Abweichung von BVerfGE 58, 1 [27]). Allerdings übt das

> Grundrechtsschutzes gegenüber den Akten von Gemeinschaftsorganen. Jedoch schränkt es seine diesbezügliche Kompetenz wieder ein, indem das BVerfG seine Gerichtsbarkeit lediglich in einem „Kooperationsverhältnis" zum EuGH ausüben will.[654] Dies bedeutet, dass das BVerfG nur dann tätig wird, wenn es der Meinung ist, dass der EuGH in seinen Entscheidungen einen unabdingbaren Grundrechtsstandard nicht gewährleisten kann.[655] Das Gemeinschaftsrecht soll demnach dem nationalen Verfassungsrecht in Form der Grundrechte solange vorgehen, bis das BVerfG zu dem Schluss kommt, dass der EuGH – im Rahmen seines Kooperationsverhältnisses zum BVerfG – einen ausreichenden Grundrechtsschutz nicht mehr bieten kann.

Es lässt sich somit sagen, dass trotz der beschriebenen Entscheidungen des BVerfG der Anwendungsvorrang des Gemeinschaftsrechts selbst gegenüber dem deutschen Verfassungsrecht gilt, allerdings mit dem Vorbehalt aus dem Maastricht-Urteil.

e. Beachtlichkeit des Europarechts für staatliche Behörden

Wie bereits oben angesprochen,[656] stellen die staatlichen Kontrollmaßnahmen VAe dar. Das hier zu prüfende Gemeinschaftsrecht muss demnach auf die vorliegende Form staatlichen Handelns anwendbar sein. Nur dann besteht überhaupt eine Möglichkeit, dass die Kontrollmaßnahmen mit dem Europarecht zu vereinbaren oder nicht zu vereinbaren sind.

Die Frage, inwieweit staatliche Behörden die Vorschriften des EGV zu beachten haben, wird in Art. 10 EGV geregelt: Art. 10 I 1 EGV bestimmt, dass die Mitgliedstaaten „*alle geeigneten Maßnahmen allgemeiner oder besonderer Art zur Erfüllung der Verpflichtungen, die sich aus diesem Vertrag oder aus Handlungen der Organe der Gemeinschaft ergeben*", treffen müssen. Art. 10 EGV enthält insoweit den sogenannten „Grundsatz der Gemeinschaftstreue".[657] Gemeint ist damit, dass die Mitgliedstaaten vor allem das sich aus dem EGV ergebende primäre und sekundäre Gemeinschaftsrecht vertragskonform auf legislativer, administrativer und judikativer Ebene auszuführen haben.[658] Art. 10 I EGV nennt als Adressaten für die Vorschriften des EGV nur ganz allgemein „die Mitgliedstaaten". Dies darf aber nicht dazu führen, dass unter diesen Rechtsbegriff nur die jeweiligen Regierungen der einzelnen Mitgliedstaaten gefasst werden. Vielmehr muss der Begriff des Mitgliedstaats weit ausgelegt werden. Nach der Rechtsprechung des EuGH sind damit die Mitgliedstaaten mit sämtlichen Trägern öffentlicher Gewalt gemeint, ungeachtet dessen, ob diese zur Legislative, Exekutive oder

---

Bundesverfassungsgericht seine Rechtsprechung über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht in Deutschland in einem „Kooperationsverhältnis" zum Europäischen Gerichtshof aus."

654 Schweitzer/Hummer, Europarecht, 5. Auflage, § 10 Rdnr. 866.

655 Insbesondere bei offensichtlichen Kompetenzüberschreitungen der europäischen Organe (einschließlich des EuGH) muss dies angenommen werden. Vgl. Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 66.

656 Vgl. oben unter B. 3. Teil. 1. Kapitel. I.

657 Vgl. hierzu ausführlich: Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 707 ff.

658 Kahl in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 10 Rdnr. 13.

Judikative gehören.[659] Auch die Länder, Regionen und sonstige Gebietskörperschaften sowie verselbständigte Verwaltungseinheiten sind unmittelbar dem Art. 10 EGV und folglich dem Primär- sowie Sekundärrecht des EGV unterworfen.[660]
Demnach haben die jeweiligen Polizei- und Sicherheitsbehörden der Länder sowie die nach dem MDStV zuständigen Behörden gemäß Art. 10 EGV bei jedem verwaltungsrechtlichen Handeln die sich aus dem EGV ergebenden Regelungen zu beachten.[661] Behördliche Anordnungen – auch die in Form eines VAs – dürfen somit grundsätzlich aufgrund des Prinzips der Gemeinschaftstreue nur ergehen, wenn sie nicht mit dem primären und sekundären Gemeinschaftsrecht kollidieren.[662]

f. Zusammenfassung

Das europäische Gemeinschaftsrecht ist aufgrund seiner unmittelbaren Wirkung und seinem Anwendungsvorrang regelmäßig immer dann auf staatliche Handlungen anwendbar, wenn ein bestimmter Sachverhalt die Voraussetzungen der jeweiligen europarechtlichen Tatbestände erfüllt, sei es nun primäres oder sekundäres Gemeinschaftsrecht.
Im folgenden soll nun zunächst die Vereinbarkeit der staatlichen Kontrollmaßnahmen mit dem primären und im Anschluss daran mit dem sekundären Gemeinschaftsrecht untersucht werden.

---

659 Vgl. EuGH, Rs. 71/76, 28.04.1977, Slg. 1977, 765, 777 Rdnr. 15/18 (Thieffry); EuGH, Rs. 14/83, 10.04.1984, Slg. 1984, 1891, 1905 Rdnr. 26 (Von Colson und Kamann); EuGH, Rs. C-91/92, 14.07.1994, Slg. 1994, I-3325, 3357 Rdnr. 26 (Faccini Dori).

660 Zulegg, „Der rechtliche Zusammenhalt der Europäischen Gemeinschaft“, ZEuP 1993, 475, 479.

661 Bleckmann, Europarecht, 6. Auflage, § 14 Rdnr. 1319.

662 Eng mit dem Grundsatz der Gemeinschaftstreue verknüpft ist der sogenannte „Effektivitätsgrundsatz“ („effet utile“). Das Effektivitätsprinzip, das der Europäische Gerichtshof (EuGH) in mehreren Entscheidungen entwickelt hat, besagt, dass die nationalen Gerichte und Behörden den Normen des Gemeinschaftsrechts optimale Wirkungskraft verschaffen müssen, damit eine effektive Durchsetzung des Gemeinschaftsrechts ermöglicht wird. Gemeint ist hier insbesondere eine europafreundliche Auslegung bei der Anwendung des nationalen Rechts sowie des Gemeinschaftsrechts. Vgl. EuGH, Rs. 9/70, 06.10.1970, Slg. 1970, 825, 838 Rdnr. 5 (Grad, sog. „Leberpfennig“); EuGH, verbundene Rs. C-46/93 und C-48/93, 05.03.1996, Slg. 1996, I-1029, 1134 ff. Rdnr. 1 ff. (Brasserie du Pecheur und Factortame); Borchardt in: Lenz (Hrsg.), EG-Vertrag Kommentar, 2. Auflage, Art. 220 Rdnr. 18; Koenig/Haratsch, Europarecht, 2. Auflage, S. 30 Rdnr. 64 und S. 122 Rdnr. 278; Pechstein/Koenig, Die Europäische Union, 3. Auflage, S. 137 Rdnr. 249 f.; Herdegen, Europarecht, 2. Auflage, § 9 Rdnr. 184; Oppermann, Europarecht, § 6 Rdnr. 549.

2. Kapitel: Vereinbarkeit von staatlichen Kontrollmaßnahmen mit dem primären Gemeinschaftsrecht

I. Eingrenzung

Wie bereits ausgeführt wurde,[663] ist von den einzelnen Rechtsgebieten des primären Gemeinschaftsrechts nur der EGV für die staatlichen Kontrollmaßnahmen von rechtlicher Relevanz. Aber auch der EGV selbst muss wiederum bezüglich seiner Anwendbarkeit auf die Kontrollmaßnahmen im Internet eingeschränkt werden. Denn bei näherer Betrachtung des EGV gibt es dort nur wenige Normen, die für staatliche Kontrollmaßnahmen bedeutsam werden können. Hierzu zählen insbesondere die sogenannten „Grundfreiheiten" des EGV[664] und die mit ihnen im Zusammenhang stehenden Vorschriften. Alle übrigen Normen des EGV sind hingegen für die vorliegende Arbeit von keinem oder nur geringem Interesse. Dies hat zur Folge, dass die staatlichen Kontrollmaßnahmen lediglich dahingehend überprüft werden müssen, ob sie mit den Grundfreiheiten (Waren-, Personen-, Dienstleistungs- bzw. Kapitalverkehrsfreiheit) des EGV zu vereinbaren sind. Dabei spielen die Freiheit des Kapital- und Zahlungsverkehrs (Art. 56 ff EGV) sowie die Arbeitnehmerfreizügigkeit (Art. 39 ff EGV) für die staatlichen Kontrollmaßnahmen keine besondere Rolle, so dass auf diese Bereiche der Grundfreiheiten nur dann eingegangen wird, wenn dies erforderlich ist. Aus primärrechtlicher Sicht sind für die behördlichen Sperr- und/oder Löschanordnungen also vor allem die Warenverkehrsfreiheit (Art. 28 f. EGV), die Niederlassungsfreiheit (Art. 43 EGV) und die Dienstleistungsfreiheit (Art. 49 EGV) von großer Bedeutung.

II. Grenzüberschreitender Sachverhalt

Werden die Vorschriften dieser Grundfreiheiten näher betrachtet, dann lässt sich aus den Art. 28 f. EGV („*zwischen den Mitgliedstaaten*"), 43 EGV („*Staatsangehörigen eines Mitgliedstaates im Hoheitsgebiet eines anderen Mitgliedstaats*") und 49 EGV („*für Angehörige der Mitgliedstaaten, die in einem anderen Staat der Gemeinschaft als demjenigen des Leistungsempfängers ansässig sind*") entnehmen, dass für die Anwendbarkeit der Waren-, Niederlassungs-, und Dienstleistungsfreiheit grundsätzlich ein sogenannter „grenzüberschreitender Sachverhalt" nötig ist. Mit diesem Begriff ist gemeint, dass es sich um keinen rein innerstaatlichen Sachverhalt handeln darf. Auch ein grenzüberschreitender Sachverhalt, bei dem lediglich Drittstaaten[665] involviert sind,

---

663 Vgl. oben unter B. 3. Teil. 1. Kapitel. II. 1. und 2. a. und b.

664 Vgl. oben unter B. 3. Teil. 1. Kapitel. II. 2. b.

665 Drittstaaten sind alle außereuropäischen Länder, die nicht der EU angehören. Eine besondere Stellung besitzen diejenigen Drittstaaten, die zwar keine Mitgliedstaaten der EU sind, die jedoch ein Assoziations- oder Kooperationsabkommen mit der EU geschlossen haben. Vgl. insoweit Art. 171 und Art. 182 EGV.

genügt hierfür nicht. Also muss zunächst festgestellt werden, wann überhaupt bei den staatlichen Kontrollmaßnahmen ein grenzüberschreitender Sachverhalt vorstellbar ist. Denn nur dann können regelmäßig die Vorschriften über die Grundfreiheiten des EGV angewendet werden.

Da sich das Internet gerade dadurch auszeichnet, dass es sich um ein grenzüberschreitendes Medium handelt, kommen zahlreiche Fallkonstellationen in Frage, wo ein grenzüberschreitender Sachverhalt bejaht werden könnte. Neben einer Vielzahl an denkbaren Fallvarianten muss zudem berücksichtigt werden, dass im Internet – abgesehen vom Nutzer – unterschiedliche Provider (der Network-, der Content-, der Service- sowie der Access-Provider) ihre Dienste anbieten. Je nachdem, gegenüber welchem Provider die staatlichen Kontrollmaßnahmen ergehen und welche Personen hiervon im Internet betroffen sein können, ergeben sich damit diverse Fall- und Unterfallgestaltungen.

Um eine übersichtliche Darstellung zu gewährleisten, ist es deshalb ratsam, die jeweils denkbaren Fallkonstellationen zunächst bei jedem Provider separat aufzuzeigen. Dadurch können bereits im Vorfeld einige rein innerstaatliche Fallvarianten oder Fallgestaltungen mit Bezug zu einem Drittstaat, auf welche die Grundfreiheiten des EGV keine Anwendung finden, ausgeschieden werden. Gleichzeitig soll veranschaulicht werden, welche Fallgestaltungen überhaupt möglich sind. Im Anschluss an diese grobe Aufteilung wird eine übersichtliche, detaillierte Überprüfung der einzelnen europarechtlich relevanten Fallvarianten durchgeführt.

III. Überblick über die möglichen europarechtlich relevanten Fallkonstellationen

1. Beim Network-Provider

Aufgrund der Tatsache, dass der Network-Provider regelmäßig nicht von Sperr- oder Löschanordnungen betroffen ist,[666] gibt es insoweit keine direkten europarechtlichen Berührungspunkte.[667]

2. Beim Content-Provider

Im Gegensatz zum Network-Provider können gegen den Content-Provider staatliche Maßnahmen in Form der Sperr- und/oder Löschanordnung ergehen. Diese richten sich gegen den eigenen rechtswidrigen Inhalt des Content-Providers. Da der Content-

---

666 Beim Network-Provider handelt es sich um einen Telekommunikationsdienst, auf den das TKG Anwendung findet. Staatliche Kontrollmaßnahmen sind im TKG jedoch nicht vorgesehen. Darüber hinaus können schon rein technisch keine Sperrmaßnahmen durchgeführt werden. Vgl. hierzu auch König/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 439 und oben unter B. 1. Teil. III. 1. c. und 2. b. sowie B. 2. Teil. II. 4. c. cc. (1).

667 Allerdings kann der Network-Provider indirekt durch staatliche Maßnahmen gegenüber den anderen Providern europarechtlich tangiert sein. Hierzu vgl. unten unter B. 3. Teil. 2. Kapitel. V. 4.

Provider sowohl aus dem Inland als auch aus dem Ausland stammen kann, sind bei ihm unterschiedliche Fallvarianten denkbar: Es kann sich zunächst um einen deutschen Content-Provider[668] handeln. Bei dieser Fallkonstellation ergeht also eine deutsche Sperr- oder Löschanordnung[669] gegen einen deutschen Content-Provider und dessen Inhalte im Internet. Dies stellt grundsätzlich einen rein innerdeutschen Sachverhalt dar, so dass europäisches Primärrecht hiervon überhaupt nicht betroffen ist. Der Content-Provider könnte jedoch auch Ausländer sein. Dann ist weiter zu differenzieren, ob es sich um einen ausländischen Content-Provider aus einem anderen Mitgliedstaat der EU handelt oder ob er aus einem Drittstaat stammt. Ist letzteres der Fall, dann ist grundsätzlich der Anwendungsbereich von Grundfreiheiten des EGV nicht erfüllt.[670] Ist der Content-Provider hingegen EU-Ausländer, d.h. kommt er aus einem anderen Mitgliedstaat, dann kann zumindest ein grenzüberschreitender Sachverhalt und somit eine europarechtliche Relevanz grundsätzlich bejaht werden.

Diese noch relativ überschaubare Unterscheidung anhand der Person des Content-Providers gewinnt jedoch schnell an Komplexität, sobald noch weitere Personen hinzukommen. Insbesondere die Person des Nutzers muss hierbei beachtet werden. Denn da der Content-Provider seine Inhalte bestimmten Nutzern im Netz zur Verfügung stellt, ist der Nutzer Teil des Content-Providings und muss bei den Fallvarianten mitberücksichtigt werden. Der Nutzer kann – genauso wie der Content-Provider – entweder aus dem Inland, aus einem Drittstaat oder aus dem EU-Ausland stammen. Dies hat zur Folge, dass sich selbst bei der zuerst genannten Fallvariante, wenn der Content-Provider Deutscher ist, dann eine europarechtliche Problematik ergeben kann, falls ein Nutzer aus dem EU-Ausland hinzutritt.[671]

3. Beim Service-Provider

Auch gegen den Service-Provider sind Lösch- und/oder Sperrmaßnahmen möglich. Diese richten sich – im Unterschied zum Content-Provider – aber gegen fremde rechtswidrige Inhalte. Beim Service-Provider gibt es deshalb zunächst zwei Parameter: nämlich den Service-Provider selbst und den Content-Provider, der seinen Inhalt vom Service-Provider im Internet bereithalten lässt. Wie bei der Person des Content-Providers muss auch beim Service-Provider danach gefragt werden, welche Nationalität er besitzt. Handelt es sich beim Service-Provider um einen deutschen Internet-Dienst oder stammt er

---

668 Wann ein Provider als deutsch, aus einem Drittstaat oder aus dem EU-Ausland anzusehen ist, wird unter B. 3. Teil. 2. Kapitel. IV. 2. und 3. ausführlich behandelt.

669 Als deutsche Kontrollmaßnahmen sind die Sperr- und/oder Löschanordnungen zu verstehen, welche von der jeweils zuständigen Polizei- oder Sicherheitsbehörde der Länder angeordnet werden.

670 Wie bereits erwähnt wurde, ist auf Drittstaaten der EGV nicht anwendbar. Lediglich über bestimmte Assoziierungsabkommen zwischen der EU und diversen Drittstaaten besteht die Möglichkeit, dass Teilbereiche des EGV auch für Drittstaaten gelten. Vgl. hierzu Martenczuk/Zimmermann in: Schwarze (Hrsg.), EU-Kommentar, Art. 181 und Art. 182 EGV.

671 Hierzu ausführlich unten unter B. 3. Teil. 2. Kapitel. V. 1. c.

aus einem Drittstaat, dann ist zunächst das Europarecht durch ihn nicht betroffen. Allein die staatlichen Kontrollmaßnahmen gegen den Service-Provider aus einem anderen Mitgliedstaat der EU tangieren unmittelbar die Grundfreiheiten des EGV, da es sich hierbei um einen grenzüberschreitenden Sachverhalt handelt.

Aber auch der Content-Provider selbst, der seinen Inhalt vom Service-Provider speichern lässt, besitzt möglicherweise europarechtliche Relevanz.[672] Denn der fremde rechtswidrige Inhalt kann von unterschiedlichen Personen in das Internet eingespeist worden sein. Es muss hier ebenfalls danach gefragt werden, welchem Land der Content-Provider zuzuordnen ist. Stammt der Inhalt von einem deutschen Content-Provider, dann wird das Europarecht bei einer Lösch- und/oder Sperranordnung dieses Inhalts in der Regel nicht berührt. Das Gleiche gilt, wenn der Inhalt von einer Person aus einem Drittstaat herrührt. Europarechtlich interessant sind somit die Fälle, in denen der fremde Inhalt von einem EU-Ausländer stammt.

Schließlich muss erneut die Person des Nutzers betrachtet werden, die ebenfalls entweder dem Inland oder (EU-)Ausland zuzurechnen ist.

4. Beim Access-Provider

Wie bereits ausgeführt wurde, sind gegenüber dem Access-Provider lediglich Sperranordnungen möglich.[673] Der Access-Provider kann, neben der Möglichkeit dass er Deutscher oder Angehöriger eines Drittstaates ist, auch aus dem EU-Ausland stammen. Dieser Umstand könnte dann das Europarecht tangieren. Des weiteren hängt eine europarechtliche Relevanz davon ab, welcher Zugang an sich gesperrt werden soll. Befindet sich der rechtswidrige Inhalt des Content-Providers,[674] zu dem der Zugang gesperrt wird, in Deutschland, im EU-Ausland oder in einem Drittstaat? Für den Fall, dass der fragliche Inhalt in einem anderen Mitgliedstaat der EU angeboten wird, wäre das Europarecht betroffen, da bei einer Sperrung ein grenzüberschreitender Sachverhalt vorliegen würde.

Schließlich spielt ebenfalls der Nutzer eine entscheidende Rolle, der sich über den Access-Provider in das Internet einwählt und sich von ihm den Zugang zu den gewünschten Daten des Content-Providers vermitteln lässt. Je nachdem, ob er aus dem Inland oder (EU-) Ausland kommt, ergeben sich hierdurch zusätzliche unterschiedliche Fallvarianten.

5. Zusammenfassung

Aus den vorangegangenen Überlegungen wird deutlich, dass das Europarecht immer dann zu prüfen ist, wenn zumindest ein Provider aus einem Mitgliedstaat der EU stammt. Sämtliche Fallkonstellationen, bei denen sowohl der Inhalt des Content-

---

672 Vgl. hierzu auch die vorstehenden Ausführungen.

673 Siehe insoweit oben unter B. 1. Teil. III. 1. d.

674 Dieser Inhalt könnte natürlich wiederum bei einem Service-Provider gespeichert sein.

Providers als auch die übrigen Provider einem Drittstaat zugerechnet werden müssen, sind für die vorliegende Arbeit irrelevant, da insofern kein Europarecht betroffen ist. Das Gleiche gilt für die Varianten, bei denen es sich lediglich um deutsche Provider handelt. Hier liegt ein rein innerstaatlicher Vorgang vor, auf den die Grundfreiheiten des EGV keine Anwendung finden. Auf diese rein innerstaatlichen Fälle sowie die Fälle mit ausschließlicher Beteiligung von Personen aus Drittstaaten soll deshalb nicht mehr eingegangen werden.

Wenngleich durch die unterschiedlichen Möglichkeiten der einzelnen Provider bereits ein hohes Maß an Komplexität erreicht ist, wird die Anzahl der europarechtlich relevanten Fallgestaltungen noch einmal dadurch erhöht, dass auch der Nutzer des Internets einerseits Deutscher, EU-Ausländer oder Staatsangehöriger eines Drittstaates sein kann. Folglich werden für jeden Provider drei weitere Fallvarianten eröffnet, weil ein zusätzlicher Parameter hinzugetreten ist.

Insgesamt gibt es demnach, obwohl einige Fallvarianten bereits von der Bearbeitung mangels europarechtlicher Relevanz herausgenommen worden sind, zahlreiche Konstellationen mit staatlichen Kontrollmaßnahmen, für die das Europarecht geprüft werden muss. Die Untersuchung jeder dieser Fallvarianten anhand des Europarechts soll nun im folgenden stattfinden.

IV. Vorfragen

Bevor allerdings auf die einzelnen Provider und deren Fallvarianten eingegangen werden kann, müssen bestimmte Vorfragen angesprochen und geklärt werden, um eine verständliche europarechtliche Prüfung gewährleisten zu können.

Bei den folgenden Überlegungen handelt es sich um allgemeine Rechtsfragen, die für die Unterscheidung zwischen den Providern und deren Fallvarianten von grundsätzlicher Bedeutung sind:

1. Territorialitätsprinzip

So muss zunächst geprüft werden, wie sich die deutsche Rechtsordnung gegenüber ausländischen Personen verhält. Weil es sich bei den staatlichen Kontrollmaßnahmen um öffentlich-rechtliche Sachverhalte handelt, interessiert hier lediglich das öffentliche Recht.

Durch Überschreiten der deutschen Grenze begeben sich ausländische Personen in das Hoheitsgebiet der Bundesrepublik Deutschland und somit in seinen Rechtskreis. Nach dem Grundsatz der Gebietshoheit, dem sogenannten „Territorialitätsprinzip“[675], deckt

---

675 Vgl. hierzu auch Schack, „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet“, MMR 2000, 59, 62 und dessen Kritik an dem Territorialitätsprinzip.

sich im allgemeinen der räumliche und persönliche Geltungsbereich eines Gesetzes mit dem Zuständigkeitsbereich des gesetzgebenden Hoheitsträgers.[676] Danach richten sich die Rechtsnormen regelmäßig an alle, die es im territorialen Geltungsbereich angeht. Dies gilt ohne Rücksicht auf Wohnsitz, Nationalität oder Art des Rechtssubjekts. So verpflichten beispielsweise Normen des Landespolizeirechts Ausländer in gleicher Weise wie Inländer.[677] Folglich sind sämtliche Normen des öffentlichen Rechts aufgrund des Territorialitätsprinzips in der Regel auch auf ausländische Provider in Deutschland anwendbar. Staatliche Kontrollmaßnahmen, die gegen ausländische Provider im Inland ergehen, sind also zulässig, da sie sich in die deutsche Rechtsordnung begeben haben.
Diese grundsätzliche Anwendbarkeit des deutschen Rechts könnte jedoch durch sekundäres Gemeinschaftsrecht eingeschränkt sein:

a. Fernsehrichtlinie

Eine Einschränkung könnte sich aus Art. 2 I und 3 II EG-Fernsehrichtlinie 1989[678] sowie der Rechtsprechung des EuGH hinsichtlich der Auslegung des Begriffs „Rechtshoheit" i.S.d. Art. 2 I der EG-Fernsehrichtlinie ergeben.[679] Denn in Art. 2 I Fernsehrichtlinie 1989 wurden die Mitgliedstaaten dazu verpflichtet, bei den ihrer „*Rechtshoheit unterworfenen Fernsehveranstaltern*" für die Einhaltung in den von der Richtlinie erfassten Sendungen zu sorgen. Ziel dieser Regelung war es, ein System der Kontrolle gegenüber den Fernsehveranstaltern durch jeweils einen einzigen Mitgliedstaat, den sogenannten „Sendestaat", zu errichten. Dieses in Art. 2 I, 3 II Fernsehrichtlinie 1989 festgelegte „Sendestaatsprinzip"[680] besagt, dass der jeweilige Sendestaat dafür verantwortlich ist, dass Fernsehsendungen oder Veranstalter, die seiner Rechtshoheit unterworfen sind, dem innerstaatlichen Rundfunkrecht entsprechen und diese Veranstalter die Bestimmungen der Richtlinie einhalten.[681] Der Empfangsstaat kann also seine nationalen Gesetze nicht mehr geltend machen, da für die Fernsehveranstalter ausschließlich das Recht des Sendestaats maßgeblich ist. Wer als Sendestaat anzusehen ist, richtet sich nach Art. 2 I Fernsehrichtlinie 1989. Danach ist grundsätzlich derjenige Mitgliedstaat als Sendestaat zu qualifizieren, der die Rechtshoheit über einen Fernsehveranstalter innehat. Der Begriff der Rechtshoheit wird allerdings in der Richtlinie nicht näher definiert. Die Mitgliedstaaten versuchten diesen Begriff großzügig auszulegen, um möglichst wenig Einfluss auf das nationale Rundfunkwesen zu verlieren. Demgegenüber

---

676 Becker, Grundzüge des öffentlichen Rechts, 7. Auflage, § 3 S. 11.

677 Ossenbühl in: Erichsen/Badura (Hrsg.), Allgemeines Verwaltungsrecht, 11. Auflage, § 8 III S. 191.

678 Richtlinie des Rates 89/552/EWG vom 03.10.1989 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG 1989 Nr. L 298/23.

679 EuGH, Rs. 222/94, 10.09.1996, Slg. 1996, I-4025, 4077 Rdnr. 58 (Kommission/Vereinigtes Königreich); Dörr, „Rechtshoheit über Rundfunkveranstalter im Sinne des EG-Rechts", JuS 1997, 557 f.

680 Vgl. zu diesem Begriff auch Helberger, „Die Konkretisierung des Sendestaatsprinzip in der Rechtsprechung des EuGH", ZUM 1998, 50, 54 f.

681 Greissinger, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie", CR 1999, 112, 113.

waren die Fernsehveranstalter auf eine enge Auslegung bedacht. Denn nur auf diese Weise hätten sie die Vorteile der Richtlinie nutzen und ihre Sendungen in Europa beschränkungsfrei ausstrahlen können, ohne die rundfunkrechtlichen Voraussetzungen der anderen Mitgliedstaaten erfüllen zu müssen. Deshalb hatte sich der EuGH nach dem Inkrafttreten der Fernsehrichtlinie 1989 insbesondere mit der Frage auseinanderzusetzen, welcher Mitgliedstaat im konkreten Fall diese Rechtshoheit auszuüben hat. In der Rechtssache Kommission gegen Vereinigtes Königreich Großbritannien[682] hat der EuGH hierzu entschieden, dass bei mehreren Niederlassungen eines Fernsehveranstalters in verschiedenen Mitgliedstaaten der die Rechtshoheit ausübende Mitgliedstaat derjenige sein müsse, wo der Veranstalter den „Mittelpunkt seiner Tätigkeit" habe und in dem insbesondere „die Entscheidung über die Programmpolitik und die endgültige Zusammenstellung der zu sendenden Programme getroffen würden".[683] Wichtig ist anzumerken, dass der hier vom EuGH verwendete Begriff der Niederlassung nicht mit dem des Art. 43 EGV im Rahmen der Niederlassungsfreiheit deckungsgleich ist. Denn nach dem allgemeinen Niederlassungsbegriff des EGV besteht grundsätzlich die Möglichkeit, dass zwei Mitgliedstaaten für einen Fernsehveranstalter zuständig sind. Gerade dies würde jedoch der Zielsetzung dieser Richtlinie widersprechen, wonach der Fernsehveranstalter ausnahmslos der Rechtshoheit eines Mitgliedstaates unterworfen sein soll.[684] Deshalb wird häufig, um die unterschiedlichen Niederlassungsbegriffe auseinanderhalten zu können, für den vom EuGH zur Fernsehrichtlinie 1989 benutzten Begriff der Niederlassung von einer „qualifizierten Niederlassung" gesprochen.[685] Die Bestimmung der qualifizierten Niederlassung ist deshalb sehr bedeutsam, weil der Fernsehveranstalter sich nur noch dieser Rechtsordnung zu unterwerfen hat. Eine zweite Kontrolle der Sendungen durch die Empfangsstaaten darf nicht mehr stattfinden.[686] Insoweit wird also das ursprüngliche Territorialitätsprinzip aufgehoben. Die nationalen Vorschriften der Empfangsstaaten müssen sich den Vorschriften des Staates beugen, in dem sich die qualifizierte Niederlassung befindet. Dies gilt aber nur für die nationalen Normen, die in den Anwendungsbereich der Fernsehrichtlinie, den sogenannten „koordinierten Bereich", fallen.[687] Zudem sind Ausnahmen denkbar.[688]

---

682 EuGH, Rs. 222/94, 10.09.1996, Slg. 1996, I-4025, 4077 Rdnr. 58 (Kommission/Vereinigtes Königreich).

683 Bröhmer in Callies/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 EGV Rdnr. 14; vgl. auch die Anmerkungen zu dem oben genannten Urteil, EuGH, Rs. 222/94, 10.09.1996, Slg. 1996, I-4025-4083 (Kommission/Vereinigtes Königreich) von Dörr in: JuS 1997, 557 f.

684 Greissinger, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie", CR 1999, 112, 115.

685 Vgl. insoweit Bröhmer in Callies/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 EGV Rdnr. 14.

686 Greissinger, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie", CR 1999, 112, 113.

687 Vgl. hierzu Greissinger, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie", CR 1999, 112, 116 ff.

688 EuGH, verbundene Rs. C-34/95, C-35/95, C-36/95, 09.07.1997, Slg. 1997, I-3843, 3888 Rdnr. 34 (Konsumentenombudsmannen).

Zu beachten ist jedoch, dass die Fernsehrichtlinie nur das Fernsehen im herkömmlichen Sinne und nicht Kommunikationsdienste, die auf individuellen Abruf Informationen oder andere Inhalte übermitteln, also das Internet, umfasst.[689] Eine direkte Anwendung der Fernsehrichtlinie auf das Internet ist demnach nicht möglich. Auch eine analoge Anwendung der Fernsehrichtlinie und der hierzu ergangenen Rechtsprechung des EuGH ist nicht statthaft. Denn entgegen dem Vorschlag des Europäischen Parlaments ist die Fernsehrichtlinie durch die Novellierungsrichtlinie[690] ganz bewusst nicht auf Multimediadienste erweitert worden. Des weiteren gibt es bereits die am 17.07.2000 veröffentlichte E-Commerce-Richtlinie, die das Internet in einem gewissen Rahmen regeln soll.[691] Sie enthält einen wesentlich größeren koordinierten Bereich als die Fernsehrichtlinie in ihrer neuen Fassung. Es besteht also bezüglich des Internets keine Regelungslücke, die durch eine Analogie der Fernsehrichtlinie geschlossen werden müsste.[692] Folglich gibt es keine Möglichkeit, durch die Fernsehrichtlinie eine Anwendung von nationalen Vorschriften auf das Internet einzuschränken.

b. E-Commerce-Richtlinie

Ähnlich wie die Fernsehrichtlinie besitzt auch die E-Commerce-Richtlinie die Gedanken des Sendestaatsprinzips und qualifizierten Niederlassungsbegriffs. Das Sendestaatsprinzip, das auch mit dem allgemeinen Begriff des „Herkunftslandprinzips“ umschrieben wird, ist in Art. 3 I und II ECRL aufgenommen worden.[693] Der qualifizierte Niederlassungsbegriff wird dagegen in der Richtlinie nicht ausdrücklich genannt. Sie definiert in Art. 2 c ECRL lediglich den „*niedergelassenen Diensteanbieter*“. Allerdings wird in Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie auf die oben vorgestellte Rechtsprechung des EuGH zur Niederlassung bei der Fernsehrichtlinie verwiesen.
Aufgrund der Tatsache dass die E-Commerce-Richtlinie von der Bundesrepublik Deutschland mittlerweile umgesetzt worden ist, muss sie hier beachtet werden. Vor allem das Herkunftslandprinzip könnte durch seine Anwendung eine Ausnahme zum Territorialitätsprinzip darstellen, so dass bestimmte Fallgestaltungen nicht mehr vom nationalen Recht erfasst werden.[694] Gemäß Art. 3 I ECRL hat jeder Mitgliedstaat dafür Sorge

---

689 Hesse, „Zur aktuellen Entwicklung des Rundfunkrechts“, BayVBl. 1997, 165, 172; Degenhart, „Rundfunk und Internet“, ZUM 1998, 333, 338.

690 Richtlinie 97/36/EG des Europäischen Parlaments und des Rates vom 30.06.1997 zur Änderung der Richtlinie 89/552/EWG zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG Nr. L 202, 60 ff.

691 Vgl. insoweit unten unter B. 3. Teil. 3. Kapitel. II.

692 Larenz, Methodenlehre der Rechtswissenschaft, 6. Auflage, S. 381 ff.

693 Geis, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen“, CR 1999, 772, 774; weiterführend: Ahrens, „Das Herkunftslandprinzip in der E-Commerce-Richtlinie“, CR 2000, 835 ff.

694 Das Herkunftslandprinzip ist durch die Umsetzung der E-Commerce-Richtlinie in § 4 TDG n.F. erstmalig im deutschen Rechtssystem festgeschrieben worden. Im Gegensatz zur Richtlinie wurden die im Anhang genannten Ausnahmen zu Art. 3 I und II ECRL, auf die in Art. 3 III ECRL verwiesen wird, in § 4 TDG n.F. mit eingearbeitet. Abgesehen von diesem formalen Unterschied hat der deut-

zu tragen, dass „*die Dienste der Informationsgesellschaft, die von einem in seinem Hoheitsgebiet niedergelassenen Diensteanbieter erbracht werden, den in diesem Mitgliedstaat geltenden innerstaatlichen Vorschriften entsprechen, die in den koordinierten Bereich fallen*“. Des weiteren dürfen gemäß § 3 II ECRL die Mitgliedstaaten, „*den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die in den koordinierten Bereich fallen*“. Das Herkunftsland zeichnet sich also dadurch aus, dass der Diensteanbieter nur den rechtlichen Anforderungen des Mitgliedslandes entsprechen muss, wo er niedergelassen ist, und nicht den rechtlichen Anforderungen anderer Mitgliedsländer.[695] Der Vorteil für die Diensteanbieter, der sich hieraus ergibt, liegt auf der Hand: Sie müssen sich nur nach einer Rechtsordnung richten und an eine Aufsichtsbehörde halten.[696] Dies hat auch die Verpflichtung der gegenseitigen Anerkennung der Regelungen und Standards der anderen Mitgliedstaaten zur Folge. Häufig wird in der Literatur deshalb vor einem „Race to the Bottom“[697] gewarnt.[698] Dieser Vorbehalt gegenüber dem Herkunftslandprinzip ist nachvollziehbar und in einem gewissen Maße begründet. Allerdings überwiegt der Vorteil, nämlich ein hohes Maß an Rechtssicherheit, den Nachteil eines möglicherweise eintretenden „Race to the Bottom“.[699] Im übrigen ist das Herkunftslandprinzip ein geeignetes Mittel, den europäischen Gedanken eines Europas gleichberechtigter Nationen voran zu bringen. Denn ohne die Anerkennung und Gleichsetzung der verschiedenen Regelungen in den einzelnen Mitgliedsländern kann ein weiteres Zusammenwachsen der Mitgliedstaaten nicht erfolgen. Wenn bestimmte nationale Regelungen für die Mehrheit der Mitgliedstaaten zu liberal sein sollten, dann muss dies auf zwischenstaatlicher Ebene besprochen und geklärt werden. Insbesondere ein wirksames Arbeiten der

---

sche Gesetzgeber die Vorschrift des Art. 3 ECRL jedoch in § 4 TDG n.F. vollständig übernommen. Vgl. hierzu Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1, 3 und 7.

695 Schack, „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet“, MMR 2000, 59, 62 f.; Geis, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen“, CR 1999, 772, 774; Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 255; Bullinger/Mestmäcker, Multimediadienste, 1997, S. 100 ff.; Mankowski, „Wettbewerbsrechtliches Gerichtspflichtigkeits- und Rechtsanwendungsrisiko bei Werbung über Websites“, CR 2000, 763, 767.

696 Eichhorn, Internet-Recht, S. 52:
„Die Anwendung dieses Rechtsgedankens würde zur Folge haben, dass z.B. die Internet-Verbreitung aus Frankreich von in Deutschland nach § 184 StGB verbotener Pornographie in Deutschland straflos wäre, wenn im Ursprungsland der Sendung, d.h. im Beispiel in Frankreich, diese Pornographie nicht unter Strafe steht.“

697 Gemeint ist damit, dass sich letztendlich die schwächsten Regelungen gegenüber den strengen Regelungen anderer Mitgliedstaaten durchsetzen werden. Strengere Regelungsstandards können dadurch aufgeweicht werden.

698 Lehmann, „Rechtsgeschäfte und Verantwortlichkeit im Netz – Der Richtlinienvorschlag der EU-Kommission“, ZUM 1999, 180; Spindler, „Der neue Vorschlag einer E-Commerce-Richtlinie“, ZUM 1999, 775, 780 ff.; Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 8 mit weiteren Nachweisen; Hamann, „Der Entwurf der E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290, 292.

699 Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 5.

nationalen Behörden und die Durchsetzung der staatlichen Vorschriften tragen wesentlich dazu bei, den anderen Mitgliedstaaten die Angst vor einem „Race to the Bottom“ zu nehmen und als gleichberechtigte Nation in der Staatengemeinschaft akzeptiert zu werden.[700]

Die Diensteanbieter können gemäß dem Herkunftslandprinzip gemeinschaftsweit tätig werden, sofern sie den Regeln ihres Herkunftslands entsprechen, selbst wenn das Mitgliedsland des Nutzers andere Regeln vorsehen sollte. Die Mitgliedstaaten dürfen also den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken, die im koordinierten Bereich der E-Commerce-Richtlinie wurzeln.[701] Dieser Umstand, dass das Herkunftslandsprinzip nur für den in Art. 2 h ECRL definierten koordinierten Bereich gilt, muss besonders beachtet werden. Denn sobald der koordinierte Bereich verlassen wird, kommt es nicht mehr zur Anwendung, sondern es sind wieder die allgemeinen nationalen Anknüpfungsregeln und Normen, die in jedem Mitgliedstaat unterschiedlich ausgestaltet sind, anzuwenden.[702] Besondere Bedeutung hat dies vor allem für die Online-Bestellung von Waren, da die Bestellung noch unter den koordinierten Bereich zu fassen ist, hingegen gemäß Art. 2 h ii) 1. und 2. Spiegelstrich ECRL die Ware selbst und deren Lieferung nicht mehr von ihm betroffen ist.

Im Zusammenhang mit den Einschränkungen des Herkunftslandprinzips müssen auch die in Ziff. 57 der Erwägungsgründe zur E-Commerce-Richtlinie festgehaltenen Grundsätze der Rechtsprechung des EuGH zur Niederlassungsfreiheit genannt werden. Demnach ist ein Mitgliedstaat weiterhin berechtigt, Maßnahmen gegen einen in einem anderen Mitgliedstaat niedergelassenen Diensteanbieter zu ergreifen, falls dessen Tätigkeit ausschließlich oder überwiegend auf das Hoheitsgebiet des ersten Mitgliedstaates ausgerichtet ist und diese Niederlassung gewählt wurde, um die Rechtsvorschriften zu umgehen, die auf den Anbieter Anwendung fänden, wenn er sich im Hoheitsgebiet des ersten Mitgliedstaats niedergelassen hätte.[703] Folglich darf ein Mitgliedstaat trotz des Herkunftslandprinzips Maßnahmen gegen einen Diensteanbieter mit Sitz in einem anderen Mitgliedstaat ergreifen, wenn dessen Tätigkeit allein auf den ersten Mitgliedstaat ausgerichtet ist und die Niederlassung nur zu Umgehungszwecken gewählt wurde. Diese Regelung wirkt nicht nur dem „Race to the Bottom“ entgegen, sondern schränkt richtigerweise das Herkunftslandprinzip ein, da es sich – obwohl sich der Anbieter im EU-

---

700 In Ziff. 22 der Erwägungsgründe zur E-Commerce-Richtlinie wird deshalb festgestellt, dass die Aufsicht über die Dienste der Informationsgesellschaft am Herkunftsort zu erfolgen hat, um einen wirksamen Schutz der Ziele des Allgemeininteresses zu gewährleisten. Deshalb muss dafür gesorgt werden, dass die zuständigen Behörden diesen Schutz nicht allein für die Bürger ihres Landes, sondern für alle Bürger der Gemeinschaft sichern.

701 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 188.

702 Dann gilt wieder das eben beschriebene Territorialitätsprinzip.

703 Vgl. Ziff. 57 der Erwägungsgründe zur E-Commerce-Richtlinie.

Ausland befindet – eigentlich um einen rein innerstaatlichen Sachverhalt handelt. Denn die Tätigkeit des Anbieters hat lediglich Auswirkungen auf einen Mitgliedstaat, der deshalb berechtigt ist, dagegen Regelungen zu treffen. Darüber hinaus gibt es noch weitere Einschränkungen des Herkunftslandprinzips. So gilt die E-Commerce-Richtlinie und somit auch das Herkunftslandsprinzip nicht für Diensteanbieter aus Drittstaaten.[704] Ebenfalls kann das Herkunftslandprinzip keine Wirkungen für die vom Anwendungsbereich der Richtlinie ausgeschlossenen Rechtsgebiete und Bereiche entfalten.
Das Herkunftslandprinzip beeinflusst also die Geltung nationaler Vorschriften im Rahmen des koordinierten Bereichs der E-Commerce-Richtlinie unmittelbar. Das Territorialitätsprinzip kann demnach vom Herkunftslandprinzip gemäß Art. 3 I und II ECRL eingeschränkt werden. Allerdings ist zu beachten, dass die E-Commerce-Richtlinie nicht auf alle Bereiche des Internets Anwendung findet. Des weiteren lässt Art. 3 III und IV ECRL gewisse Ausnahmen zum Herkunftslandprinzip unter bestimmten Umständen zu.[705] Schließlich darf auch die – vorstehend erwähnte – vom EuGH festgestellte Einschränkung des Herkunftslandprinzips nicht vergessen werden. Aus diesen Gründen sind trotz des Art. 3 I und II ECRL genügend Fälle denkbar, in denen das Territorialitätsprinzip weiterhin anzuwenden ist. Das Territorialitätsprinzip wird von der E-Commerce-Richtlinie deshalb nur bedingt tangiert.

c. Zwischenergebnis

Das Territorialitätsprinzip und somit das deutsche Recht werden durch das Herkunftslandprinzip der E-Commerce-Richtlinie in einem gewissen Maße eingeschränkt. Das deutsche Recht ist deswegen nur zum Teil auf alle sich in Deutschland ansässigen Provider anwendbar. Wegen der zahlreichen Ausnahmen zu dem in der E-Commerce-Richtlinie fixierten Herkunftslandprinzips und weil es nur für den koordinierten Bereich der Richtlinie gilt, lässt die nachfolgende Prüfung diese Besonderheit zunächst unberücksichtigt und geht davon aus, dass das deutsche Recht uneingeschränkt auf die jeweiligen Provider, die sich im Inland befinden, zur Anwendung kommt. Die E-Commerce-Richtlinie und die Vorschriften zum Herkunftslandprinzip werden an späterer Stelle noch ausführlich besprochen.[706]

---

704 Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 8.

705 Vgl. hierzu die Ausführungen zur E-Commerce-Richtlinie unten unter B. 3. Teil. 3. Kapitel II.

706 Natürlich gilt es zu beachten, dass es mittlerweile Ausnahmen zum Territorialitätsprinzip im Zusammenhang mit dem Internet gibt. Zum besseren Verständnis und aus Gründen der Übersichtlichkeit sollten die Prüfungen des EGV und der E-Commerce-Richtlinie allerdings nicht vermischt werden. Außerdem gibt es genügend denkbare Fallgestaltungen, in denen nur der EGV und nicht die E-Commerce-Richtlinie, also auch nicht das Herkunftslandprinzip, zur Anwendung kommt. Ebenfalls denkbar ist eine parallele Anwendung dieser beiden Gesetzeswerke. Für diese Fälle muss eine Vermischung der nebeneinander existierenden europäischen Regelwerke vermieden werden. Da sich die Anwendungsbereiche des EGV und der E-Commerce-Richtlinie z.T. überschneiden, fällt dies manchmal etwas schwer.
Die Tatsache, dass die E-Commerce-Richtlinie an dieser Stelle noch nicht beachtet wird, bleibt ohne Konsequenzen. Denn alle Fälle, auf die der EGV nicht zur Anwendung kommt und die vom koordi-

2. Zuordnung zu bestimmten Rechtsordnungen

Des weiteren wird bei den einzelnen Fallvarianten – wie bereits oben angesprochen[707] – insbesondere nach der jeweiligen Nationalität (inländisch, europäisch, aus einem Drittstaat) der Internet-Provider bzw. des Nutzers unterschieden. Da es sich bei diesen Personen sowohl um natürliche als auch juristische Personen handeln kann, ist es zunächst wichtig, sie einer bestimmten Rechtsordnung zuzuordnen: Juristisch ausgedrückt handelt es sich dabei um das sogenannte „Personalstatut", das für die natürliche Person in Art. 5 Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB)[708] geregelt ist. Demnach gilt für die natürliche Person grundsätzlich das Staatsangehörigkeitsprinzip, d.h. die Staatsangehörigkeit legt die Zugehörigkeit der natürlichen Person zur Rechtsordnung eines Staates fest.[709] Der Wohnsitz einer natürlichen Person spielt insoweit für die Bestimmung der Rechtsordnung, die für ihre Rechtsverhältnisse maßgebend ist, keine Rolle.[710]

Im Gegensatz dazu enthält das EGBGB keine entsprechende Kollisionsnorm für juristische Personen. Die Bestimmung der Rechtsordnung, die für die Rechtsverhältnisse der juristischen Person maßgeblich ist, bleibt deshalb der Rechtsprechung und Lehre überlassen.[711] Dabei werden für die Bestimmung der Zugehörigkeit einer juristischen Person zu einem Staat grundsätzlich zwei wesentliche Theorien vertreten: So existiert zum einen die Ansicht, dass die juristische Person derjenigen Rechtsordnung unterstellt werden soll, nach der die juristische Person gegründet worden ist. Diese Meinung wird als die sogenannte „Gründungstheorie" bezeichnet. Die Gründungstheorie ist vor allem im angloamerikanischen Rechtskreis herrschend. Sie lässt dem Parteiwillen Spielraum, birgt aber das Risiko der Manipulation.[712] Zum anderen gibt es die „Sitztheorie". Sie besagt, dass die Rechtsordnung zur Anwendung kommen soll, wo der Sitz der juristischen Person liegt, d.h. der Schwerpunkt der tatsächlichen geschäftlichen Aktivität der juristischen Person, gemeint ist also die Hauptniederlassung oder -verwaltung, anzusiedeln ist.[713] In Kontinentaleuropa und somit auch in Deutschland wird vermehrt die Sitztheorie vertreten,[714] da sie der Praxis näher kommt. Zudem können hierdurch sogenann-

---

nierte Bereich der E-Commerce-Richtlinie erfasst werden, finden später noch eine ausführliche rechtliche Behandlung. Insoweit ist nach unten zu verweisen. Vgl. unten unter B. 3. Teil. 3. Kapitel II.

707 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. III.

708 BGBl. I S. 2494, BGBl. III/FNA 400-1.

709 Palandt-Heldrich, 60. Auflage, Art. 5 EGBGB Rdnr. 1.

710 Etwas anderes gilt nur, falls die natürliche Person als staatenlos anzusehen ist, vgl. Art. 5 II EGBGB.

711 Palandt-Heldrich, 60. Auflage, Anhang zu Art. 12 EGBGB Rdnr. 1.

712 So kann mit Hilfe der Gründungstheorie über „Briefkastenfirmen" sehr leicht eine Rechtsform für eine Gesellschaft erlangt werden, die mit der tatsächlichen Rechtslage nicht übereinstimmt.

713 Scheuer in: Lenz (Hrsg.), EG-Vertrag Kommentar, 2. Auflage, Art. 48 EGV Rdnr. 2.

714 BGHZ 97, 269, 271; BGH in NJW 95, 1032; BGH in NJW 96, 54, 55; Palandt-Heldrich, 60. Auflage, Art. 5 EGBGB Rdnr. 2 mit weiteren Fundstellen.

te „Briefkastenfirmen“ rechtlich erfasst und ihre negativen Auswirkungen auf das Wirtschaftsleben vermieden werden.[715]

In Europa selbst werden beide Theorien vertreten, so dass es vom jeweiligen Land abhängt, nach welchen Kriterien geprüft wird, woher die juristische Person „stammt“. Dies kann zu unterschiedlichen Ergebnissen führen. Insbesondere bei einer Verlagerung des Firmensitzes von einem europäischen Land in ein anderes kann es zu erheblichen gesellschaftsrechtlichen Schwierigkeiten kommen.[716]

Da in dieser Arbeit Kontrollmaßnahmen einer deutschen Behörde auf ihre Vereinbarkeit mit dem Europarecht untersucht werden, ist eine deutsche Sichtweise sinnvoll. Aus diesem Grund und wegen der oben aufgezeigten Vorteile der Sitztheorie muss der Sitztheorie gefolgt werden. Denn die Sitztheorie ermöglicht es, dem aktuellen und tatsächlichen Verhältnis einer Gesellschaft zu bestimmten Staaten zu entsprechen. Deshalb soll sich die Abstammung einer juristischen Person nach dem Sitz der Gesellschaft richten, also danach, wo die juristische Person ihre Hauptverwaltung oder -niederlassung hat. Es handelt sich somit um eine rein innerstaatliche juristische Person, wenn sie ihren Sitz in Deutschland hat, selbst wenn eine Firma von EU-Ausländern gegründet wird Das Gleiche gilt für den Fall, dass eine juristische Person aus dem EU-Ausland ihren Sitz nach Deutschland verlegt.[717] Denn sobald sich die Hauptverwaltung bzw. die Hauptniederlassung eines Unternehmens in Deutschland befindet, besteht nur noch ein Bezug dieser juristischen Person zur deutschen Rechtsordnung. In beiden Fällen kann nicht mehr von einer juristischen Person aus dem EU-Ausland gesprochen werden. Eine juristische Person aus dem Ausland liegt also nur dann vor, wenn sich ihr (Haupt)-Sitz im EU-Ausland befindet.

Im Ergebnis ist also festzuhalten, dass die natürliche Person und die juristische Person auf unterschiedliche Art und Weise bestimmten Rechtsordnungen zugewiesen werden. Bei der natürlichen Person entscheidet die Staatsangehörigkeit, bei der juristischen Person dagegen deren (Haupt)-Sitz der Gesellschaft. Dies hat zur Folge, dass eine Differenzierung zwischen einer natürlichen und juristischen Person erforderlich ist, um die

---

715 Abgesehen von der Gründungs- und Sitztheorie gibt es auch noch die „Kontrolltheorie“. Sie besagt, dass für die Bestimmung der Zugehörigkeit einer Gesellschaft zu einem Staat allein die Staatsangehörigkeit der die Gesellschaft kontrollierenden Personen maßgeblich ist. Diese Theorie wird nur vereinzelt vertreten und hat deutliche Schwächen. Sie ist vor allem nicht praktikabel. So fehlt häufig die Kenntnis der Staatsangehörigkeit der einzelnen Gesellschafter. Außerdem versagt die Theorie in den Fällen, wo die Gesellschaft von mehreren Nationalitäten kontrolliert wird. Sie ist deshalb abzulehnen.

716 Vgl. insoweit EuGH, Rs. C-212/97, 09.03.1999, Slg. 1999, I-1484 ff. (Centros); EuGH, Rs. 81/87, 27.09.1988, Slg. 1988, 5483 ff. (Daily Mail).

717 Der Akt als solcher, also die Sitzverlagerung der Hauptverwaltung von einem Mitgliedstaat in das Inland, berührt die Art. 43 ff. EGV. Befindet sich die Gesellschaft jedoch erst einmal im Inland, dann hat sie sich der deutschen Rechtsordnung unterworfen und sämtliche nationale Regelungen müssen von ihr beachtet werden. Für das Europarecht ist insoweit kein Raum mehr, da es sich lediglich um inländische Vorgänge handelt.

Frage beantworten zu können, ob ein Provider, gegen den sich die behördliche Maßnahme richtet, aus dem EU-Ausland stammt.[718]

3. Der Provider aus dem EU-Ausland

Die eben festgestellten Unterschiede bei der Frage, welcher Rechtsordnung die natürliche und juristische Person zuzurechen sind, haben erhebliche Konsequenzen für die Provider. Denn jeder Provider kann seine Dienste in unterschiedlicher Art und Weise anbieten. Problematisch und für diese Arbeit von großer Bedeutung ist der Provider aus dem EU-Ausland. Insofern ist erneut zu unterscheiden:

a. Natürliche Person

Der Provider aus dem EU-Ausland kann zunächst eine natürliche Person sein, die ihre Dienste im Internet anbietet. Demnach sind zwei Fallgestaltungen denkbar: Die natürliche Person hat ihren Wohnsitz, d.h. ihren gewöhnlichen Aufenthalt,[719] im Inland und fungiert von dort als Provider. Oder die natürliche Person hat ihren Wohnsitz im EU-Ausland und bietet von dort ihre Dienste über das Internet an. Häufig geschieht dies dann ohne direkten Inlandsbezug. Es besteht aber auch die Möglichkeit, dass sie zwar weiterhin ihren Wohnsitz im EU-Ausland hat, jedoch das jeweilige Providing im Inland stattfindet. So kann die natürliche Person die Hard- und Software, die für die entsprechenden Internet-Dienste benötigt wird, im Inland stationieren. Neben dieser Technik können auch noch weitere Komponenten oder Aktivitäten der natürlichen Person im Zusammenhang mit dem Internet-Providing hinzutreten. So ist es denkbar, dass auch der Geschäftsbetrieb für das Providing durch die natürliche Person im Inland abgewickelt wird. Darüber hinaus können hierfür im Inland Büros, Agenturen oder Zweigniederlassungen gegründet werden.

b. Juristische Person

Im Gegensatz zur natürlichen Person, bei der sich der jeweilige Wohnsitz nicht auf die Nationalität auswirkt, findet aus den oben angesprochenen Gründen bei der juristischen Person eine Differenzierung nach dem Gesellschaftssitz statt.[720] Je nachdem wo die Gesellschaft ihren (Haupt)-Sitz hat, ist dieses Recht auf die Gesellschaft anwendbar. Dies hat zur Folge, dass eine Gesellschaft nur dann eine juristische Person aus dem EU-Ausland darstellt, wenn ihr (Haupt)-Sitz im EU-Ausland liegt.

---

718 Wenn im folgenden von Providern aus dem EU-Ausland oder Nutzern aus dem EU-Ausland, die ebenfalls natürliche oder juristische Personen sein können, die Rede ist, dann sind damit entweder natürliche Personen mit einer EU-ausländischen Staatsangehörigkeit oder juristische Personen mit einem Sitz im EU-Ausland gemeint.

719 Palandt-Heinrichs, BGB-Kommentar, 60. Auflage, § 7 BGB Rdnr. 1.

720 Siehe oben unter B. 3. Teil. 2. Kapitel. IV. 2.

Ist der Provider eine juristische Person aus dem EU-Ausland, dann kann erneut differenziert werden, weil allein der Ort des Gesellschaftssitzes einer juristischen Person noch nichts darüber aussagt, welche Unternehmensstruktur sie aufweist. So können bei einem Provider die (Haupt)-Verwaltung und der Ort, wo sich die Technik für das Providing befindet zusammenfallen. Ist dies zu bejahen, dann ist der Provider ausschließlich im EU-Ausland vertreten und bietet seine Dienste im Internet von dort aus an.[721] Die juristische Person könnte jedoch die Technik oder bestimmte Gesellschaftsteile auslagern. Ist dies der Fall, könnte sich dadurch ein Inlandsbezug ergeben. Denn es besteht – wie vorstehend bei der natürlichen Person – die Möglichkeit, dass die juristische Person die Technik für das Providing im Inland unterhält. Neben diesen technischen Mitteln könnte die juristische Person jedoch auch noch weitere Komponenten (beispielsweise Büroräume, etc.) im Inland besitzen. Denkbar wäre auch die Gründung einer inländischen Agentur, einer Zweigniederlassung oder sogar einer Tochtergesellschaft, die für die inländische Technik und für den bereitgestellten Inhalt verantwortlich ist.

c. Gegenüberstellung der natürlichen und juristischen Person

Werden die möglichen Arten des Erscheinungsbildes der Provider bei der natürlichen Person und der juristischen Person gegenübergestellt, so ergibt sich folgende Besonderheit:

Im Gegensatz zur natürlichen Person wirkt sich bei der juristischen Person der Sitz der Gesellschaft auf die europarechtliche Betrachtung aus. Denn liegt der Sitz der juristischen Person im Inland, dann besteht kein Bezug zum Europarecht, da es sich nach der Sitztheorie um ein deutsches Unternehmen in Deutschland handelt. Ein grenzüberschreitender Sachverhalt kann insoweit nicht bejaht werden. Selbst bei der Sitzverlagerung eines Unternehmens aus dem EU-Ausland nach Deutschland ist höchst umstritten, ob Europarecht oder nationale Vorschriften einschlägig sein sollen.[722] Etwas anderes gilt dagegen bei der natürlichen Person. Stammt diese aus dem EU-Ausland und hat sie mittlerweile ihren Wohnsitz in Deutschland, dann kann sie sich dennoch auf europarechtliche Vorschriften berufen, da ein grenzüberschreitender Sachverhalt angenommen werden muss. Nicht umsonst wurde deshalb in der Literatur oft die Frage gestellt, ob Gesellschaften in Europa „Niederlassungsberechtigte minderen Rechts“ seien.[723] Abgesehen von diesem Unterschied haben die natürlichen und die juristischen Personen die-

---

721 Diese Dienste können dann natürlich auch von inländischen Nutzern via Internet abgerufen werden.

722 Hierzu eingehender: Timme/Hülk, „Das Ende der Sitztheorie im Internationalen Gesellschaftsrecht? – EuGH, EuZW 1999, 216“, JuS 1999, 1055 ff.; dies muss wohl trotz des Wortlauts von Art. 43 i.V.m. Art. 48 EGV mit der herrschenden Meinung in der Literatur abgelehnt werden. Vgl. insoweit Geiger, EUV/EGV, 3. Auflage, Art. 48 Rdnr. 12. Auf diese Problematik muss in dieser Arbeit jedoch nicht näher eingegangen werden, da eine derartige Konstellation im Hinblick auf staatliche Kontrollmaßnahmen im Internet nicht denkbar ist. Denn eine Lösch- oder Sperrverfügung kann nur gegen ein bereits bestehendes Unternehmen erfolgen.

723 Behrens, „Sind Gesellschaften Niederlassungsberechtigte minderen Rechts?“, EuZW 1991, 97.

selben Möglichkeiten, inwieweit sie neben der Technik im Inland vertreten sind: So kann sich jeweils der Sitz im EU-Ausland und nur die reine Technik für das Anbieten der Dienste im Inland befinden. Denkbar ist allerdings auch, dass der jeweilige Sitz wiederum im EU-Ausland liegt, neben der reinen Hard- und Software aber auch noch weitere Komponenten (wie Büroräume) vorhanden sind, die entweder wirtschaftlich noch kaum Bedeutung haben oder bereits als Agenturen, Zweigniederlassungen, ja sogar schon als Tochtergesellschaften anzusehen sind.[724] Schließlich besteht noch die Möglichkeit, dass die natürliche oder juristische Person ihre Dienste ohne Inlandsbezug ausschließlich im EU-Ausland erbringt. Für die vorliegende Arbeit sind allerdings grundsätzlich die Fallvarianten mit Inlandsbezug interessant, da sich durch das Vorhandensein der Technik oder weiterer Komponenten für das jeweilige Providing die natürliche bzw. juristische Person aus dem EU-Ausland in den deutschen Rechtskreis begeben hat. Wie bereits oben festgestellt wurde,[725] greift somit das Territorialitätsprinzip ein, so dass die nationalen Behörden gegen diese Provider tätig werden können. Demzufolge sind die Personen aus dem EU-Ausland, die – abgesehen vom Internet – über keine Verbindung zum Inland verfügen, da sich ihr Gesellschaftssitz, die Technik und die übrigen Mittel für das Providing im EU-Ausland befinden, für die Kontrollmaßnahmen grundsätzlich ohne Bedeutung.[726] Es bestehen keine Berührungen zum deutschen Recht. Die deutschen Behörden können also nur begrenzt gegen sie tätig werden. Außerdem gibt es neben dem technischen auch ein praktisches Problem: An wen sollen die Kontrollmaßnahmen im EU-Ausland adressiert werden?[727]

4. Relevante Sichtweise bei der Bearbeitung der einzelnen Fallausgestaltungen

Durch die staatlichen Kontrollmaßnahmen, die an die jeweiligen Provider adressiert sind, können nicht nur die Provider betroffen sein. Auch die Nutzer, die den von diesen Kontrollmaßnahmen tangierten Inhalt abrufen wollen, können durch die staatlichen Lösch- oder Sperranordnungen (un)mittelbar in einer ihrer Grundfreiheiten aus dem EGV beeinträchtigt werden. Folglich besteht die Möglichkeit, dass die gegen einen Provider gerichteten staatlichen Kontrollmaßnahmen auch aus der Sicht des Nutzers europarechtlich bedeutsam sind.

---

724 Vgl. bezüglich der denkbaren Fallvarianten auch die Überlegungen bei Osthaus in: „Die Renaissance des Privatrechts im Cyberspace“, AfP 2001, 13, 14 ff.

725 Vgl. oben unter B. 3. Teil. 2. Kapitel. IV. 1.

726 Etwas anderes gilt nur, wenn die zuständigen Behörden rechtswidrige Inhalte im EU-Ausland über einen Access-Provider sperren lassen wollen. Der Unterschied liegt hier darin, dass die Kontrollmaßnahmen nicht direkt gegen den Content- bzw. Service-Provider gerichtet sind. Vielmehr ist hier der Access-Provider der Adressat dieser Maßnahmen. Vgl. hierzu unten unter B. 3. Teil. 2. Kapitel. V. 3. a.

727 Wenn eine Adresse existiert, bestehen aber keine Rechtsgrundlagen für eine Durchsetzbarkeit der staatlichen Anordnungen. Sie sind also sehr ineffektiv.

Als Adressaten der jeweiligen Kontrollmaßnahmen sind jedoch allein die Provider die hiervon unmittelbar betroffenen Personen. Auch wirtschaftlich gesehen spielen sie eine im Gegensatz zum Nutzer weitaus größere Rolle. Deshalb soll ausschließlich aus der Perspektive der Provider die Vereinbarkeit behördlicher Sperr- und/oder Löschanordnungen mit dem Europarecht überprüft werden.[728] Diese Einschränkung ist nicht nur aus Gründen der Übersichtlichkeit notwendig.[729] Vielmehr kommt den beim Nutzer zu erwartenden Ergebnissen nur eine untergeordnete Bedeutung zu. Denn die behördlichen Sperr- und/oder Löschanordnungen haben auf die Provider weit größere Auswirkungen als auf den einzelnen Nutzer. Die Person des Nutzers bleibt jedoch für die einzelnen Fallvarianten sehr bedeutsam, da jedes Providing vom Nutzer abhängig ist. Somit muss in allen Fällen, in denen die Sichtweise der Provider auf ihre europarechtliche Relevanz hin untersucht wird, auch die Person des Nutzers in differenzierter Form einbezogen werden.

Diese Arbeit befasst sich also im folgenden ausschließlich mit den Providern. Und zwar primär mit solchen, gegen die unmittelbar die staatlichen Maßnahmen gerichtet sind. Aber auch die Provider, die mittelbar von der behördlichen Maßnahme betroffen sein könnten, werden bei der Prüfung nicht vernachlässigt. Aus ihrer jeweiligen Perspektive wird ebenfalls gefragt, ob staatliche Kontrollanordnungen gegen die Grundfreiheiten des EGV verstoßen oder nicht. Um dies herauszufinden, wird zunächst bei den einzelnen Providern jede Fallkonstellation daraufhin geprüft, ob Europarecht von den behördlichen Sperr- und/oder Löschanordnungen betroffen ist. Erst nach Feststellung sämtlicher Fälle, in denen die Grundfreiheiten des EGV tangiert werden, ist anschließend ausführlich zu prüfen, ob dies in rechtmäßiger Art und Weise geschehen ist.[730]

5. Wirtschaftliche Tätigkeit der Provider

Vor der anschließenden Prüfung von Kontrollmaßnahmen, die gegen unterschiedliche Provider ergehen können, auf ihre Europarechtskonformität ist darauf zu verweisen, dass von den Grundfreiheiten des EGV nur Sachverhalte erfasst werden können, die eine wirtschaftliche Komponente besitzen.[731] Denn die Grundfreiheiten des EGV for-

---

728 Obwohl auf die Person des Nutzers und dessen europarechtliche Rolle in den nachstehenden Prüfungen nicht eingegangen wird, soll trotzdem an dieser Stelle darauf hingewiesen, dass noch weitere europarechtlich relevante Fälle existieren könnten, wenn die Perspektive gewechselt wird und die Fallvarianten aus der Sicht der unterschiedlichen Nutzer betrachtet werden würden.

729 Zu bedenken ist, dass beim Service-Provider Fallkonstellationen mit vier Personen denkbar sind, die alle möglicherweise durch die staatlichen Kontrollmaßnahmen in Europarecht betroffen sein könnten. Eine Überprüfung sämtlicher Personen und Fallvarianten hätte eine Komplexität und eine Ausuferung des Umfangs zur Folge, so dass die Arbeit unübersichtlich werden würde. Außerdem würde hierdurch der wesentliche Inhalt der Arbeit durch bedeutungslose Prüfungen überlagert.

730 Dadurch bleibt die Übersichtlichkeit gewahrt, weil – wie sich zeigen wird – mehrere Fallvarianten zusammengefasst werden können.

731 Vgl. beispielsweise Art. 50 I EGV, der entgeltliche Dienstleistungen voraussetzt.

dern regelmäßig eine wirtschaftliche Betätigung der natürlichen und juristischen Personen innerhalb der EU, damit sie zur Anwendung kommen können.[732] Diese wirtschaftliche Betätigung muss zwar nicht im Vordergrund stehen. Rein private Internet-Aktivitäten ohne ökonomischen Bezug können jedoch nicht unter die Grundfreiheiten des EGV subsumiert werden.[733] Dies ist bei den nachfolgenden Prüfungen zu berücksichtigen.

V. Europarechtskonformität der staatlichen Kontrollmaßnahmen gegen die einzelnen Provider

1. Kontrollmaßnahmen gegen den Content-Provider

a. Grundkonstellation

Die Ausgangslage beim Content-Provider für die verschiedenen Fallausgestaltungen ist folgende: Der inländische Content-Provider wird durch einen behördlichen Bescheid angewiesen, einen bestimmten Inhalt, den er im Internet bereithält, entweder zu sperren oder zu löschen. Durch diese Maßnahme ist der Content-Provider insoweit betroffen, als er seinen gespeicherten Inhalt nicht mehr den jeweiligen Nutzern anbieten kann.[734]

Der Standardfall setzt sich somit aus einem deutschen Content-Provider und einem deutschen Nutzer zusammen. Der Content-Provider bekommt die behördliche Anordnung, worauf er den gerügten Inhalt sperrt bzw. löscht. Dem Nutzer steht daraufhin dieser Inhalt nicht mehr zur Verfügung. Dieser Grundfall stellt kein europarechtliches Problem dar, da es sich hierbei lediglich um einen rein innerdeutschen Sachverhalt handelt, auf den das primäre Gemeinschaftsrecht mangels Grenzüberschreitung nicht anwendbar ist. Etwas anderes kann sich aber dadurch ergeben, dass entweder der Content-Provider oder der Nutzer in Beziehung zu einem anderen Mitgliedstaat der EU steht. Insoweit muss deshalb zwischen diesen beiden Fällen differenziert werden.

---

732 Herdegen, Europarecht, 2. Auflage, § 15 Rdnr. 281.

733 Vgl. aber bezüglich dieser Fälle unten unter B. 3. Teil. 4. Kapitel.

734 Auch der Nutzer selbst wird durch diese Sperr- und/oder Löschanordnung beeinträchtigt, da er nicht mehr auf diesen Inhalt mit Hilfe eines Access-Providers zugreifen kann. Wie bereits oben ausführlich dargestellt, wird auf die Sichtweise des Nutzers und dessen europarechtliche Situation nicht eingegangen. Es soll hier nur zum besseren Verständnis erklärt werden, welche praktische Auswirkung die Sperr- bzw. Löschanordnung hat.
Obwohl die Tatsache angesprochen wird, dass zusätzlich ein Access-Provider bei dieser Fallvariante involviert sein kann, ja häufig auch ist, soll er an dieser Stelle noch nicht geprüft werden. Denn auf den Access-Provider und seine Funktion im Internet wird später noch ausführlich eingegangen. Es wäre nur verwirrend und überflüssig, ihn schon an dieser Stelle einzubauen und eingehend zu prüfen.

b. Fallvariante I: Content-Provider aus EU-Ausland, deutscher Nutzer

Mit der ersten Fallvariante soll zunächst der Content-Provider behandelt werden, der aus dem EU-Ausland stammt.[735] Der Nutzer ist weiterhin Deutscher.

Wie bereits bei den Vorfragen festgestellt wurde,[736] kann es sich beim Content-Provider aus dem EU-Ausland sowohl um eine natürliche Person mit einer EU-ausländischen Staatsangehörigkeit als auch um eine juristische Person mit (Haupt)-Sitz im EU-Ausland handeln. Europarechtlich relevant sind somit nachstehende Konstellationen der Fallvariante I:

Zum einen die natürliche Person aus dem EU-Ausland, die ihren Wohnsitz, eventuell ihre Büroräume sowie die Technik für das Content-Providing im Inland hat. Zum anderen die natürliche oder juristische Person, die ihren Sitz zwar im EU-Ausland hat, deren Hard- und Software aber im Inland zu finden ist. Schließlich ist noch die dritte Variante wichtig, bei der die natürliche oder juristische Person wiederum ihren Sitz im EU-Ausland hat und sich – je nach Ausgestaltung – neben der reinen Technik auch noch andere Komponenten, die im Zusammenhang mit dem Content-Providing stehen (vor allem Büroräume), im Inland befinden.

aa. Der Content-Provider ist eine natürliche Person aus dem EU-Ausland mit Wohnsitz/Technik und eventuell Büroräumen im Inland

Inwieweit hier das Europarecht durch staatliche Sperr- und/oder Löschanordnungen betroffen ist, richtet sich zunächst danach, welche Inhalte der Content-Provider für den Nutzer bereithält. Denn je nachdem, welche Art von Inhalten im Internet durch den Content-Provider angeboten wird, können unterschiedliche Anwendungsbereiche der Grundfreiheiten des EGV betroffen sein.

Das Angebot der Content-Provider ist äußerst vielfältig. Es reicht von rein privat eingestellten Informationen ohne kommerziellen Hintergrund[737] bis hin zu virtuellen Einkaufsgalerien.[738] Diese Warenangebote im Internet können mit Katalogen von Versandhäusern verglichen werden. So kann meistens lediglich die Bestellung der Ware über das Internet erfolgen. Die angeforderten Produkte werden hingegen auf herkömmlichen Weg – oft mit der Post – zum Besteller gebracht. Etwas anderes gilt jedoch für die Waren bzw. Dienstleistungen, die aus Daten bestehen, wie beispielsweise Computerspiele, Software, Text-, Bild-, Film- oder Musikdateien. Diese können direkt vom Anbieter zum Besteller via Internet verschickt werden. Darin kann die Erbringung einer Dienst-

---

735 Die Herkunft aus einem Drittstaat ist – wie bereits oben dargelegt – für vorliegende Arbeit nicht von Interesse, so dass hier einzig und allein die europäischen Content-Provider behandelt werden.

736 Siehe oben unter B. 3. Teil. 2. Kapitel. IV. 3.

737 Darauf ist, wie bereits oben erwähnt, der EGV nicht anwendbar. Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. IV. 5.

738 Brisch, "EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr", CR 1999, 235, 236.

leistung gesehen werden.[739] Neben diesen virtuellen Kaufhäusern gibt es aber auch Informationsforen, die entweder privaten oder kommerziellen Charakter besitzen. Zudem existieren auch zahlreiche Mischformen. So gibt es im Internet sehr viele Informationsforen oder Datenangebote, auf die kostenlos zugegriffen werden kann, die jedoch mit Werbung Dritter ausgestaltet sind und hierdurch finanziert werden.[740]
Letztendlich kann gesagt werden, dass mittlerweile in der virtuellen Welt alle Waren, Dienstleistungen, Informationen, etc. angeboten werden, die es in der realen Welt auch gibt.[741]

(1) Warenverkehrsfreiheit

Die staatlichen Kontrollmaßnahmen, die sich gegen einen Content-Provider richten, der rechtswidrige Waren zum Verkauf anbietet,[742] könnten deshalb zunächst gegen die Warenverkehrsfreiheit gemäß den Art. 28 ff. EGV verstoßen. Ferner wäre der freie Warenverkehr möglicherweise dann betroffen, wenn die staatlichen Sperr- und/oder Löschanordnungen lediglich gegen die Werbung für derartige Waren gerichtet sind.[743] Denn weil die Werbung für Produkte sehr stark mit diesen Waren im Zusammenhang steht, werden staatliche Maßnahmen gegen Produktwerbung grundsätzlich nicht an der Dienstleistungsfreiheit sondern an der Warenverkehrsfreiheit nach den Art. 28 ff EGV gemessen.[744] Die Werbung stellt in diesem Fall lediglich einen Annex zum Produkt dar.[745]
Allgemein sind Waren i.S.d. Warenverkehrsfreiheit des EGV körperliche Gegenstände, die über eine Grenze verbracht werden und Gegenstand von Handelsgeschäften sein

---

739 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 250 f.; er kommt jedoch zu dem Schluss, dass die Warenverkehrsfreiheit durch die staatlichen Kontrollmaßnahmen nicht tangiert werden kann, da sie sich lediglich gegen Daten im Internet richten. Er verkennt hier jedoch den Art. 28 EGV, der jegliche Art von Einführbeschränkungen – selbst wenn sie gegen Daten gerichtet sind und somit nur indirekt den gemeinschaftlichen Handel betreffen (vgl. Dassonville-Formel) – grundsätzlich verbietet. Eine Verletzung der Art. 23 ff., 28 ff. EGV durch eine inhaltliche Beschränkung des Internets kann deshalb durchaus gegeben sein.

740 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission", MMR 1999, 187, 188.

741 Brisch, "EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr", CR 1999, 235, 236.

742 Als Beispiele hierfür können Bücher mit rassistischem, politisch radikalen oder terroristischen Hintergrund genannt werden. Des weiteren sind Videokassetten oder DVDs mit kinderpornographischen Inhalten als Warenangebote denkbar. Aber auch bestimmte Produkte wie verschreibungspflichtige Medikamente können durch den Content-Provider in unerlaubter Weise angeboten werden.

743 Schwarze, „Medienfreiheit und Medienvielfalt im Europäischen Gemeinschaftsrecht", ZUM 2000, 779, 785.

744 Dickie, Internet and Electronic Commerce Law in the European Union, S. 68 f.; Waldenberger, „Electronic Commerce: der Richtlinienvorschlag der EG-Kommission", EuZW 1999, 296, 297.

745 Holoubek in: Schwarze (Hrsg.), EU-Kommentar, Art. 50 Rdnr. 15; etwas anderes gilt dagegen für die Werbung von Dienstleistungen. In diesem Fall stellt die Werbung ein Annex zur Dienstleistungsfreiheit dar, so dass bei staatlichen Maßnahmen gegen die Werbung die Dienstleistungsfreiheit betroffen wäre, vgl. Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 15.

können.[746] Demnach wird der Anwendungsbereich der Art. 28 ff. EGV nur dann eröffnet, wenn Waren über eine Grenze verbracht werden. Da sich aber der Content-Provider und somit sein Warenangebot im Inland befindet und auch der Nutzer aus dem Inland stammt, besteht insoweit schon kein grenzüberschreitender Sachverhalt. Auf die Nationalität der Warenanbieter und –empfänger kommt es insoweit nicht an.[747] Folglich kann die Warenverkehrsfreiheit von staatlichen Kontrollmaßnahmen bei dieser Fallkonstellation nicht betroffen sein.

Etwas anderes könnte sich nur dann ergeben, wenn der Content-Provider Waren anbietet oder Waren bewirbt, die aus dem EU-Ausland in das Inland importiert werden müssen. Denkbar ist beispielsweise, dass der inländische Nutzer Waren bestellen kann, die ihm aus dem EU-Ausland zugeschickt werden. In diesem Fall wäre die Warenverkehrsfreiheit des Art. 28 EGV von staatlichen Sperr- und/oder Löschmaßnahmen, die sich gegen rechtswidrige Warenangebote oder Werbung dafür richten, mittelbar betroffen. Dies reicht nach der vom EuGH entwickelten Dassonville-Formel[748] aus, um die staatlichen Kontrollmaßnahmen grundsätzlich als Maßnahmen gleicher Wirkung i.S.d. Art. 28 EGV zu qualifizieren. Demzufolge wäre Europarecht hiervon tangiert.

Letztendlich hängt die Frage, ob durch staatliche Kontrollmaßnahmen bei dieser Fallvariante die Warenverkehrsfreiheit betroffen ist, davon ab, um welche Waren es sich handelt: Befinden sich die vom Content-Provider angebotenen oder beworbenen Waren bereits im Inland, dann fehlt dieser Ware für die Anwendung von Art. 28 EGV der grenzüberschreitende Sachverhalt. Andernfalls liegt ein Eingriff in die Warenverkehrsfreiheit vor.

(2) Niederlassungsfreiheit

Außerdem könnten staatliche Sperr- und/oder Löschanordnungen gegen die in Art. 43 ff. EGV garantierte Niederlassungsfreiheit verstoßen.

Art. 43 I 1 EGV bestimmt, dass die „*Beschränkungen der freien Niederlassung von Staatsangehörigen eines Mitgliedstaats im Hoheitsgebiet eines anderen Mitgliedstaats*“ nach Maßgabe der nachfolgenden Bestimmungen verboten sind. Weiterhin regelt Art. 43 II EGV, dass die Niederlassungsfreiheit auch die „*Aufnahme und Ausübung selbständiger Erwerbstätigkeiten*“ umfasst. Folglich ist zunächst zu klären, was unter dem Begriff „Niederlassungsfreiheit“ i.S.d. EGV zu verstehen ist. Dabei kann für diese Definition kein nationales Recht zur Anwendung kommen, da ansonsten für jedes Mitgliedsland der EU unterschiedliche Voraussetzungen gegeben wären und somit der

---

746 EuGH, Rs. C-2/90, 09.07.1992, Slg. 1992, I-4431, 4478 Rdnr. 26 (Kommission/Belgien); Lux in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, zu den Artikeln 18 bis 29 Rdnr. 12.

747 Leible in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, Art. 28 EGV Rdnr. 8; Becker in: Schwarze (Hrsg.), EU-Kommentar, Art. 28 Rdnr. 8.

748 EuGH, Rs. 8/74, 11.07.1974, Slg. 1974, 837, 852 (Dassonville) Rdnr. 5; vgl. hierzu ausführlich unten unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (1).

Grundgedanke der EU, eine Vereinheitlichung des Rechts innerhalb von Europa herbei zu führen, konterkariert wäre.[749] Vielmehr muss die Frage, wann von einer Niederlassung i.S.d. Art. 43 EGV gesprochen werden kann und wann die Niederlassungsfreiheit insgesamt anwendbar ist, europarechtlich geklärt werden.[750] Nach herrschender Lehre umfasst die Niederlassungsfreiheit jede unabhängige Erwerbstätigkeit in einem fremden Mitgliedstaat, die von einer dort eingerichteten Niederlassung ausgeht.[751] Demnach begründet die Niederlassungsfreiheit das Recht zur Aufnahme und Ausübung selbständiger Erwerbstätigkeiten sowie zur Gründung und Leitung von Unternehmen in einem anderen Mitgliedstaat.[752] Die Niederlassungsfreiheit des Art. 43 EGV betrifft selbständige, d.h. – in Abgrenzung zur Arbeitnehmerfreizügigkeit – nicht weisungsgebunden tätige natürliche und juristische Personen.[753] Auf die Art der Tätigkeit kommt es dabei nicht an; sie muss allerdings dem wirtschaftlichen Leben zuzurechnen sein und einem Erwerbszweck dienen.[754] Für Tätigkeiten im Rahmen des Kapitalverkehrs gelten hingegen die Sonderregelungen der Art. 56 ff. EGV.[755] Der Begriff Niederlassung i.S.d. Art. 43 EGV wird vom EuGH als die „tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung in einem anderen Mitgliedstaat auf unbestimmte Zeit“ definiert.[756] Die Niederlassung setzt danach zunächst eine feste Einrichtung in einem anderen Mitgliedstaat voraus. Dazu zählen vor allem bauliche Einrichtungen wie beispielsweise Produktionsstätten, Lager- und Büroräume.[757] Das Merkmal der festen Einrichtung alleine genügt jedoch nicht, um eine Niederlassung annehmen zu können. Hinzutreten muss daneben das Element der Dauerhaftigkeit. Hierunter versteht der EuGH die „stetige und dauerhafte“ bzw. „stabile und kontinuierliche“ Teilnahme am Wirtschaftsleben im Niederlassungsland.[758] Im Gegensatz zu der in Art. 49 ff. EGV geregelten Dienstleistungsfreiheit begibt sich der Niederlassungswillige dauerhaft in den Niederlassungsstaat und nicht nur „*vorübergehend*“ in den anderen Mitgliedstaat, wie es Art. 50 III EGV für den Dienstleistenden bestimmt. Die feste Einrichtung als Abgrenzungsmerkmal zu der in Art. 49 ff. EGV niedergeschriebenen Dienstleistungsfreiheit zu benutzen, ist somit manchmal nicht ausreichend.[759] Denn das maßgebliche Kriterium hierfür ist – wie Art. 50 III EGV bestimmt – nur der vorübergehende Charakter der Leistungserbringung. Der vorübergehende Charakter einer Tätigkeit schließt

---

749 Dies gilt im übrigen für jeden europarechtlichen Begriff.
750 Streinz, Europarecht, 4. Auflage, § 8 Rdnr. 499 f.
751 Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1592.
752 Koenig/Haratsch, Europarecht, 2. Auflage, Rdnr. 485.
753 Clausnitzer in: Lenz (Hrsg.), EG-Handbuch Recht im Binnenmarkt, 2. Auflage, S. 241.
754 Von der Niederlassungsfreiheit sind demnach Idealvereine nach § 21 BGB, wozu auch Berufs- und Wirtschaftsverbände zählen, ausgeschlossen.
755 Fastenrath/Müller-Gerbes, Europarecht, Rdnr. 116.
756 EuGH, Rs. C-221/89, 25.07.1991, Slg. 1991, I-3905, 3965 Rdnr. 20 (Factortame).
757 Bröhmer, in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 10.
758 EuGH, Rs. C-70/95, 17.06.1997, Slg. 1997, I-3395, 3432 Rdnr. 24 (Sodemare); EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4198 Rdnr. 39 (Gebhard).
759 Bröhmer, in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 12.

deshalb nicht aus, dass sich der Dienstleistungserbringer im Aufnahmemitgliedstaat mit einer Infrastruktur in Form von Büros, einer Praxis oder Kanzlei ausstattet, soweit sie für die Erbringung der Leistung erforderlich ist.[760] Im übrigen ist der Begriff der Niederlassung weit gefasst und impliziert die Möglichkeit für einen Gemeinschaftsangehörigen, in stabiler und kontinuierlicher Weise am Wirtschaftsleben eines anderen als seines Herkunftsstaates teilzunehmen und daraus Nutzen zu ziehen.[761] Die erforderliche rechtliche Eingliederung in das Wirtschaftsleben setzt nicht voraus, dass sich der selbständig Erwerbstätige ausschließlich in diesem Mitgliedstaat niederlässt.[762]

Werden diese Überlegungen auf vorliegende Fallvariante übertragen, so kann regelmäßig für eine natürliche Person, die ihren Wohnsitz im Inland hat und mittels der nötigen Technik samt eventuell vorhandenen Büroräumen im Inland einen Content-Provider unterhält, von einer Niederlassung gesprochen werden. Dies gilt aber nur, falls die natürliche Person mit dem Content-Providing am wirtschaftlichen Leben teilnimmt, d.h. das Content-Providing einem Erwerbszweck dient.[763] Demnach darf ein Entgelt für die Tätigkeit nicht völlig unerheblich sein. Bietet also die natürliche Person ihren Inhalt völlig ohne Gegenleistung im Internet an,[764] dann kann Art. 43 EGV nicht zur Anwendung kommen. Die Gewinnerzielung muss aber nicht vorrangigstes Ziel sein.[765]

Die natürliche Person besitzt zudem die Staatsangehörigkeit eines anderen Mitgliedstaats und hat ihren Wohnsitz im Inland. Ein grenzüberschreitender Sachverhalt – wie ihn Art. 43 I EGV vorschreibt – ist demnach gegeben. Wegen der Tatsache, dass die natürliche Person neben der Technik, die für das Content-Providing nötig ist, auch noch ihren Wohnsitz und eventuell Büroräume oder ähnliche Einrichtungen im Inland hat, kann hier sowohl das Kriterium der festen Einrichtung als auch der Dauerhaftigkeit bejaht werden. Schließlich stellt das Content-Providing durch eine natürliche Person eine selbständige Tätigkeit dar.

Es sind also sämtliche Voraussetzungen für die Anwendbarkeit der Niederlassungsfreiheit i.S.d. Art. 43 ff. EGV erfüllt. Sobald nun dem Content-Provider durch staatliche Maßnahmen aufgetragen wird, gewisse Inhalte zu sperren und/oder zu löschen, kann darin ein Eingriff in die Niederlassungsfreiheit gesehen werden. Denn der Content-

---

760 Koenig/Haratsch, Europarecht, 2. Auflage, Rdnr. 504; Bröhmer, in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 12.

761 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 25 (Gebhard).

762 Weitergehend zum Begriff der Niederlassungsfreiheit und der Niederlassung sowie deren Abgrenzung zu den übrigen Grundfreiheiten vgl. bei Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 52 EGV Rdnr. 1 ff.

763 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. IV. 5.

764 Gemeint ist damit, dass der Content-Provider auch nicht von Seiten Dritter, beispielsweise aufgrund eines Werbevertrags, eine Gegenleistung für seine unentgeltlichen Angebote bekommt. Es geht hier lediglich um die – meist von Privatleuten – eingestellten, frei zugänglichen Daten. Hierbei handelt es sich häufig um Newsgroups oder informative Homepages.

765 Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 9.

Provider wird durch die Kontrollmaßnahmen in der Ausübung seiner selbständigen Erwerbstätigkeit beschränkt.

(3) Dienstleistungsfreiheit

Ob ein Verstoß gegen die Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV durch staatliche Sperr- bzw. Löschanordnungen vorliegen könnte, ist wegen des in Art. 50 EGV enthaltenen Subsidiaritätsgrundsatzes nicht zu prüfen.[766] Denn da oben bereits eine Betroffenheit der Niederlassungsfreiheit bejaht worden ist, würde ein eventuell gegebener Verstoß gegen die Dienstleistungsfreiheit hiervon verdrängt.

bb. Der Content-Provider ist eine natürliche oder juristische Person, die ihren Sitz im EU-Ausland hat, deren Hard- und Software allerdings im Inland zu finden ist

(1) Warenverkehrsfreiheit

Ein Verstoß gegen die in den Art. 28 ff. EGV geregelte Warenverkehrsfreiheit hängt ebenso wie in obiger Fallvariante davon ab,[767] welche Art von Waren der Content-Provider anbietet bzw. bewirbt. Es fehlt dann an einem grenzüberschreitenden Sachverhalt hinsichtlich der angebotenen oder beworbenen Waren, wenn sich diese Waren bereits im Inland befinden und somit nicht mehr aus dem EU-Ausland die Grenze überschreiten müssen, um zum Nutzer zu gelangen.

(2) Niederlassungsfreiheit

In diesem Fall könnte durch eine staatliche Kontrollmaßnahme ebenfalls in die Niederlassungsfreiheit der natürlichen oder juristischen Person eingegriffen werden.
Aus Art. 43 II i.V.m. Art. 48 EGV folgt, dass die Niederlassungsfreiheit nicht nur natürlichen Personen, sondern auch „*Gesellschaften*“, also juristischen Personen, zusteht.[768] Nach Art. 48 II EGV gelten als Gesellschaften, die den natürlichen Personen gleichgestellt sind und somit in den Genuss der Niederlassungsfreiheit kommen, „*die Gesellschaften des bürgerlichen Rechts und des Handelsrechts einschließlich der Genossenschaften und die sonstigen juristischen Personen des öffentlichen und privaten Rechts*“. Nach allgemeiner Meinung ist diese Bestimmung im Hinblick auf die Wortfassung in anderen Vertragssprachen berichtigend dahin auszulegen, dass auch nicht-rechtsfähige Gesellschaften, insbesondere die nach deutschem Recht gegründete BGB-Gesellschaft hiervon erfasst werden.[769] Art. 48 II a.E. EGV besagt zudem, dass die Niederlassungsfreiheit nur auf solche Gesellschaften zur Anwendung kommen darf, die einen Erwerbs-

---

766 Zur Problematik der Subsidiarität vgl. Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 13.

767 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1)

768 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4194 Rdnr. 23 (Gebhard).

769 Geiger, EUV/EGV, 3. Auflage, Art. 48 Rdnr. 2; mittlerweile hat der BGH der BGB-Gesellschaft ohnehin eine gewisse Art an Teilrechtsfähigkeit zugesprochen.

zweck verfolgen. Diesbezüglich gilt somit das Gleiche wie bei der natürlichen Person. Auch hinsichtlich der übrigen Kriterien, die den Anwendungsbereich der Niederlassungsfreiheit bei juristischen Personen eröffnen, kann auf die obigen Darstellungen zur natürlichen Person verwiesen werden.[770]

Fraglich ist jedoch, ob – wie bei der vorhergehenden – bei dieser Fallkonstellation wieder sämtliche Voraussetzungen vorhanden sind, um einen Eingriff in die Niederlassungsfreiheit durch staatliche Kontrollmaßnahmen bejahen zu können. Denn anders als in der vorstehenden Fallgestaltung agieren jetzt die natürliche und juristische Person nicht mehr ausschließlich im Inland, sondern sie haben ihren Wohn- bzw. Firmensitz im EU-Ausland und nur die technische Ausrüstung für das Content-Providing befindet sich im Inland. Damit könnte durch eine staatliche Lösch- bzw. Sperranordnung nicht die Niederlassungsfreiheit nach Art. 43 ff. EGV, wohl aber die Dienstleistungsfreiheit gemäß Art. 49 ff. EGV betroffen sein.

Zu beachten ist bei der Dienstleistungsfreiheit allerdings erneut ihre Subsidiarität.[771] Denn wie aus Art. 50 I EGV folgt, sind Dienstleistungen i.S.d. EGV solche, „*die in der Regel gegen Entgelt erbracht werden, soweit sie nicht den Vorschriften über den freien Waren- und Kapitalverkehr und über die Freizügigkeit der Person unterliegen*“. Demnach gehen die Bestimmungen über den freien Warenverkehr (Art. 28 ff. EGV), den Kapitalverkehr (Art. 56 ff.) und die Freizügigkeit der Personen (Art. 39 f., Art. 43 ff.) der Dienstleistungsfreiheit vor.

Sowohl der freie Kapitalverkehr als auch die Arbeitnehmerfreizügigkeit als Unterfall der Freizügigkeit der Person spielen hier keine Rolle. Bedeutsam sind allerdings der freie Warenverkehr sowie die Niederlassungsfreiheit als weiterer Unterfall der Freizügigkeit der Person:

Denn wie oben bereits angesprochen wurde,[772] kann der Content-Provider bestimmte Waren in einem virtuellen Kaufhaus für die Internet-Gemeinde bereithalten. Auch Werbung via Internet für bestimmte Produkte ist denkbar. Insoweit könnte der freie Warenverkehr beeinträchtigt werden, wenn die staatliche Sperr- und/oder Löschanordnung gerade in diesem Bereich zum Tragen kommt. Die Warenverkehrsfreiheit kann jedoch keine verdrängende Wirkung gegenüber der Dienstleistungsfreiheit entfalten. Zum einen ist schon fraglich, ob die eventuell angebotenen Waren eine Grenze überschreiten und somit ein Verstoß gegen die Warenverkehrsfreiheit bejaht werden kann.[773] Zum anderen hätte der Umstand, dass hier die Warenverkehrsfreiheit zur Anwendung kommen würde, keinen Einfluss auf die Dienstleistungsfreiheit, da es sich insoweit um unterschiedliche Angebote von Waren und Dienstleistungen handelt. Die Warenverkehrs-

---

770 Vgl. insoweit obige Ausführungen unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (2)

771 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4194 Rdnr. 22 (Gebhard).

772 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa.

773 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1).

freiheit kann die Dienstleistungsfreiheit dann nicht verdrängen, sondern beide Grundfreiheiten sind bei unterschiedlichen Produkten parallel anwendbar.

Daneben unterhält die natürliche oder juristische Person die gesamten technischen Einrichtungen für das Content-Providing im Inland. Deswegen könnte in diesem Fall erneut von einem Eingriff in die Niederlassungsfreiheit durch die staatlichen Kontrollmaßnahmen gesprochen werden. Problematisch ist hier jedoch das Verhältnis der Dienstleistungsfreiheit zur Niederlassungsfreiheit. Denn bei dieser Fallvariante ist es äußerst schwierig zu entscheiden, ob eine Niederlassung i.S.d. Art. 43 EGV oder nur eine Dienstleistung gemäß Art. 50 EGV vorliegt: So besitzt einerseits die natürliche bzw. juristische Person aufgrund der im Inland belegenen Hard- und Software eine ständige – vor allem virtuelle – Präsenz in diesem Mitgliedstaat. Dies würde grundsätzlich dafür sprechen, darin eine Niederlassung zu sehen. Andererseits werden sämtliche inhaltlichen und geschäftlichen Entscheidungen im EU-Ausland getroffen. Die wirtschaftliche Betätigung der natürlichen sowie juristischen Person spielt sich einzig und allein im EU-Ausland ab. Wenn nun ein Nutzer im Inland auf ein Angebot des Content-Providers zurückgreift, sind das eigentlich Leistungen aus dem EU-Ausland, die er in Anspruch nimmt. Es spricht insoweit viel dafür, die Fallvariante der Dienstleistungsfreiheit zuzuordnen. Dies wird um so plausibler, wenn darüber hinaus die natürliche bzw. juristische Person das Inhaltsangebot des Content-Providers beim inländischen Server via Internet vom EU-Ausland aus verändert. Denn dann stellt dies eine offensichtliche grenzüberschreitende Dienstleistung dar, die vom EU-Ausland kommend im Inland angeboten wird.

Problematisch ist hier aber auch, dass sich die Technik für die Erbringung der Leistung permanent im Inland befindet. Der EuGH hat in derartigen Fällen entschieden, dass die Zuordnung eines Sachverhalts zur Dienstleistungsfreiheit oder Niederlassungsfreiheit im Einzelfall unter Berücksichtigung von Dauer, Häufigkeit, Periodizität und Kontinuität der Tätigkeit erfolgen muss.[774] Ebenfalls ist nach einer Entscheidung des EuGH der Gedanke zu berücksichtigen, dass die Existenz einer bestimmten Infrastruktur, wie beispielsweise eines Büros, als solche noch nicht die Anwendung der Dienstleistungsfreiheit ausschließen soll.[775]

Die im Inland befindliche Hard- und Software stellt eine gewisse Art von Infrastruktur i.S.d. EuGH-Rechtsprechung dar.[776] Die technische Einrichtung zur Erbringung von Internet-Diensten kann durchaus mit einer Kanzlei oder Praxis verglichen werden. Diese Einrichtungen stellen alle insgesamt nur die Möglichkeit zur Verfügung, bestimmte Dienstleistungen zu erbringen. Die Technik ist jedoch auf Dauer im Inland installiert. Fraglich ist somit, ob dies noch von der Dienstleistungsfreiheit gedeckt wird, da das

---

774 EuGH, Rs. C-3/95, 12.12.1996, Slg. 1996, I-6511, 6536 Rdnr. 21 (Reisebüro Broede).

775 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 27 (Gebhard).

776 Koenig/Haratsch, Europarecht, 2. Auflage, Rdnr. 504.

maßgebliche Kriterium für ihre Abgrenzung zur Niederlassungsfreiheit gemäß Art. 50 III EGV der nur vorübergehende Charakter der Leistungserbringung ist. Wie sich jedoch bereits aus dem Wortlaut ergibt, wird auf die Leistungserbringung abgestellt. Zunächst muss geklärt werden, aus wessen Sicht die Leistungserbringung zu beurteilen ist. Denn es sind zwei verschiedene Perspektiven denkbar, die des Nutzers und die des Content-Providers. Der Content-Provider hält die Inhalte im Internet grundsätzlich permanent bereit. Demgegenüber benutzt der User den Content-Provider regelmäßig nur sporadisch. Es geht hier allerdings nicht primär um den Nutzer, sondern Gegenstand der Untersuchung ist die Vereinbarkeit der staatlichen Kontrollmaßnahmen mit dem Europarecht, die gegenüber dem Content-Provider ergehen. Also muss hier die Sichtweise des Content-Providers gelten. Folglich fällt es sehr schwer, diese Fallvariante eindeutig der Niederlassungsfreiheit oder der Dienstleistungsfreiheit zuzuordnen. Dies liegt vor allem an der Besonderheit des Internets, dass die darin enthaltenen Dienste vom Nutzer ohne Zutun des Providers abgerufen werden. Folglich reicht die Technik grundsätzlich aus, um diese Internet-Dienste anbieten zu können. In einer jüngeren Entscheidung hat der EuGH festgestellt, dass eine Niederlassung nur dann unter Abweichung vom vorrangigen Kriterium des Sitzes der wirtschaftlichen Tätigkeit als Ort der Dienstleistungen betrachtet werden kann, wenn sie einen hinreichenden Grad an Beständigkeit sowie eine Struktur hat, die von der personellen und technischen Ausstattung her eine autonome Erbringung der betreffenden Dienstleistung ermöglicht.[777] Abzustellen ist demnach darauf, ob die natürliche oder juristische Person mit der Installierung der Hard- und Software eine Struktur geschaffen hat, die die autonome Erbringung einer Dienstleistung ermöglicht. Ist dies zu bejahen, wenn also die natürliche bzw. juristische Person über eigenes Personal und über eine Struktur im Inland verfügt, in deren Rahmen Verträge abgefasst oder Entscheidungen über die Geschäftsführung getroffen werden können, dann besitzt sie eine feste Niederlassung in diesem Mitgliedstaat.[778]

Falls sich lediglich die Technik im Inland befindet, alle übrigen Geschäftsvorgänge hingegen im EU-Ausland getätigt werden, kann – trotz des sehr weiten Begriffs der Niederlassung[779] – eine Niederlassung i.S.d. Art. 43 EGV nicht mehr angenommen werden. Hierfür sprechen gewichtige Argumente: Zum einen stellt die im Inland liegende Technik nur die zur Erbringung des Content-Providings benötigte Infrastruktur dar, welche die natürliche bzw. juristische Person für die Erbringung ihrer Dienstleistung benötigt.[780] Es macht eigentlich keinen Unterschied, ob der inländische Nutzer via Internet auf das Angebot des Content-Providers aus dem EU-Ausland zurückgreift, das er im EU-Ausland installiert hat oder ob er den Inhalt im Inland gespeichert hat. Eine Nieder-

---

777 EuGH, Rs. C-190/95, 17.07.1997, Slg. 1997, I-4383, 4402 f. Rdnr. 6 (ARO Lease BV).

778 EuGH, Rs. C-190/95, 17.07.1997, Slg. 1997, I-4383, 4403 f. Rdnr. 9 (ARO Lease BV).

779 EuGH, Rs. C-3/95, 12.12.1996, Slg. 1996, I-6511, 6535 Rdnr. 20 (Reisebüro Broede); EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 25 (Gebhard).

780 Vgl. insoweit die Leitsätze bei EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165 f. (Gebhard).

lassung kann nicht allein schon durch die bloße Wahl des Standorts der Technik bejaht werden. Dies macht auch die E-Commerce-Richtlinie deutlich, die hier als Auslegungshilfe herangezogen werden kann. Da die E-Commerce-Richtlinie sekundäres Gemeinschaftsrecht darstellt, das auf dem primärrechtlichen EGV basiert,[781] können ihre Rechtsgedanken durchaus auch auf das europäische Primärrecht des EGV übertragen werden. Es spricht somit nichts dagegen, die Richtlinie hier als Ansatzpunkt für die rechtliche Einordnung dieser Fallvariante heranzuziehen. Gemäß Art. 2 c ECRL ist ein niedergelassener Diensteanbieter ein Anbieter, der „*mittels einer festen Einrichtung auf unbestimmte Zeit eine Wirtschaftstätigkeit tatsächlich ausübt; Vorhandensein und Nutzung technischer Mittel und Technologien, die zum Anbieten des Dienstes erforderlich sind, begründen allein keine Niederlassung des Anbieters*". Vor allem der letzte Halbsatz dieser Definition besagt, dass die reine Technik nicht ausreicht, um unter den Niederlassungsbegriff des Art. 43 EGV subsumiert werden zu können. Denn mittels der Technik allein kann die natürliche bzw. juristische Person aus einem Mitgliedstaat nicht in stabiler und kontinuierlicher Weise am Wirtschaftsleben eines anderen Mitgliedstaats als seines Herkunftsstaats teilnehmen und daraus Nutzen ziehen.[782] Sämtliche Geschäftsvorgänge werden nicht im Inland, wo sich die Technik befindet, sondern im EU-Ausland abgewickelt. Auch die Entscheidungen über die Nachbesserung und Neuinstallierung der Inhalte beim Content-Provider werden im EU-Ausland beschlossen und häufig via Internet-Leitung getätigt. Von einer Niederlassung, Zweigniederlassung, Agentur oder Tochtergesellschaft – wie es Art. 43 EGV vorschreibt – kann insoweit noch nicht gesprochen werden, da hierfür durch die Technik noch kein hinreichender Grad an Beständigkeit und Struktur erreicht ist. Folglich stellt die Technik, die sich im Inland befindet, allein keine Niederlassung i.S.d. Art. 43 EGV dar. Die Fallgruppe orientiert sich somit an der Dienstleistungsfreiheit der Art. 49 ff. EGV.

(3) Dienstleistungsfreiheit

Es könnte somit ein Verstoß gegen die Dienstleistungsfreiheit vorliegen. Unter der Dienstleistungsfreiheit wird gemäß den Art. 49 ff. EGV generell das Recht verstanden, ungehindert von einem Mitgliedstaat aus einzelne Dienstleistungstätigkeiten in einem anderen Mitgliedstaat zu erbringen, ohne dort eine ständige Niederlassung zu unterhalten.[783] Des weiteren verlangt Art. 50 EGV, dass es sich um eine selbständige Tätigkeit handelt, die „*in der Regel gegen Entgelt*" erbracht, nur „*vorübergehend*" und grenzüberschreitend ausgeübt wird.[784]

---

781 Hamann, Der Entwurf einer E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten", ZUM 290, 295; Spindler, „Verantwortlichkeit der Diensteanbieter nach dem Vorschlag einer E-Commerce-Richtlinie", MMR 1999, 199, 200.

782 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 25 (Gebhard).

783 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 116.

784 Fastenrath/Müller-Gerbes, Europarecht, Teil 3 Rdnr. 131.

Wie eben geklärt, unterhält die natürliche oder juristische Person keine ständige Niederlassung im Inland. Die Tätigkeit des Content-Providers ist eine selbständige Tätigkeit, die – da eine Niederlassung i.S.d. Art. 43 EGV verneint worden ist – auch lediglich vorübergehenden Charakter aufweist. Neben Waren kann der Content-Provider regelmäßig diverse Daten für den Nutzer bereithalten, auf die der Nutzer über das Internet Zugriff nehmen kann. Es wurde schon ausführlich dargestellt, dass der Content-Provider sämtliche Informationen zur Abfrage anbieten kann, die in eine digitalisierte Form gebracht werden können. Als wichtigste Dateien sind die Text-, Bild- und Tondateien zu nennen. Software wird häufig ebenfalls von Content-Providern im Internet angeboten. Aber auch die einzelnen Internet-Dienste, wie E-mail, Chat-Rooms, etc. und das Content-Providing insgesamt sind Dienstleistungen. Selbst die Werbung für diese Dienste und bereitgehaltenen Daten stellt als Annex hierzu eine Dienstleistung dar.[785] Nur wenige dieser Dienste und Informationen sind kostenlos. Häufig muss der Nutzer für gewisse Daten mit seiner Kreditkarte zahlen. Eine weitere Finanzierungsmöglichkeit ist die Einstellung von bestimmter Werbung Dritter. In beiden Fällen ist von einer entgeltlichen Dienstleistung zu sprechen.[786]

Problematisch ist jedoch, ob die erbrachten Leistungen des Content-Providers überhaupt eine Grenze überschreiten. Es geht also darum, inwieweit in diesem Fall ein grenzüberschreitender Sachverhalt gegeben ist. Denn man könnte den Standpunkt vertreten, dass – wie bei der Warenverkehrsfreiheit an obiger Stelle[787] – der inländische Nutzer die Dienstleistungen des Content-Providers im Inland abruft und deswegen ein rein innerstaatlicher Vorgang vorliegt. Dieser Gedanke ist jedoch zu verneinen. Zu den Anwendungsfällen der Dienstleistungsfreiheit zählen sowohl die aktive als auch die passive Dienstleistungsfreiheit sowie die Produktverkehrsfreiheit.[788] Bei der aktiven Dienstleistungsfreiheit, die in Art. 43 EGV explizit geregelt ist, begibt sich der Dienstleistende in einen anderen Mitgliedstaat, um seine Leistung zu erbringen.[789] Im Gegensatz dazu kommt bei der passiven Dienstleistungsfreiheit der Dienstleistungsempfänger in den Mitgliedstaat des Leistenden. Vom Wortlaut der Art. 49, 50 EGV wird die passive Dienstleistungsfreiheit nicht ausdrücklich erfasst. Selbst von der Literatur[790] und Rechtsprechung[791] wurde die Tatsache erst spät anerkannt, dass sich – als Pendant zur aktiven Dienstleistungsfreiheit – im Rahmen der Art. 49 ff. EGV auch der Leistungsempfänger

---

785 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 15.

786 EuGH, Rs. 352/85, 26.04.1988, Slg. 1988, 2085, 2131 Rdnr. 16 (Bond van Adverteerders).

787 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1). und bb. (1).

788 Oppermann, Europarecht, § 24 Rdnr. 1496 ff.

789 Fastenrath, Müller-Gerbes, Europarecht, Teil 3 Rdnr. 133.

790 Oppermann, Europarecht, § 23 Rdnr. 1499 ff.; Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 27 f.; Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1676.

791 EuGH, verb. Rs. 286/82 und 26/83, 31.01.1984, Slg. 1984, 377, 401 Rdnr. 10 (Luisi und Carbone); EuGH, Rs. 196/87, 05.10.1988, Slg. 1988, 6159, 6137 Rdnr. 15 (Steymann); EuGH, Rs. C-158/96, 28.04.1998, Slg. 1998, I-1931, 1945 ff. Rdnr. 29 ff. (Kohl).

problemlos über die Grenze zum Leistungserbringer begeben kann.[792] Schließlich wurde mit der Bejahung der Produktverkehrsfreiheit durch den EuGH der Rahmen der Dienstleistungsfreiheit erneut ausgedehnt.[793] So geht es bei der Produktverkehrsfreiheit nur noch um die Leistung an sich. Sowohl der Leistende als auch der Leistungsempfänger überschreiten keine Grenze mehr, sondern nur noch die Leistung selbst begibt sich von einem Mitgliedstaat in einen anderen.[794]

In dieser Fallkonstellation überqueren weder der Content-Provider noch der Nutzer eine mitgliedstaatliche Grenze. Es kommt hier also nur noch die Produktverkehrsfreiheit in Betracht. Dabei ist für Daten der Begriff „Produkt" etwas unglücklich gewählt. Hier passt der synonym verwendete Begriff der „Korrespondenzdienstleistung" besser.[795] Der Datentransfer vom Content-Provider zum Nutzer muss also einen grenzüberschreitenden Vorgang bezüglich der Leistung darstellen, so dass die Dienstleistungsfreiheit von den staatlichen Sperr- und/oder Löschanordnungen betroffen sein kann. Um diese Frage beantworten zu können, soll die Ähnlichkeit des Internets mit dem Rundfunk zur Hilfe genommen werden. Die Installation der Daten im Inland kann durchaus mit der Ausstrahlung von Rundfunkprogrammen verglichen werden.[796] Auch in diesen Fällen befinden sich sowohl der Nutzer als auch die Leistung in demselben Staat. Gleichwohl hat der EuGH vor Erlass der Fernsehrichtlinie 1989 in mehreren Urteilen festgestellt, dass selbst die Ausstrahlung von Rundfunksendungen, die eine bloße Grenzüberschreitung der Leistung darstellt, von der Dienstleistungsfreiheit erfasst werden soll.[797] Nichts anderes kann für vorliegenden Fall gelten: Die Inhalte, die der Content-Provider für seine Nutzer im Inland bereithält, sind von der natürlichen bzw. juristischen Person entweder im Inland selbst eingerichtet worden[798] oder die Einspeisung der Inhalte erfolgt über das Netz vom EU-Ausland aus.[799] Insgesamt lässt sich deshalb sagen, dass der Dienstleistungsbegriff i.S.d. Art. 50 EGV in Form der Korrespondenzdienstleistung bei dieser Fallvariante erfüllt ist.[800]

---

792 Völker, Passive Dienstleistungsfreiheit im Europäischen Gemeinschaftsrecht, S. 62 ff.

793 EuGH, verbundene Rs. C-271/90, C-281/90 und C-289/90, 17.11.1992, I-5833 ff. (Spanien/Kommission).

794 Holoubek in: Schwarze (Hrsg.), EU-Kommentar, Art. 49 Rdnr. 47 ff.

795 Vgl. hierzu Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 29; Geiger, EUV/EGV, 3. Auflage, Art. 50 EGV Rdnr. 10.

796 Koenig/Loetz, Sperrungsanordnungen gegenüber Network- und Access-Providern, CR 1999, 438, 444.

797 Koenig/Haratsch, Europarecht, 2. Auflage, Rdnr. 506 mit weiteren Verweisen; Clausnitzer in Lenz (Hrsg.), EG-Handbuch Recht im Binnenmarkt, 2. Auflage, S. 247.

798 Dies wäre dann ein Fall der aktiven Dienstleistungsfreiheit.

799 Da es sich hierbei um den einfacheren und bequemeren Weg handelt, wird diese Möglichkeit vom Content-Provider wohl häufiger genutzt. Dies wäre dann ein Fall der dritten Variante der Dienstleistungsfreiheit, bei der keine Person (d.h. Erbringer oder Empfänger der Leistung), sondern nur noch die Leistung die Grenze zwischen zwei Mitgliedstaaten überschreitet. Insoweit wäre diese Leistung mit dem grenzüberschreitenden Rundfunk vergleichbar. Allerdings kann die eingespeiste Leistung im Internet mehrfach und zeitlich unabhängig abgerufen werden.

800 Ob nun die aktive Dienstleistungsfreiheit oder die Korrespondenzdienstleistungsfreiheit in diesem Fall betroffen ist, spielt jedoch keine Rolle. Wichtig ist lediglich, dass feststeht, dass eine grenzüber-

Da bereits oben bejaht wurde, dass die Leistung des Content-Providers nur vorübergehend und in der Regel gegen Entgelt erbracht wird, sind sämtliche Kriterien der Dienstleistungsfreiheit gegeben, so dass die Art. 49 ff. EGV hierauf anwendbar sind.
Eine Sperr- und/oder Löschanordnung gegen den Content-Provider stellt somit bei dieser Fallvariante einen Eingriff in die Dienstleistungsfreiheit dar. Denn der Content-Provider kann den Usern seine Angebote im Internet nicht mehr ungehindert bereitstellen.

cc. Der Content-Provider ist eine natürliche bzw. juristische Person, bei der sich – je nach Ausgestaltung – neben der reinen Technik auch noch andere Komponenten, die im Zusammenhang mit dem Content-Providing stehen (vor allem Büroräume), im Inland befinden

(1) Warenverkehrsfreiheit

Ein möglicher Eingriff in die Warenverkehrsfreiheit richtet sich wiederum nach der Art der Ware, die im Internet angeboten bzw. beworben wird und zwar danach, wie sie zum Nutzer gelangt, grenzüberschreitend oder nicht.[801] Dies ist eine Frage des Einzelfalls und kann an dieser Stelle nicht abschließend geklärt werden.

(2) Niederlassungsfreiheit

Bei der Frage, ob die Niederlassungsfreiheit von staatlichen Kontrollmaßnahmen gegen den Content-Provider beeinträchtigt sein kann, ist an die vorangegangene Diskussion anzuknüpfen.[802] Problematisch ist auch bei dieser Fallgruppe, welche Grundfreiheit tangiert wird: die Niederlassungs- oder die Dienstleistungsfreiheit.
In dieser Variante befindet sich nicht nur die reine Infrastruktur, nämlich die Technik, sondern auch noch weitere Einrichtungen im Inland, welche die natürliche bzw. juristische Person im Inland repräsentieren. Zwar ist der Übergang zwischen der Dienstleistungs- und der Niederlassungsfreiheit fließend. Es kommt somit letztendlich auf eine Bewertung des Einzelfalls an, ob die neben der Technik vorhandene Struktur des Content-Providers im Inland bereits als Niederlassung i.S.d. EGV anzusehen ist. Häufig wird wohl eine Struktur erreicht sein, die den weit auszulegenden Begriff der Niederlassung[803] i.S.d. Art. 43 EGV bereits erfüllt: Die natürliche bzw. juristische Person aus dem EU-Ausland übt also als Content-Provider im Inland eine wirtschaftliche Tätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit aus.[804] Demnach ist re-

---

schreitende Leistung vorliegt. Vgl. hierzu Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 21 ff.

801 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1) und bb. (1).

802 Vgl. vorhergehende Diskussion bei B. 3. Teil. 2. Kapitel. V. 1. b. bb. (2).

803 EuGH, Rs. C-3/95, 12.12.1996, Slg. 1996, I-6511, 6535 Rdnr. 20 (Reisebüro Broede); EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 25 (Gebhard).

804 Dies kann sowohl in Form einer Agentur, Zweigniederlassung oder Tochtergesellschaft geschehen.

gelmäßig durch die staatlichen Kontrollmaßnahmen die europäische Grundfreiheit der Niederlassung und nicht der Dienstleistung betroffen.

(3) Dienstleistungsfreiheit

Gemäß dem Subsidiaritätsprinzip nach Art. 50 I EGV kommt die Dienstleistungsfreiheit nicht mehr in Betracht.

c. Fallvariante II: Deutscher Content-Provider, Nutzer aus dem EU-Ausland

Wie bereits an obiger Stelle angedeutet, kann der Nutzer ebenfalls eine natürliche oder juristische Person sein.[805]
Dies hat zur Konsequenz, dass wiederum unterschieden werden muss, so dass sich bei der Fallvariante II zwei Unterfälle ergeben:
Einerseits besteht die Möglichkeit, dass es sich bei dem Nutzer um eine natürliche Person aus dem EU-Ausland handelt, die ihren Wohnsitz im Inland hat. Andererseits kann der Nutzer aber auch eine natürliche oder juristische Person aus dem EU-Ausland sein, wobei der Wohn- bzw. Firmensitz ebenfalls im EU-Ausland liegt. Der Content-Provider ist jedes Mal Deutscher.

aa. Der Nutzer ist eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland

In diesem Fall nimmt also die natürliche Person, die die Staatsangehörigkeit eines anderen Mitgliedstaats besitzt, das Angebot des deutschen Content-Providers im Inland wahr.

(1) Warenverkehrsfreiheit

Ein Verstoß gegen die Warenverkehrsfreiheit nach Art. 28 EGV ist diesmal grundsätzlich zu verneinen. Da es sich um einen deutschen Content-Provider handelt, wird er hauptsächlich Waren im Internet anbieten oder bewerben, die sich in Deutschland befinden. Ein grenzüberschreitender Sachverhalt bezüglich der Waren – der Nutzer befindet sich in dieser Fallvariante ebenfalls im Inland – ist somit in der Regel auszuschließen.

(2) Dienstleistungsfreiheit

Dagegen könnte die Dienstleistungsfreiheit durch staatliche Kontrollmaßnahmen gemäß den Art. 49 ff. EGV betroffen sein. Aufgrund der Tatsache, dass die natürliche Person hier ihren Wohnsitz im Inland hat, sie sich also nicht nur wegen der Entgegennahme einer Dienstleistung dort aufhält, liegt lediglich ein rein innerstaatlicher Sachverhalt vor. Denn indem die natürliche Person ihren Wohnsitz im Inland gewählt hat, macht sie deutlich, dass sie ständig oder für unbestimmte Zeit dort verbleiben will. Neben der

---

805 Vgl. oben unter B. 3. Teil. 2. Kapitel. IV. 2.

Nutzung des Angebots, das der Content-Provider bereithält, muss sie noch zahlreiche andere Dienstleistungen wahrnehmen, die mit ihrem Aufenthalt im Inland verbunden sind. Ein Auslandsbezug, der für die Anwendbarkeit der Grundfreiheiten des EGV nötig ist, kann – trotz der unterschiedlichen Nationalität des Nutzers – in diesen Fällen nicht mehr bejaht werden.[806]
Mangels eines grenzüberschreitenden Sachverhalts besteht somit keine Möglichkeit, dass in dieser Fallgestaltung durch eine staatliche Kontrollmaßnahme gegen den deutschen Content-Provider ein nach dem EGV festgelegtes europäisches Recht betroffen ist. Denn aus der Sicht des Content-Providers liegt lediglich ein innerstaatlicher Vorgang vor.

bb. Der Nutzer ist eine natürliche oder juristische Person, deren Firmen- bzw. Wohnsitz sich im EU-Ausland befindet

(1) Warenverkehrsfreiheit

Bei dieser Fallkonstellation könnten staatliche Kontrollmaßnahmen zunächst gegen die Warenverkehrsfreiheit gemäß den Art. 28 ff. EGV verstoßen. Wie bereits oben dargestellt[807] besteht durchaus die Möglichkeit, dass der Content-Provider in seinem Angebot auch Waren zur Bestellung bereithält oder hierfür Werbung betreibt. Wenn nun eine behördliche Anordnung ergeht, einen bestimmten Teil dieser Inhalte im Internet zu sperren oder zu löschen, dann könnte die Warenverkehrsfreiheit hiervon betroffen sein.
Eine Einfuhrbeschränkung von Waren sowie eine damit vergleichbare Maßnahme, die gemäß Art. 28 EGV unzulässig ist, kommt nicht in Betracht. Denn der Content-Provider bietet seine Waren im Inland an. Auch wirbt er für diese grundsätzlich im Inland. Folglich kann durch staatliche Kontrollmaßnahmen nicht gegen Art. 28 EGV verstoßen werden, da sich die im Internet angebotenen Waren bzw. die beworbenen Waren regelmäßig bereits im Inland befinden. Allerdings bestimmt Art. 29 EGV, dass auch „*mengenmäßige Ausfuhrbeschränkungen sowie alle Maßnahmen gleicher Wirkung*“ zwischen den Mitgliedstaaten verboten sind. Eine Sperr- und/oder Löschanordnung von Warenangeboten oder dafür eingerichtete virtuelle Werbung hat zwar keine Kontingentierung, d.h. eine mengenmäßige Ausfuhrbeschränkung[808] zur Folge. Jedoch könnte darin eine Maßnahme gleicher Wirkung gesehen werden.
Wegen der grundsätzlichen Parallelen im Verbotszweck von Art. 28 EGV und Art. 29 EGV spricht nichts dagegen, für die europarechtliche Definition der Maßnahmen gleicher Wirkung i.S.d. Art. 29 EGV von den Kriterien der vom EuGH für die gleichlauten-

---

806 So der EuGH, Rs. C-70/95, 17.06.1997, Slg. 1997, I-3395, 3435 f. Rdnr. 38 f. (Sodemare SA).
807 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa.
808 Léger, Commentaire Article Par Article Des Traités UE Et CE, Art. 28 Rdnr. 10; Doerfert, Europarecht, A I S. 87.

den Begriffe in Art. 28 EGV aufgestellten „Dassonville-Formel“[809] auszugehen.[810] Die Dassonville-Formel besagt, dass als Maßnahme gleicher Wirkung i.S.d. Art. 28 EGV jede Regelung der Mitgliedstaaten anzusehen ist, die geeignet ist, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern.[811] Da aber nahezu jede einzelstaatliche Maßnahme, die sich regulierend auf die Produktion und den Vertrieb von Waren auswirkt, auch geeignet sein kann, Ausfuhren zu verhindern, die ohne diese Maßnahmen stattfinden könnten, muss die Dassonville-Formel eingeschränkt werden, um die Mitgliedstaaten in der Wahrnehmung ihrer Verantwortung für das legitime einzelstaatliche Gemeinwohl nicht handlungsunfähig zu machen. Für Art. 28 EGV hat der EuGH als Einschränkungskriterium die sogenannte „Cassis-de-Dijon-Rechtsprechung“[812] entwickelt.[813] Diese Cassis-Rechtsprechung ist allerdings nur zur Lösung des Problems ergangen, dass einzelstaatliche Regelungen den Zugang einer Ware zum inländischen Markt wegen ihrer Herkunft aus einem anderen Land im Vergleich zu Inlandswaren erschweren können. Dagegen stellt sich die Auswirkung allgemein anwendbarer Regelungen auf die Ausfuhr anders dar. Denn sie können Handelserschwernisse für Waren nicht wie bei der Einfuhr wegen der Herkunft der Waren aus einem anderen Mitgliedstaat mit anderem Regelungsregime bewirken, sondern wegen der Herkunft der Waren aus dem nämlichen Mitgliedstaat. Allgemeine einzelstaatliche Erschwernisse, die den Absatz inländischer Waren im Inland betreffen, sind aber – unabhängig von ihrer Unverzichtbarkeit oder Notwendigkeit – nach herkömmlichem Verständnis nicht primärer Gegenstand der gemeinschaftsrechtlichen Verbote zur Gewährleistung des freien Warenverkehrs. Folglich kann eine für Art. 29 EGV erhebliche Ausfuhrbeschränkung infolge allgemeiner Regelungen erst dann bejaht werden, wenn sich diese nicht nur ganz allgemein auf die Produktion und den Vertrieb, sondern gerade auf die Ausfuhr der Ware erschwerend auswirken.[814] Dieses einschränkende Kriterium der Dassonville-Formel, dass einzelstaatliche Regelungen primär eine beschränkende Wirkung auf die Ausfuhr der Waren haben müssen, um von Art. 29 EGV erfasst werden zu können, vertritt im Kern auch der EuGH. Nach seiner Rechtsprechung sind unter Maßnahmen gleicher Wirkung wie mengenmäßige Ausfuhrbeschränkungen staatliche Maßnahmen zu verstehen, die „spezifische Beschränkungen der Ausfuhrströme bezwecken oder bewirken und damit unterschiedliche Bedingungen für

---

809 Vgl. insoweit EuGH, Rs. 8/74, 11.07.1974, Slg. 1974, 837, 852 Rdnr. 5 (Dassonville); vgl. hierzu ausführlich unten unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (1).

810 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 34 EGV Rdnr. 15.

811 Herdegen, Europarecht, 2. Auflage, § 16 Rdnr. 288.

812 EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, S. 649 ff. (Rewe/Bundesmonopolverwaltung für Branntweine, sog. „Cassis de Dijon“); vgl. auch unten unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).

813 Vgl. hierzu Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 28 Rdnr. 19 ff.

814 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 34 EGV Rdnr. 17.

den Binnenhandel innerhalb eines Mitgliedstaates und seinen Außenhandel schaffen".[815] Weil auf die spezifische Beschränkung der Ausfuhrströme bei der Definition der Maßnahmen gleicher Wirkung i.S.d. Art. 29 EGV abgestellt wird, erübrigt sich eine Eingrenzung des Begriffs der Maßnahme gleicher Wirkung, wie sie in Art. 28 EGV durch die Cassis-Rechtsprechung und die Keck-Judikatur[816] vorgenommen wird.[817] Ein Verstoß gegen das in Art. 29 EGV fixierte Ausfuhrbeschränkungsverbot kommt somit nur dann in Betracht, wenn sich einzelstaatliche Regelungen und darauf gestützte behördliche Maßnahmen insbesondere auf die Ausfuhr von Waren erschwerend auswirken können.

Bei staatlichen Kontrollmaßnahmen gegen bestimmte, vom inländischen Content-Provider bereitgehaltene Warenangebote im Internet oder gegen die dafür im Internet vorhandene Werbung liegt zunächst regelmäßig eine Maßnahme gleicher Wirkung i.S.d. Dassonville-Formel vor. Gleichwohl ist Art. 29 EGV bei staatlichen Sperr- und Löschanordnungen nicht betroffen. Denn Sinn und Zweck dieser behördlichen Kontrollmaßnahmen ist einzig und allein, rechtswidrige Inhalte im Netz, die im Inland für die Nutzer bereitgehalten werden, unschädlich zu machen. Die Folge, dass Nutzer aus dem EU-Ausland möglicherweise keine Ware aus dem Inland per Internet bestellen oder sie von bestimmter Werbung nicht mehr erreicht werden können und deshalb die Ausfuhr gewisser Waren beeinträchtigt wird, ist lediglich ein Nebeneffekt der staatlichen Maßnahmen. Diese Ausfuhrbeschränkung ist aber kein primäres Ziel der staatlichen Kontrollmaßnahmen. Die Möglichkeit eines Eingriffs in den von Art. 29 EGV geschützten freien Warenverkehr durch staatliche Kontrollmaßnahmen ist für die vorliegende Fallvariante somit abzulehnen.[818]

(2) Niederlassungsfreiheit

Die Niederlassungsfreiheit i.S.d. Art. 43 ff EGV des inländischen Content-Providers ist ebenfalls von staatlichen Kontrollmaßnahmen nicht betroffen. Denn Art. 43 EGV (eventuell i.V.m. Art. 48 EGV) regelt nur „*Beschränkungen der freien Niederlassung von Staatsangehörigen eines Mitgliedstaats im Hoheitsgebiet eines anderen Mitglied-*

---

815 Vgl. EuGH, Rs. 15/79, 08.11.1978, Slg. 1979, 3409, 3415 Rdnr. 7 (Groenveld); EuGH, Rs. 155/80, 14.07.1981, Slg. 1981, 1993, 2009 Rdnr. 15 (Oebel); EuGH, Rs. C-47/90, 09.06.1992, Slg. 1992, I-3669, 3708 Rdnr. 12 (Delhaize).

816 EuGH, Rs. C-267/91 und C-268/91, 24.11.1993, Slg. 1993, I-6097, 6131 Rdnr. 15 (Keck und Mithouard); vgl. hierzu auch Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1511 sowie die späteren Ausführungen unten unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2).

817 Vgl. zu dieser Problematik ausführlich unten unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2). und (3).

818 Anstatt nur die Beeinträchtigung der Grundfreiheit zu prüfen, wurden hier bei der Prüfung der Warenverkehrsfreiheit und des Art. 29 EGV ausführlichere Untersuchungen durchgeführt. Dies entspricht nicht den übrigen Prüfungsgepflogenheiten. Aus Gründen der Übersichtlichkeit und der Vereinfachung war die eben erfolgte Bearbeitung des Art. 29 EGV und dessen Ablehnung jedoch unumgänglich.

staats".[819] Demnach ist bereits der Wortlaut nicht erfüllt, da sich der inländische Content-Provider im Inland und nicht in einem anderen Mitgliedstaat befindet.

(3) Dienstleistungsfreiheit

Durch die staatlichen Kontrollmaßnahmen könnte jedoch die in den Art. 49 ff. EGV geregelte Dienstleistungsfreiheit des Content-Providers betroffen sein.

Wie bereits an obiger Stelle erwähnt,[820] setzt die Inanspruchnahme der Dienstleistungsfreiheit zum einen ein grenzüberschreitendes Element und zum anderen das Merkmal der Entgeltlichkeit voraus.[821] Zu den Anwendungsfällen der Dienstleistungsfreiheit zählen wiederum die aktive und passive Dienstleistungsfreiheit sowie die Korrespondenzdienstleistungsfreiheit.[822] Regelmäßig wird der Nutzer aus dem EU-Ausland über das Internet an die angebotenen Daten gelangen wollen. Er wählt sich somit in das Internet ein, gelangt über das Netz an die bereitgehaltenen Informationen des Content-Providers und lässt sich von diesem die gewünschten Daten auf seinen Rechner schicken. Da weder der Dienstleistende, also der Content-Provider, noch der Dienstleistungsempfänger, sprich der Nutzer, sondern allein die Daten die Grenze der Mitgliedstaaten überschreiten, liegt hier ebenfalls ein Fall der Korrespondenzdienstleistungsfreiheit vor.[823] Denn letztendlich stellt die Verschickung der Daten vom Content-Provider zum Nutzer einen grenzüberschreitenden Vorgang bezüglich der Leistung dar.

Fraglich ist aber, ob sich der Content-Provider gerade hier auf die Korrespondenzdienstleistungsfreiheit berufen kann. Denn wie es sich aus dem Wortlaut der Art. 49 ff. EGV ergibt, sollte die Dienstleistungsfreiheit grundsätzlich nur gewährleisten, dass der Leistende seine Tätigkeit vorübergehend in dem Staat ausüben kann, wo die Leistung erbracht wird, und zwar unter den Voraussetzungen, die dieser Staat für seine eigenen Angehörigen vorschreibt. Es ist also ursprünglich Sinn und Zweck der Art. 49 ff. EGV gewesen, dass der Dienstleistende regelmäßig seine Leistungen ungehindert in einem Mitgliedstaat der EU erbringen kann. Zudem sieht die Dienstleistungsfreiheit gemäß Art. 49 I EGV eigentlich nur vor, dass der Dienstleistende gegen diskriminierende Maßnahmen des Staates geschützt ist, in dem er seine Leistungen erbringen will. Dagegen besagen die Art. 49 ff. EGV grundsätzlich nicht, dass der Inländer mit Hilfe der Dienstleistungsfreiheit auch gegen inländische Regelungen und Maßnahmen vorgehen kann.[824] Aus diesem Grund könnte der Standpunkt vertreten werden, dass sich ein in-

---

819 Vgl. hierzu Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 8.

820 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).

821 Herdegen, Europarecht, 2. Auflage, § 18 Rdnr. 324.

822 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).; Oppermann, Europarecht, § 24 Rdnr. 1496 ff.

823 Fastenrath/Müller-Gerbes, Europarecht, Teil 3 Rdnr. 132; Geiger, EUV/EGV, 3. Auflage, Art. 50 EGV Rdnr. 8.

824 Etwas anderes soll nur dann gelten, wenn sich der eigene Staatsangehörige in derselben Situation wie der ausländische Staatsangehörige befindet. Dann erscheint es dem EuGH (vgl. EuGH, Rs. 115/78, 07.02.1979, Slg. 1979, 399 ff. (Knoors)) gerechtfertigt, den eigenen Staatsangehörigen wie

ländischer Dienstleistungserbringer, der durch inländische Maßnahmen oder Regelungen an der Ausübung seiner Dienstleistungen gegenüber Dienstleistungsempfängern aus dem EU-Ausland gehindert wird, nicht auf die Art. 49 ff. EGV berufen kann.

Da der EuGH nun die Produktverkehrsfreiheit ebenfalls unter den Schutz der Dienstleistungsfreiheit gestellt hat,[825] hat er zwar die aktive und passive Dienstleistungsfreiheit dahingehend ausgedehnt worden, dass eine Grenzüberschreitung des Leistungserbringers bzw. des –empfängers nicht mehr nötig ist, weil der Grenzübertritt der Leistung für die Art. 49 ff EGV genügen soll. Diese Erweiterung der Dienstleistungsfreiheit durch den EuGH hat aber nichts an der Tatsache geändert, dass sich der Leistungserbringer – parallel zur aktiven Dienstleistungsfreiheit – bei bestimmten Beschränkungen hinsichtlich der Leistungserbringung nur auf die Art. 49 ff. EGV gegen den Mitgliedstaat, wohin er seine Leistung schickt, berufen kann. In einer jüngeren Entscheidung des EuGH[826] wurde jedoch festgestellt, dass Art. 49 EGV nicht nur für vom Staat des Leistungsempfängers, sondern auch vom Staat des Leistungserbringers auferlegte Beschränkungen gilt, selbst wenn es sich dabei um Maßnahmen handelt, die allgemein anwendbar und nicht diskriminierend sind sowie weder bezwecken noch bewirken, dem nationalen Markt einen Vorteil gegenüber den Dienstleistungserbringern aus anderen Mitgliedstaaten zu verschaffen.[827] Also fallen unter die Art. 49 ff. EGV auch staatliche Maßnahmen, durch die ein Dienstleistungserbringer aus demselben Staat daran gehindert wird, seine Leistungen in einem anderen Mitgliedstaat zu erbringen. Dies ergibt sich schon allein aus dem Wortlaut des Art. 49 EGV. Denn der Art. 49 EGV verbietet Beschränkungen des freien Dienstleistungsverkehrs innerhalb der Gemeinschaft allgemein. Folglich betrifft diese Vorschrift nicht nur vom Staat des Leistungsempfängers, sondern auch vom Staat des Leistungserbringers auferlegte Beschränkungen.[828]

---

einen fremden Staatsangehörigen zu behandeln. So sollen beispielsweise die eigenen Staatsangehörigen eines bestimmten Mitgliedstaats nicht von der Anwendung des Gemeinschaftsrechts ausgeschlossen werden, wenn sie sich auf Grund der Tatsache, dass sie rechtmäßig im Hoheitsgebiet eines anderen Mitgliedstaats ansässig waren und dort eine nach Gemeinschaftsrecht anerkannte berufliche Qualifikation erworben haben, gegenüber ihrem Herkunftsland in einer Lage befinden, die mit derjenigen anderer Personen, die in den Genuss der durch den EGV garantierten Rechte und Freiheiten kommen, vergleichbar ist. Ausführlich zu diesem viel diskutierten Problem der „umgekehrten Diskriminierung“ (auch: discrimination à rebours): Epiney, Umgekehrte Diskriminierungen. Zulässigkeit und Grenzen der discrimination à rebours nach europäischem Gemeinschaftsrecht und nationalem Verfassungsrecht, S. 19 ff.

Dieses rechtliche Problem ist für vorliegende Arbeit allerdings nicht von Bedeutung, da die staatlichen Kontrollmaßnahmen gegen den Content-Provider nicht zwischen der Nationalität des Content-Providers differenzieren, sondern unterschiedslos eine Lösch- und/oder Sperranordnung enthalten.

825 EuGH, verbundene Rs. C-271/90, C-281/90 und C-289/90, 17.11.1992, I-5833 ff. (Spanien/Kommission).

826 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141 ff. (Alpine Investments BV).

827 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1142 3. Leitsatz (Alpine Investments BV).

828 Vgl. auch: EuGH, Rs. C-18/93, 17.05.1994, Slg. 1994, I-1783, 1822 Rdnr. 30 (Corsica Ferries); EuGH, Rs. C-379/92, 14.07.1994, Slg. 1994, I-3453, 3501 Rdnr. 40 (Peralta); EuGH, Rs. C-381/93, 05.10.1994, Slg. 1994, I-5145, 5168 Rdnr. 14 (Kommission/Frankreich); in diesen Entscheidungen hat der EuGH wiederholt festgestellt, dass sich ein Unternehmen gegenüber dem Staat, in dem es

Hieraus ergibt sich folgendes: Aus Sicht des inländischen Content-Providers können die staatlichen Kontrollmaßnahmen ebenfalls in seine vom EGV gewährleistete Dienstleistungsfreiheit eingreifen, da er in seiner Korrespondenzdienstleistungsfreiheit beschränkt wird. Es handelt sich zwar um innerstaatliche Anordnungen, die aufgrund von innerstaatlichen Regelungen[829] gegen einen inländischen Content-Provider ergangen sind. Weil aber der Nutzer aus dem EU-Ausland stammt und er seinen Sitz im EU-Ausland hat, die Dienstleistung des inländischen Dienstleistungserbringers somit an das EU-Ausland adressiert ist, sind die Art. 49 ff EGV – entgegen ihres Wortlauts – auf eine derartige Fallkonstellation anwendbar.[830]
Der Content-Provider, der durch staatliche Kontrollmaßnahmen an der Erbringung seiner Daten-Dienstleistung gehindert wird, erfährt somit eine Beeinträchtigung seiner Korrespondenzdienstleistungsfreiheit gemäß den Art. 49 ff. EGV.

d. Weitere Kombinationen der genannten beteiligten Personen

Es sind nun noch weitere Kombinationen der angesprochenen Personen denkbar, die sich entweder im Inland oder EU-Ausland befinden. So könnten der Content-Provider und der Nutzer aus dem EU-Ausland stammen. Folglich besteht wiederum die Möglichkeit, diese Fallvariante bis ins Detail zu unterscheiden und jede erdenkliche Kombination, die bereits oben in den Fallvarianten I und II angesprochen wurde, auf ihre europarechtliche Relevanz hin zu überprüfen.
Dieser Aufwand ist jedoch entbehrlich. Denn da bei dieser wie bei der Fallvariante I bzw. Fallvariante II erneut der Content-Provider bzw. Nutzer aus dem EU-Ausland stammt und allein die Sichtweise des Content-Providers maßgeblich ist, ergeben sich letztendlich keine neuen Konstellationen mit anderen europarechtlichen Ergebnissen.

e. Zusammenfassung

aa. Fallvariante I

Insgesamt lässt sich somit sagen, dass bei der Fallvariante I der Content-Provider, sofern es sich hierbei um eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland oder eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland handelt, die jedoch neben der reinen Technik noch weitere Komponenten im Rahmen des Content-Providings im Inland hat, durch die staatlichen Kontrollmaß-

---

seinen Sitz hat, auf den freien Dienstleistungsverkehr berufen kann, sofern die Leistungen an Leistungsempfänger erbracht werden, die in einem anderen Mitgliedstaat ansässig sind.

829 Als Regelungen sind hier vor allem das jeweilige Polizei- und Sicherheitsrecht sowie § 5 und § 18 MDStV zu nennen. Vgl. insoweit oben unter B. 2. Teil. II. 5.

830 Darin könnte ein Widerspruch zwischen der Warenverkehrsfreiheit und der Dienstleistungsfreiheit gesehen werden. Dieses Ergebnis erklärt sich jedoch damit, dass bei den Normen zur Dienstleistungsfreiheit eine dem Art. 29 EGV entsprechende Vorschrift nicht existiert und der EuGH die Anwendbarkeit der Dienstleistungsfreiheit einseitig ausgedehnt hat.

nahmen entweder in seiner Niederlassungsfreiheit nach den Art. 43 ff. EGV oder Dienstleistungsfreiheit nach den Art. 49 ff. EGV beeinträchtigt wird.[831]
Dagegen ist der Content-Provider, sofern er eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist und sich lediglich seine zur Ausübung des Content-Providings benötigte Hard- und Software im Inland befindet, ausschließlich in seiner Dienstleistungsfreiheit gemäß den Art. 49 ff EGV betroffen.
Des weiteren kann der Content-Provider – je nachdem, ob er Waren aus dem EU-Ausland im Internet anbietet oder bewirbt und diese Waren, wenn sie vom Nutzer bestellt werden, die Grenze eines Mitgliedstaates überschreiten – mittelbar auch in seiner Warenverkehrsfreiheit nach den §§ 28 ff. EGV verletzt sein.

bb. Fallvariante II

Bei der Fallvariante II kann der inländische Content-Provider, sofern der Nutzer aus dem EU-Ausland stammt und seinen Sitz im EU-Ausland hat, in seiner Dienstleistungsfreiheit in Form der Korrespondenzdienstleistungsfreiheit tangiert sein.
Alle übrigen Fallkonstellationen weisen aus der Sicht des Content-Providers keine Berührung zum Europarecht auf.

f. Vereinbarkeit der europarechtlich relevanten Kontrollmaßnahmen mit den jeweiligen Grundfreiheiten

Welche Fallkonstellationen dazu führen, dass der Content-Provider europarechtlich durch die staatlichen Kontrollmaßnahmen beeinträchtigt wird, wurde zuvor bereits ausführlich behandelt. Diese jeweiligen Fallvarianten müssen nun daraufhin untersucht werden, ob die aufgezeigten europarechtlichen Eingriffe durch staatliche Anordnungen in rechtmäßiger Weise erfolgen. Hierfür ist es nötig, die einzelnen Grundfreiheiten näher zu betrachten und die Fallkonstellationen, die einen Eingriff in bestimmte Grundfreiheiten ergeben haben, hieran zu messen.

aa. Warenverkehrsfreiheit

Die Prüfung der Sperr- und/oder Löschanordnungen gegen den Content-Provider hat gezeigt, dass bei folgenden Fallkonstellationen die Warenverkehrsfreiheit tangiert sein kann:
Zum einen hat der Content-Provider als natürliche Person aus dem EU-Ausland seinen Wohnsitz im Inland und bietet dort seinen Dienst an. Zum anderen hält der Content-Provider als natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-

---

831 Häufig wird aber wohl nicht die Dienstleistungsfreiheit, sondern die Niederlassungsfreiheit einschlägig sein. Da der weite Niederlassungsbegriff sehr schnell durch weitere mit dem Content-Providing im Zusammenhang stehende Komponenten erfüllt ist. Dies wird bei der nachfolgenden Prüfung berücksichtigt, so dass vermehrt bei dieser Fallkonstellation von einer Beeinträchtigung der Niederlassungsfreiheit ausgegangen wird.

Ausland seinen Dienst im Inland für den Nutzer bereit, da sich die für das Content-Providing benötigte Technik im Inland befindet. Denkbar ist auch die vorgenannte Konstellation, bei der neben der Technik noch andere für das Content-Providing wichtige Komponenten im Inland vertreten. Der Nutzer stammt in jedem dieser Fälle aus Deutschland.
Ein Eingriff in die Warenverkehrsfreiheit setzt jedoch immer voraus, dass der Content-Provider in seinem für den Nutzer bereitgestellten Inhalt Waren anbietet oder für Waren wirbt[832], die aus dem EU-Ausland zum deutschen Nutzer gebracht werden müssen. Ist dies zu bejahen, dann wird die Warenverkehrsfreiheit in den genannten Fallkonstellationen mittelbar betroffen.

(1) Dassonville-Formel

Der Umstand, dass auch indirekte Beschränkungen des Handels zwischen den Mitgliedstaaten unter die Warenverkehrsfreiheit fallen, geht auf die vom EuGH zu Art. 28 EGV aufgestellte „Dassonville-Formel“[833] zurück.[834] In dieser Entscheidung definierte der EuGH, was unter dem Begriff der „*Maßnahmen gleicher Wirkung*“ i.S.d. Art. 28 EGV zu verstehen ist. Danach soll „jede Handelsregelung der Mitgliedstaaten, die geeignet ist, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern“, als Maßnahme gleicher Wirkung wie eine mengenmäßige Beschränkung i.S.d. Art. 28 EGV anzusehen sein.[835] Die Dassonville-Formel umfasst in ihrer Grundform jegliche Diskriminierung eingeführter Waren gegenüber einheimischen Erzeugnissen.[836] Folglich fallen auch Werbe- oder Anzeigenverbote für bestimmte Waren unter diese Formel, da sie zumindest indirekt dazu geeignet sind, den innergemeinschaftlichen Handel zu behindern. Der Content-Provider, der seine Waren im Internet nicht mehr seinen Nutzern zugänglich machen darf, ist in seiner Freiheit grundsätzlich beschränkt, seine Waren ungehindert europaweit anzubieten. Durch staatliche Kontrollmaßnahmen, welche die Löschung oder Sperrung der Warenangebote bzw. Werbung beim Content-Provider zum Ziel haben, wird also in die Warenverkehrsfreiheit mittelbar eingegriffen.
Wie sich jedoch unschwer erkennen lässt, würde durch eine uneingeschränkte Anwendung der Dassonville-Formel jede staatliche Maßnahme, die in gewisser Weise einen Einfluss auf den europäischen Handel hätte, unter die Norm des Art. 28 EGV fallen.

---

832 Da das virtuelle Anbieten und Bewerben von Waren als Annex zur Warenverkehrsfreiheit gilt, müssen derartige Beschränkungen der Werbung anhand der Art. 28 ff. EGV geprüft werden. Gleiches gilt demnach auch für das einfache Anbieten von Waren zum Bestellen über das Internet, da dies die Vorstufe zum Erwerb von Waren ist. Vgl. hierzu: Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 EGV Rdnr. 36.

833 EuGH, Rs. 8/74, 11.07.1974, Slg. 1974, 837, 852 Rdnr. 5 (Dassonville).

834 Vgl. insoweit auch oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (1).

835 Schweitzer/Hummer, Europarecht, § 14 Rdnr. 1116.

836 Herdegen, Europarecht, 2. Auflage, § 16 Rdnr. 289.

Der EuGH sah sich deshalb gezwungen, der durch die Dassonville-Formel nahezu uferlosen Ausweitung des Begriffs der Maßnahmen gleicher Wirkung Grenzen zu setzen. Dies geschah durch die Keck-Rechtsprechung.[837]

(2) Keck-Formel

Durch die sogenannte „Keck-Formel" des EuGH[838] wurde die Anwendbarkeit der Dassonville-Formel und somit des Art. 28 EGV grundsätzlich bei allgemein geltenden, bestimmten Verkaufsmodalitäten unter gewissen Voraussetzungen verneint.[839] Die Keck-Rechtsprechung setzt dabei voraus, dass die Behinderung auf eine bestimmte Verkaufsmodalität zurückzuführen ist, die für alle betroffenen Wirtschaftsteilnehmer gilt, also nicht diskriminierend ist, und den Absatz der inländischen Erzeugnisse und der Erzeugnisse aus anderen Mitgliedstaaten rechtlich und tatsächlich in der gleichen Weise berührt.[840] Leider versäumte es der EuGH in seinem Keck-Urteil, den Begriff der „Verkaufsmodalität" exakt zu definieren. Statt dessen zählte der EuGH lediglich Regelungstypen auf, für die es bei der bisherigen Rechtsprechung zur Dassonville-Formel bleiben soll, weil es sich nicht um eine bestimmte Verkaufsmodalität i.S.d. Keck-Formel handelt. Als solche nennt der EuGH Rechtsvorschriften, wonach Waren „hinsichtlich ihrer Bezeichnung, ihrer Form, ihrer Abmessungen, ihres Gewichts, ihrer Zusammensetzung, ihrer Aufmachung, ihrer Etikettierung und ihrer Verpackung" bestimmten Vorschriften entsprechen müssen.[841] Diesen Vorschriften ist dabei gemeinsam, dass sie sich auf das Produkt als solches beziehen, also „produktbezogen" sind.[842] Damit kann zwar der Begriff der Verkaufsmodalität in gewissem Maße negativ eingeschränkt werden. Ungeklärt bleibt allerdings, welcher Sachverhalt positiv von dieser Rechtsfigur erfasst wird. Als Auslegungshilfe, wann eine Verkaufsmodalität vorliegt, muss deshalb die Rechtsprechung des EuGH zum Keck-Urteil selbst und seine anschließenden Entscheidungen dazu herangezogen werden. So wurde im Keck-Urteil ein französisches Verbot des Weiterverkaufs von Waren zum Verlustpreis als Verkaufsmodalität eingestuft. Zu den

---

837 Schweitzer/Hummer, Europarecht, § 14 Rdnr. 1118.

838 Vgl. hierzu EuGH, verbundene Rs. C-267/91 und C-268/91, 24.11.1993, Slg. 1993, I-6097, 6131 Rdnr. 16 (Keck und Mithouard):
„Demgegenüber ist entgegen der bisherigen Rechtsprechung die Anwendung nationaler Bestimmungen, die bestimmte Verkaufsmodalitäten beschränken oder verbieten, auf Erzeugnisse aus anderen Mitgliedstaaten nicht geeignet den Handel zwischen den Mitgliedstaaten im Sinne des Urteils Dassonville unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern, sofern diese Bestimmungen für alle betroffenen Wirtschaftsteilnehmer gelten, die ihre Tätigkeit im Inland ausüben, und sofern sie den Absatz der inländischen Erzeugnisse und der Erzeugnisse aus anderen Mitgliedstaaten rechtlich wie tatsächlich in der gleichen Weise berühren."

839 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 239.

840 Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 29 Rdnr. 27.

841 Vgl. hierzu EuGH, verb. Rs. C-267/91 und C-268/91, 24.11.1993, Slg. 1993, I-6097, 6131 Rdnr. 15 (Keck und Mithouard); diese Aufzählung wiederholt der EuGH darüber hinaus in seinem Urteil EuGH, Rs. C-315/92, 02.02.1994, Slg. 1994, I-317, 335 Rdnr. 13 (Verband Sozialer Wettbewerb).

842 Schweitzer/Hummer, Europarecht, § 14 Rdnr. 1120.

Verkaufsmodalitäten rechnet der EuGH auch das Verbot der Werbung für apothekenübliche Waren außerhalb der Apotheke,[843] Regelungen über Ladenschlusszeiten[844] und den Ausschluss eines bestimmten Wirtschaftssektors von der Fernsehwerbung[845].[846] Hierbei handelt es sich regelmäßig um Vorschriften, die eher den Vertrieb der Ware betreffen. Letztendlich lässt sich deshalb sagen, dass der EuGH seit seiner Keck-Rechtsprechung bei der Frage, ob eine nationale Vorschrift unter den Begriff der bestimmten Verkaufsmodalität zu subsumieren ist, zwischen produkt- und vertriebsbezogenen nationalen Beschränkungen unterscheidet. Während er für die produktbezogenen an seiner ursprünglichen Dassonville-Rechtsprechung festhält, gilt nur für die vertriebsbezogenen, dass diese – falls die übrigen Voraussetzungen vorliegen – von der Keck-Formel erfasst werden, da sie als Verkaufsmodalitäten anzusehen sind. Somit werden vertriebsbezogene nationale Beschränkungen nicht mehr am Verbot von Art. 28 EGV gemessen, sofern die Vorschriften nicht diskriminieren und keine Aufsplitterung des Gemeinsamen Marktes in nationale Märkte zur Folge haben, selbst wenn sie geeignet sind, im Ergebnis zu einer Behinderung des freien Warenverkehrs zwischen den Mitgliedstaaten zu führen.[847]

Fraglich ist nun, wie staatliche Kontrollmaßnahmen gegen das Angebot von Waren bzw. die damit verbundene Werbung beim Content-Provider anhand der Keck-Rechtsprechung zu beurteilen sind. Zunächst ist darauf hinzuweisen, dass es verschiedene Gründe gibt, das Angebot zum Bestellen von Produkten oder die Werbung für bestimmte Waren im Internet durch staatliche Anordnung sperren bzw. löschen zu lassen. Häufig handelt es sich dabei um Waren[848] mit rassistischem, rechts- oder linksradikalem sowie pornographischem Hintergrund. In den meisten Fällen ergeht deshalb eine behördliche Verfügung gegen das Angebot oder die Werbung für solche Produkte nicht wegen der Werbung oder des eigentlichen Angebots, sondern wegen der Waren, die sich dahinter verbergen. Dies lässt eigentlich den Schluss zu, dass eine Sperr- und/oder Löschanordnung als eine produktbezogene Maßnahme anzusehen ist, auf welche die Keck-Formel keine Anwendung findet, da es sich hierbei um keine bestimmten Ver-

---

843 Vgl. EuGH, Rs. C-292/92, 15.12.1993, Slg. 1993, I-6787, ff. (Hünermund u.a.); zu einem Werbeverbot für im Einfuhrstaat nicht zugelassener Arzneimittel vgl. EuGH, Rs. C-230/93, 10.11.1994, Slg. 1994, I-5243 ff. (Ortscheid).

844 Vgl. EuGH, verbundene Rs. C-401/92 und C-402/92, 02.06.1994, Slg. 1994, I-2199 ff. (Tankstation`t Heukske vof und Boermans); EuGH, verbundene Rs. C-69/93 und C-258/93, 02.06.1994, Slg. 1994, I-2355 ff. (Punto Casa SpA).

845 Vgl. EuGH, Rs. C-412/93, 09.02.1995, Slg. 1995, I-179 ff. (Société d´importation Edouard Leclerc-Simplec). Allerdings gilt diese Rechtsprechung nicht für jede Art von Werbeverboten, vgl. insoweit Schwarze, „Medienfreiheit und Medienvielfalt im Europäischen Gemeinschaftsrecht“, ZUM 2000, 779, 786.

846 Weitere Fälle und Rechtsprechung zum Begriff der bestimmten Verkaufsmodalitäten sind bei Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 255 und Herdegen, Europarecht, 2. Auflage, § 16 Rdnr. 291 f. zu finden.

847 Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1511; Dubach, „Freier Warenverkehr in der EU: Der Gerichtshof auf neuen Pfaden?“, DVBl. 1995, S. 595, 599 f.

848 Zu nennen sind hier beispielsweise Bücher, Tonträger oder Videofilme.

kaufsmodalitäten handelt. An diesem Ergebnis ist jedoch problematisch, dass die behördliche Regelung des Internets unmittelbar in die Vertriebsmethoden des Content-Providers eingreift und diese verbietet. Denn sowohl die Werbung als auch das Angebot zum Bestellen von bestimmten Waren im Internet stellt grundsätzlich nur eine neue Art des grenzüberschreitenden Vertriebs von Waren dar.[849] Dies würde eher dafür sprechen, dass die Keck-Rechtsprechung doch einschlägig ist. Leider hat der EuGH derartige oder ähnlich gelagerte Fälle noch nicht zu entscheiden gehabt. Denn allein aufgrund der Einordnung des Versandhandels als Verkaufsmodalität kann noch nicht davon ausgegangen werden, dass das Versandverbot unter die Keck-Formel fällt. Mit dem Keck-Urteil hat der EuGH nämlich nicht allgemein alle, sondern nur „bestimmte", nicht diskriminierende Verkaufsmodalitäten dem Anwendungsbereich der Warenverkehrsfreiheit entzogen.[850] Ferner wurde vom EuGH im Mars-Urteil[851] festgestellt, dass im Rahmen von Werbeverboten zu differenzieren ist: Soweit sich ein bestimmtes nationales Werbeverbot unmittelbar auf die Produktdarbietung und seine physische Erscheinung auswirkt, der Importeur etwa nationale Sonderverpackungen herstellen muss und ihm durch die Umstellung der Produktion Mehrkosten in Herstellung und Entwicklung der Verpackung entstehen, dann stellt eine solche Regelung keine Verkaufsmodalität i.S.d. Keck-Formel dar, sondern eine Maßnahme gleicher Wirkung gemäß Art. 28 EGV.[852]
Wird nun diese Entscheidung des EuGH als wesentlicher Anhaltspunkt herangezogen und die darin enthaltenen Überlegungen werden auf die Sperr- bzw. Löschanordnungen gegenüber bestimmten Warenangeboten und Werbung im Internet übertragen, ergibt sich folgendes: Der EuGH nimmt bereits dann einen Verstoß gegen die Warenverkehrsfreiheit und somit eine Maßnahme gleicher Wirkung i.S.d. Art. 28 EGV an, wenn staatliche Regelungen ein Werbeverbot enthalten, wodurch der Warenanbieter Kosten erhöhende Maßnahmen an seinem Produkt vornehmen muss, um die Ware in diesem Mitgliedstaat anbieten zu können. Der Importeur kann also durch bestimmte Maßnahmen am Produkt den Vorschriften des das Werbeverbot verhängenden Mitgliedstaates entsprechen.[853] Etwas anderes gilt dagegen für die Waren, gegen deren Werbung bzw. Bestellmöglichkeiten sich die staatlichen Kontrollmaßnahmen richten. Diese Produkte sind im Inland generell nicht erwünscht. Lediglich die komplette Abänderung der indizierten in eine nicht zu beanstandende Produktpalette würde die Sperr- bzw. Löschmaßnahmen wieder aufheben. Die staatlichen Kontrollmaßnahmen stellen demnach ein Mehr an Auswirkungen auf die beworbenen bzw. angebotenen Produkte dar, als dies im Mars-Urteil der Fall gewesen ist. Folglich muss hier erst recht eine produktspezifische Aus-

---

849 Lüder, „Mars: Zwischen Keck und Cassis", EuZW 1995, 609.

850 Koenig/Engelmann, „E-Commerce mit Arzneimitteln im Europäischen Binnenmarkt und die Freiheit des Warenverkehrs", ZUM 2001, 19, 21.

851 EuGH, Rs. C-470/93, 09.07.1995, Slg. 1995, I-1923 ff. (Mars).

852 Vgl. zu diesem Thema, da ebenso entschieden, auch EuGH, Rs. C-315/92, 02.02.1994, Slg. 1994, I-317, 335 Rdnr. 13 (Verband Sozialer Wettbewerb).

853 Beispielsweise hätte der Warenanbieter im Mars-Urteil seine Verpackung neu gestalten müssen.

wirkung durch die Sperr- und Löschanordnungen auf die Waren bejaht werden. Bestimmte Verkaufsmodalitäten i.S.d. Keck-Rechtsprechung liegen hier nicht mehr vor, vielmehr wird durch die Kontrollmaßnahmen der Zugang zum Markt selbst verhindert.[854] Die Dassonville-Formel bleibt also anwendbar, so dass eine Maßnahme gleicher Wirkung gegeben und der Art. 28 EGV einschlägig ist.

(3) Cassis-de-Dijon-Rechtsprechung

Neben der Keck-Formel hat der EuGH bereits in einem viel früheren Urteil, dem sogenannten „Cassis-de-Dijon-Fall“[855] versucht, die ausufernde Anwendbarkeit der Dassonville-Formel im Rahmen von Art. 28 EGV einzudämmen.[856] Im Gegensatz zum Keck-Urteil, wo der EuGH unter bestimmten Umständen die Dassonville-Formel für unanwendbar erklärt, schränkt er im Cassis-de-Dijon-Urteil die Anwendbarkeit des Art. 28 EGV ein.[857] Denn wie sich aus Art. 30 EGV ergibt, verbietet der EGV Handelsbeschränkungen i.S.d. Art. 28 f. EGV nicht absolut, sondern sie können unter bestimmten Voraussetzungen gerechtfertigt sein. Neben diesen ausdrücklichen Rechtfertigungen hat der EuGH für Art. 28 EGV tatbestandsimmanente Schranken entwickelt, die für bestimmte Beschränkungen eine Rechtfertigung nach Art. 30 EGV entbehrlich machen, da bereits die Norm des Art. 28 EGV dann nicht erfüllt und somit kein Verstoß gegen die Warenverkehrsfreiheit gegeben ist.[858] Diese immanenten Schranken hat der EuGH in der „Cassis-de-Dijon-Formel“[859] aufgestellt.[860] Demnach können Beschränkungen der Warenverkehrsfreiheit wegen zwingender Erfordernisse gerechtfertigt sein.

---

854 So auch Koenig/Engelmann in: „E-Commerce mit Arzneimitteln im Europäischen Binnenmarkt und die Freiheit des Warenverkehrs“, ZUM 2001, 19, 22 und Leible in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, Band 1, Art. 28 Rdnr. 30.

855 EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, 649 ff. (Reve/Bundesmonopolverwaltung für Branntwein, sog. „Cassis-de-Dijon“).

856 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 192.

857 Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 28 Rdnr. 21.

858 Dubach, „Freier Warenverkehr in der EU: Der Gerichtshof auf neuen Pfaden?“, DVBl. 1995, 595, 598; Streinz, Europarecht, 4. Auflage, § 12 Rdnr. 738 ff.; Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1135; Leible in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, Band 1, Art. 28 Rdnr. 20; eine andere Meinung in der Literatur vertritt dagegen die Ansicht, dass die Cassis-de-Dijon-Rechtsprechung zusätzlich zu Art. 30 EGV weitere Rechtfertigungsgründe enthält. So beispielsweise: Becker in: Schwarze (Hrsg.), EU-Kommentar, Art. 28 Rdnr. 108 f.

859 EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, 649, 662 Rdnr. 8 (Reve/Bundesmonopolverwaltung für Branntwein, sog. „Cassis-de-Dijon“):
„In Ermangelung einer gemeinschaftlichen Regelung der Herstellung und Vermarktung von Weingeist [...] ist es Sache der Mitgliedstaaten, alle die Herstellung und Vermarktung von Weingeist und alkoholischen Getränken betreffenden Vorschriften für ihr Hoheitsgebiet zu erlassen. Hemmnisse für den Binnenhandel der Gemeinschaft, die sich aus den Unterschieden der nationalen Regelungen ergeben, müssen hingenommen werden, soweit diese Bestimmungen notwendig sind, um zwingenden Erfordernissen gerecht zu werden, insbesondere den Erfordernissen einer wirksamen steuerlichen Kontrolle, des Schutzes der öffentlichen Gesundheit, der Lauterkeit des Handelsverkehrs und des Verbraucherschutzes.“

860 Mittlerweile haben sich deshalb – neben den Rechtfertigungsgründen oder Ausnahmetatbeständen, die im EGV bei den jeweiligen Grundfreiheiten verankert sind – durch eine derartige gefestigte

Wegen des Begriffs „insbesondere“ in der Cassis-Formel ist der Katalog der „zwingenden Erfordernisse“ nicht abschließend. In der Folgezeit hat der EuGH bei anderen Entscheidungen Handelshemmnisse, die sich aus Gründen des Umweltschutzes[861] oder aus kulturellen Gründen[862] ergeben, teilweise ebenfalls hingenommen. Das Erfordernis des Gesundheitsschutzes prüft der EuGH dagegen neuerdings nur noch im Rahmen von Art. 30 EGV, wo es explizit genannt ist.[863] Des weiteren ist zu beachten, dass nach seiner Rechtsprechung die Cassis-Formel nur unterschiedslose Maßnahmen – also Maßnahmen, die inländische und aus EG-Staaten importierte Waren gleichermaßen treffen – rechtfertigen kann.[864]

Die staatlichen Kontrollmaßnahmen differenzieren nicht zwischen inländischen und eingeführten Waren,[865] sondern wollen vielmehr jedes rechtswidrige Warenangebot bzw. die Werbung hierfür sperren bzw. löschen lassen. Folglich handelt es sich bei ihnen um nicht diskriminierende Maßnahmen, worauf die Cassis-de-Dijon-Formel Anwendung findet. Die Behinderung der Warenverkehrsfreiheit kann nach der Cassis-Rechtsprechung nur dann gerechtfertigt sein, wenn sie in einem Bereich erfolgt, für den keine abschließende Gemeinschaftsregelung besteht.[866] Da noch keine abschließende Gemeinschaftsregelung für derartige Lösch- und/oder Sperrmaßnahmen existiert,[867] ist dieses Kriterium erfüllt. Gemäß der Cassis-Formel sind die auf die staatlichen Kontrollmaßnahmen beruhenden Handelshemmnisse also dann hinzunehmen, wenn sie notwendig sind, um zwingenden Erfordernissen gerecht zu werden – insbesondere den

---

Rechtsprechung des EuGH Grundzüge einer richterrechtlichen Schrankensystematik herauskristallisiert. Diese gemeinsame Schrankensystematik findet, trotz der unterschiedlichen sachlichen Reichweite und der strukturellen Abweichungen der einzelnen Grundfreiheiten, in mehr oder weniger abgewandelter Form auf jede Grundfreiheit Anwendung. Letztendlich ist die Grundstruktur der vom EuGH aufgestellten Schrankensystematik wie folgt ausgestaltet: Es besteht ein absolutes Verbot offener Diskriminierungen aus Anlass der Staatsangehörigkeit. Es müssen also nationale Maßnahmen in nichtdiskriminierender Weise angewandt werden. Des weiteren sind die Beschränkungen nur aus zwingenden Gründen des Allgemeininteresses zulässig. Außerdem müssen sie geeignet sein, die Verwirklichung des mit ihnen verfolgten Ziels zu gewährleisten und sie dürfen nicht über das hinausgehen, was zur Erreichung des Ziels erforderlich ist (Verhältnismäßigkeit). Vgl. hierzu insbesondere: Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 53 f.; Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1680.

861 EuGH, Rs. 240/83, 07.02.1985, Slg. 1985, 531, 549 Rdnr. 14 (ADBHU); EuGH, Rs. 302/86, 20.09.1988, Slg. 1988, 4607, 4630 Rdnr. 8 ff. (Kommission/Dänemark); EuGH, Rs. C-2/90, 09.07.1992, Slg. 1992, 4431, 4479 f. Rdnr. 32 ff. (Kommission/Belgien).

862 EuGH, verbundene Rs. 60/84 und 61/84, 11.07.1985, Slg. 1985, 2605, 2626 Rdnr. 22 (Cinéthèque).

863 EuGH, Rs. 178/84, 12.03.1987, Slg. 1987, 1227, 1273 f. Rdnr. 42 ff. (Kommission/Bundesrepublik Deutschland).

864 EuGH, Rs. 113/80, 17.06.1981, Slg. 1981, 1625, 1639 Rdnr. 10 (Kommission/Irland); EuGH, Rs. 59/82, 20.04.1983, Slg. 1983, 1217, 1227 Rdnr. 11 (Weinvertriebs-GmbH); EuGH, Rs. 229/83, 10.01.1985, Slg. 1985, 1, 35 Rdnr. 30 (Leclerc).

865 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 195.

866 EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, 649, 662 Rdnr. 8 (Reve/Bundesmonopolverwaltung für Branntwein sog. „Cassis-de-Dijon“); EuGH, Rs. 261/81, 10.11.1982, Slg. 1982, 3961, 3972 Rdnr. 12 (Rau); EuGH, Rs. 298/87, 14.07.1988, Slg. 1988, 4489, 4511 Rdnr. 15 (SMANOR).

867 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 254.

Erfordernissen einer wirksamen steuerlichen Kontrolle, der Lauterkeit des Handelsverkehrs und des Verbraucherschutzes – und mit denen ein im allgemeinen Interesse liegendes Ziel verfolgt wird, das den Erfordernissen des freien Warenverkehrs, der eine der Grundlagen der Gemeinschaft darstellt, gerecht wird.[868]

Es könnte zwar die Ansicht vertreten werden, dass eine gegen virtuelle Werbung bzw. gegen die Möglichkeit der Bestellung von illegalen Waren gerichtete staatliche Sperr- bzw. Löschverfügung aus Erwägungen des Gemeinwohls zwingend erforderlich ist,[869] zumal die Cassis-Formel nicht abschließend ist und somit nicht ausgeschlossen werden kann, dass auch derartige Handelsbeschränkungen hierunter gefasst werden dürfen. Dieser Gedankengang ist aber abzulehnen. Denn die Cassis-Formel stellt eine Ausnahmeregelung zu Art. 28 EGV dar und muss daher – wie Art. 30 EGV – restriktiv angewendet werden.[870] Lediglich die Fallgruppen, die der EuGH in seiner Cassis-Entscheidung und in der darauffolgenden Rechtsprechung genannt hat,[871] sind auf die Sperr- und/oder Löschverfügungen sinnvollerweise anzuwenden. Darüber hinaus werden nationale Beschränkungen der Warenverkehrsfreiheit, die aus Gründen der öffentlichen Sicherheit, Ordnung bzw. Sittlichkeit ergehen, bereits von Art. 30 EGV geregelt.

Dies hat zur Folge, dass die Cassis-Formel insoweit nicht einschlägig ist. Denn zwingende Erfordernisse für diese staatlichen Kontrollmaßnahmen ergeben sich weder aus Gründen einer wirksamen steuerlichen Kontrolle, der Lauterkeit des Handelsverkehrs, des Verbraucherschutzes sowie aus sonstigen Erwägungen des Allgemeinwohls, die der EuGH mittlerweile anerkannt hat[872]. Folglich greifen die tatbestandsimmanenten

---

868 EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, 649, 662 und 664 Rdnr. 8 und 14 (Reve/Bundesmonopolverwaltung für Branntwein sog. „Cassis-de-Dijon"); vgl. auch: Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 28 Rdnr. 20.

869 So beispielsweise Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern", CR 1999, 438, 444. In diesem Aufsatz wird allerdings diese Meinung für die Dienstleistungsfreiheit angenommen. Demnach soll eine Rechtfertigung aus zwingenden Gründen des Allgemeinwohls grundsätzlich möglich sein. Wenn dies für die Dienstleistungsfreiheit gilt, wäre es nur konsequent, den Rechtfertigungsgrund auch bei der Warenverkehrsfreiheit zu bejahen. Etwas anderes kann sich auch nicht daraus ergeben, dass in dem Aufsatz (fälschlicherweise, vgl. unten unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).) eine Anwendbarkeit des „ordre public" i.S.d. Art. 55, 46 EGV abgelehnt wird. Aus den nachstehenden Gründen kann dieser Ansicht jedoch nicht gefolgt werden.

870 Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1522.

871 Vgl. hierzu die bei Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 186 Fn. 420 zusammengestellte Rechtsprechung des EuGH.

872 Hierzu zählen insbesondere der Umweltschutz, die Verbesserung der Lebens- und Arbeitsbedingungen der Arbeitskräfte, die Kulturpolitik, der Schutz landesweiter oder regionaler sozialer und kultureller Besonderheiten, der Schutz und der ordnungsgemäße Betrieb des öffentlichen Fernmeldenetzes, die Erhaltung des finanziellen Gleichgewichts und der Sozialsysteme und der Statistik. Vgl. die Aufstellung der einzelnen Rechtsprechungen bei Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 224 ff. Fn. 525 ff. sowie bei Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 28 Rdnr. 22 Fn. 34.

Schranken der Cassis-Formel nicht, so dass Art. 28 EGV erfüllt und ein Verstoß gegen die Warenverkehrsfreiheit durch die Sperr- bzw. Löschanordnungen gegeben ist.

(4) Rechtfertigung nach Art. 30 EGV

Diese nach Art. 28 EGV verbotene Beschränkung des innergemeinschaftlichen Handels könnte jedoch gemäß Art. 30 EGV gerechtfertigt sein.

Nach Art. 30 EGV stehen die Bestimmungen der Art. 28 und 29 EGV „*Einfuhr-, Ausfuhr- oder Durchfuhrverboten oder –beschränkungen nicht entgegen, die aus Gründen der öffentlichen Sittlichkeit, Ordnung und Sicherheit, zum Schutz der Gesundheit und des Lebens von Menschen, Tieren oder Pflanzen, des nationalen Kulturguts von künstlerischem, geschichtlichem oder archäologischem Wert oder des gewerblichen und kommerziellen Eigentums gerechtfertigt sind*". Es handelt sich hierbei um eine abschließende Aufzählung nichtwirtschaftlicher Ziele.[873] Wie sich aus dem Wortlaut des Art. 30 EGV ergibt, können grundsätzlich nur Ein-, Aus- und Durchfuhrbeschränkungen gerechtfertigt werden. Wegen dem Sinn und Zweck dieser Vorschrift gehen die herrschende Lehre und die ständige Rechtsprechung davon aus, dass auch Maßnahmen gleicher Wirkung von Art. 30 EGV erfasst werden.[874]

Hier könnten die staatlichen Kontrollmaßnahmen aus Gründen der öffentlichen Ordnung und Sicherheit sowie der öffentlichen Sittlichkeit, dem sogenannten „ordre public",[875] eine Rechtfertigung finden. Dabei bereiten die Begriffsbestimmungen dieser Rechtfertigungsgründe erhebliche Schwierigkeiten, weil die Rechtsprechung des EuGH häufig nur punktuell erfolgt ist und bisher allgemeine Aussagen eher selten waren.[876] Nach der bisherigen Rechtsprechung und Lehre können folgende Definitionen zu diesen Begriffen herangezogen werden: Unter dem Begriff der „öffentlichen Ordnung und Sicherheit" versteht man „hoheitlich festgelegte Grundregeln, die wesentliche Interessen des Staates berühren",[877] „öffentliche Sittlichkeit" bedeutet den „Inbegriff der Moralvorstellungen einer bestimmten Gesellschaft zu einer bestimmten Zeit".[878] Die staatlichen Sperr- und/oder Löschanordnungen können demnach aus Gründen der öffentlichen Ordnung und Sicherheit sowie der Sittlichkeit gerechtfertigt sein. So ist es sinnvoll, die Kontrollmaßnahmen gegen das Angebot oder die Werbung von Waren mit rechts- oder linksradikalem, staatsfeindlichem, menschenverachtendem sowie rassistischem Hinter-

---

873 EuGH, Rs. 95/81, 09.06.1982, Slg. 1982, 2187, 2204 Rdnr. 27 (Kommission/Italien).

874 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 36 EGV Rdnr. 10; Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 30 Rdnr. 8; EuGH, Rs. 178/84, 12.03.1987, Slg. 1987, 1227, 1272 Rdnr. 40 (Kommission/Deutschland).

875 Oppermann, Europarecht, § 18 Rdnr. 1165.

876 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1128.

877 EuGH, Rs. 30/77, 27.10.1977, Slg. 1977, 1999, 2013 Rdnr. 33/35 (Bouchereau).

878 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 36 EGV Rdnr. 49; EuGH, Rs. 121/85, 11.03.1986, Slg. 1986, 1007, 1022 Rdnr. 14 ff. (Conegate); Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1129.

grund als Maßnahmen der öffentlichen Ordnung und Sicherheit anzusehen. Dagegen fallen Maßnahmen, die sich gegen unzulässige pornographische Waren richten, eher unter den Rechtfertigungsgrund der Sittlichkeit.[879] Damit lassen sich sämtliche Sperr- und Löschanordnungen, die gegen rechtswidrige Inhalte im Internet ergehen, entweder unter den Begriff der öffentlichen Ordnung und Sicherheit oder die öffentliche Sittlichkeit und somit unter den Art. 30 I 1 EGV subsumieren.[880]

Gemäß Art. 30 I 2 1. Halbsatz EGV dürfen die Verbote oder Beschränkungen kein Mittel zur willkürlichen Diskriminierung sein. Dies kann hier ausgeschlossen werden, da die Kontrollmaßnahmen unterschiedslos wirken. Denn die allgemeinen polizei- und sicherheitsrechtlichen Vorschriften bzw. die Multimedia-Gesetze gelten sowohl für und gegen inländische als auch ausländische natürliche und juristische Personen. Die Sperr- und/oder Löschanordnungen basieren folglich auf unterschiedslosen nationalen Regelungen.

Art. 30 I 2 2. Halbsatz EGV bestimmt zudem, dass die Kontrollmaßnahmen keine verschleierte Beschränkung des Handels zwischen den Mitgliedstaaten herbeiführen dürfen. Damit ist das Prinzip der Verhältnismäßigkeit angesprochen.[881] Die Maßnahmen sind verboten, selbst wenn ein Rechtfertigungsgrund i.S.d. Art. 30 I 1 EGV vorliegt, falls sie nicht geeignet, erforderlich und angemessen sind.[882] Demzufolge verlangt die Verhältnismäßigkeitsprüfung, dass die Maßnahme geeignet ist, um das angestrebte Ziel zu erreichen, sie also – hier in Bezug auf die Beeinträchtigung des freien Warenverkehrs – das mildeste Mittel darstellt und das Ausmaß der Beeinträchtigung des freien Warenverkehrs und der angestrebte Rechtsgüterschutz in einem angemessenen Verhältnis zueinander stehen.[883] Daher sind nun die Sperr- und/oder Löschanordnungen gegen den Content-Provider auf ihre Verhältnismäßigkeit zu untersuchen:

Ziel staatlicher Kontrollmaßnahmen ist es, die Werbung bzw. die Einfuhr von unerwünschten Waren im Inland zu verhindern. Fraglich ist dabei, ob die Sperrung und/oder Löschung von Internet-Seiten, auf denen diese Waren beworben oder zur Bestellung angeboten werden, hierfür ein geeignetes Mittel darstellen. Eine Maßnahme ist jedenfalls dann nicht geeignet, wenn sie gänzlich untauglich ist, um das angestrebte Ziel zu erreichen. Dies muss jedoch verneint werden. Denn durch die staatlichen Kontrollmaßnahmen kann sehr wohl verhindert werden, dass der Nutzer weiter zum Erwerb illegaler Waren animiert wird. Der Umstand, dass die Maßnahmen das Ziel nicht in vollem Umfang erreichen, sondern nur einen geringen Beitrag hierzu zu leisten im Stande sind,

---

879 So auch der EuGH (im Falle eines Pornographieverbots): EuGH, Rs. 121/85, 11.03.1986, Slg. 1986, 1007, 1022 Rdnr. 14 ff. (Conegate); Oppermann, Europarecht, § 18 Rdnr. 1166.

880 Vgl. Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 30 Rdnr. 26 ff.

881 EuGH, Rs. 174/82, 14.07.1983, Slg. 1983, 2445, 2463 Rdnr. 18 (Sandoz); EuGH, Rs. 247/84, 10.12.1985, Slg. 1985, 3887, 3905 Rdnr. 23 (Motte).

882 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1131.

883 EuGH, Rs. 274/87, 02.02.1989, Slg. 1989, 229, 252 Rdnr. 6 (Kommission/Deutschland).

steht einer Bejahung der Geeignetheit nicht entgegen.[884] Die Sperr- und/oder Löschanordnungen sind somit als geeignete Maßnahmen anzusehen, um das gewünschte Ziel, die illegalen Waren bzw. die Werbung hierfür vom Inland fernzuhalten, zu erreichen.
Des weiteren müssten die Maßnahmen erforderlich sein. Eine Maßnahme ist immer dann nicht erforderlich, wenn das angestrebte Schutzziel durch weniger einschränkende Maßnahmen gegenüber dem Warenverkehr erreicht werden kann. Es gilt zu bedenken, dass schon allein aus technischen Gründen nur eine Sperr- und/oder Löschanordnung in Frage kommt, um den ungewünschten Inhalt unschädlich zu machen. Mittels dieser Maßnahmen kann der rechtswidrige Inhalt gezielt aus dem Internet beseitigt werden, so dass der übrige rechtmäßige Inhalt des Content-Providers dem Nutzer auch weiterhin frei zur Verfügung steht. Die gegen den Content-Provider erlassenen Sperr- und/oder Löschanordnungen stellen somit schon das mildeste Mittel dar, um gegen die schädlichen Angebote bzw. Werbungen im Internet erfolgreich vorgehen zu können. Wenn der Content-Provider von staatlicher Seite nur verpflichtet würde, zu seinen Warenangeboten und seiner Werbung für rechtswidrige Waren den Zusatz in das Internet einzustellen, dass es sich bei den angebotenen oder beworbenen Waren um illegale Produkte handelt, hätte dies wenig Erfolgsaussichten. Denn wie die Erfahrung zeigt, hindern derartige Hinweise den Nutzer nicht, solche Waren zu bestellen. Demnach sind die Lösch- und Sperranordnungen durchaus ein erforderliches Mittel, um das Inland vor den unerwünschten Waren zu schützen. Ob nun nur das mildere Mittel der Sperrverfügung oder die radikalere Maßnahme der Löschung von Inhalten angeordnet werden muss, ist eine Frage des Einzelfalles. Häufig wird jedoch nur die Löschanordnung den nötigen Schutz bieten, da gesperrte Inhalte sehr leicht von den jeweiligen Nutzern über Umwege im Netz doch abgerufen werden können.[885]
Schließlich müssen die Maßnahmen auch angemessen sein. Es geht hier um die Mittel-Zweck-Relation von Handelsbeschränkungen. Dabei sind die Beeinträchtigung des freien Warenverkehrs einerseits und das damit verfolgte Schutzinteresse andererseits gegeneinander abzuwägen. Bei dieser Prüfung zieht der EuGH zunehmend die Garantien der Europäischen Menschenrechtskonvention (EMRK) und die Gemeinschaftsgrundrechte heran.[886] Die mitgliedstaatlichen Verfassungsprinzipien sind mittlerweile in der Charta der Grundrechte der Europäischen Union (EGRC)[887] niedergeschrieben worden. Die Gemeinschaftsgrundrechte brauchen deshalb nicht mehr aus den einzelnen Verfassungs- und Rechtsgrundsätzen der jeweiligen Mitgliedstaaten abgeleitet zu werden, vielmehr kann direkt auf die Europäische Grundrechtscharta zurückgegriffen werden.

---

884 Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 30 Rdnr. 46.
885 Vgl. insoweit oben unter B. 1. Teil. III. 1. c. cc. (1).
886 Leible in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, Band 1, Art. 28 Rdnr. 19; Herdegen, Europarecht, 2. Auflage, § 16 Rdnr. 296; EuGH, Rs. C-368/95, 26.06.1997, Slg. 1997, I-3689, 3717 Rdnr. 24 f. (Familiapress).
887 Charta der Grundrechte der Europäischen Union 2000/C 364/01, ABl. EG Nr. C 364 vom 18.12.2000 S. 1.

Das staatliche Ziel, das Inland von rassistischen, rechts- bzw. linksradikalen, demokratiefeindlichen, terroristischen, menschenverachtenden, brutalen oder pornografischen Waren frei zu halten, steht im Einklang mit dem Schutz der Menschenwürde und der Achtung des Demokratieprinzips.[888] Die Erhaltung der Grundwerte der Gesellschaft steht im Vordergrund.[889] Gleichwohl wird durch derartige Sperr- und/oder Löschaktionen von Internet-Inhalten in das Recht auf informationelle Selbstbestimmung und die allgemeine Handlungsfreiheit des Einzelnen eingegriffen.[890] Denkbar ist darüber hinaus, in manchen Fällen eine gewisse Beeinträchtigung der Berufsfreiheit und des Rechts zu arbeiten sowie der unternehmerischen Freiheit anzunehmen.[891] Dennoch wiegen hier die Interessen des Staates schwerer als die des Content-Providers, seine Waren ungehindert im Netz anbieten oder hierfür werben zu dürfen. Denn gemäß Art. 6 I EUV hat sich jeder Mitgliedstaat dazu verpflichtet, die Demokratie und die Menschenrechte zu achten, die durch rechtswidrige Waren bedroht sind. Die Beeinträchtigung des freien gemeinschaftlichen Warenverkehrs muss hinter diese Schutzgüter zurücktreten; zumal der Content-Provider durch die staatlichen Maßnahmen nur verhältnismäßig gering in seinen Rechten verletzt wird, da die Kontrollmaßnahmen gezielt gegen den rechtswidrigen Inhalt gerichtet werden können. Folglich verbleiben alle rechtmäßigen Inhalte im Netz, die Sperr- bzw. Löschmaßnahmen sind demnach angemessen. Weil sie gleichzeitig geeignet und erforderlich sind, ist das von Art. 30 EGV geforderte Kriterium der Verhältnismäßigkeit erfüllt.

(5) Zusammenfassung

Durch die staatlichen Kontrollmaßnahmen liegt zwar eine Beeinträchtigung der Warenverkehrsfreiheit gemäß Art. 28 EGV vor. Dieser Verstoß ist jedoch nach Art. 30 EGV gerechtfertigt. Europarecht ist insoweit nicht verletzt.

bb. Niederlassungsfreiheit

Wie sich aus der oben vorgenommenen Prüfung ergeben hat, wird bei zwei Fallkonstellationen durch die behördlichen Sperr- und/oder Löschverfügungen gegen die Niederlassungsfreiheit i.S.d. Art. 43 ff. EGV verstoßen. Einmal, wenn der Content-Provider eine natürliche Person aus dem EU-Ausland mit Sitz im Inland ist. Zweitens, falls es sich beim Content-Provider um eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland handelt, wobei sich allerdings die Technik und weitere mit dem Content-Providing im Zusammenhang stehende Komponenten im Inland befinden. Beide Male ist der Nutzer aus dem Inland.

---

888 Vgl. hierzu Art. 1 EGRC sowie Art. 6 EUV.
889 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 255.
890 Vgl. Art. 11 EGRC bzw. Art. 10 EMRK .
891 Vgl. Art. 15, 16 EGRC.

(1) Inländergleichbehandlung

Gemäß Art. 43 II EGV garantiert die Niederlassungsfreiheit die Aufnahme und Ausübung selbständiger, d.h. nicht weisungsgebundener Erwerbstätigkeiten sowie die Gründung und Leitung von Unternehmen nach den Bestimmungen des Aufnahmestaates für seine eigenen Angehörigen. Die Niederlassungsfreiheit umfasst demzufolge die gemeinschaftliche Inländergleichbehandlung. Die natürlichen und juristischen Personen haben also das Recht, in einem anderen Mitgliedstaat als ihrem Heimatstaat eine dauernde, selbständige Tätigkeit zu den gleichen Bedingungen wie Inländer auszuüben.[892] Der Art. 43 II EGV ist somit lex specialis zu der Generalnorm des Art. 12 EGV, worin das allgemeine Diskriminierungsverbot festgeschrieben ist.
Der EuGH geht in seiner Rechtsprechung allerdings über das bloße Diskriminierungsverbot hinaus und macht den Umfang der Niederlassungsfreiheit – wie dies bei der Warenverkehrsfreiheit bereits in Art. 28 EGV normiert ist – zu einem allgemeinen Beschränkungsverbot.[893] Danach sind auch nichtdiskriminierende Maßnahmen verboten, wenn sie nicht gerechtfertigt und verhältnismäßig sind.[894]

(2) Rechtfertigung

(a) Zwingende Gründe des Allgemeininteresses

Eine Rechtfertigung von unterschiedslosen staatlichen Maßnahmen aus zwingenden Gründen des Allgemeininteresses, die eine Beschränkung der Niederlassungsfreiheit nach sich ziehen, ist bei der Niederlassungsfreiheit erst durch den EuGH, vor allem in der Gebhard-Entscheidung,[895] eingeführt worden und besitzt im EGV (noch) keine Entsprechung. Art. 46 EGV kann schon allein wegen des Wortlauts nicht angewendet werden, wenn es um eine Rechtfertigung aufgrund des Allgemeininteresses und der Verhältnismäßigkeitsprüfung geht.[896] Falls der EuGH eine Behinderung der Niederlassungsfreiheit durch die zwingenden Gründe des Allgemeininteresses rechtfertigen will,[897] verweist er deshalb auf die allgemeine Grundfreiheitendogmatik.[898] Danach müssen nationale Maßnahmen, welche die Ausübung der durch den Vertrag garantierten grundlegenden Freiheiten behindern oder weniger attraktiv machen, vier Voraussetzungen erfüllen: Sie dürfen nicht in diskriminierender Weise angewendet werden, aus

---

892 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1172.

893 Vgl. EuGH, Rs. 96/85, 30.04.1986, Slg. 1986, 1475, 1485 f. Rdnr. 11 (Kommission/Frankreich); EuGH, Rs. C-340/89, 07.05.1991, Slg. 1991, I-2357, 2383 Rdnr. 15 (Vlassopoulou); EuGH, Rs. C-19/92, 31.03.1991, Slg. 1993, I-1663, 1697 Rdnr. 32 (Kraus).

894 Herdegen, Europarecht, 2. Auflage, § 17 Rdnr. 319 f.; EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4197 f. Rdnr. 37 (Gebhard); vgl. auch Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1655.

895 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165 ff., insbesondere 4197 f. Rdnr. 37 (Gebhard).

896 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 56 Rdnr. 1 f.

897 EuGH, Rs. C-19/92, 31.03.1991, Slg. 1993, I-1663, 1697 Rdnr. 32 (Kraus).

898 Vgl. Fn. 860 sowie oben bei B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).

zwingenden Gründen des Allgemeininteresses gerechtfertigt sein, geeignet sein, die Verwirklichung des mit ihnen verfolgten Zieles zu gewährleisten und nicht über das hinausgehen, was zur Erreichung des Zieles erforderlich ist.[899]

Vom EuGH wurde in der vorerwähnten Gebhard-Entscheidung allerdings nichts dazu ausgeführt, wie die Rechtfertigung nach den zwingenden Gründen des Allgemeininteresses rechtlich einzuordnen ist. Soll diese weitere Einschränkungsmöglichkeit der Niederlassungsfreiheit – in Anlehnung an die für die Warenverkehrsfreiheit entwickelte Cassis-Rechtsprechung – ebenso als tatbestandsimmanente Schranke des Art. 43 EGV angesehen werden[900] oder stellen die zwingenden Gründe des Allgemeininteresses nur eine zusätzliche Rechtfertigungsmöglichkeit neben den Art. 45, 46 EGV für unterschiedslose nationale Maßnahmen dar? Zu bedenken ist hierbei, dass die Cassis-Formel insbesondere den Zweck hatte, die Dassonville-Formel, also eine Definition des Begriffs „*Maßnahmen gleicher Wirkung*“ in Art. 28 EGV, wegen ihres weiten Anwendungsbereiches angemessen einzuschränken. Dies ist bei der Niederlassungsfreiheit nicht veranlasst. Zwar sind die vom EuGH aufgestellten Fallgruppen zu den zwingenden Gründen des Allgemeinwohls größtenteils der Cassis-Rechtsprechung entnommen.[901] Dennoch kann die vom EuGH entwickelte Schrankensystematik der zwingenden Gründe des Allgemeininteresses – abgesehen von der Warenverkehrsfreiheit[902] – nicht als tatbestandsimmanente Schranke der jeweiligen Grundfreiheit angesehen werden. Vielmehr ist dies eine weitere Rechtfertigungsmöglichkeit für unterschiedslose Regelungen, die parallel zu den allgemeinen Beschränkungsverboten bei den Grundfreiheiten entwickelt wurde.

Wenn nun eine Beschränkung der Niederlassungsfreiheit durch nationale Maßnahmen bejaht werden kann, ist zunächst der Tatbestand des Art. 43 EGV erfüllt. Eine Verletzung seiner Grundfreiheit liegt somit vor. Jedoch kann dieser grundsätzlich unzulässige Eingriff in die Niederlassungsfreiheit gerechtfertigt sein, und zwar aufgrund zwingende Gründe des Allgemeininteresses sowie der Art. 45 und 46 EGV enthaltenen Ausnahmetatbestände. Eine Rangfolge zwischen den gesetzlich normierten und den durch den EuGH entwickelten Schranken der Niederlassungsfreiheit ist dabei nicht zu erkennen.[903]

---

899 Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 53 Rdnr. 25 f.

900 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).

901 Koenig/Haratsch, Europarecht, 2. Auflage, S. 234 Rdnr. 496.

902 Und auch dies ist mittlerweile nicht unumstritten, vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).

903 Dadurch dass aber bei der Warenverkehrsfreiheit die Cassis-de-Dijon-Formel und die darin aufgeführten zwingenden Gründe des Allgemeininteresses in der Regel vor den in Art. 30 EGV fixierten Rechtfertigungsgründen geprüft wird, soll hier, um eine einheitliche Prüfungsreihenfolge zu erreichen, auch bei der Niederlassungsfreiheit (und später bei der Dienstleistungsfreiheit) zunächst die richterrechtliche Schranke des EuGH geprüft werden, bevor auf die Art. 45 und 46 EGV eingegangen wird.

Es stellt sich daher die Frage, ob die festgestellte Beschränkung der Niederlassungsfreiheit aus zwingenden Gründen des Allgemeininteresses gerechtfertigt ist. Wie eben ausgeführt,[904] handelt es sich bei den Sperr- bzw. Löschverfügungen um nichtdiskriminierende staatliche Maßnahmen. Denn es gelten die allgemeinen polizei- und sicherheitsrechtlichen Vorschriften bzw. die Multimedia-Gesetze in gleicher Weise sowohl für und gegen inländische als auch für und gegen ausländische natürliche und juristische Personen. Was unter den zwingenden Gründen des Allgemeininteresses im Rahmen der Niederlassungsfreiheit zu verstehen ist, kann jedoch nicht eindeutig geklärt werden. Zunächst könnte auf die Cassis-de-Dijon-Formel abgestellt werden. Da diese aber nur für die Warenverkehrsfreiheit aufgestellt worden ist, kommt sie nicht direkt zur Anwendung. Es scheint aber sinnvoll zu sein, die Fallgruppen der Cassis-Formel zumindest als Anhaltspunkte für den Terminus „zwingende Gründe des Allgemeininteresses" zu nutzen. Hierunter sind insbesondere eine wirksame steuerliche Kontrolle, der Verbraucherschutz, die Lauterkeit des Handelsverkehrs sowie der Umweltschutz hierunter zu verstehen.[905] Die Kontrollmaßnahmen ergehen jedoch nicht aufgrund einer dieser Fallgruppen, vielmehr werden sie – wie vorstehend festgestellt wurde – aus Gründen der öffentlichen Sicherheit und Ordnung sowie der Sittlichkeit gegen den Provider angeordnet. Die öffentliche Sittlichkeit, Sicherheit und Ordnung werden aber in der Cassis-Formel vom EuGH nicht genannt. Dies ist bei der Warenverkehrsfreiheit auch nicht erforderlich, da diese Rechtfertigungsgründe bereits in Art. 30 EGV explizit geregelt sind. Das Gleiche gilt für die Niederlassungsfreiheit, bei der in Art. 46 EGV ebenfalls eine Beschränkung aufgrund der öffentlichen Ordnung, Sicherheit und Gesundheit zulässig ist. Demzufolge können – schon allein wegen der Systematik – diese Rechtfertigungsgründe nicht von den zwingenden Gründen des Allgemeininteresses erfasst werden.

(b) Rechtfertigung nach den Art. 45, 46 EGV

Ein Verstoß gegen die Niederlassungsfreiheit könnte allerdings gemäß den Art. 45 und 46 EGV auf zweierlei Arten gerechtfertigt sein: Nach Art. 45 I EGV finden die Vorschriften der Niederlassungsfreiheit auf Tätigkeiten, die in einem Mitgliedstaat „*dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt verbunden sind*", in dem betreffenden Mitgliedstaat keine Anwendung. Insoweit wird schon durch Art. 45 EGV der Anwendungsbereich der Niederlassungsfreiheit eingeschränkt. Andererseits kann nach Art. 46 EGV die Niederlassungsfreiheit auch durch Rechts- und Verwaltungsvorschriften, die eine „*Sonderregelung für Ausländer vorsehen und aus Gründen der öffentlichen Ordnung, Sicherheit oder Gesundheit gerechtfertigt sind*", rechtmäßig

---

904 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

905 Vgl. Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 28 Rdnr. 20 ff.

fentlichen Ordnung, Sicherheit oder Gesundheit gerechtfertigt sind", rechtmäßig eingeschränkt werden.

Die Beeinträchtigungen der Niederlassungsfreiheit durch die staatlichen Sperr- und/oder Löschanordnungen erfüllen nicht den Tatbestand des Art. 45 EGV. Denn der Content-Provider wird regelmäßig nicht im Inland in Ausübung öffentlicher Gewalt tätig.

Des weiteren wird der Content-Provider auch nicht durch Maßnahmen in seiner Niederlassungsfreiheit beeinträchtigt, die auf nationale Regelungen für Ausländer zurückgehen. Vielmehr gelten die allgemeinen polizei- und sicherheitsrechtlichen Vorschriften bzw. die Multimedia-Gesetze für alle Inländer im gleichen Umfang. Die Sperr- und/oder Löschanordnungen basieren folglich auf unterschiedslosen nationalen Regelungen.[906] Diese nichtdiskriminierenden Beschränkungen werden – wenn nur der Wortlaut des Art. 46 EGV betrachtet wird – nicht von dieser Ausnahmevorschrift erfasst. Es ist jedoch fraglich, ob die Rechtfertigungsgründe der öffentlichen Ordnung, Sicherheit und Gesundheit gemäß Art. 46 I EGV nur für diskriminierende oder auch für nichtdiskriminierende Maßnahmen gelten. Der Wortlaut spricht sich eindeutig dafür aus, nur diskriminierende Maßnahmen vom Anwendungsbereich der Schrankenbestimmung erfasst zu sehen, da explizit von „*Sonderregelungen für Ausländer*" die Rede ist.[907] Art. 46 EGV wollte damit grundsätzlich klar stellen, dass die Niederlassungsfreiheit nicht zur Abschaffung allen Ausländerrechts führen muss. Die in Art. 46 EGV genannten Sonderregelungen, also insbesondere das Ausländerpolizeirecht mit seinen Vorschriften über Ein- und Ausreise, Meldewesen, Ausweisungen usw., sollten also nicht notwendigerweise Beschränkungen i.S.d. Art. 43 EGV sein.[908]

Mittlerweile hat der EuGH über den Wortlaut des Art. 46 I EGV hinaus aber auch nichtdiskriminierende Maßnahmen an Art. 46 I EGV überprüft.[909] Dies lässt den Schluss zu, dass er den Art. 46 I EGV sowohl auf diskriminierende als auch auf unterschiedslose Maßnahmen und somit – wie bei den übrigen Grundfreiheiten – als allgemeine „ordre public"-Klausel anwenden will.[910] Die Formulierung „*Sonderregelung für*

---

906 Hierunter fallen das jeweilige Polizei- und Sicherheitsrecht der Länder sowie die §§ 5, 18 MDStV.

907 Auch Schwarze in: „Medienfreiheit und Medienvielfalt im Europäischen Gemeinschaftsrecht", ZUM 2000, 779, 782, geht anscheinend von einer Sonderregelung für Ausländer aus und will den Art. 46 EGV lediglich auf diskriminierende Regelungen anwenden.

908 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 256; häufig stellen sie nur eine schlichte Ungleichbehandlung ungleicher Tatbestände im Verhältnis zum Inländerrecht dar, ohne dass eine besondere Belastung des Ausländers aus ihnen entsteht.

909 EuGH, verbundene Rs. C-34/95, C-35/95 und C-36/95, 09.07.1997, Slg. 1997, I-3843, 3892 f. Rdnr. 48 ff. (Konsumentenombudsmannen); vgl. auch EuGH, Rs. 352/85, 26.04.1988, Slg. 1988, 2085, 2134 ff. Rdnr. 31 ff. (Bond van Adverteerders); EuGH, Rs. C-260/89, 18.06.1991, Slg. 1991, I-2951, 2960 Rdnr. 24 (Griechische Monopole); EuGH, Rs. C-353/89, 25.07.1991, Slg. 1991, I-4067, 4093 Rdnr. 15 f. (Mediawet).

910 Vgl. hierzu die Diskussion bei Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 56 Rdnr. 3. Leider nimmt Troberg zu der aufgeworfenen Frage, ob Art. 46 I auf das Ausländerrecht beschränkt bleiben muss, nicht Stellung. Er deutet nur an, dass der EuGH vor allem in seiner Fernsehrechtsprechung vermehrt unterschiedslose Maßnahmen anhand des Art. 46 EGV geprüft hat. Welche Meinung Troberg vertritt, bleibt letztendlich unklar.

Ausländer“ in Art. 46 I EGV muss demnach konsequenterweise überlesen werden. Denn nur wenn Art. 46 I EGV gleichermaßen für unterschiedslose und diskriminierende nationale Maßnahmen gilt, kann die Niederlassungsfreiheit (und die Dienstleistungsfreiheit, für die über Art. 55 EGV der Art. 46 I EGV ebenfalls zur Anwendung kommt) in ein einheitliches System der gesamten Grundfreiheiten eingegliedert werden. Weiterhin wird dadurch erreicht, dass die vom EuGH propagierte und entwickelte Schrankensystematik[911] hinsichtlich der zwingenden Gründe des Allgemeininteresses ebenfalls in dieses einheitliche Schema aufgenommen werden kann: So ergibt sich die Möglichkeit, dass jede Beschränkung einer Grundfreiheit über die zwingenden Gründe des Allgemeininteresses und darüber hinaus durch den im EGV enthaltenen „ordre public“ gerechtfertigt werden kann.[912] Neben dieser Ansicht wird in der Literatur auch die Meinung vertreten, dass Art. 46 I EGV, der in seinem Wortlaut lediglich eine Anwendbarkeit für diskriminierende Maßnahmen erklärt, gerade für unterschiedslose Maßnahmen gelten muss. Denn wenn Art. 46 I EGV schon eine Ausnahme für die äußerst gravierenden und dem EGV zuwider laufenden (vgl. Art. 12 EGV) diskriminierenden nationalen Regelungen zulässt, dann muss dies erst recht für die weniger einschneidenden unterschiedslosen Maßnahmen gelten.[913]

Beide Begründungen können hier überzeugen. Sowohl der Aspekt, dass mit der Anwendung des Art. 46 I EGV auf unterschiedslose staatliche Maßnahmen ein gemeinschaftsrechtlich einheitliches Prüfungsschema begünstigt wird, als auch der Erst-Recht-Schluss sind plausibel. Folglich kann Art. 46 I EGV auch auf die nichtdiskriminierenden Sperr- und /oder Löschanordnungen angewendet werden.[914]

Bei den Begriffen der öffentlichen Ordnung und Sicherheit des Art. 46 I EGV handelt es sich – wie oben bei Art. 30 EGV[915] – um autonome gemeinschaftsrechtliche Begriffe, die grundsätzlich europarechtlich definiert werden müssen.[916] Da der Art. 46 EGV hingegen in erster Linie auf das Ausländerpolizeirecht abzielt, kann bei der Auslegung des Art. 46 EGV durchaus der allgemeine verwaltungs- und insbesondere polizeirechtliche

---

911 Vgl. hierzu Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 53 f.

912 Koenig/Haratsch, Europarecht, 2. Auflage, S. 234 f. Rdnr. 499.

913 Hailbronner in: Hailbronner/Klein/Magiera/Müller-Graff, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Art. 56 Rdnr. 3; Hailbronner kommt jedoch zu dem Schluss, dass bei unterschiedslosen Maßnahmen schon eine Rechtfertigung durch die zwingenden Gründe des Allgemeininteresses, die er als tatbestandsausschließende Schranke des Art. 43 EGV versteht, vorliegt und der Art. 46 EGV deshalb ohnehin für die nichtdiskriminierenden Regelungen nicht mehr benötigt wird. Wie bereits oben aufgezeigt, werden die Gründe der öffentlichen Sicherheit und Ordnung aber gerade nicht von den zwingenden Erfordernissen des Allgemeinwohls erfasst, so dass der Art. 46 EGV für unterschiedslose Maßnahmen sehr wohl eine Rolle spielt.

914 So im Ergebnis auch Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1634. Er vertritt die Ansicht, dass die öffentliche Sicherheit und Ordnung Zulässigkeits- und Berufsausübungsregelungen generell gegen Ausländer und Inländer gestattet, weil die Art. 43 ff. EGV grundsätzlich nur die Inländergleichheit, nicht aber ein Grundrecht der Berufsfreiheit begründen.

915 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

916 Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 46 Rdnr. 3.

Begriff der öffentlichen Sicherheit und Ordnung zugrunde gelegt werden.[917] Zur öffentlichen Sicherheit gehört der Schutz der Allgemeinheit und des Einzelnen gegen Bedrohungen des Bestands eines Staats und seiner Einrichtungen, sowie des Lebens, der Gesundheit, der Freiheit und der Ehre.[918] Ferner fällt unter den Begriff der öffentlichen Ordnung der Schutz gegen Bedrohungen eines geordneten menschlichen und staatsbürgerlichen Zusammenlebens.[919] Sowohl die öffentliche Sicherheit als auch die Ordnung werden von illegalen Inhalten im Internet bedroht. Denn zum einen muss das Individuum bei politisch radikalen bzw. terroristischen Inhalten gegen Bedrohungen des Bestands des Staates und seiner Einrichtungen geschützt werden. Zum anderen stellen derartige Inhalte auch eine Bedrohung des geordneten menschlichen und staatsbürgerlichen Zusammenlebens dar. Folglich liegen in der Regel Rechtfertigungsgründe nach Art. 46 I EGV vor.

Obwohl Art. 46 EGV hierzu keine Aussage macht, wird allgemein verlangt, dass die von Art. 46 I EGV erfassten staatlichen Maßnahmen dem Grundsatz der Verhältnismäßigkeit entsprechen müssen.[920] Die Sperr- bzw. Löschmaßnahmen können hier als verhältnismäßig angesehen werden. Denn sind sie geeignet, den unerwünschten Inhalt beim Content-Provider für den Internet-Nutzer unzugänglich zu machen. Technisch sind die Sperr- bzw. Löschverfügungen die einzigen Möglichkeiten, um gegen die illegalen Angebote des Content-Providers vorzugehen. Deshalb sind die Maßnahmen erforderlich. Das Interesse des Staates, die oben genannten Bedrohungen für sich und die Bürger abzuwehren, überwiegt das Interesse der natürlichen oder juristischen Person an einer uneingeschränkten Niederlassungsfreiheit. Die staatlichen Sperr- und/oder Löschanordnungen sind demnach mithin angemessen.[921] Die Voraussetzungen für eine gerechtfertigte Beeinträchtigung der Niederlassungsfreiheit liegen also vor.

---

917 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 56 Rdnr. 10.

918 Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, zu Art. 2 S. 9.

919 Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, zu Art. 2 S. 9.

920 Koenig/Haratsch, Europarecht, 2. Auflage, S. 242 Rdnr. 513.

921 Vgl. hierzu auch die Ausführungen zur Verhältnismäßigkeitsprüfung bei der Warenverkehrsfreiheit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4). Darüber hinaus ist noch folgendes zu bedenken: Der Niederlassungswillige begibt sich dauerhaft und freiwillig in das Gebiet eines anderen Mitgliedstaats und damit in die Obhut einer anderen Rechtsordnung. Im Gegensatz zur Warenverkehrsfreiheit, bei der der Importeur grundsätzlich einer anderen Rechtsordnung angehört und unter ihren Vorschriften bestimmte Waren produziert oder erwirbt und diese dann in einem anderen Mitgliedstaat anbieten will, unterstellt sich der Niederlassende einer neuen Rechtsordnung – und zwar dauerhaft. Der Unterschied ist eklatant. Deshalb dürfen die Kriterien für eine Rechtfertigung von Beschränkungen der Niederlassungsfreiheit aufgrund der Sicherheit und Ordnung nicht so streng gehandhabt werden, wie dies bei der Warenverkehrsfreiheit (und bei der Dienstleistungsfreiheit) der Fall ist. Vgl. Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 53 Rdnr. 29; dort wird dieses Argument für die Rechtfertigung nach den zwingenden Gründen des Allgemeinwohls benutzt. Allerdings spricht nichts dagegen, diesen Gedanken auch auf den Art. 46 I EGV zu übertragen.

(3) Zusammenfassung

Zwar verstoßen die staatlichen Kontrollmaßnahmen gegen die Niederlassungsfreiheit gemäß Art. 43 II EGV. Da diese Maßnahmen aber unter den Ausnahmetatbestand des Art. 46 I EGV subsumiert werden können, geschieht dies in rechtmäßiger Form.

cc. Dienstleistungsfreiheit

Eine Beeinträchtigung der Dienstleistungsfreiheit durch gegen den Content-Provider gerichtete behördliche Sperr- bzw. Löschanordnungen wurde zum einen für die Fallkonstellation bejaht, bei der der Content-Provider eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist. Allerdings befindet sich die Technik für das Content-Providing im Inland. Der Nutzer stammt ebenfalls aus dem Inland. Zum anderen liegt ein Verstoß gegen die Dienstleistungsfreiheit dann vor, wenn es sich zwar um einen inländischen Content-Provider handelt, dafür aber der Nutzer aus dem EU-Ausland stammt und auch seinen Sitz im EU-Ausland hat.

(1) Inländergleichbehandlung

Nach Art. 50 III EGV umfasst die Freiheit des Dienstleistungsverkehrs die Freiheit des Leistenden, seine Tätigkeit nach dem Grundsatz der Inländergleichbehandlung vorübergehend in dem Staat auszuüben, wo die Leistung erbracht wird.[922] Dieses Diskriminierungsverbot gilt im Zuge der erweiterten Anwendung der Dienstleistungsfreiheit konsequenterweise auch für die passive Dienstleistungsfreiheit und die Korrespondenzdienstleistungsfreiheit.[923]

Wie der Wortlaut in Art. 43 I EGV zur Niederlassungsfreiheit, enthält die Dienstleistungsfreiheit darüber hinaus auch noch ein in Art. 49 I EGV verankertes Beschränkungsverbot.[924] Demnach sind „*Beschränkungen des freien Dienstleistungsverkehrs innerhalb der Gemeinschaft für Angehörige der Mitgliedstaaten, die in einem anderen Staat der Gemeinschaft als demjenigen des Leistungsempfängers ansässig sind,*“ nach Maßgabe der Art. 50 ff. EGV verboten. Die Literatur interpretiert diesen Wortlaut so, dass hier „anders und deutlicher als andere Grundfreiheiten“ der Art. 49 I EGV nicht nur die Inländergleichbehandlung, sondern auch die Beseitigung sonstiger Beschränkungen des grenzüberschreitenden Dienstleistungsverkehr verlangt.[925] Diese Schlussfolgerung kann zwar nicht nachempfunden werden, wenn der Wortlaut des Art. 43 I mit dem des Art. 49 I EGV verglichen wird. Denn in Art. 43 I 1 EGV ist ebenfalls lediglich von „*Beschränkungen*“ die Rede. Es ist jedoch durchaus plausibel, aus Art. 49 I EGV ein allgemeines Beschränkungsverbot der Dienstleistungsfreiheit herzuleiten.

---

922 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1186; vgl. zu den unterschiedlichen Arten der Dienstleistungsfreiheit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).

923 Völker, Passive Dienstleistungsfreiheit im Europäischen Gemeinschaftsrecht, S. 129.

924 Trautwein, „Dienstleistungsfreiheit und Diskriminierungsverbot im Europäischen Gemeinschaftsrecht“, JURA 1995, 191, 192.

925 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 38.

ein allgemeines Beschränkungsverbot der Dienstleistungsfreiheit herzuleiten. Denn die Dienstleistungen, die vorübergehend in einem anderen Mitgliedstaat erbracht werden, können mit der Lieferung von Waren verglichen werden.[926] Der Hauptunterschied besteht nur darin, dass keine Ware, sondern eine Dienstleistung, also grundsätzlich kein körperlicher Gegenstand, geliefert wird. Entscheidend ist in beiden Fällen der Grenzübertritt der Ware bzw. Leistung.[927] Eine Ähnlichkeit der Dienstleistungsfreiheit zur Warenverkehrsfreiheit, die insbesondere bei der Korrespondenzdienstleistungsfreiheit deutlich sichtbar wird, hat auch der EuGH früh erkannt. Vor allem traten vermehrt Abgrenzungsschwierigkeiten zwischen der Dienstleistungsfreiheit und der Warenverkehrsfreiheit auf.[928] Der EuGH hat deshalb zur Dienstleistungsfreiheit sehr bald entschieden,[929] dass über das Diskriminierungsverbot hinausgegangen und bei den Art. 49 ff. EGV ein allgemeines Beschränkungsverbot angenommen werden muss.[930] Diese Rechtsprechung wurde in zahlreichen Urteilen bestätigt.[931] Mittlerweile fasst der EuGH den Beschränkungsbegriff sehr weit und ordnet ihm nicht nur das Unterbinden und Behindern von Dienstleistungen zu, sondern auch den Fall, dass aufgrund der betreffenden Regelung die Erbringung der Dienstleistung weniger attraktiv gemacht wird.[932]
Wie bereits festgestellt wurde, beschränken die staatlichen Kontrollmaßnahmen, die grundsätzlich unterschiedslos angeordnet werden, die Dienstleistungsfreiheit des Content-Providers. Folglich sind Sperr- bzw. Löschanordnungen nur zulässig, wenn sie gerechtfertigt sind.

---

926 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 Rdnr. 5.

927 Troberg spricht in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 Rdnr. 6 diesbezüglich von einer sogenannten „produktbezogenen Betrachtungsweise".

928 So musste der EuGH in einer Entscheidung, feststellen, EuGH, Rs. 155/73, 30.04.1974, Slg. 1974, 409, 410 13. Leitsatz des Urteils (Sacchi), dass zwar die Ausstrahlung von Fernsehsendungen einschließlich der Werbesendungen unter die Dienstleistungsfreiheit fällt, während der Handel mit sämtlichen Materialien, Apparaten, Videokassetten, usw., die für die Ausstrahlung von Fernsehsendungen benutzt werden, den Bestimmungen des freien Warenverkehr unterliegen.

929 EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen); explizit EuGH, Rs. 205/84, 04.12.1986, Slg. 1986, 3755, 3802 (Kommission/Bundesrepublik Deutschland) in Rdnr. 25:
„Diese Artikel (d.h. Art. 49 und 50 EGV, Anm. d. Bearbeiters) verlangen nicht nur die Beseitigung sämtlicher Diskriminierungen des Leistungserbringers aufgrund seiner Staatsangehörigkeit, sondern auch die Beseitigung aller Beschränkungen des freien Dienstleistungsverkehrs, die damit zusammenhängen, dass der Leistungserbringer in einem anderen Mitgliedstaat als dem, in dem die Leistung erbracht wird, niedergelassen ist."

930 Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1678 f.; Trautwein, „Dienstleistungsfreiheit und Diskriminierungsverbot des Europäischen Gemeinschaftsrechts", JURA 1995, 191 ff.

931 EuGH, Rs. C-353/89, 25.07.1991, Slg. 1991, 4069, 4093 f. Rdnr. 15 ff. (Mediawet); EuGH, Rs. C-76/90, 25.07.1991, Slg. 1991, I-4221, 4243 Rdnr. 12 (Säger).

932 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 und 4197 f. Rdnr. 25 und 37 (Gebhard).

(2) Analoge Anwendung der Keck-Rechtsprechung

Bevor auf die möglichen Rechtfertigungsgründe eingegangen wird, ist zunächst zu prüfen, ob nicht – in Analogie zur Keck-Rechtsprechung[933] – nationale Verkaufsmodalitäten die Anwendbarkeit der Dienstleistungsfreiheit von vornherein ausschließen. Dies hätte zur Folge, dass die staatlichen Kontrollmaßnahmen, falls sie als nichtdiskriminierende Verkaufsmodalitäten zu qualifizieren sind, nicht gegen Europarecht verstoßen würden, da insoweit eine rechtmäßige Organisation des Marktgeschehens im Inland vorliegen würde.[934]

Bei den Dienstleistungen gibt es ebenfalls „Verkaufsmodalitäten". Diese können zwar nicht einer physischen Beschaffenheit gegenübergestellt werden, wie dies bei der Warenverkehrsfreiheit geschieht. Dennoch lässt sich der Inhalt einer Dienstleistung von den Umständen der Leistungserbringung abgrenzen.[935] Der EuGH hat bislang die Frage, ob die Keck-Rechtsprechung auch auf die Dienstleistungsfreiheit entsprechend angewendet werden kann, nicht entschieden, obwohl er die Möglichkeit hierzu hatte.[936] Dies lässt die Vermutung zu, dass der EuGH die Keck-Formel nicht auf die Dienstleistungsfreiheit ausdehnen will. Im übrigen gibt es auch Unterschiede zwischen Waren und Dienstleistungen, so dass eine analoge Anwendung der Keck-Rechtsprechung eher abzulehnen ist. So weisen Dienstleistungen häufig einen ständigen grenzüberschreitenden Bezug auf, der bei Waren nach ihrem Import nicht mehr gegeben ist. Des weiteren sind Waren nach der Produktion nur noch anhand ihrer Qualität zu beurteilen. Dagegen bleiben Dienstleistungen oft von dem Dienstleister abhängig und müssen deshalb in der Regel zusammen betrachtet werden. Nationale Regelungen betreffen deshalb Waren grundsätzlich losgelöst vom Produzenten bzw. Importeur im Gegensatz zur Dienstleistung, bei der sich die nationalen Vorschriften auch gegen den Dienstleistenden richten können.[937] Aufgrund dieser Unterschiede ist die für die Warenverkehrsfreiheit entwickelte Keck-Rechtsprechung nicht auf die Dienstleistungsfreiheit übertragbar.[938]

---

933 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2).

934 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2).

935 So kann beispielsweise zwischen bestimmten Versicherungstypen und ihrem Vertrieb unterschieden werden. Vgl. hierzu Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 Rdnr. 34.

936 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1176 ff. Rdnr. 33 ff. (Alpine Investments).

937 Knobl, „Ein Meilenstein im Europarecht der Bank- und Wertpapierdienstleistungen sowie im Anwendungsbereich der Dienstleistungsfreiheit", WBl. (Wien) 1995, 309.

938 Zudem wäre die Keck-Formel hier nicht einschlägig gewesen, da sich die Sperr- und/oder Löschanordnungen direkt gegen den Inhalt der Dienstleistungen richten, so dass eine Verkaufsmodalität sowieso nicht zu bejahen gewesen wäre.

(3) Rechtfertigung

(a) Entsprechende Anwendung von Cassis de Dijon

In seiner frühesten Rechtsprechung zur Dienstleistungsfreiheit[939] hatte der EuGH ausgeführt, dass an den Dienstleistenden Anforderungen gestellt werden können, „die sich aus der Anwendung durch das Allgemeinwohl gerechtfertigter Berufsregelungen – namentlich der Vorschriften über Organisation, Befähigung, Berufspflichten, Kontrolle, Verantwortlichkeit und Haftung – ergeben".[940] Diese Formulierung erinnert stark an die Cassis-Formel[941]. Deshalb ist zu fragen, ob die erst fünf Jahre später entwickelte Cassis-Formel nicht auch auf die Dienstleistungsfreiheit als tatbestandsimmanente Schranke des Art. 49 I EGV angewendet werden kann. Ein Vergleich zwischen dem Wortlaut der zitierten Passage aus dem Van Binsbergen-Urteil und der Cassis-de-Dijon-Formel zeigt allerdings,[942] dass die Cassis-Formel nicht auf die Dienstleistungsfreiheit übertragen werden darf. Denn jede Formulierung der Urteile passt entweder nur auf die Warenverkehrsfreiheit (Cassis-Formel) oder auf die Dienstleistungsfreiheit (Van Binsbergen). Daran ist abzulesen, dass der EuGH den Waren- und den Dienstleistungsverkehr bewusst auseinander halten wollte, indem er für den ersten typisch produktbezogene Regelungen (Gesundheit, Verbraucherschutz) zitiert, während er für den letzteren deutlich auf das Gewerberecht (Berufsregelungen, Organisation, Befähigung, etc.) verweist.[943] Zudem ist eine entsprechende Anwendung der Cassis-Rechtsprechung schon allein deswegen nicht erforderlich, weil der EuGH mittlerweile für alle Grundfreiheiten, also auch für die Dienstleistungsfreiheit, eine Rechtfertigung von Beeinträchtigungen der Grundfreiheiten aus zwingenden Gründen des Allgemeininteresses bejaht hat.[944] Somit scheidet die analoge Anwendbarkeit der Cassis-Formel auf die Dienstleistungsfreiheit aus.

(b) Zwingende Erfordernisse des Allgemeininteresses

Wie bereits zuvor erwähnt, hat der EuGH in seinem zur Dienstleistungsfreiheit grundlegenden Van Binsbergen-Urteil[945] ausgeführt, dass durch das Allgemeininteresse gerechtfertigte Berufsregelungen der Mitgliedstaaten an sich mit Art. 49 EGV vereinbar sein können. Diese Rechtsprechung zur Rechtfertigung von Beschränkungen der Dienst-

---

939 EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen).

940 EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen).

941 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).

942 Wichtig ist vor allem folgender Teil in EuGH, Rs. 120/78, 20.02.1979, 649, 662 Rdnr. 8 („Cassis-de-Dijon"): "[...] notwendig sind, um zwingenden Erfordernissen gerecht zu werden, insbesondere den Erfordernissen einer wirksamen steuerlichen Kontrolle, des Schutzes der öffentlichen Gesundheit, der Lauterkeit des Handelsverkehrs und des Verbraucherschutzes".

943 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 Rdnr. 20 f.

944 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3) bzw. die nachfolgende Prüfung.

945 EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen).

leistungsfreiheit wurde vom EuGH fortgeführt und weiter ausgestaltet.[946] Bereits bei der Prüfung der Niederlassungsfreiheit wurde eine ähnliche richterrechtliche Schrankensystematik aufgezeigt,[947] die grundsätzlich auch die Warenverkehrsfreiheit in Form der Cassis-de-Dijon-Formel besitzt. Des weiteren wurde bereits an obiger Stelle festgestellt,[948] dass der EuGH in jüngerer Zeit auch für die übrigen Grundfreiheiten ähnliche Schranken aufgestellt hat, die eine Beschränkung aus Gründen des Allgemeininteresses ausnahmsweise zulassen.[949] Dies führt dazu, dass die durch den EuGH entwickelte höchstrichterliche Schrankensystematik bei jeder Grundfreiheit zu beachten ist.[950] Demnach müssen nationale Maßnahmen in nichtdiskriminierender Weise angewendet werden.[951] Darüber hinaus sind die Beschränkungen nur aus zwingenden Gründen des Allgemeininteresses zulässig, müssen geeignet sein, die Verwirklichung des mit ihnen verfolgten Ziels zu gewährleisten und dürfen nicht über das hinausgehen, was zur Erreichung des Ziels erforderlich ist (Verhältnismäßigkeit).[952] Diese Grundsätze sind nun im Rahmen der Prüfung der Dienstleistungsfreiheit auf die gegen den Content-Provider gerichteten Sperr- bzw. Löschanordnungen zu übertragen:

Die staatlichen Kontrollverfügungen stellen unterschiedslose Maßnahmen dar, weil sie unabhängig von der Staatsangehörigkeit des Content-Providers oder Nutzers ergehen. Ferner könnte die Motivation der staatlichen Behörde, rechtswidrige Inhalte im Internet beim Content-Provider zu beseitigen, um die Nutzer bzw. die Gesellschaft vor ihnen zu schützen, als zwingende Gründe des Allgemeinwohls angesehen werden. Allerdings ist dieser Gedanke abzulehnen. Denn wie sich aus der Rechtsprechung des EuGH zur Dienstleistungsfreiheit ergibt[953] sowie ein Vergleich mit der Niederlassungsfreiheit und der Warenverkehrsfreiheit zeigt, sind schützenswerte Allgemeininteressen insbesondere der Verbraucher- und Gläubigerschutz, die Lauterkeit des Handelsverkehrs, der Schutz des geistigen Eigentums, kulturpolitische Belange, die wirksame steuerliche Kontrolle und das Funktionieren der Rechtspflege.[954] Auf diese Allgemeininteressen können die Kontrollmaßnahmen jedoch nicht gestützt werden. Die staatlichen Behörden werden vielmehr aus Gründen der öffentlichen Sittlichkeit, Sicherheit und Ordnung tätig. Diese Gründe fallen aber nicht unter den Begriff der zwingenden Gründe des Allgemeininte-

---

946 EuGH, Rs. C-43/93, 09.08.1994, Slg. 1994, I-3803, 3824 Rdnr. 16 (Vander Elst); EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1175 ff. Rdnr. 23 ff. (Alpine Investments); EuGH, Rs. C-398/95, 05.06.1997, Slg. 1997, I-3091, 3120 Rdnr. 21 (Ergasias).

947 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (a).

948 Vgl. hierzu die Anmerkungen in der Fn. 860.

949 Schwarze, „Medienfreiheit und Medienvielfalt im Europäischen Gemeinschaftsrecht“, ZUM 2000, 779, 783.

950 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 53 f.

951 Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1680.

952 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 54.

953 Vgl. EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen); EuGH, verbundene Rs. 110/78 und 111/78, 18.01.1979, Slg. 1979, 35, 52 f. Rdnr. 27 ff. (Van Wesemael); EuGH, Rs. 279/80, 17.12.1981, Slg. 1981, 3305, 3325 Rdnr. 19 (Webb).

954 Koenig/Haratsch, Europarecht, 2. Auflage, S. 242 Rdnr. 512.

resses.[955] Folglich können solche die Dienstleistungsfreiheit beschränkenden Kontrollmaßnahmen nicht durch die zwingenden Gründe des Allgemeininteresses gerechtfertigt werden.

(c) Art. 55 i.V.m. Art. 45, 46 EGV

Es könnte sich jedoch eine Rechtfertigung der Sperr- und/oder Löschverfügungen aus den über Art. 55 EGV anwendbaren Ausnahmetatbeständen der Art. 45 und 46 EGV ergeben.

Da der Content-Provider seine Dienste regelmäßig nicht in Ausübung öffentlicher Gewalt anbietet, ist Art. 45 EGV nicht erfüllt.

Art. 46 EGV würde allein nach seinem Wortlaut als Rechtfertigungsnorm ebenfalls ausscheiden, weil die staatlichen Kontrollmaßnahmen nicht auf Sonderregelungen für Ausländer beruhen. Wie aber bereits oben bei der Prüfung der Niederlassungsfreiheit festgestellt wurde,[956] darf man Art. 46 EGV nicht strikt wörtlich nehmen, sondern muss ihn ohne den Satzteil der „*Sonderregelungen für Ausländer*“ lesen.[957] Daher ist Art. 46 I EGV auch auf unterschiedslose staatliche Regelungen anzuwenden. Eine staatliche Maßnahme, die die Dienstleistungsfreiheit beschränkt, ist also dann gemäß Art. 46 I EGV i.V.m. Art. 55 EGV gerechtfertigt, wenn sie aus Gründen der öffentlichen Ordnung, Sicherheit oder Gesundheit ergeht und verhältnismäßig ist.[958]

Wie schon bei der Warenverkehrsfreiheit – speziell beim Art. 30 EGV – und bei der Niederlassungsfreiheit aufgezeigt,[959] lassen sich die Ziele der staatlichen Behörden, welche die Sperr- und/oder Löschanordnungen verfügen, unter die europarechtlichen Begriffe der öffentlichen Sicherheit und Ordnung subsumieren.[960] Der Staat hat nämlich ein großes Interesse daran, den unbeschränkten Zugang von (jugendlichen) Nutzern zu beispielsweise rassistischen, menschenverachtenden oder pornographischen Internet-Seiten zu verhindern. Auch will er sich selbst und seine demokratische Struktur vor diesen Inhalten schützen. Um dieses Ziel zu erreichen, ist es schon allein aus technischer Sicht erforderlich, den Content-Provider aufzufordern, den ungewünschten Inhalt zu sperren und/oder zu löschen. Diese Maßnahmen sind auch geeignet, (zumindest teilweise) den Zugang für die Nutzer und somit eine weitere Verbreitung des Inhalts zu verhindern. Ferner wird hier der Grundsatz der Erforderlichkeit beachtet, da die Kontrollmaßnahmen nicht über das hinausgehen, was zur Erreichung des Ziels notwendig ist.

---

955 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a).

956 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).

957 Koenig/Haratsch, Europarecht, 2. Auflage, S. 242 Rdnr. 513.

958 Koenig/Haratsch, Europarecht, 2. Auflage, S. 242 Rdnr. 513.

959 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4). und bb. (2). (b).

960 Wie bereits oben bei der Niederlassungsfreiheit festgestellt wurde, gehört zur öffentlichen Sicherheit der Schutz der Allgemeinheit und des Einzelnen gegen Bedrohungen des Bestands des Staats und seiner Einrichtungen, sowie des Lebens, der Gesundheit, der Freiheit und der Ehre. Des weiteren fällt unter den Begriff der öffentlichen Ordnung der Schutz gegen Bedrohungen eines geordneten menschlichen und staatsbürgerlichen Zusammenlebens.

Schließlich sind die Sperr- bzw. Löschmaßnahmen als angemessen anzusehen. Zwar wird hierdurch normalerweise auch in die Rechte des Content-Providers eingegriffen, da er seine Inhalte den Nutzern im Internet nicht mehr frei zur Verfügung stellen kann. Diese Rechtsverletzung muss er jedoch hinnehmen, weil sie im Gegensatz zum Schaden, der dem Nutzer und dem Staat durch die rechtswidrigen Inhalte droht, vergleichsweise gering ist. Die staatlichen Maßnahmen zielen ausschließlich gegen die unerwünschten Angebote des Content-Providers.[961] In weitere Rechte wird nicht eingegriffen. Folglich werden die Rechte des Content-Providers nur moderat verletzt. Die staatlichen Maßnahmen sind deshalb verhältnismäßig.

(4) Zusammenfassung

Zwar greifen die staatlichen Kontrollmaßnahmen in die durch Art. 49 EGV gewährleistete Dienstleistungsfreiheit des Content-Providers ein. Diese Verletzung der Dienstleistungsfreiheit ist aber aufgrund der Art. 55, 46 I EGV gerechtfertigt, so dass die staatlichen Sperr- bzw. Löschverfügungen in den genannten Fallkonstellationen aus europarechtlicher Sicht als zulässig anzusehen sind.

dd. Zwischenergebnis

Aus den vorangegangenen Prüfungen hat sich ergeben, dass sämtliche gemeinschaftsrechtlichen Verstöße gegenüber dem Content-Provider, die durch staatliche Kontrollmaßnahmen begangen werden, sei es bei der Warenverkehrsfreiheit, Niederlassungs- oder Dienstleistungsfreiheit, letztlich rechtmäßig erfolgen. Insoweit ist keine Europarechtswidrigkeit festzustellen.

2. Kontrollmaßnahmen gegen den Service-Provider

a. Grundkonstellation

Der Service-Provider hält im Gegensatz zum Content-Provider keine eigenen, sondern fremde Inhalte im Internet bereit. Sein Internet-Dienst besteht lediglich darin, die Inhalte des Content-Providers zu speichern. Es ergibt sich somit folgende Grundkonstellation:

Der Nutzer wählt sich mit Hilfe eines Access-Providers in das Netz ein.[962] Via Internet gelangt der Nutzer zum bereitgehaltenen Inhalt des Content-Providers. Dieser Inhalt kann – wie oben bereits ausführlich besprochen[963] – verschiedenartig ausgestaltet sein.

---

961 Vgl. hierzu die Ausführungen weiter oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

962 Wie beim Content-Provider wird auch beim Service-Provider der Access-Provider, obwohl er regelmäßig bei der genannten Konstellation in der Praxis beteiligt ist, nicht auf seine europarechtliche Relevanz hin überprüft. Denn auf ihn wird später noch gesondert eingegangen, vgl. unten unter B. 3. Teil. 2. Kapitel. V. 3.

963 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa.

Der Content-Provider besitzt in diesem Fall jedoch keine eigenen Speicherplätze und verfügt auch nicht über die für das reine Content-Providing benötigte Hard- und Software. Vielmehr nimmt er hierfür die Dienste eines Service-Providers in Anspruch. Der Service-Provider bietet somit dem Nutzer die fremden Inhalte des Content-Providers im Netz an, da er diese Inhalte in das Internet einspeist. An diesem Vorgang sind also regelmäßig drei Personen beteiligt: Der Nutzer, der Content-Provider und der Service-Provider.

Geht die zuständige Polizei- oder Sicherheitsbehörde gegen rechtswidrige Inhalte vor, die der Content-Provider mit Hilfe des Service-Providers in das Internet eingestellt hat, so kann sie eine Sperr- und/oder Löschanordnung direkt gegen den Content-Provider erlassen. Sie kann dieselbe Maßnahme aber auch gegen den Service-Provider richten. Scheinbar führt beides zum gleichen Erfolg, weil in beiden Fällen auf denselben Inhalt mit derselben Maßnahme eingewirkt wird. Doch dieser Gedanke ist nur dann richtig, wenn sich sowohl der Content-Provider als auch der Service-Provider im Inland befinden und die zuständige Behörde Maßnahmen an beide Provider richten kann. Ist dies nicht der Fall, dann gilt es zu bedenken, dass der Service-Provider die Herrschaftsgewalt über sämtliche technischen Geräte inne hat, die für das Service-Providing nötig sind. Er ist damit vor allem in der Lage, den rechtswidrigen Inhalt, den der Content-Provider in das Netz eingestellt hat, sofort zu sperren bzw. zu löschen. Ein Rückgriff auf den Content-Provider ist oft sehr zeitintensiv, da er erst ausfindig gemacht werden muss.[964] Deshalb ist es wohl effektiver, die Lösch- bzw. Sperranordnung gegen den Service-Provider zu richten, insbesondere dann, wenn sich der Content-Provider nicht im Inland aufhält.[965] Die anschließenden Fallgestaltungen gehen deswegen davon aus, dass die behördlichen Kontrollmaßnahmen gegen den Service-Provider gerichtet sind. Er ist demnach im folgenden Adressat der staatlichen Maßnahme.[966]

Des weiteren werden die einzelnen Fallvarianten sowohl aus der Perspektive des Service-Providers als auch aus der Sichtweise des Content-Providers, der mittelbar durch die gegen den Service-Provider erlassene Sperr- bzw. Löschanordnung in Europarecht betroffen sein kann, betrachtet.[967]

Die Perspektive des Nutzers, der den Inhalt vom Content-Provider beim Service-Provider abfragt, wird – wie bereits oben bei der reinen Betrachtung des Content-

---

964 Holznagel, „Verantwortlichkeit im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte“, ZUM 2000, 1007, 1022.

965 Natürlich sind auch Sperr- und/oder Löschanordnungen gegenüber dem Content-Provider oder gegen beide möglich und sinnvoll. Dies ist aber letztendlich eine Frage des Einzelfalls.

966 Falls die Sperr- und/oder Löschanordnungen auch oder nur gegen den Content-Provider gerichtet sind, ergibt sich die gleiche Prüfung wie oben beim Content-Provider. Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. Die europarechtliche Problematik bezüglich des Service-Providers verändert sich dadurch nicht und stellt sich wie folgt dar.

967 Letztendlich wird ja der Inhalt des Content-Providers vom Service-Provider auf behördliche Veranlassung gesperrt und/oder gelöscht.

Providers – aus den genannten Gründen nicht behandelt.[968] Denn der einzelne Nutzer ist von den staatlichen Maßnahmen im Vergleich zu den Providern nur am Rande betroffen. Er könnte sich bei manchen Fallkonstellationen sicherlich auch auf das Europarecht berufen. Allerdings interessieren in dieser Arbeit vor allem die Provider, die von den staatlichen Kontrollmaßnahmen direkt oder indirekt tangiert werden. Bei ihnen ist die wirtschaftliche Auswirkung solcher Maßnahmen bedeutend größer als beim Nutzer. Der einzelne Nutzer spielt insoweit nur eine untergeordnete Rolle. Seine Sichtweise ist daher zu vernachlässigen, zumal damit ein erheblicher Gewinn an Übersichtlichkeit für die vorliegende Arbeit erreicht wird.

b. Fallvariante I: Deutscher Service-Provider, Content-Provider aus EU-Ausland, Deutscher Nutzer

Zunächst soll der Content-Provider aus dem EU-Ausland stammen. Wie bei der oben durchgeführten separaten Betrachtung der Kontrollmaßnahmen gegen den Content-Provider sind verschiedene Differenzierungen beim Content-Provider möglich.[969] Denn insoweit kann es sich erneut um eine natürliche oder juristische Person aus dem EU-Ausland handeln. Zu beachten ist hingegen in diesem Fall, dass der Content-Provider keine eigene Technik für das Anbieten seiner eigenen Inhalte besitzt. Diese Funktion hat der Service-Provider übernommen. Deshalb ergeben sich im Detail doch andere Unterfälle, als sie von der Prüfung des Content-Providings bekannt sind:[970]
Zum einen ist ein Content-Provider als natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland denkbar. Zum anderen kann der Content-Provider eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland sein, wobei sich lediglich der von dem Content-Provider beim Service-Provider gespeicherte Inhalt im Inland befindet. Schließlich besteht auch die Möglichkeit, dass der Content-Provider zwar aus dem EU-Ausland kommt und seinen Sitz im EU-Ausland hat, aber neben dem eingestellten Inhalt noch weitere mit dem Content-Providing im Zusammenhang stehende Komponenten (etwa Büroräume) im Inland zu finden sind.

aa. Der Content-Provider ist eine natürliche Person aus dem EU-Ausland, die ihren Wohnsitz und eventuell ihre Büroräume im Inland hat

Weil in den folgenden Fallkonstellationen sowohl der Content-Provider als auch der Service-Provider in ihren Grundfreiheiten aus dem EGV beeinträchtigt werden können, ist es wichtig, zwischen diesen beiden Personen zu differenzieren: So muss einerseits die Perspektive des Content-Providers und andererseits die Sicht des Service-Providers betrachtet werden. Denn sie können in unterschiedlicher Form durch die staatlichen Kontrollmaßnahmen in ihren Grundfreiheiten betroffen sein. Da die Kontrollmaßnah-

968 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. IV. 4.
969 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b.
970 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1.

men an den Service-Provider adressiert sind, soll zunächst auf dessen Sichtweise eingegangen werden.

(1) Sicht des Service-Providers

(a) Warenverkehrsfreiheit

Der Service-Provider stellt dem Content-Provider für dessen Inhalte regelmäßig Speicherkapazität zur Verfügung. Da es sich hierbei um keine Ware i.S.d. 23 ff. EGV – also um einen körperlichen, geldwerten Gegenstand – handelt,[971] kann die Warenverkehrsfreiheit von staatlichen Kontrollmaßnahmen insoweit nicht betroffen sein.

(b) Dienstleistungsfreiheit

Der Service-Provider könnte aber durch die gegen ihn gerichteten staatlichen Kontrollmaßnahmen in seiner nach den Art. 49 ff EGV garantierten Dienstleistungsfreiheit beeinträchtigt werden.
Hierfür müsste es sich beim Service-Providing zunächst um eine Dienstleistung i.S.d. Art. 50 EGV handeln. Unter den Begriff der gemeinschaftsrechtlichen Dienstleistungsfreiheit fallen zeitlich begrenzte, in grenzüberschreitender Weise gegen Entgelt erbrachte selbständige Leistungen.[972] Das Service-Providing stellt eine selbständige, regelmäßig gegen Entgelt erbrachte Leistung dar. Fraglich ist jedoch schon, ob die Speicherung des vom Content-Provider eingestellten Inhalts als nur von vorübergehender Dauer angesehen werden kann. Denn Ziel ist es, diesen Inhalt den Nutzern des Internets sehr lange und kontinuierlich zur Verfügung zu stellen.[973]
Letztlich kommt es auf die Beantwortung dieser Frage nicht an. So scheitert in dieser Fallvariante die Anwendbarkeit der Art. 49 ff. EGV schon allein daran, dass das Kriterium der Grenzüberschreitung nicht gegeben ist.[974] Es liegt weder ein Sachverhalt der aktiven oder passiven Dienstleistungsfreiheit noch der Korrespondenzdienstleistungsfreiheit vor. Aus Sicht des Service-Providers muss ein rein innerstaatlicher Sachverhalt angenommen werden. Daran ändert selbst die Tatsache nichts, dass der Content-Provider aus dem EU-Ausland stammt.[975] Die Leistung, die der Service-Provider dem

---

971 Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 249 ff.

972 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1186.

973 Vgl. hierzu die Diskussion oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (2). sowie Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 13:
„Die Zuordnung eines Sachverhalts zur Dienstleistungsfreiheit oder Niederlassungsfreiheit muss im Einzelfall unter Berücksichtigung von Dauer, Häufigkeit, Periodizität und Kontinuität der Tätigkeit erfolgen". Ob darin schon eine Niederlassungsfreiheit oder nur eine Dienstleistungsfreiheit zu sehen ist, vgl. insoweit die Ausführungen in Fn. 984.

974 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 117.

975 Wie sich aus dem EuGH-Urteil, Rs. 52/79, 18.03.1980, Slg. 1980, 833, 855 Rdnr. 9 (Debauve) ergibt, sind die Vertragsbestimmungen über den freien Dienstleistungsverkehr nicht auf Betätigungen anwendbar, „[...] deren wesentlichen Elemente sämtlich nicht über die Grenzen eines Mitgliedstaats hinausweisen". Vgl. zu dieser Thematik auch unten unter B. 2. Teil. 2. Kapitel. V. 3. b. aa. (a).

Content-Provider bietet, bleibt im Inland. Die Rechtsprechung des EuGH zur Rechtssache Alpine Investments[976] greift hier gerade nicht ein, da die Leistung nicht in einem anderen Mitgliedstaat erbracht wird.
Die gemeinschaftsrechtliche Dienstleistungsfreiheit ist somit nicht tangiert.

(c) Niederlassungsfreiheit

Mangels eines grenzüberschreitenden Sachverhalts kommen auch die Normen der Niederlassungsfreiheit i.S.d. Art. 43 ff. EGV nicht zur Anwendung.

(2) Sicht des Content-Providers

(a) Warenverkehrsfreiheit

Zunächst könnte der Content-Provider durch die staatlichen Kontrollmaßnahmen, die gegenüber dem Service-Provider ergangen sind, in seinem Recht auf freien Warenverkehr gemäß Art. 28 EGV mittelbar verletzt sein. Wie bereits an obiger Stelle gesagt,[977] richtet sich dies nach der durch den Content-Provider angebotenen bzw. beworbenen Ware. Wird diese, wenn der Nutzer sie bestellt, erst aus dem EU-Ausland über die Grenze zum inländischen Nutzer verbracht, ist Art 28 EGV tangiert. Befindet sich die Ware allerdings schon im Inland, dann fehlt der Ware ein von Art. 28 EGV geforderter grenzüberschreitender Sachverhalt, so dass die Warenverkehrsfreiheit nicht betroffen ist.

(b) Niederlassungsfreiheit

Des weiteren könnte in den staatlichen Kontrollmaßnahmen ein Eingriff in die Niederlassungsfreiheit gemäß den Art. 43 ff. EGV gesehen werden. Problematisch ist hier jedoch, dass der Content-Provider zwischen Service-Provider und Nutzer steht: Zum einen nutzt der Content-Provider die Speicherkapazität des Service-Providers und zum anderen bietet er seinen eingestellten Inhalt dem Nutzer im Internet an. Demnach könnte neben der Warenverkehrsfreiheit auch die Dienstleistungsfreiheit betroffen sein. Diese ist aber gegenüber der Niederlassungsfreiheit nach Art. 50 I EGV subsidiär. Da die natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland in stabiler und kontinuierlicher Weise durch ihre Tätigkeit als Content-Provider am Wirtschaftsleben im Inland teilnimmt,[978] liegt eine Niederlassung i.S.d. Art. 43 EGV vor.[979] Demzufolge sind die Art. 43 ff EGV anwendbar. Die Niederlassungsfreiheit des Content-Providers ist somit

---

976 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141 ff. (Alpine Investments BV); vgl. auch oben unter B. 3. Teil. 2. Kapitel. V. 1. c. bb. (3).

977 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1).

978 Natürlich gibt es bei den Content-Providern hiervon auch Ausnahmen, wenn sie ihren Inhalt kostenlos im Internet anbieten und keine kommerziellen Ziele damit verfolgen. Dies dürfte aber nur einen geringen Teil der Content-Provider im Internet ausmachen.

979 Herdegen, Europarecht, 2. Auflage, § 17 Rdnr. 317; EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4195 Rdnr. 25 (Gebhard).

durch staatliche Sperr- und/oder Löschanordnungen tangiert, da der Service-Provider seine Dienste nicht mehr ungestört an den Content-Provider leisten und dieser sie somit nicht mehr nutzen kann. Zudem wird der Content-Provider daran gehindert, seine Dienste dem Nutzer frei zur Verfügung zu stellen.

(c) Dienstleistungsfreiheit

Wegen des Grundsatzes der Subsidiarität scheidet eine Anwendbarkeit der Dienstleistungsfreiheit deshalb aus.

bb. Der Content-Provider ist eine natürliche oder juristische Person, die ihren Sitz im EU-Ausland hat, deren gespeicherte Inhalte sich jedoch allein beim Service-Provider im Inland befinden

(1) Sicht des Service-Providers

(a) Dienstleistungsfreiheit

Die staatlichen Kontrollmaßnahmen könnten in die Dienstleistungsfreiheit des Service-Providers eingreifen. Denn durch eine Sperr- und/oder Löschanordnung, die gegen den Inhalt des Content-Providers gerichtet ist, wird der Service-Provider daran gehindert, seine Hauptleistungspflicht bezüglich des Content-Providers zu erfüllen, den Inhalt jedem Nutzer des Internets bereit zu halten. Fraglich ist jedoch, ob die gemeinschaftsrechtliche Dienstleistungsfreiheit aus seiner Sicht überhaupt zur Anwendung kommt, da sich der Rechner des deutschen Service-Providers im Inland befindet. Er erbringt also seine Leistung gänzlich im Inland. Obwohl der Content-Provider aus dem EU-Ausland stammt, handelt es sich bei der Speicherung seines Inhalts aus der Sichtweise des Service-Providers – wie oben – um einen rein innerstaatlichen Sachverhalt.[980]
Ein Eingriff in die Dienstleistungsfreiheit ist demnach nicht gegeben.

(b) Niederlassungsfreiheit

Auch die übrigen Grundfreiheiten, insbesondere die Niederlassungsfreiheit, sind aus dem selben Grund nicht anwendbar.

(2) Sicht des Content-Providers

(a) Warenverkehrsfreiheit

Zunächst besteht wiederum die Möglichkeit, dass durch behördliche Sperr- und/oder Löschanordnungen mittelbar gegen die Warenverkehrsfreiheit verstoßen wird. Je nachdem, wie die angebotenen bzw. beworbenen Waren des Content-Providers zum Nutzer gelangen – grenzüberschreitend oder nicht – ist Art. 28 EGV einschlägig. Denn wenn

---

980 Bleckmann, Europarecht, 6. Auflage, § 20 Rdnr. 1676.

die vom Nutzer bestellten Waren eine Grenze zwischen den Mitgliedstaaten passieren müssen, ist die Warenverkehrsfreiheit von den staatlichen Kontrollmaßnahmen mittelbar betroffen.[981]

(b) Niederlassungsfreiheit

Dagegen kommt ein Eingriff in die Niederlassungsfreiheit nicht in Betracht. Eine Niederlassung i.S.d. Art. 43 EGV liegt seitens des Content-Providers nicht vor. Denn der gespeicherte Inhalt des Content-Providers durch den Service-Provider, der sich im Inland befindet, kann nicht ausreichen, um darin eine Niederlassung zu sehen. Eine rein virtuelle Niederlassung in Form einer Homepage kann für Art. 43 EGV nicht genügen. Dies wird schon aus der E-Commerce Richtlinie[982] vom 17.07.2000 deutlich, die in Art. 2 c ECRL selbst das Vorhandensein und die Nutzung von technischen Mitteln und Technologien, die zum Anbieten des Dienstes erforderlich sind, nicht ausreichen lässt, um eine gemeinschaftsrechtliche Niederlassung zu begründen.

(c) Dienstleistungsfreiheit

Da die Niederlassungsfreiheit und somit der Subsidiaritätsgrundsatz nicht anwendbar sind, könnte die Dienstleistungsfreiheit von den staatlichen Kontrollmaßnahmen tangiert sein. Dabei ist zwischen dem Verhältnis des Content-Providers zum Service-Provider sowie des Content-Providers zum Nutzer zu unterscheiden. Denn hier handelt es sich um unterschiedliche Fälle der Dienstleistungsfreiheit:
Bezüglich des Service-Providers nimmt der Content-Provider dessen Dienste in Anspruch. Dieses Service-Providing ist aus der Sicht des Content-Providers, der aus dem EU-Ausland stammt, eine Dienstleistung i.S.d. Art. 49 ff. EGV.[983] Sie wird regelmäßig gegen Entgelt erbracht, hat in gewisser Weise vorübergehenden Charakter[984] und besitzt, da sich der Content-Provider aus dem EU-Ausland für die Erbringung der Dienst-

---

981 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1).

982 Richtlinie 2000/31/EG des Europäischen Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. EG Nr. L 178 vom 17.07.2000.

983 Hance, Internet-Business & Internet-Recht, S. 78 f.

984 Natürlich kann diesbezüglich eingewendet werden, dass der Content-Provider seinen Inhalt auf Dauer durch den Service-Provider für die Internet-Gemeinde bereithalten will. Diesem Gedanken muss aber entgegen gehalten werden, dass dies nicht der Praxis entspricht. Denn häufig wird der eingestellte Inhalt aktualisiert oder verändert. Dadurch wird die Kontinuität der Leistung unterbrochen. Außerdem stellt diese Leistung – trotz ihrer Dauerhaftigkeit – eine Dienstleistung i.S.d. Art. 49 ff. EGV dar. Das Element der zeitlichen Begrenzung wurde vor allem deswegen als Voraussetzung für die Dienstleistungsfreiheit eingeführt, um eine bessere Abgrenzung zwischen ihr und der Niederlassungsfreiheit zu erreichen. Hier scheidet die Bejahung einer Niederlassung von vornherein aus (siehe oben), so dass – obwohl die Leistung des Service-Providers auf Dauer angelegt ist – eine Dienstleistung bejaht werden kann. Schließlich muss weiterhin bedacht werden, dass der Content-Provider (wenn überhaupt) nur für kurze Dauer das Inland aufgesucht hat, um seinen Inhalt beim Service-Provider speichern zu lassen. Vgl. auch Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 13.

leistung ins Inland begeben muss, ein grenzüberschreitendes Element. Demnach liegt hier die Variante der passiven Dienstleistungsfreiheit vor.[985]

Im Hinblick auf den Nutzer erbringt der Content-Provider eine Leistung, da er für ihn seine in das Internet eingestellten Daten bereithält. Diese Leistung wird im Inland erbracht. Der Content-Provider befindet sich jedoch im EU-Ausland. Es könnte sich deshalb insoweit um einen Fall der aktiven Dienstleistungsfreiheit handeln. Allerdings müsste sich der Content-Provider zu seiner Leistungserbringung ebenfalls in das Inland begeben. Wenn nun der Content-Provider selbständig oder mit Hilfe Dritter seine Inhalte beim Service-Provider im Inland eingestellt hat, dann wäre diese Voraussetzung erfüllt. Die grenzüberschreitende Leistung des Content-Providers, die er im Inland erbracht hat, wird quasi beim Service-Provider „zwischengeparkt", bis der Nutzer diese Leistung abruft. Häufig dürfte der Fall aber anders liegen. Es besteht die Möglichkeit, dass der Content-Provider seine Inhalte via Internet beim Service-Provider deponiert, so dass lediglich seine Leistung die Grenze überschreitet. Insofern müsste hier dann von einer Korrespondenzdienstleistung gesprochen werden. Letztendlich kommt es jedoch nicht darauf an, welcher Typ der Dienstleistungsfreiheit vorliegt, sondern nur, dass überhaupt eine Form der Dienstleistungsfreiheit gegeben ist und somit die Art. 49 ff. EGV zur Anwendung kommen können.[986]

Der Content-Provider wird demnach durch die staatlichen Sperr- bzw. Löschmaßnahmen gleich zweimal in seiner Dienstleistungsfreiheit beeinträchtigt.

cc. Der Content-Provider ist eine natürliche bzw. juristische Person, bei der sich – je nach Ausgestaltung – noch andere Komponenten, die im Zusammenhang mit dem Content-Providing stehen (vor allem Büroräume), im Inland befinden

(1) Sicht des Service-Providers

An der Art der Leistung des Service-Providers hat sich im Vergleich zur vorhergehenden Fallunterscheidung nichts geändert. Er speichert immer noch als deutscher Service-Provider im Inland den Inhalt des Content-Providers aus dem EU-Ausland. Seine Dienstleistung ist rein innerstaatlicher Natur, so dass der EGV, vor allem seine Niederlassungsfreiheit und Dienstleistungsfreiheit, auf ihn hier nicht zur Anwendung kommt.[987]

---

985 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1189; zu denken ist außerdem an einen Fall der Korrespondenzdienstleistung, da sich der Content-Provider nur im EU-Ausland aufhält und er seine Inhalte auch via Internet auf den Server des Service-Providers schicken kann. Welche Art der Dienstleistungsfreiheit vorliegt, ist letztendlich eine Frage des Einzelfalls.

986 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 21 ff.

987 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 60 EGV Rdnr. 16.

(2) Sicht des Content-Providers

(a) Warenverkehrsfreiheit

Die Warenverkehrsfreiheit gemäß Art. 28 EGV ist von staatlichen Kontrollmaßnahmen wiederum dann mittelbar betroffen, wenn die vom Content-Provider angebotenen oder beworbenen Waren grenzüberschreitend zum Nutzer gelangen.[988]

(b) Niederlassungsfreiheit

Ob die Niederlassungsfreiheit oder die Dienstleistungsfreiheit in dieser Fallvariante zur Anwendung kommt, richtet sich danach, welche anderen Komponenten sich neben dem Inhalt des Content-Providers im Inland befinden. Denn die Tatsache, dass sich der Content-Provider mit einer gewissen Infrastruktur im Inland ausgestattet hat, reicht allein nicht aus, um eine Niederlassung i.S.d. Art. 43 ff. EGV anzunehmen, solange sie für die Erbringung der Dienstleistung erforderlich ist.[989] Der vom Content-Provider angebotene Inhalt wird in diesem Fall aber vom Service-Provider bereitgehalten. Er besitzt die Infrastruktur – sprich die Technik und Software – für die Speicherung und somit ständige Präsenz im Internet. Dies ist auch im Interesse des Content-Providers, dessen Inhalte ohne eigene Rechner in das Internet eingestellt werden. Besitzt der Content-Provider neben dem Inhalt beispielsweise noch Büroräume im Inland, die im Zusammenhang mit dem Content-Providing stehen,[990] dann ist dies schon ein Mehr im Vergleich zur reinen Infrastruktur für das Content-Providing. Denn diese notwendige Infrastruktur stellt bereits der Service-Provider zur Verfügung. Besitzt der Content-Provider also nicht nur eine vernachlässigbare Komponente im Rahmen des Content-Providings, die neben dem Inhalt im Inland existiert, dann kommt eher die Niederlassungsfreiheit als die Dienstleistungsfreiheit zur Anwendung. Letztlich bleibt es jedoch eine Frage des Einzelfalls, wie hier das Content-Providing nach dem EGV zu beurteilen ist.

c. Fallvariante II: Deutscher Service-Provider, Deutscher Content-Provider, Nutzer aus dem EU-Ausland

Auch bei dieser Fallvariante kann wiederum untergliedert werden und zwar in der Person des Nutzers:

---

988 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (1).

989 Koenig/Haratsch, Europarecht, 2. Auflage, Rdnr. 504.

990 Zu denken ist hier an eine Stelle, die Bestellungen von Internet-Angeboten entgegennimmt oder die Abrechnungen für das Inland durchführt.

aa. Der Nutzer ist eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland

(1) Sicht des Service-Providers

Für den Service-Provider stellt die behördliche Sperr- bzw. Löschanordnung keinen Eingriff in das Europarecht dar. Aus seiner Sicht liegt ein rein inländischer Sachverhalt vor, so dass die Grundfreiheiten des EGV, insbesondere die Niederlassungs- und Dienstleistungsfreiheit, keine Anwendung finden.

(2) Sicht des Content-Providers

(a) Warenverkehrsfreiheit

Ein Verstoß gegen die Warenverkehrsfreiheit nach Art. 28 EGV ist zu verneinen. Denn da es sich um einen deutschen Content-Provider handelt, wird er hauptsächlich Waren im Internet anbieten oder bewerben, die sich in Deutschland befinden. Ein grenzüberschreitender Sachverhalt bezüglich der Waren – der Nutzer befindet sich in dieser Fallvariante ebenfalls im Inland – ist somit in der Regel auszuschließen.

(b) Dienstleistungsfreiheit

Auch eine Beeinträchtigung der Dienstleistungsfreiheit gemäß den Art. 49 ff. EGV ist nicht gegeben. Zwar müssen hier zum einen die durch den Content-Provider in Anspruch genommenen Dienste des Service-Providers sowie die Abrufung der Inhalte des Content-Providers durch den Nutzer getrennt voneinander betrachtet werden. In beiden Fällen ist aber eine Anwendbarkeit der Dienstleistungsfreiheit i.S.d. Art. 49 ff EGV nicht zu bejahen, denn es handelt sich jeweils um einen innerstaatlichen Sachverhalt ohne grenzüberschreitendes Element, so dass die Dienstleistungsfreiheit insoweit nicht einschlägig ist.

bb. Der Nutzer ist eine natürliche bzw. juristische Person aus dem EU-Ausland, deren Wohn- bzw. Geschäftssitz ebenfalls im EU-Ausland zu finden ist

(1) Sicht des Service-Providers

Wiederum liegt aus der Sicht des Service-Providers ein rein innerstaatlicher Sachverhalt vor. Er hat lediglich die Aufgabe, für den inländischen Content-Provider dessen Inhalte zu speichern und im Internet bereitzuhalten. Ob der Nutzer aus dem EU-Ausland stammt und auf diesen Inhalt Zugriff nimmt, ändert an seiner Leistungsbeziehung zum Content-Provider nichts. Der EGV, zu denken ist hier zunächst an die Niederlassungsfreiheit und Dienstleistungsfreiheit, ist auf ihn somit nicht anwendbar.

(2) Sicht des Content-Providers

Hier ist von vornherein zwischen dem Leistungsverhältnis Content-Provider/Service-Provider und dem Leistungsverhältnis Content-Provider/Nutzer zu differenzieren:

(a) Content-Provider/Service-Provider

Da der Content-Provider und der Service-Provider im Inland ansässig sind, ist ihre Leistungsbeziehung rein inländisch. Wird sie durch staatliche Kontrollmaßnahmen gestört, liegt stets nur ein inländischer Sachverhalt vor. Der EGV ist hierfür nicht einschlägig.

(b) Content-Provider/Nutzer

Etwas anderes gilt jedoch für die Leistungsbeziehung zwischen dem Content-Provider und dem Nutzer:

(aa)Warenverkehrsfreiheit

Zunächst könnte in staatlichen Kontrollmaßnahmen mittelbar ein Verstoß gegen die Warenverkehrsfreiheit gemäß Art. 29 EGV gesehen werden. Da aber die Sperr- und/oder Löschmaßnahmen keine spezifischen Beschränkungen der Ausfuhrströme bezwecken oder bewirken sollen,[991] kann eine für Art. 29 EGV notwendige Maßnahme gleicher Wirkung nicht angenommen werden.[992]

(bb)Dienstleistungsfreiheit

Hingegen lässt sich ein Verstoß gegen die Dienstleistungsfreiheit bejahen: Der Nutzer aus dem EU-Ausland nimmt via Internet Zugriff auf den Inhalt des Content-Providers. Der vom Nutzer gewünschte Inhalt gelangt über die Datenautobahn auf den Rechner des Nutzers. Dieser Vorgang stellt eine Dienstleistung i.S.d. Art. 50 EGV dar. Denn sie erfolgt im Regelfall entgeltlich, vorübergehend und grenzüberschreitend. Indem weder der Dienstleistende noch der Dienstleistungsempfänger für das Erbringen der Leistung die Grenze passieren, sondern allein die Leistung vom Inland in das EU-Ausland wandert, liegt hier ein Fall der Korrespondenzdienstleistung vor, die unter den Schutz der Art. 49 ff EGV fällt.[993] Der Content-Provider kann sich im übrigen auf die gemeinschaftsrechtliche Dienstleistungsfreiheit auch gegenüber Maßnahmen berufen, die sein Staat erlassen hat.[994] Die Dienstleistungsfreiheit ist somit von den staatlichen Kontrollmaßnahmen tangiert.

---

991 Vgl. zu dieser Problematik ausführlich oben unter B. 3. Teil. 2. Kapitel. V. 1. c. bb. (1).

992 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 34 EGV Rdnr. 18.

993 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).

994 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1176 Rdnr. 30 (Alpine Investments BV); vgl. zur selben Thematik auch oben unter B. 3. Teil. 2. Kapitel. V. 1. c. bb. (3).

d. Fallvariante III: Service-Provider aus dem EU-Ausland, Deutscher Content-Provider, Deutscher Nutzer

Bei dieser Fallvariante findet eine Differenzierung beim Service-Provider statt:

aa. Der Service-Provider ist eine natürliche Person aus dem EU-Ausland, die ihren Wohnsitz und eventuell ihre Büroräume sowie die Technik für das Service-Providing im Inland hat

(1) Sicht des Service-Providers

(a) Niederlassungsfreiheit

Der Service-Provider könnte durch die behördlichen Sperr- und/oder Löschanordnungen in seinem Recht auf Niederlassungsfreiheit gemäß den Art. 43 ff. EGV tangiert sein.
Dies ist zu bejahen. Denn die natürliche Person aus dem EU-Ausland, die ihren Wohnsitz im Inland hat und als Service-Provider fungiert, erfüllt die Kriterien der Niederlassungsfreiheit. Die natürliche Person übt auf Dauer eine Erwerbs- bzw. Geschäftstätigkeit in einem – aus ihrer Sicht – anderen Mitgliedstaat aus.[995] Die staatlichen Kontrollmaßnahmen greifen somit in die Niederlassungsfreiheit des Service-Providers ein.

(b) Dienstleistungsfreiheit

Wegen des Grundsatzes der Subsidiarität[996] scheidet eine Verletzung der Dienstleistungsfreiheit aus.

(2) Sicht des Content-Providers

Für den Content-Provider stellt die Fallgestaltung sowohl bezüglich des Service-Providers als auch bezüglich des Nutzers als einen rein innerstaatlichen Vorgang dar. Es handelt sich um einen im Inland gespeicherten Inhalt, der Nutzer ist Deutscher und der Service-Provider befindet sich ebenfalls ausschließlich im Inland. Deswegen scheidet eine Anwendbarkeit des EGV, vor allem ihre Niederlassungsfreiheit oder Dienstleistungsfreiheit, von vornherein aus.

bb. Der Service-Provider ist eine natürliche oder juristische Person, die ihren Sitz im EU-Ausland hat, während ihre Hard- und Software im Inland zu finden ist

(1) Sicht des Service-Providers

Die Tatsache, dass allein die für das Service-Providing benötigte Technik im Inland stationiert ist, lässt noch nicht den Schluss zu, die Niederlassungsfreiheit sei deswegen

---

995 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 110.

996 Vgl. hierzu Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 13.

berührt. Denn da sich der Service-Provider im übrigen im EU-Ausland befindet, muss vielmehr ein Verstoß gegen die Dienstleistungsfreiheit angenommen werden. Insoweit sind dieselben Überlegungen anzustellen wie bei der oben aufgeführten Prüfung,[997] wo ebenfalls zwischen der Niederlassungsfreiheit und Dienstleistungsfreiheit abgegrenzt werden musste. Deshalb ist die Technik hier gleichermaßen als Infrastruktur für das Service-Providing zu qualifizieren.[998] Statt der Niederlassungsfreiheit ist somit durch die staatlichen Kontrollmaßnahmen die Dienstleistungsfreiheit gemäß den Art. 49 ff. EGV tangiert.

(2) Sicht des Content-Providers

Aus der Perspektive des Content-Providers ergibt sich erneut keine europarechtlich relevante Konstellation. Für ihn stellt sich seine Funktion – sowohl gegenüber dem Service-Provider als auch gegenüber dem Nutzer – als rein innerstaatlicher Sachverhalt dar. Der EGV und seine Grundfreiheiten sind demnach nicht einschlägig.

cc. Der Service-Provider ist eine natürliche oder juristische Person aus dem EU-Ausland, allerdings befinden sich – je nach Ausgestaltung – neben der reinen Technik auch noch andere Komponenten, die im Zusammenhang mit dem Service-Providing stehen (vor allem Büroräume), im Inland

(1) Sicht des Service-Providers

Im Gegensatz zur vorherigen Fallvariante gibt es jetzt neben der reinen Technik noch weiteres Zubehör, das dem Service-Providing zuzurechen ist. Folglich muss ab einem gewissen Grad dieser zusätzlichen Komponenten von einer Niederlassung i.S.d. Art. 43 ff. EGV gesprochen werden. Wann die Schwelle überschritten ist und nicht nur – neben der Hard- und Software – eine reine Infrastruktur für das Service-Providing zu bejahen ist, richtet sich nach dem Einzelfall. Sobald der Service-Provider Büroräume oder vergleichbare Komponenten im Inland unterhält, ist häufig eine Niederlassung, beispielsweise in Form einer Agentur, Zweigniederlassung oder Tochtergesellschaft, anzunehmen. Somit liegt in diesen Fällen bei staatlichen Kontrollmaßnahmen vermehrt eine Beeinträchtigung der Niederlassungsfreiheit vor.

(2) Sicht des Content-Providers

Da sich nur an der Person des Service-Providers etwas geändert hat, die Rechner für die Speicherung des eingestellten Inhalts des Content-Providers sich aber weiterhin im Inland befinden und der Nutzer ebenfalls aus dem Inland stammt, ist ein grenzüberschreitender Sachverhalt aus der Sicht des Content-Providers zu verneinen. Deshalb ist Euro-

---

997 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (2).

998 Geiger, EUV/EGV, 3. Auflage, Art. 50 Rdnr. 1.

parecht, insbesondere die Niederlassungsfreiheit und Dienstleistungsfreiheit, von behördlichen Sperr- und/oder Löschmaßnahmen nicht betroffen.

e. Weitere Kombinationen der genannten beteiligten Personen

Selbst wenn nicht nur eine der beteiligten Personen aus dem EU-Ausland stammt, sondern eine zweite oder alle drei, sind keine weiteren Erkenntnisse und Ergebnisse zu erwarten. Denn letztendlich ist die jeweilige Perspektive des Content- bzw. Service-Providers hinsichtlich der Betroffenheit der einzelnen gemeinschaftsrechtlichen Grundfreiheiten entscheidend und diesbezüglich wurde schon jede denkbare Kombination durchgeprüft.

f. Zusammenfassung

aa. Fallvariante I

Bei der Fallvariante I sind nur europarechtliche Verstöße aus der Sicht des Content-Providers möglich. In allen drei Unterkonstellationen dieser Fallvariante I kann zunächst mittelbar durch staatliche Kontrollmaßnahmen gegen die Warenverkehrsfreiheit nach § 28 EGV verstoßen werden, wenn der Content-Provider Waren anbietet oder bewirbt und diese Waren, falls sie vom Nutzer bestellt werden, grenzüberschreitend zu ihm gelangen würden.
Des weiteren greifen die behördlichen Sperr- und/oder Löschanordnungen in die Niederlassungsfreiheit des Content-Providers ein, wenn es sich bei ihm um eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland handelt.
Ist der Content-Provider dagegen eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland und befindet sich allein sein Inhalt im Inland beim Service-Provider, dann liegt ein Eingriff in die Dienstleistungsfreiheit vor.
Sind hingegen neben dem reinen Inhalt noch weitere Komponenten, die im Zusammenhang mit dem Content-Providing stehen, im Inland, dann ist es der Bewertung des Einzelfalls überlassen, ob noch die Dienstleistungsfreiheit oder bereits die Niederlassungsfreiheit zur Anwendung kommt. Bei dieser Konstellation dürfte wohl häufiger die Niederlassungsfreiheit als die Dienstleistungsfreiheit durch staatliche Kontrollmaßnahmen betroffen sein.[999]

bb. Fallvariante II

In der Fallvariante II gibt es lediglich aus Sicht des Content-Providers bei der Leistungsbeziehung Content-Provider/Nutzer einen Eingriff in die Dienstleistungsfreiheit nach den Art. 49 ff EGV, sofern der Nutzer eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist.

---

[999] Deswegen wird in der folgenden Prüfung bei dieser Konstellation eine Niederlassungsfreiheit angenommen.

cc. Fallvariante III

Hingegen ist in der Fallvariante III allein die Sichtweise des Service-Providers von europarechtlicher Bedeutung: Handelt es sich beim Service-Provider um eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland, so wird die Niederlassungsfreiheit gemäß den Art. 43 ff EGV von den staatlichen Kontrollmaßnahmen tangiert.
Im Gegensatz dazu liegt nur ein Verstoß gegen die Dienstleistungsfreiheit vor, wenn der Service-Provider aus dem EU-Ausland stammt, seinen Sitz ebenfalls im EU-Ausland hat und sich nur die für das Service-Providing notwendige Technik im Inland befindet.
Ein fließender Übergang zwischen der Dienstleistungsfreiheit und der Niederlassungsfreiheit ist dann gegeben, sofern neben der reinen Hard- und Software noch andere Komponenten wie Büroräume, die im Zusammenhang mit dem Service-Providing stehen, im Inland liegen. Häufig ist dann schon eine Beeinträchtigung der Niederlassungsfreiheit zu bejahen, so dass die Dienstleistungsfreiheit gemäß Art. 50 EGV dahinter zurücktritt.[1000]

g. Vereinbarkeit der europarechtlich relevanten Kontrollmaßnahmen mit den jeweiligen Grundfreiheiten

Wieder sind sämtliche – zuvor festgestellte – europarechtliche Beeinträchtigungen, die durch die an den Service-Provider gerichteten Sperr- bzw. Löschanordnungen hervorgerufen werden, bei jeder Fallkonstellation anhand der jeweils betroffenen Grundfreiheit zu prüfen. Schwierig ist dabei nun, dass zwei Sichtweisen geprüft worden sind: Die des Service-Providers, an den die staatliche Kontrollanordnung zur Sperrung bzw. Löschung bestimmter Internet-Seiten gerichtet ist, und die des Content-Providers, der für den Inhalt verantwortlich ist. Diese unterschiedlichen Perspektiven und die daraus resultierende verschiedenartige Bejahung von Verstößen gegen die einzelnen Grundfreiheiten des EGV wird in den anschließenden Prüfungen der jeweiligen Grundfreiheiten durch eine getrennte Betrachtung der Personen berücksichtigt:

aa. Sicht des Service-Providers

(1) Niederlassungsfreiheit

Der Service-Provider wird bei der Fallvariante III in seiner Niederlassungsfreiheit in zwei Konstellationen verletzt. Zum einen, wenn es sich bei dem Service-Provider um eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland handelt. Zum anderen kann die Niederlassungsfreiheit tangiert sein, falls der Service-Provider eine na-

---

[1000] Deswegen wird in der folgenden Prüfung bei dieser Konstellation eine Niederlassungsfreiheit angenommen.

türliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist, wobei sich aber die Technik und weitere mit dem Service-Providing im Zusammenhang stehende Komponenten im Inland befinden.

(a) Inländergleichbehandlung

Wie bereits oben festgestellt wurde,[1001] beinhaltet die Niederlassungsfreiheit nicht nur das Gebot der Inländergleichbehandlung, sondern enthält darüber hinaus ein von der Rechtsprechung aufgestelltes allgemeines Beschränkungsverbot.[1002] Die staatlichen Maßnahmen, die grundsätzlich nicht diskriminierend sind, beeinträchtigen den Service-Provider in seiner Niederlassungsfreiheit, da er dem Content-Provider nicht mehr ungehindert Speicherplatz für dessen Inhalte zur Verfügung stellen kann.

(b) Rechtfertigung

Diese Beeinträchtigung der Niederlassungsfreiheit des Service-Providers könnte jedoch gerechtfertigt sein.

(aa)Zwingende Gründe des Allgemeininteresses

Als Rechtfertigungsgrund kommt zunächst der vom EuGH für alle Grundfreiheiten – somit auch für die Niederlassungsfreiheit[1003] – aufgestellte Rechtfertigungsstandard der zwingenden Gründe des Allgemeininteresses in Betracht.[1004] Demnach sind die Verstöße gegen die Niederlassungsfreiheit dann gerechtfertigt, wenn sie einem gemeinschaftsrechtlich anerkennenswerten Belang dienen, nichtdiskriminierend und zur Erreichung des verfolgten Zwecks geeignet sowie erforderlich sind.[1005]
Das Ziel, Web-Seiten sperren oder löschen zu lassen, weil sie aufgrund ihres politisch radikalen, rassistischen oder pornographischen Inhalts als rechtswidrig anzusehen sind, kann jedoch unter keinen vom EuGH festgelegten gemeinschaftsrechtlich anerkennenswerten Belang subsumiert werden.[1006] Folglich darf hierfür eine Rechtfertigung aus zwingenden Gründen des Allgemeininteresses nicht angenommen werden.

(bb)Art. 45, 46 EGV

Es könnten allerdings die Ausnahmetatbestände der Art. 45, 46 EGV zur Anwendung kommen.
Art. 45 EGV greift nicht ein, da die Tätigkeit des Service-Providers in der Regel nicht mit der Ausübung öffentlicher Gewalt verbunden ist.

1001 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (1).
1002 Herdegen, Europarecht, 2. Auflage, § 15 Rdnr. 282.
1003 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4179 f. Rdnr. 37 (Gebhard).
1004 Vgl. hierzu auch Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 26.
1005 Herdegen, Europarecht, 2. Auflage, § 15 Rdnr. 283.
1006 Siehe hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). Und bb. (2). (a).

Da aber Art. 46 EGV nach der hier vertretenen Ansicht sowohl für diskriminierende als auch für unterschiedslose Maßnahmen gelten soll,[1007] kann sich eine Zulässigkeit der Beeinträchtigung der Niederlassungsfreiheit nach Art. 46 I EGV ergeben: Die behördlichen Sperr- und/oder Löschanordnungen ergehen aus Gründen der öffentlichen Sicherheit und Ordnung. Gleichzeitig sind sie auch verhältnismäßig: Sie sind aus technischer Sicht geeignet, das verfolgte Ziel zu erreichen, die oben beschriebenen Inhalte aus dem Internet zu verbannen. Zudem stellen die Sperr- und/oder Löschverfügungen erforderliche Maßnahmen dar, da weniger einschneidende Maßnahmen nicht ersichtlich sind. Die Interessen des Service-Providers, dem Content-Provider unbeschränkt Speicherplatz bereit zu stellen, werden darüber hinaus nur sehr gering betroffen. Denn er kann gezielt den unerwünschten Inhalt sperren bzw. löschen, während er alle übrigen Inhalte (auch die von anderen Content-Providern) weiterhin den Nutzern im Netz bereitstellen darf. Demgegenüber besitzt der Staat ein berechtigtes Interesse, den Schutz der (jugendlichen) Nutzern vor derartigen illegalen Inhalten zu gewährleisten und sich selbst vor staatsfeindlichen, rechtswidrigen Web-Seiten zu schützen. Diese gravierenden Interessen des Staates überwiegen somit offensichtlich das wirtschaftliche Interesse des Service-Providers.

(c) Ergebnis

Die staatlichen Sperr- und Löschanordnungen greifen zwar in die Niederlassungsfreiheit des Service-Providers ein, sie sind jedoch wegen der Anwendbarkeit des Art. 46 I EGV gerechtfertigt.

(2) Dienstleistungsfreiheit

Aus der Perspektive des Service-Providers wird nur bei einer Konstellation der Fallvariante III die Dienstleistungsfreiheit durch staatliche Kontrollmaßnahmen tangiert, und zwar dann, wenn der Service-Provider aus dem EU-Ausland stammt und auch seinen Sitz im EU-Ausland hat. Allerdings befindet sich die Hard- und Software, die für das Service-Providing notwendig ist, im Inland. Der Content-Provider und der Nutzer sind dagegen Deutsche.

(a) Inländergleichbehandlung

Wie bereits bei der Prüfung des Content-Providers festgestellt wurde,[1008] enthält die Dienstleistungsfreiheit der Art. 49 ff. EGV nicht nur das in der Generalnorm des Art. 12 EGV enthaltene allgemeine Diskriminierungsverbot, sondern geht über die Inländergleichbehandlung hinaus und stellt mittlerweile ein durch den EuGH anerkanntes all-

[1007] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).
[1008] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (1).

gemeines Beschränkungsverbot dar.[1009] Die staatlichen Sperr- und/oder Löschanordnungen beeinträchtigen den Service-Provider, seine Leistungen gegenüber dem Content-Provider zu erbringen. Demnach sind die behördlichen Eingriffe nur dann europarechtlich zulässig, sofern sie gerechtfertigt sind.

(b) Rechtfertigung

(aa)Zwingende Erfordernisse des Allgemeinwohls

Die Beschränkungen der Dienstleistungsfreiheit können wiederum nach den bereits bekannten zwingenden Erfordernissen des Allgemeinwohls gerechtfertigt sein. Hierfür müssen sie einem gemeinschaftskonformen Allgemeinbelang dienen, diskriminierungsfrei vorgenommen werden und verhältnismäßig, also geeignet und erforderlich sein.[1010] Rechtswidrige Inhalte im Internet für die Nutzer unzugänglich zu machen und somit aus dem Internet zu verbannen, stellt nach der bisherigen Rechtsprechung des EuGH keinen berechtigten Allgemeinbelang dar.[1011] Folglich ergibt sich keine Rechtfertigung für die staatlichen Kontrollmaßnahmen aus der Schrankensystematik des EuGH.

(bb)Art. 55 i.V.m. Art. 45, 46 EGV

Über Art. 55 EGV kommen die Ausnahmetatbestände der Art. 45 und 46 EGV auch bei der Dienstleistungsfreiheit zur Anwendung.
Die Tätigkeit des Service-Providers ist – wie von Art. 45 EGV verlangt wird – grundsätzlich nicht mit der Ausübung öffentlicher Gewalt verbunden. Er ist somit nicht einschlägig.
Zwar existieren bezüglich der Kontrollmaßnahmen im Internet gemäß Art. 46 I EGV keine Sonderregelungen für Ausländer, so dass Art. 46 EGV hinsichtlich seines Wortlauts eigentlich nicht erfüllt ist. Dieser Teilsatz muss aber so gelesen werden, dass Art. 46 EGV erst recht auch für unterschiedslose staatliche Maßnahmen gilt.[1012] Die Sperr- und/oder Löschanordnungen ergehen aufgrund von nichtdiskriminierenden Vorschriften des Polizei- und Sicherheitsrechts sowie des Medienrechts. Sie können deshalb unter die in Art. 46 I EGV genannten Begriffe der Ordnung und Sicherheit subsumiert wer-

---

[1009] Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 59 Rdnr. 37; Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 53 f.

[1010] Herdegen, Europarecht, 2. Auflage, § 18 Rdnr. 325.

[1011] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a). Der EuGH hat bisher nur bestimmte Gründe als zwingende Gründe des Allgemeinwohls angesehen. Dabei sind diese vom EuGH in diversen Entscheidungen aufgeführten zwingende Gründe nicht abschließend. Es können somit jederzeit weitere hinzutreten. Vgl. insoweit bei Holoubek in: Schwarze (Hrsg.), EU-Kommentar, Art. 49 Rdnr. 100 ff.

[1012] Hailbronner in: Hailbronner/Klein/Magiera/Müller-Graff, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Art. 56 Rdnr. 3; vgl. auch oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).

den.[1013] Die Sperr- bzw. Löschmaßnahmen müssen zudem – wie vorstehend bei der Niederlassungsfreiheit – als geeignet und erforderlich, mithin als verhältnismäßig angesehen werden. Denn nur durch diese Maßnahmen kann von staatlicher Seite auf den gefährlichen Inhalt im Internet eingewirkt werden. Hinter den Interessen des Staates, sich selbst zu schützen sowie den Jugendschutz und den Schutz der Menschenwürde zu gewährleisten, müssen die wirtschaftlichen Interessen des Service-Providers zurücktreten. Demnach sind die Kontrollmaßnahmen auch verhältnismäßig. Die in Art. 46 I EGV für die Zulässigkeit von Beschränkungen der Dienstleistungsfreiheit aufgestellten Kriterien sind folglich erfüllt.

(c) Ergebnis

Zwar wird aus der Sicht des Service-Providers durch die staatlichen Sperr- und/oder Löschmaßnahmen in dessen Dienstleistungsfreiheit eingegriffen. Jedoch geschieht dies wegen Art. 46 I EGV i.V.m. Art. 55 EGV in rechtmäßiger Art und Weise, so dass gegen Europarecht insoweit nicht verstoßen wird.

(3) Zwischenergebnis

Bei sämtlichen vorgenannten Fallvarianten und –konstellationen, in denen die Grundfreiheiten des Service-Providers durch die behördlichen Kontrollmaßnahmen tangiert werden, ist das Europarecht nicht verletzt, da die Grundfreiheiten zulässigerweise beeinträchtigt werden.

bb. Sicht des Content-Providers

(1) Warenverkehrsfreiheit

Aus der Sicht des Content-Providers kann in die Warenverkehrsfreiheit durch die staatlichen Kontrollmaßnahmen für jede Fallkonstellation der Fallvariante I mittelbar eingegriffen werden, wenn der zu sperrende bzw. zu löschende Inhalt Warenangebote oder eine bestimmte Werbung hierfür enthält.
Der Content-Provider ist dabei entweder eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland oder eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland, wobei sich lediglich der gespeicherte Inhalt im Inland (auf dem Rechner des Service-Providers) befindet. Schließlich besteht auch die Möglichkeit, dass es sich beim Content-Provider um eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland handelt und darüber hinaus neben dem reinen Inhalt noch weitere, mit dem Content-Providing im Zusammenhang stehende Komponenten im Inland lokalisiert sind. In allen aufgezeigten Fallkonstellationen stammen der Service-Provider und der Nutzer aus dem Inland.

[1013] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4). und bb. (2). (b).

(a) Dassonville-Formel

Da die gegen die im Internet angebotenen Waren bzw. Werbungen gerichteten behördlichen Kontrollmaßnahmen geeignet sind, den innergemeinschaftlichen Handel zumindest mittelbar und potentiell zu behindern,[1014] stellen sie Maßnahmen gleicher Wirkung gemäß der Dassonville-Formel dar.[1015] Der Art. 28 EGV ist demnach grundsätzlich erfüllt.

(b) Keck-Formel

Die Keck-Formel, die eine Einschränkung der Dassonville-Formel enthält, ist – wie bereits oben ausführlich geklärt[1016] – hier nicht einschlägig, da die Sperr- bzw. Löschanordnungen nicht nur als Verkaufsmodalitäten eingreifen. Vielmehr handelt es sich bei ihnen letztlich um produktbezogene Maßnahmen, die nicht von der Keck-Formel erfasst werden.[1017] Deshalb bleibt die Dassonville-Formel und somit der Art. 28 EGV weiterhin anwendbar.

(c) Cassis-de-Dijon-Rechtsprechung

Etwas anderes ergibt sich auch nicht aus der Cassis-Formel, der tatbestandsimmanenten Schranke des Art. 28 EGV.[1018] Denn die verfolgten Ziele der nationalen Maßnahmen, die Jugend, den Bürger, den Staat und die Menschenwürde zu schützen, können nicht unter die vom EuGH aufgestellten Fallgruppen subsumiert werden.[1019]

(d) Rechtfertigung nach Art. 30 EGV

Allerdings könnten die von Art. 28 EGV grundsätzlich verbotenen Beeinträchtigungen der Warenverkehrsfreiheit durch Art. 30 EGV gerechtfertigt werden.
Art. 30 EGV nennt unter anderem als Rechtfertigungsgründe die öffentliche Sittlichkeit, Ordnung und Sicherheit. Pornographische, rassistische, politisch radikale und gewaltverherrlichende Inhalte bedrohen die öffentliche Sittlichkeit, Ordnung und Sicherheit. Folglich sind diese Rechtfertigungsgründe gegeben. Des weiteren verlangt aber Art. 30 EGV, dass die Beschränkungen verhältnismäßig erfolgen müssen, d.h. dass die angewandten Mittel auch tatsächlich für den verfolgten Zweck geeignet sind und der Zweck nicht auch in einer weniger einschneidenden Weise erreicht werden kann.[1020]
Wie bereits an vorangegangener Stelle erörtert,[1021] sind die Sperr- bzw. Löschverfügungen durchaus geeignet, gezielt die rechtswidrigen Inhalte sowie Inhalte, die mit rechts-

---

1014 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 95.
1015 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (1).
1016 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2).
1017 Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1511 ff.
1018 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).
1019 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).
1020 Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 99.
1021 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

widrigen Waren in Verbindung stehen, unschädlich zu machen. Durch die Kontrollmaßnahmen wird also verhindert, dass der jeweilige Nutzer auf die Angebote von illegalen Waren zugreifen kann. Auch die Werbung für derartige Produkte kann den Nutzer nicht mehr erreichen. Demnach besteht die Möglichkeit, sowohl die demokratische Gemeinschaft als auch jeden einzelnen Nutzer vor menschenverachtenden, pornografischen oder politisch extremen Waren und ihrer Werbung im Internet zu schützen. An einen solchen Schutz hat der Staat offenkundig ein erhebliches Interesse. Demgegenüber wiegen die Interessen des Content-Providers weniger schwer. Er wird eigentlich nur in seinem wirtschaftlichen Recht, Waren in Europa frei anbieten oder dafür werben zu können, beeinträchtigt. Darüber hinaus ist zu bedenken, dass die Technik des Internets der zuständigen staatlichen Behörde nur einen begrenzten Handlungsspielraum gewährt: Entweder Sperrung und/oder Löschung der Inhalte. Da die Sperrung vom Anbieter bzw. Nutzer sehr leicht umgangen werden kann, bleibt häufig nur die Löschung als einziges wirksames Mittel gegen die rechtswidrigen Inhalte. Weniger einschneidende Maßnahmen stehen somit der staatlichen Behörde nicht zur Verfügung. Weil der Service-Provider aber nur die indizierten Inhalte des Content-Providers sperrt bzw. löscht und der übrige Inhalt weiter frei im Internet bereitgehalten wird, müssen die staatlichen Maßnahmen als verhältnismäßig angesehen werden. Denn der Inhalt des Content-Providers wird lediglich teilweise durch die Sperr- bzw. Löschverfügungen tangiert. Die staatlichen Interessen, seine Bürger und die Wertegemeinschaft vor rechtswidrigen Inhalten im Internet zu schützen, überwiegen folglich die Interessen des Content-Providers.

(e) Ergebnis

Der Content-Provider wird zwar grundsätzlich von den staatlichen Kontrollmaßnahmen bei den genannten Fallkonstellationen in seiner Warenverkehrsfreiheit nach Art. 28 EGV verletzt. Dieser staatliche Eingriff ist jedoch gemäß Art. 30 EGV zulässig, da Rechtfertigungsgründe gegeben sind.

(2) Niederlassungsfreiheit

Die Niederlassungsfreiheit ist aus der Perspektive des Content-Providers bei der Fallvariante I in zwei Fallkonstellationen betroffen. Zum einen, wenn der Content-Provider eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland ist. Zum anderen dann, wenn es sich beim Content-Provider um eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland handelt, wobei sich allerdings der Inhalt und weitere – im Zusammenhang mit dem Content-Providing stehende – Komponenten im Inland befinden. In beiden Fällen stammen der Service-Provider und der Nutzer aus dem Inland.

(a) Inländergleichbehandlung

Wie bereits an mehreren Stellen angemerkt wurde,[1022] ist die in Art. 43 EGV verbürgte Niederlassungsfreiheit über ein Diskriminierungsverbot hinaus zu einem Beschränkungsverbot ausgeweitet worden.[1023] Unzulässig können deshalb auch unterschiedslose nationale Regelungen sein, welche die Ausübung der Niederlassungsfreiheit behindern oder weniger attraktiv machen. Dies ist hier der Fall, da die staatlichen Kontrollmaßnahmen den niedergelassenen Content-Provider darin beschränken, seine unterschiedlichen Angebote im Internet den Nutzern zugänglich zu machen. Die Ausübung der selbständigen Erwerbstätigkeit des Content-Providers, die von Art. 43 II EGV ausdrücklich geschützt wird, ist somit hiervon betroffen.

(b) Rechtfertigung

Dieser staatliche Eingriff in die Niederlassungsfreiheit kann jedoch gerechtfertigt sein.

(aa)Zwingende Gründe des Allgemeinwohls

Zwar greifen die vom EuGH[1024] für eine Rechtfertigung aus Gründen des Allgemeinwohls aufgestellten Kriterien ebenfalls nicht ein. Denn der Jugendschutz, der Schutz des Staates und der Menschenwürde können unter keine der vom EuGH in seiner Rechtsprechung genannten Fallgruppen zu den zwingenden Gründen des Allgemeininteresses[1025] subsumiert werden.

(bb)Art. 45, 46 EGV

Demnach sind wieder die Ausnahmetatbestände der Art 45 und 46 EGV zu betrachten: Art. 45 EGV scheidet als die Niederlassungsfreiheit einschränkende Norm aus, weil die Tätigkeit des Content-Providers regelmäßig nicht mit der Ausübung öffentlicher Gewalt verbunden ist.

Da aber Art. 46 I EGV sowohl für diskriminierende als auch für unterschiedslose Maßnahmen angewendet werden darf,[1026] ergibt sich hieraus wiederum eine Rechtfertigung der Lösch- bzw. Sperranordnungen: Die Kontrollmaßnahmen ergehen aus Gründen der öffentlichen Ordnung und Sicherheit.[1027] Zudem sind sie als verhältnismäßig anzusehen. Der Staat hat ein großes Interesse daran, den unbeschränkten Zugang von (jugendlichen) Nutzern zu rassistischen, menschenverachtenden oder pornographischen Internet-Seiten zu verhindern.[1028] Es geht auch darum, die staatliche demokratische Grundord-

---

1022 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (1).

1023 Fastenrath/Müller-Gerbes, Europarecht, S. 74 Rdnr. 123; vgl. auch EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4179 f. Rdnr. 37 (Gebhard).

1024 EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165, 4179 Rdnr. 37 (Gebhard)

1025 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a).

1026 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).

1027 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4). und bb. (2). (b).

1028 Holznagel, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdender Inhalte“, ZUM 2000, 1007, 1023.

nung und die Menschenwürde zu schützen. Die staatlichen Kontrollmaßnahmen sind geeignet, diesen Schutz zumindest teilweise zu gewährleisten und dafür sind die Sperr- und Löschanordnungen – insbesondere aus technischer Sicht – auch erforderlich.[1029] Hinter diesen gravierenden staatlichen Interessen hat das Interesse des Content-Providers, seine Inhalte im Internet ungehindert anzubieten, zurückzutreten.

(cc) Ergebnis

Der Content-Provider ist zwar in seiner in Art. 43 ff. EGV fixierten Niederlassungsfreiheit durch die staatlichen Maßnahmen betroffen. Dieser Eingriff ist aber aus Gründen der öffentlichen Ordnung und Sicherheit gemäß Art. 46 I EGV gerechtfertigt. Europarecht ist demnach nicht verletzt.

(3) Dienstleistungsfreiheit

Die Dienstleistungsfreiheit wird aus der Sicht des Content-Providers in der Fallvariante I und II tangiert. Dies ist bei der Fallvariante I dann gegeben, wenn der Content-Provider eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist und sich nur sein Inhalt beim Rechner des Service-Providers im Inland befindet; der Service-Provider und auch der Nutzer stammen zudem aus dem Inland. In Fallvariante II handelt es sich um die Fallkonstellation, dass der Content-Provider und Service-Provider Deutsche sind, der Nutzer hingegen eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist.

(a) Inländergleichbehandlung

Obwohl der Art. 50 III EGV lediglich die Inländergleichbehandlung vorschreibt, beinhalten die Art. 49 ff. EGV mittlerweile ein allgemeines Beschränkungsverbot.[1030] Demzufolge sind staatliche Beschränkungen der Dienstleistungsfreiheit grundsätzlich verboten. Durch die behördlichen Kontrollmaßnahmen wird der Content-Provider in der Ausübung seiner im Internet angebotenen Dienste behindert. Es liegt somit grundsätzlich ein unzulässiger Verstoß gegen die Dienstleistungsfreiheit vor.

(b) Rechtfertigung

Dieser Verstoß kann jedoch wiederum gerechtfertigt sein:

(aa) Zwingende Erfordernisse des Allgemeinwohls

Neben den im EGV enthaltenen Ausnahmetatbeständen können die Mitgliedstaaten die Dienstleistungsfreiheit – wie bereits ausführlich an obiger Stelle dargestellt[1031] – auch

---

[1029] Fastenrath/Müller-Gerbes, Europarecht, S. 74 Rdnr. 123.

[1030] Geiger, EUV/EGV, 3. Auflage, Art. 50 Rdnr. 11; EuGH, Rs. C-398/95, 05.06.1997, Slg. 1997, 3091, 3119 Rdnr. 19 (Ergasias); vgl. auch oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (1).

[1031] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (3). (b).

aufgrund zwingender Gründe des Allgemeininteresses rechtmäßig beschränken.[1032] Nach der EuGH-Rechtsprechung fallen unter den Begriff der schützenswerten Allgemeininteressen – in Anlehnung an die Cassis-de-Dijon-Rechtsprechung – der Verbraucher- und Gläubigerschutz, die Lauterkeit des Handelsverkehrs, der Schutz des geistigen Eigentums, kulturpolitische Belange, die wirksame steuerliche Kontrolle und das Funktionieren der Rechtspflege.[1033] Die mit den staatlichen Kontrollmaßnahmen verfolgten Ziele lassen sich unter keine der genannten Fallgruppen subsumieren. Demnach können die Sperr- bzw. Löschanordnungen nicht aus zwingenden Gründen des Allgemeinwohls gerechtfertigt werden.

(bb)Art. 55 EGV i.V.m. Art. 45 und 46 EGV

Da die Ausnahmevorschriften der Art. 45 und 46 EGV über Art. 55 EGV zur Anwendung kommen, könnte sich hieraus erneut ein Rechtfertigungsgrund ergeben.
Art. 45 EGV scheidet als eine die Dienstleistungsfreiheit einschränkende Norm aus, da der Content-Provider grundsätzlich nicht in Ausübung öffentlicher Gewalt tätig wird.
Art. 46 I EGV, der entgegen seines Wortlauts auch für unterschiedslose Maßnahmen gilt,[1034] verlangt, dass in die Dienstleistungsfreiheit aus Gründen der öffentlichen Ordnung, Sicherheit und Gesundheit eingegriffen wird. Wie schon bei der Prüfung der Niederlassungsfreiheit aufgezeigt wurde, lassen sich die Ziele der staatlichen Behörden, welche die Sperr- und/oder Löschanordnungen verfügen, unter die europarechtlichen Begriffe der öffentlichen Ordnung und Sicherheit subsumieren.[1035] Des weiteren müssen die staatlichen Maßnahmen als ungeschriebenes Tatbestandsmerkmal des Art. 46 I EGV den Grundsatz der Verhältnismäßigkeit erfüllen.[1036] Der Staat hat ein großes Interesse daran, den unbeschränkten Zugang von (jugendlichen) Nutzern zu rassistischen, menschenverachtenden oder pornographischen Internet-Seiten zu verhindern. Zudem will er sich selbst gegen Inhalte, welche die demokratische Grundordnung gefährden, schützen. Um diese Ziele zu erreichen, ist es angemessen und schon allein aus technischer Sicht erforderlich, den Service-Provider aufzufordern, den ungewünschten Inhalt zu sperren und/oder zu löschen. Diese Maßnahmen sind auch geeignet, den Zugang für die Nutzer zu verhindern. Denn der Service-Provider kann gezielt auf die für den Content-Provider im Internet eingestellten Inhalte Einfluss nehmen.[1037] Er ist in der Lage, ausschließlich den illegalen Inhalt zu sperren bzw. zu löschen. Dass der Content-Provider hierdurch in

---

[1032] Koenig/Haratsch, Europarecht, 2. Auflage, S. 240 f. Rdnr. 512; EuGH, Rs. 33/74, 03.12.1974, Slg. 1974, 1299, 1309 Rdnr. 10/12 (Van Binsbergen); EuGH, verbundene Rs. 110/78 und 111/78, 18.01.1979, Slg. 1979, 35, 52 f. Rdnr. 27 ff. (Van Wesemael); EuGH, Rs. 279/80, 17.12.1981, Slg. 1981, 3305, 3325 Rdnr. 19 (Webb).

[1033] Koenig/Haratsch, Europarecht, 2. Auflage, S. 240 f. Rdnr. 512.

[1034] Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).

[1035] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 2. g. bb. (2). (b). (bb).

[1036] Dies ergibt sich aus einem Vergleich mit Art. 30 EGV, in dem der Grundsatz der Verhältnismäßigkeit explizit geregelt ist.

[1037] Vgl. hierzu die Ausführungen weiter oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (3). (c).

der Ausübung seiner Dienstleistung gegenüber dem Nutzer beeinträchtigt wird, ist ihm angesichts der bedeutenden individuellen und öffentlichen Interessen in verhältnismäßiger Weise zuzumuten.

(c) Ergebnis

In die Dienstleistungsfreiheit des Content-Providers greifen die staatlichen Kontrollmaßnahmen zwar ein. Jedoch geschieht dies wegen Art. 46 I EGV, der hier erfüllt ist und über Art. 55 EGV angewendet werden kann, in zulässiger Art und Weise, so dass Europarecht insoweit nicht betroffen ist.

(4) Zwischenergebnis

Obwohl die Kontrollmaßnahmen in den einzelnen Fällen Grundfreiheiten des EGV verletzen, liegt kein Verstoß gegen das Europarecht vor, weil die Beschränkungen über die „ordre-public"-Regelungen gerechtfertigt sind.

3. Kontrollmaßnahmen gegen den Access-Provider

a. Grundkonstellation

Wie bereits weiter oben erklärt, hält der Access-Provider – im Gegensatz zum Content- und Service-Provider – keine Inhalte bereit, sondern vermittelt lediglich ihren Zugang.[1038] Der Access-Provider bietet demnach dem Nutzer einen Zugang zum Internet an, indem er die technischen Mittel bereithält, um mit anderen Internet-Nutzern in Kontakt zu treten.[1039] Der Nutzer wählt sich also mit Hilfe des Access-Providers in das Internet ein. Weiterhin sorgt der Access-Provider dafür, dass der Nutzer zu den jeweils gewünschten Adressen im Internet gelangt. Er vermittelt ihm den Zugang zu den einzelnen Content- bzw. Service-Providern. In der Regel läuft die Grundkonstellation deshalb wie folgt ab:
Der Nutzer begibt sich mit Hilfe des Access-Providers ins Internet. Der Access-Provider ermöglicht darüber hinaus, dass der Nutzer über das Netz zu den gewünschten Internet-Adressen, also zu den Inhalten der Content-Provider, gelangt. Wenn nun der Nutzer durch den Access-Provider Zugang zum Inhalt eines Content-Providers erlangt hat, werden die gewünschten Daten dann vom Content-Provider zum Nutzer über den Access-Provider zurückvermittelt. Der Access-Provider stellt somit im Grunde den Datenaustausch zwischen dem Nutzer und dem Content-Provider her. Insgesamt sind in der

---

[1038] Beucher/Leyendecker/von Rosenberg, Mediengesetze, § 3 MDStV Rdnr. 5.
[1039] Mayer, Das Internet im öffentlichen Recht, S. 50.

einfachsten Konstellation an dem Vorgang drei Personen beteiligt: der Nutzer, der Access-Provider und der Content-Provider.[1040]
Die einzigen staatlichen Kontrollmaßnahmen, die gegen den Access-Provider angeordnet werden können, sind darauf gerichtet, dass der Access-Provider den Zugang zu den Inhalten des Content-Providers für den Nutzer sperrt. Mangels einer Herrschaftsgewalt über den Inhalt des Content-Providers kann gegen den Access-Provider keine Löschanordnung ergehen.[1041] Die gegen ihn gerichteten Verfügungen sind somit ausschließlich Sperranordnungen.
Wie bereits in den vorangegangenen Fallvarianten soll bei den einzelnen Fallgruppen nur die Perspektive der beteiligten Provider betrachtet werden. Die Sichtweise des Nutzers wird – aus den genannten Gründen[1042] – wieder außer acht gelassen.

- **Vorüberlegungen zum Prüfungsablauf:**

Natürlich könnte erneut eine Prüfung – wie beim Content- und Service-Provider – nach den einzelnen beteiligten Personen durchgeführt werden. Diese Prüfung würde jedoch der Realität nicht gerecht werden. Denn gegen den Access-Provider nur eine Sperr- und keine Löschanordnung ergehen. Die Sperrung von unerwünschten Inhalten im Internet ist aber häufig nicht das geeignete und wirksame Mittel, um gegen diese Inhalte von staatlicher Seite aus vorgehen zu können. So ist zum einen die gezielte Sperrung von rechtswidrigen Inhalten durch den Access-Provider technisch sehr aufwändig und nicht immer möglich.[1043] Zum anderen wird die zuständige Behörde eine Sperranordnung gegen einen deutschen Access-Provider nicht erlassen, wenn der Inhalt von einem deutschen Content-Provider in das Internet eingestellt worden ist. Vielmehr ist dann der Content-Provider als Störer[1044] der richtige Adressat.[1045] Er hat die entsprechende Herr-

---

1040 Natürlich kann der Inhalt des Content-Providers auch durch einen Service-Provider im Internet bereitgehalten werden. Hierauf soll jedoch in dieser Fallbearbeitung nicht eingegangen werden, da diese zusätzliche Variable des Service-Providings eine ordentliche Prüfung zu sehr verkomplizieren würde. Auf den Service-Provider kann an dieser Stelle auch deswegen verzichtet werden, weil er bereits vorstehend ausführlich behandelt wurde. Für das Verständnis ist es aber wichtig, hier die Möglichkeit aufzuzeigen, dass der Inhalt der Content-Provider nicht nur durch sie selbst, sondern ebenfalls durch Service-Provider in das Internet eingestellt werden kann.

1041 Vgl. hierzu die obigen Ausführungen zu den technischen Möglichkeiten einer Kontrolle des Internets durch die jeweiligen Provider unter B. 1. Teil. III. 1. d. und 2. b.

1042 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. IV. 4.

1043 Siehe oben unter B. 1. Teil. III. 1. c. cc. (1).

1044 Fraglich ist dabei, ob er als Handlungs- oder Zustandsstörer angesehen werden muss. Grundsätzlich sind Maßnahmen, die durch das polizeiwidrige Verhalten von Personen oder den polizeiwidrigen Zustand von Sachen erforderlich werden, gegen diejenigen zu richten, die für das polizeimäßige Verhalten oder den polizeimäßigen Zustand verantwortlich sind. Die Eigenschaft als Störer wird also allein durch ein objektiv störendes Verhalten bzw. durch einen objektiv störenden Zustand begründet, Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, Art. 7 Rdnr. 1 ff. Wenn der Content-Provider rechtswidrige Inhalte in das Internet einstellt und für die Nutzer bereithält, kann er sowohl als Zustands- als auch als Handlungsstörer angesehen werden. Denn zunächst stört er durch sein Verhalten, indem er den rechtswidrigen Inhalt in das Internet einspeist. Das Bereithalten des rechtswidrigen Inhalts selbst stellt im Anschluss daran einen störenden Zustand dar, für den der Content-Provider ebenfalls verantwortlich ist.

schaftsgewalt über seinen Inhalt, so dass er ihn viel besser sperren und löschen kann als der Access-Provider. Eine Sperr- und/oder Löschanordnung gegen den Content-Provider ist somit viel effektiver als die gegen den Access-Provider. Aus diesem Grund wird die Polizei- und Sicherheitsbehörde gegen ihn und nicht gegen den Access-Provider vorgehen.

Die Fallvarianten, bei denen sich der Inhalt des Content-Providers im Inland befindet, wurden vorstehend schon ausführlich besprochen. Dort ist bereits die Situation angenommen worden, dass der behördliche Sperr- und/oder Lösch-VA gegen den Content-Provider (oder – falls vorhanden – Service-Provider) und nicht gegen den Access-Provider ergehen wird. Zu prüfen sind jetzt also nur noch die Fälle, wo der Inhalt nicht im Inland, sondern im EU-Ausland gespeichert ist. Dann muss die Sperr-Anordnung – mangels eines inländischen Störers – gegen den Access-Provider gerichtet werden. Folglich sind die Fallvarianten immer so zu bilden, dass sich der Content-Provider im EU-Ausland befindet.[1046] Beim Content-Provider handelt es sich somit immer um eine natürliche oder juristische Person, die ihren Wohn- bzw. Geschäftssitz ebenfalls im EU-Ausland hat. Andernfalls könnten die behördlichen Anordnungen statt an den Access-Provider an den Content-Provider gerichtet werden. Dies wird bei den nachfolgenden Fallvarianten berücksichtigt. An der Person des Content-Providers werden deshalb keine Veränderungen vorgenommen. Er ist jedes Mal eine natürliche oder juristische Person aus dem EU-Ausland, die ihren Wohn- bzw. Firmensitz im EU-Ausland hat.

Benutzt der Content-Provider für die Speicherung des illegalen Inhalts einen Service-Provider, dann bestehen schon zwei Störer. Der Service-Provider, der für den Content-Provider die Internet-Angebote bereithält, kann anfangs wiederum als Handlungs- und später als Zustandsstörer angesehen werden.

Die Auswahl, gegen wenn die staatliche Maßnahme bei mehreren Verantwortlichen zu richten ist, erfolgt nach den Grundsätzen der Verhältnismäßigkeit. Im Gesetz ist sie nicht geregelt. Von den Polizei- und Sicherheitsbehörden muss insbesondere die tatsächliche und rechtliche Möglichkeit, die Gefahr zu beseitigen, die zeitliche und örtliche Nähe zum Schaden, die persönliche und sachliche Leistungsfähigkeit und Eignung sowie der größere oder geringere Grad von Belästigungen, die dem Heranzuziehenden erwachsen, berücksichtigt werden. Vgl. Knemeyer, Polizei- und Ordnungsrecht, 8. Auflage, § 27 Rdnr. 337 f.

[1045] Ob der Access-Provider überhaupt als Störer in Betracht kommt oder ob er nur als Nichtstörer in Anspruch genommen werden kann, ist nicht einfach zu beantworten, vgl. nur Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 442. Allerdings wird man wohl den Access-Provider eher als Nichtstörer ansehen. Deshalb muss die Polizei- und Sicherheitsbehörde zunächst – soweit möglich – den eigentlichen Störer in Anspruch nehmen, bevor auf den Access-Provider als Nichtstörer zurückgegriffen werden kann, Knemeyer, Polizei- und Sicherheitsrecht, 8. Auflage, § 30 Rdnr. 347. So auch Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3149.

[1046] Der Inhalt des Content-Providers könnte natürlich wiederum von einem Service-Provider gespeichert und im Internet bereitgestellt werden. In diesem Fall müsste der Service-Provider gleichermaßen im Ausland sein. Ansonsten würden die Behörden aus Effizienzgründen nicht gegen den Access-Provider sondern gegen den Service-Provider vorgehen. Auf die Möglichkeit, dass neben dem Content-Provider auch noch ein Service-Provider im EU-Ausland existieren kann, wird in folgender Prüfung nicht eingegangen. Dies würde die Darstellung nur unnötig verkomplizieren. Zumal der Service-Provider, auch der im EU-Ausland befindliche, in den vorstehenden Fallvarianten ausführlich behandelt worden ist.

b. Fallvariante I: Deutscher Access-Provider, Deutscher Nutzer, Content-Provider aus dem EU-Ausland

In dieser Fallkonstellation wählt sich somit ein deutscher Nutzer über einen deutschen Access-Provider in das Internet ein. Anschließend erhält er durch den Access-Provider Zugang zu den gewünschten Inhalten des Content-Providers aus dem EU-Ausland. Dieser Content-Provider benutzt wieder den Access-Provider, um die vom Nutzer angeforderten Daten auf dessen Rechner zu übermitteln. Der Access-Provider hat demnach eine Doppelfunktion, er dient nicht nur dem Nutzer, sondern handelt auch für den Content-Provider, damit dessen Inhalte zum Nutzer übertragen werden können.[1047] Diese Besonderheit ist bei den nachfolgenden Prüfungen zu beachten.
Da in diesen Fallkonstellationen zwei Personen durch die Kontrollmaßnahmen in ihren Grundfreiheiten beeinträchtigt werden können, ist – wie oben beim Service-Provider[1048] – ebenso zwischen der Person des Access-Providers und der des Content-Providers zu differenzieren:

aa. Sicht des Access-Providers

- Dienstleistungsfreiheit

Wie bereits eben angesprochen wurde, erbringt der Access-Provider regelmäßig Dienste gegenüber dem Nutzer und dem Content-Provider. Fraglich ist aber, ob er damit den gemeinschaftsrechtlichen Begriff der Dienstleistung i.S.d. Art. 49 ff EGV erfüllt.
Hinsichtlich der Leistung gegenüber dem Nutzer ist dies zu bejahen, da der Access-Provider (meist) für den Nutzer entgeltliche Dienste[1049] erbringt. Probleme bereitet jedoch die rechtliche Einordnung des Datentransports zwischen dem Content-Provider und dem Access-Provider, der vom Access-Provider durchgeführt wird. So fehlt es eigentlich bei der Leistungsbeziehung Access-Provider/Content-Provider schon an der von Art. 50 I EGV geforderten Entgeltlichkeit. Obwohl der Access-Provider beim Datentransport vom Content-Provider zum Nutzer auch gegenüber dem Content-Provider eine Leistung erbringt, wenn er dessen Daten zum Nutzer schickt, erhält er vom Content-Provider keine Gegenleistung. Vielmehr lässt sich der Access-Provider seine Dienste üblicherweise vom Nutzer vergüten. Dennoch scheint es nicht richtig zu sein, nur bei der Leistungsbeziehung Access-Provider/Nutzer eine Entgeltlichkeit und somit eine Dienstleistung i.S.d. Art. 50 EGV zu bejahen, nicht dagegen bei der Leistungsbeziehung Access-Provider/Content-Provider. Dies wäre nicht konsequent, da der Access-Provider gleichermaßen auch für den Content-Provider tätig wird und ihm gegenüber eine Leistung erbringt. Es stellt sich somit die Frage, wie das Kriterium der Entgeltlich-

---

1047 Mayer, Das Internet im öffentlichen Recht, S. 50 f.
1048 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 2. b. aa.
1049 Zu denken ist hier vor allem an die Zugangsvermittlung zum Internet. Vgl. Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444.

keit auch bei der Leistungsbeziehung Access-Provider/Content-Provider erfüllt werden kann. Zwei Alternativen bieten sich hierfür an:
Zum einen könnte die Ansicht vertreten werden, dass der Content-Provider die Leistung des Access-Providers zwar nicht vergütet, obwohl er für ihn ebenfalls eine Leistung in Form des freien und unentgeltlichen Zur-Verfügung-Stellens der vom Nutzer abgerufenen Daten erbringt. Gemäß dem Prinzip des „do ut des“[1050] transportiert der Access-Provider die vom Nutzer beim Content-Provider abgerufenen Daten und erhält dafür vom Content-Provider den freien Zugriff auf diese Daten. Der Access-Provider kann seine Dienstleistungen gegenüber dem Nutzer nur ordentlich ausführen, wenn gleichzeitig der Content-Provider seine Dateien bereitwillig dem Access-Provider zur Verfügung stellt. Im Gegenzug dafür bringt der Access-Provider die über ihn vom Nutzer beim Content-Provider abgefragten Daten zum Nutzer.
Zum anderen müsste der Begriff der Entgeltlichkeit i.S.d. Art. 50 EGV weit ausgelegt werden, um die Entgeltlichkeit bejahen zu können. Grundsätzlich bedeutet nämlich Entgeltlichkeit i.S.d. Art. 50 EGV nur, dass der Dienstleistungserbringer mit seiner Leistung einen Erwerbszweck verfolgt. Nach der Rechtsprechung des EuGH[1051] muss das Entgelt nicht unbedingt vom Empfänger der Dienstleistung an ihren Erbringer gezahlt werden, sondern es muss sich überhaupt um eine geldwerte Leistung handeln.[1052] Folglich reicht es aus, dass der Access-Provider allein vom Nutzer auch für solche Dienste entlohnt wird, die er gleichermaßen für den Content-Provider und für den Nutzer erbringt, um eine entgeltliche Dienstleistung i.S.d. Art. 50 EGV bejahen zu können.
Beide Denkansätze sind plausibel, so dass bei der Leistungsbeziehung Access-Provider/Content-Provider die von Art. 50 EGV vorausgesetzte Entgeltlichkeit angenommen werden kann. Die Leistungsbeziehung Access-Provider/Content-Provider stellt demnach ebenfalls eine Dienstleistung i.S.d. Art. 49 ff. EGV dar. In dieser Fallvariante könnte somit der Access-Provider sowohl in der Leistungsbeziehung Access-Provider/Nutzer als auch in der Leistungsbeziehung Access-Provider/Content-Provider, durch gegen ihn gerichtete behördliche Sperrmaßnahmen in seiner Dienstleistungsfreiheit nach den Art. 49 ff. EGV verletzt sein.

(a) Leistungsbeziehung Access-Provider/Nutzer

Weil der inländische Access-Provider dem inländischen Nutzer den Zugang zum Internet vermittelt, liegt aus der Sichtweise des Access-Providers dem Nutzer gegenüber eigentlich ein rein innerstaatlicher und somit kein europarechtlich relevanter Sachverhalt vor. Problematisch ist jedoch die Tatsache, dass sich der Nutzer mit Hilfe des Ac-

---

[1050] Dieser Ausdruck stammt aus dem Lateinischen und bedeutet wörtlich übersetzt: „ich gebe, damit du gibst“. Gemeint ist damit der gegenseitige Austausch von Leistungen.
[1051] EuGH, Rs. 352/85, 26.04.1988, Slg. 1988, 2085, 2131 Rdnr. 16 (Bond van Adverteerders).
[1052] Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 60 EGV Rdnr. 7.

cess-Providers Zugang zu Inhalten verschafft, die sich im EU-Ausland befinden, also ein Grenzübertritt bestimmter Daten vorliegt.

Eine Auslegungsfrage ähnlicher Art wurde dem EuGH[1053] schon vor einigen Jahren gestellt, doch von ihm nicht beantwortet. In einer anderen Rechtssache[1054] hat der EuGH jedoch festgestellt, dass die Vertragsbestimmungen über den freien Dienstleistungsverkehr nicht auf Betätigungen anwendbar sind, deren wesentliche Elemente sämtlich nicht über die Grenzen eines Mitgliedstaats hinausweisen.[1055] Zudem hat er in einem weiteren Urteil[1056] bestimmt, dass als wichtigstes Kriterium für die Feststellung eines grenzüberschreitenden Sachverhalts die Ansässigkeit der an der Dienstleistung Beteiligten in verschiedenen Staaten ist.[1057] Es stellt sich somit die Frage, wie im vorliegenden Fall zu entscheiden ist, wenn ein inländischer Dienstleistender seine Leistung für einen inländischen Dienstleistungsempfänger zum Teil im Ausland erbringt, ohne dass er sich für die Leistungserbringung in das Ausland begeben muss.

Bereits in der Alpine Investments-Entscheidung des EuGH[1058] wurde angeführt, dass sich ein Inländer durchaus mit Hilfe der Dienstleistungsfreiheit nach den Art. 49 ff. EGV gegen inländische Regelungen oder darauf beruhende Maßnahmen wehren kann. Demnach könnte sich der inländische Access-Provider grundsätzlich wegen der gegen ihn ergangenen behördlichen Sperranordnungen auf die Dienstleistungsfreiheit berufen. Problematisch ist hier aber, dass der Dienstleistungsempfänger – im Gegensatz zur Alpine Investments-Entscheidung – ebenfalls im Inland und nicht im EU-Ausland ansässig ist. Den einzigen grenzüberschreitenden Sachverhalt stellt der Datentransport vom Nutzer zum Content-Provider und zurück dar. Sämtliche für das Access-Providing notwendigen Handlungen übt der Access-Provider hingegen für den Nutzer regelmäßig im Inland aus. Denn der Datentransport selbst erfolgt automatisch, sobald die Daten in ihre Datenpakete aufgeteilt und verschickt worden sind.[1059] Demzufolge beinhaltet die Betätigung des Access-Providers gegenüber dem Nutzer hauptsächlich Elemente, die nicht über die Grenzen eines Mitgliedstaats hinausweisen. Des weiteren sind die Beteiligten dieses Access-Providings allein im Inland ansässig. Aus diesen Gründen kann sich der Access-Provider nicht auf die Dienstleistungsfreiheit im Leistungsverhältnis Access-Provider/Nutzer berufen.

1053 Es ging um das Recht einer inländischen Gesellschaft für Kabelfernsehen, einen im Ausland ausgestrahlten Film ihren Kunden im Inland zuzuspielen, vgl. EuGH Rs. 62/79, 18.03.1980, Slg. 1980, 881, 901 f. und 904 Rdnr. 7, 8 und 19 (Coditel/CinéVog).

1054 EuGH, Rs. 52/79, 18.03.1980, Slg. 1980, 833, 855 Rdnr. 9 (Debauve).

1055 Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 60 EGV Rdnr. 16.

1056 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1174 Rdnr. 21 (Alpine Investments BV).

1057 Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 8.

1058 EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141, 1176 Rdnr. 30 (Alpine Investments BV).

1059 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. c. bb. (3).

(b) Leistungsbeziehung Access-Provider/Content-Provider

Etwas anderes gilt jedoch für das Leistungsverhältnis Access-Provider/Content-Provider. Wichtigster Unterschied ist zunächst, dass der Content-Provider im EU-Ausland zu finden ist. Ein grenzüberschreitender Sachverhalt ist demnach gegeben. Es liegt eine ähnliche Konstellation wie bei der Alpine Investments-Entscheidung vor. Folglich ist der Access-Provider zumindest im Leistungsverhältnis Access-Provider/Content-Provider durch staatliche Sperrmaßnahmen in seiner Dienstleistungsfreiheit nach den Art. 49 ff. EGV tangiert.

bb. Sicht des Content-Providers

Auch der Content-Provider besitzt zwei Leistungsbeziehungen. Zum einen besteht – wie vorstehend bei der Sichtweise des Access-Providers angesprochen – ein Leistungsverhältnis zwischen dem Content-Provider und dem Access-Provider, zum anderen gibt es auch noch das Verhältnis Content-Provider/Nutzer. Insoweit muss deshalb erneut unterschieden werden:

(1) Leistungsbeziehung Content-Provider/Access-Provider

Hinsichtlich der Leistungsbeziehung Content-Provider/Access-Provider könnten die gegen den Access-Provider gerichteten staatlichen Kontrollmaßnahmen mittelbar in die Dienstleistungsfreiheit des Content-Providers eingreifen. Da der Content-Provider Leistungen des Access-Providers, der in einem anderen Mitgliedstaat ansässig ist, entgegennimmt, liegt eigentlich ein Fall der passiven Dienstleistungsfreiheit vor,[1060] der von den Art. 49 ff. EGV geschützt wird.[1061] Zudem erbringt der Content-Provider, der seine Daten dem Access-Provider überlässt, ebenfalls eine Dienstleistung.[1062] Deswegen könnte auch eine Korrespondenzdienstleistung zwischen dem Content-Provider und dem Access-Provider angenommen werden. Letztendlich kommt es jedoch nicht darauf an, welche Art der Dienstleistungsfreiheit, sondern dass die Dienstleistungsfreiheit betroffen ist.[1063] Dies ist hier zu bejahen, weil der Content-Provider durch Sperrmaßnahmen beim Access-Provider jedenfalls mittelbar daran gehindert wird, seine Daten dem Access-Provider zu überlassen und sie von ihm zum Nutzer zu transportieren.
Demnach verstoßen behördliche Sperrmaßnahmen, die an den Access-Provider gerichtet sind, mittelbar gegen die Dienstleistungsfreiheit des Content-Providers.

[1060] Allerdings in Form der Korrespondenzdienstleistungsfreiheit, da nur die Leistung die Grenze passiert.

[1061] Kluth in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 50 Rdnr. 27.

[1062] Vgl. vorstehende Ausführungen.

[1063] Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 60 EGV Rdnr. 24.

(2) Leistungsbeziehung Content-Provider/Nutzer

(a) Warenverkehrsfreiheit

Bei der Leistungsbeziehung Content-Provider/Nutzer könnte mittelbar zunächst durch staatlichen Sperranordnungen die Warenverkehrsfreiheit des Content-Providers betroffen sein. Sobald der Content-Provider Waren im Internet anbietet oder dafür wirbt und insoweit gegenüber dem Access-Provider eine Sperranordnung ergeht, wird der Content-Provider daran gehindert, den deutschen Nutzer auf seine Warenangebote zugreifen zu lassen. Hierdurch wird der Content-Provider in seiner Warenverkehrsfreiheit gemäß Art. 28 EGV tangiert.

(b) Dienstleistungsfreiheit

Bietet der Content-Provider dem Nutzer dagegen Dienstleistungen an[1064] oder stellt der Inhalt, den der Content-Provider für den Nutzer im Internet bereithält, eine Dienstleistung dar, dann ist auch eine Beeinträchtigung der Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV gegeben.[1065]

c. Fallvariante II: Access-Provider aus dem EU-Ausland, Deutscher Nutzer, Content-Provider ist wieder eine natürliche oder juristische Person aus dem EU-Ausland

Wie bei den einzelnen Fallvarianten, die im Rahmen von Sperr- und/oder Löschanordnungen gegen den Content- bzw. Service-Provider gebildet wurden,[1066] ist zwischen den möglichen Personen des Access-Providers zu unterscheiden:

aa. Der Access-Provider ist eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland

Zunächst ist der Access-Provider eine natürliche Person mit einer Staatsangehörigkeit aus dem EU-Ausland, die ihren Wohnsitz im Inland hat. Darüber hinaus kann sie optional auch noch eine mit dem Access-Providing im Zusammenhang stehende Infrastruktur (beispielsweise Büroräume, etc.) im Inland errichtet haben.

(1) Sicht des Access-Providers

(a) Warenverkehrsfreiheit

Der Access-Provider handelt nicht mit Waren, sondern bietet lediglich Internet-Dienste an. Werden diese Dienste durch staatliche Maßnahmen beeinträchtigt, dann kann die Warenverkehrsfreiheit hiervon nicht betroffen sein.

1064 Schon allein das Content-Providing selbst kann bereits als Dienstleistung angesehen werden.
1065 Vgl. die obigen Ausführungen unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).
1066 Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. und 2.

(b) Niederlassungsfreiheit

Da der aus dem EU-Ausland stammende Access-Provider im Inland auf Dauer eine Erwerbs- oder Geschäftstätigkeit ausübt, hat er sich niedergelassen.[1067] Die Art. 43 ff. EGV sind demnach anwendbar. Eine staatliche Sperranordnung tangiert somit die Niederlassungsfreiheit des Access-Providers.

(c) Dienstleistungsfreiheit

Wegen des Grundsatzes der Subsidiarität nach Art. 50 I EGV braucht ein Verstoß gegen die Dienstleistungsfreiheit nicht angeprüft werden.

(2) Sicht des Content-Providers

Wieder ist zwischen den jeweiligen Leistungsbeziehungen zu unterscheiden:

(a) Leistungsbeziehung Content-Provider/Nutzer

Hinsichtlich der Leistungsbeziehung Content-Provider/Nutzer kann sich der Content-Provider, je nachdem, welchen Inhalt er im Internet anbietet, entweder auf eine mittelbare Beeinträchtigung der Warenverkehrsfreiheit und/oder der Dienstleistungsfreiheit[1068] berufen. Denn wenn der Content-Provider Warenangebote und/oder Dienstleistungen bzw. –werbung hierfür im Internet für den Nutzer bereithält, wird der Content-Provider durch die Sperranordnung daran gehindert, dass diese Angebote vom Nutzer empfangen und in Anspruch genommen werden können. Deshalb kann hier durch die ursprünglich gegen den Access-Provider gerichteten staatlichen Kontrollmaßnahmen zumindest ein mittelbarer Eingriff in die Warenverkehrsfreiheit und/oder Dienstleistungsfreiheit bejaht werden.

(b) Leistungsbeziehung Content-Provider/Access-Provider

Weil der Content-Provider weiterhin eine natürliche oder juristische Person aus dem EU-Ausland ist, die ihren Wohn- bzw. Firmensitz im EU-Ausland hat, liegt hier in der Leistungsbeziehung Content-Provider/Access-Provider aus der Sicht des Content-Providers ebenfalls ein Verstoß gegen die passive Dienstleistungsfreiheit bzw. Korres-

---

[1067] Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 110.

[1068] Zwar besagt Art. 50 I EGV, dass die Dienstleistungsfreiheit gegenüber der Warenverkehrsfreiheit ebenfalls subsidiär ist. Allerdings wird aus dem Wortlaut des Art. 50 I EGV deutlich, dass nur die Dienstleistungen nicht von den Art. 49 ff. EGV erfasst werden, die unter die Warenverkehrsfreiheit subsumiert werden können. Damit ist gemeint, dass eine Leistung nicht zugleich Ware und Dienstleistung sein kann. Die Warenverkehrsfreiheit und die Dienstleistungsfreiheit stehen somit hinsichtlich eines bestimmten Angebots in einem Ausschlussverhältnis. Eine Dienstleistung liegt dann nicht vor, wenn die Leistung in einer beweglichen Sache verkörpert ist, vgl. Geiger, EUV/EGV, 3. Auflage, Art. 50 Rdnr. 1. Besitzt ein Anbieter jedoch mehrere Angebote, die – getrennt betrachtet – sowohl der Waren- als auch der Dienstleistungsfreiheit zugerechnet werden können. Beispielsweise bietet der Content-Provider neben Daten in Form von Software auch Waren im Internet an. Dann kann sich der Anbieter unter gewissen Umständen auf die Waren- und auf die Dienstleistungsfreiheit berufen, da verschiedene Arten von Leistungen betroffen sein können.

pondenzdienstleistung vor.[1069] Daran ändert auch der Umstand nichts, dass der Access-Provider aus dem EU-Ausland stammt. Denn wesentlich für die Dienstleistungsfreiheit nach den Art. 49 ff. EGV ist, dass der Dienstleistungsempfänger in einem anderen Mitgliedstaat als der Dienstleistungserbringer ansässig ist und deshalb die Dienstleistung innerhalb der EG über eine nationale Grenze hinweg erbracht wird.[1070]

bb. Der Access-Provider ist eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland, während sich die Technik für das Access-Providing im Inland befindet

(1) Sicht des Access-Providers

Fraglich ist, ob der Access-Provider durch die staatliche Sperrverfügung in seiner Niederlassungsfreiheit oder Dienstleistungsfreiheit beeinträchtigt wird. Es muss zwischen diesen beiden Grundfreiheiten – wie bereits oben bei der Überprüfung von Kontrollmaßnahmen gegen den Content-Provider ausführlich geschehen[1071] – abgegrenzt werden. Als Abgrenzungskriterium wird danach gefragt, ob die Tätigkeit des Dienstleistenden lediglich vorübergehender Natur oder auf Dauer angelegt ist.[1072] Da der Access-Provider seinen Sitz im Ausland hat und sich lediglich die Technik für das Access-Providing im Inland befindet, kann keine Niederlassung i.S.d. Art. 43 ff. EGV angenommen werden. Denn dafür fehlen weitere Komponenten. Die reine Technik – zu verweisen ist insoweit auf den Rechtsgedanken des Art. 2 c der ECRL – reicht hierfür noch nicht aus. Zudem beansprucht der Nutzer die Dienste des Access-Providers nur nach Bedarf. Also übt der Access-Provider seine Dienste nur vorübergehend im Inland aus, so dass nicht die Niederlassungsfreiheit, sondern nur die Dienstleistungsfreiheit gemäß den Art. 49 ff. EGV von behördlichen Sperranordnungen tangiert wird.
Darüber hinaus kann ein weiterer Verstoß gegen die Dienstleistungsfreiheit darin gesehen werden, dass der Access-Provider durch die Sperrverfügung daran gehindert wird, auf die Daten des Content-Providers zuzugreifen. Obwohl der Access-Provider seinen Sitz im Ausland hat, wählt sich der inländische Nutzer mit seiner Hilfe im Inland in das Netz ein. Danach versucht der Nutzer, den Inhalt des Content-Providers im EU-Ausland abzurufen. Demzufolge liegt ein grenzüberschreitender Sachverhalt vor, der von den Art. 49 ff. EGV geschützt wird. Denn der Access-Provider will Daten vom Content-Provider aus dem EU-Ausland zum Nutzer in das Inland transportieren. Dieser Vorgang der Korrespondenzdienstleistung[1073] muss schon allein wegen der Zweckbestimmung dieser Normen unter die Art. 49 ff. EGV subsumiert werden, obwohl der Access-

---

1069 Vgl. hierzu die obigen Ausführungen unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).
1070 Clausnitzer in: Lenz (Hrsg.) EG-Handbuch Recht im Binnenmarkt, 2. Auflage, S. 245.
1071 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (2).
1072 Fastenrath/Müller-Gerbes, Europarecht, Rdnr. 131.
1073 Möglich wäre auch, darin eine passive Dienstleistungsfreiheit zu sehen, vgl. Geiger, EUV/EGV, 3. Auflage, Art. 50 Rdnr. 7.

Provider seinen Sitz im EU-Ausland hat. Folglich besteht bei dieser Fallkonstellation ein weiterer Verstoß gegen die Dienstleistungsfreiheit.

(2) Sicht des Content-Providers

Wiederum ist zwischen den jeweiligen Leistungsbeziehungen zu unterscheiden:

(a) Leistungsbeziehung Content-Provider/Nutzer

Der Content-Provider wird erneut durch die gegen den Access-Provider gerichteten staatlichen Sperrmaßnahmen gegenüber dem Nutzer mittelbar in seiner Warenverkehrs- und/oder Dienstleistungsfreiheit betroffen.[1074]

(b) Leistungsbeziehung Content-Provider/Access-Provider

Im Verhältnis Content-Provider/Access-Provider besteht auch noch ein Verstoß gegen die Dienstleistungsfreiheit. Der Content-Provider wird daran gehindert, dem Access-Provider seine Daten grenzüberschreitend frei zur Verfügung zu stellen, damit er sie dem Nutzer übermitteln kann. Insoweit liegt eine Beeinträchtigung der Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV in Form der Korrespondenzdienstleistungsfreiheit vor.

cc. Der Access-Provider ist eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland, wobei neben der reinen Technik noch weitere mit dem Access-Providing im Zusammenhang stehende Komponenten (wie beispielsweise Büroräume) im Inland vorhanden sind

(1) Sicht des Access-Providers

(a) Niederlassungsfreiheit

Im Gegensatz zur vorhergehenden Fallkonstellation besitzt nun der Access-Provider neben der reinen Technik noch weiteres Zubehör im Inland, das mit dem Access-Providing im Zusammenhang steht. Die Abgrenzung zwischen der Niederlassungsfreiheit und der Dienstleistungsfreiheit richtet sich jetzt danach, ob die Komponenten und die Technik im Inland ausreichen, um dem Niederlassungsbegriff der Art. 43 ff. EGV zu genügen. Letztlich ist dies eine Einzelfallentscheidung und kann deshalb hier nicht abschließend geklärt werden. Der Übergang von der Dienstleistungsfreiheit zur Niederlassungsfreiheit ist bei dieser Konstellation fließend. Da jedoch schon beim Vorliegen der reinen Technik eine Abgrenzung nur schwer durchzuführen ist, können neben der Technik schon wenige Komponenten im Inland ausreichen, um eine Niederlassung bejahen zu können. Demnach wird wohl durch staatliche Sperr- und/oder Löschanordnungen bei dieser Fallkonstellation vermehrt in die Niederlassungsfreiheit gemäß den Art.

[1074] Vgl. insofern die ausführlichen Darstellungen bei vorhergehender Prüfung unter B. 3. Teil. 2. Kapitel. V. 3. c. aa. (2).

43 ff. EGV und weniger in die Dienstleistungsfreiheit nach den Art. 49 ff. EGV eingegriffen.

(b) Dienstleistungsfreiheit

Falls die Niederlassungsfreiheit zur Anwendung kommt, tritt die Dienstleistungsfreiheit wegen Art. 50 I EGV aufgrund der Subsidiarität dahinter zurück.

(2) Sicht des Content-Providers

Wieder ist eine Unterscheidung zwischen den einzelnen Leistungsbeziehungen nötig:

(a) Leistungsbeziehung Content-Provider/Nutzer

Hinsichtlich der Leistungsbeziehung Content-Provider/Nutzer ist der Content-Provider wie gehabt durch die staatlichen Sperrverfügungen mittelbar in seiner Warenverkehrsfreiheit und/oder in seiner Dienstleistungsfreiheit verletzt.[1075]

(b) Leistungsbeziehung Content-Provider/Access-Provider

Bezüglich des Verhältnisses Content-Provider/Access-Provider kann sich der Content-Provider zudem auf die Dienstleistungsfreiheit in Form der Korrespondenzdienstleistung berufen.[1076]

d. Fallvariante III: Deutscher Access-Provider, Nutzer aus dem EU-Ausland, Content-Provider ist eine natürliche oder juristische Person aus dem EU-Ausland

Bei dieser Fallvariante findet in der Person des Nutzers eine Unterscheidung statt.

aa. Der Nutzer ist eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland

(1) Sicht des Access-Providers

Hier muss ebenfalls zwischen den Leistungsbeziehungen differenziert werden:

(a) Leistungsbeziehung Access-Provider/Nutzer

Das gleiche Problem wie in der Fallvariante I ergibt sich auch hier:[1077] Eigentlich stellt der genannte Sachverhalt dieser Fallkonstellation aus der Sicht des Access-Providers einen rein innerstaatlichen Vorgang dar. So vermittelt der inländische Access-Provider dem Nutzer im Inland Daten eines Content-Providers aus dem EU-Ausland. Die Leistungsbeziehung Access-Provider/Nutzer hat ihren Schwerpunkt im Inland. Mangels

---

[1075] Vgl. insofern die ausführlichen Darstellungen bei vorhergehender Prüfung unter B. 3. Teil. 2. Kapitel. V. 3. c. aa. (2).

[1076] Vgl. insofern die ausführlichen Darstellungen bei vorhergehender Prüfung unter B. 3. Teil. 2. Kapitel. V. 3. c. bb. (2). (b).

[1077] Siehe insoweit oben unter B. 3. Teil. 2. Kapitel. V. 3. b. aa. (a).

grenzüberschreitenden Sachverhalts kann der EGV deshalb nicht angewendet werden. Diese Schlussfolgerung ist jedoch fragwürdig, da die Daten, die der Nutzer vom Content-Provider über den Access-Provider erhält, aus dem EU-Ausland stammen und somit eine Auslandsberührung vorliegt. Gleichwohl kann ein Verstoß gegen die Dienstleistungsfreiheit nicht bejaht werden. Denn Dienstleistender und –empfänger befinden sich im Inland. Die Leistung zwischen Access-Provider und Nutzer ist nicht grenzüberschreitend, da die Daten, die vom Content-Provider stammen, zunächst via Internet über die Grenze(n) ins Inland zum Access-Provider geschickt werden. Erst dort werden die Daten an den Nutzer weitergeleitet. Dieser letzte Vorgang spielt sich jedoch ausschließlich im Inland ab, so dass Europarecht hiervon nicht betroffen ist.

(b) Leistungsbeziehung Access-Provider/Content-Provider

Demgegenüber greifen bei der Leistungsbeziehung Access-Provider/Content-Provider die behördlichen Sperrmaßnahmen in die Dienstleistungsfreiheit des Access-Providers ein. Dies ist ein typischer Fall der Alpine Investments-Entscheidung des EuGH:[1078] Der inländische Dienstleistungserbringer (Access-Provider) wird durch inländische Maßnahmen daran gehindert, seine Leistung gegenüber einem Dienstleistungsempfänger im EU-Ausland (Content-Provider) zu erbringen. Damit liegt hier ebenfalls die Form der Korrespondenzdienstleistung vor.

(2) Sicht des Content-Providers

Wiederum erfolgt eine Unterscheidung zwischen den jeweiligen Leistungsbeziehungen:

(a) Leistungsbeziehung Content-Provider/Nutzer

Beim Leistungsverhältnis zwischen dem Content-Provider und Nutzer greifen die gegen den Access-Provider gerichteten Sperrverfügungen wie schon bei den vorangegangenen Fallkonstellationen[1079] zumindest mittelbar in die Warenverkehrs- und/oder Dienstleistungsfreiheit ein.

(b) Leistungsbeziehung Content-Provider/Access-Provider

Gegenüber dem Access-Provider wird der Content-Provider ebenfalls mittelbar in seiner Dienstleistungsfreiheit beeinträchtigt, da er ihm seine Daten nicht zur Verfügung stellen kann. Insoweit ist er also in seiner Korrespondenzdienstleistungsfreiheit betroffen.[1080]

[1078] EuGH, Rs. C-384/93, 10.05.1995, Slg. 1995, I-1141ff. (Alpine Investments BV).
[1079] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 3. c. aa. (2). und bb. (2). (b).
[1080] Vgl. insoweit auch oben unter B. 3. Teil. 2. Kapitel. V. 3. c. bb. (2). (b).

bb. Der Nutzer ist eine natürliche und juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland

(1) Sicht des Access-Providers

Sowohl in der Leistungsbeziehung Access-Provider/Nutzer als auch gegenüber dem Content-Provider wird der Access-Provider durch die behördlichen Sperrmaßnahmen in seiner Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV tangiert. In beiden Fällen liegt ein grenzüberschreitender Sachverhalt vor, bei dem allein die Leistung[1081] die Grenzen der Mitgliedstaaten überschreitet.

(2) Sicht des Content-Providers

Auch hier findet eine Differenzierung zwischen den einzelnen Leistungsbeziehungen statt:

(a) Leistungsbeziehung Content-Provider/Nutzer

(aa)Dienstleistungsfreiheit

Wieder wird der Content-Provider beim Leistungsverhältnis Content-Provider/Nutzer mittelbar in der Dienstleistungsfreiheit nach den Art. 49 ff. EGV verletzt. Er kann nämlich dem Nutzer seine – in der Regel gegen Entgelt – angebotenen Daten nicht mehr zur Verfügung stellen. Weil sich der Access-Provider im Inland befindet, müssen die Daten über das Inland vom Content-Provider zum Nutzer verschickt werden. Folglich liegt ein von den Art. 49 ff. EGV vorausgesetzter grenzüberschreitender Sachverhalt vor.

(bb)Warenverkehrsfreiheit

Problematisch ist hier jedoch die Frage, ob auch die Warenverkehrsfreiheit nach Art. 28 EGV mittelbar beeinträchtigt wird. Denn sowohl der Nutzer als auch der Content-Provider befinden sich im EU-Ausland. Wird der Nutzer durch die behördliche Sperranordnung daran gehindert, auf das eventuell vorhandene Warenangebot und die dafür bereitgehaltene Werbung des Content-Providers zuzugreifen, hätte dies lediglich die Wirkung, dass der Content-Provider seine Waren nicht dem Nutzer anbieten kann. Er ist somit in seiner Möglichkeit, dem Nutzer die Waren zukommen zu lassen, mittelbar beeinträchtigt. Damit ist allerdings nicht gesagt, dass die angebotenen Waren, auch wenn der Nutzer diese bestellt, die inländischen Grenzen überschreiten. Denn es besteht die Möglichkeit, die Waren an den Grenzen des Inlands vorbei zu transportieren. Zwar könnte der gemeinschaftliche Warenverkehr durch die inländische Sperranordnung indirekt behindert werden, ohne dass das Inland hiervon tangiert wäre. Art. 28 und 29 EGV

[1081] Die Leistung des Access-Providers ist beide Male der Datentransport zum einen für den Nutzer zum anderen für den Content-Provider. Des weiteren ermöglicht der Access-Provider als weitere Leistung dem Nutzer den Zugang zum Internet.

sprechen jedoch in ihren Wortlauten entweder von „Einfuhrbeschränkungen“ oder von „Ausfuhrbeschränkungen“. Nicht geregelt ist dagegen der Fall, dass inländische Maßnahmen den Warenverkehr zwischen zwei anderen Mitgliedstaaten beeinträchtigen. Der EuGH hat allerdings in seiner Dassonville-Formel[1082] festgelegt, dass Maßnahmen gleicher Wirkung i.S.d. Art. 28 EGV, also staatliche Maßnahmen den Einfuhrbeschränkungen gleich stehen, die allgemein geeignet sind, den innergemeinschaftlichen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern.[1083] Ob das Inland selbst von den Maßnahmen betroffen ist, stellt demnach kein Kriterium dar. Folglich müssen ebenfalls die gegen den Access-Provider gerichteten Sperrmaßnahmen hierunter gefasst werden, weil sie potentiell geeignet sind, den innergemeinschaftlichen Handel zu beeinträchtigen. Somit ist also auch in diesem Fall die Warenverkehrsfreiheit durch die staatlichen Sperrverfügungen tangiert.[1084]

(b) Leistungsbeziehung Content-Provider/Access-Provider

Bezüglich der Leistungsbeziehung Content-Provider/Access-Provider liegt wiederum ein Verstoß gegen die Dienstleistungsfreiheit in Form der Korrespondenzdienstleistung vor.[1085]

e. Weitere Kombinationen der genannten beteiligten Personen

Zusätzliche Fallkonstellationen, bei denen beispielsweise sowohl der Nutzer als auch der Access-Provider aus dem EU-Ausland stammen, lassen keine neuen Erkenntnisse bzw. Ergebnisse erwarten. Denn letztendlich ist allein die jeweilige Sichtweise der beteiligten Personen für die Frage nach der europarechtlichen Relevanz von Bedeutung. Und diese Sichtweisen wurden mit den vorstehenden Fallkonstellationen abschließend durchgeprüft. Deswegen ist es unnötig, noch weitere Kombinationen zwischen dem Access-Provider, Nutzer und Content-Provider aus dem Inland bzw. EU-Ausland zu bilden.

f. Zusammenfassung

aa. Fallvariante I

Bei der Fallvariante I, die von einem deutschen Access-Provider und Nutzer sowie dem Content-Provider im EU-Ausland ausgeht, wird aus der Sicht des Access-Providers durch die staatlichen Sperranordnungen in die Dienstleistungsfreiheit eingegriffen. Aus der Perspektive des Content-Providers muss ebenfalls gegenüber dem Access-Provider

---

1082 EuGH, Rs. 8/74, 11.07.1974, Slg. 1974, 837, 852 Rdnr. 5 (Dassonville).

1083 Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1499.

1084 Eine Ausnahme von diesem Ergebnis ist jedoch dann vorstellbar, wenn sowohl der Content-Provider als auch der Nutzer aus dem gleichen Mitgliedstaat stammen. Dann würde die Ware keine gemeinschaftliche Grenze passieren, so dass die Warenverkehrsfreiheit nicht zur Anwendung kommt.

1085 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 3. c. bb. (2). (b)

ein Verstoß gegen die Dienstleistungsfreiheit angenommen werden. Je nachdem, welchen Inhalt der Content-Provider dem Nutzer anbietet, besteht zudem die Möglichkeit, dass bei der Leistungsbeziehung Content-Provider/Nutzer neben der Anwendbarkeit der Dienstleistungsfreiheit auch die Warenverkehrsfreiheit mittelbar durch die Sperrverfügungen betroffen ist.

bb. Fallvariante II

Die Fallvariante II besitzt drei weitere Konstellationen zwischen denen unterschieden werden muss, da der Access-Provider verschiedenartig im Inland vertreten sein kann: Ist der Access-Provider eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland, dann ist aus der Sicht des Access-Providers die Niederlassungsfreiheit durch staatliche Sperranordnungen beeinträchtigt. Aus dem Blickwinkel des Content-Providers ist bei der Leistungsbeziehung Content-Provider/Nutzer ein Verstoß gegen die Dienstleistungsfreiheit sowie in bestimmten Fällen gegen die Warenverkehrsfreiheit zu bejahen. Hinsichtlich der Leistungsbeziehung Content-Provider/Access-Provider findet lediglich die Dienstleistungsfreiheit Anwendung.

Ist der Access-Provider dagegen eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland, wobei sich nur die für das Access-Providing erforderliche Technik im Inland befindet, dann wird die Dienstleistungsfreiheit des Access-Providers gleich zweimal verletzt, nämlich sowohl im Verhältnis Access-Provider/Nutzer als auch im Verhältnis Access-Provider/Content-Provider. Aus der Perspektive des Content-Providers folgt, dass wiederum bezüglich der Leistungsbeziehung Content-Provider/Nutzer die Dienstleistungsfreiheit und/oder die Warenverkehrsfreiheit mittelbar betroffen sind. Bei dem Leistungsverhältnis Content-Provider/Access-Provider ist hingegen allein die Dienstleistungsfreiheit von den staatlichen Kontrollmaßnahmen tangiert.

Schließlich kann der Access-Provider eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland sein. Neben der reinen Technik befinden sich noch weitere Komponenten (wie beispielsweise Büroräume) im Inland, die mit dem Access-Providing im Zusammenhang stehen. Bei dieser Fallkonstellation kommt es auf den jeweiligen Einzelfall an, ob aus der Sicht des Access-Providers die Dienstleistungsfreiheit oder die Niederlassungsfreiheit anwendbar ist. Häufig werden wohl die Kriterien der Niederlassungsfreiheit erfüllt sein.[1086] Aus dem Blickwinkel des Content-Providers ergibt sich, dass bei der Leistungsbeziehung Content-Provider/Nutzer die Dienstleistungsfreiheit und/oder die Warenverkehrsfreiheit mittelbar verletzt sind. Schließlich besteht ein Verstoß gegen die Dienstleistungsfreiheit im Leistungsverhältnisses Content-Provider/Access-Provider.

[1086] Deshalb wird im folgenden von einer Verletzung der Niederlassungsfreiheit für diese Fallkonstellation ausgegangen.

cc. Fallvariante III

Die Fallvariante III besitzt zwei Fallkonstellationen: Diesmal wird beim Nutzer unterschieden. Zunächst ist der Nutzer eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland. Hier wird aus der Sicht des Access-Providers beim Leistungsverhältnis Access-Provider/Content-Provider durch die behördlichen Sperrverfügungen in die Dienstleistungsfreiheit eingegriffen. Aus der Perspektive des Content-Providers ergeben sich sogar Verstöße gegen die Dienstleistungsfreiheit und/oder Warenverkehrsfreiheit, wenn die Leistungsbeziehung Content-Provider/Nutzer betrachtet wird, sowie ein weiteres Mal gegen die Dienstleistungsfreiheit bei der Leistung des Content-Providers an den Access-Provider.
Handelt es sich beim Nutzer um eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland, dann ist zunächst aus der Sichtweise des Access-Providers eine doppelte Verletzung der Dienstleistungsfreiheit zu bejahen. Des weiteren werden aus der Perspektive des Content-Providers mittelbar die Dienstleistungsfreiheit und/oder – unter Umständen – die Warenverkehrsfreiheit bezüglich der Leistungsbeziehung Content-Provider/Nutzer berührt. Im Hinblick auf das Leistungsverhältnis Content-Provider/Access-Provider liegt durch die staatlichen Sperrmaßnahmen dagegen lediglich ein Eingriff in die Dienstleistungsfreiheit vor.

g. Vereinbarkeit der europarechtlich relevanten Kontrollmaßnahmen mit den jeweiligen Grundfreiheiten

Es erscheint sinnvoll, im folgenden aus Gründen der Übersichtlichkeit zwischen der Perspektive des Access-Providers und des Content-Providers zu unterscheiden:

aa. Sicht des Access-Providers

(1) Niederlassungsfreiheit

Wie sich aus den vorstehend angestellten Untersuchungen ergeben hat, wird die Niederlassungsfreiheit des Access-Providers durch die gegen ihn verfügten behördlichen Sperranordnungen in der Fallvariante II bei zwei Fallkonstellationen tangiert: Zum einen, wenn der Access-Provider eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland ist. Zum anderen, wenn es sich beim Access-Provider um eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland handelt, bei der aber die Technik und weitere mit dem Access-Providing im Zusammenhang stehende Komponenten im Inland befindlich sind. Bei beiden Fallkonstellationen ist der Nutzer Deutscher und der Content-Provider im EU-Ausland.

(a) Inländergleichbehandlung

Mittlerweile geht der Schutz der Art. 43 ff. EGV über das in Art. 43 II EGV fixierte Diskriminierungsverbot hinaus. Es besteht somit ein allgemeines Beschränkungsverbot,

so dass der Access-Provider in seinem Recht auf Aufnahme und Ausübung einer selbständigen Erwerbstätigkeit i.S.d. Art. 43 II EGV verletzt ist.[1087] Dieser Eingriff in die Grundfreiheit des EGV ist nur zulässig, wenn ihm ein Rechtfertigungsgrund zur Seite steht.

(b) Rechtfertigung

Eine Rechtfertigung kann sich wieder aus der bereits an obiger Stelle ausführlich besprochenen,[1088] vom EuGH entwickelten Schrankensystematik sowie aus den gesetzlich normierten Ausnahmetatbeständen der Art. 45, 46 EGV ergeben.

(aa)Zwingende Gründe des Allgemeininteresses

Der EuGH hat für die Niederlassungsfreiheit entschieden, dass ein Eingriff in diese Grundfreiheit durch zwingende Gründe des Allgemeininteresses gerechtfertigt sein kann.[1089] Allerdings können Sperrmaßnahmen im Internet, die vor allem aus polizei- und sicherheitsrechtlichen Gründen ergehen, nicht unter die vom EuGH genannten Fallgruppen der zwingenden Gründe des Allgemeininteresses eingeordnet werden.[1090] Insoweit scheidet ein Rechtfertigungsgrund aus.

(bb)Art. 45, 46 EGV

Die Schranke des Art. 45 EGV ist ebenfalls nicht einschlägig. Die Tätigkeit des Access-Providers ist regelmäßig nicht mit der Ausübung öffentlicher Gewalt verbunden.
Es könnte jedoch Art. 46 I EGV erfüllt sein. Art. 46 I EGV findet entgegen seinem Wortlaut auch auf unterschiedslose Regelungen Anwendung.[1091] Die behördlichen Kontrollmaßnahmen ergehen aus Gründen der öffentlichen Ordnung und Sicherheit i.S.d. Art. 46 I EGV.[1092]
Darüber hinaus müssen sie den Grundsatz der Verhältnismäßigkeit einhalten, damit Art. 46 I EGV erfüllt ist. Demzufolge ist es notwendig, beide Seiten und ihre Interessen zu betrachten:
Die Sperranordnungen sind grundsätzlich geeignet, den Nutzer davon abzuhalten, auf rechtswidrige Inhalte zuzugreifen und somit den Inhalt in das Inland einzuführen bzw. dort zu verbreiten. Des weiteren ist die Sperrmaßnahme auch erforderlich, da sie – technisch gesehen – die einzige Möglichkeit darstellt, gegen den ausländischen Inhalt direkt vorzugehen. Allerdings müssen hier die Nachteile der Sperrung von Internet-Seiten durch den Access-Provider in Erinnerung gerufen werden.[1093] Demnach ist es technisch

---

[1087] Vgl. hierzu die Ausführungen an obiger Stelle unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (1).
[1088] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). Und bb. (2). (a).
[1089] EuGH, Rs. C-19/92, 31.03.1993, Slg. 1993, 1663, 1697 Rdnr. 32 (Kraus).
[1090] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (a).
[1091] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).
[1092] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).
[1093] Siehe insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (1).

noch nicht möglich, gezielt nur den rechtswidrigen Inhalt sperren zu lassen. Vielmehr werden durch das Sperren von bestimmten Port-Adressen neben dem illegalen Inhalt auch viele rechtmäßige, im Internet bereitgehaltene Angebote für den Nutzer gesperrt. Darüber hinaus ist zu bedenken, dass der eigentliche Störer nicht der Access-Provider, sondern der Content-Provider ist, der den rechtswidrigen Inhalt in das Internet eingestellt hat.[1094] Dies ist bei der Frage nach der Angemessenheit der Sperrungsanordnungen zu berücksichtigen. Es muss somit abgewogen werden, ob die Interessen des Staates und der Allgemeinheit gewichtiger sind als die des Access-Providers, so dass die Interessen des Access-Providers gegenüber den staatlichen und individuellen Interessen zurückzutreten haben. Hierbei ist zunächst die Schwere der Beeinträchtigung beim Access-Providers zu betrachten. Der Access-Provider kann dem Nutzer bestimmte Inhalte von einem Content-Provider aus dem EU-Ausland nicht mehr vermitteln. Zudem ist er daran gehindert, für den Content-Provider die vom Nutzer abgerufenen Daten diesem zuzuleiten. In beiden Fällen kann der Access-Provider seine Dienste nicht mehr erfüllen. Außer den gesperrten Inhalten bleiben aber alle anderen Inhalte im Internet für den Nutzer zugänglich, so dass der Access-Provider insoweit seine Dienste sowohl für den Nutzer als auch für den jeweiligen Content-Provider ungehindert ausführen kann. Dies wird wohl in der Regel den größten Teil seiner Tätigkeit ausmachen. Der Umstand, dass er bestimmte Inhalte nicht mehr zwischen dem Content-Provider, dessen Inhalte zu sperren sind, und dem Nutzer vermitteln kann, ist daher als eher unbedeutend anzusehen. Denn fast alle übrigen Daten im Netz können von ihm abgerufen und zum Nutzer transportiert werden. Wenn dabei vereinzelt einige Internet-Adressen zusätzlich gesperrt werden, ist dies ein unbedeutender Eingriff. Demgegenüber wird durch die Sperrung von illegalen ausländischen Inhalten viel erreicht. Zum einen kann zunächst ein staatliches Zeichen gesetzt werden, dass bestimmte Inhalte unerwünscht sind. Zum anderen wird der Nutzer vor rechtswidrigen Inhalten geschützt und der Staat kann – zumindest anfangs – erreichen, dass der illegale Inhalt nicht in das Inland getragen und dort verbreitet wird. Allerdings bleibt die Möglichkeit, die verhängte Sperrung zu umgehen.[1095] Gleichwohl ist es viel wichtiger, bestimmte Inhalte vom Nutzer und somit vom Inland fern zu halten sowie dadurch den Access-Provider an der Ausführung seiner Dienstleistung zu hindern. Dies muss der Access-Provider in Kauf nehmen. Die staatlichen Kontrollmaßnahmen sind demnach auch angemessen. Hinzu kommt, dass sich der Access-Provider aus freien Stücken in den inländischen Rechtskreis begeben hat, um sich dort dauerhaft niederzulassen. Er ist somit nicht so schutzwürdig wie ein nur für kurze Zeit seine Dienste Anbietender. Er ist mehr als Inländer zu behandeln und hat somit die nationalen Vorschriften zu beachten. Das Beschränkungsverbot ist insoweit schwächer als

---

[1094] Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444.

[1095] Vgl. hierzu oben unter B. 1. Teil. III. 1. c. cc. (1).

dies bei der Dienstleistungsfreiheit der Fall ist,[1096] was bei der Verhältnismäßigkeitsprüfung berücksichtigt werden muss. Die Sperrmaßnahmen sind geeignet, den Nutzer vor rechtswidrigen Inhalten zu schützen. Auch der Staat erfährt hierdurch Schutz, da der illegale Inhalt nicht in das Inland eingeführt werden kann. Hinter diesen staatlichen Schutzinteressen müssen die Interessen des Access-Providers, seine Dienste dem Content-Provider und dem Nutzer uneingeschränkt anbieten zu können, zurücktreten. Folglich sind die Sperrmaßnahmen aus Sicht des Access-Providers als verhältnismäßig anzusehen.[1097] Der Rechtfertigungsgrund des Art. 46 I EGV ist somit gegeben.

(cc) Ergebnis

Zwar wird in die Niederlassungsfreiheit des Access-Providers durch die staatlichen Kontrollmaßnahmen eingegriffen, dies geschieht jedoch wegen Art. 46 I EGV in zulässiger Art und Weise.

(2) Dienstleistungsfreiheit

Die Dienstleistungsfreiheit wird beim Access-Provider durch die Sperranordnungen in sämtlichen Fallvarianten (Varianten I bis III) tangiert. Zunächst, wenn es sich um einen deutschen Access-Provider sowie Nutzer handelt und sich der Content-Provider im EU-Ausland befindet. Des weiteren, wenn der Access-Provider eine natürliche oder juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland ist, wobei allein die Technik für das Access-Providing im Inland liegt. Der Nutzer ist wiederum Inländer und der Content-Provider befindet sich wie vorher im EU-Ausland. Schließlich wird die Dienstleistungsfreiheit dann beeinträchtigt, wenn der Access-Provider Deutscher, der Nutzer entweder eine natürliche Person aus dem EU-Ausland mit Wohnsitz im Inland oder eine natürliche bzw. juristische Person aus dem EU-Ausland mit Sitz im EU-Ausland und der Content-Provider erneut im EU-Ausland seine Inhalte für die Nutzer bereithält.

(a) Inländergleichbehandlung

Es wurde bereits mehrfach erwähnt,[1098] dass auch bei der Dienstleistungsfreiheit der EuGH über das bloße Diskriminierungsverbot hinausgeht und den Umfang dieser Grundfreiheit zu einem Beschränkungsverbot macht.[1099]

1096 Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 43 Rdnr. 29.

1097 Es könnte der Gedanke aufgeworfen werden, dass als schwächere Maßnahme statt der Sperrverfügung gegen den grundsätzlich nichtstörenden Access-Provider die nationale Behörde den Mitgliedstaat, auf dessen Territorium sich der Content-Provider (oder der Service-Provider) befindet, zur Sperrung oder Löschung aufgefordert wird. Vgl. hierzu ausführlich unten unter B. 3. Teil. 2. Kapitel. V. 3. g. bb. (1). (d). Diese Ansicht ist an dieser Stelle jedoch abzulehnen, da die Beeinträchtigung des Access-Providers dermaßen gering ist, so dass der staatliche Aufwand, die Sperrung bzw. Löschung über den Mitgliedstaat zu erreichen, im Vergleich viel größer und als unangemessen angesehen werden muss.

1098 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. cc. (1).

1099 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1192.

Weil der Access-Provider durch die staatlichen Sperrmaßnahmen in seinem Recht beeinträchtigt wird, seine Dienstleistungen sowohl gegenüber dem Nutzer als auch gegenüber dem Content-Provider frei erbringen zu können, liegt ein Verstoß gegen die Dienstleistungsfreiheit gemäß den Art. 49 ff. EGV vor,[1100] der nur dann als zulässig angesehen werden kann, wenn er gerechtfertigt ist.

(b) Rechtfertigung

Eine Rechtfertigung kann sich wiederum aus der vom EuGH entwickelten Schrankensystematik, also aufgrund von zwingenden Gründen des Allgemeininteresses, sowie aus den im EGV normierten Ausnahmetatbeständen der Art. 45, 46 EGV ergeben, die über Art. 55 EGV zur Anwendung kommen.

(aa)Zwingende Gründe des Allgemeininteresses

Da die Sperrmaßnahmen polizei- und sicherheitsrechtlicher Natur sind, können sie nicht unter eine der vom EuGH entwickelten Fallgruppen der zwingenden Gründe des Allgemeininteresses subsumiert werden.[1101] Diese Rechtfertigungsmöglichkeit kommt somit nicht in Betracht.

(bb)Art. 55 i.V.m. Art. 45, 46 EGV

Auch Art. 45 EGV ist nicht erfüllt, weil die Tätigkeit des Access-Providers regelmäßig nicht mit der Ausübung öffentlicher Gewalt verbunden ist.
Es könnte jedoch wiederum der Rechtfertigungstatbestand des Art. 46 I EGV einschlägig sein. Die Sperrverfügungen ergehen aus Gründen der öffentlichen Ordnung und Sicherheit. Die Tatsache, dass es sich hierbei um unterschiedslose Maßnahmen handelt, der Art. 46 I EGV aber explizit bestimmt, dass nur diskriminierende Regelungen von ihm erfasst werden sollen, ist – wie bereits an anderer Stelle ausführlich dargestellt – insoweit unerheblich.[1102] Schließlich müssen die Kontrollmaßnahmen verhältnismäßig sein: Die Sperrung ist geeignet, den Nutzer und den Staat vor den im Ausland befindlichen rechtswidrigen Inhalten zu schützen. Sie stellt – technisch gesehen – darüber hinaus die einzige mögliche Kontrollmaßnahme dar. Schon bei der vorigen Prüfung wurde zudem festgestellt, dass der Access-Provider durch die Sperranordnung nur marginal in der Ausübung des Access-Providings beeinträchtigt wird.[1103] Zwar kann der Access-Provider durch die Sperrverfügung dem Nutzer bestimmte Inhalte nicht mehr von einem Content-Provider aus dem EU-Ausland vermitteln. Auch ist er daran gehindert, für den Content-Provider die vom Nutzer abgerufenen Daten diesem zuzuleiten. Zu bedenken

---

[1100] Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444.
[1101] Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a).
[1102] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).
[1103] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 3. g. aa. (1). (b). (bb).

ist jedoch, dass – abgesehen von den gesperrten Inhalten – alle anderen Inhalte im Internet für den Nutzer zugänglich bleiben, so dass der Access-Provider insoweit seine Dienste sowohl für den Nutzer als auch für den jeweiligen Content-Provider weiter ungehindert ausführen kann. Da es im Internet eine Unmenge an frei zugänglichen Inhalten gibt, auf die der Nutzer mit Hilfe des Access-Providers in unbedenklicher Form Zugriff nehmen kann, spielt die Tatsache, dass der Access-Provider hinsichtlich des gesperrten Inhalts sowohl für den Nutzer als auch für den störenden Content-Provider nicht mehr tätig werden darf, insgesamt keine Rolle.[1104] Deshalb wiegen die staatlichen Interessen, sich und die Nutzer vor den ungewünschten rechtswidrigen Inhalten zu schützen, stärker. Die Sperrmaßnahmen sind somit aus Sicht des Access-Providers als verhältnismäßig anzusehen.
Art. 46 I EGV ist demnach erfüllt.

(c) Ergebnis

Zwar verstoßen die Sperrmaßnahmen gegen die Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV. Die staatlichen Kontrollmaßnahmen sind jedoch gemäß dem Art. 46 I EGV i.V.m. Art. 55 EGV gerechtfertigt und damit zulässig.

(3) Zwischenergebnis

Obwohl durch die staatlichen Sperrverfügungen in die Niederlassungsfreiheit und Dienstleistungsfreiheit eingegriffen wird, ergibt sich hieraus kein Verstoß gegen das Europarecht, da jedes Mal ein Rechtfertigungsgrund vorliegt.

bb. Sicht des Content-Providers

(1) Warenverkehrsfreiheit

Die Warenverkehrsfreiheit wird unter bestimmten Umständen beim Content-Provider gemäß der oben angestellten Prüfung[1105] in allen Fallvarianten und in sämtlichen Unterkonstellationen tangiert. So erfolgt ein Eingriff in die Warenverkehrsfreiheit, wenn es sich um einen deutschen Access-Provider, einen deutschen Nutzer und den Content-Provider aus dem EU-Ausland handelt (Fallvariante I). Zum gleichen Ergebnis kommt man mit der Kombination des Access-Providers aus dem EU-Ausland, dem deutschen Nutzer sowie dem Content-Provider aus dem EU-Ausland (Fallvariante II). Auch das Zusammentreffen eines deutschen Access-Provider und eines Nutzers aus dem EU-Ausland mit dem Content-Provider aus dem EU-Ausland (Fallvariante III) ergibt eine Beeinträchtigung der Warenverkehrsfreiheit. Für diese Beeinträchtigung ist aber bei

---

[1104] Die Tatsache, dass nicht nur die rechtswidrigen, sondern auch rechtmäßige Inhalte des gleichen oder anderer Content-Provider von den Sperrungen betroffen sind, vgl. insoweit unten unter B. 3. Teil. 2. Kapitel. V. 3. g. bb. (1). (d)., ändert hieran nichts. Es geht an dieser Stelle einzig und allein um die Perspektive des Access-Providers.

[1105] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 3. b. bis d.

allen Fallvarianten gleichermaßen erforderlich, dass der Content-Provider bestimmte Waren oder Produkte bzw. deren Werbung im Internet für den Nutzer bereithält, die von den staatlichen Sperrmaßnahmen betroffen sind.

(a) Dassonville-Formel

Da die behördlichen Kontrollverfügungen geeignet sind, den gemeinschaftlichen Warenverkehr unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern,[1106] liegt eine Maßnahme gleicher Wirkung i.S.d. Art. 28 EGV vor, so dass grundsätzlich diese Beschränkung der Warenverkehrsfreiheit nicht erlaubt ist.

(b) Keck-Formel

Die Keck-Rechtsprechung findet auf diese Kontrollmaßnahmen keine Anwendung.[1107] Die Dassonville-Formel wird hierdurch nicht eingeschränkt. Ein nach Art. 28 EGV verbotener Eingriff in die Warenverkehrsfreiheit besteht demnach weiter.

(c) Cassis-de-Dijon-Rechtsprechung

Die tatbestandsimmanente Schranke der Cassis-Formel, die einen Teil der vom EuGH aufgestellten Schrankensystematik darstellt,[1108] kommt ebenfalls nicht zum Zug. Denn die einzelnen Fallgruppen, die der EuGH als zwingende Gründe des Allgemeinwohls genannt hat,[1109] decken sich nicht mit den Gründen, wonach die zuständige Behörde die Kontrollmaßnahmen erlässt. Diese sind polizei- und sicherheitsrechtlicher Natur. Derartige Gründe hat der EuGH in seiner Rechtsprechung jedoch bis jetzt noch nicht als zwingende Gründe des Allgemeininteresses anerkannt. Solche Gründe werden nämlich explizit in den jeweiligen Ausnahmevorschriften zu den einzelnen Grundfreiheiten – bei der Warenverkehrsfreiheit in Art. 30 EGV – genannt. Insoweit ist eine richterrechtliche Schranke nicht notwendig.

(d) Rechtfertigung nach Art. 30 EGV

Gemäß Art. 30 EGV stehen Einfuhrbeschränkungen der Bestimmung des Art. 28 EGV nicht entgegen, die aus Gründen der öffentlichen Sittlichkeit, Ordnung und Sicherheit gerechtfertigt sind. Die staatlichen Sperrmaßnahmen ergehen aus Gründen der Sittlichkeit, Ordnung und Sicherheit. So soll damit versucht werden, das Inverkehrbringen von pornographischen, politisch radikalen, antidemokratischen sowie menschenverachtenden Waren oder deren Werbung hierfür zu unterbinden. Die Sperrverfügungen gegen

---

[1106] Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1116.
[1107] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (2).
[1108] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3).
[1109] Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 30 Rdnr. 188 ff.

den Access-Provider fallen somit unter die Rechtfertigungsgründe der öffentlichen Sittlichkeit, Ordnung und Sicherheit des Art. 30 EGV.[1110]

Art. 30 S. 2 EGV bestimmt weiter, dass die nationalen Beschränkungen verhältnismäßig sein müssen, damit Art. 30 EGV seine rechtfertigende Wirkung entfalten kann.[1111] Die Sperrmaßnahmen müssen also geeignet, erforderlich und angemessen sein.[1112] Die Sperranordnung ist zunächst geeignet, den Nutzer und den Staat vor rechtswidrigen Waren sowie deren Bestellangebote und Werbung zu schützen. Da die Sperrung durch den Access-Provider aus technischer Sicht das einzige Mittel ist, um auf die Verbreitung von illegalen Inhalten bei einem Content-Provider im (EU)-Ausland Einfluss zu nehmen, muss die staatliche Kontrollmaßnahme grundsätzlich auch als erforderlich angesehen werden. Ein milderes Mittel ist allein aus technischer Sicht nicht gegeben.

Anstelle einer Sperranordnung gegen den Access-Provider zu verfügen, wäre es auch möglich, dem Mitgliedstaat, auf dessen Territorium sich der rechtswidrige Inhalt des Content-Providers befindet, anzuzeigen, dass auf seinem Staatsgebiet illegale Inhalte in das Internet eingespeist werden. Mit dieser Anzeige kann zugleich die Aufforderung zur gezielten Löschung oder Sperrung des beanstandeten Inhalts verbunden werden. Ob mit diesem Gesuch um Amtshilfe[1113] bei den jeweiligen Mitgliedstaaten die mit der Sperrmaßnahme verfolgten Ziele ebenso gut erreicht werden können, muss angezweifelt werden. Häufig vergeht sehr viel Zeit zwischen der Bitte um Amtshilfe und der Ausführung durch den angerufenen Mitgliedstaat, weil damit eine große Anzahl an bürokratischen Zwischenschritten verbunden ist. In der Regel müssen die illegalen Inhalte jedoch sehr schnell gesperrt werden, damit durch sie kein weiterer Schaden entstehen kann. Deshalb erscheint die Anzeige gegenüber einem Mitgliedstaat – verbunden mit der Aufforderung zur Löschung und/oder Sperrung – als kein gleichwertiges Mittel, so dass es in den meisten Fällen eher angebracht ist, mit Hilfe des Access-Providers eine rasche Sperrung der rechtswidrigen Inhalte zu erreichen, als den langen und zeitaufwändigen Weg über die „horizontale Amtshilfe“[1114] zu beschreiten. Diese Schlussfolgerung verstößt jedoch gegen den europäischen Grundgedanken eines Europas gleichberechtigter Partnerstaaten. Denn allein wegen der zeitlich schleppenden Umsetzung von derartigen Hinweisen eines Mitgliedstaats durch einem anderen Mitgliedstaat darf eigentlich eine

---

1110 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

1111 Epiney in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 30 Rdnr. 42 ff.; Bleckmann, Europarecht, 6. Auflage, § 19 Rdnr. 1524.

1112 Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1131.

1113 Kooperations- und Rücksichtnamepflichten der Mitgliedstaaten untereinander, die sogenannte „horizontale Amtshilfe“, lassen sich nicht nur aus Art. 10 EGV herauslesen. Dass solche Pflichten existieren, ergibt sich vor allem aus Art. 11 II, III, Art. 12, Art. 19, Art. 20, Art. 23 I, Art. 34 I EUV, Art. 99 I, Art. 126 II, Art. 152 II, Art. 155 II, Art. 157 II, Art. 159 I, Art. 280 III 2 und Art. 307 II 2 EGV. Wie sich aus den Art. 29 ff. EUV bzw. aus den Art. 61 und 65 EGV herauslesen lässt, soll eine vertrauensvolle Kooperation zwischen den Mitgliedstaaten auf den Gebieten der nationalen Zivil- und Strafgerichte sowie der Verwaltung (Polizei und Staatsanwaltschaft) stattfinden.

1114 Vgl. zu diesem Begriff vorstehende Fn. 1113.

stärker eingreifende nationale Maßnahme nicht begründet werden. Vielmehr muss das Vertrauen in die jeweiligen Mitgliedstaaten und deren Behörden gestärkt werden. Demzufolge sind Hinweise gegenüber Mitgliedstaaten, bestimmte Inhalte bei den Service- oder/und Content-Providern löschen und/oder sperren zu lassen, die sich auf ihren Hoheitsgebieten befinden, als genauso effektiv anzusehen, wie dies im Inland üblich ist.[1115] Nur so lässt sich das einheitliche Haus Europa aufbauen.[1116] Je nachdem, welcher Meinung gefolgt wird, kann entweder die Erforderlichkeit der Sperrmaßnahme bejaht oder verneint werden. Allein aufgrund von Erfahrungen in der Praxis müssten die staatlichen Sperrmaßnahmen als erforderlich angesehen werden.[1117] Will man jedoch den EGV und den europäischen Gedanken ernst nehmen, so wäre die Erforderlichkeit abzulehnen.
Abgesehen von diesem Streitpunkt ist aber auch noch fraglich, ob die Sperranordnung für angemessen erklärt werden kann. Denn aufgrund der eingeschränkten technischen Möglichkeiten[1118] wird sich eine Sperrung im Internet nur über die IP-Adresse des betroffenen Systems realisieren lassen. Dies hat jedoch zur Folge, dass nicht nur gezielt der rechtswidrige Inhalt, sondern auch völlig legale Inhalte auf dem betroffenen Server für den Nutzer gesperrt werden. Es sind also neben dem rechtswidrigen Inhalt des Content-Providers möglicherweise noch seine rechtmäßigen Inhalte sowie weitere Content-Provider, die legale Inhalte für Waren im Internet bereithalten, von der staatlichen Maßnahme betroffen.[1119] Des weiteren muss beachtet werden, dass im Europarecht, speziell bei der Grundfreiheit des Art. 28 EGV, das – bereits weiter oben angesprochene – „Herkunftslandprinzip“[1120] gilt.[1121] Danach soll jeder Mitgliedstaat das als rechtmäßig

---

[1115] Allein schon die europaweit gleichwertige Anerkennung von universitären Abschlüssen hat sehr lange gedauert. Mittlerweile gibt es aber, vor allem durch die Rechtsprechung des EuGH, immer mehr Fälle, in denen das Prinzip gilt, dass behördliches Tätigwerden anderer Mitgliedstaaten genauso ernst zu nehmen ist wie das Handeln der eigenen Behörden. Dass dies der Praxis nicht immer entspricht, ist selbstverständlich. Aber nur wenn sich diese Haltung durchsetzt, hat die EU die Möglichkeit, dass die Mitgliedstaaten über die Grenzen hinweg zur Zusammenarbeit bereit sind. Ansonsten werden sich die einzelnen Mitgliedstaaten auch weiterhin auf ihren gewohnten Behördenapparat verlassen und ein europäisches Zusammenwachsen bleibt auf Dauer behindert.

[1116] Vgl. zu diesem Gedanken auch Art. 3 ECRL.

[1117] Eine andere Ansicht kann hier durchaus vertreten werden. Vor allem die europafreundlichen Gedanken des „effet utile“ sowie des Herkunftslandsprinzips können eine andere Meinung begründen. Denn nur wenn zwischen den einzelnen Mitgliedstaaten auch auf polizeilicher Ebene effektiv und vertrauensvoll zusammengearbeitet werden kann, rückt das Ziel eines einheitlichen Europas ein Stückchen näher.

[1118] Vgl. insoweit oben unter B. 1. Teil. III. 1. c. cc. (1). und d.

[1119] Darüber hinaus geben Koenig/Loetz in: „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444 zu bedenken, dass – wie bereits oben aufgezeigt – bei rechtswidrigen Warenangeboten sowie Werbung hierfür, die sich auf inländischen Servern befinden, gegen den Content- oder Service-Provider direkt von Seiten der nationalen Behörden mit Sperr- und/oder Löschanordnungen vorgegangen wird. Von den Sperranordnungen werden demnach vor allem ausländische Server betroffen. Faktisch führt dies dazu, dass Sperranordnungen nicht nur eine beschränkende, sondern eine diskriminierende Wirkung haben. Tatsächlicher Anknüpfungspunkt für eine Sperrung ist nicht nur das Vorliegen eines rechtswidrigen Inhalts, sondern auch der Standort des Rechners außerhalb des deutschen Hoheitsgebiets. Eine solche Diskriminierung der Content-Provider im EU-Ausland lässt sich deshalb kaum noch rechtfertigen.

[1120] Vgl. oben unter B. 3. Teil. 2. Kapitel. IV. 1. b. und unter B. 3. Teil. 3. Kapitel. II. 1. b. aa.

ansehen, was in einem anderen Mitgliedstaat erlaubt ist.[1122] Sofern ein Content-Provider in einem anderen Mitgliedstaat der EU ungehindert seinen – aus unserer Sicht rechtswidrigen – Inhalt im Internet für den Nutzer bereithalten darf, müsste dies eigentlich wegen des Herkunftslandprinzips akzeptiert werden. Lediglich bei krassen illegalen Inhalten, die offensichtlich von keinem Mitgliedstaat geduldet würden, könnte weiterhin eine Sperrung durch den inländischen Access-Provider erfolgen. Somit wird hier möglicherweise gegen das Herkunftslandprinzip verstoßen und damit unzulässig in die fremde Staatshoheit eines Mitgliedstaates eingegriffen. Der Content-Provider besitzt darüber hinaus aufgrund der EMRK und der EGRC berechtigte Interessen, seine Inhalte im Netz frei für jedermann anbieten zu können. Diese Interessen werden sowohl durch Art. 10 EMRK als auch durch Art. 11 EGRC geschützt. Da die Beschränkungsmöglichkeiten der Grundfreiheiten gerade bei der Frage der Verhältnismäßigkeit im Lichte des gemeinschaftlichen Grundrechtsstandards unter Einbeziehung der EMRK sowie EGRC auszulegen sind,[1123] spielt dieser Punkt hier eine gewichtige Rolle.
Aus diesen angeführten Gründen und dabei insbesondere dem Aspekt, dass häufig mit einer Sperrung eine Beeinträchtigung von weiteren, rechtmäßigen Inhalten – möglicherweise unterschiedlicher Content-Provider – verbunden ist, dürfte es nicht angemessen sein, Sperrmaßnahmen gegen den Access-Provider zu verfügen, wodurch der Content-Provider in seiner Warenverkehrsfreiheit derart beeinträchtigt wird.[1124] Die Frage, ob die Sperranordnungen schon wegen einer fehlenden Erforderlichkeit als unverhältnismäßig anzusehen sind, braucht somit nicht entschieden zu werden, da zumindest die Angemessenheit zu verneinen ist und demzufolge die Sperrmaßnahmen insgesamt nicht verhältnismäßig sind.
Eine Rechtfertigung nach Art. 30 EGV ist somit nicht gegeben.

(e) Ergebnis

Die Sperrmaßnahmen verstoßen aus der Sicht des Content-Providers gegen die Warenverkehrsfreiheit. Sie sind auch nicht nach Art. 30 EGV gerechtfertigt. Deshalb ist das Europarecht diesbezüglich verletzt.

(2) Dienstleistungsfreiheit

Parallel zur Warenverkehrsfreiheit ist die Dienstleistungsfreiheit aus der Perspektive des Content-Providers in sämtlichen Fallvarianten und –konstellationen betroffen. Erstens:

1121 Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr", K&R Beilage 1 zu Heft 12/2001 S. 9.

1122 Vgl. hierzu auch die Ausführungen zur E-Commerce-Richtlinie und dem Herkunftslandprinzip, oben unter B. 3. Teil. 2. Kapitel. IV. 1. b. sowie Art. 3 ECRL.

1123 Herdegen, Europarecht, 2. Auflage, § 15 Rdnr. 283.

1124 A.A. jedoch Holznagel in: „Verantwortlichkeit im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte", ZUM 2000, 1007, 1023, der zumindest für den Fall einer Sperrung von 282 Newsgroups (vgl. CompuServe-Fall) dem Ziel einer Verhinderung der Kinderpornographie den Vorzug geben will.

Ein deutscher Access-Provider, ein deutscher Nutzer und der Content-Provider im EU-Ausland (Fallvariante I); zweitens: Ein Access-Provider aus dem EU-Ausland, ein deutsche Nutzer und wiederum der Content-Provider im EU-Ausland (Fallvariante II); drittens: Ein deutsche Access-Provider, ein Nutzer aus dem EU-Ausland und der Content-Provider im EU-Ausland (Fallvariante III).

(a) Inländergleichbehandlung

Bereits mehrfach wurde an obiger Stelle der Umstand angesprochen, dass der Umfang der Dienstleistungsfreiheit i.S.d. Art. 49 ff. EGV von einem reinen Diskriminierungsverbot zu einem allgemeinen Beschränkungsverbot gewachsen ist.[1125] Nach Art. 49 I EGV sind deshalb die Beeinträchtigungen, die beim Content-Provider durch die gegenüber dem Access-Provider verfügten staatlichen Sperrmaßnahmen hervorgerufen werden, grundsätzlich verboten. Eine Zulässigkeit der Sperranordnungen ist nur dann gegeben, wenn sie gerechtfertigt sind.

(b) Rechtfertigung

Eine Rechtfertigung kann sich entweder aus der vom EuGH entwickelten Schrankensystematik der zwingenden Gründe des Allgemeinwohls sowie aus den Art. 45, 46 EGV, die über Art. 55 EGV zur Anwendung kommen, ergeben.

(aa)Zwingende Gründe des Allgemeininteresses

Dadurch dass die Sperrverfügungen aus polizei- und sicherheitsrechtlichen Gründen ergehen, können sie nicht unter eine der vom EuGH aufgestellten Fallgruppen subsumiert werden.[1126] Eine Rechtfertigung wegen zwingender Gründe des Allgemeininteresses kommt somit nicht in Betracht.

(bb)Art. 55 i.V.m. Art. 45, 46 EGV

Art. 45 EGV ist nicht einschlägig, weil die Tätigkeit des Content-Providers in der Regel nicht mit der Ausübung öffentlicher Gewalt verbunden ist.
Es besteht jedoch auch hier die Möglichkeit, dass die Sperranordnungen aus Gründen der öffentlichen Ordnung und Sicherheit gemäß Art. 46 EGV gerechtfertigt sind. Die Tatsache, dass Art. 46 EGV in seinem Wortlaut lediglich von Sonderregelungen für Ausländer spricht, ist ohne Bedeutung. Mittlerweile wird anerkannt, dass Art. 46 I EGV auch für unterschiedslose nationale Maßnahmen gilt.[1127]
Die behördlichen Kontrollmaßnahmen ergehen aus Gründen der öffentlichen Sicherheit und Ordnung. Obwohl die in Art. 46 I EGV genannten Begriffe europarechtlich auszulegen sind, können die aufgrund des Polizei- und Sicherheitsrechts ergehenden Sperran-

---

[1125] Herdegen, Europarecht, 2. Auflage, § 17 Rdnr. 319.
[1126] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a).
[1127] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. bb. (2). (b).

ordnungen hierunter subsumiert werden. Denn diese Begriffe unterscheiden sich nur unwesentlich von den nationalen Begriffen der polizei- und sicherheitsrechtlichen Regelungen.[1128] Somit findet Art. 46 I EGV auf diese Maßnahmen Anwendung. Darüber hinaus muss aber noch der in Art. 46 I EGV nicht genannte Rechtsgrundsatz der Verhältnismäßigkeit als ungeschriebenes Tatbestandsmerkmal des Art. 46 I EGV erfüllt sein, damit diese Schranke rechtfertigende Wirkung entfalten kann.[1129] Es ist also nötig, dass die Sperranordnungen geeignet, erforderlich und angemessen sind. Hierzu gilt das oben bei der Warenverkehrsfreiheit Gesagte:[1130] Zwar sind die Sperrmaßnahmen geeignet, die von der Behörde verfolgten Ziele zumindest teilweise zu erreichen. Es ist aber bereits fraglich, ob die Sperranordnungen als erforderliches Mittel gegen den im Ausland befindlichen, rechtswidrigen Inhalt anzusehen sind.[1131] Zumindest sind in jedem Fall die Kontrollmaßnahmen letztendlich nicht angemessen und somit unverhältnismäßig:

Durch die gegen den Access-Provider verfügten Sperranordnungen werden in der Regel zu viele geschützte Interessen des Content-Providers sowie (eventuell) der übrigen Internetteilnehmer verletzt. So ist es technisch nicht möglich, gezielt nur den illegalen Inhalt sperren zu lassen. Das heißt, dass auch rechtmäßige Inhalte desselben oder anderer Content-Provider für den Nutzer nicht mehr zugänglich sind. Damit werden nicht nur die wirtschaftlichen Interessen der anbietenden Content-Provider verletzt, sondern auch das Recht auf Information, die erlaubten Daten dem Nutzer frei zugänglich anzubieten, ist von den staatlichen Maßnahmen tangiert. Das Recht auf informationelle Selbstbestimmung ist ein elementares Grundrecht und wird durch Art. 10 EMRK bzw. Art. 11 EGRC ausdrücklich geschützt.[1132] Dieses Recht auf informationelle Selbstbestimmung muss bei der Interessenabwägung im Rahmen der Verhältnismäßigkeitsprüfung ebenfalls Berücksichtigung finden.[1133] Demnach werden durch die Sperrungsanordnungen zum einen die wirtschaftlichen Interessen des Content-Providers tangiert, seine Dienste im Internet bereitzuhalten. Zum anderen ist aber auch der Gedanke des „Free Flow of Information“[1134] in Form der Art. 10 EMRK und Art. 11 EGRC zu be-

---

[1128] Troberg in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Art. 56 Rdnr. 10.

[1129] Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 120.

[1130] Siehe oben unter B. 3. Teil. 2. Kapitel. V. 1. g. bb. (1). (d).

[1131] Vgl. die Überlegungen bei B. 3. Teil. 2. Kapitel. V. 3. g. bb. (1). (d).

[1132] Natürlich wird im Gegenzug auch das Recht auf informationelle Selbstbestimmung seitens des Nutzers verletzt. Auch sein Interesse an den frei zugänglichen, rechtmäßigen Daten wird beeinträchtigt. Da in dieser Arbeit lediglich die einzelnen Provider, die – wirtschaftlich gesehen – die weitaus größere Rolle spielen, betrachtet werden sollen, kann diese Problematik nur am Rande aufgezeigt werden. Dieser Aspekt spricht jedenfalls außerdem dafür, dass die Sperranordnungen für unverhältnismäßig erklärt werden müssen.

[1133] Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 255; Stock, „EU-Medienfreiheit – Kommunikationsgrundrecht oder Unternehmerfreiheit?“, K&R 2001, 289, 294.

[1134] Vgl. zu diesem Begriff oben unter B. 2. Teil. I. sowie Mayer, Das Internet im öffentlichen Recht, S. 112.

achten. Schon allein deswegen müssen die Interessen des Staates, sich und den Nutzer vor einem häufig eher geringen rechtswidrigen Teil des gesperrten Inhalts zu schützen, hinter den gewichtigeren Interessen der Content-Provider zurücktreten.[1135] Da ferner durch die Sperranordnungen möglicherweise gegen Hoheitsrechte der Mitgliedstaaten und gegen das Herkunftslandsprinzip verstoßen wird[1136] und ein Service-Provider, der sämtliche Inhalte für die einzelnen Content-Provider speichert, ebenfalls von der Sperrmaßnahme betroffen sein kann,[1137] sind diese Kontrollmaßnahmen als unangemessen und daher als unverhältnismäßig anzusehen.[1138] Dieses Ergebnis wird zudem durch die Tatsache gestützt, dass es sich bei Art. 46 I EGV um eine eng auszulegende Ausnahmevorschrift handelt[1139] und dieser Grundsatz vor allem in Fällen der Beschränkung von Korrespondenzdienstleistungen angewendet werden soll,[1140] die grundsätzlich bei Internet-Dienstleistungen vorliegen.[1141]
Der Rechtfertigungsgrund des Art. 46 EGV i.V.m. Art. 55 EGV ist somit wegen fehlender Verhältnismäßigkeit nicht erfüllt.

(c) Ergebnis

Der Content-Provider wird in seinem nach den Art. 49 ff. EGV garantierten Recht auf Dienstleistungsfreiheit durch die gegen den Access-Provider gerichteten Sperrmaßnahmen verletzt. Rechtfertigungsgründe sind nicht gegeben, so dass gegen Europarecht in unrechtmäßiger Weise verstoßen wird.

(3) Zwischenergebnis

Aus der Sicht des Content-Providers wird durch die staatlichen Sperrverfügungen sowohl in seine Warenverkehrsfreiheit als auch Dienstleistungsfreiheit in unzulässiger

---

1135 A.A. denkbar. Insbesondere dann, wenn ein großer Anteil der von der Sperrung betroffenen Inhalte als rechtswidrig anzusehen sind.

1136 EuGH, Rs. 279/80, 17.12.1981, Slg. 1981, 3305, 3325 Rdnr. 19 (Webb).

1137 Auf diesen Spezialfall, dass der Content-Provider im EU-Ausland seinen Inhalt mit Hilfe eines Service-Providers in das Internet einstellt, wurde nicht mehr in den obigen Fallvarianten und –konstellationen eingegangen, da sonst die Übersichtlichkeit hierunter zu sehr gelitten hätte. Sicherlich sind aber derartige Fälle denkbar. Dann wäre der Service-Provider durch die gegen den Access-Provider gerichteten Sperrmaßnahmen ebenfalls in seiner Dienstleistungsfreiheit beeinträchtigt. Vgl. hierzu Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444, die diesen Fall ebenfalls kurz erwähnen. Letztendlich ergibt sich hieraus nichts Neues. Denn in diesem Fall wird nur ein weiterer Dienstleister dazwischen geschaltet. Wie dieser Service-Provider in welche Grundfreiheiten verletzt wird, wurde bereits an obiger Stelle ausführlich behandelt, so dass auch diese Fallvariante mit den schon aufgezeigten Fallkombinationen zufriedenstellend gelöst werden kann.

1138 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 3. g. bb. (1). (d).

1139 Bröhmer in: Calliess/Ruffert (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Art. 46 Rdnr. 1.

1140 EuGH, Rs. C-76/90, 25.07.1991, Slg. 1991, I-4221, 4243 Rdnr. 13 (Säger); Hailbronner in: Hailbronner/Klein/Magiera/Müller-Graff, Handkommentar zum Vertrag über die Europäische Union (EUV/EGV), Art. 60 Rdnr. 29a.

1141 Siehe insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (3).

Weise eingegriffen. Insoweit sind diese Kontrollmaßnahmen als europarechtswidrig zu werten.

4. Kontrollmaßnahmen gegen den Network-Provider

Wie bereits oben erwähnt,[1142] können gegen den Network-Provider direkt keine staatlichen Kontrollmaßnahmen ergehen, da er auf den Datentransport keinen Einfluss nehmen kann.[1143] Denn der Network-Provider stellt lediglich die Transportwege für den Datenfluss zur Verfügung. Während des Transports ist aber ein gezieltes Eingreifen auf bestimmte, unerwünschte Inhalte im Internet nicht möglich.[1144] Deshalb wäre es unsinnig, gegen den Network-Provider behördliche Kontrollmaßnahmen zu verfügen. Die Prüfung einer Vereinbarkeit von staatlichen Kontrollmaßnahmen gegenüber dem Network-Provider mit dem Europarecht ist somit obsolet.

Gleichwohl spielt der Network-Provider eine europarechtlich relevante Rolle. So stellt das Network-Providing genauso wie das Access-, Content- oder Service-Providing eine Dienstleistung dar.[1145] Unter bestimmten Umständen kann deshalb mittelbar die Dienstleistungsfreiheit der Art. 49 ff. EGV zur Anwendung kommen. Zu denken wäre beispielsweise an Fälle, wo Inhalte im Netz beim Content-Provider gelöscht bzw. gesperrt werden oder der Access-Provider daran gehindert wird, dem Nutzer den Zugang zu bestimmten Inhalten zu vermitteln. Durch solche staatlichen Maßnahmen kann zugleich auch der Network-Provider betroffen sein. Denn seine Dienstleistung, die Nutzung der Übertragungswege, würde nur noch eingeschränkt in Anspruch genommen werden können.

Der Network-Provider ist jedoch bewusst bei den oben dargestellten Fallvarianten nicht einbezogen worden. Zum einen wäre die Prüfung noch komplizierter geworden, so dass eine übersichtliche Darstellung nicht mehr machbar gewesen wäre. Zum anderen gibt es einen viel wichtigeren Grund aus der Praxis: Der Access-Provider hat häufig mit dem Network-Provider vertraglich vereinbart, dass er dessen Übertragungswege gegen eine entsprechende Gebühr nutzen darf. Dieses Nutzungsrecht stellt einen wesentlichen Bestandteil vom Leistungsangebot des Access-Providers dar. Folglich bietet der Access-Provider dem Nutzer neben dem reinen Access-Providing zugleich auch das Network-Providing an.[1146] Indem an obiger Stelle das Access-Providing ausführlich geprüft worden ist, wurde somit gleichzeitig inzident auch das Network-Providing mitbehandelt.

[1142] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. III. 1.

[1143] König/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 439.

[1144] Wischmann, „Rechtsnatur des Access-Providing“, MMR 2000, 461.

[1145] König/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444.

[1146] Vgl. hierzu die Ausführungen bei Hoeren, „Vorschlag für eine EU-Richtlinie über E-Commerce“, MMR 1999, 192, 194.

Denn jedes Mal, wenn der Access-Provider durch staatliche Kontrollmaßnahmen in seinen Grundfreiheiten verletzt wird, dann könnte genauso gut der Network-Provider hinzugedacht werden. Bei einer separaten Prüfung des Network-Providings im Rahmen der einzeln untersuchten Fallvarianten sind daher neue Erkenntnisse nicht zu erwarten. Folglich war es sinnvoll, eine eigene Prüfung des Network-Providers außer acht zu lassen und ihn lediglich bei der europarechtlichen Betrachtung der Fallvarianten des Access-Providers inzident zu berücksichtigen.

5. Gesamtbetrachtung

Aus den angestellten Prüfungen ergibt sich zusammengefasst folgendes Fazit:

1. Die staatlichen Sperr- und/oder Löschmaßnahmen, die gegen den Content-Provider oder Service-Provider ergehen, stehen im Einklang mit den Grundfreiheiten des EGV.

2. Auch aus der Sicht des Access-Providers ergibt sich aus dem EGV keine Europarechtswidrigkeit, wenn die zuständige Behörde ihm gegenüber Sperrverfügungen anordnet.

3. Lediglich aus der Sicht des im EU-Ausland befindlichen Content-Providers verstoßen diese Sperranordnungen beim Access-Provider gegen die Grundfreiheiten des EGV und zwar unter bestimmten Umständen gegen die Warenverkehrsfreiheit und die Dienstleistungsfreiheit.
Wird somit beim Content- oder Service-Provider gezielt gegen rechtswidrige Inhalte vorgegangen, geschieht dies europarechtskonform. Sind hingegen durch Sperrmaßnahmen gegenüber dem Access-Provider nicht nur illegale, sondern auch rechtmäßige Inhalte, die im EU-Ausland lokalisiert sind, von den staatlichen Anordnungen betroffen, dann werden die Maßnahmen unverhältnismäßig und es wird gegen Europarecht verstoßen.[1147]

[1147] Natürlich existieren in der Praxis neben den genannten Fallbeispielen noch viel komplexere Provider-Varianten. So können manche Anbieter im Netz sowohl Content-, Service- und Access-Provider zugleich sein. Diese lassen sich dann jedoch alle unter die vorgestellten Fallvarianten einordnen, wenn strikt zwischen den einzelnen Providern getrennt wird. Aber auch Provider aus Drittstaaten können im Netz ihre Dienste anbieten. Ist dies der Fall, dann müsste weiter unterschieden werden. Auf das Europarecht haben diese Provider jedoch direkt keinen Einfluss. Deshalb wurde – wie gesagt – hierauf nicht eingegangen.

3. Kapitel: Vereinbarkeit der staatlichen Kontrollmaßnahmen mit dem sekundären Gemeinschaftsrecht

Nachdem die staatlichen Kontrollmaßnahmen in sämtlichen sinnvollen Fallvarianten anhand des primären Gemeinschaftsrechts auf ihre Vereinbarkeit mit dem Europarecht überprüft worden sind, könnte zudem noch sekundäres Gemeinschaftsrecht von den behördlichen Sperr- und/oder Löschanordnungen betroffen sein. Hierfür ist zunächst die Prüfung wichtig, ob überhaupt ein sekundäres Gemeinschaftsrecht existiert, das den Sachverhalt der staatlichen Kontrolle des Internets zumindest ansatzweise regeln soll. Gegebenenfalls ist anschließend zu klären, unter welchen Umständen das Sekundärrecht zur Anwendung kommt und welche Regelungen es für staatliche Eingriffe in das Internet bereithält.

I. Europäische Fernsehrichtlinie und ihre Novellierung 1997

In Ergänzung zur Fernsehrichtlinie vom 03.10.1989[1148] wurde eine Novellierungsrichtlinie[1149] ausgearbeitet, die zum einen die bis dahin ergangene Rechtsprechung des Europäischen Gerichtshofs (EuGH) und zum anderen die rasanten technischen Veränderungen berücksichtigte.[1150] Allerdings stellt diese neue Richtlinie klar, dass sie nicht auf das Internet angewendet werden darf.[1151] Vielmehr wird an einem engen Rundfunkbegriff festgehalten, der nur Fernsehen im herkömmlichen Sinne umfassen soll. Deshalb hat diese Richtlinie unmittelbar keine Auswirkungen auf die neuen Multimediadienste. Als einzige Ausnahme sollen aber fernsehnahe bzw. –ähnliche Dienste[1152] auch noch unter ihren Regelungsbereich fallen. Dadurch könnten sich schon in naher Zukunft Abgrenzungsschwierigkeiten und Überschneidungen zum Internet-TV ergeben.[1153]

1148 Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. IV. 1. a.

1149 Richtlinie 97/36/EG des Europäischen Parlaments und des Rates vom 30.06.1997 zur Änderung der Richtlinie 89/552/EWG zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG Nr. L 202, 60 ff.

1150 Greissinger, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie“, CR 1999, 112, 112.

1151 Eichhorn, Internet-Recht, S. 51; Lehmann, Rechtsgeschäfte im Netz – Electronic Commerce, S. 39; Mayer, Das Internet im öffentlichen Recht, S. 126.

1152 Hierzu zählen beispielsweise Pay-Per-View oder Near-Video-on-Demand.

1153 Des weiteren befasst sich die Richtlinie mit dem Teleshopping und dessen rechtlicher Behandlung. Ferner räumt die Richtlinie den Mitgliedstaaten die Möglichkeit ein, durch staatliche Maßnahmen zu verhindern, dass Ereignisse von erheblicher gesellschaftlicher Bedeutung (zu denken ist hier vor allem an bedeutende sportliche Ereignisse wie die Olympischen Spiele oder Weltmeisterschaften) nicht ausschließlich im „Pay-TV“ angeboten werden. Dabei dürfen die Mitgliedstaaten selbst entscheiden, wann ein derart bedeutendes Ereignis vorliegt. Das „Pay-TV“ zeichnet sich dadurch aus, dass es sich nicht durch Werbung oder durch staatliche Gebühren finanziert. Vielmehr kann Pay-TV – meistens mit einem Abonnement – bestellt werden. Gegen einen bestimmten Betrag kann dann individuell ein bestimmtes Fernsehprogramm abgerufen werden. Schließlich enthält die Richtlinie auch Regelungen zum Minderjährigenschutz. Vgl. hierzu Greissinger in: „Die EuGH-Rechtsprechung zur Fernsehrichtlinie“, CR 1999, 112, 119 ff.

Obwohl die Novellierungsrichtlinie von 1997 nicht direkt auf das Internet anwendbar ist, hat sie mittelbar Bedeutung für die neuen Multimediadienste: Da es für diese Dienste noch relativ wenig europäische Bestimmungen gibt, und wenn doch, dann nur sehr junge, kann die neue Fernsehrichtlinie, die letztlich eine ähnliche Materie regelt, zumindest als Auslegungshilfe dienen. Weil das Fernsehen bereits seit über zehn Jahren europäisch genormt wird, bestehen genügend Anhaltspunkte, die auch auf das Internet – vielleicht leicht modifiziert – übertragen werden können.

II. E-Commerce-Richtlinie

Im Gegensatz zur Fernsehrichtlinie könnte jedoch die am 17.07.2000 veröffentlichte E-Commerce-Richtlinie[1154] für vorliegende Arbeit von großem Interesse sein. Allerdings entfaltet die Richtlinie nicht wie die Verordnung eine direkte Rechtswirkung auf nationaler Ebene, sondern wird rechtlich erst von Bedeutung, wenn sie von den Mitgliedstaaten umgesetzt worden ist.[1155] Hierfür hatten die Mitgliedstaaten gemäß Art. 22 ECRL bis zum 17.01.2002 Zeit.[1156] Die Bundesrepublik Deutschland hat die E-Commerce-Richtlinie mittlerweile umgesetzt. Dies geschah vor allem durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG).[1157]
Durch die Umsetzung der Richtlinie in nationales Recht hat sie nun innerhalb des nationalen Rechtsbereichs gemeinschaftsrechtliche Wirkung.[1158] Der Umstand, dass die Richtlinie umgesetzt worden ist, hat jedoch nicht zur Folge, dass sie obsolet geworden ist. Vielmehr bleibt die Richtlinie trotz ihrer Umsetzung weiterhin bestehen. Dies ergibt sich aus dem europarechtlichen Grundprinzip, dass im Hoheitsbereich der EU-Mitgliedstaaten zwei Rechtsordnungen nebeneinander und unabhängig voneinander existent und anwendbar sind: das nationale Recht und das Gemeinschaftsrecht.[1159] Daraus folgt, dass die Richtlinie in der Bundesrepublik Deutschland auch nach der Umsetzung nicht nur als nationales Recht, sondern ebenfalls als sekundäres Europarecht zu beachten ist. Schon allein aufgrund der Tatsache, dass alle rechtlichen Begriffe in den nationalen Regelungen, da es sich um Europarecht handelt, anhand der Richtlinie auszulegen sind,[1160] bleibt sie bedeutsam. Aber auch wegen des Anwendungsvorrangs[1161], der

---

1154 RL 2000/31/EG des Europäischen Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. EG Nr. L 178, 1 ff. vom 17.07.2000.

1155 Herdegen, Europarecht, 2. Auflage, § 9 Rdnr. 176 f.; vor Ablauf der Umsetzungsfrist besteht für die Mitgliedstaaten grundsätzlich nur eine Verpflichtung, den Richtlinienzweck nicht zu gefährden. Vgl. EuGH, Rs. C-129/96, 18.12.1997, Slg. I-7411, 7443 ff. Rdnr. 39 ff. (Inter-Environnement Wallonie).

1156 Bezüglich ihrer Umsetzung vgl. Härting, „Gesetzentwurf zur Umsetzung der E-Commerce-Richtlinie", CR 2001, 271 ff.

1157 Vgl. hierzu: Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr", K&R Beilage 1 zu Heft 12/2001, 1, 2 f.

1158 Oppermann, Europarecht, § 6 Rdnr. 465.

1159 Fischer, Europarecht in der Verwaltung, S. 100.

1160 Arndt, Europarecht, S. 72 f.

insbesondere bei Umsetzungsfehlern eingreift, ist es notwendig, dass die Richtlinie trotz ihrer Umsetzung in nationales Recht entscheidend weiter wirkt. Deshalb wird im folgenden nicht das nationale Recht betrachtet, sondern allein die Richtlinie. Wenn auf bestimmte Artikel in der Richtlinie näher eingegangen wird, soll aber nicht vergessen werden, dass diese Vorschriften – vielleicht in abgewandelter Form – bereits auch als nationale Normen vorliegen.[1162]

Da die E-Commerce-Richtlinie möglicherweise Regelungen enthält, die für die zu untersuchenden staatlichen Kontrollmaßnahmen relevant sein können und ein großer Teil des oben bei den jeweiligen Providern angewendeten Primärrechts durch die E-Commerce-Richtlinie ergänzt wird, ist es sinnvoll und geboten, auf diese Richtlinie ausführlicher einzugehen:

1. Überblick

a. Ziele und Zweck

Im Gefolge der Globalität des Internets bestand schon sehr lange ein Harmonisierungsbedürfnis für die multimedialen Dienste. Mit der E-Commerce-Richtlinie, die auf die Art. 47 bis 66, 95 EGV gestützt wird,[1163] zielt die EU darauf ab, einen kohärenten Rechtsrahmen für den elektronischen Geschäftsverkehr zu schaffen.[1164] Welche Absichten sich hinter der E-Commerce-Richtlinie verbergen, lässt sich insbesondere aus Art. 1 ECRL sowie aus den Ziff. 1 ff. der Erwägungsgründe zu dieser Richtlinie entnehmen.[1165] Danach soll die E-Commerce-Richtlinie hauptsächlich die Dienstleistungsfreiheit der Art. 49 ff. EGV – von einigen Ausnahmen abgesehen – für die Dienste der Informationsgesellschaft in der EU durchsetzen.[1166] Die Regelung verfolgt einen querschnittartigen, sogenannten „horizontalen“[1167] Ansatz, mit der Absicht, einen Mindestrechtsrahmen auf EU-Ebene für die in Art. 2 a ECRL definierten „*Dienste der Informationsgesellschaft*“ zu schaffen. Gegenstand der Regelung sind interaktive, im Fernabsatz und auf elektronischem Wege erbrachte Dienstleistungen.

1161 Vgl. hierzu oben unter B. 3. Teil. 1. Kapitel. II. 2. d.

1162 Wenn auf bestimmte Artikel in der Richtlinie näher eingegangen wird, werden natürlich auch die hierzu ergangenen, einschlägigen nationalen Normen genannt.

1163 Hamann, Der Entwurf einer E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 290, 295; Spindler, „Verantwortlichkeit der Diensteanbieter nach dem Vorschlag einer E-Commerce-Richtlinie“, MMR 1999, 199, 200.

1164 Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252.

1165 Vgl. insoweit die Beilage in der NJW 2000, Heft 36, S. 3; darin sind sämtliche Erwägungsgründe zur E-Commerce-Richtlinie aufgeführt.

1166 Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252.

1167 Spindler, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4; Spindler, „Verantwortlichkeit der Diensteanbieter nach dem Vorschlag einer E-Commerce-Richtlinie“, MMR 1999, 199, 201.

Bevor nun auf die für vorliegende Arbeit relevanten Vorschriften eingegangen werden kann, sind zunächst die E-Commerce-Richtlinie und ihre wesentlichen Regelungen vorzustellen:[1168]

b. Wesentliche Regelungsbestandteile

aa. Allgemeine Bestimmungen (Kapitel I)

Neben der Zielsetzung der E-Commerce-Richtlinie enthält Art. 1 ECRL Fragen nach der Anwendbarkeit der Richtlinie.

Art. 2 ECRL enthält zahlreiche Begriffsbestimmungen. Für den Anwendungsbereich und die Reichweite der Richtlinie spielen insbesondere die Definitionen in Art. 2 ECRL eine zentrale Rolle. Vor allem die Begriffe „*Dienste der Informationsgesellschaft*“, „*niedergelassener Diensteanbieter*“ und „*koordinierter Bereich*“ sind dabei von großer Bedeutung:[1169]

(1) Dienste der Informationsgesellschaft

Gemäß Art. 2 a ECRL sind die „Dienste der Informationsgesellschaft“ „*Dienste im Sinne von Artikel 1 Nummer 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG*“. Das Gemeinschaftsrecht enthält bereits in der Richtlinie 98/34/EG[1170] sowie in der Richtlinie 98/84/EG[1171] eine Definition der Dienste der Informationsgesellschaft. Der Grund, den Begriff „Dienste der Informationsgesellschaft“ aus einer früheren Richtlinie zu übernehmen, besteht darin, eine einheitliche Gesetzgebung mit identischen Rechtsbegriffen aufzubauen. Dadurch wird die Gefahr einer divergierenden Auslegung desselben Begriffs verhindert.[1172] Gemäß der genannten Richtlinien umfassen die Dienste der Informationsgesellschaft alle Dienstleistungen, die in der Regel gegen Entgelt im Fernabsatz mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten auf individuellen Abruf eines Empfängers erbracht werden. Ausgangspunkt dieser Definition ist hier der Begriff „Dienst“,

---

1168 Zudem wird im Laufe der Prüfung auf gewisse Rechtsbegriffe hingewiesen, die von der Richtlinie definiert werden. Hierauf muss ebenfalls im Vorfeld eingegangen werden. Dies ist deshalb nötig, um die gesamte Richtlinie und bestimmte Teilbereiche besser verstehen zu können.

1169 Tettenborn, „E-Commerce-Richtlinie: Politische Einigung in Brüssel erzielt“, K&R 2000, 59, 60.

1170 Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.06.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. EG L 204 vom 21.07.1998, S. 37 geändert durch die Richtlinie 98/48/EG, ABl. EG L 217 vom 05.08.1998, S. 18. Diese Richtlinie in ihrer geänderten Form wird auch die „Transparenzrichtlinie“ genannt, vgl. hierzu Waldenberger in „Electronic Commerce: Der Richtlinienvorschlag der EG-Kommission“, EuZW, 1999, 296.

1171 Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20.11.1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, ABl. EG L 320 vom 28.11.1998, S. 54.

1172 Hamann, „Der Entwurf der E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290, 291.

der als Dienstleistung i.S.d. Art. 50 EGV verstanden werden muss.[1173] Nicht unter diese Definition fallen die Dienstleistungen, auf die in der Liste von Beispielen in Anhang V der Richtlinie 98/34/EG Bezug genommen wird und die ohne Verarbeitung und Speicherung von Daten erbracht werden.[1174]

Zusammenfassend lässt sich sagen, dass die Dienste der Informationsgesellschaft lediglich die Online-Geschäfte, nicht jedoch den Abschluss und die Abwicklung von Offline-Geschäften erfassen. So fallen der Transport oder die Versendung von im Internet bestellter Ware nicht mehr unter die Dienste der Informationsgesellschaft. Ähnlich wie bei der Dienstleistungsfreiheit[1175] kann die Vergütung für Dienste auch von Dritten geleistet werden, um das Kriterium der Entgeltlichkeit zu erfüllen.[1176] Die einzelnen Provider sollen als Dienste der Informationsgesellschaft angesehen werden. Zwar nennt Ziff. 18 der Erwägungsgründe zur E-Commerce-Richtlinie explizit lediglich das Access-Providing und das Service-Providing als Dienste der Informationsgesellschaft. Aber auch das Content-Providing muss als Dienst der Informationsgesellschaft angesehen werden, da der Online-Verkauf von Waren, der ebenfalls gemäß Ziff. 18 der Erwägungsgründe zur E-Commerce-Richtlinie zu den Diensten der Informationsgesellschaft zu zählen ist, ein Teil des Content-Providings ausmacht.[1177] Da der Rundfunk ausdrücklich durch die E-Commerce-Richtlinie ausgeschlossen wird, schließt sie begrifflich die Lücke zur Fernsehrichtlinie, aus deren Anwendungsbereich wiederum die Kommunikationsdienste auf individuellen Abruf herausfallen.[1178] Point-to-Point-Übermittlungen sind zwar grundsätzlich Dienste der Informationsgesellschaft, allerdings wird klargestellt, dass die reine Nutzer-Nutzer-Ebene, wie der Austausch elektronischer Post zwischen zwei natürlichen Personen außerhalb ihrer gewerblichen oder beruflichen Tätigkeit, kein Dienst der Informationsgesellschaft ist.[1179] Auch Tätigkeiten, die normalerweise vor Ort, aber mit Hilfe der modernen Elektronik jetzt aus der Ferne durchgeführt werden können, sollen nicht als Dienste der Informationsgesellschaft angesehen werden. Immanent ist jedoch allen diesen Diensten der Informationsgesellschaft, dass es sich um eine wirtschaftliche Tätigkeit handelt.

1173 Maennel in: Ehlers/Wolffgang/Pünder (Hrsg.), Rechtsfragen des Electronic Commerce, S. 34.

1174 Ziff. 18 der Erwägungsgründe zur E-Commerce-Richtlinie nennt ausführlich die Dienste, die unter den Begriff der Dienste der Informationsgesellschaft fallen sollen.

1175 Siehe oben bei B. 3. Teil. 2. Kapitel. V. 1. b. aa. (3).

1176 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 188.

1177 Vgl. Ziff. 18 der Erwägungsgründe zur E-Commerce-Richtlinie; unter die Dienste, die Informationen über ein Kommunikationsnetz übermitteln, kann sicherlich auch der Network-Provider gefasst werden. Da gegen ihn jedoch aus bekannten technischen Gründen, vgl. insoweit oben unter B. 1. Teil. III., keine Sperr- geschweige denn Löschanordnungen ergehen können, soll er hier nur am Rande erwähnt werden.

1178 Hamann, „Der Entwurf der E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290, 293.

1179 Tettenborn, „E-Commerce-Richtlinie: Politische Einigung in Brüssel erzielt“, K&R 2000, 59, 61.

(2) Niedergelassener Diensteanbieter

Nach Art. 2 c ECRL ist ein „niedergelassener Diensteanbieter“ „*ein Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit eine Wirtschaftstätigkeit tatsächlich ausübt; Vorhandensein und Nutzung technischer Mittel und Technologien, die zum Anbieten des Dienstes erforderlich sind, begründen allein keine Niederlassung*“.[1180] Aus Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie lässt sich entnehmen, dass die Bestimmung des Ortes der Niederlassung der Anbieter gemäß den in der Rechtsprechung des EuGH entwickelten Kriterien zu erfolgen hat. Ist ein Anbieter an mehreren Orten niedergelassen, muss bestimmt werden, von welchem Niederlassungsort aus der betreffende Dienst erbracht wird. Sofern es im Falle mehrerer Niederlassungsorte schwierig zu entscheiden ist, von welchem Ort aus ein bestimmter Dienst erbracht wird, so soll als solcher der Ort gelten, wo sich der Mittelpunkt der Tätigkeiten des Anbieters in bezug auf diesen Dienst befindet.[1181]

Mit der Bestimmung des Orts der Niederlassung eines Providers findet zugleich die Festlegung statt, woran für die jeweiligen Regelungen angeknüpft wird. Bis jetzt wird in einzelnen Mitgliedstaaten an den Standort des Servers, in anderen an den (entweder faktischen oder satzungsmäßigen) Sitz des Unternehmens angeknüpft.[1182] Diese Rechtsunsicherheit soll nun der Art. 2 c ECRL beseitigen: Für die Niederlassung und damit für die Anknüpfung sind allein die qualitativen Kriterien der Tatsächlichkeit und der Dauerhaftigkeit der Wirtschaftstätigkeit maßgeblich. Es kommt also nicht auf formale (Briefkasten) oder technologische (Standort der technischen Geräte)[1183] Kriterien an, aufgrund derer sich die Akteure leicht jeglicher Kontrolle entziehen könnten.[1184]

(3) Koordinierter Bereich

Art. 2 h ECRL bestimmt, dass der Begriff „koordinierter Bereich“ „*die für die Anbieter von Diensten der Informationsgesellschaft und die Dienste der Informationsgesellschaft in den Rechtssystemen der Mitgliedstaaten festgelegten Anforderungen, ungeachtet der Frage, ob sie allgemeiner Art oder speziell für sie bestimmt sind*“ bezeichnet.

Der Begriff des koordinierten Bereichs hat vor allem Bedeutung für das Herkunftslandprinzip[1185]. Der koordinierte Bereich bestimmt dabei die Reichweite des Herkunftsland-

---

1180 Eine inhaltsgleiche Definition ist nun nach Umsetzung der Richtlinie in § 3 Nr. 6 TDG n.F. zu finden.

1181 Vgl. Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie.

1182 Hier kommt es darauf an, welcher Theorie gefolgt wird, die der Sitz- oder Gründungstheorie. Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. IV. 2.

1183 Wie bereits an obiger Stelle mehrmals darauf hingewiesen wurde, macht Art. 2 c 2. HS ECRL explizit klar, dass die Technik zum Anbieten der Dienste nicht ausreicht, um eine Niederlassung i.S.d. Art. 43 ff EGV annehmen zu können, vgl. Kloepfer/Neun, „Rechtsfragen der europäischen Informationsgesellschaft, EuR 2000, 512, 543.

1184 Hoeren, „Vorschlag für eine EU-Richtlinie über E-Commerce“, MMR 1999, 192, 194.

1185 Vgl. hierzu oben unter B. 3. Teil. 3. Kapitel. IV. 1. b. und unten unter B. 3. Teil. 3. Kapitel. II. 1. b. aa.

prinzips. Mit seiner Hilfe soll eine Abgrenzung zur Warenverkehrsfreiheit und zu den klassischen Dienstleistungsbereichen ermöglicht werden. Wie sich aus der Vorschrift des Art. 2 h ECRL und Ziff. 21 der Erwägungsgründe zur E-Commerce-Richtlinie entnehmen lässt, umfasst der koordinierte Bereich weder Anforderungen bezüglich der Waren selbst, noch die Lieferung von Waren und Anforderungen betreffend Dienste, die nicht auf elektronischem Weg angeboten werden. Der koordinierte Bereich umfasst somit nur Anforderungen im Bezug auf Online-Tätigkeiten, nicht jedoch die Sicherheitsnormen, Kennzeichnungspflichten oder die Haftung für Waren oder Anforderungen an die Beförderung und Lieferung von Waren.[1186]

Die wohl wichtigste Regelung der E-Commerce-Richtlinie enthält Art. 3 ECRL. In ihm ist das Herkunftslandprinzip festgelegt.[1187] Das Herkunftslandprinzip ist durch die Umsetzung der E-Commerce-Richtlinie in § 4 TDG n.F. erstmalig im deutschen Rechtssystem festgeschrieben worden.[1188] Im Gegensatz zur Richtlinie wurden die im Anhang genannten Ausnahmen zu Art. 3 I und II ECRL, worauf in Art. 3 III ECRL verwiesen wird, in § 4 TDG n.F. eingearbeitet. Abgesehen von diesem formalen Unterschied hat der deutsche Gesetzgeber die Vorschrift des Art. 3 ECRL vollständig in § 4 TDG n.F. übernommen.[1189] Das Herkunftslandprinzip ist in den ersten beiden Absätzen des Art. 3 ECRL fixiert. Da auf das Herkunftslandprinzip des Art. 3 I und II ECRL bereits an früherer Stelle ausführlich eingegangen worden ist, kann insoweit nach oben verwiesen werden.[1190]
Art. 3 III ECRL befasst sich mit den Bereichen, auf die das Herkunftslandprinzip keine Anwendung finden soll, indem es auf die Ausnahmetatbestände im Anhang verweist. Wichtig ist, dass für die über Art. 3 III ECRL im Anhang genannten spezifischen Ausnahmetatbestände die E-Commerce-Richtlinie außerhalb von Art. 3 ECRL in vollem Umfang weiter anwendbar ist. Darunter fallen Bereiche wie das Urheberrecht, wofür das Schutzlandprinzip erhalten bleibt.[1191] Weitere Bereiche betreffen den Versiche-

---

[1186] In Ziff. 21 der Erwägungsgründe ist auf deutschen Wunsch die Lieferung von Humanarzneimitteln ausdrücklich aufgenommen worden. Wie die Online-Bestellung von Arzneimitteln aus einem EU-Mitgliedsstaat und deren Lieferung nach Deutschland europarechtlich zu behandeln ist, wird bei Koenig/Engelmann in: „E-Commerce mit Arzneimitteln im Europäischen Binnenmarkt und die Freiheit des Warenverkehrs“, ZUM 2001, 19 ff. ausführlich besprochen. Vgl. auch Tettenborn in: „E-Commerce-Richtlinie: Politische Einigung in Brüssel erzielt“, K&R 2000, 59, 61.

[1187] Geis, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen“, CR 1999, 772, 774; weiterführend: Ahrens, „Das Herkunftslandprinzip in der E-Commerce-Richtlinie“, CR 2000, 835 ff.

[1188] Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1, 3.

[1189] Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1, 7.

[1190] Vgl. oben unter B. 3. Teil. 2. Kapitel. IV. 1. b.

[1191] Schack, „Internationale Urheber- Marken- und Wettbewerbsrechtsverletzungen im Internet“, MMR 2000, 59, 62; vgl. zu diesem Thema auch Intveen, Internationales Urheberrecht und Internet, 1999.

rungsmarkt, der bereits intensiv durch verschiedene Richtlinien der EU reguliert ist, sowie die Ausgabe von elektronischem Geld.
Schließlich sieht Art. 3 IV bis VI ECRL eben diesen im Anhang aufgelisteten Ausnahmen eine Art Schutzklauselverfahren für bestimmte Bereiche vor, sofern ein Mitgliedstaat Vorschriften zum Schutz der öffentlichen Gesundheit und Sicherheit, insbesondere Schutz vor Rassenhass, Aufstachelung, etc., der Menschenwürde sowie der Verbraucher und Anleger erlassen oder beibehalten will.[1192]

bb. Grundsätze (Kapitel II)

Art. 4 I ECRL bestimmt, dass der Zugang zur Tätigkeit eines Anbieters von Diensten der Informationsgesellschaft nicht zulassungspflichtig ist.[1193]
Art. 5 ECRL enthält eine Reihe von Informationspflichten, die dem Nutzer helfen sollen, sich über Identität und Beschaffenheit der angebotenen Dienste der Informationsgesellschaft klar zu werden.
Die Art. 6 bis 8 ECRL befassen sich mit der kommerziellen Kommunikation, die in Art. 2 f. ECRL legaldefiniert wird.[1194]
Die Art. 9 bis 11 ECRL behandeln den Abschluss von Verträgen auf elektronischem Weg.[1195] Diese Vorschriften sind für den Geschäftsverkehr wohl am bedeutendsten, da sie den Mitgliedstaaten auferlegen, für einen anerkannten und wirksamen Abschluss elektronischer Verträge einheitliche rechtliche Rahmenbedingungen zu schaffen. Dazu gehört vor allem die einheitliche Ausgestaltung von Angebot und Annahme bei einem elektronischen Vertrag.[1196]
Art. 12 bis 15 ECRL regeln die Verantwortlichkeit der einzelnen Provider.[1197]

cc. Umsetzung (Kapitel III)

Die Art. 16 bis 20 ECRL enthalten Bestimmungen für die Umsetzung der in den vorangegangenen Kapiteln angesprochenen Regelungen.[1198]

[1192] Vgl. hierzu ausführlich: Spindler in „E-Commerce in Europa“, MMR-Beilage 7/2000, 4, 8 f.
[1193] Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 189.
[1194] Hoeren, „Vorschlag für eine EU-Richtlinie über E-Commerce“, MMR 1999, 192, 194; Tettenborn, „E-Commerce-Richtlinie: Politische Einigung in Brüssel erzielt“, K&R 2000, 59, 62.
[1195] Obwohl diese Vorschriften für den Vertragsschluss auf elektronischem Weg große Auswirkungen auf die einzelnen Rechtsgebiete der Mitgliedstaaten haben werden, sind sie für vorliegende Arbeit weitgehend uninteressant, da hiervon regelmäßig nur das Zivilrecht betroffen ist. Für staatliche Kontrollmaßnahmen spielen diese Normen keine Rolle, so dass sie hier nur – der Ordnung halber – kurz Erwähnung gefunden haben.
[1196] Vgl. zu den Regelungen der elektronischen Verträge: Tettenborn, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252, 257 f. und Hamann, „Der Entwurf der E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290, 292.
[1197] Vgl. insoweit die obigen Ausführungen unter B. 2. Teil. II. 5. b. ff. (2).
[1198] Vgl. hierzu Brisch, „EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr“, CR 1999, 235, 243 sowie Ziff. 49, 51, 52 und 54 der Erwägungsgründe zur E-Commerce-Richtlinie.

dd. Schlussbestimmungen (Kapitel IV)

Art. 21 ECRL befasst sich mit der künftigen Rolle der E-Commerce-Richtlinie. So soll ihre Anwendung regelmäßig überprüft werden. Des weiteren wird die Frage nach einer späteren Anpassung der Richtlinie im Hinblick auf die Haftung der Anbieter von Hyperlinks,[1199] von Instrumenten zur Lokalisierung von Informationen und Verfahren zur Meldung sowie Entfernung rechtswidriger Inhalte („notice and take down"-Verfahren)[1200] aufgeworfen.

Art. 22 ECRL legt die Umsetzungsfrist fest. Danach müssen die Mitgliedstaaten die E-Commerce-Richtlinie vor dem 17.01.2002 umgesetzt haben.

Gemäß Art. 23 ECRL tritt die E-Commerce-Richtlinie am Tag ihrer Veröffentlichung im Amtsblatt der Europäischen Gemeinschaften in Kraft; dies war am 17.07.2000,. Sie ist nach Art. 24 ECRL an die Mitgliedstaaten gerichtet.

ee. Anhang

Wie bereits an vorstehender Stelle erwähnt wurde, enthält der Anhang der E-Commerce-Richtlinie Ausnahmen im Rahmen von Art. 3 ECRL.

2. Auswirkungen der E-Commerce-Richtlinie auf staatliche Kontrollmaßnahmen

Nach Darstellung der E-Commerce-Richtlinie und ihrer Regelungsinhalte, stellt sich jetzt die Frage, welche Auswirkungen die Richtlinie auf die staatlichen Kontrollmaßnahmen in der Praxis hat.

Da die Art. 12 bis 15 ECRL, also die Normen zur Verantwortlichkeit, auf die verwaltungsbehördlichen Maßnahmen keine Anwendung finden[1201] und die übrigen Vorschriften aus den Kapiteln II bis IV der E-Commerce-Richtlinie für die staatlichen Sperr- und/oder Löschanordnungen – wenn überhaupt – nur von untergeordneter Bedeutung sind,[1202] ist das Hauptaugenmerk auf Art. 3 ECRL zu richten, weil er aufgrund seiner Regelungsbestandteile für die Kontrollmaßnahmen bedeutsam sein könnte. Es ist des-

---

1199 Siehe zu diesem äußerst umstrittenen Problem oben unter B. 2. Teil. II. 5. b. cc. (6).

1200 Das „notice and take down"-Verfahren umschreibt eine Maßnahme, um rechtswidrige Inhalte beim Verantwortlichen sperren bzw. löschen zu lassen. Da die E-Commerce-Richtlinie (ebenso wie § 5 TDG a.F. bzw. MDStV) Kenntnis von den rechtswidrigen Inhalten beim Service-Provider verlangt, damit er für die illegalen Inhalte verantwortlich gemacht werden kann, soll der Service-Provider durch die Behörden über bestimmte von ihm gespeicherte rechtswidrige Inhalte informiert werden. Indem er hierdurch Kenntnis erlangt, muss er nun handeln, die Inhalte also sperren oder löschen, da er nun Kenntnis von ihnen hat. Durch die behördliche Benachrichtigung (engl. notice) wird somit der Service-Provider gezwungen, die rechtswidrigen Inhalte vom Netz zu nehmen (engl. take down).

1201 Vgl. oben unter B. 2. Teil. II. 5. b. ff. (3). (b).

1202 Der Grund liegt vor allem darin, dass die übrigen Kapitel primär zivilrechtliche Regelungen sowie Verfahrensvorschriften enthalten. Die Sperr- und/oder Löschanordnungen stellen jedoch öffentlich-rechtliche Maßnahmen dar, für die lediglich das erste Kapitel der E-Commerce-Richtlinie materiell-rechtlich von Bedeutung ist.

halb zu untersuchen, inwieweit Art. 3 ECRL auf die staatlichen Lösch- und/oder Sperrmaßnahmen zur Anwendung kommen kann:

a. Art. 3 I ECRL

Gemäß Art. 3 I ECRL trägt jeder Mitgliedstaat dafür Sorge, „*dass die Dienste der Informationsgesellschaft, die von einem in seinem Hoheitsgebiet niedergelassenen Diensteanbieter erbracht werden, den in diesem Mitgliedstaat geltenden innerstaatlichen Vorschriften entsprechen, die in den koordinierten Bereich fallen*“. Was unter den europarechtlichen Rechtsbegriffen der „niedergelassenen Diensteanbieter“ und dem „koordinierten Bereich“ zu verstehen ist, wurde schon oben aufgezeigt.[1203] Auch auf die „Dienste der Informationsgesellschaft“ ist bereits ausführlich eingegangen worden.[1204]
Wie sich aus dem Wortlaut der Vorschrift des Art. 3 I ECRL ergibt, ist für jeden Diensteanbieter nur die Rechtsordnung des Staates seiner (Haupt)-Niederlassung relevant. Dies bedeutet, dass Kontrollmaßnahmen, die gegen einen im Inland niedergelassenen Provider – ganz egal ob es sich dabei um eine natürliche oder juristische Person handelt – angeordnet werden, keine europarechtliche Relevanz besitzen. Denn die Frage nach der Rechtmäßigkeit solcher Kontrollmaßnahmen ist gemäß Art. 3 I ECRL allein nach nationalem Recht zu beurteilen. Falls also eine Niederlassung des Diensteanbieters in der Bundesrepublik Deutschland bejaht werden kann, gelten für den Diensteanbieter ausschließlich diese innerstaatliche Vorschriften. Die Rechtmäßigkeit der staatlichen Kontrollmaßnahmen richtet sich nach den inländischen Vorschriften, hier speziell nach dem § 5 TDG a.F. bzw. den §§ 5, 18 MDStV sowie den jeweiligen polizei- und sicherheitsrechtlichen Vorschriften.[1205] Für die Frage, ob eine europarechtliche oder lediglich nationale Fallkonstellation besteht, kommt es demnach entscheidend darauf an, wo der Provider niedergelassen ist – im Inland oder EU-Ausland.[1206]

b. Art. 3 II ECRL

Art. 3 II ECRL regelt nun die Fälle, in denen der Diensteanbieter im EU-Ausland niedergelassen ist, die Dienste jedoch (auch) im Inland erbracht werden. Art. 3 II ECRL

[1203] Vgl. insoweit Ziff. 19 und Ziff. 21 der Erwägungsgründe zur E-Commerce-Richtlinie sowie oben unter B. 3. Teil. 3. Kapitel. II. 1. b. aa. (3).

[1204] Vgl. Ziff. 17 und 18 der Erwägungsgründe zur E-Commerce-Richtlinie sowie oben unter B. 3. Teil. 3. Kapitel. II. 1. b. aa. (1).

[1205] Nach Inkrafttreten des TDG n.F. sind für Teledienste freilich nur noch die allgemeinen Gesetze, d.h. das jeweilige Polizei- und Sicherheitsrecht, relevant.

[1206] Problematisch sind in diesem Zusammenhang die Fälle, in denen ein Anbieter an mehreren Orten niedergelassen ist. Ist dies zu bejahen, dann soll zunächst ermittelt werden, von welchem Niederlassungsort aus der betreffende Dienst erbracht wird. Ist im Falle mehrerer Niederlassungsorte schwierig zu bestimmen, von welchem Ort aus ein bestimmter Dienst erbracht wird, so gilt als solcher der Ort, an dem sich der Mittelpunkt der Tätigkeiten des Anbieters in bezug auf diesen bestimmten Dienst befindet. Vgl. Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie. Der Gedanke, der hinter diesen Erwägungsgründen steckt, ist die oben unter B. 3. Teil. 2. Kapitel. IV. 2. erwähnte Sitztheorie.

bestimmt, dass die Mitgliedstaaten den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht aus Gründen einschränken dürfen, die in den koordinierten Bereich fallen.

Dieser stellt ein allgemeines Beschränkungsverbot dar, wie es bereits in Art. 28 EGV hinsichtlich der Warenverkehrsfreiheit geregelt ist. Demnach sind sämtliche Beeinträchtigungen des freien Verkehrs von Diensten der Informationsgesellschaft aus Gründen, die in den koordinierten Bereich i.S.d. Art. 2 h ECRL fallen, unzulässig. Gemäß Art. 2 h ECRL erfasst der koordinierte Bereich „*die für die Anbieter von Diensten der Informationsgesellschaft und die Dienste der Informationsgesellschaft in den Rechtssystemen der Mitgliedstaaten festgelegten Anforderungen, ungeachtet der Frage, ob sie allgemeiner Art oder speziell für sie bestimmt sind*".[1207] Wird nun diese Definition auf den Art. 3 II ECRL übertragen, dann folgt hieraus, dass für die rechtliche Beurteilung von Online-Tätigkeiten nur noch die Rechtsordnung desjenigen Mitglied-staats maßgeblich ist, wo der Diensteanbieter seine Niederlassung i.S.d. Art. 2 c ECRL hat. Das Recht des Empfangsstaats wäre insoweit irrelevant.[1208] Dies wirft indes die Frage auf, wie das hier fixierte Herkunftslandsprinzip zu verstehen ist. Verbietet es dem Empfangsstaat generell, Maßnahmen des koordinierten Bereichs gegen Dienste der Informationsgesellschaft zu ergreifen oder darf er zwar auch weiterhin Regelungen treffen, allerdings nur unter Beachtung des Rechtssystems des Staates, woraus der Dienst stammt?

Weil Art. 3 II ECRL explizit anordnet, dass Dienste aus einem anderen Mitgliedstaat nicht aus Gründen eingeschränkt werden dürfen, die in den koordinierten Bereich fallen, kann nur die erste Möglichkeit angenommen werden. Denn Art. 3 II ECRL enthält in seinem Wortlaut keine Anhaltspunkte dafür, dass eine innerstaatliche Beschränkung der Dienste der Informationsgesellschaft aus einem anderen Mitgliedstaat dann zulässig sein soll, wenn die Rechtsordnung des anderen Mitgliedstaats beachtet wird. Dieses Ergebnis harmoniert im übrigen sehr gut mit dem Rechtsgedanken des Art. 3 I ECRL. Gemäß Art. 3 I ECRL soll jeder Mitgliedstaat dafür Sorge tragen, dass die Dienste der Informationsgesellschaft, die von einem in seinem Hoheitsgebiet niedergelassenen Diensteanbieter erbracht werden, den in diesem Mitgliedstaat geltenden innerstaatlichen Vorschriften entsprechen, die in den koordinierten Bereich fallen. Jeder Mitgliedstaat hat danach darauf zu achten, dass die Diensteanbieter, die in seinem Territorium niedergelassen sind, aus der Sicht des jeweiligen Mitgliedstaats keine rechtswidrigen Inhalte verbreiten. Das Herkunftslandprinzip beinhaltet somit auch die Verpflichtung der Mitgliedstaaten, dafür zu sorgen, dass die Diensteanbieter alle Rechtsvorschriften des Staats ihrer Niederlassung beachten.[1209] Die Verantwortung für eine Verbreitung von uner-

---

[1207] Vgl. zum Begriff des „koordinierten Bereichs" auch oben unter B. 3. Teil. 3. Kapitel. II. 1. b. aa. (3).

[1208] Spindler, „E-Commerce in Europa", MMR-Beilage 7/2000, 4, 7; er spricht in diesem Zusammenhang von einer "quantité négligeable" bezüglich des Rechts des Empfangstaates.

[1209] Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission", MMR 1999, 187, 189.

wünschten Informationen über das Internet trägt somit jeder Staat für sich und zwar im Hinblick auf die dort niedergelassenen Diensteanbieter. Jeder andere Mitgliedstaat hat dies zu akzeptieren und hat darauf zu vertrauen, dass die nationalen Kontrollorgane der einzelnen Mitgliedstaaten ähnlich ordnungsgemäß arbeiten wie die des Mitgliedsstaats selbst. Insoweit werden die Mitgliedstaaten dazu verpflichtet, die Regelungen und Standards der anderen Mitgliedstaaten gegenseitig anzuerkennen. Für den Fall, dass ein Mitgliedstaat seine Vorschriften gar nicht oder nur sehr verhalten gegenüber den Diensteanbietern durchsetzt, besteht immer noch die Möglichkeit der in Art. 19 ECRL fixierten mitgliedstaatlichen Zusammenarbeit.
Fraglich ist jedoch, ob nicht generell staatliche Kontrollmaßnahmen, die sich gegen Informationen aus einem anderen Mitgliedstaat wenden, rechtmäßig sind, sofern die Inhalte, gegen die vorgegangen werden soll, auch im Ursprungsland unzulässig wären. Dieser Gedanke ist jedoch zu verneinen. Zum einen würde hierdurch eine erhebliche Rechtsunsicherheit entstehen, da in bestimmten Grenzbereichen nicht ohne weiteres entschieden werden kann, ob ein anderer Mitgliedstaat den Inhalt nun für rechtswidrig oder zulässig erachtet. Zudem würde der Sinn und Zweck des Herkunftslandprinzips konterkariert. Sobald ein rechtswidriger Inhalt vorliegt, der auch in der Rechtsordnung des Mitgliedstaats, wo der Diensteanbieter niedergelassen ist, als unerwünscht gilt, dann muss grundsätzlich dieser Mitgliedstaat gemäß Art. 3 I ECRL für seine Sperrung und/oder Löschung sorgen.
Nach Art. 3 II ECRL ist es demnach keinem Mitgliedstaat gestattet, den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat einzuschränken. Diese Kompetenz besitzt nur der Sendestaat. Sperr- und/oder Löschanordnungen, die sich gegen Dienste aus einem anderen Mitgliedstaat richten, sind somit grundsätzlich nicht zulässig, soweit sie den koordinierten Bereich betreffen. Kontrollmaßnahmen gegen Dienste eines Providers, der im EU-Ausland niedergelassen ist, würden also in der Regel gegen Art. 3 II ECRL verstoßen und wären somit nicht mit dem sekundären Europarecht in Form der E-Commerce-Richtlinie zu vereinbaren.

c. Art. 3 III ECRL

Art. 3 III ECRL stellt aber eine Ausnahmevorschrift zum Herkunftslandprinzip dar. Demnach soll Art. 3 I und II ECRL nicht für die im Anhang genannten Bereiche gelten. Wie bereits oben teilweise erwähnt,[1210] findet das Herkunftslandprinzip auf das Urheberrecht, den Versicherungsmarkt, die Ausgabe elektronischen Geldes, vertragliche Schuldverhältnisse in Bezug auf die Verbraucherverträge, die unerbetene kommerzielle Kommunikation sowie formale Gültigkeit von auf Immobilien und verwandte Rechte bezogenen Verträge betreffend keine Anwendung. Diese Ausnahmebereiche haben jedoch regelmäßig keinen Einfluss auf staatliche Kontrollmaßnahmen. Denn diese Berei-

[1210] Siehe oben unter B. 3. Teil. 3. Kapitel. II. 1. b.

che beinhalten normalerweise keine rechtswidrigen Inhalte, gegen die von Seiten der zuständigen Behörde vorgegangen werden müsste.
Auf die staatlichen Sperr- bzw. Löschanordnungen ist demnach weiterhin das Herkunftslandprinzip des Art. 3 I und II ECRL anzuwenden, so dass sie eigentlich gegen Dienste der Informationsgesellschaft aus einem anderen Mitgliedstaat nicht ergehen dürften.

d. Art. 3 IV und V ECRL

Abweichend von Art. 3 II ECRL enthält Art. 3 IV ECRL jedoch zulässige Schutzmaßnahmen, welche die Mitgliedstaaten gegenüber einem bestimmten Dienst der Informationsgesellschaft unter gewissen Bedingungen ergreifen können. Dabei ist zu berücksichtigen, dass Art. 3 IV ECRL eine Ausnahmevorschrift von Art. 3 II ECRL ist.[1211] Folglich werden von ihr nur die staatlichen Kontrollmaßnahmen erfasst, die sich gegen Dienste „*aus einem anderen Mitgliedstaat*“ der EU richten. Die Diensteanbieter dürfen also nicht im Inland niedergelassen sein, da ansonsten keine europarechtlichen, hier die der E-Commerce-Richtlinie, sondern rein nationale Vorschriften gemäß Art. 3 I ECRL zur Anwendung kommen würden.
Art. 3 V ECRL enthält lediglich eine Ausnahmevorschrift zu dem in Art. 3 IV b ECRL genannten Verfahren.

e. Art. 3 VI ECRL

Diese Norm richtet sich nicht an die Mitgliedstaaten, sondern ausschließlich an die EU-Kommission. Sie spielt somit für die vorliegende Arbeit keine Rolle. Nach Art. 3 VI ECRL hat die Kommission innerhalb kürzester Zeit zu prüfen, ob die ihr nach Art. 3 IV b bzw. V ECRL mitgeteilten Maßnahmen mit dem Gemeinschaftsrecht vereinbar sind. Falls sie zu dem Schluss kommt, dass die Maßnahmen nicht mit dem Gemeinschaftsrecht vereinbar sind, hat sie den betreffenden Mitgliedstaat aufzufordern, von den geplanten Maßnahmen Abstand zu nehmen oder bereits ergriffene Maßnahmen unverzüglich einzustellen.

f. Zwischenergebnis

Art. 3 ECRL ist grundsätzlich – abgesehen von Art. 3 VI ECRL – auf die staatlichen Kontrollmaßnahmen anwendbar. Folglich kommen gemäß Art. 3 I ECRL auf im Inland niedergelassene Diensteanbieter zunächst nur die nationalen Vorschriften zur Anwendung. Eine Kollision mit dem Europarecht ist insoweit nicht möglich. Des weiteren wird durch Art. 3 II ECRL bestimmt, dass jegliche Kontrolle von im EU-Ausland niedergelassener Provider durch eine deutsche Behörde unzulässig ist. Demnach wären alle ge-

---

[1211] Zu beachten ist, dass Ausnahmevorschriften im Europarecht regelmäßig eng auszulegen sind; vgl. EuGH, Rs. 229/83, 10.011985, Slg. 1985, 1, 35 Rdnr. 30 (Leclerc).

gen diese Diensteanbieter gerichteten nationalen Lösch- und/oder Sperrmaßnahmen als rechtswidrig anzusehen. Allerdings besteht die Möglichkeit, dass die Ausnahmevorschrift des Art. 3 IV ECRL zur Anwendung kommt. Dann könnte eine Europarechtskonformität der Kontrollmaßnahmen doch noch erreicht werden. Dies gilt es jetzt zu untersuchen.

3. Europarechtskonformität der staatlichen Kontrollmaßnahmen gegen die einzelnen Provider

Da die Sperr- und /oder Löschanordnungen je nach Fallgestaltung an den Content-, Service- oder Access-Provider adressiert werden können, ist wieder jeder einzelne Provider, gegen den die Maßnahme in Form eines VAs ergehen kann, separat zu betrachten und die oben bei den Grundfreiheiten gewählte Prüfungsreihenfolge beizubehalten.[1212] Es werden also nacheinander die unterschiedlichen Provider[1213] betrachtet, gegen die staatliche Sperr- und/oder Löschanordnungen gerichtet sein können:

a. Kontrollmaßnahmen gegen den Content-Provider

aa. Vorüberlegungen

Wie bereits ausgeführt wurde,[1214] erfüllt der Content-Provider nur dann die Kriterien des Art. 3 II ECRL, sofern er in einem anderen Mitgliedstaat niedergelassen ist.[1215] Gemäß der Legaldefinition des Art. 2 c ECRL kann eine Niederlassung dann bejaht werden, wenn der Content-Provider mittels einer festen Einrichtung auf unbestimmte Zeit eine Wirtschaftstätigkeit tatsächlich ausübt. Diese Begriffsbestimmung des niedergelassenen Diensteanbieters ist an die Rechtsprechung des EuGH zur Niederlassung i.S.d. Art. 43 ff EGV angelehnt.[1216] Hierdurch wird erreicht, dass beide Begriffe ein und dieselbe Definition erhalten.[1217] Art. 2 c ECRL bestimmt weiter, dass das Vorhandensein und die Nutzung technischer Mittel und Technologien, die zum Anbieten des Dienstes erforderlich sind, noch allein keine Niederlassung des Anbieters begründen, was glei-

---

[1212] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1., 2., und 3.

[1213] Wie bei der Prüfung der Grundfreiheiten handelt es sich bei den Providern wieder um natürliche oder juristische Personen. Bei der Frage nach der Niederlassung sind die oben durchgeführten Erwägungen, vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. IV. 2. und 3., ebenfalls zu beachten. Allerdings stehen natürlich die Definition des Art. 2 c ECRL und Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie für die Beurteilung, wann ein Provider wo niedergelassen ist, im Vordergrund.

[1214] Vgl. oben unter B. 3. Teil. 3. Kapitel. II. 2. b.

[1215] Da hier allein auf die Niederlassung abgestellt wird, ist es egal, ob es sich um eine natürliche oder juristische Person handelt. Eine Unterscheidung zwischen einer natürlichen und juristischen Person ist somit nicht nötig.

[1216] Geis, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen“, CR 1999, 772, 773.

[1217] Vgl. insoweit oben zur Definition der Niederlassungsfreiheit unter B. 3. Teil. 2. Kapitel. V. 1. b. aa. (2). sowie die Definition der niedergelassenen Diensteanbieter unter B. 3. Teil. 3. Kapitel. II. 1. b. aa. (2).

chermaßen bereits oben bei der primärrechtlichen Prüfung hinsichtlich der Abgrenzung von Niederlassungs- und Dienstleistungsfreiheit festgestellt wurde.[1218] Das technische Equipment, das lediglich die notwendige Infrastruktur für das Anbieten der Internet-Dienste darstellt, reicht für die Bejahung einer Niederlassung noch nicht aus. Vielmehr müssen weitere Komponenten hinzutreten, die im Zusammenhang mit dem Content-Providing stehen, damit von einem niedergelassenen Diensteanbieter gesprochen werden kann. Dabei sind die Grenzen zur Erfüllung der Kriterien für eine Niederlassung fließend. Zumindest gilt es zu beachten, dass die Hard- und Software allein für den Niederlassungsbegriff noch nicht ausreichen.

Für den Content-Provider, gegen den staatliche Kontrollmaßnahmen ergehen, sind zwei Fallkonstellationen denkbar, um in den Anwendungsbereich des Art. 3 II ECRL zu gelangen: Zum einen kann er seine Niederlassung samt Technik und damit auch den gespeicherten Inhalt im EU-Ausland haben. Die Dienste aus einem anderen EU-Mitgliedstaat, wie es Art. 3 II ECRL verlangt, kommen dann nur mit Hilfe des Nutzers[1219] in das Inland. Zum anderen kann der Content-Provider zwar seine Niederlassung im EU-Ausland errichtet haben, die Technik für das Content-Providing und damit die für den Nutzer bereitgestellten Dienste befinden sich hingegen im Inland.[1220] In beiden Fällen ist der Content-Provider im EU-Ausland niedergelassen und die Dienste stammen aus dem EU-Ausland.[1221]

In der Praxis dürfte wohl nur die zweite Fallvariante von Bedeutung sein.[1222] Da sich zumindest die Technik für das Content-Providing im Inland befindet, besitzt die anord-

---

1218 Vgl. oben unter B. 3. Teil. 2. Kapitel. V. 1. b. bb. (2).

1219 Der sich wiederum häufig eines Access-Providers bedient. Hierzu aber unten unter B. 3. Teil. 3. Kapitel. II. 3. c.

1220 Denkbar ist außerdem noch ein weiterer Fall, bei dem der Content-Provider durch staatliche Sperr- und/oder Löschanordnungen, die gegen den Service-Provider ergehen, beeinträchtigt wird. Nämlich dann, wenn der Service-Provider im Inland und der Content-Provider im EU-Ausland niedergelassen ist. Bei dieser Konstellation kann sich zwar nicht der Service-Provider auf europarechtliche Normen berufen. Für den Content-Provider, der von den staatlichen Maßnahmen betroffen ist, sind jedoch die Vorschriften des Art. 3 II-VI ECRL anwendbar. Die Frage, ob diese Maßnahmen aus der Sicht des Content-Providers zulässig sind, wird im folgenden beantwortet, da es für den Content-Provider keinen Unterschied macht, ob der Staat direkt oder mit Hilfe des Service-Providers gegen ihn vorgeht. Vgl. insoweit auch unten unter B. 3. Teil. 3. Kapitel. II. 3. b.

1221 Zwar könnte die Frage aufgeworfen werden, ob die Dienste, also die angebotenen Inhalte des Content-Providers, wirklich aus einem anderen Mitgliedstaat stammen, da sie ja eigentlich bereits im Inland befindlich sind. Dieser Gedanke ist jedoch abzulehnen. So sind die Inhalte ursprünglich von einem Content-Provider aus dem EU-Ausland in das Inland gebracht worden. Die Tatsache, dass sich die Dienste nun im Inland befinden, ändert hieran nichts. Dieses Ergebnis wird von Art. 2 c) ECRL, der gerade solche Fälle regeln soll, und durch den Wortlaut des Art. 3 II ECRL untermauert.

1222 Als dritte Fallvariante kommt auch noch in Betracht, dass der Content-Provider zwar eine Zweigniederlassung im Inland unterhält, jedoch die Hauptniederlassung im EU-Ausland befindlich ist. Auch der Fall, dass der Content-Provider mehrere gleichberechtigte Niederlassungen sowohl im Inland als auch im EU-Ausland unterhält, ist möglich. In beiden Varianten kommt es darauf an, von welchem Niederlassungsort aus der betreffende Dienst erbracht wird, vgl. Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie. Wird der Dienst von der Niederlassung im Inland angeboten, so greift Art. 3 I ECRL ein, so dass lediglich nationales Recht auf den Dienst zur Anwendung kommt. Befindet sich der vom Content-Provider bereitgehaltene Inhalt jedoch bei einer Niederlassung im Ausland

nende Behörde bestimmte Anhaltspunkte und vielleicht sogar eine inländische Adresse des Content-Providers, um den VA wirksam an den Content-Provider richten zu können. Wenn der Content-Provider gänzlich im EU-Ausland ist und es eigentlich keinen inländischen Bezug gibt, sind Kontrollmaßnahmen praktisch nicht durchführbar. Infolge des Territorialitätsprinzips hätte die zuständige Behörde keine Möglichkeit, auf den Content-Provider per VA direkt einzuwirken.[1223] Dies wäre nur indirekt über dafür bestehende Vollstreckungsabkommen, mit Hilfe eines Acces-Providers oder durch Amtshilfe denkbar.

bb. Allgemeines Beschränkungsverbot

Gemäß Art. 3 II ECRL sind aber staatliche Maßnahmen, die den freien Verkehr von Diensten des Content-Providers aus anderen Mitgliedstaaten einschränken, grundsätzlich ohnehin verboten, wenn sie dem koordinierten Bereich zuzurechnen sind. Dies ist hier der Fall, da es um Anforderungen an den Inhalt des Dienstes i.S.d. Art. 2 h i) 2. Spiegelstrich geht. Nach Art. 3 I ECRL hat deshalb nur derjenige Mitgliedstaat, wo sich die Niederlassung des Content-Providers befindet, eigenverantwortlich dafür zu sorgen, dass der Content-Provider die Vorschriften dieses Staates einhält. Anderen Mitgliedstaaten steht dagegen keine Befugnis zur Kontrolle des Content-Providers zu.

cc. Ausnahmetatbestand des Art. 3 IV ECRL

Etwas anderes gilt jedoch, wenn die Voraussetzungen des Art. 3 IV ECRL erfüllt sind. Dann können auch die Mitgliedstaaten ausnahmsweise unter den in Art. 3 IV und V ECRL festgelegten Bedingungen, Maßnahmen gegen Dienste aus anderen Mitgliedstaaten ergreifen, um den freien Verkehr für Dienste der Informationsgesellschaft einzuschränken.

Die staatlichen Sperr- und/oder Löschanordnungen gegen den Content-Provider ergehen hauptsächlich aus präventiven Gründen, um eine Gefahr für die öffentliche Sicherheit und Ordnung i.S.d. jeweiligen Polizei- und Sicherheitsrechts zu verhindern.[1224] Letztlich geht es hierbei hauptsächlich um den Jugendschutz, die Abwehr von radikalen politischen Ansichten, von Rassismus, von staatsfeindlichen Inhalten sowie die Wahrung der Menschenwürde[1225]. Sowohl der einzelne Nutzer als auch der Staat sollen durch die behördlichen Maßnahmen, die sich gegen die rechtswidrigen Inhalte im Netz richten, geschützt werden. Infolge dieser Motive könnten der 1. und 3. Spiegelstrich von Art. 3

---

und wird er vom Nutzer aus dem Inland abgerufen, so dass der Dienst aus einem anderen Mitgliedstaat in das Inland erbracht wird, dann ist diese Fallvariante mit den eben angesprochenen Fallvarianten vergleichbar, in denen der Content-Provider keine Niederlassung im Inland unterhält. Denn diese spielt für den bestimmten Dienst keine Rolle.

1223 Vgl. oben unter B. 3. Teil. 2. Kapitel. IV. 1. Ist dies der Fall, dann kann die Behörde nur mit Hilfe eines inländischen Access-Providers gegen den Content-Provider vorgehen.

1224 Berner/Köhler, Polizeiaufgabengesetz, 16. Auflage, zu Art. 2 ff. S. 9 ff.

1225 Die Verbannung von Pornographie aus dem Internet stellt einen Teil der Wahrung der Menschenwürde dar. Deshalb wird der Schutz vor unzulässiger Pornographie nicht mehr extra aufgeführt.

IV a i) ECRL erfüllt sein. Denn die Kontrollmaßnahmen ergehen aus Gründen zum Schutz der öffentlichen Ordnung (Art. 3 IV a i) 1. Spiegelstrich ECRL) sowie zum Schutz der öffentlichen Sicherheit (Art. 3 IV a i) 3. Spiegelstrich ECRL).

Es wäre jedoch falsch, die in Art. 3 IV a i) ECRL genannten Begriffe mit den aus dem deutschen Polizei- und Sicherheitsrecht gleichzusetzen. Denn bei sämtlichen Begriffen der E-Commerce-Richtlinie handelt es sich um europarechtliche, die demnach auch europarechtlich zu definieren sind.[1226] Fraglich ist somit, was unter den Begriffen der öffentlichen Ordnung und Sicherheit i.S.d. Art. 3 IV a i) ECRL zu verstehen ist. Eine Definitionshilfe bietet der Wortlaut des Art. 3 IV a i) ECRL selbst an, da er insbesondere im 1. sowie im 3. Spiegelstrich Beispiele enthält, was unter diese Begriffe subsumiert werden kann. Das Wort „*insbesondere*“ im 1. Spiegelstrich zeigt deutlich, dass die dort enthaltenen Aufzählungen nicht abschließend sind. Auch das Wort „*einschließlich*“ im 3. Spiegelstrich des Art. 3 IV a i) ECRL will nur klarstellen, dass die Wahrung nationaler Sicherheits- und Verteidigungsinteressen in jedem Fall unter diesen Begriff zu fassen ist. Eine eindeutige Definition enthalten jedoch weder der 1. noch der 3. Spiegelstrich des Art. 3 IV a i) ECRL. Dies gilt ebenso für die übrigen Normen der E-Commerce-Richtlinie und ihren Erwägungsgründen. Eine zufriedenstellende Begriffsbestimmung lässt sich der E-Commerce-Richtlinie jedenfalls nicht entnehmen. Mithin ist also problematisch, eine Definition der öffentlichen Sicherheit und Ordnung zu finden, die im Einklang mit dem Wortlaut der E-Commerce-Richtlinie steht.

Zu denken wäre an die Rechtsprechung des EuGH und an die Kodifikation des EGV. Die Rechtsprechung des EuGH hilft hierbei nicht weiter, da er selbst bislang keine neue „ordre public“-Regelung richterrechtlich geschaffen hat. Selbst die mittlerweile gefestigte Schrankensystematik des EuGH, die eine Einschränkung der Grundfreiheiten aus zwingenden Gründen des Allgemeininteresses zulässt, enthält keine Ausführungen zu den Gründen der öffentlichen Ordnung und Sicherheit.[1227] Dies lässt sich plausibel damit begründen, dass jede Grundfreiheit bereits ihren Ausnahmetatbestand aus Gründen der öffentlichen Sicherheit und Ordnung im EGV besitzt und deshalb Richterrecht insoweit nicht erforderlich war.[1228]

Da der EGV hingegen diverse „ordre public“-Vorschriften besitzt,[1229] ist zu prüfen, ob nicht die dort genannten Begriffe der öffentlichen Sicherheit und Ordnung mit denen

---

[1226] Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 552 f.

[1227] Vgl. insoweit oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (3). und bb. (2). (a).

[1228] Ein anderes Ergebnis wäre wohl für den Begriff des Verbraucherschutzes i.S.d. Art. 3 IV a i) ECRL zu erwarten, der explizit vom EuGH in seiner Cassis-de-Dijon-Rechtsprechung genannt wird, vgl. Herdegen, Europarecht, 2. Auflage, § 16 Rdnr. 294, und mittlerweile als zwingender Grund des Allgemeininteresses eine Beschränkung der einzelnen Grundfreiheiten rechtfertigen würde.

[1229] Die Warenverkehrsfreiheit besitzt in Art. 30 EGV eine Ausnahmevorschrift, wonach Beschränkungen dieser Grundfreiheit ausnahmsweise aus Gründen der öffentlichen Sittlichkeit, Ordnung und Sicherheit zulässig sind. Art. 39 III EGV enthält für die Arbeitnehmerfreizügigkeit den Passus, nach dem aus Gründen der öffentlichen Ordnung und Sicherheit die Rechte der Arbeitnehmer rechtmäßig

aus der E-Commerce-Richtlinie vergleichbar sind. Gegebenenfalls können ihre Definitionen dann auf die Richtlinie übertragen werden.[1230]

Mittlerweile gilt zwar aufgrund der Rechtsprechung des EuGH, dass die Grundfreiheiten des EGV gegenüber der allgemeinen Norm des Art. 12 EGV nicht mehr lediglich spezielle Diskriminierungsverbote, sondern allgemeine Beschränkungsverbote darstellen.[1231] Der Wortlaut des EGV enthält in den für die vorliegende Arbeit relevanten Grundfreiheiten, der Warenverkehrs-, Niederlassungs- und Dienstleistungsfreiheit,[1232] aber nur in dem Ausnahmetatbestand des Art. 30 S. 1 EGV bei der Warenverkehrsfreiheit einen mit Art. 3 IV a i) i.V.m. II ECRL vergleichbaren Wortlaut. Denn in beiden Fällen geht es um die Zulässigkeit der Einschränkung eines Beschränkungsverbots durch innerstaatliche Maßnahmen. Sowohl die Richtlinie in Art. 3 II ECRL als auch die Warenverkehrsfreiheit in Art. 28 und 29 EGV enthalten explizit ein Beschränkungsverbot. Als weitere Gemeinsamkeit nennen beide Regelwerke in ihren Ausnahmetatbeständen den Schutz der öffentlichen Ordnung und Sicherheit sowie den Gesundheitsschutz[1233]. Auffällig ist weiter, dass die E-Commerce-Richtlinie an diversen Stellen bemüht ist, Parallelen zum primärrechtlichen EGV zu ziehen und seine Begriffsbestimmungen auf Rechtsbegriffe der Richtlinie zu übertragen, wie dies signifikant beispielsweise beim Begriff der Niederlassung i.S.d. Art. 43 ff. EGV und des niedergelassenen Diensteanbieters i.S.d. Art. 2 c ECRL geschehen ist.[1234] Ebenso werden die Dienste der Informationsgesellschaft i.S.d. Art. 2 a ECRL auch als Dienstleistungen i.S.d. Art. 49 ff. EGV angesehen.[1235] Dies zeigt, dass es durchaus gewollt und gewünscht ist, im Sekundärrecht die gleichen Begriffe zu verwenden wie im Primärrecht, da nur so der Aufbau eines einheitlichen europäischen Rechtssystems ermöglicht wird. Deshalb ist es konsequent und sinnvoll, auch die Definitionen der Rechtsbegriffe der öffentlichen Sicherheit und Ordnung von Art. 30 EGV auf Art. 3 IV a i) ECRL zu übertragen. Zwar besitzt der EGV selbst keine nähere Definition für diese Begriffe. Auch in den Art. 39 III und 46, 55 EGV, die ebenfalls in ihrem Wortlaut Begriffe der öffentlichen Ordnung und Sicherheit enthalten, wird nicht ausgeführt, was damit gemeint ist. Hingegen ist hierzu bereits höchstrichterlich umfangreich entschieden worden, so dass diese Begriffe durch Rechtsprechung und Literatur eine ausreichende Definition erhalten haben:[1236] Demnach ist

---

beschränkt werden dürfen. Für die Niederlassungsfreiheit und für die Dienstleistungsfreiheit ist der ordre public in Art. 46 I EGV geregelt.

1230 Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 552 f.

1231 Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (1)., bb. (1). Und cc. (1).

1232 Brisch, „EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr“, CR 1999, 235.

1233 Der Gesundheitsschutz spielt jedoch für diese Arbeit nur eine untergeordnete Rolle.

1234 Siehe oben unter B. 3. Teil. 3. Kapitel. II. 3. a. aa.

1235 Maennel, „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 188; Waldenberger in: „Electronic Commerce: Der Richtlinienvorschlag der EG-Kommission“, EuZW, 1999, 296.

1236 Vgl. hierzu auch: Oppermann, Europarecht, § 18 Rdnr. 1166 sowie Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1129.

unter der „öffentlichen Ordnung“ i.S.d. Art. 30 S. 1 EGV die Gesamtheit der hoheitlich festgelegten, unverzichtbaren Grundregeln, die im Interesse der politischen und sozialen Struktur der Gesellschaft von einem Mitgliedstaat erlassen werden, sowie den dadurch angestrebten Zustand, zu verstehen.[1237] Darüber hinaus hat der EuGH in einer Entscheidung[1238] zu diesem Rechtsbegriff[1239] gefordert, dass für die Rechtfertigung aus Gründen der öffentlichen Ordnung – neben weiteren Kriterien – eine tatsächliche und hinreichend schwere Gefährdung vorliegen muss, die ein Grundinteresse der Gesellschaft berührt.[1240] Wichtig ist in diesem Zusammenhang auch, dass die in Art. 30 S. 1 EGV separat genannte öffentliche Sittlichkeit ein Unterfall der öffentlichen Ordnung ist und hierunter subsumiert werden kann.[1241] Auch die „öffentliche Sicherheit“ ist eigentlich ein Teilbereich der öffentlichen Ordnung.[1242] Eine Definition der öffentlichen Sicherheit fehlt im EGV ebenfalls, jedoch finden sich in den vorrangigen Art. 296 und 297 EGV einige Beispiele, wobei in Art. 297 EGV die „*öffentliche Sicherheit*“ sogar ausdrücklich genannt wird. Die öffentliche Sicherheit ist demzufolge in ihrem Kern als das Schutzsystem zur Bekämpfung von Gewaltanwendung (im Innern oder von außen), also als innere und äußere Sicherheit eines Mitgliedstaats anzusehen.[1243] Zur öffentlichen Sicherheit zählt dabei auch die Sicherung der Existenz des Staates.[1244]

Werden nun diese primärrechtlichen Definitionen auf die sekundärrechtliche E-Commerce-Richtlinie übertragen, dann zeigt sich zunächst, dass die Idee einer Übernahme dieser Begriffsbestimmungen richtig gewesen ist. Denn Art. 3 IV a i) ECRL spiegelt genau die jeweiligen Begriffsbestimmungen wider. Sie stehen also im Einklang mit der E-Commerce-Richtlinie. So lässt sich der 1. Spiegelstrich des Art. 3 IV a i) ECRL mit seinen Beispielen in die genannte Definition zur öffentlichen Ordnung einfügen. Dasselbe gilt für den 3. Spiegelstrich des Art. 3 IV a i) ECRL, dessen Wortlaut sogar Teile der erwähnten Definition beinhaltet. Insgesamt kann mit Hilfe der primärrechtlichen Definitionen bezüglich der Begriffe öffentliche Ordnung und Sicherheit sowie den im 1. und 3. Spiegelstrich des Art. 3 IV a i) ECRL genannten Beispielen klar

---

1237 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, 5. Auflage, Art. 36 Rdnr. 50.

1238 EuGH, Rs. 30/77, 27.10.1977, Slg. 1977, 1999, 2013 Rdnr. 35 (Bouchereau).

1239 Allerdings ging es in dieser Entscheidung nicht um die öffentliche Ordnung des Art. 30 EGV sondern um den Rechtsbegriff in Art. 39 III EGV.

1240 Dies stellt wiederum eine weitere Parallelität zwischen der E-Commerce-Richtlinie und dem Primärrecht dar, wie ein Blick auf Art. 3 IV a ii) ECRL zeigt.

1241 Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, 5. Auflage, Art. 36 Rdnr. 56.

1242 EuGH, Rs. 72/83, 10.071984, Slg. 1984, 2727, 2751 Rdnr. 33 (Campus Oil).

1243 EuGH, Rs. C-367/89, 04.10.1991, Slg. 1991, I-4621, 4652 Rdnr. 22 (Richardt); vgl. auch Jestaedt/Hohenstatt, „Europarecht bricht nationales Exportkontrollrecht“, EuZW 1992, 44 ff.

1244 EuGH, Rs. 72/83, 10.07.1984, Slg. 1984, 2727, 2751 Rdnr. 22 (Campus Oil); vgl. Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, 5. Auflage, Art. 36 Rdnr. 55.

herausgearbeitet werden, was sich unter die Rechtsbegriffe der öffentlichen Ordnung und Sicherheit fassen lässt.

Da die staatlichen Sperr- und/oder Löschanordnungen hauptsächlich aus Gründen des Jugendschutzes, zur Verhinderung von Rassismus und politischem Radikalismus, zur Abwehr von Gewaltverherrlichung sowie Wahrung der Menschenwürde ergehen, können sie vor allem unter den 1. Spiegelstrich des Art. 3 IV a i) ECRL subsumiert werden. Letztlich will sich der Staat aber auch selbst gegen Bedrohungen aus dem Internet schützen, die das staatliche Gefüge angreifen. Insoweit sind somit auch nationale Sicherheitsinteressen des Staates betroffen, die unter den 3. Spiegelstrich des Art. 3 IV a i) ECRL fallen. Die Sperr- und/oder Löschanordnungen ergehen somit aus Gründen der öffentlichen Ordnung und Sicherheit und erfüllen folglich Art. 3 IV a i) ECRL.

Gemäß Art. 3 IV a ii) ECRL müssen die Kontrollmaßnahmen darüber hinaus einen „*bestimmten Dienst der Informationsgesellschaft, der die unter Art. 3 IV a i) ECRL genannten Schutzziele beeinträchtigt oder eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung dieser Ziele darstellt*“, betreffen. Das erste Kriterium ist rasch zu bejahen, da sich die Sperr- und/oder Löschanordnungen gegen den Content-Provider, also einem bestimmten Dienst der Informationsgesellschaft, richtet. Hingegen ist fraglich, wann von einer Beeinträchtigung der in Art. 3 IV a i) ECRL enthaltenen Schutzziele gesprochen werden kann bzw. eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung dieser Ziele vorliegt. Auch hier handelt es sich wieder um europarechtliche Begriffe, die nicht national, sondern allein mit Hilfe des Europarechts ausgelegt bzw. definiert werden dürfen.[1245]

Eine Beeinträchtigung der Schutzziele des Art. 3 IV a i) ECRL liegt dann vor, wenn die Schutzziele konkret von bestimmten Inhalten des Internets betroffen sind. So tangiert eine Internet-Seite, die zum Rassenhass aufruft oder Kinderpornographie anbietet, direkt die Schutzziele des 1. Spiegelstrichs von Art. 3 IV a i) ECRL, namentlich die Verhütung von Straftaten, die Bekämpfung der Hetze aus Gründen der Rasse sowie die Verletzung der Menschenwürde[1246]. Dies zeigt, dass der Content-Provider, der rechtswidrige Inhalte in das Internet eingestellt hat, grundsätzlich die in Art. 3 IV a i) ECRL genannten Schutzziele direkt beeinträchtigt.

Es stellt sich jedoch die Frage, wann eine ernsthafte und schwerwiegende Gefahr angenommen werden darf. Die E-Commerce-Richtlinie schweigt hierzu ebenfalls. Auch der EGV besitzt direkt keine Norm, die die Rechtsbegriffe einer ernsthaften und schwerwiegenden Gefahr beinhaltet. Wie bereits eben erwähnt wurde, hat der EuGH jedoch in einem Urteil zum Begriff der öffentlichen Ordnung i.S.d. Art. 39 III EGV Stellung genommen und festgestellt, dass außer der Störung der öffentlichen Ordnung durch eine

---

[1245] Bleckmann, Europarecht, 6. Auflage, § 8 Rdnr. 552 f.

[1246] Die öffentliche Sittlichkeit, die von kinderpornographischen Internet-Angeboten sicherlich auch betroffen ist, wird hier unter den Begriff der Menschenwürde gefasst.

Gesetzesverletzung eine tatsächliche und hinreichend schwere Gefährdung vorliegen muss, die ein Grundinteresse der Gesellschaft berührt.[1247] Auf den Begriff der Gefährdung ist der EuGH ferner in zwei Urteilen zu Art. 30 EGV eingegangen. So muss die Gefährdung eines nach Art. 30 EGV anerkannten Schutzguts „ernstzunehmend" sein.[1248] Die bloße Behauptung einer Gefahr reicht nicht aus. Ebenso wenig würden allgemeine Überlegungen genügen.[1249] Die Gefahr muss vielmehr substantiiert und nachvollziehbar auf das jeweilige Schutzgut und die jeweilige innergemeinschaftlich grenzüberschreitende Ware bezogen, von dem Mitgliedstaat dargetan werden, der sich auf Art. 30 EGV beruft.[1250] Sinn und Zweck der Rechtsprechung des EuGH war es, dass nicht jeder Staat durch allgemeine Behauptungen, er müsse durch bestimmte staatliche Maßnahmen möglichen Gefahren vorbeugen, in den Genus des „ordre public" kommen darf. Diese Rechtsprechung wurde anscheinend für die E-Commerce-Richtlinie übernommen und in Art. 3 IV a ii) ECRL eingearbeitet.[1251] Eine ernsthafte und schwerwiegende Gefahr liegt demnach vor, wenn eine tatsächliche und hinreichend schwere Gefährdung bejaht werden kann. Die Gefahr muss schon so konkret im Raum stehen, dass bei weiterem Zeitablauf eine Beeinträchtigung der in Art. 3 IV a i) ECRL genannten Schutzgüter sehr wahrscheinlich ist. Diese Definition lässt sich vom Wortlaut des Art. 3 IV a ii) ECRL direkt ableiten. Denn zunächst fordert diese Norm ganz konkret eine Beeinträchtigung der in Art. 3 IV a i) ECRL enthaltenen Schutzziele. Es ist aber auch möglich, dass der Staat vorbeugend, vgl. Art. 3 IV a i) 1. Spiegelstrich ECRL, durch entsprechende Maßnahmen schon vor einer Beeinträchtigung der Schutzziele gegen unmittelbare Gefahren tätig wird. Allerdings muss diese präventive Möglichkeit sehr eng gehandhabt werden, um Missbrauch zu vermeiden und die ratio des Art. 3 I und II ECRL ins Gegenteil zu verkehren. Deshalb kann von Art. 3 IV a ii) ECRL nur eine konkrete, hinreichend schwere und unmittelbar bevorstehende Gefahr einer Beeinträchtigung der Schutzziele gemeint sein.[1252]

[1247] EuGH, Rs. 30/77, 27.10.1977, Slg. 1977, 1999, 2013 Rdnr. 35 (Bouchereau).

[1248] EuGH, Rs. 227/82, 30.11.1983, Slg. 1983, 3883, 3905 Rdnr. 40 (Van Bennekom).

[1249] EuGH, Rs. C-17/93, 14.07.1994, Slg. 1994, I-3537, 3560 Rdnr. 17 (Van der Veldt).

[1250] Vgl. Müller-Graff in: Groeben/Thiesing/Ehlermann (Hrsg.), Kommentar zum EU-/EG-Vertrag, 5. Auflage, Art. 36 Rdnr. 99.

[1251] Dieser Gefahr, dass sich die Mitgliedstaaten mit harmlosen Sachverhalten auf den „ordre public" berufen, könnte auch im Rahmen der Verhältnismäßigkeit von Art. 3 IV a iii) ECRL begegnet werden. Zumindest sollte, falls von einem Mitgliedstaat eine ernsthafte und schwerwiegende Gefahr behauptet wird, diese Gefahr in der Verhältnismäßigkeitsprüfung erneut untersucht werden, um einem Missbrauch vorzubeugen.

[1252] Die 2. Alternative des Art. 3 IV a iii) ECRL ist vor allem für den Access-Provider von großer Bedeutung. Denn im Gegensatz zum Content- bzw. Service-Provider kommt er erst mit den im Internet bereitgehaltenen rechtswidrigen Inhalten in Berührung, wenn er für den Nutzer aktiv wird. Eine Beeinträchtigung der Schutzziele i.S.d. Art. 3 IV a i) ECRL kann somit höchstens erst dann bejaht werden, wenn er den rechtswidrigen Inhalt an den Nutzer weiterleitet. Zuvor besteht – wenn überhaupt – nur eine ernsthafte und schwerwiegende Gefahr, dass der Access-Provider den unerwünschten Inhalt weiter verbreitet. Vgl. hierzu auch die Ausführungen weiter unten unter B. 3. Teil. 3. Kapitel. II. 3. c. cc.

Ob dies bei gegen einen Content-Provider staatlich angeordneten Sperr- und/oder Löschanordnungen der Fall ist, bleibt Tatfrage. Sicherlich besteht jedoch häufig durch rechtswidrige Inhalte, die der Content-Provider bereithält, bereits eine direkte Beeinträchtigung der in Art. 3 IV a i) ECRL genannten Schutzziele, so dass es auf die oft schwer zu beurteilende Frage, ob eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung besteht, nicht mehr ankommt. Art. 3 IV a ii) ECRL ist somit in den meisten Fällen ebenfalls erfüllt.

Schließlich verlangt Art. 3 IV a iii) ECRL, dass die behördlichen Kontrollmaßnahmen in einem angemessenen Verhältnis zu den in Art. 3 IV a i) ECRL genannten Schutzzielen stehen. Auch hier ist wieder deutlich eine Parallele zum Primärrecht zu erkennen, das den Grundsatz der Verhältnismäßigkeit bei jedem „ordre public"-Ausnahmetatbestand anwendet.[1253] Die Sperr- bzw. Löschanordnungen müssen also geeignet, erforderlich und angemessen sein.[1254]

Bei einer Beeinträchtigung der in Art. 3 IV a i) ECRL aufgelisteten Schutzziele durch den Content-Provider, sind – rein technisch gesehen – die Sperr- und/oder Löschanordnungen die geeigneten Maßnahmen, um diese Schutzziele zu erreichen.[1255] Fraglich ist, ob sie auch erforderlich sind, da sich die Maßnahmen gegen Content-Provider richten, die in einem anderen Mitgliedstaat niedergelassen sind. Gemäß Art. 3 I ECRL, der trotz Art. 3 IV ECRL[1256] weiter zur Anwendung kommt, ist eigentlich der Mitgliedstaat, wo der Content-Provider seine Niederlassung hat, für Maßnahmen gegen dessen Dienste verantwortlich. Darüber hinaus besteht die Möglichkeit, den Mitgliedstaat durch die in Art. 19 ECRL fixierte Amtshilfe zu geeigneten Maßnahmen aufzufordern. Folglich könnten die staatlichen Kontrollmaßnahmen schon allein wegen der fehlenden Erforderlichkeit als unverhältnismäßig angesehen werden. Dieser Gedanke ist allerdings wegen Art. 3 IV b 1. Spiegelstrich ECRL abzulehnen. Denn die Ausnahmevorschrift des Art. 3 IV ECRL ist nur dann erfüllt, wenn gemäß Art. 3 IV b 1. Spiegelstrich ECRL der Mitgliedstaat vor Ergreifen seiner Kontrollmaßnahmen den in Art. 3 I ECRL genannten Mitgliedstaat aufgefordert hat, Maßnahmen gegen den Content-Provider zu ergreifen und dieser der Aufforderung nicht Folge geleistet hat oder die von ihm getroffenen Maßnahmen unzulänglich gewesen sind. Dass die staatlichen Sperr- und/oder Löschanordnungen eigentlich durch den Mitgliedstaat ergehen müssten, wo der Content-Provider niedergelassen ist und deshalb die vorbeschriebenen staatlichen Maßnahmen nicht erforderlich sind, ist bereits in Art. 3 IV b 1. Spiegelstrich ECRL als eine Tatbestandsvoraussetzung für Art. 3 IV ECRL ausdrücklich normiert worden. Dieser Aspekt darf somit bei der Frage nach der Verhältnismäßigkeit in Art. 3 IV a iii) ECRL nicht

---

[1253] Hakenberg, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, S. 98 f.; Herdegen, Europarecht, 2. Auflage, § 18 Rdnr. 325.

[1254] Schweitzer/Hummer, Europarecht, 5. Auflage, § 14 Rdnr. 1131.

[1255] Vgl. oben unter B. 1. Teil. III. 1. a. bis d.

[1256] Dort ist nur eine Abweichung von Art. 3 II und nicht von I ECRL vorgesehen.

mehr geprüft werden. Demnach sind die gegen den Content-Provider staatlich angeordneten Sperr- und/oder Löschverfügungen als erforderlich anzusehen, um den Schutz der öffentlichen Ordnung und Sicherheit i.S.d. Art. 3 IV a i) ECRL zu gewährleisten.
Zudem müssen diese Maßnahmen auch angemessen sein. Die Sperr- und/oder Löschmaßnahmen können gezielt gegen rassistische, politisch radikale, demokratiefeindliche, terroristische, menschenverachtende, brutale oder pornographische Inhalte gerichtet werden. Rechtmäßige Inhalte werden von den staatlichen Maßnahmen nicht betroffen. Die behördlichen Anordnungen ergehen nur punktuell und betreffen ausschließlich die rechtswidrigen Inhalte des Content-Providers, die äußerst wichtige Schutzgüter, wie den Jugendschutz, die staatliche Sicherheit oder die Menschenwürde, verletzen. Demgegenüber wird der Content-Provider durch die Maßnahmen in seiner wirtschaftlichen Freiheit, Dienste anzubieten, sowie in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt. Werden nun diese Rechte gegeneinander abgewogen und dabei die Intensität des Eingriffs beim Content-Provider durch die staatlichen Kontrollmaßnahmen berücksichtigt, dann ergibt sich folgendes: Weil die Sperr- bzw. Löschanordnungen gezielt gegen die rechtswidrigen Inhalte des Content-Providers eingesetzt werden können, stellt sich dieser Eingriff in die Rechte des Content-Providers als nicht sehr gravierend dar. Im Gegensatz dazu werden durch die rechtswidrigen Inhalte hohe Schutzgüter verletzt. Der Staat hat ein großes Interesse daran, die Beeinträchtigung dieser Schutzgüter zu beseitigen. Das Interesse des Content-Providers an einem ungestörten Bereithalten seiner in das Internet eingestellten Angebote muss deshalb hinter das staatliche Interesse an der Beseitigung der rechtswidrigen Inhalte zurücktreten. Folglich stehen die behördlichen Kontrollmaßnahmen in einem angemessenen Verhältnis zu den staatlichen Schutzzielen i.S.d. Art. 3 IV a iii) ECRL. Die staatlichen Sperr- und/oder Löschanordnungen gegen den Content-Provider erfüllen somit grundsätzlich die Kriterien des Art. 3 IV a i) bis iii) ECRL.
Damit die staatlichen Maßnahmen gegen den Content-Provider in Abweichung zu Art. 3 II ECRL zulässig sind, muss neben den Voraussetzungen des Art. 3 IV a ECRL auch noch das Verfahren nach Art. 3 IV b ECRL beachtet werden. Danach hat jeder Mitgliedstaat vor Ergreifen bestimmter Maßnahmen den in Art. 3 I ECRL genannten Mitgliedstaat unbeschadet etwaiger Gerichtsverfahren, einschließlich Vorverfahren und Schritten im Rahmen einer strafrechtlichen Ermittlung, aufzufordern, die jeweils erforderlichen Maßnahmen zu ergreifen. Erst wenn der Mitgliedstaat dieser Aufforderung nicht Folge geleistet hat oder die von ihm getroffenen Maßnahmen unzulänglich gewesen sind, sofern er die Kommission und den in Art. 3 I ECRL genannten Mitgliedstaat vorher über seine Absicht unterrichtet hat, bestimmte Maßnahmen gegen den Content-Provider zu ergreifen, dann darf er seine staatlichen Kontrollmaßnahmen trotz des Art. 3 II ECRL in zulässiger Weise gemäß Art. 3 IV b ECRL anordnen.

Hat die zuständige Behörde, die gegen den Content-Provider Sperr- und/oder Löschanordnungen erteilt, dieses Verfahren nach Art. 3 IV b ECRL beachtet,[1257] dann sind diese Maßnahmen insgesamt gemäß Art. 3 IV ECRL rechtmäßig ergangen.

dd. Zwischenergebnis

Im Ergebnis lässt sich somit sagen, dass auch nach der E-Commerce-Richtlinie bei Beachtung des Verfahrens in Art. 3 IV b ECRL – außer es liegt ein Fall des Art. 3 V ECRL vor – staatliche Kontrollmaßnahmen gegen den Content-Provider zulässig sind.

b. Kontrollmaßnahmen gegen den Service-Provider

aa. Vorüberlegungen

Wie beim Content-Provider muss auch der Service-Provider in einem anderen Mitgliedstaat niedergelassen sein, damit Art. 3 II bis VI ECRL zur Anwendung kommen kann. Ansonsten wären gemäß Art. 3 I ECRL lediglich die nationalen Rechtsvorschriften einschlägig.[1258] Folglich gibt es wiederum zwei Fallvarianten, die eine Anwendbarkeit des Art. 3 II bis VI ECRL ermöglichen: Zum einen den Service-Provider, der sich samt Technik in einem anderen Mitgliedstaat niedergelassen hat. Zum anderen den Service-Provider, dessen Niederlassung sich zwar in einem anderen Mitgliedstaat der EU, die Technik für das Service-Providing allerdings im Inland befindet. Wieder kann davon ausgegangen werden, dass lediglich der zweite Fall in der Praxis relevant ist, da insoweit ein Bezug zum Inland vorhanden ist und somit die staatlichen Behörden ihre Sperr- und/oder Löschanordnungen möglicherweise direkt an ihn adressieren können. Letztendlich geht es jedoch bei den staatlichen Kontrollmaßnahmen darum, mit Hilfe des Service-Providers die rechtswidrigen Inhalte zu beseitigen, die der Content-Provider beim Service-Provider zur Speicherung eingestellt hat. Insoweit muss weiter differenziert werden. Denn der Content-Provider kann ebenfalls seine Niederlassung sowohl im EU-Ausland als auch im Inland haben. Hat sich der Content-Provider im Inland niedergelassen, dann wird die zuständige Polizei- oder Sicherheitsbehörde schon nicht gegen

---

[1257] Ist das Verfahren nach Art. 3 IV b ECRL nicht eingehalten worden, besteht noch die Möglichkeit des Art. 3 V ECRL. So können die Mitgliedstaaten in dringenden Fällen von den in Art. 3 IV b ECRL genannten Bedingungen abweichen. In diesem Fall müssen die Maßnahmen sobald wie möglich und unter Angabe der Gründe, aus denen der Mitgliedstaat der Auffassung ist, dass es sich um einen dringenden Fall handelt, der Kommission und den in Art. 3 I ECRL genannten Mitgliedstaat mitgeteilt werden. Wenn also ein dringender Fall vorliegt, bei dem das Verfahren nach Art. 3 IV b ECRL – etwa aus Zeitgründen – nicht durchgeführt werden kann, können staatliche Kontrollmaßnahmen schon bei Vorliegen der Voraussetzungen des Art. 3 IV a ECRL angeordnet werden.

[1258] Denkbar ist auch, dass zwar der Service-Provider im Inland und nur der Content-Provider im Ausland niedergelassen ist. Dann wäre das Europarecht der E-Commerce-Richtlinie nicht aus der Sicht des Service-Providers sondern nur im Hinblick auf den Content-Provider betroffen. Die Art. 3 II bis VI ECRL fänden nur gegenüber dem Content-Provider Anwendung. Dies hätte zur Folge, dass sich im Grunde dieselbe Fallkonstellation wie oben beim Content-Provider mit den gleichen Prüfungsergebnissen ergeben würde. Insoweit kann deshalb nach oben zu B. 3. Teil. 3. Kapitel. II. 3. a. verwiesen werden.

den im EU-Ausland niedergelassenen Service-Provider, sondern gleich i.S.d. Art. 3 I ECRL infolge einer nationalen Rechtsgrundlage direkt gegen den Content-Provider vorgehen. Dies dürfte effektiver sein. Die Maßnahmen werden sich also nur dann gegen den Service-Provider richten, sofern der Content-Provider ebenfalls im EU-Ausland niedergelassen ist. Eine Unterscheidung beim Content-Provider, ob er seine Technik für das Content-Providing im Inland oder in einem anderen Mitgliedstaat hat, entfällt, da er selbst keine Technik besitzt. Folglich werden in der Regel behördliche Sperr- und/oder Löschanordnungen gegen den Service-Provider nur dann ergehen, wenn der Service-Provider im EU-Ausland niedergelassen ist und seine für das Service-Providing notwendige Hard- und Software im Inland befindet. Darüber hinaus muss der Content-Provider, dessen Inhalte der Service-Provider speichert, seine Niederlassung gleichermaßen in einem anderen Mitgliedstaat haben.[1259]

Die gegen den Service-Provider gerichtete Aufforderung, bestimmte Inhalte zu sperren oder zu löschen, die er für den Content-Provider speichert, beeinträchtigt den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat. Sowohl die Dienste des Service-Providers als auch die Dienste des Content-Providers werden durch die staatlichen Kontrollmaßnahmen eingeschränkt. Hinsichtlich der Beeinträchtigung des Content-Providers kann nach oben verwiesen werden.[1260] Im Folgenden ist deshalb ausschließlich die Zulässigkeit der staatlichen Maßnahme gegen den Service-Provider zu betrachten:[1261]

bb. Allgemeines Beschränkungsverbot

Gemäß Art. 3 II ECRL sind Beeinträchtigungen des Service-Providers, der seine Dienste gegenüber dem Content-Provider nicht mehr ordnungsgemäß erfüllen kann, nicht erlaubt, sofern sie aus Gründen erfolgen, die in den koordinierten Bereich nach Art. 2 h ECRL fallen. Dies ist grundsätzlich bei den polizei- und sicherheitsrechtlichen Kontrollmaßnahmen zu bejahen, da es hier um Anforderungen an den Inhalt des Dienstes geht. Art. 2 h i) 2. Spiegelstrich ECRL. Art. 3 II ECRL findet somit Anwendung. Die

---

[1259] Falls der Service-Provider und/oder der Content-Provider mehrere Niederlassungen sowohl im Inland als auch im Ausland besitzen, greift wiederum Ziff. 19 der Erwägungsgründe der E-Commerce-Richtlinie ein. Vgl. insoweit auch oben Fn. 1222.

[1260] Vgl. oben unter B. 3. Teil. 3. Kapitel. II. 3. a. Dadurch dass der Service-Provider ebenfalls gezielt auf die rechtswidrigen Inhalte zugreifen kann, besteht letztendlich kein Unterschied, ob der Service-Provider die Inhalte beim Content-Provider sperrt bzw. löscht oder ob die staatlichen Kontrollmaßnahmen direkt gegen den Content-Provider verfügt werden. Der Service-Provider kann insoweit als quasi-vollstreckendes Organ angesehen werden. Im Ergebnis werden – aus der Sicht des Content-Providers – nur dessen rechtswidrigen Inhalte erfasst, egal ob nun an ihn die Sperr- und/oder Löschanordnungen oder an den Service-Provider ergehen. Die Auswirkungen derartiger staatlicher Kontrollmaßnahmen gegenüber dem Content-Provider im Hinblick auf die E-Commerce-Richtlinie wurden jedoch schon vorstehend ausführlich besprochen, so dass hierauf nicht mehr einzugehen ist.

[1261] Wie beim Content-Provider, vgl. oben Fn. 1221, kann auch hier daran gezweifelt werden, ob die Dienste des Service-Providers, die im Inland angeboten werden, als Dienste aus dem EU-Ausland i.S.d. Art. 3 II ECRL zu qualifizieren sind. Wegen Art. 2 c) ECRL und dem Wortlaut des Art. 3 II ECRL muss dieser Gedanke jedoch abgelehnt werden.

Sperr- bzw. Löschanordnungen sind also wegen Art. 3 II ECRL eigentlich nicht zulässig.

cc. Ausnahmetatbestand des Art. 3 IV ECRL

Es könnte aber wiederum der Ausnahmetatbestand des Art. 3 IV ECRL erfüllt sein, so dass von dem Beschränkungsverbot nach Art. 3 II ECRL in rechtmäßiger Weise abgewichen werden darf. Die Kontrollmaßnahmen können – wie beim Content-Provider – mit dem Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit begründet werden, Art. 3 IV a i) ECRL.[1262] Die Maßnahmen betreffen darüber hinaus einen bestimmten Dienst der Informationsgesellschaft, hier den Service-Provider, der in der Regel die öffentliche Ordnung bzw. Sicherheit gemäß Art. 3 IV a ii) ECRL beeinträchtigt.[1263] Schließlich ist es notwendig, dass die Sperr- und/oder Löschanordnungen in einem angemessenen Verhältnis zu den Schutzzielen stehen, also geeignet, erforderlich und angemessen sein müssen.

Die staatlichen Kontrollmaßnahmen sind geeignet, die öffentliche Ordnung und Sicherheit zu schützen. Denn mit ihrer Hilfe können die durch den Content-Provider beim Service-Provider gespeicherten rechtswidrigen Inhalte beseitigt werden. Dies hat zur Folge, dass eine durch den Service-Provider hervorgerufene Beeinträchtigung der in Art. 3 IV a i) ECRL genannten Schutzziele verhindert wird.[1264] Des weiteren sind die Sperr- und Löschanordnungen erforderlich. Denn sie stellen die einzige technische Möglichkeit dar, die unerwünschten Inhalte des Content-Providers über den Service-Provider zu beseitigen bzw. unschädlich zu machen. Fraglich ist hingegen, ob die Maßnahmen im Hinblick auf die verfolgten Schutzziele auch angemessen sind. Dabei müssen wiederum die Interessen des Service-Providers, die von der staatlichen Anordnung betroffen sind, und die des Staates miteinander abgewogen werden: Der Service-Provider wird durch die gegen ihn gerichteten Sperr- bzw. Löschverfügungen in dem Recht auf ungehinderte Ausübung seines Service-Providing-Dienstes gestört. Es liegt zumindest eine Einschränkung seiner unternehmerischen Freiheit sowie seiner Berufsfreiheit vor, vgl. Art. 15 und 16 EGRC. Neben diesen Rechten des Service-Providers, die von den staatlichen Kontrollmaßnahmen beeinträchtigt werden, steht das Interesse des Staates, seine Bürger – vor allem die Nutzer – vor den rechtswidrigen Inhalten zu schützen. Ferner geht es auch um seinen eigenen Schutz, insbesondere bei demokratiefeindlichen, verfassungsfeindlichen, terroristischen oder rassistischen Inhalten. Die Auswirkungen der staatlichen Kontrollmaßnahmen beim Service-Provider sind demge-

---

1262 Vgl. oben unter B. 3. Teil. 3. Kapitel. II. 3. a. cc.

1263 Hierzu kann ebenfalls nach oben zu B. 3. Teil. 3. Kapitel. II. 3. a. cc. verwiesen werden.

1264 Natürlich ist neben dem Service-Provider hauptsächlich der Content-Provider für den im Internet angebotenen rechtswidrigen Inhalt verantwortlich. Aber dadurch dass der Service-Provider den Inhalt für den Content-Provider im Internet bereithält, trägt er entscheidend zur Beeinträchtigung bei, da ohne ihn auf den gespeicherten Inhalt nicht zugegriffen werden könnte. Folglich ist der Service-Provider ebenfalls als Störer anzusehen.

genüber häufig relativ gering. Denn der Service-Provider hält in der Regel Angebote von verschiedenen Content-Providern für die Nutzer im Internet bereit. Falls er nun durch eine staatliche Anordnung dazu veranlasst wird, einen bestimmten Inhalt bei einem bestimmten Content-Provider zu sperren bzw. zu löschen, fällt das insgesamt nicht weiter ins Gewicht, da er sämtliche anderen Inhalte weiter speichern darf und so seine übrigen Dienste ungehindert erbringen kann. Die wirtschaftlichen Interessen des Service-Providers werden also nur unwesentlich beeinträchtigt. Im Gegensatz dazu besitzt der Staat ein gesteigertes Interesse daran, die in Art. 3 IV a i) 1. und 3. Spiegelstrich ECRL enthaltenen Schutzziele zu gewährleisten. Dieses Interesse überlagert bei weitem die Interessen des Service-Providers. Die Sperr- und/oder Löschanordnungen stehen somit in einem angemessenen Verhältnis zu den verfolgten Schutzzielen i.S.d. Art. 3 IV a iii) ECRL, so dass die Voraussetzungen des Art. 3 IV a ECRL insgesamt erfüllt sind.

dd. Zwischenergebnis

Beachtet die zuständige Polizei- oder Sicherheitsbehörde das Verfahren nach Art. 3 IV b ECRL,[1265] dann sind die gegen den Service-Provider gerichteten Kontrollmaßnahmen – trotz des Art. 3 II ECRL – als zulässig anzusehen. Sie verstoßen nicht gegen die E-Commerce-Richtlinie und somit das Europarecht.

c. Kontrollmaßnahmen gegen den Access-Provider

aa. Vorüberlegungen

Wegen Art. 3 I ECRL muss auch bei Sperrverfügungen[1266] gegen den Access-Provider gefragt werden, welche Fallvarianten überhaupt von Art. 3 II bis VI ECRL erfasst werden können. Dies richtet sich danach, wo der Access-Provider niedergelassen ist. Hat er seine Niederlassung im Inland, so gilt für die gegen ihn gerichteten Sperranordnungen allein das nationale Recht, Art. 3 I ECRL. Der Access-Provider muss also im EU-Ausland niedergelassen sein.

Den staatlichen Behörden geht es vor allem darum, mit Hilfe der Sperrverfügungen zu verhindern, dass rechtswidrige Inhalte zum Nutzer ins Inland gelangen. Somit kommt eigentlich nur die Fallvariante in Betracht, wo der Access-Provider zwar in einem anderen Mitgliedstaat niedergelassen ist, seine Technik für das Access-Providing sich jedoch im Inland befindet.[1267]

[1265] Es sei denn, Art. 3 V ECRL kann ausnahmsweise bejaht werden.

[1266] Wie bereits an mehreren Stellen ausgeführt wurde, vgl. oben unter B. 1. Teil. III. 1. c. und d., können aus technischen Gründen gegen den Access-Provider nur Sperrverfügungen ergehen, da er keine Herrschaftsgewalt über die rechtswidrigen Inhalte hat.

[1267] Es besteht auch die Möglichkeit, dass der Access-Provider Inländer ist und sich allein der Inhalt im EU-Ausland beim Content-Provider (eventuell zusätzlich bei einem Service-Provider im EU-Ausland gespeichert) befindet. Wenn ein inländischer Nutzer nun diese Inhalte über den Access-Provider abrufen lässt, gelangen die Dienste des Content-Providers ebenfalls ins Inland.

Der Access-Provider hat zunächst die Aufgabe, dem Nutzer den Zugang zum Internet zu verschaffen. Darüber hinaus vermittelt der Access-Provider dem Nutzer den Zugang zu den jeweiligen Inhalten der Content-Provider.[1268] Insoweit ist weiter zu unterscheiden: Wo ist der Content-Provider niedergelassen? Befindet er sich im Inland oder hat er seine Niederlassung im EU-Ausland? Falls sich der Content-Provider im Inland niedergelassen hat, wird die zuständige Behörde ihre Kontrollmaßnahmen nicht gegen den Access-Provider, sondern gleich gegen den Content-Provider richten. Denn der Content-Provider ist der eigentliche Störer. Im Gegensatz dazu kann der Access-Provider als Nichtstörer angesehen werden.[1269] Zudem ist es viel effektiver, den inländischen Content-Provider, der eine Schlüsselposition im Internet einnimmt, zum Sperren oder Löschen des rechtswidrigen Inhalts aufzufordern als den Access-Provider zu bemühen.[1270] Folglich machen Sperranordnungen gegen den Access-Provider nur Sinn, wenn der Content-Provider im EU-Ausland niedergelassen ist.[1271] Die einzige Fallvariante, die zu einer Anwendbarkeit des Art. 3 II bis VI ECRL beim Access-Provider führt, besteht somit aus einem Access-Provider, der zwar im EU-Ausland niedergelassen ist, dessen Technik für das Access-Providing sich aber im Inland befindet.[1272] Des weiteren müssen durch die staatlichen Kontrollmaßnahmen, die an den Access-Provider adressiert sind, rechtswidrige Inhalte eines Content-Providers gesperrt werden, der ebenfalls seine Niederlassung in einem anderen Mitgliedstaat hat.[1273]

bb. Allgemeines Beschränkungsverbot

Gemäß Art. 3 II ECRL sind Sperranordnungen grundsätzlich nicht zulässig, da sie den freien Verkehr von Diensten der Informationsgesellschaft, sowohl die des Access-Providers als auch mittelbar die des Content-Providers aus einem anderen Mitgliedstaat

---

[1268] Diese Inhalte können natürlich wiederum von einem Service-Provider im Internet bereitgehalten werden.

[1269] Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3149.

[1270] Holznagel, „Verantwortlichkeit im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte“, ZUM 2000, 1007, 1022.

[1271] Fraglich bleibt hier, ob es effektiver ist, gegenüber dem Content-Provider, der zwar im EU-Ausland niedergelassen ist, dessen Technik für das Content-Providing aber im Inland befindlich ist, Sperr- und/oder Löschanordnung ergehen zu lassen oder ob dann nicht schon eine Sperrverfügung gegen den Access-Provider wirkungsvoller wäre. Dies kann nur für jeden Fall gesondert entschieden werden. Je nachdem, ob die staatlichen Kontrollmaßnahmen schnell und einfach an den Content-Provider gerichtet werden können. Vgl. Zimmermann, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145, 3149.

[1272] Dies gilt nur für den Access-Provider. Falls der Sperr-VA gegen einen Access-Provider ergeht, der im Inland niedergelassen ist, die zu sperrenden Inhalte allerdings bei einem Content-Provider im EU-Ausland befindlich sind, dann kann sich zwar nicht der Access-Provider, aber der betroffene Content-Provider auf Art. 3 II bis VI ECRL berufen. An der Prüfung des Content-Providers ändert sich bei dieser Fallvariante nichts. Die Ergebnisse bleiben gleich. Vgl. deshalb unten unter B. 3. Teil. 3. Kapitel. II. 3. c. cc. (2).

[1273] Für den Fall, dass der Access-Provider und/oder der Content-Provider mehrere Niederlassungen in verschiedenen Mitgliedstaaten besitzen, dann kommt wieder Ziff. 19 der Erwägungsgründe zur E-Commerce-Richtlinie zu Anwendung. Vgl. auch obige Fn. 1222.

regelmäßig aus Gründen einschränken, die in den koordinierten Bereich i.S.d. Art. 2 h ECRL fallen.[1274]

cc. Ausnahmetatbestand des Art. 3 IV ECRL

Es könnte jedoch hier erneut die Ausnahmevorschrift des Art. 3 IV ECRL eingreifen. Da der Access-Provider und der Content-Provider von der Sperranordnung unterschiedlich betroffen sind, ist allerdings zwischen den beiden Providern und ihrer jeweiligen Sichtweise zu differenzieren:

(1) Sichtweise des Access-Providers

Eine Abweichung von den Bestimmungen des Art. 3 II ECRL setzt voraus, dass die Sperrmaßnahmen die Kriterien des Art. 3 IV ECRL erfüllen: Die Sperrmaßnahmen ergehen aus Gründen der öffentlichen Ordnung und Sicherheit i.S.d. Art. 3 IV a i) 1. und 3. Spiegelstrich ECRL.[1275] Des weiteren müssen sie einen bestimmten Dienst der Informationsgesellschaft, der die in Art. 3 IV a i) ECRL genannten Schutzziele beeinträchtigt oder eine ernsthafte und schwerwiegende Gefahr für die Beeinträchtigung dieser Ziele darstellt, betreffen. Der Access-Provider stellt einen bestimmten Dienst der Informationsgesellschaft i.S.d. Art. 2 a ECRL dar.[1276] Problematisch ist jedoch, dass der Access-Provider selbst die Schutzziele des Art. 3 IV a i) ECRL direkt nicht beeinträchtigt. Lediglich durch das Tätigwerden des Nutzers, der eine bestimmte Internet-Adresse auswählt, worauf der rechtswidrige Inhalt des Content-Providers zum Abruf bereitgehalten wird, kommt der Access-Provider mit den ungewünschten Internet-Angeboten in Kontakt. Er stellt den Zugang zu den Inhalten her und bringt dem Nutzer die rechtswidrigen Daten auf dessen Rechner. Ob in diesem automatischen Vorgang des Access-Providings eine direkte Beeinträchtigung der öffentlichen Ordnung und Sicherheit i.S.d. Art. 3 IV a ii) ECRL zu sehen ist, braucht nicht entschieden zu werden.[1277] Denn zumindest kann darin eine ernsthafte und schwerwiegende Gefahr für eine Beeinträchtigung der in Art. 3 IV a i) ECRL genannten Schutzziele gesehen werden, so dass jedenfalls Art. 3 IV a ii) ECRL erfüllt ist.

Schließlich bestimmt Art. 3 IV a iii), dass die Sperrmaßnahmen in einem angemessenen Verhältnis zu den angestrebten Schutzzielen stehen: Die gegen den Access-Provider gerichteten Sperrmaßnahmen sind geeignet, diese Schutzziele zu erreichen, weil durch sie ein Ausbreiten der rechtswidrigen Inhalte verhindert wird. Der Nutzer kann die unerwünschten Internet-Seiten im Inland nicht mehr mit Hilfe des Access-Providers aufru-

---

[1274] Vgl. oben bei B. 3. Teil. 3. Kapitel. II. 3. a. bb. und b. bb.

[1275] Siehe oben unter B. 3. Teil. 3. Kapitel. II. 3. a. cc.

[1276] Hoeren, „Vorschlag für eine EU-Richtlinie über E-Commerce“, MMR 1999, 192, 194; vgl. insoweit auch Ziff. 18 der Erwägungsgründe zur E-Commerce-Richtlinie.

[1277] Es erscheint aber durchaus vertretbar, dass bereits beim reinen Access-Providing, das für eine Vervielfältigung der rechtswidrigen Inhalte verantwortlich ist, eine unmittelbare Beeinträchtigung der Schutzziele des Art. 3 IV a i) ECRL angenommen wird.

fen. Die rechtswidrigen Daten bleiben somit beim Content-Provider und können wenig Schaden anrichten, da sie nicht mehr in das Inland zu den jeweiligen Nutzern gelangen können. Eine Vervielfältigung der rechtswidrigen Inhalte wird hierdurch eingedämmt. Die Sperrmaßnahmen sind darüber hinaus auch erforderlich, weil sie – aus technischer Sicht – die einzige Möglichkeit darstellen, auf den rechtwidrigen Inhalt Einfluss zu nehmen. Schließlich sind sie auch angemessen. Denn der Umstand, dass der Access-Provider bestimmte Adressen im Internet für den Nutzer nicht mehr zugänglich machen darf, beeinträchtigt ihn nur marginal. So gibt es im Internet weiterhin unzählige Inhalte, die für den Nutzer frei zugänglich sind. Falls nur ein paar Internet-Seiten nicht mehr abrufbar sind, wird dies häufig vom Nutzer gar nicht bemerkt. Für ihn erfüllt der Access-Provider ordnungsgemäß den gewünschten Dienst. Folglich hat der Access-Provider durch die staatlichen Sperranordnungen kaum Schwierigkeiten auch künftig dem Nutzer seine Dienste anzubieten. Der Access-Provider ist von der Sperrung einzelner Internet-Adressen ohnehin nur unmerklich betroffen, weil seine Dienste von zahlreichen Nutzern in Anspruch genommen werden und nur die wenigsten einen Zugang zu den gesperrten Inhalten wollen. Die Beeinträchtigung seines Dienstes ist also für ihn kaum spürbar. Auch der technische Aufwand zur Sperrung hält sich – wie oben bereits ausführlich dargestellt[1278] – in Grenzen. Dagegen werden durch die Verbreitung der rechtswidrigen Inhalte des Content-Providers durch den Access-Provider hohe Rechtsgüter bedroht. Das Interesse des Staates, sich und seine Bürger vor den rechtswidrigen Inhalten zu schützen, ist sehr groß. Dahinter muss das Interesse des Access-Providers, seine Dienste ungehindert anbieten zu können, zurücktreten. Die Sperrmaßnahmen sind mithin aus der Sicht des Access-Providers als angemessen und insgesamt als verhältnismäßig anzusehen. Die Sperrmaßnahmen erfüllen somit den Art. 3 IV a ECRL.

(2) Sichtweise des Content-Providers

Durch die gegen den Access-Provider verfügten Sperrmaßnahmen werden zwangsläufig auch die Dienste des Content-Providers beeinträchtigt, der die zu sperrenden Inhalte für die Nutzer im Internet bereithält. Da der Content-Provider nicht im Inland, sondern im EU-Ausland niedergelassen ist, stammen seine Dienste aus einem anderen Mitgliedstaat. Falls nun ein Nutzer aus dem Inland diese Dienste der Informationsgesellschaft i.S.d. Art. 2 h ECRL mit Hilfe eines Access-Providers abrufen will und der Content-Provider wegen der Sperranordnung daran gehindert wird, bestimmte Inhalte dem Nutzer anzubieten, ist der Wortlaut des Art. 3 II ECRL erfüllt. Folglich sind auch diese Beschränkungen des Content-Providings wegen Art. 3 II ECRL grundsätzlich verboten. Allerdings könnte wieder die Ausnahmevorschrift des Art. 3 IV ECRL gegeben sein:

[1278] Vgl. hierzu oben unter B. 1. Teil. III. 1. c.

Die staatlichen Sperranordnungen ergehen aus Gründen der öffentlichen Ordnung und Sicherheit i.S.d. Art. 3 IV a i) ECRL.[1279] Des weiteren betreffen sie einen bestimmten Dienst der Informationsgesellschaft, den Content-Provider.[1280] Durch die unerwünschten Inhalte des Content-Providers, die der Access-Provider sperren soll, werden die in Art. 3 IV a i) ECRL genannten Schutzziele regelmäßig beeinträchtigt oder stellen zumindest eine ernsthafte und schwerwiegende Gefahr einer Beeinträchtigung dieser Ziele dar,[1281] so dass Art. 3 IV a ii) ECRL ebenfalls erfüllt ist. Schließlich müssen gemäß Art. 3 IV a iii) ECRL die Sperranordnungen in einem angemessenen Verhältnis zu den in Art. 3 IV a i) ECRL genannten Schutzzielen stehen:

Die gegenüber dem Access-Provider angeordneten Sperrverfügungen sind grundsätzlich geeignet, die Schutzziele des Art. 3 IV a i) ECRL (teilweise) zu erreichen. Da kein milderes Mittel zur Verfügung steht, auf den rechtwidrigen Inhalt des Content-Providers einzuwirken sowie den Staat und die Nutzer vor ihm zu schützen, ist die Sperranordnung zudem als erforderlich anzusehen.[1282] Fraglich bleibt jedoch, ob die staatliche Sperrverfügung auch angemessen ist. Wie bereits an früherer Stelle ausführlich geprüft wurde,[1283] kann der Access-Provider aus technischen Gründen nicht gezielt nur den rechtswidrigen Inhalt des Content-Providers sperren, da eine Sperrung im Internet nur über die IP-Adresse des betroffenen Systems effizient zu realisieren ist. Dies hat zur Folge, dass nicht nur das rechtswidrige Angebot des Content-Providers auf einem Server gesperrt wird, sondern der gesamte Inhalt des Servers nicht mehr zum Abruf verfügbar ist.[1284] Befindet sich nur ein Content-Provider auf dem Server, dann werden auch seine rechtmäßigen Angebote von der Sperrverfügung erfasst und der Nutzer kann hierauf nicht mehr zugreifen. Denkbar ist jedoch, dass der Content-Provider seine Inhalte auf dem Rechner eines Service-Providers gespeichert hat, worauf noch weitere Content-

---

1279 Siehe oben unter B. 3. Teil. 3. Kapitel. II. 3. a. cc.

1280 Es könnte sich bei Art. 3 IV a ii) ECRL die Frage stellen, ob von ihm nur diejenigen Dienste der Informationsgesellschaft erfasst werden, gegen die auch die staatliche Anordnung gerichtet ist (die des Adressaten also). Denn Art. 3 IV a ii) ECRL spricht lediglich von „*Maßnahmen*“, die einen „*bestimmten*“ Dienst der Informationsgesellschaft „*betreffen*“. Es hängt letztendlich davon ab, wie das Wort „betreffen“ auszulegen ist. Eine Auslegung muss zunächst anhand der E-Commerce-Richtlinie vorgenommen werden, da es sich um einen darin befindlichen europarechtlichen Begriff handelt. Gemäß Art. 1 I ECRL soll die Richtlinie „*einen Beitrag zum einwandfreien Funktionieren des Binnenmarktes leisten, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt*“. Die E-Commerce-Richtlinie will demnach – ganz allgemein – sämtliche Dienste der Informationsgesellschaft erfassen. Ein freier Verkehr der Dienste ist nur möglich, wenn alle Dienste von ihr geregelt werden. Dies darf aber nicht nur für das allgemeine Beschränkungsverbot des Art. 3 II ECRL gelten, sondern muss auch beim „ordre public“ des Art. 3 IV ECRL berücksichtigt werden. Deshalb ist das Wort „betreffen“ in Art. 3 IV a ii) ECRL wörtlich zu verstehen: Sobald durch eine staatliche Maßnahme eines Mitgliedstaates ein bestimmter Dienst der Informationsgesellschaft tangiert wird, egal ob die Maßnahme an ihn adressiert ist oder nicht, ist er hiervon betroffen und Art. 3 IV ECRL kann auf ihn angewendet werden.

1281 Vgl. hierzu oben beim Content-Provider unter B. 3. Teil. 3. Kapitel. II. 3. a. cc.

1282 Siehe oben unter B. 3. Teil. 3. Kapitel. II. 3. c. cc. (1).

1283 Vgl. oben unter B. 1. Teil. III. 1. c. cc. (1).

1284 Koenig/Loetz, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438, 444.

Provider ihre Angebote für die jeweiligen Nutzer bereithalten. In diesem Fall hätte eine Sperrung durch den Access-Provider zur Folge, dass auch deren Dienste den deutschen Markt nicht mehr erreichen können, obwohl sie völlig harmlos sind.[1285] Demnach hat eine Sperrung durch den Access-Provider eine viel größere Wirkung als die Sperr- bzw. Löschanordnungen gegenüber dem Service- und/oder Content-Provider. Der bzw. die Content-Provider wird/werden durch die Sperrung des Access-Providers weit gravierender als in den vorher geprüften Fällen beeinträchtigt. Zwar kann das Interesse des Staates, den Schutz der öffentlichen Ordnung und Sicherheit zu gewährleisten, nachvollzogen werden. Allerdings ist der Preis, mit dem dieses Ziel erreicht wird, sehr hoch. Zu berücksichtigen ist zudem der Umstand, dass mit der Sperrung durch den Access-Provider noch nicht viel erreicht wird. Denn der rechtswidrige Inhalt befindet sich weiter im Internet und kann von anderen Access-Providern bzw. Nutzern jederzeit abgefragt werden. Eine Vervielfältigung des unerwünschten Inhalts wird durch die Sperrung des Access-Providers also nur bedingt verhindert.[1286] Lediglich die Nutzer, die mit Hilfe des Access-Providers, an den die Sperranordnung adressiert war, den rechtswidrigen Inhalt abrufen wollen, werden durch die staatliche Maßnahme daran gehindert. Alle übrigen Nutzer – die Mehrzahl also – können auch weiterhin mit Hilfe anderer Access-Provider auf das illegale Angebot zugreifen. Letztlich bleibt eine Beeinträchtigung der in Art. 3 IV a i) ECRL genannten Schutzziele weiter bestehen. Die Sperrung ist insoweit nicht sehr effektiv. Zudem greift sie in das Recht des Content-Providers auf informationelle Selbstbestimmung in beträchtlichem Maße ein. Das Ergebnis der durch den Access-Provider erfolgten Sperrung und ihre Auswirkungen auch auf rechtmäßige Inhalte des oder der Content-Provider(s) stehen demnach außer Verhältnis. Die Sperrmaßnahmen sind deshalb nicht angemessen und somit unverhältnismäßig.

Art. 3 IV a iii) ECRL ist daher nicht erfüllt. Die Ausnahmevorschrift des Art. 3 IV ECRL findet aus der Sicht des von der Sperrverfügung betroffenen Content-Providers keine Anwendung. Folglich ist weiterhin Art. 3 II ECRL einschlägig, der die Sperrverfügung generell verbietet.

[1285] Dies hat zur Folge, dass hierdurch auch der Service-Provider selbst beeinträchtigt wird, da seine Dienste durch die Port-Sperrung für die Content-Provider fehlerhaft geworden sind. Auf diese Problematik des Service-Providers soll an dieser Stelle nur hingewiesen werden. Eine ausführliche Prüfung der Perspektive des Service-Providers wird aus Gründen der Übersichtlichkeit nicht durchgeführt. Zumal der Inhalt des Content-Providers primär betroffen ist und der Service-Provider nur mittelbar von der Sperrung tangiert wird. Diese Beeinträchtigung des Service-Providers sollte jedoch – der Ordnung halber – aufgezeigt werden. Bezüglich den sich daraus ergebenden Konsequenzen kann auf die Prüfung der Kontrollmaßnahmen, die direkt gegen den Service-Provider ergehen, verwiesen werden. Vgl. insoweit oben unter B. 3. Teil. 3. Kapitel. II. 3. b.

[1286] Vgl. insoweit die Ausführungen bei: Tettenborn/Bender/Lübben/Karenfort, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001 S. 27.

dd. Zwischenergebnis

Zwar sind aus der Sicht des Access-Providers die Voraussetzungen des Art. 3 IV a ECRL erfüllt. Falls die zuständige staatliche Behörde das Verfahren nach Art. 3 IV b ECRL beachtet,[1287] wären eigentlich die staatlichen Maßnahmen als Ausnahme von Art. 3 II ECRL gemäß Art. 3 IV ECRL rechtmäßig. Allerdings erfüllen die Sperranordnungen aus der Perspektive des Content-Providers die Kriterien des Art. 3 IV a ECRL, insbesondere Art. 3 IV a iii) ECRL, nicht. Die Beschränkungen des bzw. der Content-Provider(s) durch die gegen den Access-Provider gerichteten Sperranordnungen sind insoweit unzulässig. Demzufolge sind die Sperrmaßnahmen gegen den Access-Provider insgesamt als rechtswidrig anzusehen. Sie verstoßen gegen Art. 3 II ECRL und demnach gegen das Europarecht.

d. Zusammenfassung

Insgesamt lässt sich nach der vorstehenden Prüfung feststellen, dass üblicherweise sämtliche Sperr- und/oder Löschanordnungen, die gegen einen im EU-Ausland niedergelassenen Content-, Service- oder Access-Provider von den zuständigen staatlichen Polizei- bzw. Sicherheitsbehörden angeordnet werden, gemäß Art. 3 II ECRL verboten sind, da sie den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedstaat einschränken. Abweichend von diesem Grundsatz sind jedoch Sperr- und/oder Löschmaßnahmen, die aus Gründen der öffentlichen Ordnung und Sicherheit gegenüber einem Content- oder Service-Provider verfügt werden, gemäß Art. 3 IV ECRL zulässig, sofern das Verfahren des Art. 3 IV b ECRL beachtet wurde oder Art. 3 V ECRL einschlägig ist.
Gleichwohl ergibt sich aber keine Rechtfertigung nach dem „ordre public“ des Art. 3 IV ECRL für Sperrmaßnahmen, die an den Access-Provider adressiert sind, um bestimmte rechtswidrige Inhalte eines Content-Providers im EU-Ausland für die Nutzer unzugänglich zu machen. Diese Maßnahmen sind aufgrund ihrer negativen Auswirkung auch für rechtmäßige Inhalte und wegen ihrer geringen Effizienz als unverhältnismäßig anzusehen. Da die Ausnahmevorschrift nicht einschlägig ist, bleibt das Verbot des Art. 3 II ECRL für die an den Access-Provider gerichteten Sperrmaßnahmen bestehen. Sie sind insoweit unzulässig und verstoßen gegen das Europarecht.

4. Gegenüberstellung: E-Commerce-Richtlinie und das primäre Gemeinschaftsrecht

Zwischen der E-Commerce-Richtlinie und dem EGV gibt es nicht nur zahlreiche begriffliche, sondern auch inhaltliche Überschneidungen. Beide Regelwerke wollen einen freien Verkehr von Diensten. Auch der „ordre public“ ist sowohl im EGV als auch in

[1287] Es sei denn Art. 3 V ECRL kommt ausnahmsweise zur Anwendung.

der E-Commerce-Richtlinie explizit geregelt. Insoweit hat sich die Richtlinie stark am EGV orientiert. Dies ist wohl auch der Grund, warum bei der Prüfung der einzelnen Provider anhand des Art. 3 ECRL nahezu dieselben Ergebnisse wie bei der weiter vorne vorgenommenen EGV-Prüfung erzielt wurden.[1288]

Allerdings variiert der Anwendungsbereich der Richtlinie und des EGV. Bestimmte Inhalte können nicht vom Anwendungsbereich der Richtlinie erfasst werden,[1289] während der EGV hierauf sehr wohl zur Anwendung kommt. Die Richtlinie stellt somit in manchen Bereichen das speziellere Gesetz dar.[1290] Der EGV bleibt aber daneben weiter anwendbar und kann als ein allgemeines rechtliches Netz für solche Sachverhalte angesehen werden, die nicht unter die E-Commerce-Richtlinie subsumiert werden können. Dieses Netz fängt dann alle europarechtlich relevanten Fälle auf, die nicht unter die E-Commerce-Richtlinie fallen. Die Richtlinie ergänzt somit den EGV und umgekehrt.[1291]

[1288] Vgl. hierzu oben unter B. 3. Teil. 2. Kapitel. V.

[1289] So werden beispielsweise der Warenverkehr sowie bestimmte Internet-Dienste von der E-Commerce-Richtlinie nicht erfasst.

[1290] Vor allem das in Art. 3 IV b und Art. 3 V ECRL enthaltene Verfahren fehlt bei den Grundfreiheiten des EGV.

[1291] Maennel, Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 189.

4. Kapitel: Vereinbarkeit der staatlichen Kontrollmaßnahmen mit dem Europäischen Verfassungsrecht

Neben dem europäischen Primär- und Sekundärrecht in Form des EGV sowie der E-Commerce-Richtlinie könnte durch die staatlichen Kontrollmaßnahmen auch europäisches Verfassungsrecht tangiert sein.

Wesentlich für eine Anwendung des Gemeinschaftsrechts war das Vorliegen einer wirtschaftlichen Komponente bei den jeweiligen Fallvarianten. So verlangen sowohl der EGV als auch die E-Commerce-Richtlinie eine irgendwie ausgestaltete wirtschaftliche Tätigkeit der Diensteanbieter im Internet. Hierfür genügt es zwar schon, dass das bereitgehaltene Angebot bzw. die Dienste der Provider durch Dritte finanziert werden.[1292] Hingegen können rein private Web-Seiten oder Internet-Dienste ohne jeglichen wirtschaftlichen Hintergrund vom EGV bzw. von der E-Commerce-Richtlinie nicht erfasst werden. Diese – häufig zum Meinungsaustausch – bereitgehaltenen Inhalte sind von den staatlichen Kontrollmaßnahmen gleichermaßen betroffen wie die kommerziellen Internet-Angebote. Da auf die Sperr- und/oder Löschanordnungen, die sich gegen diese privaten Provider richten oder die von diesen Kontrollmaßnahmen (un)mittelbar beeinträchtigt werden, weder der EGV noch die E-Commerce-Richtlinie anwendbar ist, kann sich hieraus keine europarechtliche Unzulässigkeit ergeben. Allerdings könnten die staatlich angeordneten Sperr- und/oder Löschmaßnahmen gegen europäisches Verfassungsrecht verstoßen.

I. Europäische Grundrechtscharta

Zunächst könnte ein Verstoß gegen die Charta der Grundrechte der Europäischen Union[1293] (EGRC) in Betracht kommen. Die EGRC wurde am 7. Dezember 2000 in Nizza vom Europäischen Parlament, dem Rat und der Kommission feierlich proklamiert.

Der Präambel dieser Charta ist zu entnehmen, dass sich die Union „*in dem Bewusstsein ihres geistig-religiösen und sittlichen Erbes*“ „*auf die unteilbaren und universellen Werte der Würde des Menschen, der Freiheit, der Gleichheit und der Solidarität*“ gründet. Die Charta „*beruht auf den Grundsätzen der Demokratie und der Rechtsstaatlichkeit. Sie stellt die Person in den Mittelpunkt ihres Handelns, indem sie die Unionsbürgerschaft und einen Raum der Freiheit, der Sicherheit und des Rechts begründet*“. Des weiteren heißt es in der Präambel, dass die Charta „*unter Achtung der Zuständigkeiten und Aufgaben der Gemeinschaft und der Union und des Subsidiaritätsprinzips die Rechte*“ bekräftigt, „*die sich vor allem aus den gemeinsamen Verfassungstraditionen und den gemeinsamen internationalen Verpflichtungen der Mitgliedstaaten, aus dem Vertrag*

[1292] Maennel, Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187, 188.

[1293] Charta der Grundrechte der Europäischen Union vom 18.12.2000, ABl. EG Nr. C 364.

über die Europäische Union und den Gemeinschaftsverträgen, aus der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, aus den von der Gemeinschaft und dem Europarat beschlossenen Sozialchartas sowie aus der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften und des Europäischen Gerichtshofs für Menschenrechte ergeben".

Gemäß Art. 51 I 1 EGRC gilt die Charta „*für die Organe und Einrichtungen der EU unter Einhaltung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union*". Demnach ist die Charta nur dann für die Mitgliedstaaten beachtlich, wenn sie EU-Recht ausüben.[1294] Auf nationale Normen und deren Durchführung hat die Charta offensichtlich keinen Einfluss.[1295] Die Charta stellt also lediglich einen unverbindlichen Grundrechtskatalog dar, den die Behörden bei der Ausübung nationalen Rechts (noch) nicht zu beachten haben.[1296] Für die staatlichen Sperrmaßnahmen, die auf nationalen Gesetzen beruhen, spielt die Europäische Grundrechtscharta deshalb bislang keine Rolle.[1297]

II. Europäische Menschenrechtskonvention

Im Gegensatz zur Europäischen Grundrechtscharta wurde die Konvention zum Schutze der Menschenrechte und Grundfreiheiten[1298] (EMRK) bereits am 4. November 1950 in Rom unterzeichnet. Die Konvention trat am 3. September 1953 nach der Ratifizierung durch 10 Staaten in Kraft. Im Jahre 1996 waren von den 40 Mitgliedstaaten des Europarates 34 an die EMRK gebunden.[1299] Unter diesen Staaten befinden sich sämtliche Mitgliedstaaten der EU, also auch die Bundesrepublik Deutschland. Folglich könnte die EMRK für die staatlichen Kontrollmaßnahmen von Bedeutung sein.

1. Einleitung

Die EMRK ist grundsätzlich ein völkerrechtlicher Vertrag. Ein derartiger Vertrag regelt üblicherweise nur Verpflichtungen zwischen den Mitgliedstaaten. Allerdings haben diese Mitgliedstaaten gemäß Art. 62 EMRK die normalen Streitbeilegungsmechanismen des Völkerrechts ausgeschaltet, um den Verfahren der kollektiven Durchsetzung durch die in der Konvention geschaffenen Organe (Kommission und Gerichtshof) den Vor-

---

1294 Siehe auch Sporn, „Das Grundrecht der Meinungs- und Informationsfreiheit in einer Europäischen Grundrechtscharta", ZUM 2000, 537, 539.

1295 Vgl. Stock, „EU-Medienfreiheit – Kommunikationsgrundrecht oder Unternehmerfreiheit?", K&R 2001, 289, 294 f. sowie Zulegg, „Zum Verhältnis nationaler und europäischer Grundrechte", EuGRZ 2000, 511, 514.

1296 Zulegg, „Zum Verhältnis nationaler und europäischer Grundrechte", EuGRZ 2000, 511, 514.

1297 Vgl. hierzu auch die Gedanken bei Kingreen in: „Die Gemeinschaftsgrundrechte", JuS 2000, 857, 864.

1298 Abgedruckt in: Beck´sche Gesetzestexte, Menschenrechte, 4. Auflage, Nr. 29.

1299 Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Einl. Rdnr. 2.

rang zu geben. Zudem haben alle Vertragsstaaten das Individualbeschwerderecht anerkannt, so dass sich – wie beim EGV – jeder einzelne Bürger der Vertragsstaaten auf die in der Konvention festgelegten Rechte berufen und sie vor dem Europäische Gerichtshof für Menschenrechte (EGMR) einklagen kann. Ohne die Anerkennung des Rechts auf die Individualbeschwerde nach Art. 25 EMRK hätte nur eine Staatenbeschwerde diese Individualrechte sichern können.[1300]

Die Stellung der Konvention im Recht der Mitgliedstaaten ist sehr unterschiedlich. So hat sie in Österreich Verfassungsrang. In der Schweiz ist sie unmittelbar anwendbar und kann Grundlage für eine staatsrechtliche Beschwerde an das Schweizerische Bundesgericht sein, ihr Rang steht dem Verfassungsrecht somit sehr nahe. In Belgien, Luxemburg, den Niederlanden und Frankreich besitzt sie Übergesetzesrang. In Deutschland, Italien, Griechenland, der Türkei und Zypern hat die Konvention hingegen seit ihrer Ratifizierung lediglich den Rang eines innerstaatlichen Gesetzes,[1301] das sowohl die deutschen Gerichte als auch die Verwaltungsbehörden zu beachten haben. Die Behörden dürfen also bei ihrer Tätigkeit nicht gegen die EMRK verstoßen, was gleichermaßen auch für die Polizei- und Sicherheitsbehörden gilt.

Falls staatliche Kontrollmaßnahmen gegen die Provider ergehen, um rechtswidrige Inhalte im Netz zu beseitigen, dann sind diese VAe nur rechtmäßig, wenn sie nicht im Widerspruch zur EMRK stehen. Dies lässt sich auch aus Art. 6 II EUV ableiten, wonach die EU die Grundrechte zu achten hat, wie sie in der EMRK gewährleistet sind und sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben.

Bei der Prüfung der Kontrollmaßnahmen anhand des EGV bzw. der E-Commerce-Richtlinie wurde die EMRK im Rahmen der Verhältnismäßigkeitsprüfung bereits berücksichtigt.[1302] Dies bedeutet, dass nur in den Fällen, wo der EGV sowie die E-Commerce-Richtlinie nicht zur Anwendung kommen, die staatlichen Sperr- und/oder Löschanordnungen ausschließlich anhand der EMRK zu prüfen sind.

2. Relevante Normen der Europäischen Menschenrechtskonvention

Die EMRK enthält verschiedene Regelungen zum Schutz der Menschenrechte und Grundfreiheiten. Davon sind aber nur wenige für die staatlichen Kontrollmaßnahmen relevant. In Betracht kommen lediglich Art. 9 (Gedanken-, Gewissens- und Religionsfreiheit), Art. 10 (Freiheit der Meinungsäußerung), Art. 11 (Versammlungs- und Vereinigungsfreiheit) und Art. 14 EMRK (Diskriminierungsverbot).

[1300] Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Einl. Rdnr. 5.
[1301] Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Einl. Rdnr. 6.
[1302] Vgl. beispielsweise oben unter B. 3. Teil. 2. Kapitel. V. 1. f. aa. (4).

a. Vereinbarkeit der Kontrollmaßnahmen mit Art. 9 EMRK

Zunächst sind Inhalte mit religiösem Inhalt im Internet denkbar. Dabei handelt es sich nicht nur um die friedliche Ausübung bestimmter Religionen und Weltanschauungen. Vielmehr ist es durchaus möglich, dass religiöse Eiferer Webseiten in das Internet stellen, die als rechtswidrig und gefährlich anzusehen sind. Gerade durch die katastrophalen Ereignisse des 11. Septembers 2001 in den USA wird deutlich, wie verheerend sich religiöser Fanatismus auswirken kann. Untersuchungen haben ergeben, dass die Terrororganisation „Al Qaida", die ihre Handlungen mit der Lehre des Islam rechtfertigt, das Internet nicht nur als internes Kommunikationsmittel, sondern vermehrt auch als Forum für ihre Religions- und Weltansichten genutzt hat. Deshalb müssen die zuständigen staatlichen Behörden versuchen, terroristische, intolerante, rassistische und staatsfeindliche Inhalte mit religiösem oder weltanschaulichem Hintergrund durch entsprechende Anordnungen sperren bzw. löschen zu lassen.

Solche Kontrollmaßnahmen könnten allerdings gegen die Gedanken-, Gewissens- und Religionsfreiheit i.S.d. Art. 9 EMRK verstoßen. Aber auch die Meinungsfreiheit des Art. 10 EMRK könnte hiervon betroffen sein. Die Meinungsfreiheit nach Art. 10 EMRK unterscheidet sich von der in Art. 9 EMRK gewährten unantastbaren Gedankenfreiheit dadurch, dass sich bei ihr die Gedanken bereits zu einem mehr oder weniger feststehenden Werturteil verdichtet haben. Die Meinungsfreiheit stellt demnach eine Art Komponente der Gedankenfreiheit dar.[1303] Dies bedeutet zugleich, dass eine klare Trennung der Anwendungsbereiche von Art. 9 und Art. 10 EMRK nicht möglich ist. Beide Vorschriften garantieren Freiheitsrechte, die sich auf den geistigen Betätigungsbereich des Menschen beziehen. Sie unterscheiden sich in ihrem materiellen Inhalt aber insofern, als das Recht der Gedankenfreiheit nach Art. 9 EMRK die Freiheit des Vorgangs einer geistigen Leistung garantiert, während von Art. 10 EMRK sowohl die objektive Seite des Vorgangs der Meinungsbildung, die Informationsfreiheit, als auch die subjektive, die persönlichkeitsinterne Meinungsbildung und die Äußerungsfreiheit, erfasst werden. Die Bedeutung beider Bestimmungen der Konvention liegt darin, dass ihre Freiheitsgarantien den gesamten Bereich der geistigen Betätigung der Person gewährleisten. Diese Freiheitsrechte bilden somit eine Einheit.

Auch die Trennung von religiösen und weltanschaulichen Bekenntnissen einerseits und einer Meinungsäußerung andererseits ist schwierig. Zwar garantiert die Konvention in Art. 9 EMRK gesondert die Freiheit der Religion und der Weltanschauung. Allerdings wird die religiöse und weltanschauliche Bekenntnisäußerung zusätzlich durch Art. 10 EMRK geschützt. Der eigentliche Unterschied zwischen diesen Freiheitsrechten liegt also lediglich im Gegenstand ihrer Äußerung.[1304] Besitzen die Äußerungen einen religi-

---

[1303] Ragaz, Die Meinungsäußerungsfreiheit in der Europäischen Menschenrechtskonvention, S. 53.

[1304] Tsakiridis, Das Recht der Meinungsäußerungsfreiheit nach Artikel 10 der Europäischen Menschenrechtskonvention und die Frage seiner Drittwirkung, S. 121 ff.

ösen oder weltanschaulichen Hintergrund, dann ist wohl zunächst Art. 9 EMRK zu prüfen sein, bevor auf Art. 10 EMRK eingegangen wird. Dabei ist aber zu bedenken, dass Art. 9 EMRK nur die Äußerungen erfasst, die zur Weltanschauungs- bzw. Religionsausübung zu zählen sind.[1305] Da eine genaue Trennung von religiösen bzw. weltanschaulichen Bekenntnissen und Meinungsäußerungen kaum möglich ist und derartige Bekenntnisse in jedem Fall unter Art. 10 EMRK subsumiert werden können,[1306] sind sinnvollerweise sämtliche Meinungsäußerungen – ob mit oder ohne religiösem Hintergrund – anhand des Art. 10 EMRK zu prüfen. Denn die in der nachfolgenden Untersuchung zu Art 10 EMRK gewonnenen Ergebnisse können dann ohne weiteres auch auf Art. 9 EMRK übertragen werden.

b. Vereinbarkeit der Kontrollmaßnahmen mit Art. 10 EMRK

Wie bereits vorstehend festgestellt worden ist, kann vor allem Art. 10 EMRK von den behördlichen Sperr- bzw. Löschanordnungen verletzt sein. Denn in den meisten Fällen wird der Staat gegen rechtswidrige, private Internet-Seiten vorgehen, die ein Content-Provider für die Nutzer zur freien Verfügung in das Internet eingestellt hat. Da hier nur nicht-kommerzielle Inhalte untersucht werden, stellen die Inhalte in der Regel Meinungsäußerungen und Informationen dar. Diese können beispielsweise radikale politische, rassistische, terroristische und pornographische Inhalte aufweisen. Zu denken ist hierbei nicht nur an Text-Dateien, vielmehr können diese frei zugänglichen Angebote auch illegale Bild-, Video- und Musikdateien enthalten. Die fragwürdigen Inhalte stammen regelmäßig von einem Content-Provider, der sie in das Internet eingebracht hat. Für die Speicherung seiner Inhalte kann er sich eines Service-Providers bedienen. Der Nutzer wird sich grundsätzlich mit Hilfe eines Access-Providers Zugang zum Internet und zu den rechtswidrigen Inhalten verschaffen. Die staatlichen Kontrollanordnungen können sich wiederum gegen den Content-Provider direkt, den Service-Provider und/oder den Access-Provider richten, um den unerwünschten Inhalt unschädlich zu machen Allerdings erbringen der Service- und der Access-Provider üblicherweise ihre Internet-Dienste nicht unentgeltlich, so dass auf sie der EGV bzw. die E-Commerce-Richtlinie Anwendung finden.[1307]

Dies hat zur Folge, dass nur der Content-Provider, der seine Informationen im Netz unentgeltlich anbietet und von den Sperr- und/oder Löschanordnungen unmittelbar bzw. mittelbar betroffen ist, in seinem nach Art. 10 EMRK garantierten Recht auf freie Meinungsäußerung verletzt sein kann.[1308] Die Kontrollmaßnahmen können dabei alternativ

---

[1305] Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 9 Rdnr. 1 ff.

[1306] Tsakiridis, Das Recht der Meinungsäußerungsfreiheit nach Artikel 10 der Europäischen Menschenrechtskonvention und die Frage seiner Drittwirkung, S. 123.

[1307] Diesbezüglich kann nach oben verwiesen werden. Vgl. unter B. 3. Teil. 2. Kapitel. und 3. Kapitel.

[1308] Deswegen soll im folgenden nur auf den Content-Provider eingegangen werden. Außerdem können sie nicht in Art. 10 EMRK verletzt sein, da sie nur in ihren Diensten eingeschränkt werden.

bzw. kumulativ gegen ihn, den Service- sowie den Access-Provider ergehen. Bei einem ungerechtfertigten Verstoß gegen Art. 10 EMRK wären die Kontrollmaßnahmen unzulässig.

aa. Art. 10 EMRK und das Internet

Damit die staatlichen Kontrollmaßnahmen auf ihre Vereinbarkeit mit Art. 10 EMRK untersucht werden können, müsste diese Vorschrift zunächst auch auf das Internet Anwendung finden, was zu bejahen ist. Denn Art. 10 I 1 EMRK besagt, dass jede Person das Recht auf freie Meinungsäußerung hat, gleichviel, ob diese Meinung nun verbal, per Radio, Fernsehen oder Internet verbreitet wird. Grundsätzlich fallen daher alle denkbaren Medien und Kommunikationsmöglichkeiten unter den Schutz der Äußerungsfreiheit.[1309] Dies ergibt sich nicht zuletzt aus Art. 10 I 3 EMRK, der zeigt, dass die EMRK auf sämtliche Medien angewendet werden darf.[1310]

bb. Art. 10 I EMRK

Die Meinungsfreiheit des Art. 10 I EMRK enthält verschiedene Unterfälle. So spricht Art. 10 I 1 EMRK zwar noch ausschließlich von der Freiheit, seine Meinung zu äußern. Art. 10 I 2 EMRK macht jedoch deutlich, dass auch die Freiheit, Informationen und Ideen zu empfangen sowie weiterzugeben, unter die Meinungsfreiheit zu fassen ist. Als Vorstadium muss auch die Meinungsbildungsfreiheit, die zum Teil schon von Art. 9 EMRK geschützt wird,[1311] den Schutz der Meinungsfreiheit des Art. 10 EMRK genießen.[1312] Sowohl die Freiheit, Mitteilungen zu empfangen, als auch die Meinungsbildungsfreiheit werden von den staatlichen Kontrollmaßnahmen nur im Hinblick auf den Nutzer, der auf den rechtswidrigen Inhalt des Content-Providers nicht mehr zugreifen kann, relevant. Der Content-Provider selbst, der seine oder fremde Ideen und Informationen für den Nutzer im Internet bereithält, hat hingegen seine Meinung bereits gebildet und will sie nun einer breiten Öffentlichkeit zugänglich machen. Da aber die Sicht des Nutzers bei der vorliegenden Arbeit nicht im Vordergrund steht[1313] und nur die Provider betrachtet werden, die von den staatlichen Sperr- und/oder Löschanordnungen tangiert sein könnten, spielt eine mögliche Rechtsverletzung des Nutzers im Rahmen der EMRK keine Rolle.[1314]

1309 Starmer, European Human Rights Law, Art. 10 Rdnr. 3.143; Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 10 Rdnr. 5.

1310 Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 10 Rdnr. 18.

1311 Vgl. vorstehende Ausführungen. Hier besteht wie in Art. 9 EMRK bei der Gedankenfreiheit ein Vorgang des Innenlebens, der vor jeder Äußerung der Meinung stattfinden muss. Der Staat darf dem Bürger keine Meinungen durch Indoktrinierung oder anderer Mittel aufdrängen.

1312 Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 10 Rdnr. 3; EGMRE vom 07.12.1976, Série A Nr. 23, S. 26 f. Ziff. 53 (Kjeldsen u.a.).

1313 Vgl. oben unter B. 3. Teil. 2. Kapitel IV. 4.

1314 Auf den Nutzer wird deshalb im folgenden nicht eingegangen, sondern es wird nur der Content-Provider betrachtet.

Die Meinungsäußerungsfreiheit ist nach Art. 10 I 1 und 2 EMRK das Recht, Informationen und Ideen anderen ohne Behinderung durch Behörden mitzuteilen. Ausdrücklich wird das Recht auf die Übermittlung über Staatsgrenzen hinweg einbezogen. Dies bedeutet, dass es hier irrelevant ist, ob der Provider, gegen den die Kontrollmaßnahmen angeordnet werden, aus dem Inland oder EU-Ausland stammt.
Ergehen nun behördliche Kontrollmaßnahmen mit dem Ziel, bestimmte Inhalte eines Content-Providers zu sperren bzw. zu löschen, dann stellt dies einen Eingriff in die Meinungsäußerungsfreiheit nach Art. 10 I EMRK dar, der grundsätzlich unzulässig ist. Die Kontrollmaßnahmen wären demnach rechtswidrig. Allerdings könnte Art. 10 II EMRK einschlägig sein, so dass die behördlichen Sperr- und/oder Löschanordnungen doch als rechtmäßig würden, da sie gerechtfertigt sind.

cc. Art. 10 II EMRK

Als einzige Vorschrift der EMRK beginnt Art. 10 II EMRK mit einer Begründung für die Einschränkungsmöglichkeiten der in Art. 10 I EMRK enthaltenen Freiheiten, wonach die Ausübung dieser Freiheiten Pflichten und Verantwortung mit sich bringt. Hieraus kann jedoch keine eigene rechtliche Grundlage für Einschränkungen abgeleitet werden. Eine Beschränkung des Art. 10 I EMRK ist also nur im Rahmen der in Art. 10 II EMRK genannten Bedingungen zulässig.[1315] Als mögliche direkte Beschränkungen der Meinungsfreiheit nennt Art. 10 II EMRK „*Formvorschriften, Bedingungen, Einschränkungen oder Strafandrohungen*“, „*die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung und zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung*“. Der EGMR hat in einer Entscheidung festgestellt, dass – wie im Gemeinschaftsrecht – das Regel/Ausnahmeprinzip auch für die EMRK gilt, so dass Ausnahmen restriktiv zu interpretieren sind.[1316] Die Sperr- und/oder Löschanordnungen stellen aus der Sicht des Content-Providers, dessen rechtswidrige Inhalte von den Kontrollmaßnahmen betroffen sind, Einschränkungen seiner Meinungsäußerungsfreiheit dar. Diese Einschränkungen sind im nationalen Polizei- und Sicherheitsrecht bzw. in den Multimedia-Gesetzen vorgesehen.[1317]
Fraglich ist nun, auf welche Rechtfertigungstatbestände die staatlichen Kontrollmaßnahmen gestützt werden können. Eine Rechtfertigung für die Beeinträchtigung der Meinungsfreiheit könnte vor allem darin gesehen werden, dass die Kontrollmaßnahmen – je

---

[1315] EGMRE vom 25.06.1992, Série A Nr. 239, S. 24 ff. Ziff. 55 ff. (Thorgeirson).
[1316] EGMRE vom 15.07.1982, Série A Nr. 51, S. 33 Ziff. 73 (Eckle).
[1317] Cohen-Jonathan in : Pettiti/Decaux/Imbert/Teitgen, La Convention Européenne Des Droits De L`Homme, 2. Auflage, Art. 10 S. 390.

nach Art des rechtswidrigen Inhalts – in einer demokratischen Gesellschaft für die nationale Sicherheit, für die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung und zur Verhütung von Straftaten, zum Schutz der Moral und zum Schutz des guten Rufs oder der Rechte anderer notwendig sind. Diese aufgelisteten Rechtsbegriffe der EMRK sind allerdings auslegungsbedürftig, da sie sehr allgemein gehalten wurden. Zudem benötigen sie – soweit möglich – eine Definition. Wichtig ist dabei, dass sich die Konvention und ihre Rechtsbegriffe nicht an der Qualifizierung nach nationalem Recht orientieren kann, wenn ihr Schutz nicht illusorisch bleiben soll. Denn jedes Land könnte durch eine Auslegung nach nationalem Recht die Regelungsbestandteile der Konvention aufweichen. Dies gilt insbesondere für die Begriffe, die den Schutzbereich der Konventionsrechte umschreiben. Sie müssen vielmehr – wie die Begriffe des Gemeinschaftsrechts – autonom, also anhand der EMRK und ihrer ratio legis, d.h. ihrem Sinn und Zweck nach, aber nicht ohne Beziehung zu den nationalen Rechtsordnungen und ihrem wertenden Vergleich verstanden werden.[1318] Häufig gibt es aber keine abschließende Definition für die jeweiligen Rechtsbegriffe. Bei Abgrenzungs- und Subsumtionsschwierigkeiten hilft in diesen Fällen ein Blick in die Entscheidungen des EGMR bzw. der Europäischen Kommission für Menschenrechte (EKMR). Darin sind oft Anhaltspunkte enthalten, wann ein bestimmter Sachverhalt noch von einem Rechtsbegriff erfasst wird und wann er nicht mehr unter diesen subsumiert werden kann.[1319] Deshalb sind die zu diesen Begriffen ergangenen wichtigen Urteile und Entscheidungen des EGMR bzw. der EKMR näher zu betrachten, um mit ihrer Hilfe die vorstehend erwähnten unbestimmten Rechtsbegriffe mit Inhalt zu erfüllen:

(1) Nationale und öffentliche Sicherheit

Ein berechtigter Schutz der nationalen und öffentlichen Sicherheit wurde von der EKMR bei der Überprüfung einer Verurteilung wegen neonazistischer Äußerungen in Österreich angenommen.[1320] Auch die Verurteilungen wegen eines Verstoßes nach § 86 StGB, dem Verbreiten von Propagandamitteln verfassungswidriger Organisationen, sind zum Schutz der nationalen Sicherheit und der Rechte anderer als gerechtfertigt angesehen worden.[1321]

[1318] Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Einl. Rdnr. 8; EGMRE vom 15.07.1982, Série A Nr. 51, S. 33 Ziff. 73 (Eckle); EGMRE vom 25.04.1978, Série A Nr. 26, S. 15 Rdnr. 30 (Tyrer).

[1319] Vgl. zu den einzelnen Rechtsbegriffen weiterführend: Bosshard, Die Meinungsäußerungsfreiheit gemäss Art. 10 EMRK unter Berücksichtigung der neueren Entscheide und der neuen Medien, B. V S. 143 ff.

[1320] E 1747/62, Yb 6, 424, 443 f.

[1321] E 12194/86, DR 56, 205, 209.

(2) Aufrechterhaltung der Ordnung und Verhütung von Straftaten

Hinsichtlich der Rechtsbegriffe der Aufrechterhaltung der Ordnung und Verhütung von Straftaten ist als Ordnung nicht nur die Grundlage der öffentlichen Ordnung, sondern auch die Ordnung einer spezifischen sozialen Gruppe oder Institution anzusehen.[1322] Die Verurteilung wegen der sog. „Ausschwitzlüge“ (Rassenhetze) sah die EKMR zum Schutz der öffentlichen Ordnung und zum Schutz des guten Rufes und der Rechte anderer als gerechtfertigt an.[1323] Nicht auszulegen sind die Rechtsbegriffe der Verhütung von Straftaten. Wichtig ist jedoch, dass eine Voraussehbarkeit bei strafrechtlichen Normen gegeben ist.[1324]

(3) Schutz der Moral

Der EGMR hat in einem Urteil zum Rechtsbegriff des Schutzes der Moral betont, dass keine europäische Konzeption der Moral besteht und daher gerade hier die staatlichen Behörden besser zu ihrer Beurteilung in der Lage sind als ein internationales Gericht.[1325] Demnach sind die nationalen Gerichte und Behörden durchaus berechtigt, zu beurteilen, wann eine schädliche Wirkung für die Moral von Kindern und Heranwachsenden zu bejahen ist. Natürlich hängt die Moral sehr stark von staatlichen Traditionen ab, die in gewissem Maße zu berücksichtigen sind.[1326] Der EGMR schränkt den vorgenannten Ermessensspielraum jedoch dadurch ein, dass er ihn einer europäischen Kontrolle unterwirft.[1327]

(4) Schutz des guten Rufes

Der gute Ruf wird in der Regel durch die nationalen Beleidigungsvorschriften geschützt. Zwar sind die Beleidigungsvorschriften zum Schutz des Rechtsfriedens unverzichtbar, jedoch kann mit ihrer Hilfe, je nach Fassung und Anwendung, eine erhebliche Beschränkung der Meinungsfreiheit verbunden sein.[1328] Vor allem, wenn es nicht um die Ehre von Einzelpersonen geht, sondern um Kritik an öffentlichen Institutionen und Amtsträgern, kann die Meinungsfreiheit in ungerechtfertigter Art und Weise unterdrückt werden.[1329] Inzwischen ist aber durch die Rechtsprechung des EGMR geklärt worden,

---

1322 EGMRE vom 08.06.1976, Série A Nr. 22, S. 25 Ziff. 58 (Engel u.a.); Frowein in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 10 Rdnr. 30.

1323 E 25096/94 ; DR 82, 117 ; E 9235/81, DR 29, 194.

1324 Bericht der EKMR vom 12.10.1978, Ziff. 79 ff.; No. 8710/79, DR 28, 77.

1325 EGMRE vom 07.12.1976, Série A Nr. 24, S. 20 ff. Ziff. 42 ff. (Handyside).

1326 EGMRE vom 24.05.1988, Série A Nr. 133, S. 21 ff. Ziff. 31 ff. (Müller u.a.).

1327 EGMRE vom 07.12.1976, Série A Nr. 24, S. 20 ff. Ziff. 42 ff. (Handyside).

1328 Frowein, „Reform durch Meinungsfreiheit“, AöR 105 (1980), 169, 176 f.

1329 Zu nennen ist hierzu ein Beispiel aus der SZ vom 19.06.2001, S. 3. Der Artikel besitzt die Überschrift „Misshandelte Türkinnen“. Darin wird folgender Sachverhalt beschrieben:
„Nazli Top ist Krankenschwester, sie war 32 und im dritten Monat schwanger, als sie vor neun Jahren auf dem Weg nach Hause zu einer Polizeistation geschleppt, zehn Tage festgehalten und schwer misshandelt wurde. Nazli Top war im Juni vor einem Jahr dabei, als in Istanbul erstmals Frauen öf-

dass die Anwendung von Beleidigungsvorschriften dort nicht zu rechtfertigen ist, wo in Wahrheit öffentliche Kritik unterdrückt werden soll.[1330]

(5) Schutz der Rechte anderer

Wie oben beim Rechtsbegriff des guten Rufes schon angedeutet wurde, werden häufig die Rechte anderer durch beleidigende Meinungsäußerungen verletzt. Insofern gibt es Überschneidungen zwischen diesen beiden Einschränkungsgründen. Während aber der Eingriffszweck zum des Schutz des guten Rufes anderer vor allem beleidigende Meinungsäußerungen einschränkt, umfasst ein Schutz der Rechte anderer verschiedenste Sachverhalte. So hat die EKMR in einer Entscheidung das Verbot für einen Lehrer, auf dem Grundstück der Schule mit Plaketten und Aufkleber für seine politischen, moralischen oder religiösen Überzeugungen zu werben, als zum Schutz der Rechte anderer als notwendig bezeichnet.[1331] Unter diesen Schutz fallen also die Rechte der Eltern, dass ihre religiösen und philosophischen Überzeugungen in der Erziehung ihrer Kinder respektiert werden, die Rechte der weiblichen Mitglieder des Lehrkörpers, dass sie nicht durch die Aufkleber des Beschwerdeführers verletzt werden, und die Rechte der Kinder, dass sie nicht durch diese Aufkleber beunruhigt werden. In einem anderen Fall hat die EKMR das Verbot, in der Nähe einer Abtreibungsklinik mit drastischen Fotos gegen Abtreibungen Stellung zu nehmen, ohne nähere Begründung als zum Schutz der Rechte anderer als rechtmäßig angesehen.[1332] Auch der Schutz von religiösen Überzeugungen wird vom EGMR unter die Rechte anderer gefasst.[1333]

(6) Zusammenfassung

Die einzelnen Berichte bzw. Entscheidungen der EKMR und des EGMR sind zwar nur bezüglich bestimmter Sachverhalte ergangen. Gleichwohl können aus ihnen gewisse Grenzen abgeleitet werden, wann ein Eingriff in die Meinungsäußerungsfreiheit gerechtfertigt ist. So können demokratiefeindliche, radikale politische Ansichten unter den Schutz der nationalen und öffentlichen Sicherheit subsumiert werden. Rassistische und volksverhetzende Meinungen dürfen aus Gründen der Aufrechterhaltung der Ordnung in zulässiger Weise gemäß Art. 10 II EMRK verboten werden. Hinsichtlich des Schutzes der Moral besitzen staatliche Behörden einen großen Beurteilungsspielraum,[1334] so dass sich mit der Begründung einer schädlichen Wirkung für die Moral von Kindern

---

fentlich über Gewalt in Polizeihaft sprachen. Sechs Monate nach der Konferenz wurden Nazli Top und andere Sprecherinnen wegen „Beleidigung" der türkischen Sicherheitskräfte angeklagt."

1330 EGMRE vom 26.11.1991, Série A Nr. 217, S. 30 f. Ziff. 52 ff. (Sunday Times); EGMRE vom 26.11.1991, Série A Nr. 216, S. 75 ff Ziff. 79 ff. (Observer und Guardian).

1331 E 8010/77; DR 16, 101.

1332 E 22838/93, DR 80 A, 147, 151.

1333 EGMRE vom 20.09.1994, Série A Nr. 295, S. 17 f. Ziff. 46 ff (Otto-Preminger-Institut); EGMRE vom 25.11.1996, Nr. 23, 1996-V, Ziff. 52 ff. (Wingrove).

1334 EGMRE vom 07.12.1976, Série A Nr. 24, S. 1 ff. Ziff. 1 ff. (Handyside); Bericht der EKMR vom 30.09.1975 zum Fall Handyside, Serie B Nr. 22, S. 8-115.

und Jugendlichen Beschränkungen der Meinungsäußerung rechtfertigen lassen. Eine Rechtfertigung wegen des Schutzes des guten Rufes findet ihre Grenzen dort, wo in Wahrheit öffentliche Kritik unterdrückt werden soll. Dies gilt ebenso für den Schutz der Rechte anderer, was hier oft zu einer Abwägung führt. Bei diesen Ausnahmetatbeständen, die einen Eingriff in die Meinungsfreiheit erlauben, ist jedoch ihre restriktive Anwendung zu beachten.

Diese Erkenntnisse sind nun auf die rechtswidrigen bzw. unerwünschten Inhalte des Content-Providers zu übertragen:

Die häufigsten Arten rechtswidriger Inhalte im Internet stellen pornographische, rassistische, menschenverachtende, demokratiefeindliche, volksverhetzende, terroristische und politisch radikale Gedanken und Meinungen dar. Diese Informationsangebote, die der Content-Provider für die jeweiligen Nutzer bereithält, können demnach aus Gründen des Schutzes der nationalen und öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung sowie des Schutzes der Moral, des guten Rufes und der Rechte anderer in rechtmäßiger Weise nach Art. 10 II EMRK eingeschränkt werden. Natürlich kommt es bei diesen Eingriffen in die Meinungsäußerungsfreiheit auf den Einzelfall an.[1335] Die Sperr- und/oder Löschanordnungen, die gegen die rechtswidrigen bzw. unerwünschten Internet-Inhalte des Content-Providers gerichtet sind, müssen demnach jedes Mal erneut auf ihre Rechtmäßigkeit i.S.d. Art. 10 II EMRK überprüft werden. Im Gegensatz zu den Rechtfertigungsgründen des EGV und der E-Commerce-Richtlinie (Schutz der öffentlichen Ordnung und Sicherheit) besitzt Art. 10 II EMRK noch weitere Rechtfertigungsgründe. Folglich sind die Sperrungen bzw. Löschungen von bestimmten Inhalten im Internet leichter zu rechtfertigen als dies beim EGV bzw. der E-Commerce-Richtlinie möglich ist. Insbesondere der Rechtfertigungsgrund des Schutzes der Moral bietet den staatlichen Behörden sehr leicht die Möglichkeit, auf die unerwünschten Inhalte Einfluss zu nehmen. Wichtig ist jedoch, dass – trotz der Bejahung eines Rechtfertigungsgrundes i.S.d. Art. 10 II EMRK – stets das Prinzip der Verhältnismäßigkeit beachtet wird:[1336]

dd. Verhältnismäßigkeit

In die Meinungsäußerungsfreiheit darf nur dann zulässig eingegriffen werden, wenn durch die Sperr- und/oder Löschanordnungen in verhältnismäßiger Art und Weise gegen die im Internet geäußerten Ideen oder Informationen vorgegangen wird. Die staatlichen Kontrollmaßnahmen müssen also geeignet, erforderlich und angemessen sein.

[1335] So ist es für die Beurteilung der Rechtmäßigkeit einer Einschränkung der Meinungsfreiheit ganz entscheidend, welche Art von Meinung eingeschränkt wird. Politische Kritik unterliegt beispielsweise einem größeren Schutz als Pornographie oder rassistische Äußerungen. Vgl. Starmer, European Human Rights Law, Art. 10 Rdnr. 3.144.

[1336] EGMRE vom 26.09.1995, Série A Nr. 323, S. 47 f. Ziff. 59 ff. (Vogt).

Bevor hierauf konkret eingegangen wird, soll noch einmal hervorgehoben werde, dass eine exakte Prüfung, ob die Kontrollmaßnahmen verhältnismäßig und damit rechtmäßig nach Art. 10 II EMRK ergangen sind, kaum möglich ist. Dies hängt sehr stark vom jeweiligen konkreten Sachverhalt des zu beurteilenden Falles ab,[1337] wobei auch der Rechtfertigungsgrund mitentscheidend ist. Allerdings ist zu bedenken, dass in dieser Arbeit vor allem staatliche Maßnahmen untersucht werden, die sich gegen unerwünschte, rechtswidrige und strafbare Inhalte im Netz richten. Diese Inhalte verstoßen häufig gegen nationales Gesetz und sind deshalb in der Regel nicht als harmlos anzusehen. Wie vorstehend aufgezählt wurde, besitzen sie gefährliches Gedankengut, das sowohl den einzelnen Bürger als auch bestimmte Gruppierungen sowie den Staat selbst bedroht. Es besteht somit grundsätzlich ein berechtigtes Interesse seitens der zuständigen staatlichen Stellen, gegen diese Inhalte vorzugehen und deren Beseitigung zu erwirken.
Bei der Verhältnismäßigkeitsprüfung ist auch zu berücksichtigen, wie dieses Ziel der Beseitigung von rechtswidrigen Inhalten durchgesetzt wird. Die staatlichen Kontrollmaßnahmen können – wie bereits oben angesprochen[1338] – gegen die unterschiedlichen Provider erfolgen.[1339] Dies hat zur Folge, dass unterschiedliche Ergebnisse bei der Frage nach der Verhältnismäßigkeit für den Content-Provider möglich sind:[1340]

(1) Kontrollmaßnahmen gegen den Content-Provider

Die erste Möglichkeit besteht darin, die Sperr- und/oder Löschanordnungen gegen den Content-Provider direkt zu richten. Dies ist dann sinnvoll und effektiv, wenn sich der Content-Provider im Inland befindet oder zumindest ein Inlandsbezug zum Content-Providing besteht.[1341] Ist er jedoch im Ausland niedergelassen, dann ist diese Kontrollmaßnahme häufig nicht von Erfolg gekrönt.[1342]
Die Kontrollanordnungen können dabei gezielt gegen den rechtswidrigen Teil des Informationsangebots des Content-Providers eingesetzt werden. Deshalb ist diese Maßnahme als verhältnismäßig anzusehen. So sind die Sperr- und/oder Löschanordnungen geeignet, die rechtswidrigen Inhalte zu beseitigen. Technisch sind diese Maßnahmen darüber hinaus erforderlich.[1343] Schließlich sind diese Maßnahmen auch angemessen. Das Interesse des Staates, sich, seine Bürger, einzelne Organisationen oder Religionsgemeinschaften vor den rechtswidrigen Inhalten zu schützen, überwiegt bei weitem das

---

1337 Starmer, European Human Rights Law, Art. 10 Rdnr. 3.144.
1338 Vgl. oben unter B. 1. Teil. III. 2. b.
1339 Vgl. hierzu die bei der Prüfung des EGV und der E-Commerce-Richtlinie durchgeführten Verhältnismäßigkeitsprüfungen.
1340 Es sei erneut darauf hingewiesen, dass hier nur ein Verstoß gegen die EMRK beim Content-Provider interessiert. Denn regelmäßig kann nur auf ihn die EMRK allein angewendet werden.
1341 Dies kann beispielsweise dann bejaht werden, wenn die Technik für das Content-Providing im Inland belegen ist.
1342 Dies ergibt sich aus dem Territorialitätsprinzip. Die Behörde besitzt keine inländische Adresse, an die sie die Anordnungen richten kann.
1343 Vgl. hierzu oben unter B. 1. Teil. III. 1. und 2.

Interesse des Content-Providers, seine Ideen oder Informationen frei zu äußern,[1344] zumal die Kontrollmaßnahme nur gegen den rechtswidrigen Inhalt beim Content-Provider gerichtet ist. Seine übrigen Informationen darf er auch weiterhin im Netz anbieten. Die Beeinträchtigung der Meinungsäußerungsfreiheit ist also nicht so gravierend.
Hieraus ergibt sich folgendes Ergebnis: Der Content-Provider wird zwar in seinem Recht auf freie Meinungsäußerung gemäß Art. 10 I EMRK verletzt. Dies geschieht jedoch, sofern ein Rechtfertigungsgrund i.S.d. Art. 10 II EMRK vorliegt, in verhältnismäßiger und damit rechtmäßiger Art und Weise.

(2) Kontrollmaßnahmen gegen den Service-Provider

Des weiteren können staatliche Behörden ihre Kontrollmaßnahmen gegen den Service-Provider richten, der dem Content-Provider den Speicherplatz für dessen rechtswidrige Inhalte zur Verfügung stellt. Dadurch wird der Service-Provider verpflichtet, den illegalen Inhalt, den er auf seinem Rechner für die Nutzer bereithält, zu sperren und/oder zu löschen. Dies ist dann sinnvoll, wenn sich der Content-Provider im Ausland befindet. Hierfür muss aber der Service-Provider im Inland niedergelassen sein oder sich seine Technik zumindest im Inland befinden. Nur so kann gegen ihn effektiv ein Kontrollmaßnahmen-VA erlassen werden.
Letztlich ist durch die gegen den Service-Provider gerichtete Sperr- bzw. Löschanordnung wieder der Content-Provider in seinem Recht auf freie Meinungsäußerung betroffen. Da der Service-Provider ebenfalls, wie vorher der Content-Provider, gezielt lediglich den rechtswidrigen Part des Internet-Angebots beseitigen kann, ist auch diese Maßnahme – aus der Sicht des Content-Providers – als verhältnismäßig anzusehen: Die Sperr- und/oder Löschanordnungen sind geeignet, den unerwünschten Inhalt zu beseitigen, technisch erforderlich.[1345] Und zudem angemessen, weil das Interesse des Content-Providers auf freie Meinungsäußerung hinter den weit gravierenderen Interessen des Staates auf Beseitigung zurücktreten muss. Kann darüber hinaus ein Rechtfertigungsgrund i.S.d. Art. 10 II EMRK bejaht werden, ist die Einschränkung der Meinungsfreiheit als rechtmäßig anzusehen.

(3) Kontrollmaßnahmen gegen den Access-Provider

Schließlich kann sich die staatliche Behörde auch an den Access-Provider wenden und ihn zur Sperrung des Zugangs zum Content-Provider, der den rechtswidrigen Inhalt anbietet, aufzufordern. Eine Löschung des Inhalts mit Hilfe des Access-Providers ist aus technischen Gründen nicht möglich.[1346] Die Inanspruchnahme des Access-Providers ist

---

[1344] Dies gilt zumindest dann, wenn es sich bei den rechtswidrigen Inhalten um solche Inhalte mit krassem politischen, pornographischen, rassistischen, menschenverachtenden bzw. volksverhetzendenden Einschlag handelt.
[1345] Siehe oben unter B. 1. Teil. III. 1. b. und 2. b.
[1346] Vgl. oben unter B. 1. Teil. III. 1. c. cc. (1)., d. und 2. b.

nur dann sinnvoll, wenn sich der Content-Provider und – falls vorhanden – der Service-Provider im Ausland aufhalten. Dann besteht nur noch die Möglichkeit, mittels des Access-Providers auf den Inhalt des Content-Providers Einfluss zu nehmen, indem der Nutzer daran gehindert wird, den fragwürdigen Inhalt über den Access-Provider abzurufen. Dadurch bleibt allerdings der Inhalt des Content-Providers unangetastet. Lediglich die Verbreitung der rechtswidrigen Informationen oder Ideen wird teilweise verhindert.[1347] Ferner hat die Sperranordnung die Wirkung, dass nicht nur gezielt der rechtswidrige Inhalt betroffen ist, sondern sämtliche Inhalte auf dem gesperrten Server von der Kontrollmaßnahme erfasst werden, wodurch auch rechtmäßige Meinungen und Ansichten nicht mehr allen Internet-Nutzern zugänglich gemacht werden können.
Folglich ist die Sperrung des Zugangs zum Server des Content-Providers[1348] grundsätzlich als geeignet anzusehen, um zumindest teilweise erfolgreich gegen den rechtswidrigen Inhalt des Content-Providers vorzugehen. Diese Kontrollmaßnahme ist auch erforderlich, da sie technisch die einzige Möglichkeit darstellt, auf den unerwünschten Inhalt Einfluss zu nehmen. Fraglich bleibt aber, ob sie auch als verhältnismäßig angesehen werden kann. Denn durch die Sperranordnung werden in der Regel auch rechtmäßige Inhalte tangiert.[1349] Es liegt also ein Verstoß gegen Art. 10 I EMRK vor. Zwar könnte auf einen Rechtfertigungsgrund verwiesen werden, jedoch muss angesichts der schwachen Effizienz der Sperrung durch den Access-Provider und der Tatsache, dass neben dem rechtswidrigen Inhalt auch rechtmäßige Inhalte hiervon betroffen sind, die Frage gestellt werden, ob diese Kontrollmaßnahme noch angemessen ist. Dies wurde bei der Prüfung des EGV und der E-Commerce-Richtlinie verneint. Die Rechtfertigungstatbestände des Art. 10 II EMRK sind zwar restriktiv auszulegen, besitzen allerdings keine so hohen Anforderungen wie das Gemeinschaftsrecht. Folglich kann hier nur schwer entschieden werden, ob eine generelle Unverhältnismäßigkeit für diese Fälle angenommen werden soll. Dies richtet sich sehr stark nach dem jeweiligen konkreten Inhalt, wogegen vorgegangen wird. Auch die negativen Auswirkungen einer Adress-Sperrung beim Content-Provider durch den Access-Provider und der Rechtfertigungsgrund sind hierbei wesentlich. Dies zeigt, dass es sich bei dieser Entscheidung um eine Frage des Einzelfalls handelt, die an dieser Stelle nicht abstrakt und abschließend geklärt werden kann.

[1347] Vgl. oben unter B. 1. Teil. III. 1. c. cc. (1).

[1348] Wenn der Content-Provider seinen rechtswidrigen Inhalt bei einem Service-Provider gespeichert hat, ist der gesamte Rechner des Service-Providers mit zahlreichen – vermehrt rechtmäßigen – Inhalten von verschiedenen Content-Provider von dieser Sperrung betroffen.

[1349] Unter Umständen können von den Sperrmaßnahmen auch noch rechtmäßige Inhalte anderer Content-Provider betroffen sein.

ee. Zwischenergebnis

Grundsätzlich sind Sperr- und/oder Löschanordnungen, die in die Meinungsäußerungsfreiheit des Content-Providers eingreifen und damit sein Recht aus Art. 10 I EMRK verletzen, rechtmäßig, sobald ein Rechtfertigungstatbestand des Art. 10 II EMRK vorliegt.[1350] Lediglich bei Sperrmaßnahmen gegenüber dem Access-Provider, die mittelbar den Content-Provider betreffen, muss in manchen Fällen eine Unverhältnismäßigkeit angenommen werden, so dass diese staatlichen Kontrollverfügungen rechtswidrig sind. Sie verstoßen gegen Art. 10 I EMRK, können nicht aus Gründen des Art. 10 II EMRK gerechtfertigt werden und sind deshalb mit dem Europarecht nicht zu vereinbaren.

c. Vereinbarkeit der Kontrollmaßnahmen mit Art. 11 EMRK

Wie bereits an anderer Stelle angesprochen wurde, bietet das Internet virtuelle Meinungsforen und Chat-Rooms an.[1351] Diese Internet-Dienste erlauben den Nutzern, sich virtuell zu versammeln und Meinungen auszutauschen. Natürlich kann diese Art der Internet-Nutzung ebenfalls missbraucht werden,[1352] so dass hier der Staat kontrollierend eingreifen muss. Deshalb kann sich bei einer Sperrung und/oder Löschung solcher virtuellen Versammlungsplätze ein Verstoß gegen Art. 11 EMRK ergeben. Von Art. 11 EMRK, der eigentlich nur die tatsächlichen Versammlungen regeln sollte, dürften auch Versammlungen im Netz erfasst sein, was sich schon aus der ratio des Art. 11 EMRK ergibt. Art. 11 EMRK stellt in gewissem Maße eine Komplementärgarantie zu Art. 10 EMRK dar, so dass derartige Meinungsforen im Internet ebenfalls von ihm geschützt werden müssen.[1353] Zwischen Art. 10 und Art. 11 EMRK besteht eine Art Wechselwirkung, da die Meinungsäußerungsfreiheit nicht von der Versammlungsfreiheit getrennt werden kann. Denn sich zu versammeln und Ansichten austauschen zu können, ist für die von Art. 10 EMRK garantierte Meinungsbildungs- und Meinungsäußerungsfreiheit unabdingbar.[1354] Art. 11 EMRK schützt demnach die kollektive Meinungsfreiheit.[1355]
Wenn nun bestimmte Meinungsforen oder ungewünschte Chat-Rooms durch staatliche Anordnungen gesperrt oder beseitigt werden, ist hiervon regelmäßig Art. 11 I EMRK betroffen. Ein Verstoß gegen die Versammlungs- und Vereinigungsfreiheit liegt also in diesen Fällen vor. Allerdings würde aber – wie bei der Prüfung von Art. 10 EMRK – der rechtfertigende Tatbestand des Art. 11 II EMRK eingreifen. Dieser ist dem Art. 10 II EMRK sehr ähnlich. Für die Frage, inwieweit die durch die staatlichen Kontrollmaß-

---

1350 So auch Herzog, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, S. 275.

1351 Vgl. hierzu oben unter B. 1. Teil. I. 3. b. und c.

1352 Tatsächlich wird vor allem von der rechten Szene in Deutschland diese Art der Internet-Nutzung missbraucht, um ihre rassistischen, volksverhetzenden und demokratiefeindlichen Ansichten weiterzugeben. Des weiteren wird durch einen Zusammenschluss im Netz einzelner politisch radikaler Gruppen das Gemeinschaftsgefühl auf gefährliche Art und Weise gestärkt.

1353 Tsakiridis, Das Recht der Meinungsäußerungsfreiheit nach Artikel 10 der Europäischen Menschenrechtskonvention und die Frage seiner Drittwirkung, S. 123 ff.

1354 E 8317/78, DR 20, 44; E 8440/78, DR 21, 138.

1355 Vgl. EGMRE vom 13.08.1981, Série A Nr. 44, S. 23 f. Ziff. 56 ff. (Young u.a.).

nahmen erfolgte Beeinträchtigung des Art. 11 I EMRK von Art. 11 II EMRK gerechtfertigt werden kann, darf daher auf die Prüfung des Art 10 II EMRK verwiesen werden.[1356]

Im Ergebnis sind also Kontrollmaßnahmen gegen den Content- und Service-Provider als zulässig anzusehen. Nur bei Sperranordnungen gegenüber dem Access-Provider kann es rechtliche Schwierigkeiten geben, sofern die Maßnahmen nicht mehr der Verhältnismäßigkeitsprüfung standhalten. Dann verstößt die staatliche Anordnung gegen Art. 11 EMRK und ist mit dem geltenden Europarecht nicht vereinbar.

d. Vereinbarkeit der Kontrollmaßnahmen mit Art. 14 EMRK

Die Sperrung bzw. Löschung von bestimmten Inhalten im Netz könnte zudem diskriminierende Wirkung haben. Deshalb ist auch ein Verstoß gegen Art. 14 EMRK denkbar. Allerdings besitzt Art. 14 EMRK keine selbständige, von den übrigen normativen Vorschriften der Kommission losgelöste Bedeutung.[1357] Vielmehr verbietet Art. 14 EMRK Diskriminierungen hinsichtlich der in den übrigen normativen Vorschriften der Konvention enthaltenen Rechte und Freiheiten.[1358] Dabei ist jedoch zu beachten, dass eine Maßnahme, die für sich betrachtet den Erfordernissen einer bestimmten Konventionsnorm entspricht, dennoch gegen jene Norm in Verbindung mit Art. 14 EMRK verstoßen kann, weil sie im Ganzen gesehen diskriminierend ist. Art. 14 EMRK stellt also einen integralen Bestandteil aller anderen Konventionsrechte und Freiheiten dar und ist insoweit am Schluss einer möglichen Prüfung der EMRK zu beachten, soweit die Ausübung einer der Rechte aus der Konvention in Frage steht. Dies ist vor allem dann geboten, wenn die Maßnahme kraft eines Schrankenvorbehalts eine zulässige Beschränkung des in Frage stehenden Konventionsrechts darstellt.[1359]

Wie eben ausgeführt, können staatliche Maßnahmen in die Rechte des Art. 9, Art. 10 und Art. 11 EMRK eingreifen. Allerdings sind sie meistens nach dem „ordre-public" der Art. 9 II, Art. 10 II und Art. 11 II EMRK als gerechtfertigt anzusehen. Durch die Sperrung und/oder Löschung von radikalen religiösen oder politischen Ansichten im Internet, besteht somit die Möglichkeit, dass Art. 14 i.V.m. Art. 9, Art. 10 sowie Art. 11 EMRK beeinträchtigt ist. Eine Verletzung von Art. 14 EMRK ist dann zu bejahen, wenn eine willkürliche Ungleichbehandlung gleicher Sachverhalte vorliegt,[1360] wobei eine ungleiche Behandlung nicht immer zu einer Verletzung des Art. 14 EMRK führt. Vielmehr darf die Unterscheidung keinen objektiven und angemessenen Rechtfertigungsgrund haben.[1361] Gemäß dem EGMR ist das Bestehen eines solchen Rechtfertigungs-

---

[1356] Vgl. oben unter B. 3. Teil. 4. Kapitel. II. 2. b. cc.
[1357] EGMRE vom 23.07.1968, Série A Nr. 6, S. 33 f. Ziff. 9 f. (Belgischer Sprachenfall).
[1358] Peukert in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 14 Rdnr. 1 f.
[1359] Peukert in: Frowein/Peukert, Europäische Menschenrechtskonvention, 2. Auflage, Art. 14 Rdnr. 3 f.
[1360] EGMRE vom 07.12.1976, Série A Nr. 24, S. 31 Ziff. 66 (Handyside).
[1361] EGMRE vom 23.07.1968, Série A Nr. 6, S. 34 Ziff. 10 (Belgischer Sprachenfall).

grundes im Verhältnis zu Ziel und Wirkung der zu prüfenden Maßnahme zu beurteilen.[1362] Diese Grundsätze muss die Polizei- und Sicherheitsbehörde beachten. Sie hat die rechtswidrigen Internet-Seiten hinsichtlich der Beurteilung ihrer Rechtswidrigkeit unterschiedslos zu behandeln und entsprechende Anordnungen gegenüber den Providern zu treffen. Ist dies der Fall, dann liegt kein Verstoß gegen Art. 14 i.V.m. Art. 9, Art. 10 bzw. Art. 11 EMRK vor.
Diese Ausführungen zeigen jedoch, dass die Frage, ob generell eine Verletzung des Art. 14 EMRK bejaht werden kann, nicht abstrakt zu beantworten ist, denn dies richtet sich nach der jeweiligen konkreten Sachlage des Einzelfalls und kann hier nicht entschieden werden.

3. Zusammenfassung

Kontrollmaßnahmen der staatlichen Polizei- und Sicherheitsbehörden, die den Content-Provider direkt oder mittelbar betreffen, können gegen die in Art. 9 I , Art. 10 I, Art. 11 I und Art. 14 EMRK garantierten Rechte verstoßen. Dabei sind aber die Sperr- und/oder Löschanordnungen, die gegenüber dem Content- oder Service-Provider ergehen, von Art 9 II, 10 II und 11 II EMRK gerechtfertigt, sobald ein darin enthaltener Rechtfertigungsgrund erfüllt ist.
Sperranordnungen gegen den Access-Provider sind dagegen problematisch. Sie können – je nach Sachlage – unverhältnismäßig und damit unzulässig sein. Das Gleiche gilt im Fall von Art. 14 EMRK, da es auch bei dieser Vorschrift sehr stark auf den Einzelfall ankommt. In diesen beiden letzten Fallkonstellationen ist eine konkrete Prüfung nötig, um ihre Vereinbarkeit mit dem Europarecht, hier mit der EMRK, entscheiden zu können.

[1362] Tsakiridis, Das Recht der Meinungsäußerungsfreiheit nach Artikel 10 der Europäischen Menschenrechtskonvention und die Frage seiner Drittwirkung, S. 129.

C. Endergebnis

Nach Abschluss sämtlicher Prüfungen anhand des relevanten Europarechts ergibt sich aus der vorliegenden Arbeit zusammenfassend folgendes wesentliche Endergebnis:

1. Grundsätzlich sind die staatlichen Möglichkeiten zur Kontrolle des Internets bislang äußerst begrenzt. Je nachdem gegen welchen Provider die Kontrollmaßnahmen gerichtet sind, kommen entweder Sperr- und/oder Löschanordnungen oder nur Sperranordnungen in Betracht. Die zuständigen Behörden dürfen aus nationalrechtlicher Sicht dann tätig werden, wenn die nationalen Vorschriften, d.h. das allgemeine Polizei- und Sicherheitsrecht sowie die Multimediagesetze TDG bzw. MDStV[1363], für die Kontrollmaßnahmen erfüllt sind.

2. Ob diese Kontrollmaßnahmen auch mit dem Europarecht im Einklang stehen, beurteilt sich danach, gegen welchen Provider die Sperr- und/oder Löschanordnungen verfügt werden und welche Art von Diensten der Provider anbietet. Dabei muss zwischen dem angebotenen Dienst, der zumindest mittelbar für den Provider eine wirtschaftliche Tätigkeit darstellt und dem Dienst, der frei und unentgeltlich vom Provider im Internet für die Nutzer bereitgestellt wird, unterschieden werden: Handelt der Provider mit wirtschaftlicher Absicht, so findet das Gemeinschaftsrecht des EGV und der E-Commerce-Richtlinie Anwendung. Sind die Dienste des Providers dagegen ausschließlich privater Natur und weisen sie keinerlei wirtschaftliche Berührungspunkte auf, dann haben die staatlichen Behörden bei ihren Kontrollmaßnahmen nur die EMRK zu beachten.

3. Besitzen die Dienste des Providers auch wirtschaftliche Komponenten und sind demnach der EGV sowie die E-Commerce-Richtlinie anwendbar, so verstoßen die Sperr- und/oder Löschanordnungen, die gegenüber dem Content- und dem Service-Provider verfügt werden, zwar grundsätzlich gegen die Grundfreiheiten des EGV gemäß Art. 28, 43 und 49 EGV sowie gegen das in Art. 3 II ECRL fixierte Beschränkungsverbot verstoßen. Jedoch greift in allen relevanten Fällen die jeweilige „ordre public“-Vorschrift als Rechtfertigungsgrund ein, wodurch letztlich diese Kontrollmaßnahmen europarechtlich zulässig werden.
   Hingegen sind die Sperr-VAe gegen den Access-Provider als europarechtswidrig zu werten. Denn eine Rechtfertigung aus Gründen der öffentlichen Ordnung und Sicherheit scheitert aus der Sicht des Content-Providers an dem Grundsatz der Verhältnismäßigkeit.

[1363] Nach Umsetzung der E-Commerce-Richtlinie können sie nur noch aufgrund des § 5 und § 18 MDStV sowie des Polizei- und Sicherheitsrechts tätig werden. Vgl. oben unter B. 2. Teil. II. 5. b. ff.

4. Werden die Dienste der Provider dagegen ohne finanziellen Hintergrund angeboten – was in der Regel nur beim Content-Provider der Fall ist – kann durch staatliche Kontrollmaßnahmen gegen Art. 9 I, 10 I 11 I und/oder 14 EMRK verstoßen werden. Die Sperr- und/oder Löschanordnungen, die gegen den Content-Provider direkt oder Service-Provider ergehen, sind jedoch zulässig, sobald ein in Art. 9 II, 10 II und/oder 11 II EMRK genannter Rechtfertigungsgrund erfüllt ist. Dies ist regelmäßig der Fall.

   Bei Sperrverfügungen gegen den Access-Provider ist dagegen eine generelle Aussage, ob sie noch durch Art. 10 II EMRK gerechtfertigt seien, problematisch, da dies entscheidend von der Prüfung der Verhältnismäßigkeit und somit der Situation des Einzelfalls abhängt. Gleiches gilt im Ergebnis auch bei der Anwendbarkeit von Art. 14 EMRK.

D. Bewertung und Ausblick

Aus den Ergebnissen der einzelnen Prüfungen resultiert, dass staatliche Behörden in Einklang mit dem Europarecht rechtswidrige Inhalte im Internet sperren bzw. löschen lassen können, wenn ihre Kontrollmaßnahmen an die Content-Provider und Service-Provider gerichtet werden. Kritisch sind jedoch die Sperranordnungen gegen die Access-Provider. Letztendlich handelt es sich dabei im wesentlichen um ein technisches Problem. Denn die Sperrung durch den Access-Provider kann zur Zeit nicht gezielt auf den rechtswidrigen Inhalt beschränkt werden. Je nach Sachlage werden durch die Sperrung vermehrt noch andere – rechtmäßige – Inhalte beim Content-Provider erfasst und häufig darüber hinaus auch Inhalte von anderen Content-Providern gesperrt. Folglich ist/sind der oder die Content-Provider regelmäßig durch die vom Access-Provider vorgenommene Sperrung in unangemessener Art und Weise betroffen. Die Sperranordnung ist deshalb unverhältnismäßig und damit europarechtswidrig.

Gleichwohl ist auch der Standpunkt vertretbar, dass bei besonders schwerwiegenden und gefährlichen Inhalten negative Nebenfolgen für den oder die Content-Provider, die durch eine Sperrung seitens des Access-Providers hervorgerufen werden, von ihm bzw. ihnen in Kauf zu nehmen sind.[1364] Allerdings ist dieser Gedanke schon wegen der Ineffektivität derartiger Sperrungen abzulehnen, denn der Inhalt bleibt weiterhin auf dem Rechner des Content- bzw. Service-Providers, so dass über andere Access-Provider ein Zugriff auf den rechtswidrigen Inhalt jederzeit möglich ist. Die Technik ist momentan leider noch nicht ausgereift, um mit Hilfe des Access-Providers gezielt gegen die unerwünschten Inhalte vorgehen zu können.

Die Internet-Technologie wird jedoch laufend verbessert. Es ist deshalb nur noch eine Frage der Zeit, wann der Access-Provider rechtswidrige Inhalte auf fremden Servern störungsfrei sperren kann. Wenn diese technischen Schwierigkeiten bei der Sperrung erst einmal behoben sind, können auch die Sperranordnungen gegenüber dem Access-Provider dann mit dem Europarecht vereinbar sein. Dies bleibt abzuwarten.

Da die nationalen Behörden die vorbeschriebenen Schwierigkeiten haben, gegen Inhalte im Ausland vorgehen zu können, stellt sich verstärkt die Frage, ob ein weltweites oder zumindest europaweites System zur Kontrolle des Internets eingeführt werden soll. Im Gespräch ist zur Zeit das sogenannte „Platform for Internet Content Selection (PICS)-System".[1365] Auch eine Selbstverpflichtung der Wirtschaft, gegen bestimmte Inhalte im Netz vorzugehen, wird propagiert. Daneben existiert seit längerem die Netiquette, die dem Nutzer gewisse Verhaltensregeln im Internet vorgibt. Alle diese Versuche, unerwünschte Inhalte aus dem Netz zu verbannen, haben jedoch noch nicht die erhoffte Wirkung. Denn die Missachtung dieser – meist freiwilligen – Regulierungsansätze zieht

---

[1364] Vgl. hierzu Holznagel in: „Verantwortlichkeit im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte", ZUM 2000, 1007, 1023.

[1365] Vgl. oben in Fn. 214.

weder für die Provider noch den Nutzer Konsequenzen nach sich. Sie sind also nur eine stumpfe Waffe: So kann das PICS-System von „schwarzen Schafen“ im Internet missbraucht werden. Bis jetzt gibt es nur wenig Provider, die sich ausdrücklich an der Selbstverpflichtung der Wirtschaft beteiligen. Gerade die Vielzahl von kleineren Internet-Diensten hat schon aus Kostengründen kein Interesse, sich bestimmten, verpflichtenden Regelungen zu unterwerfen. Schließlich stellen die Netiquette und andere Verhaltenskodizes im Netz nur den kleinsten gemeinsamen Nenner von Mindeststandards dar, die nur in manchen Bereichen des Internets praktiziert werden und primär für die Nutzer gelten. Die Provider sind hiervon nicht betroffen. Diese vorgestellten Ansätze sind somit – zumindest momentan – ungeeignet, in zufrieden stellender Art und Weise kontrollierend auf das Internet einzuwirken.

Dies bedeutet, dass der Staat auch weiterhin dazu verpflichtet ist, Kontrollmaßnahmen gegen rechtswidrige Inhalte durchzuführen. Werden diese von den jeweiligen Providern nicht beachtet, dann können die staatlichen Behörden bestimmte, von den Gesetzen vorgegebene Zwangsmaßnahmen ergreifen, um dadurch eine schnelle und effektive Kontrolle zu gewährleisten. Allerdings versagen diese Kontrollmechanismen meist bei Inhalten, die jenseits der staatlichen Grenze in das Netz eingespeist werden. Aus diesem Grund muss in Zukunft verstärkt international gegen unerwünschte Inhalte im Internet vorgegangen werden. Der Optimalzustand wäre eine unabhängige, weltweite Kontrollinstanz. Davon sind wir heute noch sehr weit entfernt. Ob dies jemals Wirklichkeit werden kann, lässt sich als Prognose derzeit infolge der mannigfaltigen Einflussfaktoren kaum abschätzen.

Wahrscheinlicher ist dagegen jedoch der Aufbau einer grenzüberschreitenden Zusammenarbeit auf europäischer Ebene. Wie bereits durch bestimmte Initiativen der EU[1366] offensichtlich wurde, besitzt die EU ein erhebliches Interesse an einer Kontrolle des Internets. Vor allem der Kinder- und Jugendschutz spielt dabei eine herausragende Rolle. Die EU hätte auch die nötige Kompetenz, eine umfassende Regelung für das Netz zu entwickeln, was durch die E-Commerce-Richtlinie deutlich wird. Bis ein derartiges

---

[1366] Folgende Initiativen der EU sind insbesondere zu nennen:
- Mitteilung der Kommission über den Jugendschutz und der Menschenwürde in den audiovisuellen und den Informationsdiensten, KOM (96) 487 endg.; hierzu ausführlich bei Bortloff, „Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten“, ZUM 1997, 167, 173 f. sowie Tettenborn, „Die neuen Informations- und Kommunikationsdienste im Kontext der Europäischen Union“, EuZW 1997, 462, 465.
- Grünbuch der Kommission über den Jugendschutz und der Menschenwürde in den audiovisuellen- und Informationsdiensten, KOM (96) 483 endg.; vgl. hierzu ausführlich bei Freytag, Haftung im Netz, S. 24.
- Mitteilungen der Europäischen Kommission für eine Empfehlung des Rates zur Gewährleistung des Jugendschutzes und des Schutzes der Menschenwürde in den audiovisuellen und den Informationsdiensten, KOM (97) 570 endg.; vgl. hierzu ausführlich bei Freytag, Haftung im Netz, S. 25.
- Aktionsplan der Kommission zur Förderung einer sicheren Nutzung des Internets, KOM (97) 582; vgl. hierzu ausführlich in: Lehmann, Rechtsgeschäfte im Netz – Electronic Commerce, S. 41 und Kloepfer/Neun, „Rechtsfragen der europäischen Informationsgesellschaft, EuR 2000, 512, 518 ff.

Gemeinschaftsrecht in Kraft tritt, sollten die Mitgliedstaaten wenigstens untereinander auf dem Wege der Amtshilfe versuchen, der Flut an rechtswidrigen Inhalten im Netz Herr zu werden. Zu denken wäre dabei beispielsweise an eine polizei- und sicherheitsbehördliche Zusammenarbeit innerhalb der EU.[1367] Als Koordinator und Schirmbehörde könnte dabei eine Behörde von Europol dienen. Eine Aufwertung und Erweiterung von Europol für die Kriminalität im Internet wäre wünschenswert. Sobald diese EU-weite Zusammenarbeit funktioniert, könnte an ihre Ausweitung und somit an eine Einbeziehung von Drittstaaten gedacht werden. Vielleicht gelingt es langfristig sogar – zumindest bei Kinderpornographie und Terrorismus im Netz – eine weltweite Ausweitung der internationalen Internet-Kontrolle, gegebenenfalls durch die Einbeziehung der bestehenden Strukturen von Interpol.

Dies alles ist jedoch zunächst noch Zukunftsmusik. Es bereitet den einzelnen Nationen – selbst in Europa – große Probleme, einen Teil ihrer staatlichen Kompetenzen aufzugeben. Die Tatsache, dass damit entscheidend für eine sichere Nutzung des Internets beigetragen wird, überzeugt nicht jedes Land. Durch die E-Commerce-Richtlinie wurde allerdings ein Schritt in die richtige Richtung getan.

Vielleicht ist es besser, wenn die EU – ohne Einverständnis aller Mitgliedstaaten[1368] – ihre bereits bestehenden Kompetenzen vollständig einsetzt, um sich im Interesse aller europäischen Bürger gegen den nationalen Machterhalt durchzusetzen. Zumindest was die Kontrolle des Internets anbelangt, ist eine einheitliche europäische und keine nationale Regelung wünschenswert und unerlässlich.

Bis ein derartiges europäisches Regelwerk für Kontrollmaßnahmen im Internet existiert, ist weiterhin das nationale Recht zu beachten, das allerdings das bereits bestehende Europarecht zu respektieren hat. Zur Zeit können deshalb die Polizei- und Sicherheitsbehörden der jeweiligen Länder nur gegen den Content- und Service-Provider Sperr- und/oder Löschanordnungen ergehen lassen, ohne Gefahr zu laufen, gegen europäisches Recht zu verstoßen. Sperrmaßnahmen gegen den Access-Provider bedürfen dagegen einer intensiven Prüfung, weil sie häufig nicht mit dem Europarecht zu vereinbaren sind.

[1367] So auch Holznagel/Kussel, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347, 351.

[1368] Mit Hilfe von Mehrheitsbeschlüssen.

Literaturverzeichnis

Ackermann Stefan, Ausgewählte Rechtsprobleme der Mailbox-Kommunikation, Saarbrücken 1994.

Ahrens Hans-Jürgen, „Das Herkunftslandprinzip in der E-Commerce-Richtlinie“, CR 2000, 835-841.

Arndt Hans-Wolfgang/Fischer Kristian, Europarecht, 5. Auflage, Heidelberg 2001.

Badach Anatol/Hoffmann Erwin/Knauer Olaf, High Speed Internetworking, Bonn 1994.

Bechtold Stefan, „Multimedia und Urheberrecht“, GRUR 1998, 18-27.

Becker Franz, Grundzüge des öffentlichen Rechts, 7. Auflage, München 2000.

Behrens Peter, “Sind Gesellschaften Niederlassungsberechtigte minderen Rechts?”, EuZW 1991, 97.

Bergmann Magnus, Die Haftung gem. § 5 TDG am Beispiel des News-Dienstes unter Berücksichtigung des EU-Richtlinienvorschlags über den elektronischen Geschäftsverkehr, Münster 2000.

Berner Georg/Köhler Gerd Michael, Polizeiaufgabengesetz, 16. Auflage, München 2000.

Bettinger Torsten/Freytag Stefan, „Privatrechtliche Verantwortlichkeit für Links“, CR 1998, 545-556.

Beucher Klaus/ Leyendecker Ludwig/von Rosenberg Oliver, Mediengesetze, München 1999.

Bleckmann Albert, Europarecht, 6. Auflage, Berlin 1997.

Bleisteiner Stefan, Rechtliche Verantwortlichkeit im Internet, Berlin 1999.

Boele-Woelki/Kessedjian Cathérine (Hrsg.), Internet: Which Court Decides? Which Law Applies?, Den Haag 1998.

Boese Oliver, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, Frankfurt am Main 2000.

Bortloff Nils, „Die Verantwortlichkeit von Online-Diensten“, GRUR Int. 1997, 387-401.

Bortloff Nils, „Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten“, ZUM 1997, 167-175.

Bosshard Irene Laeuchli, Die Meinungsäußerungsfreiheit gemäß Art. 10 EMRK unter Berücksichtigung der neueren Entscheide und der neuen Medien, Bonn 1990.

Bremer Karsten, Strafbare Internet-Inhalte in internationaler Hinsicht, Frankfurt am Main 2001.

Brisch Klaus M., „EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr", CR 1999, 235-244.

Bröhl Georg M., „Rechtliche Rahmenbedingungen für neue Informations- und Kommunikationsdienste", CR 1997, 73-79.

Büchner Wolfgang/Ehmer Jörg/Geppert Martin/u.a. (Hrsg.), Beck´scher TKG-Kommentar, 2. Auflage, München 2000.

Bullinger Martin/Mestmäcker Ernst-Joachim, Multimediadienste – Aufgaben und Zuständigkeit von Bund und Ländern, Rechtsgutachten, Baden-Baden 1997.

Burnstein Matthew R., „Conflicts on the Net: Choise of Law in Transnational Cyberspace", Vand. J. Transnational L. 29 (1996) 75-116.

Calliess Christian/Ruffert Matthias (Hrsg.), Kommentar zu EU-Vertrag und EG-Vertrag, Neuwied 1999.

Cheswick William R./Bellovin Steven M., Firewalls und Sicherheit im Internet: Schutz vernetzter Systeme vor cleveren Hackern, Bonn 1996.

Creifelds Carl/Weber Klaus (Hrsg.), Rechtswörterbuch, 15. Auflage, München 1999.

Decker Ute, „Haftung für Urheberrechtsverletzungen im Internet", MMR 1999, 7-14.

Degenhart Christoph, "Rundfunk und Internet", ZUM 1998, 333-349.

Den Heijer Piet C., DFÜ Daten-Fernübertragung, Niederhausen 1990.

Dern Daniel P., The Internet Guide For New Users, New York 1994.

Dickie John, Internet and Electronic Commerce Law in the European Union, Oxford 1999.

Dietz Ingo Marco/Richter Michael, „Netzzugänge unter Internet Service Providern", CR 1998, 528-535.

Doerfert Carsten, Europarecht, Neuwied 2001.

Dörr Dieter, „Rechtshoheit über Rundfunkveranstalter im Sinne des EG-Rechts", JuS 1997, 557-558.

Dörr Dieter, Anmerkungen zum Urteil des EuGH, Rs. 222/94, 10.09.1996, Slg. 1996, I-4015-4083 (Kommission/Vereinigtes Königreich), JuS 1997, 557-558.

Dubach Alexander, „Freier Warenverkehr in der EU: Der Gerichtshof auf neuen Pfaden?“, DVBl.. 1995, 595-603.

Edwards Lilian/Waelde Charlotte, Law & the Internet, 2. Auflage, Oxford 2000.

Ehlers Dirk/Wolffgang Hans-Michael/Pünder Hermann, Rechtsfragen des Electronic Commerce, Münster 2001.

Ehrkamp Jörg/Mansfeld Godehard, Das Telekommunikations Buch, Düsseldorf 1994.

Eichhorn Bert, Internet-Recht, Köln 2000.

Eichler Alexander, Tagungsberichte zur Bekämpfung der Kriminalität im Internet, CR 1999, 200-204.

Eichler Alexander/Helmers Sabine/Schneider Thorsten, „Link(s) – Recht(s)“, BB-Beilage 18/1997, 23-26.

Engel-Flechsig Stefan, „Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer“, ZUM 1997, 231-239.

Engel-Flechsig Stefan/Maennel Frithjof A./Tettenborn Alexander, „Das neue Informations- und Kommunikationsdienste-Gesetz“, NJW 1997, 2981-2992.

Engel-Flechsig Stefan/Maennel Frithjof A./Tettenborn Alexander, Beck´scher I-uKDG-Kommentar, München 2001.

Engel-Flechsig Stefan/Maennel Frithjof A./Tettenborn Alexander, Neue gesetzliche Rahmenbedingungen für Multimedia, Heidelberg 1998.

Engels Stefan, „Haftung für Anzeigen in Online-Angeboten“, K&R 2001, 338-344.

Epiney Astrid, Umgekehrte Diskriminierungen. Zulässigkeit und Grenzen der discrimination à rebours nach europäischem Gemeinschaftsrecht und nationalem Verfassungsrecht, München 1995.

Erichsen Hans-Uwe/Badura Peter (Hrsg.), Allgemeines Verwaltungsrecht, 11. Auflage, Berlin 1998.

Ernst Stefan, „Rechtliche Fragen bei der Verwendung von Hyperlinks im Internet“, NJW-CoR 1997, 224-228.

Etling-Ernst Martina, TKG Kommentar, Ratingen 1996.

Fangmann Helmut/Scheurle Klaus-Dieter/Wehner Ewald/Schwemmle Michael, Handbuch für Post und Telekommunikation, 2. Auflage, Köln 1990.

Fastenrath Ulrich/Müller-Gerbes Maike, Europarecht, Baden-Baden 2000.

Fischer Hans Georg, Europarecht in der öffentlichen Verwaltung, München 1993.

Fischer Hans Georg, Europarecht, 3. Auflage, München 2001.

Fischer Peter/Köck Heribert Franz, Europarecht, 3. Auflage, Wien 1997.

Flechsig Norbert P./Gabel Detlev, „Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks“, CR 1998, 351-358.

Freytag Stefan, „Digital Millenium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft“, MMR 1999, 207-213.

Freytag Stefan, „Providerhaftung im Binnenmarkt“, CR 2000, 600-609.

Freytag Stefan, „Urheberrechtliche Haftung im Netz“, ZUM 1999, 185-195.

Freytag Stefan, Haftung im Netz, Band 1, München 1999.

Frowein Jochen Abr., „Reform durch Meinungsfreiheit“, AöR 105 (1980), 169-187.

Frowein Jochen/Peukert Wolfgang, Europäische Menschenrechtskonvention, EMRK-Kommentar, 2. Auflage, Kehl 1996.

Fuentes-Camacho Teresa, The International Dimensions of Cyberspace Law, Band 1, Aldershot 2000.

Funk Axel, „Wettbewerbsrechtliche Grenzen von Werbung per E-Mail“, CR 1998, 411-420.

Gabel Detlev, Kommentar zum Urteil des LG Düsseldorf vom 29.04.1998 – Az. 12 O 347/97, K&R 1998, 555-557.

Geiger Rudolf, EUV/EGV, 3. Auflage, München 2000.

Geis Ivo, „Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen“, CR 1999, 772-777.

Gercke Marco, „<<Virtuelles>> Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei der Einrichtung von Hyperlinks“, ZUM 2001, 34-40.

Gounalakis Georgios, „Der Mediendienste-Staatsvertrag der Länder“, NJW 1997, 2993-3000.

Grabitz Eberhard/Hilf Meinhard (Hrsg.), Das Recht der Europäischen Union, Band 1, Loseblattsammlung, München Stand: Juli 2000.

Greissinger Christian, „Die EuGH-Rechtsprechung zur Fernsehrichtlinie“, CR 1999, 112-121.

Greiner Arved, „Sperrungsverfügungen als Mittel der Gefahrenabwehr im Internet“, CR 2002, 620-623.

Gruber Michael (Hrsg.)/**Mader Michael**, Internet und e-commerce, Wien 2000.

Günther Andreas, „Erwünschte Regelung unerwünschter Werbung?“, CR 1999, 172-184.

Hailbronner Kay/Klein Eckart/Magiera Siegfried/Müller-Graff Peter-Chistian, Handkommentar zum Vertrag über die Europäische Union, Band 1, Loseblattsammlung, Köln Stand: November 1998.

Hakenberg Waltraud, Grundzüge des Europäischen Gemeinschaftsrechts, 2. Auflage, München 2000.

Hamann Andreas, „Der Entwurf einer E-Commerce-Richtlinie unter rundfunkrechtlichen Gesichtspunkten“, ZUM 2000, 290-297.

Hance Olivier, Internet Business & Internet Recht, Brüssel 1996.

Härting Niko, „Gesetzentwurf zur Umsetzung der E-Commerce-Richtlinie“, CR 2001, 271-277.

Härting Niko, Internetrecht, Köln 1999.

Helberger Natali, „Die Konkretisierung des Sendestaatsprinzip in der Rechtsprechung des EuGH“, ZUM 1998, 50-60.

Henkel Frank, Tagungsbericht zum VII. Hamburger Datenschutzkolloquium, CR 1999, 536-537.

Herbert Ina, Das Internet, Braunschweig 1995.

Herdegen Matthias, Europarecht, 2. Auflage, München 1999.

Herzog Marco, Rechtliche Probleme einer Inhaltsbeschränkung im Internet, Frankfurt am Main 2000.

Hesse Albrecht, „Zur aktuellen Entwicklung des Rundfunkrechts“, BayVBl. 1997, 132-143.

Hesse Albrecht, „Zur aktuellen Entwicklung des Rundfunkrechts“, BayVBl. 1997, 165-173.

Hilty Reto (Hrsg.), Information Highway, Bern 1996.

Hochstein Reiner, „Teledienste, Mediendienste und Rundfunkbegriff – Anmerkungen zur praktischen Abgrenzung multimedialer Erscheinungsformen“, NJW 1997, 2977-2981.

Hoeren Thomas, „Vorschlag für eine EU-Richtlinie über E-Commerce“, MMR 1999, 192-199.

Hoeren Thomas, Anmerkungen zu den Begründungen des Generalbundesanwalts zur Haftung eines Access-Providers für rechtswidrigen Inhalt in der Einstellungsverfügung vom 26.11.1997 (Az.: 2 BJs 104/96-4), MMR 1998, 93-97.

Hoeren Thomas, Rechtsfragen des Internet: Ein Leitfaden für die Praxis, Köln 1998.

Holznagel Bernd, „Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte“, ZUM 2000, 1007-1028.

Holznagel Bernd/Holznagel Ina, „Zukunft der Haftungsregeln für Internet-Provider“, K&R 1999, 103-106.

Holznagel Bernd/Kussel Stephanie, „Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet“, MMR 2001, 347-352.

Inmon William H., Client-Server-Anwendungen, Berlin 1993.

Intveen Carsten, Internationales Urheberrecht und Internet, Baden-Baden 1999.

Jäger Ulrike/Collardin Markus, „Die Inhaltsverantwortlichkeit von Online-Diensten“, CR 1996, 236-240.

Jarass Hans D./Pieroth Bodo, GG-Kommentar, 5. Auflage, München 2000.

Jessen Tanja, „Vertragsgestaltung und –praxis der Online-Dienste“, ZUM 1998, 282-292.

Jestaedt Thomas/Hohenstatt Klaus-Stefan, „Europarecht bricht nationales Exportkontrollrecht“, EuZW 1992, 44-64.

Johnson David R./Post David, “Law And Borders – The Rise of Law in Cyberspace”, Stanford Law Review 48 (1996), 1367-1402.

Kingreen Thorsten, „Die Gemeinschaftsgrundrechte“, JuS 2000, 857-865.

Klesczewski Diethelm, “Das Ende des Auskunftsersuchens nach § 12 FAG”, JZ 1997, 719-721.

Kloepfer Michael, “Innere Pressefreiheit” und Tendenzschutz im Lichte des Artikels 10 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, Berlin 1996.

Kloos Bernhard, Anmerkungen zum Urteil des LG Frankfurt am Main vom 27.05.1998 (Az.: 3/12 O 173/97), CR 1999, 45-47.

Klußmann Niels, Lexikon der Kommunikations- und Informationstechnik, 2. Auflage, Heidelberg 2000.

Knemeyer Franz-Ludwig, Polizei- und Ordnungsrecht, 8. Auflage, München 2000.

Knobl Peter, „Ein Meilenstein im Europarecht der Banken- und Wertpapierdienstleistungen sowie im Anwendungsbereich der Dienstleistungsfreiheit“, WBl. (Wien) 1995, 309-314.

Koch Frank A., „Neue Rechtsprobleme der Internet-Nutzung“, NJW-CoR 1998, 45-48

Koch Frank A., „Rechtsfragen der Nutzung elektronischer Kommunikationsdienste“, BB 1996, 2049-2058.

Koch Frank A., „Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“, CR 1997, 193-203.

Koch Frank A., Internet-Recht, München 1998.

Koenig Christian, „Regulierungsoptionen für die neuen Medien in Deutschland“, MMR-Beilage 12/1998, 1-12.

Koenig Christian/Engelmann Christina, „E-Commerce mit Arzneimitteln im Europäischen Binnenmarkt und die Freiheit des Warenverkehrs“, ZUM 2001, 19-27.

Koenig Christian/Haratsch Andreas, Europarecht, 2. Auflage, Tübingen 1998.

Koenig Christian/Loetz Sascha, „Sperrungsanordnungen gegenüber Network- und Access-Providern“, CR 1999, 438-445.

Koepfer Michael/Neun Andreas, „Rechtsfragen der europäischen Informationsgesellschaft“, EuR 2000, 512-563.

Köhler Markus/Arndt Hans-Wofgang, Recht des Internet, Heidelberg 2000.

Köhntopp Marit/Köhntopp Kristian, „Datenspuren im Internet“, CR 2000, 248-257.

Kopp Ferdinand O., Verwaltungsverfahrensrecht, 7. Auflage, München 2000.

Kröger Detlef/Gimmy Marc A., Handbuch zum Internetrecht, Berlin 2000.

Kröger Detlef/Moos Flemming, „Mediendienst oder Teledienst?“, AfP 1997, 675-680.

Kröger Detlef/Moos Flemming, „Regelungsansätze für Multimediadienste“, ZUM 1997, 462-471.

Krol Ed, Die Welt des Internet, Bonn 1995.

Kuhlmann Ulrike, „Reingeschaut“, c´t Heft 8, 1997, 148-151.

Kuner Christopher, Internet für Juristen, 2. Auflage, München 1999.

Kyas Othmar, Internet, Bergheim 1994.

Lammarsch Joachim/Steenweg Helge, Internet & Co, 2. Auflage, Bonn 1995.

Larenz Karl, Methodenlehre der Rechtswissenschaft, 6. Auflage, Berlin 1991.

Lecheler Helmut, Einführung in das Europarecht, München 2000.

Léger Philippe, Commentaire Article Par Article Des Traités UE Et CE, Basel 2000.

Lehmann Michael (Hrsg.), Internet- und Multimediarecht (Cyberlaw), Stuttgart 1997.

Lehmann Michael (Hrsg.), Rechtsgeschäfte im Netz – Electronic Commerce, Stuttgart 1999.

Lehmann Michael, „Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht“, CR 1998, 232-234.

Lent Wolfgang, Rundfunk-, Medien-, Teledienste, Frankfurt am Main 2001.

Lenz Carl Otto (Hrsg.), EG-Handbuch Recht im Binnenmarkt, 2. Auflage, Berlin 1994.

Lenz Carl Otto (Hrsg.), EG-Vertrag Kommentar, 2. Auflage, Köln 1999.

Lessing Lawrence, „The Zones of Cyberspace“, Stanford Law Review 48 (1996), 1403-1411.

Leupold Andreas, “Die massenweise Versendung von Werbe-eMails: Innovatives Direktmarketing oder unzumutbare Belästigung des Empfängers?”, WRP 1998, 270-280.

Leupold Andreas, „ <<Push>> und <<Narrowcasting>> im Lichte des Medien- und Urheberrechts“, ZUM 1998, 99-107.

Libertus Michael, „Medienrechtliche Aspekte der Umsetzung der E-Commerce-Richtlinie in Deutschland“, RTkomm 2001, 79-82.

Loewenheim Ulrich/Koch Frank A., Praxis des Online-Rechts, Weinheim 1998.

Lüder Tilman, „Mars: Zwischen Keck und Cassis“, EuZW 1995, 609-610.

Maennel Frithjof A., „Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission“, MMR 1999, 187-192.

Mankowski Peter, „Wettbewerbsrechtliches Gerichtspflichtigkeits- und Rechtsanwendungsrisiko bei Werbung über Websites“, CR 2000, 763-769.

Manssen Gerrit (Hrsg.), Telekommunikations- und Multimediarecht, Loseblattsammlung, Berlin Stand: 22.11.2001.

Marwitz Petra, „Das System der Domainnamen“, ZUM 2001, 398-404.

Marwitz Petra, „Haftung für Hyperlinks“, CR 1998, 369-374.

Mayer Franz C., „Recht und Cyberspace“, NJW 1996, 1782-1791.

Mayer Patrick G., Das Internet im öffentlichen Recht: unter Berücksichtigung europarechtlicher und völkerrechtlicher Vorgaben, Berlin 1999.

Mayer Patrick, „Selbstregulierung im Internet: Institutionen und Verfahren zur Setzung technischer Standards“, K&R 2000, 13-19.

Moritz Hans-Werner, „§ 5 TDG im deutschen Recht – die wissenschaftliche Diskussion ist eröffnet“, MMR 1998, 625-626.

Müller-Using Detlev/Lücke Richard, „Neues Recht für Multimedia-Dienste“, ArchivPT 1997, 101-109.

o.V., Die ZEIT, Nr. 18 vom 25.04.1997, S. 22.

o.V., PC Magazin 2/2002, „Es wächst und wächst...“, S. 12.

o.V., Süddeutsche Zeitung vom 19.03.2001, S. 3.

Orwell George, 1984, 33. Auflage, Frankfurt am Main 2000.

Ory Stephan, „http://www.medienpolizei.de?“, AfP 1996, 105-110.

Osthaus Wolf, „Die Renaissance des Privatrechts im Cyberspace“, AfP 2001, 13-23.

Palandt Otto, Bürgerliches Gesetzbuch, 60. Auflage, München 2001.

Palm Franz/Roy Rudolf, “Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte”, NJW 1996, 1791-1797.

Pankoke Stefan L., Von der Presse- zur Providerhaftung, München 2000.

Paulweber Michael, „Europäische Telekommunikationspolitik an der Schwelle zum 21. Jahrhundert: Liberalisierung und Wettbewerb versus Harmonisierung und Reregulierung“, ZUM 2000, 11-36.

Pechstein Matthias/Koenig Christian, Die Europäische Union, 3. Auflage, Tübingen 2000.

Pelz Christian, „Die strafrechtliche Verantwortlichkeit von Internet-Providern“, ZUM 1998, 530-534.

Perritt Henry, Law and the Information Highway, New York 1996.

Pettiti Louis-Edmond/Decaux Emmenuel/Imbert Pierre-Henri/Teitgen Pierre-Henri, La Convention Européenne Des Droits de L´Homme, 2. Auflage, Paris 1999.

Pichler Rufus, „Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG“, MMR 1998, 79-88.

Ragaz Peter Curdin, Die Meinungsäußerungsfreiheit in der Europäischen Menschenrechtskonvention, Bern 1979.

Reich Norbert, Bürgerrechte in der Europäischen Union, Baden-Baden 1999.

Riehm Thomas, „Die Brandschutzmauer“, NJW-CoR 1997, 337-342.

Rosenbaum Oliver, PC/EDV-Lexikon, Berlin 2000.

Rossnagel Alexander, Recht der Multimedia-Dienste, Loseblattsammlung, München Stand: 1. Januar 2000.

Rutkowsky Heinz/Gerhardt Bernd, Leitfaden des Computerrechts, Stuttgart 1989.

Sachs Michael/Battis Ulrich, Grundgesetz, 2. Auflage, München 1999.

Säcker Christopher, „Die Haftung von Diensteanbietern nach dem Entwurf des EGG“, MMR-Beilage 9/2001, 2-4.

Santifaller Michael, TCP/IP and ONC/NFS, 2. Auflage, Workingham 1994.

Schaar Peter, „Datenschutzfreier Raum Internet?“, CR 1996, 170-177.

Schack Haimo, „Internationale Urheber-, Marken- und Wettbewerbsrechtsverletzungen im Internet“, MMR 2000, 59-65.

Schaefer Martin/Rasch Clemens/Braun Thorsten, „Zur Verantwortlichkeit von Online-Diensten und Zugangsvermittlern für fremde urheberrechtsverletzende Inhalte“, ZUM 1998, 451-458.

Scheja Katharina, „Das Grünbuch zur Konvergenz“, CR 1998, 358-360.

Schneider Hans-Jochen (Hrsg.), Lexikon Informatik und Datenverarbeitung, 4. Auflage, München 1997.

Schneider Jochen, Handbuch des EDV-Rechts, 2. Auflage, Köln 1997.

Schrader Hans-Hermann, „Datenschutz bei Multimediadiensten“, CR 1997, 707-710.

Schuppert Stefan, „Web-Hosting-Verträge“, CR 2000, 227-234.

Schuster Fabian/Müller Ulf, „Entwicklung des Internet- und Multimediarechts von Juli 2000 bis März 2001“, MMR-Beilage 7/2001, 1-40.

Schwarz Mathias (Hrsg.), Recht im Internet, Loseblattsammlung, Stadtbergen Stand: Mai 2001.

Schwarze Jürgen (Hrsg.), EU-Kommentar, Baden-Baden 2000.

Schwarze Jürgen, „Medienfreiheit und Medienvielfalt im Europäischen Gemeinschaftsrecht“, ZUM 2000, 779-790.

Schweitzer Michael/Hummer Waldemar, Europarecht, 5. Auflage, Berlin 1996.

Sieber Ulrich, „Computerkriminalität und Informationsstrafrecht“, CR 1995, 100-113.

Sieber Ulrich, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I)“, CR 1997, 581-598.

Sieber Ulrich, „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II)“, CR 1997, 653-669.

Sieber Ulrich, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1)“, JZ 1996, 429-442.

Sieber Ulrich, „Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (2)“, JZ 1996, 494-507.

Sieber Ulrich, Anmerkungen zum CompuServe-Urteil des AG München, MMR 1998, 438-448.

Sieber Ulrich, Verantwortlichkeit im Internet, München 1999.

Spindler Gerald, „Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme“, ZUM 1996, 533-563.

Spindler Gerald, „Die Haftung von Online-Diensteanbieter im Konzern“, CR 1998, 745-757.

Spindler Gerald, „E-Commerce in Europa“, MMR-Beilage 7/2000, 4-21

Spindler Gerald, „Haftungsrechtliche Grundprobleme der neuen Medien“, NJW 1997, 3193-3199.

Spindler Gerald, „Verschuldensabhängige Produkthaftung im Internet“, MMR 1998, 23-29.

Spindler Gerald, „Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-Commerce-Richtlinie“, MMR 1999, 199-207.

Sporn Stefan, „Das Grundrecht der Meinungs- und Informationsfreiheit in einer Europäischen Grundrechtscharta“, ZUM 2000, 537-544.

Starmer Keir, European Human Rights Law, London 2000.

Steckler Brunhilde, Grundzüge des EDV-Rechts, München 1999.

Stock Anja, „Kinder und Internet – eine Bestandsaufnahme“, DRiZ 1997, 431-438.

Stock Martin, „EU-Medienfreiheit – Kommunikationsgrundrecht oder Unternehmerfreiheit?“, K&R 2001, 289-302.

Stögmüller Thomas, „Konvergenz in der Telekommunikation“, CR 1998, 733-738.

Streinz Rudolf, Europarecht, 5. Auflage, Heidelberg 2001.

Strömer Tobias H., Online§Recht, 2. Auflage, Heidelberg 1999.

Tanenbaum Andrew S., Computernetzwerke, 3. Auflage, München 1997.

Tettenborn Alexander, „Die neuen Informations- und Kommunikationsdienste im Kontext der Europäischen Union“, EuZW 1997, 462-467.

Tettenborn Alexander, „E-Commerce-Richtlinie: Politische Einigung in Brüssel erzielt“, K&R 2000, 59-63.

Tettenborn Alexander, „Europäischer Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R 1999, 252-258.

Tettenborn Alexander/Bender Gunnar/Lübben Natalie/Karenfort Jörg, „Rechtsrahmen für den elektronischen Geschäftsverkehr“, K&R Beilage 1 zu Heft 12/2001, 1-40.

Thomas Oppermann, Europarecht, 2. Auflage, München 1999.

Tilch Horst (Hrsg.), Deutsches Rechts-Lexikon, Band 3, 2. Auflage, München 1992.

Timme Michael/Hülk Fabian, „Das Ende der Sitztheorie im internationalen Gesellschaftsrecht? – EuGH, EuZW 1999, 216“, JuS 1999, 1055-1058.

Trautwein Thomas, „Dienstleistungsfreiheit und Diskriminierungsverbot des Europäischen Gemeinschaftsrechts“, JURA 1995, 191-193.

Tsakiridis Panagiotis, Das Recht der Meinungsäußerungsfreiheit nach Artikel 10 der Europäischen Menschenrechtskonvention und die Frage seiner Drittwirkung, Frankfurt am Main 1988.

van der Groeben Hans/Thiesing Jochen/Ehlermann Claus-Dieter (Hrsg.), Kommentar zum EU-/EG-Vertrag, Band 1, 5. Auflage, Baden-Baden 1997.

Vassilaki Irini E., “Mittäterschaft von arbeitsteilig tätigen Teilorganisationen von Diensteanbietern – Fall CompuServe“, NStZ 1998, 518-522.

Vassilaki Irini E., “Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG”, MMR 1998, 630-638.

Vielhaber Sabine, „Neuer Schutz vor neuen Gefahren? – Jugendschutz im Internet“, MMR-Beilage 9/2001, 16-19.

Völker Stefan, Passive Dienstleistungsfreiheit im Europäischen Gemeinschaftsrecht, Berlin 1990.

von Bonin Andreas/Köster Oliver, „Internet im Lichte neuer Gesetze“, ZUM 1997, 821-829.

von Heyl Cornelius, „Teledienste und Mediendienste nach Teledienstegesetz und Mediendienste-Staatsvertrag“, ZUM 1998, 115-120.

von Hinden Michael, Persönlichkeitsverletzungen im Internet, Tübingen 1999.

Waldenberger Arthur, „Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet – ein Fall des LG Hamburg“, AfP 1998, 373-375.

Waldenberger Arthur, „Electronic Commerce: Der Richtlinienvorschlag der EG-Kommission“, EuZW 1999, 296-303.

Waldenberger Arthur, „Teledienste, Mediendienste und die <<Verantwortlichkeit>> ihrer Anbieter“, MMR 1998, 124-129.

Waltermann Jens/Machill Marcel (Hrsg.), Verantwortung im Internet, Gütersloh 2000.

Washburn Kevin/Evans Jim, TCP/IP, Bonn 1994.

Wetzstein Thomas/Dahm Hermann/Steinmetz Linda/u.a., Datenreisende, Opladen 1995.

William Gibson, Neuromancer, New York 1984.

Wimmer Norbert/Kleineidam Roswitha A./Zang Peter, „Die Verantwortlichkeit für die Verletzung von Urheberrechten im Internet“, K&R 2001, 456-461.

Wischmann Tim, „Rechtsnatur des Access-Providing“, MMR 2000, 461-465.

Wuermeling Ulrich/Felixberger Stefan, „Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz“, CR 1997, 230-238.

Wuermeling Ulrich/Felixberger Stefan, „Staatliche Überwachung der Telekommunikation“, CR 1997, 555-561.

Zimmer Jochen, „Online-Dienste für ein Massenpublikum?“, Media Perspektiven 1995, 476-488.

Zimmermann Andreas, „Polizeiliche Gefahrenabwehr und das Internet“, NJW 1999, 3145-3152.

Zuleeg Manfred, „Der rechtliche Zusammenhalt der Europäischen Gemeinschaft“, ZEuP 1993, 475-497.

Zuleeg Manfred, „Zum Verhältnis nationaler und europäischer Grundrechte“, EuGRZ 2000, 511-517.

Materialien:

Entscheidungen des Europäischen Gerichtshofs:

EuGH,	Rs. 26/62,	05.02.1963,	Slg. 1963, 3-61 (Van Gend en Loos)
EuGH,	Rs. 6/64,	15.07.1964,	Slg. 1964, 1251-1311 (Costa/ENEL)
EuGH,	Rs. 9/70,	06.10.1970,	Slg. 1970, 825-858 (Grad, sog. „Leberpfennig“)
EuGH,	Rs. 2/74,	21.06.1974,	Slg.1974, 631-670 (Reyners/Belgien)
EuGH,	Rs. 155/73,	30.04.1974,	Slg. 1974, 409-447 (Sacchi)
EuGH,	Rs. 8/74, 1	01.07.1974,	Slg. 1974, 837-866 (Dassonville)
EuGH,	Rs. 33/74,	03.12.1974,	Slg. 1974, 1299-1321 (Van Binsbergen)
EuGH,	Rs. 71/76,	28.04.1977,	Slg. 1977, 765-795 (Thieffry)
EuGH,	Rs. 30/77,	27.10.1977,	Slg. 1977, 1999-2028 (Bouchereau)
EuGH,	Rs. 106/77,	09.03.1978,	Slg. 1978, 629-658 (Simmenthal)
EuGH,	verb. Rs. 110/78 und 111/78,	18.01.1979,	Slg. 1979, 35-68 (Van Wesemael u.a.)
EuGH,	Rs. 115/78,	07.02.1979,	Slg. 1979, 399-417 (Knoors)

EuGH, Rs. 120/78, 20.02.1979, Slg. 1979, 649-675 (Rewe, sog. “Cassis-de Dijon”)
EuGH, Rs. 15/79, 08.11.1979, Slg. 1979, 3409-3421 (Groenveld)
EuGH, Rs. 52/79, 18.03.1980, Slg. 1980, 833-880 (Debauve)
EuGH, Rs. 62/79, 18.03.1980, Slg. 1980, 881-905 (Coditel/CinéVog)
EuGH, Rs. 113/80, 17.06.1981, Slg. 1981, 1625-1647 (Kommission/Irland)
EuGH, Rs. 155/80, 14.07.1981, Slg. 1981, 1993-2020 (Oebel)
EuGH, Rs. 279/80, 17.12.1981, Slg. 1981, 3305-3337 (Webb)
EuGH, Rs. 95/81, 09.06.1982, Slg. 1982, 2187-2212 (Kommission/Italien)
EuGH, Rs. 261/81, 10.11.1982, Slg. 1982, 3961-3982 (Rau)
EuGH, Rs. 59/82, 20.04.1983, Slg. 1983, 1217-1235 (Weinvertriebs-GmbH)
EuGH, Rs. 174/82, 14.07.1983, Slg. 1983, 2445-2474 (Sandoz)
EuGH, Rs. 227/82, 30.11.1983, Slg. 1983, 3883-3919 (Van Bennekom)
EuGH, verb. Rs. 286/82 und 26/83, 31.01.1984, Slg. 1984, 377-421 (Luisi und Carbone)
EuGH, Rs. 14/83, 10.04.1984, Slg. 1984, 1891-1920 (Von Colson und Kamann)
EuGH, Rs. 79/83, 10.04.1984, Slg. 1984, 1921-1942 (Harz)
EuGH, Rs. 72/83, 10.07.1984, Slg. 1984, 2727-2768 (Campus Oil)
EuGH, Rs. 229/83, 10.01.1985, Slg. 1985, 1-37 (Leclerc)
EuGH, Rs. 240/83, 07.02.1985, Slg. 1985, 531-552 (Procureur de la République/ADBHU)
EuGH, verb. Rs. 60/84 und 61/84, 11.07.1985, Slg. 1985, 2605-2628 (Cinéthèque)
EuGH, Rs. 247/84, 10.12.1985, Slg. 1985, 3887-3907 (Motte)
EuGH, Rs. 121/85, 11.03.1986, Slg. 1986, 1007-1026 (Conegate)
EuGH, Rs. 96/85, 30.04.1986, Slg. 1986, 1475-1488 (Kommission/Frankreich)
EuGH, Rs. 205/84, 04.12.1986 Slg. 1986, 3755-3815 (Kommission/Bundesrepublik Deutschland)
EuGH, Rs. 178/84, 12.03. 1987, Slg. 1987, 1227-1277 (Kommission/Bundesrepublik Deutschland)
EuGH, Rs. 249/85, 21.05.1987, Slg. 1987, 2345-2361 (Albako)

EuGH, Rs. 352/85, 26.04.1988, Slg. 1988, 2085-2137 (Bond van Adverteerders)

EuGH, Rs. 298/87, 14.07.1988, Slg. 1988, 4489-4516 (SMANOR)

EuGH, Rs. 302/86, 20.09.1988, Slg. 1988, 4607-4633 (Kommission/Dänemark)

EuGH, Rs. 81/87, 27.09.1988, Slg. 1988, 5483-5514 (Daily Mail)

EuGH, Rs. 196/87, 05.10.1988, Slg. 1988, 6159-6175 (Steymann)

EuGH, Rs. 274/87, 02.02.1989, Slg. 1989, 229-257 (Kommission/Deutschland)

EuGH, Rs. C-19/92, 31.03.1991, Slg. 1991, I-1663-1700 (Kraus)

EuGH, Rs. C-340/89, 07.05.1991, Slg. 1991, I-2357-2386 (Vlassopoulou)

EuGH, Rs. C-260/89, 18.06.1991, Slg. 1991, I-2951-2966 (Griechische Monopole)

EuGH, Rs. C-221/89, 25.07.1991, Slg. 1991, I-3905-3971 (Factortame)

EuGH, Rs. C-353/89, 25.07.1991, Slg. 1991, I-4069-4103 (Kommission/Niederlande)

EuGH, Rs. C-76/90, 25.07.1991, Slg. 1991, I-4221-4246 (Säger)

EuGH, Rs. C-367/89, 04.10.1991, Slg. 1991, I-4621-4654 (Richardt)

EuGH, verb. Rs. C-6/90 und C-9/90, 19.11.1991, Slg. 1991, I-5357-5418 (Francovich)

EuGH, Rs. C-47/90, 09.06.1992, Slg. 1992, I-3669-3712 (Delhaize)

EuGH, Rs. C-2/90, 09.07.1992, Slg. 1992, I-4431-4481 (Kommission/Belgien)

EuGH, verb. Rs. C-271/90, C-281/90 und C-289/90, 17.11.1992, Slg. 1992, I-5833-5870 (Spanien/Kommission)

EuGH, verb. Rs. C-267/91 und C-268/91, 24.11.1993, Slg. 1993, I-6097-6132 (Keck und Mithouard)

EuGH, Rs. C-292/92, 15.12.1993, Slg. 1993, I-6787-6824 (Hünermund u.a.)

EuGH, Rs. C-315/92, 02.02.1994, Slg. 1994, I-317-339 (Verband Sozialer Wettbewerb)

EuGH, Rs. C-18/93, 17.05.1994, Slg. 1994, I-1783-1827 (Corsica Ferries)

EuGH, verb. Rs. C-401/92 und C-402/92, 02.06.1994, Slg. 1994, I-2199-2236 (Tankstation`t Heukske vof und Boermans)

EuGH, verb. Rs. C-69/93 und C-258/93, 02.06.1994, Slg. 1994, I-2355-2370 (Punto Casa SpA)
EuGH, Rs. C-91/92, 14.07.1994, Slg. 1994, I-3325-3360 (Faccini Dori)
EuGH, Rs. C-379/92, 14.07.1994, Slg. 1994, I-3453-3506 (Peralta)
EuGH, Rs. C-17/93, 14.07.1994, Slg. 1994, I-3537-3565 (Van der Veldt)
EuGH, Rs. C-43/93, 09.08.1994, Slg. 1994, I-3803-3828 (Vander Elst)
EuGH, Rs. C-381/93, 05.10.1994, Slg. 1994, I-5145-5172 (Kommissi-on/Frankreich)
EuGH, Rs. C-230/93, 10.11.1994, Slg. 1994, I-5243-5266 (Ortscheid)
EuGH, Rs. C-412/93, 09.02.1995, Slg. 1995, I-179-223 (Société d`importation Édouard Leclerc-Simplec)
EuGH, Rs. C-384/93, 10.05.1995, Slg. I-1141-1184 (Alpine Investments BV)
EuGH, Rs. C-470/93, 09.07.1995, Slg. 1995, I-1923-1945 (Mars)
EuGH, Rs. C-55/94, 30.11.1995, Slg. 1995, I-4165-4201 (Gebhard)
EuGH, verb. Rs. C-46/93 und C-48/93, 05.03.1996, Slg. 1996, I-1029-1163 (Brasserie du pêcheur SA und Factortame Ltd.)
EuGH, Rs. C-222/94, 10.09.1996, Slg. 1996, I-4025-4083 (Kommission/Ver-einigtes Königreich)
EuGH, Rs. C-3/95, 12.12.1996, Slg. 1996, I-6511-6542 (Reisebüro Broede)
EuGH, Rs. C-398/95, 05.06.1997, Slg. 1997, I-3091-3122 (Ergasias)
EuGH, Rs. C-56/96, 05.06.1997, Slg. 1997, I-3143-3169 (VT4 Ltd.)
EuGH, Rs. C-70/95, 17.06.1997, Slg. 1997, I-3395-3440 (Sodemare SA)
EuGH, Rs. 368/95, 26.06.1997, Slg. 1997, I-3689-3720 (Familiapress)
EuGH, verb. Rs. C-34/95, C-35/95 und C-36/95, 09.07.1997, Slg. 1997, I-3843-3897 (De Agostini Förlag AB und TV Shop i Sverige AB)
EuGH, Rs. C-190/95, 17.07.1997, Slg. 1997, I-4383-4410 (ARO Lease BV)
EuGH, Rs. C-129/96, 18.12.1997, Slg. 1997, I-7411-7452 (Inter-Environnement Wallonie)
EuGH, Rs. C-158/96, 28.04.1998, Slg. 1998, I-1931-1952 (Kohll)
EuGH, Rs. C-212/97, 09.03.1999, Slg. 1999, I-1484-1498 (Centros)

Entscheidungen des Europäischen Gerichtshofs für Menschenrechte:

EGMRE vom 23.07.1968, Série A Nr. 6, 1-109 (Belgischer Sprachenfall)
EGMRE vom 08.06.1976, Série A Nr. 22, 1-71 (Engel u.a.)
EGMRE vom 07.12.1976, Série A Nr. 23, 1-33 (Kjeldsen u.a.)
EGMRE vom 07.12.1976, Série A Nr. 24, 1-37 (Handyside)
EGMRE vom 25.04.1978, Série A Nr. 26, 1-32 (Tyrer)
EGMRE vom 26.04.1979, Série A Nr. 30, 1-69 (Sunday Times)
EGMRE vom 13.08.1981, Série A Nr. 44, 1-33 (Young u.a.)
EGMRE vom 15.07.1982, Série A Nr. 51, 1-40 (Eckle)
EGMRE vom 24.05.1988, Série A Nr. 133, 1-47 (Müller u.a.)
EGMRE vom 26.11.1991, Série A Nr. 216, 1-85 (Observer und Guardian)
EGMRE vom 26.11.1991, Série A Nr. 217, 1-48 (Sunday Times Nr. 2)
EGMRE vom 25.06.1992, Série A Nr. 239, 1-41 (Thorgeirson)
EGMRE vom 20.09.1994, Série A Nr. 295, 1-38 (Otto-Preminger-Institut)
EGMRE vom 26.09.1995, Série A Nr. 323, 1-54 (Vogt)
EGMRE vom 25.11.1996, Nr. 23, 1996-V, 1937-1978 (Wingrove)

Nationale Gerichtsurteile:

Bundesverfassungsgericht:
BVerfGE 12, 205-264 vom 28.02.1961
BVerfGE 22, 293-299 vom 18.10.1967
BVerfGE 31, 145-184 vom 09.06.1971
BVerfGE 31, 357-363 vom 27.07.1971
BVerfGE 37, 271-305 vom 29.05.1974
BVerfGE 73, 339-388 vom 22.10.1986
BVerfGE 89, 155-213 vom 12,10.1993

Bundesverwaltungsgericht:
BVerwGE vom 06.10.1989, Az.: 4 C 11/86 (München), abgedruckt in NJW 1990, 849

Bundesgerichtshof in Zivilsachen:
BGHE vom 05.02.1981, abgedruckt in NJW 1981, 1726-1727

BGHE vom 04.05.1988, abgedruckt in NJW 1988, 2109-2110
BGHZ 97, 269-273 (Urteil vom 21.03.1986)
BGHE vom 28.11.1994, abgedruckt in NJW 1995, 1032-1033
BGHE vom 21.09.1995, abgedruckt in NJW 1996, 54-55

Oberlandesgericht:
Urteil des OLG München vom 08.03.2001 – Az.: 29 U 3282/00, abgedruckt in K&R 2001, 471-478

Landgericht:
Urteil des LG München vom 30.03.2000 – Az.: 7 O 3625/98, abgedruckt in NJW-CoR 2000, 303-306

Amtsgericht:
CompuServe-Urteil des AG München vom 28.05.1998 – Az.: 8340 Ds 465 Js 173158/95, abgedruckt in MMR 1998, 429-438

Gesetzesmaterialien:

Europäisch:
- Grünbuch der Europäischen Kommission über den Jugendschutz und der Menschenwürde in den audiovisuellen und den Informationsdiensten, KOM (96) 483 endg.
- Mitteilung der Kommission über den Jugendschutz und der Menschenwürde in den audiovisuellen und den Informationsdiensten, KOM (96) 487 endg.
- Mitteilung der Kommission über eine Europäische Initiative für den elektronischen Geschäftsverkehr, KOM (97) 157 endg.
- Aktionsplan der Europäischen Kommission zur Förderung der sicheren Nutzung des Internet, KOM (97) 582 endg.
- Grünbuch der Europäischen Kommission vom 01.12.1997 zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen: Ein Schritt in Richtung Informationsgesellschaft, KOM (97) 623 endg.

- Geänderter Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rats über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, KOM (99) 427 endg.

National:

- Bundesrat-Drucksache 80/96 vom 09.02.1996
- Bundesrat-Drucksache 966/96 vom 20.12.1996
- Bundestag-Drucksache 13/7385 vom 09.04.1997
- Bundestag-Drucksache 13/8153 vom 02.07.1997
- Bundestag-Drucksache 14/1191 vom 18.06.1999
- Bayerischer Landtag-Drucksache 13/7716 vom 21.03.1997
- Vorentwurf des Bundesforschungsministeriums für das IuKDG vom 07.06.1996