



universität
wien

DISSERTATION

Titel der Dissertation

Aktuelle Probleme der Durchsetzung von
Immaterialgüterrechten im Internet

Verfasser

Mag.iur. Stephan Steinhofer

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr.iur.)

Wien, im April 2011

Studienkennzahl lt. Studienblatt:

A 083 101

Dissertationsgebiet lt. Studienblatt:

Rechtswissenschaften

Betreuer:

Ao. Univ.-Prof. Dr. Wolfgang Zankl

Für meine Eltern

VORWORT

Die vorliegende Dissertation ist das Ergebnis von jahrelangem Interesse an digitaler Technologie, insbesondere am Internet, und den dadurch entstandenen (und entstehenden) rechtlichen Problemen. Besonders geprägt hat mich dabei die 2007 begonnene Tätigkeit für das Europäische Zentrum für E-Commerce und Internetrecht (e-center), das von meinem Dissertationsbetreuer ao. Univ.-Prof. Dr. Wolfgang Zankl seit bald 10 Jahren geleitet wird. Ihm gilt nicht nur für diese fachlich sehr lehrreiche Zeit, sondern auch für seine persönliche Unterstützung in allen möglichen Belangen mein herzlicher Dank. Selbiges gilt für meine e-center-Kollegen und Freunde Mag. Maximilian Raschhofer und Mag. Lukas Feiler.

In den Mittelpunkt meines juristischen Interesses rückte das Immaterialgüterrecht insbesondere durch ein Praktikum in der Practice Group IP/IT von Wolf Theiss Rechtsanwälte in Wien. Von deren Leiter Dr. Georg Kresbach stammt auch der erste Anstoß für das Thema der Rechtsdurchsetzung im Immaterialgüterrecht, wofür ich ihm damals in der Zeit der Themensuche ebenso dankbar war, wie ich es heute nach Abschluss der vorliegenden Arbeit bin.

Schon bald nach Beginn der Recherchen stellte sich heraus, dass die Konzentration der Untersuchung auf konkrete Problemstellungen im Zusammenhang mit dem Internet der beste Weg war, um nicht in der mittlerweile unüberschaubaren Stoffmenge den Überblick zu verlieren. Zu dieser Erkenntnis hat mir dankenswerter Weise nicht zuletzt Univ.-Prof. Dr. Nikolaus Forgó bei einer Melange beim Europäischen Forum Alpbach 2009 verholfen. Ebenso richtet sich mein Dank an meinen Freund Markus Schanta, der mir während den teilweise stark technisch geprägten Untersuchungen durch sein einschlägiges Fachwissen aus dem Bereich der Informatik eine unverzichtbare Hilfe war.

Den zur Erstellung der Dissertation notwendigen zeitlichen und finanziellen Freiraum verdanke ich zu großen Teilen meinen Eltern, denen diese Arbeit deswegen auch gewidmet ist. Ohne ihre Unterstützung wäre ich womöglich, so wie viele andere Dissertanten, vor der Doppelbelastung durch wissenschaftliche Forschung und notwendige Erwerbsarbeit zurückgeschreckt. Genau aus demselben Grund bedanke ich mich zu guter Letzt auch besonders bei meiner Freundin Nicole, die mich in den vielen Stunden, die ich in den letzten beiden Jahren lesend und schreibend vor dem PC verbracht habe, stets liebevoll mit Zuspruch und Nahrung versorgt hat.

Wien, im Dezember 2010

Stephan Steinhofer

INHALTSVERZEICHNIS

Vorwort.....	5
Inhaltsverzeichnis	7
Abkürzungs- und Rechtsquellenverzeichnis.....	9
A. Einleitung.....	17
A.I. Überblick	17
A.II. Problemendarstellung und Methode	17
A.II.1. Die Zielsetzung und die gewählten Probleme.....	17
A.II.2. Vorgehensweise.....	18
A.II.3. Zitierweise	18
B. Grundlagen	21
B.I. Begriffsklärung	21
B.I.1. Immaterialgüterrecht.....	21
B.I.2. Rechtsdurchsetzung	29
B.I.3. Internet.....	31
B.I.4. Internetprovider.....	32
B.II. Immaterialgüterrechtsverletzungen im Internet	36
B.II.1. Anwendbares Recht und internationale Zuständigkeit	37
B.II.2. Faktische Grenzen der Rechtsdurchsetzung im Internet	38
B.III. Immaterialgüterrecht als Querschnittsmaterie.....	39
C. Rechtsverletzende Websites	40
C.I. Informationsbeschaffung	41
C.I.1. Whois-Abfrage	41
C.I.2. Offenlegungspflichten	44
C.I.3. Zivilrechtlicher Auskunftsanspruch gegen Host-Provider	48
C.II. Unterbindung der Verletzungshandlung	58
C.II.1. Anspruch auf Unterlassung.....	58
C.II.2. Anspruch auf Unterlassung gegen Internetprovider	67
C.III. Genugtuung	107

C.III.1.	Anspruch auf angemessenes Entgelt.....	107
C.III.2.	Anspruch auf Schadenersatz und Herausgabe des Gewinns	108
C.III.3.	Anspruch auf Rechnungslegung.....	111
C.III.4.	Anspruch auf Urteilsveröffentlichung.....	112
D.	Rechtsverletzendes Filesharing.....	115
D.I.	Informationsbeschaffung	117
D.I.1.	Exkurs: Die Überwachung von BitTorrent-Filesharing.....	118
D.I.2.	Zivilrechtlicher Auskunftsanspruch gegen Access-Provider	120
D.I.3.	Auskunft über Inhaber von IP-Adressen im Strafverfahren.....	150
D.II.	Unterbindung der Verletzungshandlung.....	161
D.II.1.	Anspruch auf Unterlassung gegen Filesharer	161
D.II.2.	Anspruch auf Unterlassung gegen Access-Provider	162
D.III.	Genugtuung	167
D.III.1.	Anspruch auf angemessenes Entgelt.....	167
D.III.2.	Anspruch auf Schadenersatz und Herausgabe des Gewinns	168
D.III.3.	Anspruch auf Urteilsveröffentlichung.....	169
E.	Rechtsverletzendes Keyword-Advertising	170
E.I.	Informationsbeschaffung	172
E.II.	Unterbindung der Verletzungshandlung	172
E.II.1.	Anspruch auf Unterlassung gegen Keyword-Advertiser.....	172
E.II.2.	Anspruch auf Unterlassung gegen Suchmaschinenbetreiber	184
E.III.	Genugtuung	190
E.III.1.	Anspruch auf angemessenes Entgelt.....	190
E.III.2.	Anspruch auf Schadenersatz und Herausgabe des Gewinns	191
E.III.3.	Anspruch auf Urteilsveröffentlichung.....	191
F.	Resümee & Ausblick	193
G.	Literaturverzeichnis.....	195
	Abstract	203
	Lebenslauf	205

ABKÜRZUNGS- UND RECHTSQUELLENVERZEICHNIS

aA	anderer Ansicht
ABGB	Allgemeines Bürgerliches Gesetzbuch, JGS 946/1811, zuletzt geändert durch BGBl I 58/2010
aF	Alte Fassung
ABl	Amtsblatt der Europäischen Gemeinschaft/Union
abl	ablehnend
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
arg	argumentum
Art	Artikel
B2B	business to business
B2C	business to consumer
BGBI	Bundesgesetzblatt
BGH	(deutscher) Bundesgerichtshof
Bsp	Beispiel(e)
B-VG	Bundesverfassungsgesetz, BGBl 1/1930, zuletzt geändert durch BGBl I 98/2010
bzw	beziehungsweise
CR	Computer und Recht (Zeitschrift)
Datenschutz-RL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23.11.1995, 31-50; zuletzt geändert durch Verordnung 1882/2003/EG des Europäischen Parlaments und des Rates vom 29. September 2003
ders	derselbe
dgl	dergleichen
dh	das heißt

DSG	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl I 165/1999, zuletzt geändert durch BGBl I 133/2009
dUrhG	(Deutsches) Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz), dBGBl I 1965, 1273, zuletzt geändert durch dBGBl I 2008, 2586
ECG	Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz), BGBl I 152/2001
E-Commerce-RL	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 200 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl L 178 vom 17.7.2000, 1–16
EG	Europäische Gemeinschaft
EGZPO	Gesetz vom 1. August 1895 betreffend die Einführung des Gesetzes über das gerichtliche Verfahren in bürgerlichen Rechtsstreitigkeiten (Civilprozessordnung), RGBl 112/1895, zuletzt geändert durch BGBl I 30/2009
EK	Europäische Kommission
ELR	European Law Reporter
EMRK	Europäische Menschenrechtskonvention
EO	Gesetz vom 27. Mai 1896, über das Exekutions- und Sicherungsverfahren (Exekutionsordnung), RGBl 79/1896, zuletzt geändert durch BGBl I 111/2010
Enforcement-RL	Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl L 157 vom 30.4.2004, 45-86; zuletzt berichtigt in ABl L 195 vom 2.6.2004
Erl	Erläuterungen
ErwGr	Erwägungsgrund

etc	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EUV	Vertrag über die Europäische Union
EUGVVO	Verordnung 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, ABl L 12 vom 16.1.2001, 1; zuletzt geändert durch Verordnung 416/2010/EU der Kommission vom 12. Mai 2010
f	folgende
FN	Fußnote
Frankfurt aM	Frankfurt am Main (Stadt)
FS	Festschrift
GA	Generalanwalt
gem	gemäß
GG	Grundgesetz für die Bundesrepublik Deutschland, dBGBI 1/1949, zuletzt geändert durch dBGBI I 944/2010
GRC	Charta der Grundrechte der Europäischen Union
grds	grundsätzlich
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRURInt	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil (Zeitschrift)
GZ	Geschäftszahl
hA	herrschende Ansicht
Hg	Herausgeber
HG	Handelsgericht
HlSchG	Halbleiterschutzgesetz, BGBI 372/1988, zuletzt geändert durch BGBI I 96/2006

hM	herrschende Meinung
ICANN	Internet Corporation for Assigned Names and Numbers
idR	in der Regel
idZ	in diesem Zusammenhang
ieS	im engeren Sinne
IKT	Informations- und Kommunikationstechnologien
Info-RL	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl 167 vom 22.6.2001, 10-19; zuletzt berichtigt durch ABl L 6 vom 10.1.2002, 71
insb	insbesondere
IP	Internet Protocol bzw Intellectual Property
IPRG	Bundesgesetz vom 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz), BGBl 304/1978, zuletzt geändert durch BGBl I 135/2009
iSd	im Sinne des/der
ISP	Internet Service Provider
iSv	im Sinne von
iVm	in Verbindung mit
iW	im Wesentlichen
iwS	im weiteren Sinne
JA	Justizausschuss
KOM	Dokument/Mitteilung der Europäischen Kommission
KSchG	Konsumentenschutzgesetz
leg cit	legis citatae (das soeben zitierte Gesetz)
Lfg	Lieferung
LG	Landgericht, Landesgericht

Lit	Literatur
lit	litera
Marken-RL	Richtlinie 2008/95/EG des Europäischen Parlaments und des Rates vom 22. Oktober 2008 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Marken (kodifizierte Fassung), ABl L 299 vom 8.11.2008, 25–33
Marken-VO	Verordnung 207/2009/EG des Rates vom 26. Februar 2009 über die Gemeinschaftsmarke (kodifizierte Fassung), ABl L 78 vom 24.3.2009, 1-42
mE	meines Erachtens
MedienG	Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz), BGBl 314/1981, zuletzt geändert durch BGBl I 49/2005
MMR	Zeitschrift für Informations-, Telekommunikations- und Medienrecht
MR	Medien und Recht (Zeitschrift)
MR-Int	Medien und Recht - Internationaler Teil (Zeitschrift)
MSchG	Markenschutzgesetz 1970, BGBl 260/1970, zuletzt geändert durch BGBl I 126/2009
MuSchG	Bundesgesetz vom 7. Juni 1990 über den Schutz von Mustern (Musterschutzgesetz 1990), BGBl 497/1990, zuletzt geändert durch BGBl I 151/2005
mwN	mit weiteren Nachweisen
NR	Nationalrat
ÖBl	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht
offenb	offenbar
OGH	Oberster Gerichtshof
ÖJZ	Österreichische Juristenzeitung
OLG	Oberlandesgericht

PatG	Patentgesetz 1970, BGBl 259/1970, zuletzt geändert durch BGBl I 135/2009
Pkt	Punkt
PPG	Bundesgesetz, mit dem ergänzende Regelungen über das Vorgehen der Zollbehörden im Verkehr mit Waren, die ein Recht am geistigen Eigentum verletzen, erlassen werden (Produktpirateriegesetz 2004), BGBl I 56/2004, zuletzt geändert durch BGBl I 17/2007
Produktpiraterie-VO	Verordnung 1383/2003/EG des Rates vom 22. 7. 2003 über das Vorgehen der Zollbehörden gegen Waren, die im Verdacht stehen, bestimmte Rechte geistigen Eigentums zu verletzen, und die Maßnahmen gegenüber Waren, die erkanntermaßen derartige Rechte verletzen, ABl 2003 L 196, 7; zuletzt berichtigt durch ABl L 381 vom 28.12.2004, 87
PS	Praxisschrift
Rahmen-RL	Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, ABl L 108 vom 24.4.2002, 33-50; zuletzt geändert durch Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009
RdW	Recht der Wirtschaft (Zeitschrift)
RIS	Rechtsinformationssystem des Bundes <ris.bka.gv.at>
rk	rechtskräftig
RL	Richtlinie
Rs	Rechtssache (in der Rechtsprechung des EuGH)
RS	Rechtssatz (in der Rechtsprechung des OGH)
Rsp	Rechtsprechung
RV	Regierungsvorlage
Rz	Randziffer
S	Seite

SA	Schlussantrag eines Generalanwalts beim Gerichtshof der Europäischen Union
Slg	Sammlung der Rechtsprechung des Gerichtshofs der Europäischen Union
sog	sogenannt
StGB	Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch), BGBl 60/1974, zuletzt geändert durch BGBl I 58/2010
stRsp	ständige Rechtsprechung
Telekom-Datenschutz-RL	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl L 201 vom 31.7.2002, 37-47; zuletzt geändert durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009
TKG	Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003), BGBl I 70/2003, zuletzt geändert durch BGBl I 50/2010
TLD	Top Level Domain
TRIPS TRIPS-Abkommen	Trade-Related Aspects of Intellectual Property Rights Abkommen über handelsbezogene Aspekte der Rechte des Geistigen Eigentums, BGBl 1/1995
ua	unter anderem
udgl	und dergleichen
UrhG	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl 111/1936, zuletzt geändert durch BGBl I 58/2010
usw	und so weiter
uU	unter Umständen

UWG	Bundesgesetz gegen den unlauteren Wettbewerb 1984, BGBl 448/1984, zuletzt geändert durch BGBl I 79/2007
vgl	vergleiche
VO	Verordnung
Vorratsdatenspeicherungs-RL	Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorrats-speicherung von Daten, die bei der Bereitstellung öffent-lich zugänglicher elektronischer Kommunikations-dienste oder öffentlicher Kommunikationsnetze er-zeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl L 105 vom 13.4.2006, 54-63
VStG	Verwaltungsstrafgesetz 1991, BGBl 52/1991, zuletzt geändert durch BGBl I 111/2010
WIPO	World Intellectual Property Organisation
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
WTO	World Trade Organization
zB	zum Beispiel
zT	zum Teil
ZPO	Gesetz vom 1. August 1895, über das gerichtliche Ver-fahren in bürgerlichen Rechtsstreitigkeiten (Zivilpro-zessordnung), RGrBl 113/1895, zuletzt geändert durch BGBl I 58/2010
zust	zustimmend

A. EINLEITUNG

A.I. Überblick

Im Anschluss an die folgende Einleitung, in der die behandelten Probleme und die dazu verwendete Methode erläutert werden, behandelt Kapitel B zunächst Grundlagen wie Begriffsklärungen, die Rolle des Internets und seine Auswirkungen auf Immaterialgüter sowie die damit einhergehenden Probleme für die Rechtsdurchsetzung im Immaterialgüterrecht.

Danach werden in den Kapiteln C bis E die einzelnen konkreten Problemkreise behandelt, die derzeit aktuelle Herausforderungen für die Durchsetzung von Immaterialgüterrechten im Internet beleuchten.

Im abschließenden Kapitel F wird ein Resümee über die Ergebnisse der Arbeit gezogen und ein Ausblick sowie ein rechtspolitischer Standpunkt dargelegt.

Diese Arbeit wurde am 31.12.2010 abgeschlossen. Spätere Entwicklungen, Entscheidungen und Literaturbeiträge konnten daher nicht mehr berücksichtigt werden.

A.II. Problemdarstellung und Methode

A.II.1. Die Zielsetzung und die gewählten Probleme

Eine Darstellung des gesamten Problemkreises „Rechtsdurchsetzung im Internet“ kann heute wohl nicht mehr in vertretbarem Umfang gegeben werden. Selbst eine Beschränkung auf das Immaterialgüterrecht liefert aufgrund der dynamischen Entwicklung mittlerweile eine unüberschaubare Stoffmenge, wie auch die stetig wachsende rechtswissenschaftliche Lit zeigt.

Für die vorliegende Arbeit wurde daher der Ansatz gewählt, anhand eines einheitlichen Systems drei konkrete und abgrenzbare Problemkreise im Überlappungsbereich zwischen Immaterialgüter- und Internetrecht darzustellen und Lösungsansätze für sie zu liefern. Um dabei gleichzeitig bereits gefestigte Ergebnisse aus Lit und Rsp zu berücksichtigen und weiterführende Erkenntnisse gewinnen zu können, wurden mit rechtsverletzenden Websites, rechtsverletzendem Filesharing und rechtsverletzendem Keyword-Advertising drei Problemstellungen ausgesucht, die in ihrer Breite nicht vollkommen neu sind, aber dennoch genügend Raum für weitere wissenschaftliche und praktische Bearbeitung bieten. Das Ziel der Arbeit und der Auswahl der Problemschwerpunkte ist somit, eine praxisorientierte Analyse des österreichischen Rechts zu aktuellen Herausforderungen der Rechtsdurchsetzung an der Schnittstelle von Internet- und Immaterialgüterrecht zustande zu bringen.

Am Anfang jeden Kapitels steht dazu eine kurze Einführung in die jeweilige Materie, um den notwendigen technischen und historischen Hintergrund für die jeweils behandelten Probleme zu vermitteln. Ganz allgemein gilt, dass dem Titel der Arbeit entsprechend der Fokus der

Darstellung weniger darin liegt, ob und unter welchen Umständen eine Rechtsverletzung überhaupt vorliegt, sondern den Schwierigkeiten bei der Verfolgung bereits feststehender Rechtsverletzungen größerer Platz eingeräumt wird.

A.II.2. Vorgehensweise

Aus dem in dieser Arbeit verwendeten Begriff der „Rechtsdurchsetzung“ ergibt sich, dass zur Darstellung der genannten Probleme eine Dreiteilung der einzelnen Kapitel am besten geeignet ist.¹

Die Probleme der Informationsbeschaffung bei Rechtsverletzungen im Internet sind daher der Ausgangspunkt, um die Durchsetzung von Immaterialgüterrechten im Internet näher zu untersuchen. Dabei stellt sich insb die Frage, wie nähere Informationen zu Identität und Aktivitäten der Rechtsverletzer beigeschafft werden können.

Daran schließen Untersuchungen zur Unterbindung der Verletzungshandlung an. Am bedeutsamsten ist dabei idR der für das Immaterialgüterrecht typische Anspruch auf Unterlassung gegenüber dem Rechtsverletzer. Bei Internetsachverhalten ist weiters die Haftung von Access- oder Host-Providern, die den Zugang ins Internet vermitteln bzw Speicherplatz für Inhalte zur Verfügung stellen, besonders praxisrelevant, weil diese oft leichter greifbar sind als die unmittelbaren Verletzer selbst.

Abschließend wird bei den jeweiligen Problemen die mögliche Genugtuung für Rechteinhaber untersucht. Darunter fallen insb das Recht auf Schadenersatz und angemessenes Entgelt, weiters die Möglichkeit zur Urteilsveröffentlichung. Rechnungslegungsansprüche werden ebenfalls hier behandelt, weil sie zwar der Informationsbeschaffung dienen, als Nebenansprüche aber regelungstechnisch zu den Ansprüchen auf Genugtuung gehören.

Da die verschiedenen immaterialgüterrechtlichen Ansprüche in den einzelnen Materiengesetzen (UrhG, MSchG etc) zwar separat geregelt sind, ihre wesentlichen Punkte aber idR übereinstimmen, kann die Darstellung weitgehend gesetzesübergreifend erfolgen.

A.II.3. Zitierweise

Diese Arbeit orientiert sich hinsichtlich der Zitierweise an *Keiler/Bezemek*, leg cit (2009).

A.II.3.a. Literatur

Generell verwende ich im Fußnotenapparat zur besseren Übersichtlichkeit lediglich Kurzzitate, eine komplette Aufstellung der zitierten Literatur findet sich unter G. im entsprechenden Verzeichnis.

¹ Zum Begriff „Rechtsdurchsetzung“ vgl unten S 29 f.

Zwei Teile der vorliegenden Arbeit wurden bereits während der Entstehung der Dissertation in adaptierter Form vorab veröffentlicht. Da beide Beiträge für die in dieser Arbeit entwickelten Argumente bedeutsam sind, habe ich sie in ihrem ursprünglich vorgesehen Zusammenhang belassen, sodass sie – in ähnlicher Form – auch in meiner Dissertation zu lesen sind.² Meinen Mitautoren bei diesen beiden Publikationen, Herrn Mag. Maximilian Raschhofer und Mag. Lukas Feiler, danke ich für ihr Einverständnis und die gute Zusammenarbeit.

A.II.3.b. Rechtsquellen

Verweise auf Gesetzesstellen sind – soweit nicht ausdrücklich anders angeführt – als solche in der geltenden Fassung, wie sie dem Abkürzungs- und Rechtsquellenverzeichnis entnommen werden kann, zu lesen. Zum Abruf der zitierten Gesetze ist das vom Bundeskanzleramt betriebene Rechtsinformationssystem RIS unter <ris.bka.gv.at> hervorragend geeignet.

Europäische Richtlinien und Verordnungen werden, soweit möglich, in der neuesten, kodifizierten Fassung zitiert. Änderungen in der Nummerierung von einzelnen Bestimmungen können durch die Änderungstabelle, die jeder Neukodifizierung im Anhang beiliegt, nachvollzogen werden. Die entsprechende Datenbank findet sich unter <eur-lex.europa.eu>.

Aufgrund des Inkrafttretens des Vertrags von Lissabon und der damit verbundenen Umwandlung des bisherigen Dreisäulenmodells, insbesondere der Europäischen Gemeinschaft, in eine einheitliche Europäische Union spreche ich zudem im gesamten Dokument einheitlich von "Unionsrecht" statt, wie bisher üblich, von "Gemeinschaftsrecht".

A.II.3.c. Entscheidungen

Soweit möglich, habe ich zum Nachweis stRsp statt mehreren einzelnen Entscheidungen die entsprechenden Rechtssätze des OGH zitiert. Rechtssatznummern können über das entsprechende Formular unter <ris.bka.gv.at/Jus/> eingegeben und die jeweiligen Entscheidungen per Mausklick direkt abgerufen werden.

Entscheidungen der europäischen Gerichte sind über <curia.europa.eu> unter Eingabe der Geschäftszahl bequem abrufbar und bieten im Vergleich zu österreichischen Urteilen den Vorteil, dass einzelne Aussagen mittels der entsprechenden Randziffer leicht nachvollzogen werden können.

A.II.3.d. Internetquellen

Die im Text zitierten Internetquellen habe ich zuletzt am 31.12.2010 auf ihre Korrektheit hin überprüft. Falls einzelne Informationen nicht mehr abrufbar sein sollten, kann über den

² *Steinhofer/Feiler*, Urheberrechtliche Ansprüche auf die Sperrung von Websites durch Access-Provider, MR 2010, 322; *Raschhofer/Steinhofer*, § 87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig?, *ecolex* 2010, 716. Siehe FN 427 und 240.

Cache verschiedener Suchmaschinen, etwa unter <google.at>, oder mit der Hilfe von Wayback-Maschinen, etwa <waybackmachine.org>, versucht werden, eine historische Fassung einer Website abzurufen.

B. GRUNDLAGEN

B.I. Begriffsklärung

Zur Abgrenzung und zum besseren Verständnis des in dieser Arbeit behandelten Themenkreises müssen zunächst die grundlegenden Begriffe geklärt werden.

B.I.1. Immaterialgüterrecht

Bei weitem nicht alle Ideen und Schöpfungen unseres Geistes werden von der Rechtsordnung unter Schutz gestellt. So ist beispielsweise das Nacherzählen von Geschichten, die man gehört, gelesen oder im Fernsehen gesehen hat, jedem freigestellt. Ebenso darf ein Unternehmer idR grundlegende Geschäftsmodelle (etwa Bücher über einen Internet-Versandhandel zu vertreiben) von einem Konkurrenten „abkupfern“, ohne dass dieser sich mit rechtlichen Zwangsmitteln dagegen zur Wehr setzen könnte.

Andererseits ist es verboten, teilweise sogar strafbar, geistige Leistungen anderer für eigene Zwecke zu verwenden. Die gewinnbringende Verwertung von Werken der Literatur oder Kunst, die Verbreitung von mit Marken gekennzeichneten Waren oder der Verkauf von patentierten Erfindungen bleibt dem Inhaber dieser jeweiligen Rechte vorbehalten. Ebenso ist es nur dem „Vater“ eines Werkes gestattet, sich als dessen Urheber zu bezeichnen oder es zu bearbeiten. Nur der Erfinder hat den unverzichtbaren Anspruch auf Nennung und damit auf Schutz seiner Erfinderehre.

Seit *Josef Kohler*³ geben wir dem Rechtsbereich, der dieses Spannungsfeld regelt, den Namen „Immaterialgüterrecht“. Dieses Recht (im objektiven Sinn) muss einen Ausgleich schaffen zwischen den Freihaltebedürfnissen der Allgemeinheit und den legitimen Vermögens- und Persönlichkeitsrechten der jeweiligen Rechteinhaber.

B.I.1.a. Im objektiven Sinn

Das Immaterialgüterrecht im objektiven Sinn ist die Summe jener Normen, die die Rechte an verselbständigten, verkehrsfähigen geistigen Gütern regeln.⁴ Zu diesen Normen gehören das Markenschutzgesetz, das Musterschutzgesetz, das Patentgesetz sowie Gebrauchsmuster-, Halbleiterschutz-, Sortenschutz- und Schutzzertifikatsgesetz und das Urheberrechtsgesetz; mE auch das übrige Kennzeichenrecht, weil es denselben Zwecken dient wie das Markenrecht und eine Differenzierung daher nicht überzeugt.⁵

³ Grundlegend *Kohler*, Das Immaterialgüterrecht und seine Gegner (1887); siehe auch *Adrian*, Technikentwicklung und Patentrecht, in *Josef Kohler und der Schutz des geistigen Eigentums in Europa* 32 f.

⁴ Dazu und zum folgenden *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in *FS Troller* 57 f.

⁵ Ebenso *Thaler*, Immaterialgüterrechte und gewerblicher Rechtsschutz, in *FS 75 Jahre Österreichisches Patentamt* 251; *Walter*, Österreichisches Urheberrecht Rz 2; aA offb *Kucsko*, Geistiges Eigentum 95 u 96.

Daraus folgt zunächst, dass die durch das Immaterialgüterrecht geschützten Rechtsobjekte nicht körperlich angreifbare, materielle Gegenstände sind, sondern vielmehr aus geistigen, unkörperlichen Gütern, also „Immaterialgütern“, bestehen. Es geht daher „nicht um die Orgelpfeifen, sondern um die Musik, die aus ihnen ertönt“.⁶ Körperliche Mitteilungsträger (Farben, Worte, Töne, Schrauben, Leinwände) sind daher nicht Teil des Immaterialgutes, sondern bloß die „sinnliche Brücke“ zu diesem.⁷ Marken sind ebenfalls geistige Schöpfungen, auch wenn man sich „etwas schwer auf der Suche nach der schöpferischen Leistung“ tut.⁸ Als Kennzeichen dienen sie nämlich dem Schutz der planerischen unternehmerischen Betätigung im Wettbewerb (dem Anbieten von Waren und Dienstleistungen), die selbst eine geistige Leistung darstellt; die Marke ist ein Symbol dieser Leistung und daher auch ein Immaterialgut, allerdings nur in Bezug auf die jeweilig vom Schutzbereich der Marke umfasste Waren- oder Dienstleistungskategorie.⁹

Wichtig ist die Unterscheidung zwischen dem Immaterialgut und dem Immaterialgüterrecht. Ein Immaterialgüterrecht entsteht erst dann, wenn durch die Rechtsordnung einem bestimmten Rechtssubjekt bestimmte Rechte an einem Immaterialgut zugeordnet werden.¹⁰ Wenn daher zB in ein urheberrechtlich geschütztes Werk eingegriffen wird, wird idR nicht das Immaterialgut verletzt, sondern das Immaterialgüterrecht des Urhebers. Zudem sind auch nicht rechtlich geschützte geistige Schöpfungen Immaterialgüter, etwa eine Erfindung nach Ablauf der patentrechtlichen Schutzfrist.

Dieser Schutz durch die Rechtsordnung führt zu einem weiteren Charakteristikum der Immaterialgüterrechte: dem Enumerationsprinzip.¹¹ Sie wirken absolut (gegen jedermann) und können daher nicht wie Verträge durch einen privatautonomen Akt entstehen, sondern müssen sich aus dem Gesetz ergeben. Alles, was nicht explizit durch das Gesetz geschützt ist, unterliegt also grds der Nachahmungsfreiheit. Allerdings schützt die Generalklausel des § 1 UWG vor sittenwidrigerer (unlauterer) und die Verwechslungsgefahr fördernder bewusster Nachahmung fremder Leistungen, sofern eine andersartige Gestaltung zumutbar wäre.¹² Grds sind aber Leistungen wie Geschäftsideen oder bloße Entdeckungen nicht von der Rechtsordnung geschützt, sodass es für sie auch kein Immaterialgüterrecht gibt.

Verselbstständigt sind Immaterialgüter deswegen, weil sie durch ihren Schöpfer erst hervor- gebracht werden, aber idR auch ohne ihren Schöpfer weiter bestehen. Sie können (mit Aus-

⁶ *Kucsko*, Geistiges Eigentum 93.

⁷ *Troller*, Immaterialgüterrecht I² 51.

⁸ *Thaler*, Immaterialgüterrechte und gewerblicher Rechtsschutz, in FS 75 Jahre Österreichisches Patentamt 250.

⁹ Vgl *Troller*, Immaterialgüterrecht I²59 f; im Ergebnis ebenso EuG 22.07.2002 Rs T-323/00 (SAT.2); *Kucsko*, Geistiges Eigentum 199.

¹⁰ *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller 62.

¹¹ *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 323.

¹² RIS-Justiz RS0078297.

nahmen) vererbt und veräußert werden. Schon deshalb können sie nicht unter den Oberbegriff der Persönlichkeitsrechte eingeordnet werden¹³, auch wenn sich in den einschlägigen Gesetzen Regelungen mit zT starkem persönlichkeitsrechtlichem Gehalt finden.

Erst durch das Element der Verkehrsfähigkeit werden die durch das Immaterialgüterrecht geschützten Immaterialgüter für ihre Inhaber wertvoll. Das Gesetz ermöglicht dies durch die Einräumung von Vermögens- und Verwertungsrechten, wodurch der Inhaber seine geschützte Leistung gebrauchen, veräußern, vervielfältigen, lizenzieren, senden oder sonst wie zu Geld machen kann. Die Kehrseite dieses Rechts ist das für das Immaterialgüterrecht typische „ius excludendi“, durch das sich der Inhaber eines Immaterialgüterrechts gegen jeden unbefugten Gebrauch seiner Leistung zur Wehr setzen kann. Diese Rechte sind daher Immaterialgüterrechte im subjektiven Sinn.

B.I.1.b. Im subjektiven Sinn

Das Immaterialgüterrecht im subjektiven Sinn ist jene Befugnis, die dem einzelnen Rechts- subjekt vom Immaterialgüterrecht im objektiven Sinn (der Rechtsordnung) im Bezug auf ein Immaterialgut eingeräumt wird und deren Geltendmachung allein vom Willen des Berechtigten abhängt.¹⁴ Subjektive Immaterialgüterrechte sind idR Vermögensrechte, sie haben aber meist, jedoch nicht notwendigerweise, mehr oder weniger starken persönlichkeitsrechtlichen Gehalt.¹⁵ Sie sind absolute Rechte, die typischerweise ein (positives) Gebrauchsrecht und ein (negatives) Verbotsrecht umfassen.¹⁶ Grds sind sie frei unter Lebenden veräußerbar und auf dem Erbweg übertragbar.

Die aus der Rechtsordnung abgeleiteten subjektiven Befugnisse des Immaterialgüterrechts verfolgen nicht alle einen einheitlichen rechtspolitischen Zweck. Sie sichern zuvorderst gewerblich-kommerzielle Interessen, gleichwohl dienen sie bisweilen auch überwiegend geistig-ideellen Interessen. Anhand dieser groben Einteilung lässt sich ein lang schwelender Meinungs- und Theorienstreit zurückverfolgen, der ebenfalls auf *Kohler* zurückgeht. Dieser hatte die dualistische Theorie begründet, wonach die Persönlichkeitsrechte (nach seiner Terminologie: Individualrechte) des Urhebers von den Immaterialgüterrechten zu trennen seien. Nach dieser dualistischen Theorie wären die subjektiven Immaterialgüterrechte als reine Vermögensrechte anzusehen.¹⁷ Alle Ansprüche, die rechtspolitisch dem Schutz der ideellen Interessen dienen, wären daher nicht Teil der subjektiven Immaterialgüterrechte.

¹³ *Troller*, Immaterialgüterrecht I² 85 f; *Kucsko*, Geistiges Eigentum 101.

¹⁴ Vgl *Koziol/Welser*, Bürgerliches Recht I³ 45 f.

¹⁵ *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS *Troller* 62.

¹⁶ Vgl *Rauter*, Immaterialgüterrecht, in Fachwörterbuch Handelsrecht 174; *Walter*, Österreichisches Urheberrecht Rz 4.

¹⁷ *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS *Troller* 59.

Dies trifft den Kern der Sache aber nach neuerer Ansicht nicht, da selbst diejenigen subjektiven Immaterialgüterrechte, die primär der Befriedigung der Vermögensinteressen des jeweils von der Rechtsordnung Berechtigten dienen, sehr oft auch einen persönlichkeitsrechtlichen Gehalt aufweisen; dies insoweit, als sie „zur Wahrung der berechtigten persönlichen Belange ihres Schöpfers notwendig“ sind.¹⁸ Die dualistische Theorie ist daher zu eng und heute zugunsten der herrschenden¹⁹ monistischen Theorie überwunden. Diese geht auf *Ulmer* zurück, der die berühmte „Baumtheorie“ entwickelte, wonach das einheitliche Urheberrecht gleich einem Baum mit einheitlichem Stamm sei, der in den ideellen und materiellen Interessen wurzle, die verschiedenen urheberrechtlichen Befugnisse dagegen Äste und Zweige dieses Baumes seien und ihre Kraft bald aus beiden Wurzeln, bald aus einer Wurzel bezögen.²⁰ Nicht zuletzt ist dies auch die rechtspolitische Rechtfertigung für die zeitliche Befristung der urheberrechtlichen Schutzdauer, weil das ideelle Band zwischen dem Urheber und seinem Werk eben nicht ewig fortbestehen kann.²¹

Da es auch subjektive Immaterialgüterrechte ohne jeglichen persönlichkeitsrechtlichen Gehalt gibt (zB das verwandte Schutzrecht von Tonträgerherstellern nach § 76 UrhG), ist das typische subjektive Immaterialgüterrecht jedenfalls ein Vermögensrecht. Es bietet sich daher an, bei Rechten ohne persönlichkeitsrechtlichen Gehalt mit *Hubmann* von „reinen Immaterialgüterrechten“ zu sprechen.²² So ist auch das Urheberrecht mit seinen persönlichkeitsrechtlichen Färbungen problemlos unter die Immaterialgüterrechte einzuordnen. Im UrhG finden sich zudem (systemwidrig) auch reine Persönlichkeitsrechte, nämlich der Brief- und Bildnisschutz der §§ 77 und 78 UrhG.²³

Subjektive Rechte, die zuvorderst den ideellen Interessen der Inhaber von Immaterialgüterrechten dienen, finden sich insb im UrhG, aber auch im PatG und MuSchG.²⁴ Sie werden oft ebenfalls als „Persönlichkeitsrechte“ bezeichnet, was terminologisch und dogmatisch nicht sinnvoll ist. Die die ideellen Interessen des jeweiligen Urhebers (Erfinders, Schöpfers) schützenden Rechte sollten nicht mit den reinen Persönlichkeitsrechten wie Leben oder Ehre, die

¹⁸ *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller 59, folgend *Hubmann*; vgl auch die spätere Auflagen *Hubmann/Götting*, Gewerblicher Rechtsschutz⁶ 63 sowie *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 59.

¹⁹ Für viele: *Salomonowitz* in *Kucsko*, urheber.recht § 23 Pkt 1.

²⁰ Zitiert nach *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 29 und *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller 61.

²¹ *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 64.

²² *Hubmann/Götting*, Gewerblicher Rechtsschutz⁶ 68.

²³ Vgl *Kucsko*, Geistiges Eigentum 1333; *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 109; in Bezug auf den Bildnisschutz im dUrhG ebenso *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 14.

²⁴ Dazu zählen nach *Aicher* in *Rummel*³ 20 die in § 20 PatG („Erfinderehre“) und §§ 19 – 21 UrhG genannten Rechte, nach *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 110 zudem §§ 38 Abs 2, 39, 68, 77 und 78 UrhG; heute auch der Schutz der Schöpferehre nach § 8 MuSchG, vgl *Kucsko*, Geistiges Eigentum 748.

nicht auf geistigen Leistungen, sondern auf Geburt fußen, vermengt werden.²⁵ Als Sammelbegriff dafür bietet sich „Urheberpersönlichkeitsrechte iwS“ an.

Die Vermögensrechte bilden jedenfalls den Kern der Immaterialgüterrechte, da diese in ihrer reinen Form ausschließlich materielle Interessen schützen. Schließlich soll das Immaterialgüterrecht (im objektiven Sinn) vor allem „den wirtschaftlichen Wert eines Immaterialgutes demjenigen sichern, dem es zu verdanken ist“.²⁶

Die geschieht zB über den Verkauf von mit Marken gekennzeichneten Produkten oder über die entgeltliche Einräumung von Benutzungsrechten („Lizenz“) gegenüber Dritten – somit mittels eines Gebrauchs des Immaterialgüterrechts. Das subjektive Recht wird in der wirtschaftlichen Praxis meist aber vor allem dadurch spürbar, dass man andere vom unbefugten Gebrauch eines Immaterialgutes auszuschließen vermag (Verbotsrecht). Dies liegt einerseits daran, dass dem Inhaber eines Immaterialgüterrechts nur dann zugemutet werden kann seine Leistung öffentlich zu machen (zB in einem Register), wenn er sich auch gegen jeden Nachahmer zur Wehr setzen kann. Andererseits folgt dies aus der „potentiellen Ubiquität von Immaterialgütern“, also aus ihrer Loslösung von Zeit und Raum;²⁷ dieser Begriff führt vor Augen, dass Immaterialgüter viel einfacher „entwendet“ werden können als körperliche Güter. Für einen Diebstahl ist ein Gewahrsamsbruch erforderlich, die wertvolle Uhr fehlt dem Bestohlenen nach der Tat. Für geistige Leistungen trifft dies nicht zu, da beispielsweise ein illegal kopiertes Musikstück dem Urheber nicht „fehlt“. Daher ist etwa der Ausdruck „Raubkopie“ in jedem Fall verfehlt.

Diese erneute Zweiteilung der subjektiven Immaterialgüterrechte wird oft dadurch zum Ausdruck gebracht, dass von einer negativen (Verbotsrecht) und positiven (Gebrauchsrecht) Seite gesprochen wird.²⁸ Ganz sauber ist auch diese Trennung nicht, wie *Schönherr* nachgewiesen hat.²⁹ Zudem fallen subjektive Rechte wie das Recht auf angemessene Entschädigung oder Vergütung hierbei durch den Rost, da sie keine Ausschließungsbefugnisse umfassen,³⁰ aber auch nicht mit der in der Alltagssprache üblichen Bedeutung von „Gebrauch“ in Einklang zu bringen sind. Beide Seiten (so man diese Teilung überhaupt vornimmt) spielen aber als begriffliche Stütze in den Begriff der „Rechtsdurchsetzung“ hinein, sodass ihre Erwäh-

²⁵ *Troller*, Immaterialgüterrecht I² 85 f.

²⁶ *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 307.

²⁷ *Kucsko*, Geistiges Eigentum 94; *Hubmann/Götting*, Gewerblicher Rechtsschutz⁶39; *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 14; *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 304; *Troller*, Immaterialgüterrecht I² 49.

²⁸ *Hubmann/Götting*, Gewerblicher Rechtsschutz⁶63 f; *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 60; weitere Nachweise in *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller FN 138 f.

²⁹ *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 321 f; *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller 71 f.

³⁰ *Schönherr*, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller 64 f.

nung für die Anliegen dieser Arbeit erforderlich ist. Die praktische Handhabung von Immaterialgüterrechten erfolgt zudem häufig analog dieser Einteilung.³¹

Für die Ausschließungsrechte des Inhabers eines Immaterialgüterrechts ist es schließlich konstitutiv, dass sie absolut, also gegenüber allen anderen Rechtssubjekten, gelten, wenn auch ihr Schutzbereich (zB der einer Marke) begrenzt sein mag.

B.I.1.c. Abgrenzungen

Gebräuchlich sind auch die Begriffe „Gewerblicher Rechtsschutz“ und „Geistiges Eigentum“, die zT große Überschneidungen mit dem Begriff des Immaterialgüterrechts aufweisen.

B.I.1.c.1. Gewerblicher Rechtsschutz

Der gewerbliche Rechtsschutz umfasst grds dieselben Quellen wie das Immaterialgüterrecht, zusätzlich jedenfalls³² das Wettbewerbsrecht (ieS), nicht aber das „klassische“ Urheberrecht (sehr wohl aber die verwandten Schutzrechte des UrhG). Die Leitlinie, das eher höheren und künstlerischen Idealen dienende Urheberrecht aus dem schnöden gewerblich-kommerziellen Umfeld zu heben und den Rest gemeinsam mit dem Lauterkeitsrecht unter dem Begriff „Gewerblicher Rechtsschutz“ zu sammeln, ist heute mehrfach durchbrochen. Vor allem haben durch technologische Neuerungen Leistungen wie Software oder Datenbanken Einzug in das Urheberrecht und seinen Werksbegriff gehalten, bei denen die künstlerische Verwirklichung mit Sicherheit gegenüber gewerblichen Interessen in den Hintergrund tritt.³³ Dennoch ist für das klassische Urheberrecht die gewerbliche Verwertbarkeit keine Essentiale, sodass die Abgrenzung von den gewerblichen Schutzrechten geboten ist.³⁴ Da der gewerbliche Rechtsschutz auch das Lauterkeitsrecht umfasst, lässt er sich nicht unter den Begriff des Immaterialgüterrechts einordnen.³⁵ Das Wettbewerbsrecht wird in dieser Arbeit nicht systematisch behandelt, aber für sich dort erwähnt, wo es geboten erscheint. Der Begriff „Gewerblicher Rechtsschutz“ ist daher einerseits zu eng (ohne Urheberrecht), andererseits zu weit (mit Wettbewerbsrecht) und hier daher nicht weiter von Nutzen.

B.I.1.c.2. Geistiges Eigentum

Nicht zuletzt wegen der zunehmenden Internationalisierung ist der Begriff „Geistiges Eigentum“ bzw „Intellectual Property“ (IP) auf dem Vormarsch. Beispielsweise heißt die UN-Organisation, die sich mit der Entwicklung internationaler Standards für das Immaterialgü-

³¹ Vgl die Beispiele bei *Kucsko*, Geistiges Eigentum 95.

³² Zu den Abgrenzungsproblemen ausführlich *Thaler*, Immaterialgüterrechte und gewerblicher Rechtsschutz, in FS 75 Jahre Österreichisches Patentamt 246 f.

³³ So auch *Kucsko*, Geistiges Eigentum 100.

³⁴ *Thaler*, Immaterialgüterrechte und gewerblicher Rechtsschutz, in FS 75 Jahre Österreichisches Patentamt 253.

³⁵ Vgl die (grafische) Darstellung bei *Schönherr*, Gewerblicher Rechtsschutz und Urheberrecht Rz 105 u 110.

terrecht beschäftigt und zudem die internationalen Markenmeldungen verwaltet, „World Intellectual Property Organization“ (WIPO). Die RL 2004/48/EG trägt den Titel „... zur Durchsetzung der Rechte des geistigen Eigentums“ (Enforcement-RL). Der Begriff findet sich auch im EU-Primärrecht, zB in Art 118 AEUV³⁶ und in Art 17 Abs 2 GRC. Das WTO-Abkommen über Immaterialgüterrechte heißt „Trade-Related Aspects of Intellectual Property Rights“ (TRIPS-Abkommen).

Historisch betrachtet entwickelte sich dieser Terminus aus dem Naturrecht und der Aufklärung.³⁷ Die Lehre vom geistigen Eigentum stellte das Recht des schöpferisch tätigen Menschen in den Mittelpunkt und geht von einem naturgegebenen Recht auf die Früchte geistiger Arbeit aus, welches durch die Legislative lediglich ausgeführt werden muss. Sie geht auf die philosophischen Vorarbeiten von *Kant, Fichte, Voltaire, Diderot* und *D’Héricourt* zurück und war Programm für die französische Gesetzgebung nach der Revolution von 1789.³⁸ *Kohler* stand dem Begriff „Geistiges Eigentum“ skeptisch gegenüber, da er zu nahe an sachenrechtlichen Vorschriften für körperliche Gegenstände stünde und dort nur Verwirrung erregen würde.³⁹ Seinem Einfluss und weiteren kritischen Stimmen ist es auch zuzuschreiben, dass nach 1900 in Deutschland der Begriff „geistiges Eigentum“ wieder auf dem Rückzug befindlich war.⁴⁰

Rund um die Ausarbeitung eines neuen Urheberrechtsgesetzes kam es in Deutschland nach Ende des Zweiten Weltkrieges zu einer Renaissance der Lehre vom geistigen Eigentum, vor allem wegen der großen Legitimationskraft, die vom Begriff „Eigentum“ ausgeht.⁴¹ So forderte etwa der deutsche Komponistenverband für die Urheberrechtsreform, dass der verfassungsrechtliche Schutz vor Enteignung des Art 14 GG ebenso wie für körperliches auch für das geistige Eigentum gelten solle.⁴² In der deutschen Rsp ist bis heute die Entscheidung des BGH „Tonband/Grundig-Reporter“⁴³ von überragender Bedeutung für die heute herrschende Lehre vom geistigen Eigentum.⁴⁴ Der BGH formulierte:

„Für das moderne Urheberrecht wird allseitig anerkannt, daß (*sic*) die Nutzungsrechte des Urhebers nur die Ausstrahlungen seines durch den Schöpfungsakt begründeten geistigen

³⁶ Dazu *Handig*, Geistiges Eigentum nach dem Vertrag von Lissabon, *ecolex* 2010, 171.

³⁷ Ansätze in diese Richtung lassen sich freilich noch bis in die Antike zurückverfolgen; vgl *Walter*, Österreichisches Urheberrecht Rz 8 f.

³⁸ Vgl *Dittrich*, Geistiges Eigentum, in *Beiträge zum Urheberrecht VIII* 47; *Walter*, Österreichisches Urheberrecht Rz 20 f.

³⁹ *Kohler*, Lehrbuch des Patenrechts, 13 f, zitiert nach *Troller*, Immaterialgüterrecht I² FN 94.

⁴⁰ Vgl *Dittrich*, Geistiges Eigentum, in *Beiträge zum Urheberrecht VIII* 51 f.

⁴¹ Vgl *Jänich*, Geistiges Eigentum 110 f.

⁴² *Jänich*, Geistiges Eigentum 117.

⁴³ BGH 18.5.1955, I ZR 8/54; äußerst kritisch dazu *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 59 f.

⁴⁴ *Dittrich*, Geistiges Eigentum, in *Beiträge zum Urheberrecht VIII* 56.

Eigentums sind. Die Herrschaft des Urhebers über sein Werk, auf das sich sein Anspruch auf einen gerechten Lohn für eine Verwertung seiner Leistung durch Dritte gründet, wird ihm hiernach nicht erst durch den Gesetzgeber verliehen, sondern folgt aus der Natur der Sache, nämlich aus seinem geistigen Eigentum, das durch die positive Gesetzgebung nur seine Anerkennung und Ausgestaltung findet. Dieser das Urheberrecht beherrschende Rechtsgedanke ist bei der Auslegung urheberrechtlicher Gesetzesnormen stets im Auge zu behalten“.

In Österreich wurde diese Ansicht weder von der Gesetzgebung noch von der Judikatur oder Literatur aufgenommen. So findet sich in den ErlRV⁴⁵ zur Stammfassung des UrhG: „Der Entwurf gewährt damit dem Urheber kein totales Beherrschungsrecht, das jede Benützung des Werks durch andere ausschließt, sondern nur bestimmte ausschließliche Befugnisse, die in den §§ 14 bis 18 des Entwurfs erschöpfend aufgezählt sind“. Bei keiner der zahlreichen späteren Novellen wurde von diesem Ansatz abgegangen.⁴⁶

Der OGH lehnte in einer ähnlichen Fallkonstellation wie bei „Tonband/Grundig-Reporter“ aus methodischen Gründen die Ausdehnung des Urheberrechtsschutzes und damit mittelbar auch die vom BGH vertretene Lehre vom geistigen Eigentum als Naturrecht ab.⁴⁷ Das Gericht sei nicht berechtigt, im Wege der "Rechtsfortbildung" und unter Berufung auf "Treu und Glauben" Gedanken in das Gesetz zu tragen, die in diesem nicht enthalten seien.

Kucsko's wertvoller Grundriss des österreichischen Immaterialgüterrechts, der in dieser Arbeit häufig zitiert wird, heißt zwar „Geistiges Eigentum“, jedoch vertritt der Autor an keiner Stelle seines Buches einen naturrechtlichen Ansatz ähnlich dem des BGH. Vielmehr verwendet er den Begriff „Geistiges Eigentum“ als Synonym für Immaterialgüterrecht, weiters als Begriff für Rechte im subjektiven Sinn (arg: „Immaterialgüterrechte“) und er erklärt, dass er den Begriff als Titel seines Buches gewählt habe, weil er seines Erachtens am anschaulichsten sei.⁴⁸

Es hat daher in Österreich – im Gegensatz zu Deutschland – keine Rückkehr zur naturrechtlich geprägten Lehre vom geistigen Eigentum stattgefunden.⁴⁹ Über die Mitgliedschaft Österreichs bei EU, WIPO und TRIPS hält der Begriff „Geistiges Eigentum“ dagegen zunehmend Einzug in die österreichische Rechtssprache, nicht zuletzt wegen seiner Anschaulichkeit. *Dittrich* konstatiert richtig, dass aus ihm aber keine Schlüsse über die Rechte von Rechteinhabern zu ziehen sind, die über die herrschende Methodenlehre hinausgehen.⁵⁰ Vor allem ist

⁴⁵ Nach *Dillenz*, Materialien zum österreichischen Urheberrecht 63.

⁴⁶ *Dittrich*, Geistiges Eigentum, in Beiträge zum Urheberrecht VIII 58.

⁴⁷ OGH 28.11.1967, 4 Ob 353/67; vgl auch RIS-Justiz RS0008956.

⁴⁸ *Kucsko*, Geistiges Eigentum 97.

⁴⁹ Ebenso *Dittrich*, Geistiges Eigentum, in Beiträge zum Urheberrecht VIII 58.

⁵⁰ *Dittrich*, Geistiges Eigentum, in Beiträge zum Urheberrecht VIII 39; zust *Kucsko* in *Kucsko*, urheber.recht Einleitung 5.

man in Österreich nicht der in Deutschland verbreiteten, aber auch dort kritisierten⁵¹ Lehre vom geistigen Eigentum gefolgt.

B.I.2. Rechtsdurchsetzung

Der Begriff „Rechtsdurchsetzung“ wird in der Rechtsordnung Österreichs an 44 Stellen verwendet, am prominentesten in der Überschrift des III. Hauptstücks des UrhG (vor § 81) und als Titel des III. Teiles des TRIPS-Abkommens, das durch BGBl 1/1995 in nationales Recht Eingang gefunden hat. Ebenso findet er sich im Titel der bereits erwähnten Enforcement-RL sowie in sämtlichen Lehrplänen für die österreichischen Mittelschulen. Eine Legaldefinition existiert allerdings da wie dort nicht, auch in den einschlägigen Lexika und Wörterbüchern wird der Begriff nicht genannt.

In der (deutschen) Lit findet sich bei *Dreier* die Definition der Rechtsdurchsetzung als „die Rechtsfolgen von Verletzungen der gewährten Rechte ebenso wie die verfahrensrechtlichen Grundbedingungen ihrer gerichtlichen Geltendmachung“.⁵² In seiner eingehenden Untersuchung kommt *Anduleit* zu dem Ergebnis, dass „Rechtsdurchsetzung“ zu definieren sei als „materiellrechtlicher Schutz der Rechte [...] vom Zeitpunkt ihrer Entstehung an vor Verletzung und Gefährdung, der nach verfahrensrechtlichen Modalitäten (nicht nur gerichtlich) geltend gemacht werden kann“; er betont, dass die Rechtsdurchsetzung neben ihrer verfahrensrechtlich-formellen Seite auch eine inhaltlich-materielle Seite umfasst und zur Definition *Dreiers* auch die außergerichtliche Rechtsdurchsetzung hinzuzurechnen sei.⁵³

B.I.2.a. Wörtliche Interpretation

„Durchsetzen“ bedeutet nach der wörtlichen Interpretation „Widerstände überwinden und sich Geltung verschaffen“⁵⁴ und „etwas trotz Widerstandes erreichen“.⁵⁵ Im rechtlichen Kontext ist die zur Überwindung von Widerständen regelmäßig benötigte Gewalt durch das Verbot der Selbsthilfe ausgeschlossen. Als Kehrseite dieses Verbots besitzt man als Bürger einen (formellen) Rechtsschutzanspruch gegenüber dem Staat.⁵⁶ Zur Durchsetzung von subjektiven Rechten ist nämlich regelmäßig die Anrufung verschiedener staatlicher Organe und die Einhaltung ihrer Verfahrensvorschriften erforderlich; dies ist die formelle Seite des Begriffs der „Rechtsdurchsetzung“⁵⁷, die grundrechtlich durch Art 6 EMRK determiniert ist. Für die

⁵¹ *Hubmann/Rehbinder*, Urheber- und Verlagsrecht⁸ 59 f sprechen davon, dass der Begriff „geistiges Eigentum“ aus der Mottenkiste der Rechtsgeschichte wieder vorgeholt wurde und plädieren dafür, statt diesem „Werkherrschaft“ als Beschreibung des Rechtsverhältnisses zwischen Rechtsinhaber und Werk zu verwenden.

⁵² *Dreier*, TRIPS und die Durchsetzung von Rechten des geistigen Eigentums, GRUR Int 1996, 205.

⁵³ *Anduleit*, Die Rechtsdurchsetzung im Markenrecht 37.

⁵⁴ Duden⁶, durchsetzen.

⁵⁵ DWDS, durchsetzen.

⁵⁶ Vgl *Rechberger/Simotta*, Zivilprozessrecht⁷ Rz 18.

⁵⁷ Vgl *Koziol/Welser*, Bürgerliches Recht I³ 42.

„Rechtsdurchsetzung“ hat man sich also idR auf staatlich organisierte Verfahren zu verlassen, Widerstände können aber durchaus auch außerhalb solcher Verfahren und somit außergerichtlich überwunden werden, soweit keine Gewalt verübt wird.

B.I.2.b. Systematische Interpretation

Die systematische Interpretation zeigt, dass im österreichischen Recht neben formell-prozessualen Gesichtspunkten auch die materiellen Anspruchsgrundlagen vom Begriff der Rechtsdurchsetzung umfasst sind. Im mit „Rechtsdurchsetzung“ betitelten III. Hauptstück des UrhG finden sich materiellrechtliche Vorschriften über die Rechtsfolgen von Urheberrechtsverletzungen wie Anspruch auf Unterlassung, Beseitigung, Auskunft, Schadenersatz etc. Gleiches gilt für den III. Teil des TRIPS-Abkommens, der mit „Durchsetzung der Rechte des geistigen Eigentums“ überschrieben ist und neben Verfahrensgarantien vor allem materielle Ansprüche beinhaltet.⁵⁸ Mit „Rechtsdurchsetzung“ sind daher stets auch die materiellen Anspruchsgrundlagen und Einwände gemeint, ohne die es keine prozessuale Verfolgung eines Rechts geben kann.

B.I.2.c. Teleologische Interpretation

Schon aus der wörtlichen Bedeutung (Überwindung von Widerständen) folgt, dass die Normen über die Rechtsdurchsetzung dann Anwendung finden, wenn es einen Gegner gibt, der die Widerstände verursacht. „Widerstände“ sind hier Eingriffe oder Gefährdungen bestehender fremder Immaterialgüterrechte. Ein Beharren iS einer Überzeugtheit von der eigenen Rechtsposition ist dabei nicht erforderlich. Auch wer mit vollem Unrechtsbewusstsein fremde Rechte verletzt oder gefährdet, leistet gegenüber dem Rechteinhaber Widerstand, da jeder dieser Verletzungsakte den Anspruch auf Gültigkeit in sich trägt und man dem Ausführenden unterstellen muss, dass er auf etwaige Gegenmaßnahmen (potentiell) mit Widerstand reagieren wird.

Anduleit geht bei seiner Definition von Markenrechten aus und möchte auch deren Registrierung in den Begriff der Rechtsdurchsetzung einbeziehen. Die Registrierung und der „Gebrauch“ eines Immaterialgüterrechts (vgl dazu oben B.I.1.b) ist nun aber noch nicht von der Überwindung von Widerständen gekennzeichnet (die Anmeldung und die damit verbundene Bürokratie einmal außen vorgelassen), auch wenn man sich mit der Registrierung durchaus „Geltung verschafft“. Der Sinn und Zweck der Durchsetzungsnormen zielt aber darauf ab, bestehende Rechtsbeeinträchtigungen abzustellen und für Genugtuung zu sorgen. Die Registrierung von Rechten ist daher höchstens in einem weiteren Sinne der „Rechtsdurchsetzung“ zuzurechnen, wird in dieser Arbeit jedoch ausgeklammert. Hier umfasst „Rechtsdurch-

⁵⁸ Vgl die Analyse bei *Anduleit*, Die Rechtsdurchsetzung im Markenrecht 36 f; *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 163 f behandelt ebenfalls materiellrechtliche Ansprüche der Rechteinhaber.

setzung“ lediglich die negative Seite des subjektiven Immaterialgüterrechts, also das Verbotrecht sowie die damit verknüpfte Möglichkeit zur Genugtuung (Schadenersatz etc). Vorbereitungshandlungen, insbesondere zur Informationsbeschaffung über die Gefährdung oder Verletzung, sind dabei inbegriffen, weil Rechte nicht praktisch durchgesetzt werden können, wenn die dafür notwendigen Informationen nicht bekannt sind.

B.I.2.d. Zusammenfassung

„Rechtsdurchsetzung“ ist in dieser Arbeit zu verstehen als materiellrechtlich legitimierte Überwindung von Widerständen gegen bestehende Rechte unter Beachtung verfahrensrechtlicher Modalitäten. Die Überwindung von Widerständen umfasst die notwendigen Vorbereitungshandlungen, insbesondere die Informationsbeschaffung über die verletzenden Handlungen und den Widerstand leistenden Gegner, die Unterbindung der verletzenden Handlungen und die Genugtuung für erlittene Beeinträchtigungen.

B.I.3. Internet

Das Internet ist ein Netzwerk aus Netzwerken zwischen Computern. Es umfasst neben dem World Wide Web (WWW), das vielfach (fälschlich) als Synonym dafür verwendet wird, zahlreiche andere Dienste wie E-Mail, das Usenet und Datenübertragung (insb FTP), neuerdings auch Telefonie (Voice-over-IP) oder Fernsehen.

Technisch basiert es im Kern noch immer auf dem 1982 eingeführten Protokoll TCP/IP, das die präzise Adressierung der verschiedenen Netzwerke und Computer durch IP-Adressen⁵⁹ ermöglicht. Nur so können die unzähligen verknüpften Rechner miteinander kommunizieren und Daten austauschen. Die einzelnen verbundenen Netzwerke unterliegen der administrativen Kontrolle verschiedenster Stellen (Privathaushalte, Unternehmen, Universitäten, demokratische und repressive Regierungen etc), eine einheitliche „Internetregierung“ mit zentralen Durchgriffsmöglichkeiten besteht dagegen nicht.⁶⁰

⁵⁹ Bei einer IP-Adresse handelt es sich nach dem derzeit noch herrschenden Adressierungssystem IPv4 um eine durch Punkte getrennte Abfolge von vier Zahlen (zB 194.232.104.29), die zusammen die logische Adressierung von Computern und anderen Geräten im Internet erlauben. Jedem Gerät ist dabei eine weltweit einzigartige IP-Adresse zugeordnet. Allerdings treten Computer, die innerhalb eines lokalen Netzwerks (LAN) verbunden sind und über einen Gateway (zB Router) eine Verbindung zum Internet herstellen, nach außen hin idR nur unter einer IP-Adresse auf. Zum technischen Hintergrund vgl *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113. Wegen Kapazitätsengpässen wird dieses Format in naher Zukunft von IPv6 abgelöst werden, das deutlich mehr individuelle Adressen ermöglicht. Vgl dazu Wikipedia, <en.wikipedia.org/wiki/IPv6#Packet_format>.

⁶⁰ Einen (weiterführenden) instruktiven Überblick über die technische Funktionsweise des Internets liefert zB *Gutman*, Urheberrecht im Internet 18 f; die Geschichte des Internets beschreiben die Autoren der Online-Enzyklopädie Wikipedia, <de.wikipedia.org/wiki/Geschichte_des_Internets>.

Die zur rechtlichen Beurteilung notwendigen weiteren technischen Hintergründe des Internets werden im Zusammenhang mit den jeweiligen konkreten Problemstellungen erläutert.

B.I.4. Internetprovider

Für das Funktionieren des Internets unerlässlich sind die Dienste von Internet Providern (auch: Internet Service Provider [ISP]). Dies sind grob zusammengefasst alle Diensteanbieter, die Internetnutzern den Internetzugang, Speicherplatz oder Inhalte (Content) auf elektronischem Weg zur Verfügung stellen. Während sich der Begriff „Provider“ naturgemäß auch auf Dienstleister beziehen kann, die ihre Leistungen außerhalb von elektronischen Netzen erbringen, geht es in dieser Arbeit um Rechtsfragen hinsichtlich der Dienste von Internet Providern. Diese sind für die Zwecke dieser Arbeit auch dann gemeint, wenn der Begriff „Provider“ allein stehend verwendet wird, zB im Zusammenhang mit der Providerhaftung.

Die Abgrenzung innerhalb der verschiedenen Internetprovider nach ihrem jeweiligen Tätigkeitsgebiet ist für zahlreiche Rechtsfragen von Bedeutung, insbesondere aber dafür, inwieweit Internetprovider gegenüber Dritten haften, wenn ihre Dienste von Internetusern für Rechtsverletzungen genutzt werden. Letzteres wird in zunehmendem Maße in der rechtspolitischen Diskussion gefordert.⁶¹ Das liegt vor allem daran, dass durch die Ubiquität und grenzüberschreitende Ausrichtung des Internets die unmittelbaren Täter sehr oft nicht greifbar sind, die Internetprovider aber schon. Die de lege lata geltenden umfangreichen Haftungsbefreiungen, die in Europa und den USA für Internetprovider vorgesehen sind, werden rechtspolitisch damit begründet, dass diese idR mit den Rechtsverletzungen nur sehr mittelbar in Verbindung stehen, insbesondere durch das Bereitstellen der technischen Infrastruktur.⁶²

Je nach ihrer konkreten Tätigkeit wird ganz herrschend zwischen Content-Providern, Host-Providern und Access-Providern unterschieden. Diese Unterscheidung ist nicht personell, sondern funktional zu sehen; idR sind nämlich Unternehmen in allen drei Bereichen gleichzeitig tätig. Ihre Verantwortlichkeit richtet sich stets danach, unter welche Kategorie sie im jeweiligen Sachverhalt einzuordnen sind.⁶³

B.I.4.a. Content-Provider

Content-Provider ist derjenige, der eigene Inhalte gestaltet und zur Verfügung stellt, also beispielsweise ein User eines Web 2.0 Dienstes wie Facebook oder YouTube, der eigene Fotos

⁶¹ So zB von den USA in der Debatte rund um das Anti-Piraterie-Abkommen ACTA: vgl Futurezone vom 6.9.2010: <futurezone.at/stories/1660405/>.

⁶² Vgl Zankl, E-Commerce-Gesetz Rz 40.

⁶³ Vgl Zankl, E-Commerce-Gesetz Rz 184.

oder Videos hochlädt und damit für andere bereitstellt. Die Haftung für diese eigenen Inhalte ist geradezu selbstverständlich. Auf Content-Provider sind daher die allgemeinen Regeln im Zusammenhang mit Schadenersatz, Unterlassungspflichten etc sofort anzuwenden, ohne dass zuerst eine generelle Haftungsfreistellung geprüft werden müsste.⁶⁴

B.I.4.b. Host-Provider

Host-Provider dagegen sind diejenigen Internetprovider, "deren Tätigkeit darin besteht, die von einem Nutzer eingegebenen Informationen zu speichern, die also Speicherplätze zur Verfügung stellen".⁶⁵ Dienste wie Facebook und YouTube, die fremde Inhalte auf ihrem Server speichern und Dritten den Zugriff darauf ermöglichen, sind daher Host-Provider. Selbiges gilt für Unternehmen, die Dritten gegen Entgelt Speicherplatz auf ihren Servern zur Verfügung stellen, um dort zB Websites abrufbar zu machen. Entscheidendes Abgrenzungskriterium zum Content-Provider ist, dass der Host-Provider keinen inhaltlichen Einfluss auf die gespeicherten Daten nimmt⁶⁶, sie ihm also fremd sind.⁶⁷ Aus dieser Definition ergibt sich, dass für dieselbe Information mehrere Host-Provider „zuständig“ sein können: Etwa im Falle eines Videoportals einmal der Betreiber der Seite, der fremde Videodateien speichert, zusätzlich aber auch der Eigentümer und Vermieter des Servers, auf dem die Inhalte gespeichert werden. Diese beiden können, müssen aber nicht dieselbe Person sein.⁶⁸

B.I.4.c. Access-Provider

Davon strikt zu unterscheiden sind die Access-Provider, die lediglich den Zugang zu einem Kommunikationsnetz wie dem Internet vermitteln oder von Usern eingegebene Daten übermitteln.⁶⁹ Das entscheidende Merkmal von Access-Providern ist, dass sie die Informationsübermittlung nicht veranlassen, nicht selbst Daten bereitstellen und weder die Adressaten der Information auswählen noch auf die Daten, die User durch ihre Kanäle leiten, Einfluss nehmen.⁷⁰ Access-Provider ist somit derjenige, der eine „reine Durchleitung“ von Daten durch Informationskanäle vornimmt.⁷¹ Die Daten dürfen dabei – von technischen Notwendigkeiten wie Verschlüsselungen oder Caching abgesehen – nicht verändert oder gespeichert

⁶⁴ RIS-Justiz RS0118734.

⁶⁵ So die Materialien zum ECG: ErlRV 817 BlgNR XXI. GP 36.

⁶⁶ Vgl *Kasper*, Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 1; ausführlich *Zankl*, E-Commerce-Gesetz Rz 222 f.

⁶⁷ *Zankl*, E-Commerce-Gesetz Rz 229.

⁶⁸ Vgl OGH 11.12.2003, 6 Ob 274/03t (Online-Archiv I) mwN; ebenso die Parallelentscheidung OGH 11.12.2003, 6 Ob 218/03g.

⁶⁹ ErlRV 817 BlgNR XXI. GP 33

⁷⁰ ErlRV 817 BlgNR XXI. GP 33.

⁷¹ Vgl ErwG 43 der E-Commerce-RL.

werden, sonst handelt es sich um Hosting.⁷² Access-Provider ist ihm bisherigen Beispiel daher dasjenige Unternehmen, das dem Internetuser Leitungskapazitäten zur Verfügung stellt, damit dieser nach seinem Ermessen auf Online-Dienste wie zB Facebook oder YouTube zugreifen kann. Auch ein E-Mail-Dienst, der ausschließlich elektronische Nachrichten übermittelt und weder den Adressat der Nachricht noch die übertragenen Informationen auswählt, ist (bloßer) Access-Provider.

B.I.4.d. Einzelfragen

B.I.4.d.1. Online-Archive

Der OGH hatte zu entscheiden, ob ein Betreiber eines Online-Archives, also einer Sammlung von Zeitschriftenartikeln, die davor online und/oder in Printform erschienenen waren, Content- oder Host-Provider ist. Im Einklang mit der gängigen Definition stellte der OGH darauf ab, dass der Betreiber des Online-Archivs selbst Informationen ins Netz stellt, und kam daher zu dem Schluss, dass dieser Content-Provider ist.⁷³ *Zankl* argwöhnte, dass damit zwar dem Wortlaut genüge getan wird (arg: "Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert"), teleologisch aber wohl doch Host Providing vorliege, weil es nicht so entscheidend sei, wie (vom Nutzer oder vom Diensteanbieter) Information eingegeben wird, sondern dass sie eingegeben wird und es sich aus der Sicht des Diensteanbieters um fremde Information handelt.⁷⁴

Letzterer Ansicht ist der Vorzug zu geben, weil sie darauf abstellt, worauf es ankommt: Das Bereitstellen von fremden Informationen macht nämlich den entscheidenden Unterschied zwischen Content- und Host-Providern aus. Während dies früher damit gleichzusetzen gewesen sein mag, wer online Informationen einspeist, ist dies heute manchmal nicht mehr so eindeutig: Viele Forenbetreiber und Zeitungen (etwa die New York Times) kontrollieren zur Vermeidung von Spam oder rechtswidrigen Inhalten heute vorab, was ihre User eingeben wollen, und stellen erst nach Freigabe den fremden Text unverändert ins Internet. Bei striktem Festhalten an dem Wortlaut des Gesetzes müssten die Betreiber dadurch zu Content-Providern werden, weil sie (und nicht mehr der Nutzer) die Informationen als letztes Glied der Kette „eingeben“. Die sich daraus ergebenden Konsequenzen sind aber teleologisch nicht vertretbar.

Der OGH bestätigte freilich seine Linie in einer späteren Entscheidung mit ähnlichem Sachverhalt, ohne auf die genannten Argumente einzugehen; dies war aber auch verzichtbar, weil

⁷² *Zankl*, E-Commerce-Gesetz Rz 195 f mwN.

⁷³ Vgl OGH 11.12.2003, 6 Ob 274/03t (Online-Archiv I) mwN; ebenso die Parallelentscheidung OGH 11.12.2003, 6 Ob 218/03g.

⁷⁴ *Zankl*, Online-Archiv: Dritte OGH-Entscheidung zum E-Commerce-Gesetz, *ecolex* 2004, 524.

sich auch die beklagte Archivbetreiberin selbst (seltsamerweise) auf den Standpunkt stellte, Content-Provider zu sein.⁷⁵

B.I.4.d.2. Suchmaschinenbetreiber

Suchmaschinen erfüllen in der mittlerweile unüberblickbaren Informationsvielfalt des Internets eine wichtige Ordnungs- und Anwendungserleichterungsfunktion. Sie durchsuchen das Internet aufgrund der Eingabe von bestimmten Begriffen oder Wortfolgen und sortieren die dabei vorgefundenen Websites anhand von komplexen Algorithmen nach ihrer Relevanz.

Dabei vermitteln sie weder den Zugang zu einem Kommunikationsnetz wie dem Internet noch übermitteln sie in einem solchen von Usern eingegebene Daten, wie es Access-Provider tun. Ebenso wenig speichern Suchmaschinenbetreiber fremde Informationen auf ihren Servern, wie es Host-Providern entspricht. Schließlich stellen sie auch keine eigenen Inhalte zur Verfügung, weswegen sie auch keine Content-Provider sind.

Zwar fallen sie somit in keine der drei oben beschriebenen Kategorien. Suchmaschinen vermitteln aber – wie Access-Provider – den Zugang zu fremden Informationen, indem sie auf den Ergebnisseiten Links zu Websites anbieten, die die vom User gesuchte Information beinhalten. Im österreichischen Recht steht ihre Haftungssituation daher in einem normativen Gleichklang zu der des Access-Providers (vgl §§ 13 und 14 ECG). Auf europäischer Ebene wurde bis dato auf eine Regelung verzichtet.⁷⁶

IdZ ist aber nochmals zu betonen, dass sich die Einordnung in eine der genannten Providerkategorien stets nach funktionalen Kriterien bestimmt. Die Ähnlichkeit der Tätigkeit des Suchmaschinenbetreibers zu der des Access-Providers besteht nur bei der neutral-technischen Weiterleitung zu fremden Informationen, die auf den Servern Dritter gespeichert sind. Wenn Suchmaschinenbetreiber dagegen zusätzlich zu ihrer Kerntätigkeit Dienste anbieten, bei denen sie fremde Informationen speichern, erfüllen sie die Kriterien des Host-Providings. Das hat insb im Zusammenhang mit Keyword-Advertising große Bedeutung, weil es dort üblich ist, dass Anbieter wie Google fremde Werbetexte und damit verbundene Keywords entgegennehmen und speichern, und daran anknüpfend Anzeigen neben oder oberhalb der Suchergebnisse erscheinen lassen. Diese Tätigkeit fällt nach der Rsp des EuGH unter Host-Providing, solange der Anbieter nicht selbst eine aktive Rolle gespielt hat, die ihm eine Kenntnis der gespeicherten Daten oder eine Kontrolle über sie verschaffen konnte.⁷⁷

⁷⁵ OGH 19.2.2004, 6 Ob 190/03i (Online-Archiv II); dazu *Zankl*, *ecolex* 2004/319.

⁷⁶ Vgl *Zankl*, E-Commerce-Gesetz Rz 205.

⁷⁷ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 111 f; dazu noch ausführlich unten auf S 185 f.

B.II. Immaterialgüterrechtsverletzungen im Internet

Eine Untersuchung von Rechtsproblemen im Internet müsste früh enden, wenn das Internet ein „rechtsfreier Raum“ wäre, wie es zu Beginn der Online-Revolution manchmal geheißen hat. Diese Ansicht ist aber heute klar überholt. Das Recht selbst ist vielmehr „medienneutral“ und folgt im Internet denselben Prinzipien wie bei Sachverhalten, die sich offline abspielen. Da und dort bestehen Sonderregeln, die der Besonderheit des Internets und darin abgewickelter Transaktionen Rechnung tragen. Grds müssen aber auf rechtliche Probleme im Internet dieselben, teilweise bereits sehr alten, Normen angewendet werden wie bei „herkömmlichen“ Sachverhalten.⁷⁸ Das historisch gewachsene Immaterialgüterrecht findet also auch dann Anwendung, wenn Verletzungshandlungen im Internet gesetzt werden.

Das Immaterialgüterrecht steht in seiner Entwicklung seit jeher im Wettstreit mit technologischen Neuerungen. Viele potentielle Nutzungs- und damit Verletzungsarten von Immaterialgütern entstanden durch technische Innovationen, an die man beim Erlass der einschlägigen Gesetze nicht gedacht hatte. Besonders anfällig dafür ist das Urheberrecht, das zumindest nach kontinentaleuropäischer Tradition ohne Formalakte entsteht und dessen geschützte Güter, also zB Leistungen auf dem Gebiet der Literatur, der Ton- oder Filmkunst, zunehmend einfach zu kopieren sind. Seit jeher schwelt daher ein Zielkonflikt zwischen den Interessen der Öffentlichkeit auf Zugang zu neuen Geisteswerken und den Verwertungsinteressen der Urheber, der notgedrungen durch immer neue gesetzliche Regelungen ausbalanciert werden muss.⁷⁹ Die technologische Entwicklung ist der Schrittmacher für diese Neuerungen. Unser heutiges Urheberrecht wurzelt beispielsweise im Privilegienwesen für Buchverleger, das erst durch das Aufkommen des Buchdrucks in der Mitte des 15. Jahrhunderts notwendig wurde.⁸⁰ Ob Grammophon, Rundfunk oder Videorekorder: Stets wurden revolutionäre Innovationen in der Unterhaltungselektronik von Debatten um die Reichweite und die Grenzen des Urheberrechts begleitet. Das Internet trieb und treibt diesen Prozess auf die Spitze: Noch nie zuvor war es so einfach, urheberrechtlich geschützte Werke anzusehen, sie zu hören, zu kopieren, zu tauschen und zu speichern. Durch die Digitalisierung gibt es beim Kopieren keine Qualitätsverluste mehr, die Transportkosten liegen nahe dem Nullpunkt und die für Kopien erforderlichen Geld- und Zeitmittel sind ebenso vernachlässigbar.

Spätestens seit der Schutz von Software im Urheberrecht und nicht durch Patente erfolgt („copyright approach“⁸¹), liegt das Schwergewicht der immaterialgüterrechtlichen Probleme

⁷⁸ Vgl *Zankl*, Bürgerliches Recht⁵ Rz 252 f.

⁷⁹ Die anhaltende gesetzgeberische Aktivität ist zudem Ausdruck der ökonomischen Notwendigkeit, durch das Urheberrecht dem ansonsten drohenden Marktversagen in Bezug auf Immaterialgüter entgegenzuwirken; dazu *Stepan*, Ökonomie des Urheberrechts Ein Überblick, *juridikum* 2007, 35 f.

⁸⁰ *Kucsko*, Geistiges Eigentum 1067; *Walter*, Österreichisches Urheberrecht Rz 14.

⁸¹ *Kucsko*, Geistiges Eigentum 1091.

im Zusammenhang mit dem Internet im Urheberrecht. Besondere Herausforderungen stellen sich auch im Markenrecht, wie etwa die Problematik von rechtsverletzenden Online-Shops oder die Nutzung fremder Marken in Online-Werbeanzeigen. Die unten behandelten Probleme (Websites, Filesharing, Keyword-Advertising) sind daher in diesen beiden Rechtsbereichen konzentriert.

B.II.1. Anwendbares Recht und internationale Zuständigkeit

Aufgrund der Kommunikationsarchitektur des Internets werden idR mehrere Landesgrenzen überschritten, wenn Daten auf Websites gestellt oder unter Internetusern ausgetauscht werden. Zudem sind diese Daten auf der ganzen Welt einfach abrufbar.

Traditionell wird bei Immaterialgüterrechtsverletzungen an die Rechtsordnung des Landes, für dessen Gebiet der Schutz beanprucht wird (Schutzland), angeknüpft.⁸² Dieses Konzept stößt im Zusammenhang mit dem Internet an seine Grenzen, weil Verletzte idR Schutz für alle Rechtsordnungen begehren, in denen immaterialgüterrechtsverletzende Informationen empfangen werden können. Aus Sicht des Bereitstellers würden dadurch unabwägbare Risiken entstehen, weil er sich an alle bestehenden Rechtsordnungen halten müsste. Umgekehrt ist die Anknüpfung aufgrund technischer Kriterien (zB das Land, in dem der Server steht) ebensowenig zielführend, weil dadurch leicht und gezielt strengere Rechtsordnungen umgangen werden können, der Schaden für die betroffenen Rechteinhaber aber bestehen bliebe.⁸³ Im Unionsrecht wurde davon Abstand genommen, bei der Erbringung von Diensten der Informationsgesellschaft auch Marken- und Urheberrechte dem Herkunftslandprinzip der E-Commerce-RL zu unterwerfen, sodass die Anknüpfungproblematik bei immaterialgüterrechtlichen Internetsachverhalten auch innerhalb Europas noch existiert.⁸⁴

In der österreichischen Rsp wird tendenziell ein rechteinhaberfreundlicher Standpunkt eingenommen. So entschied der OGH, dass österreichisches materielles Urheberrecht anzuwenden sei, wenn auf einer Website mit einer in Deutschland registrierten Domain urheberrechtlich geschützte Texte verbreitet und auch dem (deutschsprachigen) Publikum in Österreich zugänglich gemacht würden.⁸⁵ Auch im Markenrecht kam er zu einem ähnlichen Ergebnis, indem er aussprach, mit einem Internetauftritt, bei dem Ware gezeigt wird, werde diese auch in Österreich angeboten und für sie geworben. Der Inlandsbezug werde dadurch hergestellt, dass die Internetseite von einem inländischen Internetzugang aus angewählt werden kann.⁸⁶

⁸² Vgl RIS-Justiz RS0076884 zu § 34 IPRG.

⁸³ Vgl *Verschraegen* in Rummel³ § 34 IPRG Rz 25 f.

⁸⁴ Vgl § 21 Z 1 ECG sowie Art 3 E-Commerce-RL iVm deren Anhang; *Fuchs*, Zulässigkeit von kontextabhängiger Suchmaschinenwerbung, wbl 2007, 414 (417).

⁸⁵ OGH 16. 12. 2003, 4 Ob 238/03h.

⁸⁶ OGH 24.4.2001, 4 Ob 81/01t.

Um diesen in der Praxis nützlichen, aber ubiquitären Ansatz sachgerecht zu beschränken, wäre es sinnvoll, dass derartige Anknüpfungen sich auf Länder beschränken, deren Publikum durch die jeweilige Website angesprochen wird. Dies kann durch Indizien wie Sprache oder Domainnamen bestimmt werden.⁸⁷

Die Zuständigkeit der Gerichte folgt ähnlichen Mechanismen, weil dasjenige Gericht zuständig ist, in dessen Sprengel die verletzende Handlung gesetzt wurde (§ 87c Abs 1 JN) bzw das Gericht des Ortes, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht (Art 5 Z 3 EUGVVO). Was Rechtsverletzungen im Internet anbelangt, ist davon auszugehen, dass jeder Ort, von welchem eine Website abgerufen werden kann, als Verletzungsort anzusehen ist.⁸⁸ Eine entsprechende Klage wird somit oft im eigenen Land unter Anwendung eigenen nationalen Rechts eingebracht werden können – damit sind die faktischen Probleme der Rechtsdurchsetzung aber nicht gelöst, sondern beginnen vielfach erst.

B.II.2. Faktische Grenzen der Rechtsdurchsetzung im Internet

Im Vergleich zu offline-Rechtsverletzungen ist nämlich schon der erste Schritt, die Ermittlung der Identität des Rechtsverletzers, oft ein Problem. Da das Internet keiner Zugangskontrolle unterliegt und auf einer dezentralen Kommunikationsarchitektur basiert, können Rechtsverletzungen (nicht nur) an Immaterialgüterrechten vielfach anonym begangen werden.

So scheitert die Klagsführung gegen Betreiber von Websites mit illegal angebotenen Datenmaterial im Regelfall daran, dass die Inhaber nicht auffindbar sind oder sich in Jurisdiktionen aufhalten, in denen keine oder mangelhafte Rechtssicherheit besteht, was die Vollstreckung ausländischer Urteile betrifft. Nur auf harmonisierten „Inseln“ wie dem Gebiet der EU sind deutliche Fortschritte bei der grenzüberschreitenden Ahndung von Immaterialgüterrechtsverletzungen erkennbar. Während daher materielle Verletzungen von Immaterialgüterrechten im Internet idR ebenso leicht zu durchschauen wie durchzuführen sind, stehen der Durchsetzung dieser Rechte oft unüberwindbare faktische Hindernisse entgegen. Im stetigen Wettlauf mit den technologischen Neuerungen liegt das Rechtssystem derzeit zweifellos deutlich zurück: Die früher „potentielle Ubiquität“ von Immaterialgütern ist heute nahe an einer tatsächlichen Ubiquität gelangt. Dieser Globalisierung der Information ist bis dato aber keine vergleichbare Globalisierung der Rechtsdurchsetzung gefolgt.

Dennoch ist es nicht so, dass die theoretische „Medienneutralität des Rechts“ gänzlich durch faktische Hindernisse ausgehöhlt wird. Immaterialgüterrechte können auch im Internet durchgesetzt werden – es braucht lediglich manchmal andere Wege als bei herkömmlichen

⁸⁷ *Verschraegen* in Rummel³ § 34 IPRG Rz 29; *Fuchs*, Zulässigkeit von kontextabhängiger Suchmaschinenwerbung, wbl 2007, 414 (416 f) mwN; dazu jüngst auch OGH 5.10.2010, 17 Ob 8/10s (Snowboards).

⁸⁸ Vgl *Walter*, Glosse zu 4 Ob 238/03h, MR 2004, 123 mwN.

Rechtsverletzungen. Das Internet selbst bietet Rechteinhabern verschiedenste Informationsquellen, was die Ausforschung von Rechtsverletzern und deren Aktivitäten betrifft. Es ist aber zu differenzieren: Während manche Informationen direkt auf Websites oder in Registern öffentlich abrufbar sein müssen, sind andere Informationen durch Datenschutzvorschriften privilegiert und nur bei Dritten verfügbar. Auf diese Daten kann nur kraft qualifizierter gesetzlicher Ermächtigung und nur im Rahmen eines geordneten Verfahrens zugegriffen werden.

So in bestimmten Konstellationen de jure oder de facto tatsächlich keine Möglichkeit besteht, subjektive Immaterialgüterrechte auch praktisch durchzusetzen, wird in den folgenden Kapiteln rechtspolitisch – in der gebotenen Kürze – darauf eingegangen werden.

B.III. Immaterialgüterrecht als Querschnittsmaterie

Der normative Schwerpunkt des Immaterialgüterrechts liegt zweifellos im Privatrecht. Die primären Instrumentarien zur Rechtsdurchsetzung sind daher auch in diesem Gebiet bzw im Zivilprozessrecht zu finden. Das „Arsenal“ der Rechteinhaber ist aber deswegen nicht auf diesen Bereich beschränkt. Insbesondere das Strafrecht liefert teilweise besonders durchgreifende Mechanismen, um die Durchsetzung von Immaterialgüterrechten zu erleichtern. Vor allem kann das typische Informationsgefälle zwischen Rechteinhabern und Verletzern durch den Einsatz spezifischer behördlicher Zwangsmaßnahmen (zB Identitätsfeststellungen, Rufdatenrückverfolgung) effektiv ausgedünnt werden.

Im Zuge der folgenden Untersuchungen wird daher gelegentlich der rein privatrechtliche Fokus der Arbeit verlassen und auf andere Rechtsgebiete eingegangen werden, wenn dies zur besseren Durchdringung der dargestellten Problemkreise geboten erscheint.

Durch die stetig fortschreitende Harmonisierung zahlreicher Rechtsgebiete innerhalb der EU kann in vielen Bereichen praktisch keine Analyse des nationalen Rechts erfolgen, ohne gleichzeitig die europarechtlichen Grundlagen zu kennen. Das gilt im besonderen Maße für das Immaterialgüter- und Internetrecht, die für grenzüberschreitende Regelungsmechanismen geradezu prädestiniert sind. Daher werden bei den verschiedenen behandelten Ansprüchen bewusst zunächst die einschlägigen Vorgaben des europäischen Sekundärrechts (RL, VO) behandelt, bevor auf die nationale Rechtslage eingegangen wird.

C. RECHTSVERLETZENDE WEBSITES

Websites sind die Knotenpunkte und „Portale“ des Internets, auf denen die zahlreichen verfügbaren Informationen zusammenlaufen und abgerufen werden können. Verletzungen von Immaterialgüterrechten passieren dort häufig, zB weil bei der Programmierung und Gestaltung von Websites gerne auf einfach verfügbares Bildmaterial zurückgegriffen wird, das man beim Surfen gefunden hat. Typischerweise ist derartiges Bildmaterial aber durch Urheberrechte geschützt. Auch Markenrechte können verletzt werden, etwa im Zusammenhang mit Online-Shops, die Produkte mit unzulässigen Markenschriftzügen vertreiben. Sehr oft werden auf Websites auch herunterladbare Inhalte zur Verfügung gestellt, die ebenfalls immaterialgüterrechtlich geschützt sind, etwa Musik- oder Videodateien.

Wichtig ist die Unterscheidung zwischen einer Website „an sich“, also der Summe aus den abrufbaren Inhalten und Unterseiten, und dem „Adressschild“ der Website, etwa <orf.at> oder <e-center.eu>, das als „Domain“ bezeichnet wird. Als das Internet, das ursprünglich lediglich für das US-Militär und US-Universitäten entwickelt wurde, noch in seinen Kinderschuhen steckte und die Zahl der Datensätze entsprechend gering war, wurden alle in Verwendung stehenden Domains zentral verwaltet und auch alle Neuregistrierungen von einer einzelnen Organisation (DARPA) durchgeführt. Die Recherche zu vergebenen IP-Adressen und Domains gestaltete sich dementsprechend einfach, weil damals noch keine datenschutzrechtlichen Bedenken bestanden und die Spam-Problematik ebenfalls noch kein Thema war. Jeder Internetnutzer konnte Informationen über alle vergebenen IP-Adressen, Domains und Personen durch eine sogenannte „Whois-Abfrage“ (aus dem engl. „Who is?“ für „Wer ist?“) beim Server der DARPA erhalten. Darunter fanden sich idR Name, Postadresse, E-Mail-Adresse und Telefonnummer der physischen Person, der eine bestimmte Domain oder IP-Adresse zugeordnet war. So konnte innerhalb der noch eher kleinen Internetgemeinde rasch und unbürokratisch Kontakt zu den Betreibern von Websites aufgenommen werden, wenn diese ihre Kontaktdaten nicht ohnehin veröffentlicht hatten.

Mit zunehmender Ausbreitung des Internet und dem damit verbundenen Hinzukommen neuer TLD-Verwalter und dem fortschreitenden Missbrauch des Internet durch Spam-Versender wurde dieses offene System immer weiter zurückgedrängt. Die Nachfolgeorganisation der DARPA wurde die ICANN, die heute alle weltweit verwendeten Domains und IP-Adressen in Letztverantwortung verwaltet und die Grundlagen für die technische Weiterentwicklung des Internet beschließt. Den theoretisch (völkerrechtlich) nicht rechtsverbindlichen ICANN-Beschlüssen kommt daher große praktische Bedeutung zu. Die ICANN ist organisatorisch eine Stiftung US-amerikanischen Rechts und war bis 1.10.2009 direkt der Kontrolle durch das US-Handelsministerium unterworfen. Heute wacht zwar ein internationales Gremium aus Interessensvertretungen und staatlichen Regierungen über die ordnungsgemäße

Erfüllung von ICANNs Aufgaben, der US-Regierung kommen aber doch noch beträchtliche Einflussmöglichkeiten zu.⁸⁹

In der Praxis übt ICANN heute insbesondere die Verwaltung von sog nichtgesponsorten TLD wie .com, .info oder .org aus. Die Verwaltung länderspezifischer TLD (wie zB .de oder .at) wurden dagegen vertraglich an Unterorganisationen („Registries“) vergeben, für Österreich etwa an nic.at.

C.I. Informationsbeschaffung

Die einfachste und kostengünstige Methode, um rechtsverletzenden Websites im Internet nachzugehen, ist die Internetrecherche. Dabei können öffentlich einsehbare Whois-Datenbanken und Pflichtangaben auf Websites genutzt werden. Anordnungen oder Bewilligungen von Behörden oder Gerichten sind dabei idR nicht vonnöten.

Für den Fall, dass Betreiber von Websites ihren Informationspflichten nicht nachkommen, spannen Auskunftsansprüche gegenüber Host-Providern ein zusätzliches Informationsnetz.⁹⁰

C.I.1. Whois-Abfrage

C.I.1.a. Überblick

„Whois“ ist ein Computerprotokoll, mit dem innerhalb eines Datenbanksystems verschiedene Informationen über Domains, IP-Adressen und den dahinter stehenden Personen abgerufen werden können. Dazu wird auf Datensätze zurückgegriffen, die entweder zentral bei den Registrierungsstellen, die für die jeweilige TLD zuständig sind („Registries“), oder bei den kommerziellen Domainhändlern, die konkrete Domainnamen an Endnutzer verkaufen („Registrare“) gespeichert sind. Damit jeder Enduser, der von einem Registrar eine Domain erwirbt, auch erfasst wird, ist in den „Registrar Accreditation Agreements“ (RAA) zwischen der ICANN und den einzelnen Registraren eine Verpflichtung vorgesehen, Daten über den Inhaber der Domain zu erheben und für whois-Abfragen öffentlich einsehbar zu machen.⁹¹

Rechtlich bindende internationale Abkommen, wie diese vertragliche Verpflichtung der einzelnen Registrare mit den jeweils anwendbaren Datenschutzgesetzen in Einklang zu bringen sind, existieren (noch) nicht. Daher kommt den Vorgaben, Empfehlungen und „Policys“ der mit der zentralen Verwaltung des „Domain Name System“ (DNS) betrauten Organisationen, wie den großen Registries und ICANN selbst, entscheidende Bedeutung zu. Mittlerweile un-

⁸⁹ Vgl heise online vom 30.9.2009: <heise.de/newsticker/meldung/Neue-Zeitrechnung-fuer-die-Internetverwaltung-798333.html>.

⁹⁰ Zankl, E-Commerce-Gesetz Rz 283.

⁹¹ Vgl Pkt 3.3 des aktuellen RAA, abrufbar unter <icann.org/en/registrars/ra-agreement-21may09-en.htm#3>.

terhalten viele Registrare eigene Whois-Datenbanken für die Websites, die unter ihrer jeweiligen TLD registriert sind.⁹²

C.I.1.b. Technische Funktionsweise

Whois-Abfragen können in der Praxis entweder über eigene Computerprogramme (Clients) oder über einen entsprechenden Online-Dienst⁹³ ausgeführt werden. Dabei muss nur die Domain (zB <orf.at>) bekannt sein und im entsprechenden Formular des Programms oder Dienstes eingetragen werden. Als Ergebnis der Suche bekommt man Informationen etwa dieser Art:

```
domain:    orf.at
registrant: OR3343723-NICAT
(...)
personname: Online Direktion-Thomas Prantner
organization: Oesterreichischer Rundfunk
street address: Wuerzburggasse 30
postal code: 1136
city:      Wien
country:   Austria
phone:     +4318787821400
fax-no:    +43187878521400
e-mail:    online.direktion@orf.at
nic-hdl:   OR3343723-NICAT
changed:   20080331 08:41:49
source:    AT-DOM
```

Diese Daten sind für jedermann binnen Sekunden im Internet abrufbar. Dementsprechend groß ist das Interesse von so unterschiedlichen Akteuren wie Strafverfolgungsbehörden, Rechteinhabern und Spam-Versendern, dass die Daten möglichst aktuell und valide sind. Die Qualität von whois-Abfragen schwankt allerdings beträchtlich. Dies liegt am heute herrschenden Fleckenteppich von Registries und Registraren, die höchst unterschiedliche Anstrengungen unternehmen, um die Angaben von Endkunden auf Korrektheit zu überprüfen. Einer Studie der ICANN zufolge sind nur 23% aller Einträge in whois-Datenbanken völlig korrekt – in etwa doppelt so viele ermöglichen über Umwege den Kontakt zum Domaininhaber.⁹⁴

⁹² Einen guten Überblick liefert <dmoz.org/Computers/Internet/Domain_Names/Name_Search//>.

⁹³ Es gibt hier zahlreiche Dienste mit verschiedenen, kostenlosen Angeboten. Für Recherchezwecke hat sich <gaijin.at/olswhois.php> bewährt.

⁹⁴ Vgl <icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf> 3.

Zahlreiche Streaming-Websites, die kostenlos auf urheberrechtlich geschütztes Material verlinken (zB Kinofilme, TV-Serien), haben sich diese Tatsache zu Nutze gemacht und für ihre Dienste solche TLD ausgewählt, die wenig oder keine Angaben zum Registrar einer Domain über Whois-Abfragen bereitstellen. So ist zB über die Betreiber von Seiten mit der TLD .to mittels Whois-Abfragen idR nichts Brauchbares eruierbar, sodass problematische Websites wie <kino.to> praktisch anonym betrieben werden können. Bei gewerbsmäßig agierenden Rechtsverletzern wird die Zuordnung einer bestimmten Website über eine whois-Abfrage idR schon deshalb fehlschlagen, weil diese sich davor hüten, korrekte Angaben bei der Registrierung ihrer Domain zu machen. Strengere Vorschriften für Registrare, die zB für fehlerhafte whois-Einträge haften sollen, sind daher Gegenstand politischer Debatten inner- und außerhalb der ICANN. Jedoch stehen die international höchst unterschiedlichen nationalen Datenschutzbestimmungen oft einer umfassenden Erhebung und Veröffentlichung personenbezogener Daten entgegen.⁹⁵

Um den Schutz ihrer Daten besorgte Domaininhaber können sich auch dazu entschließen, den Service eines anonymisierenden Proxy-Dienstes⁹⁶ in Anspruch zu nehmen. Diese Dienste registrieren die gewünschten Domains in ihrem Namen und geben sie an den jeweiligen Enduser weiter. Im Ergebnis der whois-Abfrage scheint dann der Proxy-Dienst als Kontaktadresse auf, sodass persönliche Daten des faktischen Inhabers der Domain nicht in die whois-Datenbank gelangen. Diese Praxis wird in den RAA nicht explizit behandelt, aber indirekt doch als gegeben vorausgesetzt⁹⁷ und damit toleriert. Bei einigen Proxy-Diensten besteht laut den Erkenntnissen der ICANN-Studie⁹⁸ die Möglichkeit, den tatsächlichen Domaininhaber über ein Online-Formular auf der Website des Proxy-Dienstes direkt zu kontaktieren, allerdings ohne die Identität des Domaininhabers offen zu legen.

Proxy-Anbieter müssen sich nicht bei der ICANN akkreditieren, daher unterliegt ihr Umgang mit Rechtsverletzungen unter Domains, die von ihnen betreut werden, keiner Aufsicht. Es bestehen auch insofern erhebliche Rechtsschutzdefizite, als Proxy-Dienste idR die Daten ihrer Kunden nicht vorab prüfen und auch keine Äußerungsfristen einhalten müssen.

⁹⁵ Siehe etwa heise online vom 9.3.2010: <heise.de/netze/meldung/Strafverfolger-wollen-unverfaelschte-Domaininhaber-Daten-949381.html> und vom 23.6.2008: <heise.de/netze/meldung/Die-Internet-Verwaltung-streitet-ueber-Datenschutz-fuer-Domain-Inhaber-215653.html>.

⁹⁶ Gebräuchlich sind auch die Bezeichnungen „Privacy“, „Shield“ oder „Guard“.

⁹⁷ Dies ergibt sich aus Pkt 3.4 des RAA, der auf Proxy-Dienstleistungen Bezug nimmt; vgl auch die (englischsprachigen) Erläuterungen zum RAA unter <icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm#text1>, insb Pkt 2.3.4.

⁹⁸ Vgl <icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf> 31.

C.I.1.c. Ergebnis

Für Rechteinhaber lohnt sich eine whois-Recherche bei der Informationsbeschaffung über rechtsverletzende Websites trotz aller Unzulänglichkeiten idR schon alleine aufgrund der fehlenden Kosten. Falls nur ein Proxy-Dienst als Kontaktadresse ermittelt werden kann, so kann zumindest dieser kontaktiert werden, um Auskunft über den Betreiber der Website zu bekommen. Ein Rechtsanspruch auf Auskunft besteht aber derzeit (noch) nicht.

C.I.2. Offenlegungspflichten

Um das typische Informationsdefizit zwischen Internetusern und Website-Betreibern zu verringern, ordnen diverse Gesetze Informationspflichten an. Die Tätigkeit des europäischen Gesetzgebers hat stark zur Verbreitung solcher Informationspflichten beigetragen.

C.I.2.a. Europarechtliche Grundlagen

C.I.2.a.1. E-Commerce-RL

Die E-Commerce-RL soll gem Art 1 einen Beitrag zum einwandfreien Funktionieren des Binnenmarktes leisten, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt. Dazu ordnet sie ua umfangreiche Informationspflichten für Dienstanbieter an (Art 5).

Der österreichische Gesetzgeber hat diese Informationspflichten weitgehend wortgleich in das ECG aufgenommen. Die Einzelheiten können daher unten bei § 5 ECG erläutert werden.

Da die E-Commerce-RL die Informationspflichten für Anbieter von Diensten der Informationsgesellschaft sehr detailliert regelt, sind die für die österreichische Umsetzung in § 5 ECG geltenden Grundsätze auf alle Websites, die von Diensteanbietern innerhalb der EU betrieben werden, anwendbar. Welches nationale Recht konkret anwendbar ist, richtet sich gem der E-Commerce-RL danach, wo der Diensteanbieter mittels einer festen Einrichtung eine Wirtschaftstätigkeit auf unbestimmte Zeit tatsächlich ausübt - unabhängig davon, wo der Server steht, von dem aus die Website betrieben wird (Art 2 lit c).⁹⁹ Sollte ein Diensteanbieter in mehr als einem Mitgliedstaat niedergelassen sein, so gilt nach der Rsp des EuGH das Recht jenes Mitgliedstaates, in dem er den Mittelpunkt seiner Tätigkeit hat.¹⁰⁰

⁹⁹ *Stomper*, Europäische Union regelt E-Commerce Die EU-Richtlinie über den Elektronischen Geschäftsverkehr im Überblick, SWK 2000, W 59.

¹⁰⁰ EuGH 5.6.1997 Rs C-56/96 Rz 23.

C.I.2.b. Nationale Rechtslage

Sowohl ECG wie auch MedienG ordnen für die Inhaber von Websites Offenlegungs- und Informationspflichten an. Es ist nach dem Anwendungsbereich und dem Umfang dieser Pflichten zu differenzieren.

C.I.2.b.1. § 5 ECG

Das ECG und seine Informationspflichten finden Anwendung auf Anbieter von Diensten der Informationsgesellschaft. Letzteres sind gem § 3 Z 1 ECG in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellte Dienste, insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern. Da Websites ihre Dienste ohne Zweifel elektronisch im Fernabsatz und auf individuellen Abruf des Empfängers bereitstellen, ist das entscheidende Kriterium die regelmäßige Entgeltlichkeit.

Der Entgeltlichkeitsbegriff ist des ECG ist äußerst weit.¹⁰¹ Nicht nur direkte kommerzielle Angebote, die sofort bezahlt werden müssen, fallen darunter, sondern auch werbefinanzierte Websites mit kostenlosem Content und solche, die lediglich für bestimmte Waren und Dienstleistungen werben, ohne diese selbst zum Verkauf anzubieten. Es genügt eine Gewinnerzielungsabsicht im weitesten Sinne. Websites, die marken- oder urheberrechtlich geschütztes Material zu Werbezwecken verwenden, fallen daher idR unter den Anwendungsbereich des ECG. Umso mehr gilt dies für Websites, die solches Material zum Download anbieten, sei es direkt gegen Entgelt oder indirekt durch Bannerwerbung finanziert.

Anbieter von Diensten der Informationsgesellschaft, belanglos ob natürliche oder juristische Personen, fallen ua unter die Auskunftspflichten nach § 5 ECG. Ein Diensteanbieter hat den Nutzern demnach bestimmte Informationen ständig leicht und unmittelbar zugänglich zur Verfügung zu stellen. Darunter fallen vor allem sein Name oder seine Firma sowie die geografische Anschrift, unter der er niedergelassen ist, weiters Angaben, auf Grund deren die Nutzer mit ihm rasch und unmittelbar in Verbindung treten können, einschließlich seiner elektronischen Postadresse.¹⁰²

¹⁰¹ *Zankl*, E-Commerce-Gesetz Rz 72 ff; EuGH 7.12.1993 Rs C-109/92 (Wirth); ErlRV BlgNR 817 XXI GP 18.

¹⁰² RIS-Justiz RS0118401: Aus der vom Gesetzgeber gewählten Formulierung "einschließlich seiner elektronischen Postadresse" ist abzuleiten, dass neben dieser mindestens ein anderer individueller Kommunikationsweg (arg.: "in Verbindung treten") angegeben werden muss, worunter etwa Telefon oder Telefax fallen.

C.I.2.b.2. §§ 24, 25 MedienG

Ein Medium ist nach der gesetzlichen Definition in § 1 Abs 1 Z 1 MedienG jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis im Wege der Massenherstellung oder der Massenverbreitung. Eine Website ist in dieser Definition problemlos einzuordnen, das MedienG daher grds auch auf diese anwendbar. Aus den §§ 50 und 51 MedienG ergibt sich, dass nur Medien österreichischer Medieninhaber im Vollanwendungsbereich des MedienG liegen, es sei denn, dass Medien ausländischer Medienunternehmer zur Gänze oder nahezu ausschließlich in Österreich verbreitet werden – dann ist das MedienG voll anwendbar. Da Websites weltweit abrufbar sind, wird eine (nahezu) ausschließliche Verbreitung in Österreich allerdings idR ausscheiden, sodass auf ausländische Betreiber die Informationspflichten nach dem MedienG nicht anwendbar sind. Eine Unterscheidung nach TLD ist dagegen nicht vorgesehen. Daraus folgt, dass beispielsweise auch Websites mit den Endungen .com oder .de Endungen voll unter das österreichische MedienG fallen, sofern ihr Betreiber Österreicher ist und sie in Österreich abrufbar sind.

Die in § 24 MedienG verankerte allgemeine Impressumpflicht gilt jedoch primär für „Medienwerke“. Auf jedem Medienwerk sind danach der Name oder die Firma des Medieninhabers und des Herstellers sowie der Verlags- und der Herstellungsort anzugeben. Sinn und Zweck dieser Pflicht ist es, die Medienkonsumenten darüber aufzuklären, wer hinter dem Medium steht; seine Angaben sollen aber auch den von einer Berichterstattung Betroffenen in die Lage versetzen, seine Ansprüche gegen die richtige Person zu richten und richtig zu adressieren.¹⁰³ Was ein „Medienwerk“ ist, definiert § 1 Abs 1 Z3 MedienG als ein zur Verbreitung an einen größeren Personenkreis bestimmter, in einem Massenherstellungsverfahren in Medienstücken vervielfältigter Träger von Mitteilungen oder Darbietungen mit gedanklichem Inhalt. Dies umfasst Websites nicht, weil diese keine massenweise hergestellten Träger sind.

Sie sind nach der medienrechtlichen Terminologie vielmehr „periodische elektronische Medien“, also Medien, die auf elektronischem Wege abrufbar sind (§ 1 Abs 1 Z 5a lit b MedienG). Davon strikt zu unterscheiden sind die gem § 24 Abs 3 MedienG der Impressumpflicht unterworfenen wiederkehrenden elektronische Medien. Dies sind nach § 1 Abs 1 Z 5a lit c MedienG nur solche Medien, die auf elektronischem Wege wenigstens vier Mal im Kalenderjahr in vergleichbarer Gestaltung verbreitet werden. Typischerweise sind dies regelmäßig versendete Newsletter oder Werbe-SMS, nicht aber Websites, da diese ja nicht „verbreitet“, sondern abrufbar gehalten werden.¹⁰⁴

¹⁰³ RIS-Justiz RS0067533.

¹⁰⁴ Vgl *Anderl*, Das neue Mediengesetz, ecolex 2005, 701.

Zu beachten ist aber neben der Impressumspflicht die in § 25 MedienG angeordnete Offenlegungspflicht. Danach hat der Medieninhaber jedes periodischen Mediums alljährlich die in den Abs 2 bis 4 bezeichneten Angaben zu veröffentlichen. Sollte der Websitebetreiber auch unter die Informationspflichten nach § 5 ECG fallen, so können die beiden Angaben ausdrücklich gemeinsam angegeben werden (Abs 1 letzter Satz leg cit). Periodische Medienwerke umfassen gem § 1 Abs 1 Z 2 MedienG auch Websites als periodische elektronische Medien, sodass die Offenlegungspflicht alle Betreiber von Websites trifft.¹⁰⁵

Anzugeben sind Name oder Firma, Unternehmensgegenstand, Wohnort, Sitz oder Niederlassung und Art und Höhe der Beteiligung der Medieninhaber. Falls dieser eine Gesellschaft oder ein Verein ist müssen zudem Organvertreter und Gesellschafter sowie Beteiligungsverhältnisse offengelegt werden (vgl § 25 Abs 2 MedienG).

Zu veröffentlichen ist ferner eine Erklärung über die grundlegende Richtung eines periodischen Druckwerks (Blattlinie) oder sonst eines periodischen Mediums. Auf einer Website sind all diese Angaben ständig leicht und unmittelbar auffindbar zur Verfügung zu stellen (Abs 1 4. Satz leg cit), beispielsweise durch einen stets mit einem Klick aufrufbaren Link in der Navigationsleiste.

Eine bedeutende Einschränkung erfährt die Offenlegungspflicht durch § 25 Abs 5 MedienG, nach dem in periodischen und wiederkehrenden elektronischen Medien, die keinen über die Darstellung des persönlichen Lebensbereichs oder die Präsentation des Medieninhabers hinausgehenden Informationsgehalt aufweisen, der geeignet ist, die öffentliche Meinungsbildung zu beeinflussen, lediglich der Name oder die Firma, gegebenenfalls der Unternehmensgegenstand, sowie der Wohnort oder der Sitz des Medieninhabers anzugeben sind. Für private Websites ohne kommerziellen oder publizistischen Hintergrund bedeutet das, dass die Angabe von zB „Josef Maier, Wien“ bereits ausreicht, um der Offenlegungspflicht Genüge zu tun. Anders stellt es sich mE für Seiten mit Weblogs dar, da diese idR sehr wohl geeignet sind, die öffentliche Meinung zu beeinflussen.

C.I.2.c. Ergebnis

Sofern eine Website in den Anwendungsbereich des ECG fällt, kann die Identität des Inhabers der Website durch Einsicht in die offenzulegenden Daten ermittelt werden. Der relevante Bereich auf der Website wird – in Anlehnung an die medienrechtliche Terminologie – meist als „Impressum“ bezeichnet. Sollte das ECG nicht anwendbar sein, etwa weil die Website rein privat ist und keine Erwerbsabsicht (im weitesten Sinn) mit ihr verfolgt wird, greift das MedienG. Die dort angeordneten Offenlegungspflichten sind allerdings bei nicht-kommerziellen Websites deutlich weniger weitgehend als die des ECG.

¹⁰⁵ *Anderl*, Das neue Mediengesetz, *ecolex* 2005, 701 (702).

C.I.3. Zivilrechtlicher Auskunftsanspruch gegen Host-Provider

C.I.3.a. Problemstellung

Falls weder über eine Whois-Abfrage noch durch Einsichtnahme in die Website selbst die Identität des Websitebetreibers ermittelbar sein sollte, könnte für Rechteinhaber eine Auskunft des Host-Providers Abhilfe schaffen. Letzterer stellt dem Websitebetreiber Speicherplatz und Serverkapazitäten idR entgeltlich zur Verfügung und verfügt daher auch über dessen Namen und Adressdaten. Diese beiden Daten sind auch für den Rechteinhaber notwendig, um seinerseits Ansprüche gegen den Websiteinhaber geltend zu machen.

Sollte der Host-Provider diese Daten seines Kunden preisgeben und ihn dadurch (zumindest) der zivilrechtlichen Verfolgung aussetzen, ohne dass ein rechtlicher Grund für die Preisgabe vorliegt, verstieße er gegen seine vertraglichen Schutz- und Sorgfaltspflichten. Er wird daher tendenziell geneigt sein, eine derartige Auskunft zu verweigern, um sich gegenüber seinem Kunden nicht haftbar zu machen.

C.I.3.b. Europarechtliche Grundlagen

Zur Klärung der Frage, ob ein Auskunftsanspruch gegenüber Host-Providern unionsrechtlich obligatorisch ist, ist eine Untersuchung der E-Commerce-RL, der Info-RL, der Enforcement-RL sowie der Datenschutz-RL vorzunehmen. Zu beachten ist auch die Judikatur des EuGH zur Telekom-Datenschutz-RL.

C.I.3.b.1. E-Commerce-RL

Die E-Commerce-RL soll den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellen, um so einen Beitrag zum einwandfreien Funktionieren des Binnenmarkts zu leisten (Art 1 Abs 1).

Ein Auskunftsanspruch Privater gegen Host-Provider ist der E-Commerce-RL nicht zu entnehmen. Art 15 Abs 2 E-Commerce-RL sieht lediglich vor, dass die Mitgliedstaaten Anbieter von Diensten der Informationsgesellschaft dazu verpflichten können, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.

Eine Auskunft auf Verlangen privater Dritter ist daher gerade nicht vorgesehen.¹⁰⁶ Nach ErwGr 48 lässt die RL allerdings die Möglichkeit unberührt, dass die Mitgliedstaaten von Diensteanbietern, die von Nutzern ihres Dienstes bereitgestellte Informationen speichern, verlangen, die nach vernünftigem Ermessen von ihnen zu erwartende und in innerstaatlichen

¹⁰⁶ Vgl Zankl, E-Commerce-Gesetz Rz 283.

Rechtsvorschriften niedergelegte Sorgfaltspflicht anzuwenden, um bestimmte Arten rechtswidriger Tätigkeiten aufzudecken und zu verhindern. Aus dem Wortlaut von Art 15 Abs 2 und ErwGr 48 lässt sich folglich der Schluss ziehen, dass weitergehende Auskunftspflichten grds zulässig sind, wenn sie innerhalb eines „vernünftigen Ermessens“ liegen und zur Aufdeckung bestimmter rechtswidriger Tätigkeiten dienen.

C.I.3.b.2. Info-RL

Gegenstand der Info-RL ist der rechtliche Schutz des Urheberrechts und der verwandten Schutzrechte im Rahmen des Binnenmarkts, insbesondere in Bezug auf die Informationsgesellschaft (Art 1 Abs 1). Dazu sieht Art 8 vor, dass die Mitgliedstaaten bei Verletzungen der in dieser RL festgelegten Rechte und Pflichten angemessene Sanktionen und Rechtsbehelfe vorsehen und alle notwendigen Maßnahmen treffen, um deren Anwendung sicherzustellen. Die betreffenden Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. In Art 8 Abs 3 ist zudem angeordnet, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden.

Im Zusammenhang mit Auskunftspflichten gegenüber Access-Providern wurde insb Abs 3 dieser Bestimmung als unionsrechtliche Grundlage dafür gesehen, im Hinblick auf einen effektiven Schutz des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.¹⁰⁷ Dies wurde vom EuGH unter dem Hinweis auf den Wortlaut der Bestimmung allerdings zutreffend verneint.¹⁰⁸ Dem Anlassfall lag zwar ein Filesharing-Sachverhalt zugrunde, die Überlegung ist aber auch auf rechtsverletzende Websites übertragbar. Ein Auskunftsanspruch ist nämlich schon aufgrund des Wortlautes aus Art 8 Info-RL schlicht nicht ableitbar.

C.I.3.b.3. Enforcement-RL

Die Enforcement-RL betrifft die Maßnahmen, Verfahren und Rechtsbehelfe, die erforderlich sind, um die Durchsetzung der Rechte des geistigen Eigentums sicherzustellen (Art 1), unbeschadet etwaiger Instrumente in den Rechtsvorschriften der Gemeinschaft oder der Mitgliedstaaten, die für die Rechtsinhaber günstiger sind (Art 2). Aufgrund ihres im Vergleich zur Info-RL weiteren Anwendungsbereichs, der neben dem Urheberrecht samt verwandten Schutzrechten auch Rechte aus Marken, Patenten, Geschmacksmustern, Gebrauchsmustern

¹⁰⁷ *Schanda*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 215; *Daum*, Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug!, MR 2009, 249.

¹⁰⁸ EuGH 29.1.2008 Rs C-275/06 (*Promusicae*) Rz 59 iVm Rz 70. Rz 59 lässt Art 8 Abs 3 unerwähnt, weil das spanische Vorlagegericht nicht nach dieser Bestimmung gefragt hatte. Vom Spruch ist aber auch Abs 3 mitumfasst.

etc umfasst,¹⁰⁹ wäre die Enforcement-RL daher prinzipiell geeignet, über den Bereich des Urheberrechts hinausgehende Auskunftsansprüche gegenüber Host-Providern mit Bezug auf rechtsverletzende Websites zu normieren.

Art 8 Enforcement-RL regelt den speziellen Anspruch auf Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen. Abs 1 lit c leg cit schreibt in diesem Zusammenhang vor, dass sichergestellt sein muss, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahren Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbracht.

Der „Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen“, kann mE auch eine Website umfassen, auf der immaterialgüterrechtsverletzende Inhalte zur Verfügung gestellt werden. Im Zusammenhang mit Filesharing-Sachverhalten entspricht dies bereits der hA.¹¹⁰ Die dort entwickelte Argumentation ist auch auf Websites übertragbar.

Nach Art 8 Abs 3 lit a und e Enforcement-RL gilt diese Bestimmung allerdings unbeschadet anderer gesetzlicher Bestimmungen, die (a) dem Rechtsinhaber weiter gehende Auskunftsrechte einräumen bzw (e) den Schutz der Vertraulichkeit von Informationsquellen oder die Verarbeitung personenbezogener Daten regeln. Auch hinsichtlich der Bestimmungen der Enforcement-RL kam der EuGH im erwähnte Anlassfall „Promusicae“ daher zum Schluss, dass die Mitgliedstaaten nicht verpflichtet sind, im Hinblick auf die Sicherstellung eines effektiven Schutzes des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.¹¹¹

C.I.3.b.4. Datenschutz-RL

Generell ist die Verarbeitung personenbezogener Daten im Unionsrecht nur unter besonderen Kautelen gestattet. Zu beachten ist hierbei, welche der einschlägigen RL für die jeweiligen Diensteanbieter und Daten anzuwenden ist.

¹⁰⁹ Dazu *Burgstaller*, Die Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, MR 2004, 405; die Umsetzung der Enforcement-RL erfolgte daher in allen Immaterialgüterrechtsgesetzen weitgehend inhaltsgleich: vgl *Schachter*, Umsetzung der Enforcement-Directive in Österreich, *ecolex* 2006, 810.

¹¹⁰ GA *Kokott*, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 110; *Raschhofer/Steinhofer*, § 87b Abs 3 UrhG: Gemeinschaftsrechts- und verfassungswidrig?, *ecolex* 2010, 716 (719) mwN.

¹¹¹ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 59.

Für Telekommunikation ist zwar die speziellere Telekom-Datenschutz-RL anzuwenden, die die „allgemeine“ Datenschutz-RL erweitert und präzisiert. Ihr Anwendungsbereich erstreckt sich gem Art 3 Telekom-Datenschutz-RL auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft (Union). Host-Provider, die Inhalte Dritter, zB Websites, auf ihrem Speicherplatz speichern, stellen aber nach der Definition keine „elektronischen Kommunikationsdienste“ in öffentlichen Kommunikationsnetzen bereit.¹¹² Nach dem europäischen Regelungskonzept soll nämlich die Regulierung der Übertragung von der Regulierung von Inhalten getrennt bleiben.¹¹³ Host-Provider stellen zwar keine eigenen Inhalte zur Verfügung, ihre Dienste bestehen aber auch „nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze“ – sie unterliegen daher weder der Rahmen-RL noch der Telekom-Datenschutz-RL.¹¹⁴ Für Host-Provider sind folglich die allgemeinen Regeln der Datenschutz-RL anzuwenden, anhand derer somit auch die Zulässigkeit von Auskunftsansprüchen über personenbezogene Daten von Vertragspartnern zu beurteilen ist.¹¹⁵

In diesem Zusammenhang ist auch zu beachten, dass bei einer Auskunft über Name und Adresse des Websitebetreibers (lediglich) Stammdaten¹¹⁶ herausgegeben werden. Entscheidend ist dabei, dass für diese Auskunft keine Verkehrsdaten¹¹⁷ verarbeitet werden müssen, weil der Host-Provider nur Einsicht in seine Vertragsunterlagen nehmen muss, um Namen und Adresse des Websitebetreibers mit der Domain zu verbinden. Anders ist dies etwa bei Filesharing-Sachverhalten, wo zunächst die IP-Adresse des Internetusers verarbeitet werden muss,

¹¹² „Elektronische Kommunikationsdienste“ sind gem Art 2 lit c Rahmen-RL gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben.

¹¹³ Vgl ErwGr 5 der Rahmen-RL.

¹¹⁴ Vgl ErwGr 10 der Rahmen-RL.

¹¹⁵ „Personenbezogene Daten“ sind gem Art 2 lit a Datenschutz-RL alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

¹¹⁶ Diese sind nur im nationalen Recht, nämlich in § 92 Abs 3 Z 3 TKG definiert: alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Darunter fallen insb auch Name und Adresse.

¹¹⁷ „Verkehrsdaten“ sind gem Art 2 lit b Telekom-Datenschutz-RL Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

um über die Log-Dateien des Access-Providers die gesuchte Identität zu ermitteln. Da IP-Adressen nach hA Verkehrsdaten sind, ist dabei ist nach der Rsp auch das erhöhte Schutzniveau für die Verarbeitung von Verkehrsdaten, wie es die Telekom-Datenschutz-RL vorsieht, einzuhalten.¹¹⁸

Daten wie Name und Adresse als „Informationen über eine bestimmte oder bestimmbare natürliche Person“ fallen nach unionsrechtlicher Terminologie unter die Kategorie der „personenbezogenen Daten“, wie sie in Art 2 lit a Datenschutz-RL definiert sind. Wenn diese Daten an Dritte weitergeben werden, etwa im Rahmen einer Auskunft, werden sie dadurch verarbeitet.¹¹⁹

Solche Verarbeitungen von personenbezogenen Daten dürfen in den nationalen Rechtsordnungen der Mitgliedstaaten nur im Rahmen der Art 6 und 7 Datenschutz-RL gestattet werden. Nach Art 7 lit f Datenschutz-RL ist die Verarbeitung ua dann zulässig, wenn sie zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Weiters dürfen die Rechte und Pflichten nach Art 6 Abs 1 Datenschutz-RL, die die Zulässigkeit der Verarbeitung regeln, gem Art 13 Abs 1 lit g Datenschutz-RL abgewichen werden, wenn die Beschränkung notwendig ist für den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

Nach der Rsp des EuGH ergibt diese Interessensabwägung, dass die Datenschutzbestimmungen des Unionsrechts in Situationen, in denen sich die Urheber im Rahmen eines zivilrechtlichen Verfahrens um diesen Schutz bemühen, einer Auskunftspflicht nicht entgegenstehen.¹²⁰ Einer Auskunftspflicht für Host-Provider über personenbezogene Daten ihrer Kunden aufgrund von Immaterialgüterrechtsverletzungen steht daher unionsrechtlich nichts im Wege.¹²¹

¹¹⁸ Dazu ausführlich unten S 134 f.

¹¹⁹ Art 2 lit b Datenschutz-RL: "Verarbeitung personenbezogener Daten" ("Verarbeitung") jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.

¹²⁰ Vgl EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 53; der EuGH hatte im Anlassfall die Telekom-Datenschutz-RL auszulegen, bezog sich dabei aber ausdrücklich auf die zitierte Bestimmung der Datenschutz-RL.

¹²¹ Dieses Ergebnis ist auch wertungsmäßig vertretbar, weil nach der Rsp des EuGH sogar die Verarbeitung von Verkehrsdaten für Auskunftszwecke gestattet ist (siehe unten S 129 f.). Umso mehr muss dies für weniger sensible, sonstige personenbezogene Daten (nach österreichischer Terminologie: „Stammdaten“) gelten.

C.I.3.c. Nationale Rechtslage

Eine Auskunftspflicht für Host-Provider wurde in § 18 Abs 4 ECG expressis verbis im österreichischen Recht verankert. Mangels höchstgerichtlicher Rsp zu ihrem direkten Anwendungsgebiet wurde bisher primär ihre analoge Anwendbarkeit diskutiert.

C.I.3.c.1. § 18 Abs 4 ECG

§ 18. (4) Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

§ 18 Abs 4 ECG bezieht sich auf die in § 16 ECG angesprochenen Host-Provider, und zwar – anders als § 18 Abs 1 und Abs 2 ECG - nur auf diese. Die Bestimmung soll nach den Materialien¹²² „Personen, die durch rechtswidrige Tätigkeiten oder Informationen eines ihnen nicht bekannten Nutzers in ihren Rechten verletzt werden, und Verbänden oder Gesellschaften, die sich der Wahrung der Rechte bestimmter anderer Personen widmen (etwa Verbraucherverbänden oder Verwertungsgesellschaften), die Rechtsverfolgung [erleichtern].“ Zwar ist ein derartiger Anspruch in der E-Commerce-RL nicht vorgesehen, er widerspricht aber – wie oben erörtert – nicht dem Unionsrecht und auch nicht dem „Geist der Richtlinie“ (vgl dazu ErwGr 47 der E-Commerce-RL).¹²³

Zu beachten ist weiters, dass der Anspruch als Teil des koordinierten Bereichs (§ 3 Z 8 ECG) nur gegen Provider im Anwendungsbereich des österreichischen ECG gerichtet werden kann, was Provider mit Sitz in Österreich und solche mit Sitz in Nicht-EWR-Staaten umfasst, wobei bei letzteren nach allgemeinen Anknüpfungsregeln österreichisches Recht anwendbar sein muss. Host-Provider mit Sitz im Binnenmarkt unterliegen dagegen dem Herkunftslandprinzip (§ 20 Abs 1 ECG) und damit nur den Regeln in ihrem jeweiligen Sitzstaat.¹²⁴ Innerhalb des Anwendungsbereiches des ECG ist ein Auskunftsbegehren dafür gem § 19 Abs 2 ECG auch gegenüber Host-Providern möglich, die unentgeltlich elektronische Dienste bereitstellen, und damit gem § 3 Z 1 ECG eigentlich vom Anwendungsbereich des ECG insgesamt ausgenommen wären.

So der betroffene Rechteinhaber im Fall einer rechtsverletzenden Website darlegen kann, dass er ein überwiegendes rechtliches Interesse an der Feststellung der Identität des Nutzers

¹²² ErlRV 817 BlgNR XXI. GP 39.

¹²³ ErlRV 817 BlgNR XXI. GP 40.

¹²⁴ Vgl Zankl, E-Commerce-Gesetz Rz 228.

von Hosting-Diensten hat und den rechtswidrigen Sachverhalt durch einen Nachweis, etwa einen Link zur jeweiligen Seite und entsprechende Dokumentation seines Rechtsanspruchs, bescheinigt, wird der jeweilige Host-Provider seiner Auskunftspflicht nachkommen und die Identität des jeweiligen Websitebetreibers offen legen. Die Frage, wann genau ein Host-Provider einen rechtsverletzenden Sachverhalt als bescheinigt anzusehen hat, kann in der Praxis Schwierigkeiten bereiten. Zur Lösung dieses Problems wird in den Materialien eine Parallele zu § 16 ECG gezogen und auf die Fähigkeiten und das Wissen eines juristischen Laien abgestellt. Wenn auch für diesen eine Rechtsverletzung offenkundig sei, stehe einer Herausgabe der verlangten Daten nichts im Wege.¹²⁵

Die begehrte Information muss für den Rechteinhaber schließlich eine wesentliche Voraussetzung für die Rechtsverfolgung bilden. Bei Websites, deren Betreiber seine Informationspflichten nicht erfüllt und deren Whois-Informationen ebenfalls keine Abhilfe schaffen, wird diese Voraussetzung aber idR erfüllt sein – schließlich ist zur Rechtsdurchsetzung die Kenntnis von der Identität des Rechtsverletzers nicht nur eine wesentliche, sondern eine zwingend notwendige Voraussetzung.¹²⁶ Dennoch ist die Prüfungsschwelle des § 18 Abs 4 ECG höher als bei anderen Auskunftsansprüchen (vgl etwa § 87b Abs 3 UrhG und § 55a MSchG), insb weil er den Nachweis eines überwiegenden rechtlichen Interesses erfordert.¹²⁷

Der Host-Provider hat dem Rechteinhaber lediglich Name und Adresse, somit Stammdaten, zu übermitteln. Weitergehende Informationen (die Materialien sprechen zB von Userprofilen) hat der Provider nicht herauszugeben, ebenso wenig verpflichtet ihn die Auskunftspflicht des § 18 Abs 4 ECG zur Speicherung bestimmter Daten.¹²⁸ Datenschutzrechtlich ist die Herausgabe von Stammdaten in diesem Zusammenhang durch § 8 Abs 1 Z 4 DSGVO gedeckt, weil überwiegende berechnete Interessen eines Dritten die Verwendung erfordern und somit keine schutzwürdigen Geheimhaltungsinteressen verletzt werden.

C.I.3.c.1.1. Kritik

§ 18 Abs 4 ECG und seine aus Sicht der Auskunftssuchenden einschränkende Erläuterung in den Materialien wurden von *Stomper* kritisiert.¹²⁹ Da die E-Commerce-RL Datenschutzregelungen nicht berühre, sei bei richtlinienkonformer Interpretation ausschließlich auf die in den §§ 7 f DSGVO normierten Grundsätze zurückzugreifen, die bereits eine Interessenabwägung

¹²⁵ ErlRV 817 BlgNR XXI. GP 40; zust *Hasberger*, Glosse zu 4 Ob 66/04f, MR 2004, 274 (277); diese Ansicht wurde insb von *Stomper* kritisiert, dazu sogleich.

¹²⁶ In diesem Sinn daher auch der Standpunkt der Interessensvertretung der Internetprovider (ISPA), die empfiehlt, die Auskunft bei Erfüllung der sonstigen Voraussetzungen zu erteilen; abrufbar unter <ispa.at/know-how/positions-papiere/beauskunftung-von-ip-adressen/>.

¹²⁷ *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25 (27).

¹²⁸ ErlRV 817 BlgNR XXI. GP 40.

¹²⁹ *Stomper*, Die Folgen der Megasex-Entscheidung, RdW 2005, 284 (285 f).

zwischen Auskunftsanspruch und Datenschutzinteresse regelten. Die in den EB zu § 18 Abs 4 ECG argumentierte Einschränkung der Auskunftspflicht auf nur für juristische Laien offenkundig rechtswidrige Sachverhalte widerspreche den §§ 7 f DSG und sei auch nicht sachgerecht, weil es hier nicht um die Mitverantwortlichkeit von Host-Providern, sondern lediglich um eine Auskunftspflicht über nicht-sensible Daten gehe.

Während *Stomper* mit ihrem Argument Recht hat, dass die E-Commerce-RL Datenschutzbelange unberührt lässt (das österreichische Recht vollzieht diese Einschränkung in § 2 ECG auch nach), ist ihre darauf basierende Schlussfolgerung bedenklich. Gerade weil das ECG Belange des Datenschutzes unberührt lässt, ist strikt nach dem Prüfschema des § 7 Abs 2 DSG vorzugehen:

Daten dürfen daher erstens nur übermittelt werden, wenn sie aus einer gemäß § 7 Abs 1 DSG zulässigen Datenanwendung stammen, was bei Speicherung von vertraglichen Kundendaten im Betrieb eines Host-Providers zweifellos gegeben ist. Entscheidend ist der zweite Schritt: Der Empfänger hat dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft zu machen. Im hier behandelten Fall kann der potentielle Datenempfänger diese rechtliche Befugnis im Hinblick auf den Übermittlungszweck, nämlich die Durchsetzung zivilrechtlicher Ansprüche, nur aus § 18 Abs 4 ECG ziehen. Folglich sind auch dessen Tatbestandselemente in die Prüfung aufzunehmen, weil nur so feststellbar ist, ob die rechtliche Befugnis zum Datenerhalt überhaupt besteht. Wenn daher in § 18 Abs 4 ECG der Auskunftswerber ihm Rahmen seines Auskunftsbegehrens sein überwiegendes rechtliches Interesse an der „Feststellung eines bestimmten rechtswidrigen Sachverhalts“ glaubhaft zu machen hat, muss er als logische Vorbedingung erst einmal nachweisen, dass es überhaupt einen bestimmten rechtswidrigen Sachverhalt gibt. Hier ist der in den Materialien vorgeschlagene Maßstab anzulegen, der den Host-Provider davor bewahrt, diffizilen juristischen Fragestellungen (zB ob AGB auf einer bestimmten Website gegen das Transparenzgebot des Konsumentenschutzrechts verstoßen) nachgehen zu müssen. Bei offensichtlichen Rechtsverletzungen (zB einem fehlenden Impressum) kann der Host-Provider dagegen rasch und ohne großen Prüfungsaufwand reagieren und die fragliche Auskunft erteilen, ohne dass seine Prüfpflicht¹³⁰ überspannt wird. Im dritten Schritt von § 7 Abs 2 DSG ist dann nur mehr zu prüfen, ob durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Da § 8 Abs 1 Z 4 DSG explizit anordnet, dass die Verwendung von nicht-sensiblen Daten bei überwiegenden berechtigten Interessen eines

¹³⁰ Diese darf gem § 18 Abs 1 ECG nicht derart ausgestaltet werden, dass der Diensteanbieter (Host-Provider) verpflichtet würde, die von ihm gespeicherten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

Dritten keine derartigen schutzwürdigen Geheimhaltungsinteressen verletzen, ist auch diese letzte Voraussetzung im vorliegenden Fall grds zu bejahen.

Eine (auskunftsfreundliche) richtlinienkonforme Interpretation von § 18 Abs 4 ECG im Sinne *Stompers* ist dagegen nicht möglich, weil die E-Commerce-RL es erstens dem nationalen Gesetzgeber überlässt, ob er einen Auskunftsanspruch gegen Host-Provider vorsieht oder nicht – dem Unionsrecht kann daher keine generelle Tendenz in die eine oder andere Richtung unterstellt werden. Die vom österreichischen Gesetzgeber autonom formulierte Anspruchsgrundlage in § 18 Abs 4 ECG lässt zweitens – wie von der RL gefordert – Datenschutzbelange unberührt, weil sie in die Prüfungsabfolge von § 7 Abs 2 DSGVO ohne weiteres eingeordnet werden kann und diese weder erweitert noch einschränkt. Die Schlussfolgerung *Stompers*, dass Auskünfte nach § 18 Abs 4 ECG unabhängig von der Offenkundigkeit der Rechtsverletzung zu erteilen sind, würde die Prüf- und Nachforschungspflicht des Host-Providers dagegen über das zulässige Maß hinaus erweitern und somit insb § 18 Abs 1 ECG widersprechen. Auch *Zankl* plädiert in diesem Zusammenhang dafür, von einer Subsidiarität der Auskunftspflicht auszugehen, die nur dann besteht, wenn mit Informationen auf der Website nicht das Auslangen zu finden ist bzw diese falsch sind.¹³¹

C.I.3.c.1.2. Systematische Einordnung

Die wirksame, wenn auch vorsichtige Ausgestaltung des Auskunftsanspruches gegenüber Host-Providern im österreichischen Recht ist im Zusammenhang mit § 18 Abs 1 ECG zu sehen. Dieser sieht vor, dass die in den §§ 13 bis 17 genannten Diensteanbieter (Access und Host-Provider, Suchmaschinenbetreiber, Linksetzer) nicht verpflichtet sind, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen. Unter diesen genannten Diensteanbietern ist nur der Host-Provider verpflichtet, Daten über seine Kunden auf Verlangen an private Dritte oder Verwaltungsbehörden weiterzugeben (§ 18 Abs 3 und 4 ECG). Andere Diensteanbieter, inbs Access-Provider, müssen Daten ihrer Kunden nur auf gerichtlichen Befehl und nur zum Zweck der Strafverfolgung herausgeben (§ 18 Abs 2 ECG). Die Begründung dafür, wie *Wiebe* festhält, liegt erstens darin, dass die funktional bedingte Beteiligung (Speicherung fremder Inhalte) von Host-Providern gegenüber der rein durchleitenden Tätigkeit der Access-Provider größer ist. Zweitens haben Host-Provider aufgrund ihrer Vertragsbeziehung Daten über die Identität des Kunden (Stammdaten) gespeichert, so dass auch keine aktive Überwachung oder Datenerhebung erforderlich ist.¹³² Access-Provider müssen dagegen sensible Verkehrsdaten (IP-Adressen), die in ihren Log-Files gespeichert sind, mit den Daten ihrer Kunden verknüpfen und somit ver-

¹³¹ Zankl, E-Commerce-Gesetz Rz 283 f.

¹³² Vgl *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 7.

arbeiten, um an die notwendigen Auskunftsdaten zu kommen. Dementsprechend höher muss die Seriösitätsschwelle beim Auskunftsempfänger (staatliches Gericht) liegen. Bei der Einführung von Auskunftspflichten für Access-Provider außerhalb des ECG (insb § 87b Abs 3 UrhG) wurde dieses fein austarierte System durchbrochen. Die dadurch entstehenden datenschutzrechtlichen Auswirkungen wurden nicht ausreichend bedacht, worin der Kern des späteren Problems mit derartigen Auskunftspflichten liegt.¹³³

C.I.3.c.1.3. Analoge Anwendung

Der Auskunftsanspruch des § 18 Abs 4 ECG wurde in der Rsp als Analogiegrundlage für Sachverhalte außerhalb des ECG herangezogen. Ein Telekommunikationsunternehmen, das ein öffentliches Kommunikationsnetz betreibt, hat in analoger Anwendung des § 18 Abs 4 ECG den Namen und die Adresse eines Nutzers, der auf Grund einer Vereinbarung über dieses Netz Mehrwertdienste anbietet, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben sowie überdies glaubhaft machen, dass die Kenntnis dieser Information eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.¹³⁴

Diese Entscheidung wurde von *Zankl* und *Hasberger/Schönhart* kritisiert, zum einen weil das TKG 2003 gar nicht lückenhaft sei und eine Analogie daher nicht in Frage komme, zum anderen weil das ECG nur auf Dienste der Informationsgesellschaft und somit nicht auf Sprachtelefonie Anwendung finde. Wenn überhaupt, dann müsse ein Telekommunikationsunternehmen im System des ECG wie ein Access-Provider behandelt werden.¹³⁵ *Plasser* hielt dem wiederum entgegen, dass das ECG zwar nicht direkt auf Sprachtelefonie anwendbar ist, eine allfällige analoge Anwendbarkeit dadurch aber nicht ausgeschlossen sei. Weiters sei das TKG 2003 sehr wohl lückenhaft, weil die von *Zankl* und *Hasberger/Schönhart* dagegen ins Treffen geführte Bestimmung § 24 Abs 3 TKG nicht ausreiche.¹³⁶

Zwischenzeitlich wurde das UWG novelliert und eine gesonderte Auskunftsbestimmung in § 14a UWG eingeführt. Klagslegitimiert sind aber nur die in § 14 Abs 1 UWG genannten Einrichtungen (Wirtschaftskammer Österreich, Arbeiterkammer etc) und der Schutzverband gegen unlauteren Wettbewerb. Wie auch *Plasser* selbst einräumt, könnte diese Einschränkung auf einige wenige klagslegitimierte Einrichtungen als bewusste Entscheidung des Ge-

¹³³ Siehe dazu ausführlich unten die Ausführungen zum Filesharing-Problem auf S 120 f.

¹³⁴ OGH 16.03.2004, 4 Ob 7/04i.

¹³⁵ *Zankl*, Auskunftspflicht für Mehrwertdienste?, *ecolex* 2004, 853 (854); *Hasberger/Schönhart*, Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, *MR* 2004, 297 (300).

¹³⁶ *Plasser*, Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007?, *ÖBl* 2008/40 (184 f).

setzgebers gegen eine Auskunftspflicht für Mitbewerber gewertet werden.¹³⁷ Eine Analogieschluss mittels § 18 Abs 4 ECG wäre damit versperrt. Bisher wurde der OGH mit dieser Frage aber nicht erneut befasst.

C.I.3.d. Ergebnis

Ein zivilrechtlicher Auskunftsanspruch gegen Host-Provider, den auch Private zur Durchsetzung ihrer Rechte gegen den Betreiber einer Website in Anspruch nehmen können, ist im Unionsrecht weder vorgesehen noch untersagt. Im österreichischen Recht liefert § 18 Abs 4 ECG eine passende Anspruchsgrundlage, die zwar nur unter einschränkenden Bedingungen den Zugriff auf die Daten der potentiellen Rechtsverletzer ermöglicht, in den typischen Fällen innerhalb Österreichs aber ausreichend ist.

C.II. Unterbindung der Verletzungshandlung

Der für das Immaterialgüterrecht typische Unterlassungsanspruch bildet das zentrale Sanktionsmittel für Rechteinhaber, um Rechtsverletzungen auf Websites zu unterbinden. Abgesehen von Unterlassungsansprüchen gegen den unmittelbaren Verletzer, also den Betreiber einer Website, werden auch derartige Ansprüche gegen Internetprovider diskutiert.

C.II.1. Anspruch auf Unterlassung

Rechtsgrundlagen: § 81 UrhG; § 51 MSchG

C.II.1.a. Grundsätze

Da dieser Anspruch das für das Immaterialgüterrecht typische *ius excludendi* widerspiegelt, ist er auch der in der Praxis bedeutendste Behelf zur Abwehr von Immaterialgüterrechtsverletzungen. Europarechtlich ist durch Art 11 Enforcement-RL klargestellt, dass alle Mitgliedsstaaten in ihrem nationalen Recht sicherzustellen haben, dass die zuständigen Gerichte bei Feststellung einer Verletzung eines Rechts des geistigen Eigentums eine Anordnung gegen den Verletzer erlassen können, die ihm die weitere Verletzung des betreffenden Rechts untersagt. Für Österreich hat sich daraus aber kein weiterer Umsetzungsbedarf ergeben, weil ein derartiger Unterlassungsanspruch seit jeher Kernpunkt aller immaterialgüterrechtlichen Gesetze ist.

Der Unterlassungsanspruch steht neben dem Rechteinhaber auch dem Inhaber exklusiver Rechte, etwa im Urheberrecht dem Inhaber einer Werknutzungsberechtigung, zu.¹³⁸ Er wird durch zwei Elemente konkretisiert: Eine Unterlassungspflicht und die Gefahr, dass dieser

¹³⁷ *Plasser*, Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007?, ÖBl 2008/40 (184 f).

¹³⁸ *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 163.

Unterlassungspflicht zuwidergehandelt wird. Fehlt eines dieser Elemente, dann besteht nach stRsp kein Unterlassungsanspruch.¹³⁹

Da sich die Unterlassungspflicht bei Verletzungen von Immaterialgüterrechten unmittelbar aus dem gesetzlichen *ius excludendi* ergibt, ist die entscheidende materiellrechtliche Voraussetzung für jeden Unterlassungsanspruch daher das Vorliegen von Wiederholungsgefahr.

Da er nicht früheres Fehlverhalten sanktionieren, sondern zukünftige Rechtsverletzungen verhindern soll, wäre die Gewährung eines Unterlassungsanspruches nämlich sinnlos, wenn der Verletzer ohnehin keine weiteren Rechtsverletzungen im Sinn hätte. Bei der Beurteilung der Wiederholungsgefahr kommt es nicht nur auf die Art des bereits erfolgten Eingriffs, sondern auch auf die Willensrichtung des Täters an, für die insbesondere sein Verhalten nach der Beanstandung oder während des Rechtsstreites wichtige Anhaltspunkte bieten kann.¹⁴⁰ Die Wiederholungsgefahr wird nach einer ersten Rechtsverletzung vermutet, weil von einem Rechtsverletzer angenommen wird, dass er auch zu neuerlichen Rechtsverletzungen geneigt ist.¹⁴¹ Um diese Vermutung zu widerlegen, hat der Beklagte nach stRsp besondere Umstände darzutun, die eine Wiederholung seiner Handlung als völlig ausgeschlossen oder doch zumindest äußerst unwahrscheinlich erscheinen lassen.¹⁴² Dies kann er idR dadurch erreichen, dass er dem Kläger einen vollstreckbaren Unterlassungsvergleich anbietet.¹⁴³ Der darauf folgende Wegfall der Wiederholungsgefahr ist auch im Provisorialverfahren zu berücksichtigen.¹⁴⁴ Hingegen ist das bloße Abstellen der Rechtsverletzung, auch verbunden mit der Bekundung, sie in Hinkunft unterlassen zu wollen, nicht ausreichend.¹⁴⁵

Soweit im materiellen Recht vorgesehen, besteht auch die Möglichkeit eines vorbeugenden Unterlassungsanspruches.¹⁴⁶ Für das Immaterialgüterrecht ergibt sich direkt aus der gesetzlichen Formulierung in § 81 Abs 1 UrhG und § 51 Abs 1 MSchG, dass bereits bei einer drohenden Rechtsverletzung auf Unterlassung geklagt werden kann (arg „wer... eine solche Verletzung zu besorgen hat, kann auf Unterlassung klagen“).¹⁴⁷ Voraussetzung ist dabei, dass ein unmittelbar drohender Eingriff in ein Ausschließungsrecht vorliegt oder zumindest ausrei-

¹³⁹ RIS-Justiz RS0037660.

¹⁴⁰ RIS-Justiz RS0079692

¹⁴¹ *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 164.

¹⁴² RIS-Justiz RS0012056.

¹⁴³ RIS-Justiz RS0079899; idR wird der Beklagte dem Kläger dazu nicht nur eine Unterlassungsverpflichtung, sondern auch die Ermächtigung zur Veröffentlichung des abzuschließenden Vergleiches auf seine Kosten in angemessenem Umfang anbieten müssen, vgl dazu RIS-Justiz RS0079921.

¹⁴⁴ OGH 29.01.1991, 4 Ob 176/90.

¹⁴⁵ RIS-Justiz RS0012056.

¹⁴⁶ Vgl RIS-Justiz RS0010540.

¹⁴⁷ Vgl *Gamerith*, Der vorbeugende Unterlassungsanspruch, ÖBl 2005/13; OGH 24.03.2009, 4 Ob 19/09m.

chende Anhaltspunkte in dieser Richtung bestehen.¹⁴⁸ Der Maßstab für den Wegfall dieser Erstbegehungsgefahr ist nach stRsp weniger streng als bei der Wiederholungsgefahr, weil noch keine rechtsverletzende Handlung gesetzt wurde, die nicht mehr ungeschehen gemacht werden kann.¹⁴⁹

Da eine zu enge Fassung des Unterlassungsbegehrens (und damit des stattgebenden Urteils) dazu führen kann, dass eine Variation des inkriminierten Verhaltens nicht von der Unterlassungsverpflichtung umfasst ist, kann nicht alleine auf die konkrete Verletzungshandlung abgestellt werden. Vielmehr muss das Begehren ausreichend weit gefasst werden, um dem Rechtsverletzer die Umgehung möglichst schwierig zu machen. Andererseits darf eine Unterlassungspflicht nicht zu unbestimmt sein, weil dann keinen tauglichen Exekutionstitel iS von § 7 EO vorliegt¹⁵⁰; sie muss dem Verpflichteten durch ausreichend deutliches Umschreiben des Verbotes als Richtschnur für sein künftiges Verhalten dienen können.¹⁵¹ Durch dieses Spannungsfeld ist die präzise und zielführende Formulierung des Unterlassungsbegehrens in der Praxis durchaus herausfordernd.

Prozessual wird der Unterlassungsanspruch durch vom Exekutionsgericht auf Antrag gem § 355 EO zu verhängende Beugegeldstrafen von bis zu € 100.000 pro Verstoß gegen die Unterlassungsverpflichtung durchgesetzt. Bei wiederholten Verstößen kann alternativ zur Verhängung einer weiteren Geldstrafe auch Beugehaft angeordnet werden. Die Strafen sind nach Art und Schwere des jeweiligen Zuwiderhandelns, unter Bedachtnahme auf die wirtschaftliche Leistungsfähigkeit des Verpflichteten und das Ausmaß der Beteiligung an der Zuwiderhandlung auszumessen; Haftstrafen dürfen je Antrag zwei Monate und insgesamt ein Jahr nicht übersteigen (§ 355 Abs 1 EO iVm § 366 EO).¹⁵²

Voraussetzung für die Verhängung von Strafen ist, dass den Verpflichteten ein Verschulden an der Zuwiderhandlung trifft. Einen entsprechenden Einwand hat der Verpflichtete mittels Impugnationsklage geltend zu machen.¹⁵³ In der Praxis problematisch ist, dass die zur Unterlassung Verpflichteten durch Anträge auf Exekutionsaufschiebung die Erzwingung titelkonformen Verhaltens verschleppen können, obwohl gem 56 Abs 3 MSchG und § 87c Abs 3 UrhG eine gesetzliche Gefährdungsvermutung zugunsten der Rechteinhaber besteht.¹⁵⁴

¹⁴⁸ Vgl *Ofner* in Kucsko, urheber.recht § 81 Pkt 2.1. mwN.

¹⁴⁹ Vgl RIS-Justiz RS0079944.

¹⁵⁰ Vgl RIS-Justiz RS0000771.

¹⁵¹ Vgl RIS-Justiz RS0119807.

¹⁵² Dazu *Burgstaller*, Beugestrafen zur Durchsetzung von Zivilurteilen, ÖJZ 2000, 134.

¹⁵³ Vgl *Rechberger/Oberhammer*, Exekutionsrecht⁴ Rz 443 ff; nach stRsp (vgl RIS-Justiz RS0000793) kann der Verpflichtete mittels Impugnationsklage geltend machen, er habe dem Exekutionstitel überhaupt nicht zuwider gehandelt oder es treffe ihn kein Verschulden.

¹⁵⁴ Dazu *Schultes*, Die aufschiebende Wirkung bei Unterlassungsansprüchen, *ecolex* 2009, 686 f.

C.II.1.a.1. Grundsätze der Gehilfenhaftung

Im Immaterialgüterrecht ist ebenso wie im Wettbewerbsrecht für gesetzwidrige Handlungen Dritter in wesentlich weiterem Umfang einzustehen als nach allgemeinem Zivilrecht. Die Art der Beteiligung an einer Rechtsverletzung ist hier zudem von größerer Bedeutung als dort, wie schon *Griss* festhielt, weil nicht der Ausgleich bereits entstandenen Schadens, sondern die Abwehr künftigen rechtswidrigen Verhaltens durch den verschuldensunabhängigen Unterlassungsanspruch im Vordergrund steht.¹⁵⁵

Der immaterialgüterrechtliche Unterlassungsanspruch richtet sich nicht nur gegen den unmittelbaren Täter (Störer), also gegen jene Person, von der die Beeinträchtigung ausgeht und auf deren maßgeblichem Willen sie beruht, sondern auch gegen Mittäter, Anstifter und Gehilfen des eigentlichen Störers.¹⁵⁶ Da weder im UWG noch in immaterialgüterrechtlichen Sondergesetzen definiert wird, wer Täter ist, wird die Gehilfenhaftung dogmatisch aus § 1301 ABGB, ergänzend auch aus § 12 StGB und § 7 VStG abgeleitet.¹⁵⁷ Während daher der Unterlassungsanspruch gegenüber dem unmittelbaren Täter verschuldensunabhängig ist, ist auf Seiten des Gehilfen jedenfalls Verschulden erforderlich. Fraglich ist, welcher Verschuldensgrad dabei gefordert wird.

Die bloße adäquate (insb fahrlässige) Verursachung einer Rechtsverletzung reichte nach der älteren Rsp jedenfalls noch nicht für das Bestehen einer Haftung.¹⁵⁸ Wollte man nämlich jeden, der die Verletzungshandlung (oder einen Schaden) in irgendeiner Weise adäquat verursacht hat, als Täter ansehen, dann wären die Begriffe des Gehilfen oder Anstifters überflüssig; diese Personen müssten vielmehr - unabhängig von einem etwaigen Vorsatz - immer als Täter haften. Das widerspräche aber dem in der österreichischen Rsp und Lehre entwickelten Begriff des Täters (Störers) als desjenigen, von dem die Beeinträchtigung ausgeht und auf dessen maßgeblichen Willen sie beruht. Die früher vertretene gegenteilige Auffassung¹⁵⁹ - es reiche aus, dass zwischen dem Verhalten und der Rechtsverletzung ein adäquater Kausalzusammenhang besteht - wird von der nunmehr herrschenden Rsp¹⁶⁰ ausdrücklich abgelehnt: Dem österreichischen Recht sei eine „mittelbare Urheberrechtsverletzung“ (ebenso wie eine mittelbare Markenrechts- oder Patentverletzung), wonach beim Gehilfen in subjektiver Hinsicht Fahrlässigkeit anstelle des Vorsatzes genügt, unbekannt. Wer nicht tatbestandsmäßig handelt, sondern nur einen sonstigen Tatbeitrag leistet, hafte daher nur dann, wenn er den

¹⁵⁵ *Griss*, Haftung für Dritte im Wettbewerbsrecht und im allgemeinen Zivilrecht, JBl 2005, 69 (73).

¹⁵⁶ Vgl RIS-Justiz RS0077265.

¹⁵⁷ Vgl *Griss*, Haftung für Dritte im Wettbewerbsrecht und im allgemeinen Zivilrecht, JBl 2005, 69 (73) mwN.

¹⁵⁸ Vgl OGH 19. 9. 1994, 4 Ob 97/94 (Telefonstudien); RIS-Justiz RS0026577.

¹⁵⁹ So insb OGH 28.05.1991, 4 Ob 19/91 (Tele UNO III); vgl RIS-Justiz RS0077158.

¹⁶⁰ OGH 04.07.2000, 4 Ob 173/00w mwN.

Täter bewusst fördert.¹⁶¹ Zwischenzeitlich wurde durch die PatG-Novelle 2004 (BGBl I 149/2004) freilich das Institut der „mittelbaren Patentverletzung“ gesetzlich verankert (§ 22 Abs 3 bis 5 PatG) und der Störerbegriff erweitert.¹⁶²

Für das Bestehen einer bewussten Förderung, die in den übrigen Materiengesetzen weiterhin Voraussetzung ist, wurde idR verlangt, dass dem in Anspruch Genommenen die Tatumstände bekannt sind, die den Gesetzesverstoß begründen¹⁶³, was für das Erfordernis eines qualifizierten Vorsatzes (Wissentlichkeit) spricht.¹⁶⁴ Vertreten wurde aber auch, dass es ausreiche, wenn der Gehilfe den Rechtsbruch des Dritten zumindest in Kauf nimmt (bedingter Vorsatz).¹⁶⁵

Zur Illustration dieses Konzepts kann die Entscheidung „Telefonstudien“¹⁶⁶ dienen. Der Auftraggeber eines Fotografen sollte das vom Fotografen angefertigte Lichtbild vereinbarungsgemäß nur für eine Präsentationsmappe verwenden. Er gab dennoch einen Abzug an den Veranstalter eines Wettbewerbs weiter; dieser überließ einen Abzug des Fotos einer Zeitung für einen Bericht über den Wettbewerb, ohne Rücksprache mit dem Auftraggeber oder Fotografen zu halten. Der Fotograf klagte seinen Auftraggeber auf Unterlassung, obwohl dieser an der Verbreitung und Vervielfältigung des Fotos in der Zeitung und der damit bewirkten Urheberrechtsverletzung nicht unmittelbar beteiligt war. Der Beklagte war somit zwar nicht unmittelbarer Täter, er hatte aber durch die Weitergabe des Bildes eine Bedingung für die spätere Veröffentlichung verwirklicht, „deren Adäquanz für die Rechtsverletzung jedenfalls nicht von vornherein zu verneinen war“.¹⁶⁷ Eine bewusste Förderung des Täters im oben dargestellten Sinn war ihm aber mangels Vorsatz nicht vorzuwerfen, weswegen er nicht zur Unterlassung verpflichtet wurde.

Abweichend von diesem Konzept gibt es jüngere Rsp, wonach dem Kennen der den Gesetzesverstoß begründenden Tatumstände das vorwerfbare Nichtkennen gleichzuhalten ist.¹⁶⁸ Im

¹⁶¹ Zur Entwicklung dieser Rsp vgl auch *Parschalk*, Provider-Haftung für Urheberrechtsverletzungen Dritter, *ecolex* 1999, 834 f.

¹⁶² Vgl ErlRV 621 BlgNR XXII. GP 5 f.

¹⁶³ OGH 29.01.2002, 4 Ob 279/01k mwN.

¹⁶⁴ Vgl § 5 Abs 3 StGB: „Der Täter handelt wissentlich, wenn er den Umstand oder Erfolg (...) nicht bloß für möglich hält, sondern sein Vorliegen oder Eintreten für gewiss hält.“ *Walter*, *UrhGNov* 2003 § 81 *UrhG* 140, spricht von „vorsätzlichem Handeln im Bewusstsein der Rechtswidrigkeit.“

¹⁶⁵ Vgl RIS-Justiz RS0031329; unter Hinweis auf § 1301 ABGB ebenfalls für das Ausreichen von *dolus eventualis* *Parschalk*, Provider-Haftung für Urheberrechtsverletzungen Dritter, *ecolex* 1999, 834 (835); dem offenb folgend *Wiebe*, Auskunftspflichtung der Access Provider, *MR* 2005 Beilage H 4, 3.

¹⁶⁶ OGH 19. 9. 1994, 4 Ob 97/94 (Telefonstudien).

¹⁶⁷ *Griss*, Haftung für Dritte im Wettbewerbsrecht und im allgemeinen Zivilrecht, *JBl* 2005, 69 (78).

¹⁶⁸ OGH 16.12.2003, 4 Ob 221/03h (Weinatlas); vgl *Wiebe*, Auskunftspflichtung der Access Provider, *MR* 2005 Beilage H 4, 5, der diese Rsp als „unklar“ bezeichnet.

Ergebnis bedeutet dies, dass eine Haftung auch dann eintritt, wenn die rechtswidrigen Tatsachen zwar nicht bekannt sind, bei Einhaltung der objektiv gebotenen Sorgfalt aber erkennbar wären, und dennoch der entsprechende Beitrag gesetzt wird. Damit ist der OGH wohl vom lange vertretenen Konzept der reinen Vorsatzhaftung für Gehilfen abgegangen und hat de facto eine Prüfpflicht auf Seiten der mittelbar an Rechtsverletzungen beteiligten Gehilfen eingeführt. Das Ausmaß dieser Prüfpflicht hatte der OGH dann vor allem in den Entscheidungen zu Host-Providern wiederholt zu beurteilen.

C.II.1.b. Gegen den Betreiber und Nutzer einer Website

Diese Grundsätze gelten - mit den notwendigen Anpassungen - auch für Internetsachverhalte, insbesondere auch gegenüber Betreiber (eigener) rechtsverletzender Websites sowie Nutzern, die rechtswidrige Inhalte auf Websites Dritter laden. Sie sind als Content-Provider für die Inhalte, die auf ihrer Website abrufbar sind bzw von ihnen auf fremde Websites gestellt werden, als unmittelbare Täter uneingeschränkt verantwortlich.¹⁶⁹

Das Bestehen von Wiederholungsgefahr kann der unmittelbare Täter nicht schon dadurch beseitigen, dass er die urheber- bzw markenrechtlich geschützten Inhalte entfernt. Diese Löschung kann als bloß technischer Vorgang jederzeit leicht wieder rückgängig gemacht werden.¹⁷⁰ Nach allgemeinen Grundsätzen müsste der Betreiber bzw User vielmehr einen vollstreckbaren Unterlassungsvergleich anbieten, um die Wiederholungsgefahr wegfallen zu lassen. Dabei ist zu beachten, dass ein solches Angebot idR auch eine angemessene Veröffentlichung des geschlossenen Vergleichs zu enthalten hat.¹⁷¹ Wenn der Kläger auf die Veröffentlichung in einem bundesweit erscheinenden Tageszeitung dringt und der Beklagte lediglich eine Urteilsveröffentlichung im Internet anbietet, so ist der von der Rsp für die Annahme, der Beklagte habe seine Willensrichtung geändert, verlangte umfassende Unterlassungsvergleich nicht gegeben.¹⁷²

Im Zusammenhang mit der Formulierung des Unterlassungsgebotes wurde von der Rsp der Einwand des Beklagten, dass ein Unterlassungsgebot im Zusammenhang mit urheberrechtsverletzenden Filmen auf einer Website auf das Internet einzuschränken sei, abgelehnt. Es liegt nach dem OGH nämlich nahe, den Inhalt eines Internetauftritts auch für die Werbung in anderen Medien zu verwenden. Das Unterlassungsgebot muss daher nicht auf den Kern der Verletzungshandlung - also die rechtswidrige Zurverfügungstellung im Internet - beschränkt werden, sondern darf auch dieser ähnliche Fälle umfassen.¹⁷³

¹⁶⁹ Vgl oben S 32 mwN.

¹⁷⁰ OGH 16.3.2004, 4 Ob 30/04x.

¹⁷¹ Vgl FN 143.

¹⁷² OGH 20.03.2007, 4 Ob 47/07a; die Entscheidung bezieht sich auf einen Verstoß gegen das UWG.

¹⁷³ OGH 21.11.2006, 4 Ob 178/06i.

Ein schuldhafter und die Bewilligung der Unterlassungsexekution rechtfertigender Verstoß gegen eine Unterlassungsverpflichtung ist bereits dann gegeben, wenn eine gegen den Unterlassungstitel verstoßende Veröffentlichung auf der eigenen Homepage vorgenommen wird.¹⁷⁴ In einem medienrechtlichen Fall wurde dem Unterlassungsbegehren des Klägers stattgegeben und klargestellt, dass ein Artikel selbst nach der bloßen "Verschiebung" aus der jeweils aktualisierten Seite einer Website in deren "Archiv" verbreitet und veröffentlicht im Sinn des §1 MedienG und des § 1330 ABGB wird, auch wenn sich dadurch die Aufmachung und die Zugriffsmodalitäten für die Besucher der Internetseite etwas anders darstellen.¹⁷⁵ Diese Überlegung ist mE auch auf Immaterialgüterrechtsverletzungen anzuwenden, etwa im Zusammenhang mit der Zurverfügungstellung von urheberrechtlich geschützten Inhalten gem § 18a UrhG. Ein Verschieben von immaterialgüterrechtsverletzenden Inhalten innerhalb einer Website kann einen Verstoß gegen eine aufrechte Unterlassungsverpflichtung nicht beseitigen, wenn der Besucher der Website lediglich die Navigation zu den inkriminierten Inhalten leicht ändern muss. Das notwendige Verschulden für die Verhängung von Beugestrafen wird hier bereits dadurch gegeben sein, dass der Websitebetreiber dafür Sorge tragen müsste, die inkriminierten Inhalte nicht mehr auf seiner Website zur Verfügung zu stellen.

In der Rsp musste allerdings ausgelotet werden, wie weit die Sorgfaltspflichten des Verpflichteten gehen, wenn bestimmte Inhalte auf einer verletzenden Website nicht mehr angezeigt werden dürfen, durch technische Gegebenheiten aber noch veraltete Versionen der Website abrufbar sind. Es kann – wie im Anlassfall¹⁷⁶ - nämlich aufgrund des weit verbreiteten Zwischenspeicherns von Websites am Computer eines Internetusers (Caching) und des ebenso gebräuchlichen Zwischenschalten von Vermittlungsservern (Proxy-Servern) dazu kommen, dass beim Endnutzer veraltete Versionen einzelner Websites angezeigt werden.¹⁷⁷ Der Sinn von Caches und Proxy-Servern ist idR Zeitersparnis beim Laden von Websites, weil bereits besuchte Websites am lokalen PC oder einem „Zwischenserver“ zwischengespeichert und beim erneuten Besuch nicht neuerlich aus dem Internet heruntergeladen werden müssen.¹⁷⁸ Wenn die Website zwischen zwei Besuchen verändert wird, muss der Nutzer idR allerdings gesondert auf „Aktualisieren“ klicken, damit der Cache-Speicher umgangen und die neue Seitenversion angezeigt wird. Sollte der Nutzer sich „hinter“ einem Proxy-Server befinden, kann er uU gar nicht auf die aktuellste Version zugreifen, wenn der Proxy-Server nicht entsprechend programmiert ist.

¹⁷⁴ Vgl etwa OGH 20.10.2004, 3 Ob 47/04i; OGH 18.12.2002, 3 Ob 215/02t; RIS-Justiz RS0079560 (T 15).

¹⁷⁵ OGH 19.02.2004, 6 Ob 190/03i (Online Archive II); dazu *Zankl*, *ecolex* 2004/319.

¹⁷⁶ OGH 25.2.2004, 3 Ob 261/03h (Unsere Klestils II).

¹⁷⁷ Dazu *Zankl*, *Proxy, Cache und Unterlassung*, *ecolex* 2004, 941.

¹⁷⁸ Vgl dazu *Zankl*, *E-Commerce-Gesetz Rz* 201.

Der Betreiber der Website kann das Abrufen einer veralteten Version durch eine Umbenennung des Dateinamens des entsprechenden Websitesinhalts oder –sollte er ein Content Management System (CMS) verwenden – durch eine Umstellung in seiner Datenbank abwenden. Ersteres ist laut dem OGH eine einfache, zielführende und sichere Maßnahme. Sie führe dazu, dass die bisher verwendeten Seiten nicht mehr existieren und eine Internet-Seite nur noch unter dem neuen Namen aufgerufen werden kann. Die Datenbanklösung sei ebenfalls ausreichend sicher. Die in der Entscheidung¹⁷⁹ genannten 50.000 ATS an Kosten für die Datenbanklösung sind allerdings missverständlich. Nur wenn die Website noch kein CMS verwendet, ist die Implementierung eines solchen mit erheblichen Kosten verbunden – die bloße Aktualisierung des Datenbanksystems fällt kostenmäßig dagegen nicht ins Gewicht. Das bedeutet, dass nicht bei jeder „Datenbanklösung“ großer finanzieller Aufwand betrieben werden muss, um die negativen Folgen von Caching zu umgehen.

Um zu beurteilen, ob die verpflichtete Partei in casu eine der beiden Möglichkeiten ergreifen müsse, damit eine Abrufbarkeit der verletzenden Website verhindert wird, zog der OGH einen Vergleich zur Verbreitung von verbotenen Äußerungen über ein Schaufenster. Dort müsste die verpflichtete Partei diese Äußerungen entfernen bzw verdecken. Entgegen der Beurteilung der Vorinstanzen sei aber eine darüber hinausgehende Beseitigungspflicht nicht vom Unterlassungstitel umfasst. In der realen Welt würde diese beispielsweise bedeuten, der Versender von Postwurfsendungen mit zu unterlassenden Behauptungen wäre verpflichtet, zumindest zu versuchen, von allen Haushalten, an die die Sendung ging, die betreffende Schrift zurückzubekommen. Die Funktion von Caches und Proxy-Servern wäre wiederum damit zu vergleichen, dass Personen, die Plakate oder Postwurfsendungen mit verbotenen Äußerungen wahrgenommen oder erhalten haben, von diesen Äußerungen Fotografien oder Kopien anfertigen, was natürlich bewirke, dass es außerhalb des Einflussbereichs des Äußerers bzw Verbreiters liegt, ob und wann auf diese Weise die Äußerung weiterhin für Interessenten zugänglich ist. Daher sei darin, dass die klagende Partei nicht alles ihr Mögliche und Zumutbare getan hat, um den Aufruf der bereits geänderten Internet-Seiten zu verhindern, noch kein Verstoß gegen den Exekutionstitel zu sehen.¹⁸⁰

Ob dieser Vergleich und der daraus gezogene Schluss tatsächlich zutreffen, ist zweifelhaft. Der OGH übersieht, dass ein Proxy-Server oder ein Cache auf Userseite weniger damit zu vergleichen ist, dass die Adressaten selbst Kopien einer Postsendung herstellen und damit

¹⁷⁹ OGH 25.2.2004, 3 Ob 261/03h (Unsere Klestils II).

¹⁸⁰ OGH 25.2.2004, 3 Ob 261/03h (Unsere Klestils II); für den Bereich des UWG wäre dies aufgrund der Regelung des § 15 UWG, wonach der Unterlassungsanspruch auch das Recht umfasst, die Beseitigung des den Vorschriften des Gesetzes widerstreitenden Zustandes vom Verpflichteten, soweit ihm die Verfügung hierüber zusteht, zu verlangen, anders zu beurteilen. Eine analoge Anwendung dieser Bestimmung scheidet aber nach stRsp aufgrund des mangelnden öffentlichen Interesses aus (RIS-Justiz RS0117238); dazu krit *Klicka*, Zum Umfang der Unterlassungsexekution nach § 355 EO, wbl 2003, 260 (262).

dem Einflussbereich des Versenders entziehen, sondern vielmehr bedeutet, dass derselbe Brief immer wieder im Postkasten aufzufinden ist und von den Adressaten auch immer wieder herausgenommen werden kann. Dem Versender (Websitebetreiber) ist es allerdings möglich, mit zumutbarem Aufwand dafür zu sorgen, dass der inkriminierte Inhalt aus praktisch allen Briefkästen entfernt wird.¹⁸¹

Es wäre daher mE durchaus gangbar, den Websitebetreiber im Rahmen des Unterlassungstitels zu verpflichten, durch zumutbare technische Maßnahmen wie Dateinamenänderungen oder Datenbank-Updates das Abrufen veralteter Cache-Inhalte zu unterbinden.¹⁸² Praktische Probleme könnten sich aber dadurch ergeben, dass Internetuser sehr viele unterschiedliche Programme und Zugangsvarianten (Direktleitungen, Router mit und ohne Proxyfunktion, Firmennetzwerke) verwenden, um im Internet zu surfen. Der Websitebetreiber wird nicht sicherstellen können, dass die inkriminierten Inhalte auf seiner Website in keiner der verschiedenen Konstellationen mehr abrufbar sind. Falls daher im Einzelfall besonders große Anstrengungen unternommen werden müssten, um für alle technisch denkbaren Varianten die Abrufbarkeit aus einem Zwischenspeicher auszuschließen, dürfte dem Websitebetreiber im Rahmen der Verschuldensprüfung kein Vorwurf daraus gemacht werden, wenn die verbotenen Inhalte dennoch vereinzelt (noch) abrufbar sind.

Um dieses Spannungsfeld adäquat aufzulösen, sollte es zu einer Umkehr der Beweislast kommen, wenn der Websitebetreiber nachweist, dass er zumutbare Maßnahmen wie Dateinamensänderungen und Datenbank-Updates durchgeführt hat. Sein Gegner im Impugnationsprozess müsste dann nachweisen, warum im Einzelfall dennoch Verschulden des Verpflichteten vorliegt.¹⁸³

¹⁸¹ Vgl auch *G. Korn*, Glosse zu 3 Ob 261/03h, MR 2005, 95; der Autor überdehnt allerdings mE die Sorgfaltspflicht des Websitebetreibers, wenn er meint, dass dieser die Speicherung in Proxy-Servern steuern und verhindern kann. Das ist technisch eben gerade nicht möglich, sondern hängt von der Konfiguration des Interzuges beim Enduser ab. Dem Websitebetreiber ist es nur möglich, die Löschung aus den Proxy-Servern bzw den Caches mit technischen Mitteln zu fördern.

¹⁸² Dass dadurch aus dem Unterlassungstitel eine recht weit gehende positive Handlungspflicht abgeleitet wird, ist im Lichte der Rsp zu den „Erfolgsverboten“ unbedenklich; vgl etwa OGH 22. 2. 2001, 6 Ob 307/00s (Ingrid Rs Homepage) zur Verbreitung kreditschädigender Äußerungen auf einer Website, wo festgehalten wird, dass das „Unterlassungsbegehren (...) seinem Sinn nach auch eine Leistungsverpflichtung, nämlich die Herausnahme (Beseitigung) der beanstandeten Passagen“ beinhaltet; vgl auch *Klicka*, Zum Umfang der Unterlassungsexekution nach § 355 EO, wbl 2003, 260 (261).

¹⁸³ Dieser Ansatz steht auch im Einklang mit der Rsp zur Beweislast im Impugnationsprozess; vgl RIS-Justiz RS0000756, insb (T2).

C.II.2. Anspruch auf Unterlassung gegen Internetprovider

C.II.2.a. Problemstellung

Sollte der Betreiber einer Website als unmittelbarer Täter nicht ermittelbar oder greifbar sein, wäre es für Rechteinhaber attraktiv, stattdessen auf die verschiedenen beteiligten Internetprovider zu greifen. Diese sind nämlich idR ermittelbar und klagbar, durch Sonderbestimmungen zT aber gegenüber „normalen“ Gehilfen privilegiert.

Die Abgrenzung innerhalb der verschiedenen Internetprovider ist hierbei aufgrund der unterschiedlichen Haftungsfreistellungen von entscheidender Bedeutung, weshalb bei der Prüfung des Unterlassungsanspruchs je nach Providerart zu differenzieren ist.¹⁸⁴

Da Internetprovider durch technische Maßnahmen allfälligen Rechtsverletzungen effektiv entgegen wirken könnten, aber durch das Bereitstellen der technischen Infrastruktur nur indirekt an den Rechtsverletzungen beteiligt sind, ist die rechtspolitische und –dogmatische Diskussion rund um die Providerhaftung bis heute im Fluss. Im Folgenden kann daher nur eine Momentaufnahme und eine Auswahl an einschlägiger Rsp wiedergegeben werden.

C.II.2.b. Europarechtliche Grundlagen

Die Haftungssituation von Internet Providern in Bezug auf Unterlassung rechtswidriger Tätigkeiten wurde grundlegend in der E-Commerce-RL vorgezeichnet und für den urheberrechtlichen Bereich durch die Info-RL, für die übrigen Immaterialgüterrechte durch die Enforcement-RL ergänzt.

C.II.2.b.1. E-Commerce-RL

Im 4. Abschnitt der E-Commerce-RL finden sich die Regelungen zur „Verantwortlichkeit der Vermittler“. Entgegen dem Wortlaut der Überschrift ordnen die Bestimmungen aber nicht an, wann Provider haften, sondern legen vielmehr fest, wann diese nicht haften. Aufgesplittet nach Tätigkeitsbereich des Providers wird mit den Art 12 bis 14 ein System der horizontalen Haftungsbeschränkung eingeführt.¹⁸⁵ Das bedeutet, dass bei Vorliegen der Haftungsfreieungsvoraussetzungen keinerlei Verantwortlichkeit für den jeweiligen Provider eintritt, weder zivil- noch strafrechtlich, und insbesondere auch nicht nach den Vorschriften des Urheber- oder Markenrechtes. Wenn diese Voraussetzungen nicht vorliegen, bedeutet es im umgekehrten Fall aber nicht, dass automatisch eine Haftung eintritt. Vielmehr sind dann die allgemeinen Voraussetzungen für eine Haftung nach den einschlägigen Tatbeständen (zB § 18a UrhG, § 10 MSchG etc) zu prüfen.

¹⁸⁴ Zur Abgrenzung siehe oben S 32 f.

¹⁸⁵ Zankl, Bürgerliches Recht⁵ Rz 270.

Die im Einzelnen geltenden Haftungsbefreiungsvoraussetzungen für Access-Provider und Host-Provider finden sich in Art 12 („Reine Durchleitung“) bzw Art 14 („Hosting“); Art 13 beschäftigt sich mit den Haftungsbefreiungsvoraussetzungen für Caching. Access-Provider sind demnach haftungsfrei, wenn sie eine „reine Durchleitung“ vornehmen, dh wenn sie die in ihrem Netz transportierten Daten weder auswählen, verändern noch speichern. Host-Provider trifft für fremde Inhalte, die sie auf ihren Servern speichern, keine Verantwortung, wenn sie keine Kenntnis von der Rechtswidrigkeit eines bestimmten Inhalts haben oder wenn, nachdem sie Kenntnis von rechtswidrigen Inhalten erlangt haben, sie diese rechtswidrigen Inhalte unverzüglich sperren. Da dieses Konzept vom österreichischen Gesetzgeber im Zuge der Umsetzung der E-Commerce-RL praktisch unverändert in das ECG aufgenommen wurde, kann die nähere inhaltliche Behandlung der einzelnen Bestimmungen beim Abschnitt über die nationale Rechtslage erfolgen.

Wichtig ist jedoch, dass die Art 12 bis 14 der E-Commerce-RL „die Möglichkeit unberührt [lassen], dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern“ (vgl Art 12 Abs 3, 13 Abs 2 und 14 Abs 3). Nach ErwGr 45 lassen daher „die in dieser RL festgelegten Beschränkungen der Verantwortlichkeit von Vermittlern die Möglichkeit von Anordnungen unterschiedlicher Art unberührt. Diese können insbesondere in gerichtlichen oder behördlichen Anordnungen bestehen, die die Abstellung oder Verhinderung einer Rechtsverletzung verlangen, einschließlich der Entfernung rechtswidriger Informationen oder der Sperrung des Zugangs zu ihnen.“

Im Gegenzug ordnet Art 15 an, dass die Mitgliedstaaten den in Art 12 bis 14 genannten Providern keine allgemeine Verpflichtung auferlegen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Nach ErwGr 47 ist in spezifischen Fällen die Normierung von Überwachungspflichten jedoch gestattet. Das Konzept der E-Commerce-RL ist daher, vereinfacht ausgedrückt, dass Access wie Host-Provider unter bestimmten Bedingungen Haftungsfreiheit genießen. Diese Haftungsbefreiungen schließen aber nicht aus, dass in einzelnen Fällen von Behörden oder Gerichten Anordnungen in Bezug auf bestimmte rechtswidrige Inhalte in den Netzen der Provider getroffen werden. Eine allgemeine Überwachungspflicht trifft die Provider nicht, besondere Überwachungspflichten sind aber nicht ausgeschlossen.

C.II.2.b.2. Info-RL

Die Rolle der Provider (in unionsrechtlicher Terminologie: „Vermittler“) im Gefüge des Urheberrechts wird in ErwGr 59 der Info-RL angeschnitten: „Insbesondere in der digitalen Technik können die Dienste von Vermittlern immer stärker von Dritten für Rechtsverstöße genutzt werden. Oftmals sind diese Vermittler selbst am besten in der Lage, diesen Verstößen ein Ende zu setzen. Daher sollten die Rechtsinhaber - unbeschadet anderer zur Verfügung

stehender Sanktionen und Rechtsbehelfe - die Möglichkeit haben, eine gerichtliche Anordnung gegen einen Vermittler zu beantragen, der die Rechtsverletzung eines Dritten in Bezug auf ein geschütztes Werk oder einen anderen Schutzgegenstand in einem Netz überträgt. Diese Möglichkeit sollte auch dann bestehen, wenn die Handlungen des Vermittlers nach Artikel 5 freigestellt sind. Die Bedingungen und Modalitäten für eine derartige gerichtliche Anordnung sollten im nationalen Recht der Mitgliedstaaten geregelt werden.“

Dementsprechend ist Art 8 Abs 3 Info-RL formuliert: „Die Mitgliedstaaten stellen sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden.“ Den einzelnen Mitgliedsstaaten verbleibt daher einiger Umsetzungsspielraum. Es spricht aber in vergleichender Betrachtung mit Art 8 Abs 2 Info-RL, der zwischen Klagen auf Schadenersatz, gerichtlichen Anordnungen sowie der Beschlagnahme von rechtswidrigem Material unterscheidet, einiges dafür, unter „gerichtlichen Anordnungen“ insbesondere Unterlassungs- und Beseitigungsanordnungen zu verstehen.¹⁸⁶

Für die Rolle des Access-Providers ist schließlich besonders relevant, dass allfällige Vervielfältigungen, die dieser im Zuge der technischen Übertragung in seinem Netzwerk vornimmt, im urheberrechtlichen Kontext freigestellt sind. Art 5 Abs 1 Info-RL ordnet nämlich an, dass vorübergehenden Vervielfältigungshandlungen, die zwar gem Art 2 Info-RL grds in das Vervielfältigungsrecht des Urhebers eingreifen, von diesem Recht ausgenommen werden, solange sie flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen; zudem muss ihr alleiniger Zweck sein, a) eine Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder b) eine rechtmäßige Nutzung eines Werks oder sonstigen Schutzgegenstands zu ermöglichen, und sie dürfen keine eigenständige wirtschaftliche Bedeutung haben.

C.II.2.b.3. Enforcement-RL

In der nach der Info-RL erlassenen Enforcement-RL, die nicht nur auf das Urheberrecht, sondern auf alle Rechte des geistigen Eigentums anwendbar ist, wurde in Art 11 Satz 2 ebenfalls ein Unterlassungsanspruch gegen „Mittelspersonen“, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden, eingeführt. Gleichzeitig wurde klargestellt, dass Art 8 Abs 3 Info-RL die *lex specialis* ist, sodass diese Bestimmung für den Bereich des Urheberrechts weiterhin maßgeblich ist (arg: „Unbeschadet des Artikels 8 Absatz 3 der Richtlinie 2001/29/EG stellen die Mitgliedstaaten ferner sicher...“). Für das österreichische Recht wurde von einer gesetzlichen Verankerung dieses Anspruchs gegen Mittelspersonen abgesehen, weil die RL keine Kriterien für die Haft-

¹⁸⁶ So auch die Materialien zur UrhG-Novelle 2003: ErlRV 40 BlgNR XXII. GP 42.

barkeit der Mittelsperson festlegt, sondern den nationalen Bestimmungen überlässt, sodass die bisherigen Grundsätze der Gehilfenhaftung beibehalten werden konnten.¹⁸⁷

C.II.2.c. Nationale Rechtslage

Anknüpfend an die allgemeinen Grundsätze der Unterlassungspflicht für fremdes Handeln („Gehilfenhaftung“) wird im Folgenden die Verantwortlichkeit der Host- und der Access-Provider im Zusammenhang mit Immaterialgüterrechtsverletzungen behandelt. Vorauszuschicken ist dabei, dass die Rsp zu Unterlassungsansprüchen nach dem Wettbewerbsrecht auch auf solche Ansprüche nach dem UrhG und dem MSchG angewendet werden kann.¹⁸⁸

C.II.2.c.1. Host-Provider (§ 16 ECG)

§ 16. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Wie bereits erläutert, handelt es sich bei § 16 ECG um eine horizontale Haftungsbeschränkung quer durch alle Rechtsgebiete, weil weder im Straf- noch im Zivilrecht eine Verantwortlichkeit für den Host-Provider besteht, wenn die entsprechenden Voraussetzungen erfüllt sind. Nach dem Wortlaut von § 19 Abs 1 ECG¹⁸⁹ sind Unterlassungsansprüche jedoch nicht vom Haftungsprivileg umfasst. In der Lit und Rsp wurde trotz dieses klaren Wortlauts darüber diskutiert, ob Unterlassungsansprüche nicht doch der Haftungsprivilegierung in § 16

¹⁸⁷ Vgl ErlRV 1423 BlgNR XXII. GP 4.

¹⁸⁸ Vgl RIS-Justiz RS0077249; ausdrücklich auch OGH 09.11.1999, 4 Ob 276/99p; vgl auch *Wiltshchek*, UWG⁷ § 14 E 975: Die wettbewerbsrechtlichen Erk zum Unterlassungsanspruch sind auch auf den urheberrechtlichen Unterlassungsanspruch anwendbar.

¹⁸⁹ „Die §§ 13 bis 18 lassen gesetzliche Vorschriften, nach denen ein Gericht oder eine Behörde dem Diensteanbieter die Unterlassung, Beseitigung oder Verhinderung einer Rechtsverletzung auftragen kann, unberührt“. Die Bestimmung setzt die entsprechenden Ausnahmen in Art 12 Abs 3, 13 Abs 2 und 14 Abs 3 E-Commerce-RL um: vgl ErlRV 817 BlgNR XXI. GP 40 f.

ECG unterliegen.¹⁹⁰ In der Entscheidung „Online-Gästebuch“ entschied sich der OGH schließlich dafür, dem Wortlaut von § 19 ECG zu folgen und zivilrechtliche Unterlassungsansprüche aus dem System der Haftungsprivilegien der §§ 13 – 17 ECG explizit auszunehmen.¹⁹¹ Wie sich im Ergebnis zeigen wird, ist diese Frage für das hier interessierende Problem – Unterlassungsansprüche gegen Host-Provider aufgrund von Immaterialgüterrechtsverletzungen ihrer Kunden - jedoch ohne Bedeutung.

Die oben dargestellte, „allgemeine“ Rechtsprechungslinie zur Gehilfenhaftung wurde im Zusammenhang mit Host-Providern weiterentwickelt, wobei den Entscheidungen „Megasex“ und „Online-Gästebuch“ besondere Bedeutung zukommt.

C.II.2.c.1.1. Die Entscheidung „Megasex“¹⁹²

Ein Host-Provider stellte auf seinem Server Speicherplatz für den Online-Auftritt eines Unternehmens namens „Megasex“ zur Verfügung. Megasex bot Telefonkontaktvermittlung und Partnervermittlung auf seiner Website an.

Eine Mitbewerberin des Unternehmens erklärte dem Host-Provider wiederholt, es würden sich wettbewerbswidrige Inhalte (zB irreführende Angaben über Kosten von Telefonaten, ungültige AGB, fehlendes Impressum) auf der Website des Unternehmens befinden. Trotz mehrmaliger Fristsetzung und diverser Verbesserungen ortete die Mitbewerberin nach mehreren Monaten weiterhin rechtswidrige Inhalte auf der Website von Megasex. Der Host-Provider sperrte daraufhin die Website und forderte, dass Megasex ein rechtliches Gutachten vorlegen sollte, um die Rechtskonformität seines Angebots zu belegen. Erst dann würde die Website wieder freigegeben. Ein derartiges Gutachten langte schließlich beim Host-Provider ein und dieser schaltete den Zugang wieder frei. Die Mitbewerberin aber bestand weiterhin darauf, dass rechtswidrige AGB und irreführende Werbung mit Gratis-Telefonnummern, die in Wirklichkeit kostenpflichtig wären, auf der Website vorhanden seien. Da sich der Host-Provider nun aber sträubte, die Website zu sperren, brachte die Konkurrentin Klage gegen Megasex und den Host-Provider ein. Das Erst- und Berufungsgericht wiesen das Unterlassungsbegehren gegen den Host-Provider unter Verweis auf dessen Haftungsprivileg ab.

¹⁹⁰ Dafür *Schanda*, Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, *ecolex* 2001, 920 (921 f); *Kresbach*, E-Commerce² (2003) 56; OLG Wien 15. 12. 2003, 4 RE 186/03g (nicht rk); offenbar zust *Hasberger/Semrau-Deutsch*, Host-Provider als Richter?, *ecolex* 2005, 197; aA, allerdings ohne nähere Begründung, bereits OGH 11.12.2003, 6 Ob 218/03g (Online Archiv I); auf den Wortlaut von § 19 ECG verweisend *Zankl*, Online-Privilegien für Unterlassungsansprüche? *ecolex* 2004, 361 mwN; *Zankl*, Glosse zu 6 Ob 190/03i (Online-Archiv II), *ecolex* 2004, 319; *Zankl*, E-Commerce-Gesetz Rz 296; *Burgstaller/Minichmayr*, ECG 142; *Brenn*, ECG 284, 307; offenlassend OGH 6.7.2004, 4 Ob 66/04s (Megasex); vgl auch *Pichler*, Besondere Kontrollpflicht für Host-Provider, *ecolex* 2007, 189.

¹⁹¹ OGH 21.12.2006, 6 Ob 178/04a (Online-Gästebuch).

¹⁹² OGH 6.7.2004, 4 Ob 66/04s (Megasex).

In seiner rechtlichen Beurteilung ließ der OGH offen, ob das Haftungsprivileg in § 16 ECG auf Unterlassungsansprüche anwendbar ist oder nicht. Er verwies darauf, dass der Zweitbeklagte zwar zur Erbringung der von der Erstbeklagten angebotenen Dienstleistungen beitrug, ja diese erst ermöglicht hatte, aber mit Formulierung und Gestaltung der beanstandeten Websites nichts zu tun hatte. Eine Haftung als Täter scheidet daher aus. Unter Verweis auf seine Judikatur zur Haftung der Vergabestelle für rechtswidrige Domainnamen¹⁹³ erläuterte der OGH, dass die Weigerung, rechtswidrige Inhalte zu entfernen, obwohl der Host-Provider Kenntnis von einer offenkundigen Rechtsverletzung erlangt hat, nichts anderes bedeutet, als den offenkundigen Verstoß des unmittelbaren Täters bewusst zu fördern und die Rechtsverletzung auch weiterhin zu ermöglichen. Den Maßstab für diese Offenkundigkeit zog der OGH dahingehend ein, dass die Rechtsverletzung auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig sein muss, also die Rechtswidrigkeit für den Anbieter für wie jedermann leicht erkennbar ist.¹⁹⁴

In diese Interessensabwägung spielt auch hinein, dass der Host-Provider in Fällen wie diesen gegen seinen Kunden und Vertragspartner Schritte setzen muss, die seinen Vertragspflichten zuwiderlaufen können. Der OGH hielt daher fest, dass im Hinblick auf die vertragliche Verpflichtung des Diensteanbieters gegenüber demjenigen, dem er seine technischen Dienste zur Verfügung stellt, ein Tätigwerden über den (in „MegaseX“ nicht vorliegenden) Fall einer offenkundigen Rechtsverletzung hinaus nicht zumutbar ist.

Die Entscheidung „MegaseX“ hat damit die in der jüngeren Rsp zur Gehilfenhaftung entwickelte Prüfpflicht aus Sicht der Host-Provider spürbar begrenzt, weil sie erst dann einer derartigen Pflicht unterliegen, wenn sie von Rechtsverletzungen explizit Kenntnis erlangen und die jeweilige Rechtsverletzung auch für Laien offenkundig ist. Aus allgemeiner Sicht sollen nämlich nur solche Dritte in die Unterlassungspflicht einbezogen werden, die gegen eine sie treffende Pflicht zur Prüfung auf mögliche Rechtsverletzungen verstoßen haben. Wer hingegen nur durch Einsatz organisatorischer oder technischer Mittel an der von einem anderen vorgenommenen wettbewerbswidrigen Handlung beteiligt war, haftet für eine Rechtsverletzung dann nicht, wenn ihn selbst im konkreten Fall keine Prüfpflichten getroffen haben oder ihm die Erfüllung einer solchen Pflicht nach den Umständen überhaupt nicht oder nur eingeschränkt zumutbar war.¹⁹⁵

Da die Situation von Host-Providern und Linksetzern mit Bezug auf fremde Inhalte ähnlich ist und ihre einschlägigen Haftungsbefreiungsvoraussetzungen parallel geregelt sind (vgl

¹⁹³ OGH 13.09.2000, 4 Ob 166/00s (fpo.at I) und OGH 12.09.2001, 4 Ob 176/01p (fpo.at II).

¹⁹⁴ Der OGH leitet dies aus den Materialien zu § 16 ECG (ErlRV 817 BlgNR XXI. GP 37) und aus § 9 Abs 2 StGB ab, der anordnet, dass ein Rechtsirrtum vorwerfbar ist, „wenn das Unrecht für den Täter wie für jedermann leicht erkennbar war“.

¹⁹⁵ *Stomper*, Die Folgen der MegaseX-Entscheidung, RdW 2005, 284 (286 f).

§§ 16 - 17 ECG), kann dieses Haftungskonzept im Übrigen auch auf Linksetzer übertragen werden. Diese müssen Links zu bestimmten Inhalten auf Aufforderung Dritter nur entfernen, wenn die Rechtsverletzung auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig ist.

C.II.2.c.1.2. Die Entscheidung „Online-Gästebuch“¹⁹⁶

Ein Tourismusverband stellte ein Online-Gästebuch zur Verfügung, in das die Besucher seiner Website Einträge posten konnten. In einem unter einem Nickname veröffentlichten Eintrag wurde ein örtlicher Gaststättenbetreiber ua als „schlechtester Wirt von Österreich“ bezeichnet und mit weiteren, teils persönlichen Schmähungen bedacht.

Der so verunglimpftete Wirt schickte ein Fax an den Betreiber des Gästebuches und forderte, dass der Eintrag binnen zwei Stunden gelöscht werden müsse. Dieser Aufforderung kam der Tourismusverband auch unverzüglich nach. Wenig später trudelte ein weiteres Fax des Wirten ein, wonach ua ein weiteres, dem ersten Eintrag zustimmendes Posting entfernt werden müsse. Erst dreizehn Tage später, bereits nach Einbringung einer Klage auf Unterlassung, entfernte der Gästebuchbetreiber auch dieses und weitere Postings, die sich auf das erste bezogen hatten.

Das Erstgericht wies das Unterlassungsbegehren ab, weil der Gästebuchbetreiber die inkriminierten Äußerungen rechtzeitig entfernt habe und keine Wiederholungsgefahr vorliege. Das Berufungsgericht gab dem Begehren dagegen statt. Die Beklagte, die dieses Forum anbiete, treffe eine Prüfpflicht im Sinn einer regelmäßigen Beobachtung der Foren und Löschung inkriminierender Textstellen.

Der OGH stellte zunächst klar, dass ein Gästebuchbetreiber ein Host-Provider iS des ECG ist. Weiters hielt er, wie bereits erwähnt, fest, dass § 19 ECG verschuldensunabhängige zivilrechtliche Unterlassungsansprüche aus dem Haftungsprivileg von § 16 ECG ausnehme. Ob und inwieweit dies für die Lösung der Rechtsfrage relevant sei, legte der OGH nicht dar. Die Rechtswidrigkeit sei auf jeden Fall nicht nach den Bestimmungen des ECG, sondern nach materiellrechtlichen Anspruchsgrundlagen, im gegenständlichen Fall § 1330 ABGB¹⁹⁷, zu beurteilen. Das Speichern von Informationen in einem Online-Gästebuch sei eine, wenn auch nur technische, Verbreitung iS von § 1330 Abs 2 ABGB. Zur Beantwortung der Frage des Bestehens eines auf § 1330 ABGB gestützten Unterlassungsanspruchs gegen den Betreiber eines

¹⁹⁶ OGH 21.12.2006, 6 Ob 178/04a (Online-Gästebuch).

¹⁹⁷ Dieser vermittelt nach stRsp (vgl RIS-Justiz RS0032423) ebenfalls einen verschuldensunabhängigen Unterlassungsanspruch; die folgenden Argumente des OGH sind daher prinzipiell auch auf andere derartige Anspruchsgrundlagen übertragbar. Dennoch ist zu beachten, dass bei Anwendung von § 1330 ABGB die Voraussetzungen der Gehilfenhaftung vom OGH nicht geprüft werden mussten und die Haftung des Host-Providers daher früher zu bejahen war als bei den Tatbeständen des Wettbewerbs- und Immaterialgüterrechts.

Online-Gästebuchs als Verbreiter der darin eingestellten Beiträge Dritter mit rechtsverletzendem Inhalt orientierte sich der OGH an der Vorjudikatur zur Haftung von Rundfunkanstalten, Buchhändlern und Betreibern eines Online-Archivs. Die Besonderheiten einer Veröffentlichung im Internet müssten aber beachtet werden.

In der Rsp zur Haftung der Rundfunkanstalten hatte der OGH noch ausgesprochen, dass ein Rundfunksender nicht für die Aussagen von Gästen in Live-Diskussionssendungen haftet, wenn diese Behauptungen im Rahmen eines „Meinungsforums“ geäußert und im Wesentlichen kommentarlos wiedergegeben wurden und sie nur als „Markt“ verschiedener Ansichten und Richtungen in Erscheinung getreten ist.¹⁹⁸ In Anlehnung an diese Grundsätze gilt für ein Online-Gästebuch, bei dessen Nutzung nicht der Eindruck erweckt wird, der Beitrag gebe die Meinung des Betreibers wieder, dass dem Betreiber im Regelfall Rechtsverletzungen durch Nutzer nicht zuzurechnen sind, wenn er sich weder damit identifiziert, noch sie sich zu eigen macht oder durch sein eigenes Verhalten provoziert.

Der OGH differenzierte aber im Folgenden die Situation in einem Online-Gästebuch von der bei Live-Fernsehübertragungen. Im Unterschied zu einer Ausstrahlung einer Live-Sendung im Rundfunk bleiben nämlich im Internet dort einmal zugänglich gemachte Beiträge weiterhin zugänglich. Aus § 16 Abs 1 Z 2 ECG leitete er weiters ab, dass den Host-Provider die Verpflichtung trifft, bei Bekanntwerden (offensichtlich) rechtswidriger Inhalte die entsprechenden Beiträge zu entfernen.¹⁹⁹ Bis hierher bewegte sich der OGH noch im Rahmen der bisherigen Judikatur.

Bei der Abwägung, ob eine erfolgte und dem Host-Provider gemeldete Rechtsverletzung in seinem Speicherbereich auch eine Überwachungspflicht auf zukünftige Rechtsverletzungen auslöst, betrat der OGH hingegen Neuland. Er hielt zunächst fest, eine allgemeine Verpflichtung zu einer Kontrolle des Vorgangs des Einstellens der Beiträge verstieße gegen § 18 Abs 1 ECG und schränkte die Möglichkeiten des freien Meinungs-austausches (Art 10 EMRK; Art 13 StGG) über Gebühr ein. Andererseits schließe § 18 Abs 1 ECG nicht aus, bei einem entsprechenden Anlass eine besondere Prüfungspflicht des Betreibers des Online-Gästebuchs anzunehmen.²⁰⁰ Eine derartige Pflicht sei - wägt man die widerstreitenden Rechte der Meinungsäußerungsfreiheit einerseits und auf Ehre und wirtschaftlichen Ruf andererseits ab - angemessen, wenn dem Betreiber schon mindestens eine Rechtsverletzung durch einen Beitrag

¹⁹⁸ Vgl OGH 10. 4. 1991, 1 Ob 36/89.

¹⁹⁹ Zur Problematik dieser Argumentation siehe unten S 75.

²⁰⁰ Der OGH übersieht bei diesem Umkehrschluss, dass die Möglichkeit zur Anordnung von besonderen Prüfungspflichten nur dem Gesetzgeber zusteht. Dies ergibt sich aus der Entstehungsgeschichte des § 18 ECG, weil diese Bestimmung wortwörtlich der E-Commerce-RL nachgebildet wurde und damit eigentlich an die Mitgliedstaaten gerichtet ist; vgl dazu *Zankl*, E-Commerce Gesetz Rz 275. Schon deswegen ist die "besondere Überwachungspflicht" im Rahmen des ECG als sehr bedenklich einzustufen.

bekannt gegeben wurde und sich damit die Gefahr weiterer Rechtsverletzungen durch einzelne Nutzer konkretisiert.

Im Anlassfall sah der OGH diese „Konkretisierung“ dadurch gegeben, dass der anonyme Autor der beanstandeten Äußerungen für den Kläger nicht identifizierbar und erreichbar war, sodass er nicht durch eine gegen diesen gerichtete Unterlassungsklage Schutz vor künftigen Verletzungshandlungen erreichen konnte. Es sei auch mit weiteren Rechtsverletzungen zu rechnen gewesen, weil der inkriminierte Beitrag auf Grund der massiven Angriffe gegen den Kläger zu Stellungnahmen anderer Nutzer eingeladen habe. Daher sei der Host-Provider verpflichtet gewesen, nach dem Bekanntwerden der Rechtsverletzungen die Beiträge im Online-Gästebuch laufend zu beobachten, ob sie erneute Äußerungen der beanstandeten Art, die für den betroffenen Kläger eine besonders einschneidende Wirkung haben konnten, enthielten. Eine derartige Kontrolle auf bestimmte Rechtsverletzungen hin sei mit wesentlich geringerem Aufwand möglich als die Durchführung einer allgemeinen Überwachungspflicht und sei im vorliegenden Fall jedenfalls zumutbar, drohte doch eine erhebliche Rechtsverletzung (schwere wirtschaftliche Schädigung des Klägers), was für die Beklagte offensichtlich gewesen sei. Da auch die Wiederholungsgefahr aufrecht war, bestätigte der OGH die Unterlassungspflicht des Host-Providers.

Für die somit erfolgte Einführung der insgesamt wenig spezifischen Rechtsfigur der „besonderen Überwachungspflicht“ wurde der OGH im Schrifttum kritisiert.²⁰¹ Tatsächlich sind die genauen Kriterien für diese Pflicht sowie ihr zeitlicher Umfang bis dato unklar, wodurch die Gefahr läuft, das in § 18 Abs 1 ECG normierte Verbot der allgemeinen Überwachungspflicht zu umgehen. Für zukünftige Fälle wird der OGH nicht umhinkommen, eine detailliertere Abwägung mit klar umschriebenen Kriterien vorzunehmen. Wie von *Pichler*²⁰² unter Bezug auf einschlägige deutsche Rsp vorgeschlagen, könnte dabei berücksichtigt werden, ob der Host-Provider Entgelt (im weiten Sinn des § 3 ECG) für seine Dienste bezieht, was eine Überwachung jedenfalls zumutbarer erscheinen lässt als bei privat und unentgeltlich betriebenen Websites. Derzeit müssten nämlich auch Betreiber privater Online-Gästebücher oder Online-Foren stets auf der Hut sein, weil einmal erfolgte Rechtsverletzungen in ihrem Verantwortungsbereich die besondere Überwachungspflicht auslösen können.²⁰³ Eine derartige Differenzierung ist freilich im System des ECG (§ 18 Abs 1 iVm § 19 Abs 2 ECG) so nicht vorgesehen.

²⁰¹ *Kasper*, Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 4; *Pichler*, Besondere Kontrollpflicht für Host-Provider, ecolex 2007, 189 (190).

²⁰² *Pichler*, Besondere Kontrollpflicht für Host-Provider, ecolex 2007, 189 (190).

²⁰³ Aus § 19 Abs 2 iVm Abs 1 ECG folgt, dass auch Betreiber unentgeltlicher Dienste von Gerichten zur Unterlassung verpflichtet werden können; vgl *Pichler*, Besondere Kontrollpflicht für Host-Provider, ecolex 2007, 189 (190).

C.II.2.c.1.3. Zur Übertragbarkeit auf das Immaterialgüterrecht

Aus immaterialgüterrechtlicher Sicht ist zunächst zu bestimmen, aufgrund welcher Anspruchsgrundlage Host-Provider für rechtsverletzende Websites in ihrem Speicherbereich auf Unterlassung in Anspruch genommen werden könnten. Die Argumentation des OGH in „Online-Gästebuch“ ist nämlich auf den ersten Blick verwirrend: Aus § 16 Abs 1 Z 2 ECG ergebe sich, dass den Host-Provider die Verpflichtung trifft, bei Bekanntwerden (offensichtlich) rechtswidriger Inhalte die entsprechenden Beiträge zu entfernen.²⁰⁴ Wie bereits mehrfach erwähnt, normiert § 16 Abs 1 ECG aber gerade keine Handlungspflicht, sondern lediglich Befreiungsvoraussetzungen. Richtigerweise muss es daher heißen, dass sich aus § 16 Abs 1 ECG nur ergibt, dass bei Bekanntwerden offensichtlich rechtswidriger Inhalte kein Haftungsprivileg für den Host-Provider besteht.²⁰⁵ Ob auch eine Unterlassungspflicht für den Host-Provider besteht, muss aber nach dem jeweils einschlägigen Tatbestand außerhalb des ECG beurteilt werden.²⁰⁶

Im Urheberrecht besteht mit § 81 Abs 1a UrhG seit der Umsetzung des Art 8 Abs 3 Info-RL im Zuge der UrhG-Novelle 2003 eine Sonderbestimmung zur Haftung von „Vermittlern“, worunter auch Host-Provider fallen.²⁰⁷

§ 81 (1a) Bedient sich derjenige, der eine solche Verletzung begangen hat oder von dem eine solche Verletzung droht, hiezuh der Dienste eines Vermittlers, so kann auch dieser auf Unterlassung nach Abs. 1 geklagt werden. Wenn, bei diesem die Voraussetzungen für einen Ausschluss der Verantwortlichkeit nach den §§ 13 bis 17 ECG vorliegen, kann er jedoch erst nach Abmahnung geklagt werden.

Der Wortlaut legt auf den ersten Blick nahe, dies so zu interpretieren, dass damit die allgemeinen Grundsätze, die eine Haftung Dritter ohnehin nur bei bewusster Förderung des unmittelbaren Täters und bei Bestehen der technischen Möglichkeit zur Unterbindung der Handlung vorsehen, noch weiter eingeschränkt werden.²⁰⁸ Dogmatisch stellt sich aber die Frage, wozu der Gesetzgeber diese Bestimmung eingeführt hat, wenn der (verschuldensunabhängige) Unterlassungsanspruch gegen unmittelbare Täter ohnedies durch § 81 Abs 1

²⁰⁴ Methodisch ist bereits fragwürdig, warum der OGH diese Gesetzesstelle überhaupt bemüht, wenn er § 19 Abs 1 ECG dahingehend auslegt, dass § 16 ECG bei Unterlassungsansprüchen ohnehin nicht anwendbar ist. Dies kann nur so verstanden werden, dass der OGH die §§ 13 bis 18 ECG mittelbar in eine breitere Interessensabwägung miteinbezieht, um allfällige Rechtfertigungsgründe zu ergründen; vgl dazu auch *Pichler*, Besondere Kontrollpflicht für Host-Provider, *ecolex* 2007, 189.

²⁰⁵ Da dies aber nach hA bereits aufgrund von § 19 Abs 1 ECG so ist, ist der Prüfungsschritt in diesem Zusammenhang ohnehin obsolet.

²⁰⁶ *Zankl*, E-Commerce-Gesetz Rz 225; *Ofner* in *Kucsko*, *urheber.recht* § 81 Pkt 8.5.

²⁰⁷ § 81 Abs 1a UrhG verweist explizit auf die §§ 13 bis 17 ECG, wo unter anderem die Befreiungsvoraussetzungen für Host-Provider geregelt sind. Zur Auslegung des Begriffs „Vermittler“ siehe noch ausführlich unten S 132 f.

²⁰⁸ So *Ofner* in *Kucsko*, *urheber.recht* § 81 Pkt 8.5.

UrhG besteht und eine allfällige Gehilfenhaftung, die nach stRsp vorwiegend aus § 1301 ABGB abgeleitet wird und damit Verschulden voraussetzt, mangels personeller Einschränkung auch auf Vermittler, also insb Internetprovider, anwendbar ist, ohne dass dafür eine neue Bestimmung nötig gewesen wäre. Denkbar wäre allenfalls, dass bei der Erstellung der Regierungsvorlage übersehen wurde, dass kraft § 19 Abs 1 ECG Unterlassungsansprüche ohnehin aus dem Haftungsprivileg der Vermittler (§§ 13 bis 17 ECG) ausgenommen sind. Dafür spricht, dass laut den Erläuterungen „sichergestellt“ werden sollte, dass Unterlassungs- und Beseitigungsansprüche auch gegen Vermittler geltend gemacht werden können.²⁰⁹ Dieser Eindruck wird aber durch den Bericht des Justizausschusses entkräftet, in dem explizit auf § 19 Abs 1 ECG hingewiesen und betont wird, dass der Ausschluss der Verantwortlichkeit für Diensteanbieter iS des ECG sich nicht auf Unterlassungsansprüche erstreckt.²¹⁰

Aus systematischer Sicht und vor dem Hintergrund des Art 8 Abs 3 Info-RL spricht somit einiges dafür, dass der Gesetzgeber eine urheberrechtliche Sonderhaftung für Vermittler einführen wollte, die nicht dem bisherigen Konzept der Gehilfenhaftung unterliegt, also insbesondere keine bewusste (vorsätzliche oder – nach jüngerer Rsp – zumindest grob fahrlässige) Förderung des unmittelbaren Täters voraussetzt.²¹¹ Da § 81 Abs 1a UrhG zudem mit dem allgemeinen Unterlassungsanspruch in Abs 1 leg cit verknüpft ist (Arg: „... kann auch dieser (*gemeint: Vermittler, Anm*) auf Unterlassung nach Abs. 1 geklagt werden.“), ist er so auszu-legen, dass Vermittler (und somit auch Host-Provider) verschuldensunabhängig für Urheberrechtsverletzungen Dritter haften, die unter Verwendung ihrer Dienste begangen wurden bzw drohen, begangen zu werden. Der Vermittler wird dadurch im Ergebnis dem unmittelbaren Täter gleichgestellt.²¹²

Diese äußerst breite Haftungssituation wurde durch § 81 Abs 1a Satz 2 UrhG eingeschränkt, weil dadurch Vermittler, bei denen die Voraussetzungen für einen Ausschluss der Verantwortlichkeit nach den §§ 13 bis 17 ECG vorliegen, erst nach Abmahnung geklagt werden können. Diese haben dadurch Gelegenheit, Rechtsverletzungen in ihrem Bereich nachzugehen, ohne sich bereits in einem gegen sie gerichteten Verfahren zu befinden.²¹³

Während aus dogmatischer Sicht damit im Urheberrecht in der Tat neue Wege beschritten werden, dürften die praktischen Auswirkungen sich mE in Grenzen halten. Insbesondere

²⁰⁹ ErlRV 40 BlgNR XXII. GP 42.

²¹⁰ JAB 51 BlgNR XXII. GP 2.

²¹¹ In diesem Sinn offenb auch *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 5.

²¹² Eine eigene Verletzungshandlung des Vermittlers ist daher auch nicht Voraussetzung für die Haftung; vgl auch *Dillenz/Gutman*, UrhG & VerwGesG² § 81 UrhG Rz 20.

²¹³ In diesem Sinn ist mE auch die im Bericht geäußerte Absicht des Justizausschusses zu verstehen, wonach die Einführung von Satz 2 in § 81 Abs 1a UrhG auf die Anregung zurückgeht, auf die „Fälle von Vermittlern, die als Diensteanbieter [...] nach den Bestimmungen der §§ 13 bis 17 ECG von der Verantwortlichkeit für bestimmte Tätigkeiten befreit sind“, „Rücksicht zu nehmen“. Vgl JAB 51 BlgNR XXII. GP 2.

durch das Erfordernis der Abmahnung vor einer allfälligen Klagsführung wird sich die Haftung gem § 81 Abs 1a UrhG nämlich eng an die bisher entwickelten Grundsätze der Gehilfenhaftung anlehnen. Auch bei dieser müsste ein Host-Provider jedenfalls zunächst Kenntnis von Rechtsverletzungen in seinem Speicherbereiche erlangen, was idR durch eine entsprechende Abmahnung seitens des Rechteinhabers erfolgen wird.²¹⁴ Daran anschließend müsste er sodann unverzüglich tätig werden und die offenkundig urheberrechtsverletzende Information entfernen, um sich nicht der bewussten Förderung des unmittelbaren Täters schuldig zu machen.

Weder nach § 81 Abs 1a UrhG noch im Rahmen der Gehilfenhaftung kann der Rechteinhaber daher sofort auf Unterlassung klagen, weil dem § 81 Abs 1a Satz 2 UrhG entgegensteht bzw nach allgemeinen Voraussetzungen der Host-Provider nur dann zur Unterlassung herangezogen werden kann, wenn er den unmittelbaren Täter bewusst fördert, was erst nach Kenntnis der Rechtsverletzung überhaupt möglich ist. Denkbar wäre allenfalls, dass der Host-Provider durch Dritte (zB User oder Medienberichte) von einer Urheberrechtsverletzung auf einer von ihm gehosteten Website erfahren hat²¹⁵ und sich aufgrund seiner Kenntnis nicht mehr auf das Haftungsprivileg in § 16 Abs 1 Z 1 ECG berufen kann. § 81 Abs 1a Satz 2 UrhG wäre dann mangels des Vorliegens der Voraussetzungen für einen Ausschluss der Verantwortlichkeit (§ 16 ECG) nicht mehr anwendbar, und der Rechteinhaber müsste keine Abmahnung versenden, bevor er den Host-Provider klagt. Da aber auf Seiten des Rechteinhabers derart detaillierte Kenntnisse vom Wissenstand des jeweiligen Host-Providers kaum vorliegen und idR Beweisschwierigkeiten hinzutreten werden, dürften sich jedoch auch in diesem Zusammenhang die praktischen Unterschiede zur „allgemeinen“ Gehilfenhaftung“ in engen Grenzen halten.

Da im Markenrecht eine dem § 81 Abs 1a UrhG entsprechende Sonderhaftung nicht vorgesehen ist, gelten hier in jedem Fall die Grundsätze der Gehilfenhaftung auch für Vermittler, darunter insb Host-Provider. Entscheidend bleibt dabei das Erfordernis, dass der Host-

²¹⁴ Aufgrund der Möglichkeit, das Klagebegehren in der ersten Tagsatzung anzuerkennen und dem Kläger damit die Kosten für die Prozessführung aufzubürden (§ 45 ZPO), ist es vor dem Hintergrund der uU gebotenen Dringlichkeit auch denkbar, dass der Host-Provider erst mit der Klage Kenntnis von der Rechtsverletzung erlangt. Diesfalls wäre mangels eines Erstverstoßes statt Wiederholungsgefahr freilich Begehungsgefahr zu prüfen. Die tatbestandsgemäße bewusste Förderung einer Rechtsverletzung setzt dabei begriffsnotwendig voraus, dass der Host-Provider zuvor Kenntnis von der Rechtsverletzung haben muss. Damit einher muss die Möglichkeit gehen, die Aktivlegitimation des Anspruchstellers zu prüfen und die inkriminierte Website auf offenkundig rechtswidrige Inhalte zu prüfen. Da diese Prüfung auch dann vorzunehmen ist, wenn sofort geklagt wird, ist es fraglich, ob durch die sofortige Einbringung einer Unterlassungsklage mit dem drohenden Kostenrisiko für den Kläger (§ 45 ZPO) dem Gesichtspunkt der Dringlichkeit wirklich besser Rechnung getragen wird als durch eine vorhergehende Abmahnung des Host-Providers; aA offenb *Zankl*, E-Commerce-Gesetz Rz 297.

²¹⁵ Dazu und zur Frage, wer im Unternehmen Kenntnis haben muss, damit diese Bedingung erfüllt ist, siehe *Zankl*, E-Commerce-Gesetz Rz 237.

Provider zunächst Kenntnis von einer offenkundigen Rechtsverletzung haben muss, weil er ansonsten nie zur Stufe der bewussten Förderung des Täters gelangen kann.²¹⁶

Die notwendige „Offenkundigkeit“ der Rechtsverletzung ist nach stRsp nach den Kenntnissen und Fertigkeiten eines juristischen Laien zu beurteilen, worunter jemand zu verstehen ist, der kein rechtswissenschaftliches Studium absolviert hat.²¹⁷ In der Rsp wird vertreten, dass offenkundige Tatsachen für jedermann ohne besondere Fachkenntnisse aus zuverlässigen Quellen überprüft werden können. Es ist daher also nicht auf einen Fachmann bzw Fachkreis abzustellen, sondern auf Erfahrungssätze aus der allgemeinen Lebenserfahrung, geografische Tatsachen oder Ereignisse des Zeitgeschehens. Eine offenkundige Rechtsverletzung fällt demnach in die Augen, ist daher auch für den Laien ohne größere Schwierigkeiten wahrnehm- und erkennbar.²¹⁸ Darunter subsumiert wurde in „Online-Gästebuch“ das Verunglimpfen und Beschimpfen eines Gastwirtes; verneint wurde dagegen in „Megasex“ die Fähigkeit des Durchschnittsbürgers, das zulässige Ausmaß von Haftungsfreizeichnungen in AGB juristisch korrekt zu beurteilen.

Fraglich ist, wie eine Immaterialgüterrechtsverletzung „offenkundig“ sein kann, wenn dem Durchschnittsmenschen typischerweise unbekannt ist, wem welches Immaterialgut, zB eine bestimmte Fotografie, ein Musikstück etc, zuzuordnen ist und (wie im Urheberrecht) auch kein öffentliches Register verfügbar ist. In diesen Fällen ist nämlich genau genommen nicht durch Kenntnisnahme des Inhalts selbst, sondern erst durch Kenntnis der dahinterliegenden (rechtswidrigen) Tätigkeit, also der lizenzlosen Zurverfügungstellung auf der Website, die Rechtswidrigkeit erkennbar. Daher ist die Verletzung von Immaterialgüterrechten für Außenstehende wie Host-Provider deutlich schwerer als „offenkundig“ erkennbar als zB die Verbreitung von NS-Gedankengut oder kinderpornographischen Darstellungen, weil sich bei diesen die Rechtswidrigkeit schon aus den Inhalten selbst ergibt, ohne dass darauf abgestellt werden muss, wie diese zustande gekommen sind.²¹⁹ Daher ist im Übrigen noch schwerer vorstellbar, dass ein Host-Provider anders als durch eine Mitteilung des betroffenen Rechteinhabers von einer Urheber- oder Markenrechtsverletzung Kenntnis erlangt.

Fälle, in denen etwa Musikstücke oder Fotografien umgestaltet und auf Websites zur Verfügung gestellt werden und nicht klar ist, ob bereits ein neues Werk vorliegt, werden die Schranke der „Offenkundigkeit“ wohl nicht passieren. Vom Host-Provider kann nämlich nicht erwartet werden, diffizile Auslegungen des urheberrechtlichen Werk- und Bearbei-

²¹⁶ Zur durch die Entscheidung „Online-Gästebuch“ eingeführten Rechtsfigur der „besonderen Überwachungspflicht“ siehe unten S 80.

²¹⁷ Vgl *Hasberger/Semrau-Deutsch*, Host-Provider als Richter?, *ecolex* 2005, 197 (198) mwN.

²¹⁸ *Hasberger/Semrau-Deutsch*, Host-Provider als Richter?, *ecolex* 2005, 197 (198) mwN; vgl auch RIS-Justiz RS0110714.

²¹⁹ Zu diesem Problem vgl auch *Zankl*, E-Commerce-Gesetz Rz 238.

tungsbegriffs (§ 1 iVm § 5 UrhG) vorzunehmen. Andererseits darf der Begriff „offenkundig“ auch nicht so weit überspannt werden, dass dem Rechteinhaber die faktische Möglichkeit genommen wird, sein Recht durchzusetzen. Wenn daher eine plumpe Vervielfältigung oder Zurverfügungstellung fremder Werke auf einer Website vorliegt, so wird der Nachweis der Urheberschaft ausreichend sein müssen, um die Bedingung der „offenkundigen Rechtsverletzung“ zu erfüllen. In Markenrechtsfällen wird eine mögliche Rechtsverletzung, die eine diffizile Abwägung voraussetzt, ob eine verwechslungsfähig ähnliche Marke für gleiche oder ähnliche Waren und Dienstleistungen verwendet wird, als nicht offenkundig ausscheiden.²²⁰ Eine direkte Verwendung eines eindeutig fremden Zeichens ohne Lizenz, zu der der Rechteinhaber noch einen aktuellen Markenregisterauszug vorlegt, wird aber offenkundig rechtsverletzend sein. Jedenfalls zu weitgehend wäre es im Lichte der bisherigen Rsp²²¹, vom Host-Provider die Einholung eines rechtlichen Gutachtens, zB von einem Rechtsanwalt, zu verlangen. Die genaue Abwägung, ob auch ein juristischer Laie eine Rechtsverletzung als offenkundig beurteilt, wird jedoch der Bewertung des Einzelfalls überlassen bleiben und somit im Übrigen idR auch nicht revisibel iS des § 502 ZPO sein.²²²

Auf die Abmahnung, die den Host-Provider in Kenntnis der offenkundigen Rechtsverletzung setzt, folgt konsequenterweise eine Handlungspflicht seitens des Providers.²²³ Sollte er nämlich in Kenntnis der offenkundigen Rechtsverletzung die beanstandeten Inhalte der Website nicht löschen, obwohl ihm eine Löschung technisch möglich und zumutbar ist, würde er dadurch den unmittelbaren Täter bewusst fördern und wäre als Gehilfe zur Unterlassung zu verpflichten.

Es ist daher mE auch nicht nötig, für das Begehren auf Entfernung rechtswidriger Inhalte von Websites den Beseitigungsanspruch in § 82 Abs 1 UrhG bzw § 52 MSchG zu bemühen. Dieser "passt" besser auf Situationen, in denen körperliche Eingriffsgegenstände einmalig und dauerhaft vernichtet werden sollen. Für Websites im Internet, die nicht die Hervorbringung einzelner Kopien, sondern die langfristige Zurverfügungstellung von Inhalten im Blick haben, ist der Unterlassungsanspruch dagegen deutlich besser geeignet.²²⁴ Aus Unterlas-

²²⁰ So schon dBGH 17.5.2001, I ZR 251/99 (ambiente.de).

²²¹ OGH 6.7.2004, 4 Ob 66/04s (Megasex): „Im Hinblick auf die vertragliche Verpflichtung des Diensteanbieters gegenüber demjenigen, dem er seine technischen Dienste zur Verfügung stellt, ist ein Tätigwerden über den Fall einer offenkundigen Rechtsverletzung hinaus nicht zumutbar“.

²²² OGH 19.12.2006, 4 Ob 229/06i; vgl auch RIS-Justiz RS0042742.

²²³ Die Unterlassungspflicht des Host-Providers ist daher im Ergebnis ein Erfolgsverbot, weil sie ihrem Sinn nach auch eine Leistungsverpflichtung, nämlich die Herausnahme (Beseitigung) der beanstandeten Informationen beinhaltet; vgl FN 182. Dies übersehend *Parschalk*, Provider-Haftung für Urheberrechtsverletzungen Dritter, *ecolex* 1999, 834 (836) in FN 23.

²²⁴ AA offenb *St. Korn* in Kucsko, *urheber.recht* § 82 Pkt 2.3.3; *ders* aber relativierend in Pkt 1.4. Sofern das Begehren dennoch auf Beseitigung lautet, muss statt auf das Eigentumsrecht am Trägermaterial der Daten (zB Ser-

sungstiteln können zudem auch funktionelle Beseitigungsansprüche, wie eben die Entfernung rechtsverletzender Inhalte von Websites, gem § 355 EO exekutiert werden.²²⁵

Schwierig ist die Erfassung der in „Online-Gästebuch“ entwickelten Figur der besonderen Überwachungspflicht, die die drohende Haftung für den Host-Provider zeitlich prolongiert, indem sie von ihm fordert, von sich aus seinen Speicherbereich zu überwachen. Dogmatisch setzte damit der OGH wohl die problematische Rsp fort, wonach im Einzelfall auch (grobe) Fahrlässigkeit in Bezug auf eine Rechtsverletzung Dritter ausreicht, um als Gehilfe in Anspruch genommen zu werden.²²⁶ Dabei ist aber zu beachten, dass die Argumentation in „Online-Gästebuch“ aus der Anwendung des § 1330 Abs 1 und Abs 2 ABGB heraus entwickelt wurde. Zu Recht wurde in der Lit daher darauf hingewiesen, dass die besonderen Voraussetzungen der Gehilfenhaftung nicht geprüft werden mussten und die genannte Entscheidung daher ein Ausnahmefall der Providerhaftung bleiben könnte.²²⁷ In Deutschland wurde eine derartige Überwachungspflicht aber auch in immaterialgüterrechtlichen Anlassfällen betont, wobei in vereinzelt Entscheidungen die Pflicht von Host-Providern, ihren Speicherbereich auf Rechtsverletzungen zu überprüfen, äußerst weit ausgelegt wurde.²²⁸

Für Österreich ist bisher weitgehend unklar, worin nach dem Konzept des OGH der Unterschied zwischen besonderer und allgemeiner Überwachungspflicht liegt, wobei letztere als zeitlich und inhaltlich weitgehend unbegrenzte Überwachung zu definieren ist. Aus dem Anlassfall „Online-Gästebuch“ ist in inhaltlicher Hinsicht lediglich herauszulesen, dass die besondere Überwachungspflicht jedenfalls verletzt wird, wenn zwischen erneuter Rechtsverletzung und anschließender Sperrung seitens des Providers mehr als eine Woche liegt. Konsequenterweise muss das auch gelten, wenn kein erneuter Hinweis seitens des Rechteinhabers einlangt.²²⁹ Es ist daher aus Sicht des Providers nicht ausreichend, einmal pro Woche die Website eines Nutzers aufzurufen, die in der Vergangenheit mit Rechtsverletzungen aufgefallen ist, um gegebenenfalls auf erneute Rechtsverletzungen zu reagieren. Um eine Ausuferung

ver-Festplatte) auf das tatsächliche Herrschaftsverhältnis über diese abgestellt werden; vgl *Dillenz/Gutman*, UrhG & VerwGesG² § 82 UrhG Rz 7.

²²⁵ *St. Korn* in Kucsko, urheber.recht § 82 Pkt 4.3; vgl dazu auch FN 182.

²²⁶ Siehe oben S 62 bzw FN 168.

²²⁷ *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26).

²²⁸ So insb das OLG Hamburg 2.7.2008, 5 U 73/07 (rapidshare IV), das zum bekannten Hosting-Dienst rapidshare.de aussprach, er sei verpflichtet, alles Zumutbare zu tun, um kerngleiche Verstöße (gemeint: Urheberrechtsverletzungen) zukünftig zu unterbinden. Dabei sah das Gericht es als nicht ausreichend an, wenn der Webhosting-Dienst einen MD5-Filter einsetzt, weil dieser Filter nur greift, wenn eine absolut identische Datei erneut hochgeladen werden soll. Insbesondere wenn es in der Vergangenheit mehrfach zu gleichartigen Rechtsverletzungen gekommen ist, sei der Webhosting-Dienst zu einer umfassenden, pro-aktiven Vorabprüfung verpflichtet. Dies bedeute im Zweifelsfall insbesondere auch eine umfassende IP-Speicherung und IP-Auswertung. Eine Verpflichtung, den Dienst nur noch gegen Registrierung und nicht mehr anonym anzubieten, bestehe jedoch nicht.

²²⁹ *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26).

der Haftung zu vermeiden, ist die besondere Prüfpflicht des Host-Providers jedoch auf solche Rechtsverletzungen zu beschränken, wie sie der Art nach in der Vergangenheit bereits stattgefunden haben und über die der Provider informiert war.²³⁰ In „Online-Gästebuch“ betonte der OGH zudem das Kriterium der notwendigen Zumutbarkeit für den Provider, das bereits in die tendenziell rechteinhaberfreundlichen deutsche Rsp zur Störerhaftung eingeflossen ist, wo es als einzige, wenn auch unscharfe, Beschränkung der sonst sehr weitgehenden Haftungssituation für Host-Provider dient.²³¹

Fraglich bleibt aber, wie lange der Host-Provider diese regelmäßige Prüfung durchführen muss. Bei der Beurteilung hilft womöglich eine genauere methodische Analyse der „besonderen Überwachungspflicht“.

Die Rechtsgrundlage für diese Pflicht kann nämlich entgegen der missverständlichen Wortwahl des OGH in „Online-Gästebuch“ nicht in § 16 Abs 1 Z 2 ECG liegen²³², weil sonst systemwidrig eine positive Handlungspflicht aus einer Haftungsbefreiungsvoraussetzung abgeleitet würde. Die normative Grundlage für die besondere Überwachungspflicht muss daher weiterhin der jeweilige Unterlassungsanspruch sein. Dies bedeutet, dass jedenfalls aufrechte Wiederholungsgefahr gegeben sein muss, die nach allgemeinen Grundsätzen nur dann wegfällt, wenn eine erneute Rechtsverletzung als vollkommen ausgeschlossen oder doch höchst unwahrscheinlich erscheint.²³³

Zentrale Aussage des OGH in „Online-Gästebuch“ war, dass der Host-Provider mit weiteren Rechtsverletzungen zu rechnen hatte, weil ihm bereits mindestens eine Rechtsverletzung durch einen Beitrag bekannt gegeben wurde und sich damit die Gefahr weiterer Rechtsverletzungen konkretisierte. Dreh- und Angelpunkt des bisherigen Konzepts der besonderen Überwachungspflicht ist daher, ob der Host-Provider mit weiteren Rechtsverletzungen rechnen muss oder nicht. Der Beurteilungsmaßstab dieses „Rechnen-Müssens“ muss notgedrungen weniger streng sein als derjenige, mit dem das Wegfallen der Wiederholungsgefahr als materieller Grundvoraussetzung für den Unterlassungsanspruch gemessen wird. Andernfalls würden diese beiden Kriterien zusammenfallen, was nicht aus der Entscheidung „Online-Gästebuch“ herausgelesen werden kann, weil der OGH die beiden Prüfungsschritte eindeutig trennt. Somit kann der Host-Provider nicht verpflichtet sein, seine besondere Überwachungspflicht so lange auszuüben, bis eine erneute Rechtsverletzung als vollkommen ausgeschlossen oder höchst unwahrscheinlich erscheint. Vielmehr muss es ausreichend zur Erfüllung seiner besonderen Überwachungspflicht sein, wenn er den ihm zuzurechnenden Spei-

²³⁰ *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26).

²³¹ Vgl *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26) mwN.

²³² AA offenb *Kasper*, Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 1 (4).

²³³ RIS-Justiz RS0012056.

cherbereich so lange und intensiv beobachtet, bis mit überwiegender Wahrscheinlichkeit keine drohende Rechtsverletzung mehr bevorsteht.

Für den hier interessierenden Fall einer Website mit immaterialgüterrechtsverletzenden Inhalten wird dies zB dann der Fall sein, wenn bei werbefinanzierten Streaming-Websites, die urheberrechtsverletzende Filme anbieten, das Geschäftsmodell später unter erheblichen Investitionen auf legale Bezahlmodelle geändert wird, was erneute Urheberrechtsverletzungen nicht ausschließt, aber doch überwiegend unwahrscheinlich macht. Selbiges müsste gelten, wenn zB die erforderliche Software für den Betrieb eines Online-Shops mit markenrechtsverletzenden Waren gelöscht und dies dem Host-Provider angezeigt wird. In der Rsp wurde nämlich bereits festgehalten, dass das Löschen von Software, die für die Teilnahme an Filesharing-Systemen erforderlich ist, schon die Erstbegehungsgefahr wegfallen lässt, was umso mehr für den Wegfall der besonderen Überwachungspflicht gelten muss.²³⁴

C.II.2.c.1.4. Zur Rolle der §§ 16 und 19 ECG

Auffallend ist, dass in wettbewerbsrechtlichen und damit auch immaterialgüterrechtlichen Fällen das Prüfschema der Haftungsbefreiungsvoraussetzungen nach § 16 Abs 1 ECG und die materiellen Voraussetzungen für einen Unterlassungsanspruch gegen Host-Provider exakt übereinstimmen. Das in der Rsp entwickelte Konzept der bewussten Förderung des unmittelbaren Täters stellt nämlich - von der problematischen Rechtsfigur der „besonderen Überwachungspflicht“ abgesehen - ebenso wie § 16 Abs 1 Z 1 ECG darauf ab, ob dem bloß mittelbar (technisch bzw vertrieblich) beteiligten Dritten die Rechtsverletzung tatsächlich bekannt ist.

Im Ergebnis ist es daher ohne Bedeutung, ob § 19 ECG das System der Haftungsbefreiungen in § 16 ECG durchbricht oder nicht, weil die vom OGH entwickelte Rsp zum Unterlassungsanspruch von Host-Providern dieselben Sachverhalte von einer Haftung ausnimmt wie die Haftungsprivilegien in § 16 ECG.²³⁵ Da bereits auf Ebene der materiellen Unterlassungsanspruchsgrundlage eine Haftung ausscheidet, wenn seitens des Host-Providers keine Kenntnis von der Rechtsverletzung besteht, ist die (doppelte) Befreiung auf Ebene des ECG somit nicht mehr vonnöten.²³⁶ Im gegenteiligen Fall, wo also die allgemeinen Voraussetzungen für eine Unterlassungspflicht zutreffen, würden auch die Haftungsbefreiungsvorausset-

²³⁴ Vgl OGH 22.1.2008, 4 Ob 194/07v (Limewire).

²³⁵ Dies zeigt sich besonders deutlich in der Entscheidung OGH 6.7.2004, 4 Ob 66/04s (Megasex), in der der OGH genau deswegen auch von einer Festlegung zur Bedeutung von § 19 ECG absehen konnte; bereits vor dem Erlass der E-Commerce-RL erkannte diese Wertung des damaligen Richtlinienentwurfes *Parschalk*, Provider-Haftung für Urheberrechtsverletzungen Dritter, *ecolex* 1999, 834 (837).

²³⁶ Daher ist auch nicht von Belang, ob zuerst die ECG-Privilegien oder die materielle Anspruchsgrundlage geprüft werden.

zungen des ECG dem betroffenen Provider nicht mehr weiterhelfen.²³⁷ Die in der Lit diskutierte Frage, ob die Haftungsprivilegien des ECG entgegen § 19 ECG nicht doch auch für Unterlassungsansprüche gelten, ist daher für Host-Provider im Bereich des Wettbewerbs- und Immaterialgüterrecht obsolet. Anderes gilt nach zutr hA in Schadenersatzfragen, weil hier der Host-Provider nicht erst ab Kenntnis, sondern bereits ab bewusst fahrlässiger Unkenntnis sein Haftungsprivileg verliert und bestimmte Anspruchsgrundlagen qualifiziertes Verschulden (zB Wissentlichkeit bei deliktischer Haftung nach § 1300 ABGB) erfordern, so dass sich die Voraussetzungen nicht decken. Die Unterscheidung ist daher in diesen Fällen weiterhin zu treffen.²³⁸

§ 19 ECG könnte zudem, wie von *Schanda*²³⁹ angedacht, in jenen Fälle zur Anwendung kommen, in denen ein Gericht oder eine Verwaltungsbehörde Unterlassung oder Beseitigung der Rechtsverletzung anordnet, jedoch kein zivilrechtlicher Unterlassungsanspruch zu Grunde liegt, also insb Anordnungen von Strafgerichten.

C.II.2.c.2. Access-Provider (§ 13 ECG) – „Sperransprüche“²⁴⁰

§ 13. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermitteln oder den Zugang zu einem Kommunikationsnetz vermittelt, ist für die übermittelten Informationen nicht verantwortlich, sofern er

- 1. die Übermittlung nicht veranlasst,*
- 2. den Empfänger der übermittelten Informationen nicht auswählt und*
- 3. die übermittelten Informationen weder auswählt noch verändert.*

(2) Die Übermittlung von Informationen und die Vermittlung des Zugangs im Sinn des Abs. 1 umfassen auch die automatische kurzzeitige Zwischenspeicherung der übermittelten Informationen, soweit diese Zwischenspeicherung nur der Durchführung der Übermittlung im Kommunikationsnetz dient und die Information nicht länger gespeichert wird, als es für die Übermittlung üblicherweise erforderlich ist.

Unterlassungsansprüche gegen Access-Provider im Zusammenhang mit rechtsverletzenden Websites erscheinen auf den ersten Blick wenig zielführend, weil Host-Provider für Rechte-

²³⁷ Vgl auch *Handig*, Die Nutzung des World Wide Web aus urheberrechtlicher Sicht Rechtslage nach der UrhG-Nov 2003, ÖBl 2004, 196 (202), der das Konzept der „bewussten Förderung“ für sonstige Beitragstätter mit der Haftungssituation der Dienstleister nach dem ECG vergleicht; ebenso *Kasper*, Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 1 (4).

²³⁸ Vgl *Zankl*, Haftung und Haftungsbefreiung im E-Commerce, ecolex 2005, 202; aA *Kasper*, Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 1 (3).

²³⁹ *Schanda*, Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, ecolex 2001, 920.

²⁴⁰ Dieser Teil der vorliegenden Arbeit wurde in gekürzter und adaptierter Form vorab veröffentlicht: *Steinhofer/Feiler*, Urheberrechtliche Ansprüche auf die Sperrung von Websites durch Access-Provider, MR 2010, 322.

inhaber das deutlich „attraktivere“ Ziel sind. Es ist nämlich bedeutend effektiver, an der Quelle der Rechtsverletzung anzusetzen, als mühsam alle möglichen Zugänge zu rechtsverletzenden Websites zu unterbinden. Da alleine in einem kleinen Land wie Österreich über hundert Unternehmen aktiv sind, die Access-Providing anbieten²⁴¹, müssten betroffene Rechteinhaber großen Aufwand treiben, um alle potentiellen Kanäle zur Seite zu kappen.

Bei rechtsverletzenden Websites, bei denen nicht nur der Betreiber, sondern auch der Host-Provider nicht greifbar ist, könnte der Zugriff auf den jeweiligen Access-Provider für Rechteinhaber aber noch allemal besser als nichts sein. Die Verbreitung illegaler Inhalte verlagert sich mit dem Zuwachs der verfügbaren Übertragungsraten nämlich zunehmend von Filesharing-Diensten, bei denen die einzelnen Nutzer das Film- oder Musikmaterial auf ihren jeweiligen Computern speichern, hin zu Streaming-Websites²⁴² (zB <megavideo.com>), bei denen Filme abgerufen und angesehen werden können, ohne dass man sie zuerst herunterladen müsste. Ebenfalls immer beliebter werden Downloadplattformen wie <rapidshare.com>, die Datenspeicher für Uploads zur Verfügung stellen. Um die gewünschten Inhalte zu finden, verwenden Nutzer meist Link-Provider (zB <kino.to>), die Links zu den von den Host-Providern zur Verfügung gestellten Inhalten bereithalten.

Die Host-Provider solcher Websites, die man nach dem oben dargestellten Muster früher oder später wohl dazu heranziehen könnte, die problematischen Inhalte vom Netz zu nehmen, sitzen vermehrt aber ebenfalls im Ausland und sind daher nicht greifbar.²⁴³ Die Frage einer Gehilfenhaftung für Access-Provider, die in der bisherigen österreichischen Lit nur am Rande und vornehmlich skeptisch²⁴⁴ behandelt wurde, könnte daher vermehrt in den Mittelpunkt der Diskussion rücken. Unterlassungsanordnungen gegen Access-Provider, durch die der Zugang zu bestimmten Websites erschwert werden soll, werden in der Diskussion häufig auch „Websperren“ oder „Sperransprüche“ genannt. Vor der Analyse, ob diese nach österrei-

²⁴¹ Stand 1. November 2010; vgl die Mitgliederliste der ISPA, abrufbar unter <ispa.at/mitglieder/mitgliederliste/>.

²⁴² Streaming bedeutet die kontinuierliche Versorgung eines Clients mit Daten, vergleichbar einem herkömmlichen Radio- oder TV-Programm, kann aber anders als diese durchaus individuelle Inhalte auf Abruf bereitstellen (Unterschied zum Rundfunk, der ein vorgefertigtes Programm sendet, das der Endnutzer nicht beeinflussen kann). Ein prominentes Beispiel dafür sind die Videos auf <youtube.com>. Zur reibungslosen Funktion des Streams ist es notwendig, dass einzelne Datenpakete in eine Abspielsoftware, zB MediaPlayer, geladen und dort zwischengespeichert werden. Während die bereits abgerufenen Inhalte abgespielt werden, holt sich das Programm die nächsten Datenpakete aus dem Stream und ersetzt die bereits zwischengespeicherten Elemente.

²⁴³ Eine Alternative könnte in Österreich zwar noch die Domain-Vergabestelle sein, die nach der Rsp des OGH in den fpo.at-Fällen (FN 193) bei offenkundigen Rechtsverletzungen zur Sperre von Domains verpflichtet ist. Für die Praxis relevante Websites sind aber idR nicht unter österreichischen oder europäischen Domains abrufbar, wodurch auch diese Möglichkeit wegfällt.

²⁴⁴ *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (27); *Schnider*, Killer-Spiele: Deutsche Regeln treffen Österreich, Rechtspanorama, Die Presse 21.6.2009; bezogen auf Filesharing-Sachverhalte: *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 3.

chischem Recht zulässig sind, lohnt sich zunächst ein Blick auf den technischen Hintergrund derartiger „Sperrungen“ sowie auf die einschlägige Entwicklung in Deutschland.

C.II.2.c.2.1. Exkurs: Technischer Hintergrund

Technisch ist vorzuschicken, dass ein Access-Provider keine Möglichkeit hat, eine rechtsverletzende Website in dem Sinn zu „sperrern“, dass sie überhaupt nicht mehr abgerufen werden kann. Diese Möglichkeit bleibt der physischen Löschung der Inhalte vorbehalten, die aber nur die Websitebetreiber selbst bzw deren Host-Provider vornehmen können. Der Access-Provider kann lediglich Maßnahmen setzen, um seinen Kunden den Zugang zu bestimmten Websites zu erschweren.

Dabei bestehen drei verschiedene technische Möglichkeiten, wovon jede unterschiedliche Charakteristika aufweist:

DNS-Sperrungen sind für einen Access-Provider am leichtesten zu implementieren. Für den Betreiber der betroffenen Website sind sie nur durch den Wechsel des Domainnamens, für den Nutzer jedoch sehr leicht zu umgehen: Das Domain Name System (DNS) ermöglicht die Übersetzung von Domainnamen (zB <kino.to>) in IP-Adressen, die für einen Nutzer erforderlich sind, um eine Verbindung mit der Website herzustellen.²⁴⁵ Jeder Access-Provider betreibt für seine Kunden einen DNS-Server, der durch eine wenig aufwändige Rekonfiguration daran gehindert werden kann, einen Domainnamen in die korrekte IP-Adresse aufzulösen.²⁴⁶ Findet der DNS-Server für eine aufgerufene Domain keinen Eintrag, so kann der Zugang zu der Website nicht hergestellt werden. Man kann diese Situation mit einem elektronischen Telefonbuch vergleichen, in dem Namen und Telefonnummern verknüpft werden. Fehlt die Telefonnummer, kann der Suchende den Kontakt zum gewünschten Gesprächspartner nicht herstellen, so er nicht auf alternativem Weg die Telefonnummer ermitteln und direkt eintippen kann. Obwohl in der Praxis nahezu alle Kunden eines Access-Providers dessen DNS-Server verwenden, kann ein PC durch wenige Klicks so konfiguriert werden, dass er einen alternativen DNS-Server verwendet.

IP-Sperrungen sind für Access-Provider mit mehr Aufwand verbunden und für Nutzer – jedoch nicht für den Betreiber der betroffenen Website – schwerer zu umgehen. Da jedem Internetteilnehmer grds eine eindeutige IP-Adresse zugewiesen ist (zB 91.217.178.230 im Falle von <kino.to>), kann durch die Unterbindung der Weiterleitung von Datenpaketen an eine bestimmte IP-Adresse eine unmittelbare Kommunikation mit dem hierdurch identifizierten Server unterbunden werden. Dies erfordert, dass der Access-Provider seine zahlreichen Router entsprechend konfiguriert, was im Vergleich zur Konfiguration eines einzigen DNS-Servers mit

²⁴⁵ Eine kurze Einführung in DNS bietet *Liu/Albitz, DNS and BIND*⁵ (2006) 4 ff.

²⁴⁶ Hierzu ist es schlicht erforderlich, die zu sperrende Domain auf dem DNS-Server (mit einer falschen IP-Adresse) als reguläre Domain anzulegen. Vgl *Liu/Albitz, DNS and BIND*⁵ (2006) 54 ff.

weitaus größerem Aufwand verbunden ist. Eine Umgehung einer IP-Sperre ist für Nutzer nur möglich, indem sie ihren Datenverkehr über einen Proxy-Server oder einen Anonymisierungsdienst²⁴⁷ leiten, was meist mit erheblichen Einbußen in der verfügbaren Bandbreite verbunden ist. Dies kann die Inanspruchnahme von Diensten von Download- oder Streaming-Plattformen – jedoch nicht jene von Link-Providern wie <kino.to> – nahezu unmöglich machen. Aus Sicht des Betreibers einer von einer IP-Sperre betroffenen Website ist anzumerken, dass die Sperre durch den Wechsel der verwendeten IP-Adressen leicht umgangen werden kann.²⁴⁸ Der Access-Provider müsste demgegenüber die gesperrte IP-Adresse laufend überwachen und anpassen, um die Effektivität der Maßnahme zu gewährleisten. Schließlich ist darauf hinzuweisen, dass eine IP-Adresse nicht notwendigerweise nur von einer Website verwendet wird,²⁴⁹ sodass eine IP-Sperre potentiell auch Websites, die in keinerlei Zusammenhang mit der Rechtsverletzung stehen, miterfasst.²⁵⁰

Die dritte Möglichkeit, eine Website zu „sperren“ besteht für einen Access-Provider darin, den Web-Datenverkehr (dh Datenverkehr über den Port 80) aller Kunden zwangsweise über einen eigenen Proxy-Server umzuleiten, der eine entsprechende Filterung anhand von URLs vornimmt (Zwangs-Proxy). Diese Form der Sperre ist aus Sicht der Nutzer ähnlich effektiv wie IP-Sperren, lässt sich von Betreibern gesperrter Websites jedoch dadurch leicht umgehen, dass sie ihre Website auf einem alternativen Port betreiben.²⁵¹ Die Verwendung von Proxy-Servern durch den Access-Provider ist die technisch aufwändigste und mit Abstand kostenintensivste Möglichkeit, weil sie enorme Rechenkapazitäten und eine Restrukturierung der Netzwerkarchitektur erfordern würde.

Zusammenfassend gilt, dass IP-Sperren und Zwangs-Proxies relativ leicht durch den Betreiber der gesperrten Website (jedoch nicht durch die Nutzer) umgangen werden können. Demgegenüber können DNS-Sperren sehr leicht durch Nutzer (jedoch nicht durch den Betreiber

²⁴⁷ Der wohl bekannteste Anonymisierungsdienst ist Tor. Er wurde von der Electronic Frontier Foundation entwickelt: <torproject.org>.

²⁴⁸ So sind selbst stündliche Änderungen der verwendeten IP-Adressen denkbar. Bevor eine neue IP-Adresse gesperrt werden kann, wird zu überprüfen sein, ob diese tatsächlich von der zu sperrenden Website verwendet wird, widrigenfalls es zur versehentlichen Sperrung unbeteiligter IP-Adressen kommen kann.

²⁴⁹ Beispielsweise verwendet der Link-Provider <movie-dvdrip-rapidshare.blogspot.com> (ein kleiner Blog, der rechtswidrige Links zu urheberrechtlich geschützten Filmen bereithält) dieselbe IP-Adresse wie hunderte andere (rechtmäßige) Blogs, die von Blogspot gehostet werden.

²⁵⁰ So geschehen im Fall dreier Erotikseiten und dem Access-Provider Arcor, wo 3,5 Millionen hauptsächlich unbedenkliche Websites vorübergehend nicht erreichbar waren; siehe *Lischka*, Fehlerhafte Zensur-Methode: Arcor stoppt den Porno-Filter, SPIEGEL ONLINE vom 17.9.2007, abrufbar unter <spiegel.de/netzwelt/web/0,1518,506143,00.html>. Zu diesem Problem bereits *Schöttle*, Sperrverfügungen im Internet: Machbar und verhältnismäßig? K&R 2007, 366 (367); *Sieber/Nolde*, Sperrverfügungen im Internet 186.

²⁵¹ So bereits *Schneider*, Sperren und Filtern im Internet, MMR 2004, 18 (23). Wird zB die Website example.com auf dem Port 1234 statt 80 betrieben, so lautet die URL „http://example.com:1234/“ statt „http://example.com/“.

der gesperrten Website) umgangen werden. Im Ergebnis ist die Effektivität aller drei Möglichkeiten einer Sperre daher ähnlich gering.²⁵² Bezüglich der Eingriffsintensität ist zu bemerken, dass die Kosten einer IP-Sperre oder gar eines Zwangs-Proxy ein Vielfaches der Kosten einer DNS-Sperre betragen. Weiters ist bei IP-Sperren die Wahrscheinlichkeit der versehentlichen Sperrung Websites Dritter ungleich größer.

C.II.2.c.2.2. Exkurs: Websitesperren in Deutschland

Die Debatte rund um eine mögliche Sperrpflicht für Access-Provider wurde in Deutschland durch eine Abmahnwelle der deutschen Verwertungsgesellschaft GEMA ausgelöst. Die GEMA forderte in ihren Schreiben an sämtliche Access-Provider, dass diese die Verbindung zu diversen Downloadportalen nicht mehr herstellen, weil dort urheberrechtsverletzende Werke angeboten und die Provider sich andernfalls als Mitstörer schuldig machen würden.²⁵³ Zu einschlägigen gerichtlichen Entscheidungen kam es aber erst, nachdem der Konflikt in die Erotikbranche getragen wurde.

C.II.2.c.2.3. LG Frankfurt - “youporn.com I + II”

Der Access-Provider Arcor sperrte im September 2007 nach Aufforderung der Kirchberg Logistik GmbH, eines Anbieters von kostenpflichtigem pornografischen Material, freiwillig den Zugang zu Erotikplattformen, darunter <youporn.com>, weil diese gegen deutsches Jugendschutzrecht verstießen. Dabei sperrte Arcor den gesamten IP-Bereich der Websites, was dazu führte, dass auch zahlreiche unbedenkliche Angebote (~ 3.5 Millionen Seiten), die am selben Server gespeichert waren, durch die Kunden von Arcor nicht mehr aufgerufen werden konnten. Aufgrund dieser unbeabsichtigten Kollateralschäden und ihrer technischen Unzulänglichkeit (es reichte ein Wechsel der IP-Adresse des Servers, um die Seiten wieder erreichbar zu machen) hob Arcor die Sperre nach einer knappen Woche wieder auf.

Es folgte eine Klage mit Antrag auf Erlassung einer EV gegen Arcor seitens der Kirchberg Logistik GmbH vor dem LG Frankfurt.²⁵⁴ Darin wurde gefordert, dass Arcor es im geschäftlichen Verkehr unterlasse, Nutzern den Zugang zum Internet zu ermöglichen, ohne gleichzeitig den Zugang dieser Nutzer zur Website <youporn.com> zu sperren, solange auf dieser pornografische Darbietungen ohne jegliche Zugangsbeschränkung oder persönlichen Altersnachweis verbreitet werden oder tierpornographische Darbietungen verfügbar sind. Dem Eilan-

²⁵² Zu berücksichtigen ist, dass die Umgehung einer IP-Sperre oder eines Zwangs-Proxys uU zwar schwerer ist als jene einer DNS-Sperre, jedoch automatisch für alle Nutzer den Zugang wieder freigibt, wenn sie erfolgreich ist.

²⁵³ Diese Argumentation stützt sich auf die sehr weite Mitverantwortlichkeit von Internetversteigerungsplattformen (eBay etc) in der Rsp des BGH (vgl FN 284); siehe dazu *Kamlah*, Müssen Access-Provider den Zugang ins Internet filtern?, MR-Int 2005, 97 und *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26).

²⁵⁴ Sämtliche Nennungen beziehen sich auf das LG bzw OLG Frankfurt am Main.

trag wurde vom LG Frankfurt ohne mündliche Verhandlung stattgegeben, wobei sich die Begründung auf die Nennung der wettbewerbsrechtlichen Bestimmungen beschränkte und sich dabei offensichtlich auf Rechtsbruch als wettbewerbsrechtliche Fallgruppe stützte.²⁵⁵ Arcor kam dem so erteilten Auftrag des Gerichtes durch eine DNS-Sperre von <youporn.com> nach.²⁵⁶

Im Hauptverfahren wurde die EV dagegen nach eingehender Diskussion der Rechtslage aufgehoben und eine Sperre abgelehnt.²⁵⁷ Das Gericht hielt fest, dass – neben der Rolle als Täterin – auch eine Gehilfenstellung von Arcor ausscheide, obwohl spätestens als Folge der Abmahnung bedingter Vorsatz, der das Bewusstsein der Rechtswidrigkeit einschließe, vorliegen könnte. Die Unterstützungshandlung – Vermittlung des Zugangs zu den Inhalten – sei nämlich Unternehmensgegenstand der Beklagten. Wenn dies der Fall sei, könne die objektiv gegebene – möglicherweise neutrale – Unterstützungshandlung nicht automatisch die Gehilfenstellung im strafrechtlichen Sinne bedeuten. Das Verhalten müsse zusätzlich als auf Grund der Gesamtumstände rechtswidrig bewertet werden, weswegen eine Abwägung nach den Grundsätzen der Störerhaftung vorzunehmen sei. Die für letztere notwendige „willentliche, adäquate-kausale“ Mitwirkung an der Herbeiführung oder Aufrechterhaltung einer rechtswidrigen Beeinträchtigung betreffe das Element der Zurechenbarkeit. Arcor stehe zu dem Betreibern der beanstandeten Website in keiner rechtlichen, vertraglichen Beziehung, sie kenne ihn nicht einmal. Die rechtliche Möglichkeit zur Verhinderung dieser eingegebenen Inhalte, zu denen sie den Zugang vermittelt, habe sie nicht. Funktion und Aufgabenstellung von Arcor sei Grundlage der modernen Kommunikationsinfrastruktur „Internet“ mit der Möglichkeit des grds freien Zugangs durch Betreiber und Nutzer. Berücksichtigt man diese Umstände, sei die Zugangsvermittlung durch den Access-Provider in der Tat eine inhaltsneutrale Dienstleistung. Man könne allenfalls daran denken, die Störerhaftung auf klare eindeutige Rechtsverletzungen zu beschränken. Da aber zahlreiche Problembereiche wie das Herunterladen von Musikdateien, Hackeranleitungen oder extremistische Inhalte im Rahmen eines Sperrungsverlangens auf den Access-Provider zukommen könnten und deren Überprüfung nicht mit dessen Funktion und Aufgabenstellung vereinbar sei, sei das Ergebnis der Abwägung, dass Arcor für die rechtswidrigen Inhalten auf der Website <youporn.com> nicht mitverantwortlich ist. Sie sei keine wettbewerbsrechtliche Störerin und nehme insoweit auch keine (rechtswidrige) Gehilfenstellung ein.

Im Übrigen stützte sich das Gericht in seiner Begründung auf die zwischenzeitlich ergangene Entscheidung des OLG Frankfurt im Fall Huch vs Arcor, in dem die Sperre von google.de und

²⁵⁵ LG Frankfurt aM 17.10.2007, 2/6 O 477/07 (youporn.com I).

²⁵⁶ Vgl heise online vom 24.10.2007: <heise.de/newsticker/meldung/Arcor-installiert-leicht-umgehbare-Netzsperrre-fuer-YouPorn-188617.html>.

²⁵⁷ LG Frankfurt aM 8.2.2008, 3-12 O 171/07 (youporn.com II).

google.com begehrt wurde (dazu sogleich). Weitere von der Kirchberg Logistik GmbH angestregte Sperren von youporn.com wurden in Verfahren gegen die Access-Provider KielNet²⁵⁸ und Tele2²⁵⁹ von den befassen Gerichten bereits davor mit ähnlichen Begründungen abgelehnt. Arcor entfernte alle bereits gesetzten DNS-Sperren wieder.

C.II.2.c.2.4. LG & OLG Frankfurt - „google“

Das Erotikunternehmen Huch Medien GmbH brachte nach der (stattgebenden) „youporn.com I“-Entscheidung des LG Frankfurt vor ebendiesem eine Klage mit Antrag auf EV gegen Arcor ein. Arcor wurde darin aufgefordert, den Zugang zu den Websites <google.com> und <google.de> zu sperren, weil über diese Suchmaschinen eindeutig pornographische Inhalte für Minderjährige ohne jegliche Zugangsbeschränkungen abrufbar seien. Das Urteilsbegehren lehnte sich stark an die Klagsführung der Kirchberg-Gruppe im Fall <youporn.com> an, weil der Geschäftsführer der Huch Medien GmbH, *Tobias Huch*, damit die generelle Einstellung der deutschen Gerichte zur Informationsfreiheit im Internet testen wollte.²⁶⁰

Das LG Frankfurt²⁶¹ führte in seiner Begründung aus, dass Arcor als Access-Provider nicht als unmittelbarer Täter von Wettbewerbsverstößen in Betracht komme, weil sie selbst keine pornographischen Schriften oder Bilder im Internet anbiete. Für die Qualifikation als Teilnehmer an Wettbewerbsverstößen mangle es an einer irgendwie geartete Teilnahmehandlung. Eine Beihilfe durch Unterlassung setze das Bestehen einer Garantenstellung voraus, die in Bezug zur Antragstellerin nicht ersichtlich sei; es liege seitens des Access-Providers auch keine Wettbewerbshandlung vor, was zur Einordnung in die wettbewerbsrechtliche General Klausel aber Voraussetzung sei.

Bemerkenswert ist, dass das Gericht auch keinen Fall der Störerhaftung auf Unterlassung erkennen konnte. Voraussetzung dafür sei nämlich, dass der Inanspruchgenommene eine zurechenbare Ursache für eine Verletzung von Rechten des Anspruchstellers durch den eigenverantwortlich handelnden Dritten gesetzt hat und zudem die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte. Arcor habe aber keine zurechenbare Ursache für die rechtswidrigen (pornographischen) Angebote Dritter gesetzt. Die Handlungen der Websitebetreiber von <google.de> und <google.com> oder die über diese Suchmaschinen erreichbaren Websites seien Arcor nicht zuzurechnen. Arcor stehe zu diesen in keinerlei vertraglicher Beziehung, sondern ermögliche lediglich den Zugang zu ihnen. Insoweit sei ihre Leistung

²⁵⁸ LG Kiel 23.11.2007, 14 O 125/07 (KielNet).

²⁵⁹ LG Düsseldorf 13.12.2007, 12 O 550/07 (Tele2).

²⁶⁰ Die Online-Enzyklopädie Wikipedia spricht daher von einem „Scheinprozess“: <de.wikipedia.org/wiki/Tobias_Huch#Scheinprozess_gegen_Arcor_zur_Sperrung_von_Google>; vgl auch heise online vom 4.12.2007: <heise.de/newsticker/meldung/Arcor-soll-Google-sperren-166845.html.>.

²⁶¹ LG Frankfurt aM 5.12.2007, 2-03 O 526/07 (google).

inhaltsneutral. Das bloße Internet-Angebot eines konkreten Anschlusses zur Telekommunikation könne nicht als eine von dem Anbieter der Kommunikationsleistung zu verantwortende Verletzungshandlung qualifiziert werden.

Das von Huch als Berufungsinstanz angerufene OLG Frankfurt bestätigte diese Entscheidung.²⁶² Der befasste Senat prüfte insbesondere eine Übertragbarkeit der vom BGH entwickelten Rsp zur Störerhaftung von Host-Providern (Online-Auktionsplattformen) auf Arcor in ihrer Rolle als Access-Provider.²⁶³ Das handelnde Unternehmen müsse demnach im eigenen geschäftlichen Interesse in seinem Verantwortungsbereich selbst eine Gefahrenquelle für Wettbewerbsverstöße durch Dritte schaffen. Das sei beim Betrieb einer Internet-Auktionsplattform wie eBay gegeben, weil der Betreiber einer solchen Plattform seinen Kunden die Verbreitung von erfahrungsgemäß riskanten Inhalten ermögliche und damit eine Gefahrenquelle eröffne. Dies rechtfertige, dem Urheber in den engen Grenzen des Zumutbaren eine wettbewerbsrechtliche Verkehrspflicht und damit eine Mithaftung für Wettbewerbsverstöße aufzuerlegen, die ihren Ursprung in dieser Gefahrenquelle haben.

Damit sei die Stellung und geschäftliche Tätigkeit von Arcor nicht zu vergleichen. Die Kunden des Access-Providers seien, auch wenn sie gegen entgeltliche Inanspruchnahme von dessen Diensten auf rechtswidrige Inhalte stoßen, nicht Urheber dieser Wettbewerbsverstöße, sondern allenfalls deren Nutznießer oder Opfer. Damit eröffne Arcor nicht in ihrem eigenen Verantwortungsbereich eine Gefahrenquelle für Wettbewerbsverstöße, sondern ermögliche nur den Zugang zu Wettbewerbsverstößen, die aus einer von einem Dritten eröffneten Gefahrenquelle herrühren. Nach Ansicht des Senates rechtfertigen es praktische Schwierigkeiten bei der Verfolgung der unmittelbaren Täter nicht, Dritte auch dann zur Verantwortung zu ziehen, wenn sich ihr Mitwirken am Eintritt des Wettbewerbsverstoßes auf einen derart untergeordneten Beitrag beschränkt wie im vorliegenden Fall.

Selbst wenn man abweichend von dieser Meinung dem Access-Provider eine Verkehrssicherungspflicht grds auferlegen wollte, würde eine Haftung von Arcor daran scheitern, dass eine Sperrung des Zugangs zu den beanstandeten Websites unzumutbar wäre, weil es nicht ersichtlich sei, dass Arcor den Zugang zu <google.com> oder <google.de> unter Aussparung der beanstandeten Teile dieser Seiten ermöglichen könnte. Vielmehr müsste Arcor zur Befolgung eines etwaigen Verbots ihren Kunden den Zugriff zu den beiden google-Seiten vollständig unmöglich machen, solange dort Inhalte der beschriebenen Art auffindbar sind. Das sei Arcor im Hinblick auf die Wichtigkeit von Google als - aus Sicht der Kunden - unverzichtbare Suchmaschine nicht zuzumuten.

²⁶² OLG Frankfurt aM 22.1.2008, 6 W 10/08 (google).

²⁶³ Vgl FN 284.

C.II.2.c.2.5. LG Hamburg – „DNS-Sperren I“

Eine erste immaterialgüterrechtliche Leitentscheidung gab es einem Verfahren diverser führender Filmstudios und Filmverleihe gegen einen Hamburger Access-Provider vor dem LG Hamburg.²⁶⁴ Die Kläger forderten in ihrem Begehren, dass der Access-Provider seinen Kunden den Zugang zu einer in Indien registrierten Website sperren solle, weil auf dieser Website urheberrechtsverletzende Filme als Streams abrufbar waren, die dadurch von den Kunden der Beklagten – jedenfalls vorübergehend – vervielfältigt würden. Weder Betreiber noch Host-Provider der Website konnten ermittelt bzw zur Entfernung der Inhalte bewegt werden. Der Klage war eine entsprechende Abmahnung vorhergegangen. Technisch war die Website im Übrigen so gestaltet, dass die zum Abruf angebotenen Filmdateien nicht unmittelbar auf dem Server der Website lagerten, sondern von der Website auf weltweit verstreute Server verlinkt wurde.

Das Gericht stellte zunächst fest, dass keine ausdrückliche gesetzliche Anspruchsgrundlage zur Sperrung des Zugangs zu einem Internetauftritt vorhanden sei. Eine Haftung des Access-Providers als Täter oder Teilnehmer an den seinen Kunden vorgeworfenen rechtsverletzenden Vervielfältigungen der Filme liege nicht vor, weil sein Dienst sich auf das passive automatische Verfahren der Durchleitung von fremden Informationen beschränke. In Betracht komme daher nur eine Verpflichtung nach den Regeln der Störerhaftung.

Anders als in den oben dargelegten (wettbewerbsrechtlichen) Entscheidungen qualifizierte das Gericht hier die Dienstleistung des Access-Providers als adäquat kausal für die geltend gemachten Rechtsverletzungen.²⁶⁵ Das Gegenargument, das es mit dem sozial erwünschten Geschäftsmodell der Access-Providers nicht vereinbar sei, diese zur Prüfung einer Flut von Ansprüchen gegen alle im Internet stattfindenden Verstöße gegen deutsches Recht zu verpflichten, verkenne – so das Gericht - die insoweit wertfreie Voraussetzung der Adäquanz eines ursächlichen Verhaltens. Das Korrektiv gegen eine ausufernde Haftung müsse vielmehr die Prüfung der Zumutbarkeit sein. Der Ansatz, den Verursachungsbeitrag der gebilligten und erwünschten Tätigkeit des Access-Providers bereits bei der Adäquanzprüfung dahingehend zu berücksichtigen, dass dieser Beitrag das allgemeine Lebensrisiko womöglich gar nicht in beachtlicher Weise erhöht habe, komme in der Rsp des BGH nicht zum Tragen.

²⁶⁴ LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I).

²⁶⁵ Zum selben Ergebnis kam das OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 55, wenn auch mit ausführlicherer Begründung: „Die Eröffnung des Zugangs zum Usenet schließt schon allgemein die nicht fern liegende Möglichkeit ein, dass es hierbei zu Rechtsverletzungen der vorliegenden Art kommen kann. Es ist allgemein - und damit umso mehr den Antragsgegnern - bekannt, dass sich über das Usenet rechtsverletzende Inhalte (und darunter urheberrechtlich geschützte Musikdateien) in erheblichem Umfang zugänglich machen lassen und zugänglich gemacht werden. Entsprechend adäquat kausale Zusammenhänge bestehen unzweifelhaft bei nahezu jedem Access-Provider, auch außerhalb einer Zugangsvermittlung gerade zum Usenet.“

Die Frage der Störerhaftung des Access-Providers entscheide sich daher bei der Voraussetzung(en)²⁶⁶ der technischen Möglichkeit und der Zumutbarkeit der mit der begehrten Sperrungsanordnung verbundenen Pflichten.

Zwar sei in jedem Fall ein Anspruch auf eine unmögliche Leistung ausgeschlossen. Die Sperrung sei aber (technisch) möglich, weil nach Auffassung des Gerichts dafür nicht nötig ist, dass die Erreichbarkeit einer rechtswidrigen Information endgültig verhindert wird. Es reiche vielmehr, wenn eine Zugangsbeschränkung im Sinne einer Erschwerung herbeigeführt werden könne. Allfällige Umgehungsmöglichkeiten und die Frage der überschießenden Sperrung anderer Inhalte seien nicht bei der Prüfung der Möglichkeit, sondern wiederum bei der im Rahmen der Zumutbarkeit anzustellenden Verhältnismäßigkeitsprüfung zu berücksichtigen.

Im letzten Schritt prüfte das Gericht daher die mit einer etwaigen Sperrungsanordnung verbundenen Pflichten unter Berücksichtigung aller betroffenen Interessen und relevanten rechtlichen Wertungen. Dabei betonte es, dass absolute Rechte im Bereich des Immaterialgüterrechts in gleicher Weise zu beurteilen seien wie wettbewerbliche Verkehrspflichten. Das Interesse der klagenden Rechteinhaber sei dadurch geprägt, dass in ihre urheberrechtlichen Nutzungsrechte eingegriffen und dadurch die wirtschaftliche Auswertung der Filme behindert werde. Da Host-Provider und Websitebetreiber nicht greifbar seien, stelle eine Zugangssperre die einzige Möglichkeit dar, weiteres Herunterladen zu unterbinden.²⁶⁷

Für den belangten Access-Provider spreche, dass dieser lediglich ein automatisch ablaufendes Verfahren zur Verfügung stelle, welches den Kunden den Zugriff auf die Internetinhalte vermittele. Dieser passiv neutral-automatische Beitrag sei nicht mit dem eines Auktionsplattform-Betreibers oder Forenbetreibers vergleichbar. Während diese selbst die Gefahrenquelle für Rechtsverletzungen gesetzt haben, es ihnen gerade auch auf die Inhalte ankommt und sie die Möglichkeit einer besseren Beeinflussung und Kontrolle haben, hätten Access-Provider einen deutlich größeren Abstand zu den rechtsverletzenden Inhalten, wodurch auch die Zumutbarkeitsgrenzen eingengt werden.²⁶⁸ Ohne dies explizit zu sagen, differenziert das Gericht damit im Ergebnis – wie schon das OLG Frankfurt im Fall „google“ – zwischen Host- und Access-Providern.

²⁶⁶ Das Gericht verwendet hier im Original die Einzahl, prüft die beiden genannten Punkte danach aber getrennt.

²⁶⁷ Bedauerlich ist, dass das LG Hamburg an dieser Stelle nicht darauf eingeht, ob die Kunden des beklagten Access-Providers tatsächlich als unmittelbare Täter in die Verwertungsrechte der Rechteinhaber eingreifen. Näher liegt nämlich die Formulierung des OLG Frankfurt im Fall „google“, wonach die Kunden nicht Urheber der Rechtsverletzungen, sondern allenfalls deren Nutznießer sind. Dies wird bei der Frage der Übertragbarkeit auf österreichisches Recht (siehe unten) noch zu berücksichtigen sein.

²⁶⁸ Anders ist dies nach OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 63, wenn der Access-Provider selbst Werbung für die rechtsverletzende Verwendung seiner Dienstleistung macht. Darunter fällt, wenn er (wie im Anlassfall) sein Angebot dadurch potentiellen Kunden schmackhaft macht, dass sie ohne Risiko und kostenfrei urheberrechtlich geschütztes Material herunterladen könnten.

Da der Access-Provider seinen Kunden vertraglich den ungehinderten Zugang zum Internet schulde, bedürfe es einer wirtschaftlich aufwendigen, umfassenden sachlichen und rechtlichen Prüfung, wenn die Kunden beim Aufruf einer bestimmten Website eine Rechtsverletzung begehen und Dritte Sperren verlangen.²⁶⁹ Es seien Dinge wie Aktivlegitimation von Antragstellern und der Umfang der möglichen Rechtsverletzungen zu beurteilen. Durch die dafür notwendige zusätzliche Infrastruktur würden dem Access-Provider zusätzliche Aufgaben abverlangt, die von dessen Kerngeschäft abweichen.

Schließlich sei im Rahmen der Zumutbarkeitsprüfung die Eignung der in Betracht kommenden Maßnahme (hier: DNS-Sperre) zu berücksichtigen. Denn je geringer die Eignung sei, umso weniger könne vom Access-Provider unter Berücksichtigung des dargestellten zusätzlichen Aufwandes die Einrichtung einer solchen Sperre verlangt werden. Eine DNS-Sperre sei zur Verhinderung des Zugriffs auf einen Internetauftritt nur beschränkt geeignet, weil es selbst dem Gericht binnen weniger Minuten gelungen sei, eine Internetseite mit einer Anleitung zur Umgehung der Sperre mit verfügbaren Name-Servern zu finden. Internetaktiven Jugendlichen und jungen Erwachsenen dürfte dies im Zweifel noch schneller gelingen.

Insgesamt sei unter Berücksichtigung der eingeschränkten Wirkung der geforderten DNS-Sperre, der durch die rein objektive Unterstützung der behaupteten Verletzungshandlungen durch die Antragsgegnerin eingeschränkten Zumutbarkeit und des Prüfungsaufwandes auch unter Berücksichtigung der Interessen der Antragstellerinnen ein Anspruch aus Störerhaftung zu verneinen.

Das LG Hamburg lehnte daher einen Anspruch auf DNS-Sperren ab.

C.II.2.c.2.6. LG München – „Keine DNS-Sperren im UWG“

Kläger war hier ein Interessensverband von gewerblich tätigen Vermietern und Verkäufern von CDs, Videofilmen und Computerspielen. Beklagter war ein Access-Provider, dem vorgeworfen wurde, die Verbindung zu einer Website herzustellen, auf der „Raubkopien“ von Filmen zum Download angeboten wurden. Das befasste LG München²⁷⁰ verneinte die begehrte DNS-Sperre aus dem Titel des Wettbewerbsrechts bereits aufgrund des mangelnden Wettbewerbsverhältnisses zwischen dem Kläger bzw dessen Mitgliedern und dem beklagten Access-Provider.

Das Gericht prüfte in weiterer Folge weiters eine mögliche Verantwortlichkeit aus dem Titel der Störerhaftung. Der Beklagte müsste dafür willentlich und adäquat kausal an den rechtswidrigen Handlungen von Websitebetreibern bzw seinen Kunden durch seine Vermittlungs-

²⁶⁹ Diese umfassende Prüfung wird mE noch wirtschaftlich unzumutbarer, wenn gar nicht die Kunden des prüfpflichtigen Providers, sondern (nur) diesem unbekannte Dritte die Rechtsverletzungen setzen, weil der Access-Provider dadurch noch weiter von der Quelle der Rechtsverletzung entfernt ist.

²⁷⁰ LG München 3.9.2009, 4 HKO 16685/08.

tätigkeit mitgewirkt haben. Dabei müsste für den Access-Provider eine grds gegebene Verpflichtung zum Einschreiten, also das Unterbinden der Zugangsmöglichkeiten zu den betreffenden Seiten auch zumutbar sein, wobei objektive und subjektive Umstände zu prüfen seien.

Zunächst müsse eine positive Kenntnis des Access-Provider von der Rechtswidrigkeit der Seiten-Inhalte bestehen, was durch eine entsprechende Mitteilung seitens des Klägers erfolgt sei. Dabei sei aber bereits im Rahmen der Zumutbarkeitserwägungen zu bedenken, dass die Richtigkeit solcher Mitteilungen ohne Bestandsgarantie ist, weil die Inhalte der Seiten jederzeit geändert werden können und die Beklagte nicht veranlasst sein darf, ihren zahlenden Kunden Seiten mit erlaubten Inhalte vorzuenthalten. Damit wäre eine ständige Überprüfung durch die Beklagte, die auf die Inhalte der Seiten keinerlei Einfluss hat, erforderlich, die einen Aufwand notwendig macht, der unter Berücksichtigung des, wenn überhaupt nur relativ geringfügigen Tatbeitrags des Access-Providers bei der Verbreitung rechtswidriger Inhalte von Internetseiten bloß durch Bereitstellung des Zugangs nicht zumutbar erscheint.

Dazu komme, dass nach dem Stand der Technik grds die Sperrung eines DNS-Zugangs zwar technisch möglich, aber auch ohne Probleme zu umgehen ist, und auch damit die verlangte Handlung unter Berücksichtigung des vorgenannten Aufwands und des damit tatsächlich erreichbaren Ergebnisses bzw. der erreichbaren Wirkung der Beklagten, also dem Access-Provider, ebenfalls nicht zugemutet werden kann.

Dem Access-Provider obliege auch keine besondere Verkehrspflicht, die die Klageforderung begründen könnte. Dies ergebe sich ebenfalls daraus, dass das Handeln des Beklagten, also das Vermitteln des Zugangs zum Internet bzw. den konkret hier namentlich benannten Seiten über ihren DNS-Server keine eigene Gefahrenquelle für Verstöße durch Dritte schafft. Die Gefahrenquellen stammen aus den Rechtsverletzungen Dritter. Dies gelte auch dann, soweit gegebenenfalls die Kunden des Access-Providers selbst durch Nutzung der rechtswidrigen Inhalte, die Dritte auf die gegenständlichen Seiten gesetzt haben, rechtswidrige Handlungen begehen.

Ein Anspruch auf eine DNS-Sperre wurde daher auch in diesem Fall verneint.

C.II.2.c.2.7. LG Hamburg – „DNS-Sperren II“

Dieser jüngsten Entscheidung des LG Hamburg²⁷¹ lag im Ergebnis ein ähnlicher Sachverhalt wie der Entscheidung „DNS-Sperren I“ zugrunde. Erneut sollte ein Access-Provider (Deutsche Telekom) dazu angehalten werden, mittels DNS-Sperren den Zugang zu einer Website, die tausendfach auf urheberrechtsverletzendes Material verlinkte, zu unterbinden und so seinen Kunden den Zugriff darauf verwehren. Eine erlassene EV gegen den Domaininhaber der Website konnte wegen falscher Adressdaten nicht vollzogen werden.

²⁷¹ LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II).

Das Gericht hielt fest, dass das Klagebegehren, dem Access-Provider zu verbieten, die Musikwerke dadurch öffentlich zugänglich zu machen, dass der Access-Provider über von ihm bereitgestellte Internetzugänge den Zugriff auf Links zu diesen Werken über die inkriminierte Website ermöglicht, auf eine unmögliche Leistung gerichtet sei. Denn unstreitig könnten alle derzeit bekannten technischen Möglichkeiten einer Filterung oder einer Sperre so umgangen werden, dass die Website mit den URLs zu den streitgegenständlichen Werken weiterhin über die von der Beklagten bereitgestellten Internetzugänge aufgerufen werden kann. Damit sei die Beklagte technisch nicht in der Lage, dem begehrten Verbot nachzukommen, weil die beanstandete Aufrufbarkeit der Werke nur erschwert werden kann, ansonsten aber fortbesteht. Das Gericht prüfte aber einen Anspruch auf eine derartige Zugangerschwerung²⁷² aus dem Titel der Störerhaftung, die eine willentliche und adäquat-kausale Mitwirkung an der Beeinträchtigung voraussetzt.

Bei einem Access-Provider komme eine Störerhaftung erst in Betracht, nachdem ihm Kenntnis von der Rechtsverletzung vermittelt worden ist. Weiter müssen die in Betracht kommenden Prüf- und Handlungspflichten nach allgemeinen Grundsätzen rechtlich und tatsächlich möglich und zumutbar sein.

Die Dienstleistung der Deutschen Telekom sei zwar adäquat kausal, eine DNS-Sperre auch technisch möglich.²⁷³ Es fehle aber an der notwendigen rechtlichen Zulässigkeit.

Die in Frage stehenden Filter- und Sperrmaßnahmen (neben DNS-Sperren nennt das Gericht auch IP-Sperren und die Verwendung eines Zwangs-Proxy)s²⁷⁴ setzten voraus, dass der Access-Provider sich Kenntnisse von Umständen der Telekommunikation zu Nutzen macht. Das greife in das Fernmeldegeheimnis ein, was nur bei einer gesetzlichen Beschränkung im Sinne des Art 10 Abs 2 Satz 1 GG erlaubt ist, die den Anforderungen des § 19 GG genügt.²⁷⁵ Da eine solche Beschränkung für zivilrechtliche Filter- oder Sperrmaßnahmen nicht gegeben ist, seien die Maßnahmen rechtlich nicht zulässig.

Für das hier interessierende Problem besonders interessant ist, dass damit – soweit ersichtlich – erstmals in der Rsp mit DNS-Sperren verbundene grundrechtliche Probleme diskutiert

²⁷² Das Gericht qualifizierte damit die Zugangerschwerung als Minus gegenüber dem angestrebten Verbot der Zugänglichmachung.

²⁷³ LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 44, unter Berufung auf zwei Gutachten des Max-Planck-Instituts bzw des Bundesverbands für digitale Wirtschaft. Dies muss zur Vermeidung eines Widerspruchs im Urteil so ausgelegt werden, dass eine Zugangerschwerung durch DNS-Sperren technisch möglich ist, eine absolute Unterbindung des Zugangs zu den inkriminierten Dateien aber nicht.

²⁷⁴ Zu technischer Funktion und Ablauf dieser beiden letztgenannten Maßnahmen vgl LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 48 f.

²⁷⁵ § 19 GG lautet: „Soweit nach diesem Grundgesetz ein Grundrecht durch Gesetz oder auf Grund eines Gesetzes eingeschränkt werden kann, muß das Gesetz allgemein und nicht nur für den Einzelfall gelten. Außerdem muß das Gesetz das Grundrecht unter Angabe des Artikels nennen.“

wurden. Wörtlich hielt das Gericht fest, dass „bereits die Anfrage eines Nutzers zu einem DNS-Server zwecks Auflösung eines DNS-Namens in eine IP-Adresse die Inanspruchnahme eines Kommunikationsdienstes im Internet darstellt, dessen Umstände geschützt sind.“²⁷⁶ Mangels gesetzlicher Ermächtigung für diesen Eingriff in das Fernmeldegeheimnis sei das Sperrungsbegehren daher auf eine (rechtlich) unmögliche Leistung gerichtet.

Zusätzlich scheiterte der Sperranspruch nach Ansicht des LG Hamburg an der mangelnden Zumutbarkeit dem Access-Provider gegenüber. Das Scheitern begründete das Gericht aber nicht mit dem zusätzlichen finanziellen Aufwand, weil Access-Provider durch das Zugangsschwerungsgesetz, das DNS-Sperren zur Bekämpfung von Kinderpornographie vorsieht, ohnehin eine entsprechende Infrastruktur schaffen müssen.²⁷⁷ Vielmehr sei die Maßnahme wegen der leichten Umgehbarkeit und der daraus folgenden mangelnden Eignung dem Provider nicht zumutbar. Internetaktive Jugendlichen und junge Erwachsenen, die sich für die streitgegenständlichen Musiktitel interessieren und zum aktuellen oder potentiellen Kundenkreis von Websites wie der streitgegenständlichen gehören, könnten die auf sie abzielenden Sperrmaßnahmen nach Erfahrung des Gerichts leicht umgehen.

Abschließend betonte das Gericht noch den Unterschied zur Verbreitung von Kinderpornographie: „Wenn der Gesetzgeber zu der Auffassung gelangt, zur Bekämpfung von Kinderpornographie in Kommunikationsnetzen sei eine DNS-Sperre ein geeignetes Mittel, dann folgt daraus nicht notwendigerweise eine Eignung, die es einem Access-Provider zumutbar macht, in gleicher Weise zum Schutz zivilrechtlicher Rechtspositionen tätig zu werden.“²⁷⁸

C.II.2.c.2.8. Übertragbarkeit auf österreichische Rechtslage

In der deutschen Rsp wurden häufig Fälle des Wettbewerbsrechts geprüft. Dabei wurde von den beteiligten Gerichten diskutiert, ob die beanstandeten Tätigkeiten von Access-Providern überhaupt Wettbewerbshandlungen sind.²⁷⁹ Dies kann für die Beurteilung immaterialgüterrechtlicher Ansprüche dahingestellt bleiben, weil es hier nur auf die Erfüllung des objektiven Tatbestands ankommt. In ein Verwertungsrecht oder eine Marke „muss nicht zu einem bestimmten Zweck oder in einer bestimmten Absicht eingegriffen werden, damit eine Rechtsverletzung vorliegt.“²⁸⁰

Anspruchsgrundlage:

²⁷⁶ LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 50.

²⁷⁷ Das genannte Gesetz wurde zwar erlassen, wird nach einem politischen Kompromiss und einer entsprechenden Weisung an das BKA aber nicht vollzogen; vgl heise online vom 22.2.2010: <heise.de/newsticker/meldung/Gesetz-fuer-Websperren-tritt-in-Kraft-936750.html >.

²⁷⁸ LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 56.

²⁷⁹ Eine Wettbewerbshandlung ablehnend LG Frankfurt aM 8.2.2008, 3-12 O 171/07 (youporn II); ebenso LG Frankfurt aM 5.12.2007, 2-03 O 526/07 (google); LG München 3.9.2009, 4 HKO 16685/08.

²⁸⁰ Griss, Haftung für Dritte im Wettbewerbsrecht und im allgemeinen Zivilrecht, JBl 2005, 69 (75).

Könnten sich Access-Provider gegenüber Rechteinhabern auf ihr Haftungsprivileg (§ 13 ECG) berufen, würde ihnen nicht einmal positive Kenntnis von rechtsverletzendem Material, das durch ihre Internetleitungen befördert wird, schaden, solange sie die entsprechende Übermittlung nicht veranlassen, den Empfänger der Übermittlung nicht auswählen sowie die übermittelten Daten nicht auswählen oder verändern.²⁸¹ Das allgemeine Konzept der wettbewerbs- und immaterialgüterrechtlichen Gehilfenhaftung würde dadurch stark eingeschränkt, weil dieses vor allem auf die Kenntnis der Tatumstände, die den Gesetzesverstoß begründen, abstellt.

Die hA und Rsp, die Unterlassungsansprüche aus dem Haftungsprivileg in § 13 ECG aufgrund des Wortlauts von § 19 ECG ausnimmt,²⁸² hat daher bei derartigen Fällen große Auswirkungen.²⁸³ In Deutschland wurde bereits in etlichen Entscheidungen bestätigt, dass § 8 dTMG (entspricht § 13 ECG) gem § 7 Abs 2 Satz 2 dTMG (entspricht § 19 Abs 1 ECG) nicht auf Unterlassungsansprüche anwendbar ist und Access-Provider daher grds der Störerhaftung unterliegen.²⁸⁴ Diese genannten Bestimmungen (sowohl deutsche wie österreichische) sind europarechtlich determiniert²⁸⁵ und differenzieren nicht zwischen Host- und Access-Providern. Da der OGH die prinzipielle Anwendung der Gehilfenhaftung auf Host-Provider bereits bejaht hat, wird mE daher auch in Österreich kein Raum dafür bleiben, Unterlassungsansprüche gegen Access-Provider bereits aufgrund der Haftungsbeschränkung in § 13 ECG abzuweisen.

Besonderes Augenmerk muss auf die präzise Formulierung des Urteilsbegehrens gelegt werden, weil keine Leistung, sondern eine Unterlassung begehrt wird.²⁸⁶ Ein Begehren, das sich darauf richtet, es zu unterlassen, den Zugang zu einer bestimmten Website zu ermöglichen, wäre aber auf eine unmögliche Leistung gerichtet, weil keine der oben beschriebenen technischen Möglichkeiten den Zugang zu einer Website gänzlich verhindern kann.²⁸⁷ Ein allfälliges Unterlassungsbegehren kann daher nur darauf gerichtet sein, es zu unterlassen, den Zugang

²⁸¹ Dazu im Einzelnen *Zankl*, E-Commerce-Gesetz Rz 181.

²⁸² Zum Meinungsstand vgl FN 190 und 191.

²⁸³ Hierin liegt ein markanter Unterschied zur Unterlassungshaftung von Host-Providern, wo materielle Anspruchsvoraussetzungen und Befreiungsvoraussetzungen nach dem ECG sich decken; siehe oben S 83.

²⁸⁴ OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 49; LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I); LG Hamburg 12.3.2010, 308 O 640/08 (DNS-Sperren II), jeweils unter Berufung auf BGH, GRUR 2004, 860 (Internetversteigerung I) und BGH, GRUR 2007, 708 (Internetversteigerung II); vgl auch LG Köln 12.9.2007, 28 O 339/07.

²⁸⁵ Vgl Art 12 Abs 3 E-Commerce-RL bzw Art 8 Abs 3 Info-RL.

²⁸⁶ Die teilweise unpräzise formulierten deutschen Urteilsbegehren, die man im Sinn einer Leistungsklage auslegen könnte (zB Begehren in LG München, 4 HKO 16685/08.: „Die Beklagte wird verurteilt, durch entsprechende Programmierung ihres oder ihrer DNS-Server zu verhindern, dass Kunden der Beklagten zu den Internetseiten (...) gelangen.“), sollten daher hierzulande nicht übernommen werden.

²⁸⁷ So auch LG Hamburg 12.3.2010, 308 O 640/08 (DNS-Sperren I) Rz 35.

zum Internet zu ermöglichen, ohne gleichzeitig den Zugang zu einer bestimmten rechtswidrigen Website zu erschweren.

Weiters könnte unklar sein, wer unmittelbarer Täter ist. Zunächst könnte ein Rechteinhaber daran denken, den Access-Provider selbst nach § 81 Abs 1 UrhG als unmittelbaren Täter in Anspruch zu nehmen, weil er im Rahmen der Übertragung urheberrechtlich geschützter Werke auch eine (flüchtige) Vervielfältigung im Arbeitsspeicher seiner Router vornimmt.²⁸⁸

Eine Haftung als unmittelbarer Täter gem § 81 Abs 1 UrhG scheidet aber aus, weil ein Access-Provider sich erfolgreich auf das freie Werknutzungsrecht des § 41a UrhG berufen kann: Seine vorübergehenden Vervielfältigungen sind flüchtig bzw begleitend (meist nicht länger als einen Bruchteil einer Sekunde), stellen einen integralen und wesentlichen Teil des technischen Übertragungsverfahrens dar, haben ihren alleinigen Zweck in der Übertragung in einem Netz zwischen Dritten (den Nutzern und einem Host- bzw Link-Provider) und ihnen kommt keine eigenständige wirtschaftliche Bedeutung zu.²⁸⁹ Eine markenrechtliche Haftung als unmittelbarer Täter scheidet schon an der mangelnden kennzeichenrechtlichen Verwendung (§ 10a MSchG).

In Deutschland wird daher eine Haftung nach den Grundsätzen der Störerhaftung geprüft, die in Österreich in dieser Form nicht bekannt ist. Hier wird vielmehr eine Unterlassungshaftung unter Berücksichtigung der Rsp zur Gehilfenhaftung zu prüfen sein. Die dafür notwendige gesetzliche Anspruchsgrundlage liegt nicht im ECG, sondern im jeweiligen Sondergesetz (insb § 81 Abs 1a UrhG).

Von *Wiebe* wird in diesem Zusammenhang wie erwähnt vertreten, dass durch die Sonderregelung des § 81 Abs 1a UrhG eine eigene Anspruchsgrundlage geschaffen wurde, die unabhängig von einer unmittelbaren oder „mittelbaren“²⁹⁰ Haftung des Access-Providers ein Vorgehen gegen diesen ermögliche.²⁹¹ Dem ist aufgrund der systematischen Auslegung von § 81 Abs 1a UrhG zuzustimmen. Anders als bei Host-Providern wird die Haftungssituation für den Access-Provider dadurch aber nicht erweitert, sondern eingeschränkt. Ein Access-Provider kann nämlich aufgrund von Abs 1a Satz 2 leg cit iVm § 13 ECG nicht schon dann geklagt werden, wenn er positive Kenntnis von Rechtsverletzungen hat (zB durch Hinweise von Usern) – er muss unabhängig davon in jedem Fall vom betreibenden Rechteinhaber zunächst abge-

²⁸⁸ Jeder Access-Provider betreibt eine Vielzahl von miteinander vernetzten Routern, die die Weiterleitung von Datenpaketen besorgen. Damit ein Router ein Datenpaket weiterleiten kann, muss er dieses in seinen Arbeitsspeicher kopieren, dh vervielfältigen.

²⁸⁹ Vgl *Dillenz/Gutman*, UrhG & VerwGesG² § 41a UrhG Rz 7 wonach darauf abgestellt werden muss, ob das einzelne Vervielfältigungsstück (dh das einzelne Datenpaket) wirtschaftlichen Wert besitzt. Ob die Übertragung des gesamten Werkes durch einen Access-Provider wirtschaftliche Bedeutung hat, ist irrelevant.

²⁹⁰ Damit gemeint ist eine Gehilfenhaftung.

²⁹¹ *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 5; vgl oben S 76 f.

mahnt werden. Praktische Auswirkungen könnte dies vor allem dahingehend haben, dass eine Information des Access-Providers von den stattfindenden Rechtsverletzungen nicht erst in der Klage erfolgen darf.²⁹²

Im Bereich des Markenrechts bleibt es mangels einer unmittelbaren Täterschaft bzw einer § 81 Abs 1a UrhG entsprechenden Sonderhaftung für Vermittler dabei, dass Access-Provider nur im Rahmen der Gehilfenhaftung zur Unterlassung verpflichtet werden können.

Beitragshandlung:

Fraglich ist, wen der Access-Provider fördert. Unmittelbarer Täter sind jedenfalls jene Kunden des Access-Providers, die das urheberrechtliche geschützte Werk beim Host-Provider hochladen. Ob die Kunden des Access-Providers, die derartige Inhalte herunterladen oder in Streams konsumieren, als unmittelbare Täter in Frage kommen oder sich trotz Rechtswidrigkeit der Vorlage auf die Zulässigkeit der „Privatkopie“ berufen können, ist strittig.²⁹³ Für die Prüfung der Kausalität alleine ist diese Frage jedoch vorerst zweitrangig.

Anders als in einzelnen deutschen Entscheidungen zu lesen ist, leistet der Access-Provider mE nämlich jedenfalls einen adäquat-kausalen Beitrag zur Verletzungshandlung, indem er den Zugang zur Quelle der Urheberrechtsverletzung, wer auch immer eine solche begeht, technisch ermöglicht.²⁹⁴ Sein Beitrag besteht zwar lediglich in einer Durchleitung und ist somit passiv-neutral, jedoch ist bei der Ursächlichkeitsprüfung is einer „conditio sine qua non“ wertfrei vorzugehen. Eine rechtswidrige Zurverfügungstellung (§ 18a UrhG) wäre zB nicht möglich, wenn nicht der Access-Provider seinen Kunden den Zugang dorthin herstellt, wo der rechtswidrige Inhalt gespeichert ist. Sein Beitrag ist auch adäquat, weil es mittlerweile als allgemein bekannt angesehen werden kann, dass im Internet rechtswidrige Inhalte zur Verfügung gestellt werden. Dem Access-Provider werden somit keine Folgen seiner Tätigkeit zugerechnet, für ihn nicht vorhersehbar oder beherrschbar wären.²⁹⁵ Die insofern drohende Ausuferung der Haftung kann erst durch später erfolgende Zumutbarkeitsabwägungen be-

²⁹² Vgl dazu FN 214; sonstige praktische Auswirkungen im Vergleich zur Gehilfenhaftung sind nicht ersichtlich, weil auch bei verschuldensunabhängigen Unterlassungsansprüchen die Grundsätze der Verhältnismäßigkeit zu beachten sind und somit die Zumutbarkeit etwaiger Sperrmaßnahmen zu prüfen ist.

²⁹³ Nach dem Wortlaut des § 42 Abs 4 UrhG (digitale Privatkopie) ist dies zu bejahen, wogegen aber vorgebracht wird, dass diese Bestimmung nicht auf offenkundig rechtswidrig erzeugte Quellen anwendbar sei; eine Entscheidung des OGH zu dieser Frage ist bisher nicht erfolgt. Zum Meinungsstand *Schachter* in *Kucsko*, urheber.recht § 42 Pkt 6.; *Laimer/Thiele*, Die Privatkopie nach der Urheberrechtsnovelle 2003, ÖBl 2004, 52; die Legalität bejahend zB *Dittrich*, Vervielfältigung zum eigenen Gebrauch, in *Beiträge zum Urheberrecht VIII* 1 f; *Dalus*, Der Download aus Filesharingbörsen, *ecolex* 2009, 1066; verneinend zB *Stomper*, Internet-Tauschbörsen nach der UrhG-Novelle, RdW 2003, 368; *Walter*, Österreichisches Urheberrecht Rz 969 f; differenzierend *Kucsko*, Geistiges Eigentum 1209 f.

²⁹⁴ Mit Bezug auf Filesharing ebenso: EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 43 f.

²⁹⁵ Vgl zum Begriff der Adäquananz *Koziol/Welser*, Bürgerliches Recht II³ 311.

schränkt werden.²⁹⁶ Missverständlich ist in diesem Zusammenhang die Ansicht der Frankfurter Gerichte, dass der Access-Provider lediglich einen „untergeordneten Beitrag“ leistet.²⁹⁷

Festzuhalten ist, dass der Access-Provider von der in seinem Einflussbereich stattfindenden offenkundigen Rechtsverletzung Kenntnis erlangen muss. Die Offenkundigkeit der Rechtsverletzung ist dabei, wie oben erläutert, nach den Kenntnissen und den Fertigkeiten eines juristischen Laien zu beurteilen. Da das Abrufen urheberrechtsverletzender Websites mithilfe des Zugangs des Access-Providers jedenfalls nicht offenkundig rechtswidrig, sondern dessen Zulässigkeit vielmehr strittig ist,²⁹⁸ ist eine Unterlassungspflicht des Access-Providers in Bezug auf herunterladende Nutzer zu verneinen. Eine Unterlassungspflicht kommt jedoch in Bezug auf die unmittelbaren Täter in Betracht, da diese in offenkundiger Weise eine rechtswidrige Zurverfügungstellung (§ 18a UrhG) vornehmen.

Sobald der Access-Provider positive Kenntnis von einer offenkundig rechtsverletzenden Website hat, zu der er den Zugang vermittelt, kann man von einem wissentlichen Beitrag seinerseits sprechen. Um eine (rechtswidrige) bewusste Förderung zu bejahen, muss zusätzlich geprüft werden, ob das geforderte Alternativverhalten (hier: Sperrmaßnahmen) dem Access-Provider auch zumutbar ist.²⁹⁹

Das Erfordernis der Zumutbarkeit für den Access-Provider wurde in allen einschlägigen deutschen Verfahren betont³⁰⁰ und findet sich auch in den Entscheidungen „Megasex“ und

²⁹⁶ So auch LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I) Rz 3; LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 44.

²⁹⁷ Für das Vorliegen eines adäquat-kausalen Beitrags des Access-Providers LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I); LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 44; vergleichbar auch OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 55 und LG Kiel 23.11.2007, 14 O 125/07 (KielNet); wegen mangelnder Adäquanz bereits eine Prüfpflicht verneinend OLG Frankfurt aM 22.1.2008, 6 W 10/08 (Google); dem folgend LG Frankfurt aM 8.2.2008, 3-12 O 171/07 (youporn.com II); in diesem Sinn bereits die Erstinstanz: LG Frankfurt aM 5.12.2007, 2-03 O 526/07 (Google).

²⁹⁸ Siehe FN 293.

²⁹⁹ Ähnlich OGH 21.12.2006, 6 Ob 178/04a (Online-Gästebuch) mwN: „Zwar ist der Angriff auf die Ehre und den wirtschaftlichen Ruf einer Person schon ein Indiz für die Rechtswidrigkeit, doch kann diese im Einzelfall ausgeschlossen sein, wenn eine umfassende Interessenabwägung zur Beurteilung des Verhaltens als rechtmäßig führt [...]. Dem Interesse am gefährdeten Gut müssen stets auch die Interessen des Handelnden [...] gegenübergestellt werden“. Dasselbe muss mE auch im Zusammenhang mit Urheberrechten gelten.

³⁰⁰ Zumutbarkeitserfordernisse wurden in den deutschen Entscheidungen allerdings methodisch uneinheitlich geprüft. Die Frankfurter Gerichte berücksichtigten die Zumutbarkeit bereits auf Eben der Adäquanz bzw Prüfpflicht, während die Hamburger Gerichte dies erst in einem eigenen Schritt als letztes Kriterium der Haftungsabgrenzung prüften (vgl dazu FN 297).

„Online-Gästebuch“.³⁰¹ Der OGH blieb allerdings spezifische Kriterien für die Zumutbarkeitsabwägung im Rahmen der Providerhaftung bisher schuldig,³⁰² weshalb im Folgenden versucht werden soll, anhand der vorliegenden deutschen Rsp und der Auslegung der berührten Grundrechte diese Abwägungskriterien näher zu bestimmen.³⁰³

Zumutbarkeitskriterien:

Das Tatbestandselement der Zumutbarkeit ist in dogmatischer Hinsicht als Konkretisierung des verfassungsrechtlichen Erfordernisses der Verhältnismäßigkeit von Eingriffen in die Grundrechte des Access-Providers zu begreifen.³⁰⁴ Denn durch ein stattgebendes Urteil würden ein unmittelbarer Eingriff in das Grundrecht der Freiheit der Erwerbsbetätigung und der Unversehrtheit des Eigentums erfolgen.³⁰⁵

Als Ausgangspunkt für die erforderliche Abwägung dient das Geschäftsmodell des betroffenen Access-Providers.³⁰⁶ Ein „klassischer“ Access-Provider stellt gegen Entgelt die Verbindung zum Internet her, ohne dass er Wert darauf legt, welche Inhalte übertragen werden. Er wirbt zwar idR mit der Übertragungsgeschwindigkeit seines Netzes, nicht aber damit, dass seine Kunden damit Urheberrechtsverletzungen begehen könnten. Er ist somit lediglich technisch-neutral an den einzelnen Verbindungen beteiligt. Im Gegensatz zu Host-Providern ist er idR nicht vertraglich oder sonst durch seine Dienstleistung mit dem (offenkundigen) Rechtsverletzer verbunden³⁰⁷ und ist mit seinen Dienstleistungen auch nicht die Quelle der

³⁰¹ Siehe FN 192 bzw 196; in den beiden letztgenannten Entscheidungen ging es freilich um Host-Provider; das Erfordernis der Zumutbarkeit für den Access-Provider ebenfalls betonend *Neubauer*, Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25 (26).

³⁰² Krit *C. Pichler*, Besondere Kontrollpflicht für Host-Provider, *ecolex* 2007, 189 (190).

³⁰³ Im Bezug auf Eingriffe in die Ehre und wirtschaftlichen Ruf betonte der OGH in 6 Ob 178/04a (Online-Gästebuch), es komme bei der Abwägung auf die Art des eingeschränkten Rechtes, die Schwere des Eingriffs, die Verhältnismäßigkeit zum verfolgten Zweck und den Grad der Schutzwürdigkeit des Interesses an.

³⁰⁴ Allgemein zur Wichtigkeit der Berücksichtigung der Grundrechte durch Gerichte (niederer Instanzen) vgl *Berka*, RichterInnen als GrundrechtswahrerInnen: Grundrechte und Rechtsprechung der ersten Instanz, RZ 2008, 114. Vgl weiters *Kodek*, Die Wahrung von Grundrechten durch die Gerichtsbarkeit. Bilanz – Probleme – Perspektiven, ÖJZ 2008, 216 (217).

³⁰⁵ Vgl VfGH 27. 2. 2003, G 37/02 ua, V 42/02 ua wonach eine Pflicht zur technischen Mitwirkung im Rahmen einer Telekommunikationsüberwachung einen (verhältnismäßigen) Eingriff in beide Grundrechte darstellt.

³⁰⁶ Ebenso OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 61: „Das jeweilige Geschäftsmodell muss beachtet werden, um Prüfpflichten nicht zu überspannen.“

³⁰⁷ In diesem Sinn auch OLG Frankfurt aM 22.1.2008, 6 W 10/08 (Google) in Bezug auf die Kunden des beklagten Access-Providers und die auf einer Website abrufbaren Wettbewerbsverstöße: „[D]ie Kunden [...] sind dabei – auch wenn sie unter Inanspruchnahme des Dienstes [...] auf wettbewerbswidrige Inhalte stoßen – nicht Urheber dieser Wettbewerbsverstöße, sondern allenfalls deren Nutznießer oder Opfer.“ Eine Ausnahme davon liegt dann vor, wenn die Kunden des Access-Providers selbst unmittelbare Täter sind, zB weil sie selbst urheberrechtlich geschütztes Material uploaden; vgl auch FN 293.

Verletzungshandlung. Aufgrund seines nur technisch-mittelbaren Beitrags, der nicht mit dem eines Foren- oder Gästebuchbetreibers zu vergleichen ist, ist die Zumutbarkeitsgrenze daher enger als bei Host-Providern zu ziehen.³⁰⁸ Sein berechtigtes Interesse, nicht durch fremde Rechtsverletzungen zusätzlich, insb durch die Überprüfung von Aktivlegitimationen und die technische Durchführung von Sperren, wirtschaftlich belastet zu werden, ist damit offensichtlich. Vollkommen anders liegt der Fall, wenn der Access-Provider selbst damit wirbt, dass seine Kunden nicht für Urheberrechtsverletzungen zur Verantwortung gezogen werden können, weil er ihre Daten niemals hergeben würde, und so zu Rechtsverletzungen geradezu einlädt.³⁰⁹

Auf der anderen Seite stehen die Interessen des betroffenen Rechteinhabers. Ein Eingriff in das absolut geschützte Urheberrecht, den der Access-Provider hier erst möglich macht, ist bereits ein Indiz für die Rechtswidrigkeit. Die wirtschaftlichen Interessen des Rechteinhabers können mE grds anhand des Rechts auf angemessenes Entgelt (§ 86 UrhG) bestimmt werden. Hierbei ist jedoch zu berücksichtigen, dass – wie oben ausgeführt – alle drei technischen Sperrmöglichkeiten ähnlich ineffektiv sind. Das wirtschaftliche Interesse des Rechteinhabers ist daher nicht auf Grundlage aller Verletzungen seiner Rechte, sondern nur auf Grundlage jener Verletzungen zu beurteilen, die erwartungsgemäß durch eine Sperre verhindert würden.³¹⁰

Hinzuzufügen ist, dass nach allgemeinen Grundsätzen eine Sperre das gelindeste Mittel darstellen und die tatsächliche Ausgestaltung die Rechte von Access-Providern so weit wie möglich schonen muss. Konkret bedeutet dies, dass eine Sperre nur dann in Frage kommen kann,

³⁰⁸ LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I) FN 33: „Dort (= bei Foren und Gästebuchbetreibern, Anm) hat bei der Frage der Zumutbarkeit von Pflichten darauf abgestellt werden können, dass die Betreiber [...] selbst die Gefahrenquellen für Rechtsverletzungen gesetzt haben, es ihnen gerade auch auf die Inhalte ankommt und dass dort ganz andere Möglichkeiten einer besseren Beeinflussung und Kontrolle der Inhalte bestand. Die Antragsgegnerin (= Access-Provider, Anm) hat dem gegenüber selbst keine neue Gefahrenquelle gesetzt und als neutraler technischer Vermittler mit den von ihr vermittelten Inhalten nichts zu tun und keinerlei Einfluss darauf. Sie hat damit einen deutlich größeren Abstand zu den rechtsverletzenden Inhalten, wodurch auch die Zumutbarkeitsgrenzen eingeengt werden.“

³⁰⁹ So geschehen beim deutschen Provider Alphaload; siehe OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 63: „Jedenfalls dann, wenn der Zugangsvermittler die Inanspruchnahme seines Dienstes mit der Möglichkeit der Rechtsverletzungen aktiv und offensiv bewirbt, steigert er die seinem Dienst von Natur aus innewohnende Gefahr einer Rechtsverletzung so erheblich, dass ein Entfallen der Funktionsprivilegierung geboten ist. In einem derartigen Fall treffen den Zugangsvermittler deutlich gesteigerte Prüfungspflichten schon deshalb, weil er durch sein eigenes Werbeverhalten ein deutlich höheres Risiko verursacht hat.“

³¹⁰ Vgl LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I): „Denn je geringer die Eignung ist, umso weniger wird vom Access-Provider unter Berücksichtigung des dargestellten zusätzlichen Aufwandes die Einrichtung einer solchen Sperre verlangt werden können.“

wenn (in dieser Reihenfolge) die unmittelbaren Täter, der Host-Provider und der Link-Provider nicht greifbar und zur Unterlassung zu bewegen sind.

Kommen Alternativen zu einer Sperre nicht in Betracht, so muss auch bei der Wahl der technischen Art der Sperre das Gebot des gelindesten Mittels beachtet werden. Wie oben ausgeführt, sind alle drei Arten der Sperre ähnlich (in-)effektiv, DNS-Sperren jedoch für den Access-Provider bei weitem die geringste wirtschaftliche Belastung. Daher sind mE nur DNS-Sperren für einen Access-Provider potentiell zumutbar. Wegen ihrer einhellig als gering eingestuften technischen Eignung³¹¹ wurde in der deutschen Rsp ein Sperranspruch aber bisher abgelehnt. Ohne Erfolg blieb das Argument, dass die Mehrzahl der durchschnittlichen Internetnutzer durch eine DNS-Sperre davon abgehalten würde, einen anderen Weg zu dem gesperrten Internetauftritt zu suchen. In einem Verfahren vor dem LG Hamburg³¹² wurde nämlich betont, dass es selbst dem Gericht in wenigen Minuten gelungen sei, eine Internetseite mit einer Anleitung zur Umgehung mit den verfügbaren Name-Servern zu finden. Internetaktiven Jugendlichen und jungen Erwachsenen würde dies im Zweifel noch schneller gelingen. Dieses Argument gilt mE ebenso in Österreich.

Ob im konkreten Fall die Zumutbarkeit einer DNS-Sperre zu bejahen ist, wird jedoch anhand der wirtschaftlichen Interessen des Rechteinhabers und des Access-Providers im Einzelfall zu beurteilen sein.

Berührte Grundrechte Dritter

Neben den grundrechtlich geschützten Rechtspositionen des Access-Providers, die wie oben ausgeführt im Rahmen des Tatbestandselements der Zumutbarkeit der Sperre zu berücksichtigen sind, greift ein Unterlassungsurteil, das einen Access-Provider zur Sperre einer Website verpflichtet, jedenfalls auch in die Grundrechte der Nutzer sowie in jene des Betreibers der gesperrten Website ein. Diese werden in der Rsp dogmatisch unsauber unter dem Aspekt der „Interessen der Allgemeinheit“ behandelt.³¹³

Die Kunden des Access-Providers werden durch ein Unterlassungsurteil in ihrem Grundrecht auf Informationsfreiheit (Art 10 EMRK)³¹⁴ beeinträchtigt. Dieser Eingriff ist jedenfalls in je-

³¹¹ LG Kiel 23.11.2007, 14 O 125/07 (KielNet); LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I); LG München 3.9.2009, 4 HKO 16685/08; zuletzt LG Hamburg, 12.3.2010, 308 O 640/08 (DNS-Sperren II) Rz 54; ebenso *Schneider*, Sperren und Filtern im Internet, MMR 2004, 18 (23); *Gehrke*, Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR 2008, 291 f; *Marberth-Kubicki*, Der Beginn der Internet-Zensur - Zugangssperren durch Access-Provider, NJW 2009, 1792 mwN.

³¹² LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I).

³¹³ OGH 21.12.2006, 6 Ob 178/04a (Online-Gästebuch); OLG Hamburg 28.1.2009, 5 U 255/07 (alphaload) Rz 61.

³¹⁴ Art 13 StGG schützt dem Wortlaut nach nur das Recht „seine Meinung [...] frei zu äußern“, nicht jedoch das Recht sich Informationen zu beschaffen. Art 10 EMRK umfasst dem Wortlaut nach auch „die Freiheit zum Empfang [...] von Nachrichten oder Ideen“. Vgl VfGH 16.3.1987, B154/85 wonach „eine Behinderung der Beschaffung

nem Maße gerechtfertigt, in dem er sich nur auf urheberrechtlich geschützte Inhalte bezieht, deren Beschaffung durch die Nutzer ohnedies eine rechtswidrige Vervielfältigung darstellen würde.³¹⁵ Werden von der zu sperrenden Website aber auch Inhalte angeboten, an denen Nutzer ein berechtigtes Informationsinteresse haben, so ist der Grundrechtskonflikt zwischen geistigem Eigentum (Art 17 Abs 2 GRC) und Informationsfreiheit durch eine Abwägung zwischen den Interessen des Rechteinhabers und jenen der Nutzer aufzulösen. Hierbei handelt es sich um eine diffizile Einzelfallbeurteilung, die es erfordert, das Verhältnis zwischen einerseits Art und Umfang der rechtmäßigen Inhalte und andererseits den urheberrechtswidrigen Inhalten, an denen der Kläger ein Werknutzungsrecht hat,³¹⁶ zu ergründen. Beispielsweise wäre eine Sperre von Google³¹⁷ oder YouTube.com ein unverhältnismäßiger Eingriff in die Informationsfreiheit der Nutzer, weil Art und Umfang der rechtmäßigen Inhalte ein außerordentlich großes Interesse der Nutzer begründet, dem kein vergleichbares Interesse des Rechteinhabers gegenüber stehen wird.

Durch ein Unterlassungsurteil erfolgt weiters ein Eingriff in das Grundrecht des Betreibers der gesperrten Website auf Meinungsäußerungsfreiheit (Art 13 StGG, Art 10 EMRK). Handelt es sich um einen Host-Provider, der – abgesehen von einer Benutzeroberfläche die das Hin- und Herunterladen von Inhalten ermöglicht – definitionsgemäß keine eigenen Inhalte anbietet, so ist die Eingriffsintensität tatsächlich als gering zu beurteilen. Ist die gesperrte Website hingegen jene eines Link-Providers, so kann, sofern es sich bei den Links um eigene Inhalte des Providers handelt, ein wesentlich intensiverer Grundrechtseingriff vorliegen. Wiederum gilt jedoch, dass eine Sperre, die ausschließlich urheberrechtswidrige Äußerungen betrifft, grds als gerechtfertigt anzusehen sein wird. Neben dem Grundrecht auf Meinungsäußerungsfreiheit kann die Sperre einer Website auch einen Eingriff in das Grundrecht auf Erwerbsfreiheit (Art 6 StGG) darstellen. Da dieses jedoch nur Staatsbürgern und Kraft Art 18 AEUV (ex Art 12 EUV) EWR-Bürgern zukommt, wird ein Eingriff regelmäßig zu verneinen sein.

Schließlich ist darauf hinzuweisen, dass durch eine IP-Sperre auch die Websites unbeteiligter Dritter blockiert werden könnte. Ein solcher Eingriff in die Meinungsäußerungsfreiheit Dritter wäre nicht zu rechtfertigen, weil er in keinem sachlichen – sondern bloß technischen – Verhältnis zu den Urheberrechtsverletzungen steht. Hieraus folgt zunächst, dass eine Unter-

und der Ermittlung öffentlich zugänglicher Informationen durch (aktives) Eingreifen von Staatsorganen“ einen Eingriff in Art 10 EMRK darstellt.

³¹⁵ Vgl OGH 17.12.1996, 4 Ob 2363/96w; 12.06.2001, 4 Ob 127/01g, wonach das durch Art 13 StGG und Art 10 EMRK geschützte Grundrecht auf freie Meinungsäußerung nicht den Eingriff in die urheberrechtlich geschützten Rechte über die im UrhG festgelegten freien Werknutzungen hinaus rechtfertigt.

³¹⁶ Urheberrechtswidrige Inhalte, an denen der Kläger keine Werknutzungsrechte hat, sind für die Beurteilung seiner Interessenslage irrelevant.

³¹⁷ Vgl OLG Frankfurt aM 22.1.2008, 6 W 10/08 (Google).

lassungspflicht keinesfalls zum Inhalt haben kann, IP-Adressen zu sperren, die auch von anderen Websites verwendet werden. Darüber hinaus bedeutet dies, dass eine IP-Sperre in vielen Fällen eine höhere Gefahr für die Grundrechtssphäre Dritter begründet. Sie ist daher nur dann als gelindestes Mittel anzusehen, wenn entweder eine versehentliche Sperrung Dritter ausgeschlossen werden kann oder eine DNS-Sperre erfolglos erscheint.

Durch die in „Online-Gästebuch“ entwickelte Figur der „besonderen Überwachungspflicht“ könnte die Prüfpflicht von Access-Providern auch auf den Fall des vorwerfbaren Nichtkennens von erneut auftretenden offenkundigen Rechtsverletzungen ausgedehnt werden, wenn der Access-Provider nach den Umständen des Einzelfalls damit rechnen musste. Aufgrund des – im Vergleich zum Host-Provider - äußerst großen Abstands des Access-Providers zur Verletzungshandlung sollte diese Pflicht mE – wenn überhaupt - nur sehr restriktiv angewendet werden. Eine allgemeine Überwachung des Datenverkehrs widerspräche jedenfalls § 18 Abs 1 ECG und wäre mit Blick auf das Fernmelde- (Art 10a StGG) und Kommunikationsgeheimnis (§ 93 TKG) zudem (grundrechtlich) unzulässig.

C.II.2.d. Ergebnis

Das System der Haftungsprivilegien des ECG ist im Fall von Unterlassungsansprüchen gegen Provider nicht anzuwenden. Im Falle von Host-Providern ist dies aber ohne Bedeutung, weil sich materielle Tatbestandsvoraussetzungen mit den Privilegierungsvoraussetzungen in § 16 ECG decken und damit zu denselben Ergebnissen führen.

Host-Provider haften nur, wenn sie den unmittelbaren Täter der Rechtsverletzung bewusst fördern, was in der Rsp auf offenkundige Rechtsverletzungen beschränkt wird. Sie haben die beanstandeten Inhalte sodann zu löschen. Access-Provider sind demgegenüber noch weiter von der Quelle der Rechtsverletzung entfernt und können aufgrund technischer Unzulänglichkeiten lediglich den Zugang zu dieser erschweren. Die dafür einzig in Frage kommenden DNS-Sperren sind leicht zu umgehen, was idR dazu führen wird, dass eine Sperre aufgrund berechtigter entgegenstehender Interessen der Access-Provider unzumutbar sein wird.

Durch die Sonderbestimmung des § 81 Abs 1a UrhG wurde in Bezug auf Internetprovider vom bisherigen Konzept der Gehilfenhaftung zugunsten eines verschuldensunabhängigen Unterlassungsanspruches, der dem gegen den unmittelbaren Täter nachgebildet ist, abgegangen. Da Internetprovider aber kraft gesetzlicher Anordnung (Abs 1a Satz 2 leg cit) jedenfalls vor einer Klage abzumahnern und ihre grundrechtlich geschützten Rechtspositionen zu berücksichtigen sind, werden sich praktische Auswirkungen dieser Bestimmung in Grenzen halten.

C.III. Genugtuung

Die Rechtsdurchsetzung ist erst mit der Genugtuung für den Rechteinhaber abgeschlossen. Dieser hat dafür mehrere immaterialgüterrechtliche Ansprüche zur Verfügung.

C.III.1. Anspruch auf angemessenes Entgelt

Rechtsgrundlagen: § 86 UrhG; § 53 Abs 1 MSchG

C.III.1.a. Grundsätze

Rechteinhaber und auch Werknutzungsberechtigte³¹⁸ haben Anspruch auf angemessenes Entgelt, wenn ein Werk auf eine ihnen vorbehaltenen Verwertungsart benutzt wird. Dieses Recht ist unionsrechtlich nicht direkt angeordnet³¹⁹, gem Art 16 Enforcement-RL können die Mitgliedsstaaten jedoch unbeschadet der in dieser RL vorgesehenen zivil- und verwaltungsrechtlichen Maßnahmen, Verfahren und Rechtsbehelfe in Fällen von Verletzungen von Rechten des geistigen Eigentums andere angemessene Sanktionen vorsehen.

Verschulden ist für das Recht auf angemessenes Entgelt nicht erforderlich, weil es sich im Ergebnis um einen bereicherungsrechtlichen Anspruch handelt, der die „ersparte Lizenzgebühr“ vom Verletzer an den Rechteinhaber zurückführt.³²⁰ Als solcher wurzelt er in § 1041 ABGB.³²¹

Da die immaterialgüterrechtlichen Sonderregeln eingeführt wurden, um die Geltendmachung des Rechts auf angemessenes Entgelt zu erleichtern, ist es nach der Rsp nicht erforderlich, eine konkret bezifferte Bereicherung nachzuweisen.³²² Das ändert aber nichts am Zweck von § 86 Abs 1 UrhG bzw § 53 Abs 1 MSchG, jene Vermögensverschiebung rückgängig zu machen, die durch den unberechtigten Eingriff in Ausschließungsrechte eingetreten ist. Daher steht dieser Anspruch nur zu, wenn und soweit ein Nichtberechtigter Vorteile aus der Benutzung gezogen hat. War diese dagegen auch bei objektiver Betrachtung nicht von Nutzen, so steht dem Eigentümer der Sache kein Verwendungsanspruch zu.³²³

³¹⁸ *Guggenbichler* in Kucska, urheber.recht § 86 Pkt 5. mwN.

³¹⁹ Art 13 Abs 2 Enforcement-RL spricht bei Fällen, in denen der Verletzer eine Verletzungshandlung vorgenommen hat, ohne dass er dies wusste oder vernünftigerweise hätte wissen müssen, von der Möglichkeit, dass die Gerichte die Herausgabe der Gewinne oder die Zahlung von Schadensersatz anordnen, dessen Höhe im Voraus festgesetzt werden kann. Das angemessene Entgelt österreichischer Prägung ist jedoch von Schadensersatz unabhängig und seine Höhe hängt vom konkreten Fall und nicht von einer vorherigen Festsetzung ab.

³²⁰ Vgl *Walter*, Schadensersatz, angemessenes Entgelt und Verletzergewinn bei Urheberrechtsverletzungen, MR 1995, 2 mwN.

³²¹ Vgl RIS-Justiz RS0108478; RS0019926.

³²² Zu § 86 UrhG vgl OGH 19. 11. 2009, 4 Ob 163/09p.

³²³ Vgl RIS-Justiz RS0116468 zu § 1041 ABGB.

Aus diesem bereicherungsrechtlichen Gedanken folgt insb, dass der Anspruch auf angemessenes Entgelt nach dem Urheber- oder Markenrecht sich nur gegen diejenige Person richten kann, die einen Nutzen aus der widerrechtlichen Verwendung des geschützten Immaterialguts gezogen hat. Ein Anspruch gegen Gehilfen oder Anstifter scheidet somit aus.³²⁴

Ansprüche auf angemessenes Entgelt sind gegen Website-Betreiber und andere unmittelbare Täter somit ohne weiteres möglich, weil sie durch die kostenfreie Nutzung des jeweiligen Werks objektiv profitieren, insb durch verbesserte Attraktivität ihrer Website und dadurch erhöhten Traffic, Werbeeffekte oder eine Verbesserung ihres Rufes. Die Pflicht zu Zahlung trifft im Fall von Unternehmen den Inhaber des Unternehmens, nicht aber dessen Bedienstete oder Beauftragte, weil idR nur Ersterer durch die Nutzung bereichert wird.³²⁵ Die Höhe des angemessenen Entgelts richtet sich nach den Grundsätzen, die für die Berechnung einer vertraglichen Lizenzgebühr entwickelt wurden, somit danach, was redliche Parteien als tatsächliche Nutzung vereinbart hätten.³²⁶ Die Feststellung des für vergleichbare Nutzungen üblichen Entgelts, das bei einer im Voraus eingeholten Bewilligung üblicherweise gezahlt wird, ist dabei eine prozessuale Tatfrage, wohingegen die Bemessung des für eine konkrete Rechtsverletzung gebührenden Entgelts eine Frage der rechtlichen Beurteilung ist.³²⁷

C.III.1.b. Anspruch auf angemessenes Entgelt gegen Internetprovider

Internetprovider sind gleich doppelt von der Zahlung des Entgelts befreit: Erstens sind sie durch ihre Haftungsprivilegien (§ 13 bzw § 16 ECG) grds (Access-Provider) bzw bis zur Kenntniserlangung (Host-Provider) von jeglicher Verantwortung freigestellt. Die Ausnahmeregelung des § 19 ECG, die Haftungsbefreiungen außer Kraft setzt, erstreckt sich nicht auf bereicherungsrechtliche Ansprüche. Zweitens kommen sie, wenn überhaupt, nur als Gehilfen in Betracht. Da sie als solche keinen Nutzen aus dem Ersparen der Urheber-oder Markenrechtlizenzen ziehen, kann von ihnen auch kein angemessenes Entgelt verlangt werden.

C.III.2. Anspruch auf Schadenersatz und Herausgabe des Gewinns

Rechtsgrundlagen: § 87 UrhG; § 53 Abs 2 MSchG

C.III.2.a. Grundsätze

Bei einer schuldhaften Verletzung von Rechten können Rechteinhaber oder Werknutzungs-berechtigte Schadenersatz begehren.

³²⁴ Vgl RIS-Justiz RS0125548; ohne nähere Begründung aA *Guggenbichler* in Kucsko, urheber.recht § 86 Pkt 6., unter Hinweis auf die Rsp zum Unterlassungsanspruch; ihm widersprechend OGH 19. 11. 2009, 4 Ob 163/09p.

³²⁵ Vgl RIS-Justiz RS0120905.

³²⁶ Vgl erneut RIS-Justiz RS0108478; RS0120089.

³²⁷ *Guggenbichler* in Kucsko, urheber.recht § 86 Pkt 8.3 mwN.

§ 87 Abs 1 UrhG und § 53 Abs 2 Z 1 MSchG erweitern den Umfang der Ersatzpflicht nach allgemeinem Zivilrecht (§§ 1323, 1324 ABGB), weil sie unabhängig vom Grad des Verschuldens neben dem positiven Schaden auch den entgangenen Gewinn zusprechen, und zwar im vertraglichen wie im deliktischen Bereich gleichermaßen.³²⁸

Das ist insofern wichtig, als der Schaden beim Kläger idR aus einer Umsatzminderung bzw dem Entgang der Lizenzgebühr bestehen wird und für positiven Schaden insofern wenig Raum bleibt. Dieser Umstand wird freilich dadurch relativiert, dass die Rsp eine im Verkehr als gesichert anzusehende Ertragschance im Betrieb eines Unternehmens dem positiven Schaden und nicht dem entgangenen Gewinn zurechnet.³²⁹ Die konkrete Schadensberechnung hat sich, ähnlich wie bei der Berechnung des angemessenen Entgelts, an der Höhe der verkürzten Lizenzgebühr zu orientieren. Nach der Lit muss wegen des Verschuldens des Verletzers diese „Entschädigungslizenz“ idR höher ausfallen als das bereicherungsrechtlich geprägte angemessene Entgelt.³³⁰

In der Praxis überaus bedeutsam ist die Möglichkeit, den entstandenen Vermögensschaden mit dem Doppelten des gebührenden Entgelts festzusetzen. Im Urheberrecht (§ 86 Abs 3 UrhG) besteht diese Möglichkeit bereits bei leichter Fahrlässigkeit, im Markenrecht (§ 53 Abs 3 MSchG) dagegen nur bei Vorsatz oder grober Fahrlässigkeit. Durch diese Regelung (Schadenspauschalierung) können insbesondere Beweisschwierigkeiten vermieden werden.³³¹ Vom Erfordernis für den Rechteinhaber, zumindest einen „Grundscha-den“ nachzuweisen, um die Pauschalierung der Höhe nach in Anspruch nehmen zu können, ist der OGH nach Kritik der Lehre abgegangen.³³²

§ 87 Abs 2 UrhG und § 53 Abs 4 MSchG gewähren weiters einen Anspruch auf Ersatz immaterieller Schäden, was unionsrechtlich durch Art 13 Abs 1 lit a Enforcement-RL legitimiert ist. Diese Regelungen greifen aber nur in besonders kränkenden Fällen, etwa bei einer Verletzung des Rechts am eigenen Bild gem § 78 UrhG, und sollen nicht bei jeglicher Immaterialgüterrechtsverletzung ein zusätzliches Trostpflaster sein.³³³ Grds kann eine derartige Entschädigung auch juristischen Personen zustehen, wenn die mit ihrer Vertretung betrauten physischen Personen durch die Verletzung eine ganz empfindliche, erhebliche Kränkung er-

³²⁸ Weiterführend *Guggenbichler* in Kucsko, urheber.recht § 87 Pkt 1.3 mwN.

³²⁹ Vgl RIS-Justiz RS0030452.

³³⁰ Für das UrhG: *Guggenbichler* in Kucsko, urheber.recht § 87 Pkt 1.5; vgl Art 13 Abs 1 lit b Enforcement-RL.

³³¹ *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 165.

³³² RIS-Justiz RS0110102.

³³³ Diese „Herzinfarkttheorie“ wurde insb von *Walter*, Schadenersatz, angemessenes Entgelt und Verletzerge-winn bei Urheberrechtsverletzungen, MR 1995, 2 f kritisiert, von der Rsp aber beibehalten; vgl OGH 26.5.1998, 4 Ob 63/98p.

fahren haben, die den mit jeder Immaterialgüterrechtsverletzung verbundenen Ärger erheblich übersteigt.³³⁴

So der Schädiger durch die Immaterialgüterrechtsverletzungen einen Gewinn erzielt hat, kann der Rechteinhaber die Herausgabe dieses Gewinns begehren, im urheberrechtlichen Kontext aber nur in den vom Gesetz aufgezählten Fällen (§ 87 Abs 4 UrhG). Der herauszugebende Gewinn darf nicht mit dem vom Verletzer erzielten Umsatz gleichgesetzt werden. Herauszugeben ist nämlich nur der Reingewinn nach Abzug der Kosten, den der Verletzer gerade aufgrund des widerrechtlichen Eingriffs tatsächlich erzielt hat, unabhängig davon, ob ihn der Verletzte selbst hätte erzielen können.³³⁵ Wenn der Verletzer keinen Gewinn erzielt hat, geht der Anspruch somit ins Leere.

Angemessenes Entgelt, (pauschalierter) Schadenersatz sowie Gewinnherausgabe stehen in alternativer Konkurrenz zueinander; dadurch kann nicht dreimal eine Leistung in Höhe des angemessenen Entgelts verlangt werden.³³⁶ Ein zusätzlicher Ersatz des Vermögensschadens kann nur begehrt werden, soweit dieser das (doppelte) angemessene Entgelt oder den herauszugebenden Gewinn übersteigt (vgl § 87 Abs 3 und Abs 5 UrhG bzw § 53 Abs 2 und Abs 3 MSchG). Ideeller Schadenersatz kann hingegen zusätzlich zum Ersatz des Vermögensschadens verlangt werden.³³⁷

Diesem Konzept ist auch die Enforcement-RL in Art 13 gefolgt, sodass eine Anpassung des nationalen Rechts unterbleiben konnte.³³⁸

C.III.2.b. Anspruch auf Schadenersatz gegen Internetprovider

Access-Provider sind aufgrund eines Umkehrschlusses aus § 13 ECG und Art 12 E-Commerce-RL selbst bei positiver Kenntnis von rechtsverletzenden Informationen, die sie durch ihre Leitungen transportieren, von jeglicher Schadenersatzpflicht befreit, sofern sie 1. die Übermittlung nicht veranlassen, 2. den Empfänger der übermittelten Informationen nicht auswählen und 3. die übermittelten Informationen weder auswählen noch verändern.³³⁹ Der Access-Provider hat das Vorliegen dieser Voraussetzungen im Prozess zwar zu behaupten und beweisen, wird idR aber aufgrund der horizontalen Haftungsbefreiung nicht schadenersatzrechtlich für Immaterialgüterrechtsverletzungen, die durch seine Leitungen abrufbar sind bzw transportiert werden, belangt werden können.

³³⁴ Vgl *Guggenbichler* in Kucsko, urheber.recht § 87 Pkt 2.4; zu den Kriterien, die zur Bestimmung der Schadenshöhe herangezogen werden können, siehe ebendort Pkt 2.5.

³³⁵ OGH 14. 10. 1986, 4 Ob 276/86 (Werbeunterlagen).

³³⁶ RIS-Justiz RS0110105.

³³⁷ Für das Urheberrecht: *Guggenbichler* in Kucsko, urheber.recht § 87 Pkt 1.6.

³³⁸ Vgl ErlRV 1423 BlgNR XXII. GP 4; ErlRV 1324 BlgNR XXII. GP 3.

³³⁹ Vgl weiterführend *Zankl*, E-Commerce-Gesetz Rz 199.

Host-Provider dagegen verlieren, wie bereits erwähnt, ihr Haftungsprivileg (§ 16 ECG, Art 14 E-Commerce-RL), sobald sie Kenntnis von einer Rechtsverletzung in ihrem Speicherbereich erlangen. In Bezug auf schadenersatzrechtliche Ansprüche gilt kraft § 16 Abs 1 Z 1 ECG bzw Art 14 Abs 1 lit a E-Commerce-RL Besonderes, weil der Host-Provider hier bereits sein Haftungsprivileg verliert, wenn ihm Tatsachen oder Umstände bewusst sind, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird. Diese Regelung wurde zu Recht wegen ihrer unklaren Formulierung und dafür kritisiert, dass sie in das österreichische System des Schadenersatzrechts nicht ohne weiteres einzuordnen ist.³⁴⁰ Im Ergebnis wurde damit eine neue Verschuldenskategorie, nämlich bewusst grobe Fahrlässigkeit, in das Schadenersatzrecht eingeführt. Diese liegt zwischen den Kategorien (herkömmliche) grobe Fahrlässigkeit und Vorsatz, die nach allgemeinem Zivilrecht gem § 1324 ABGB gleich behandelt werden. Die Regelung in § 16 ECG führt folglich dazu, dass die strafrechtlich notwendige Differenzierung zwischen bewusster Fahrlässigkeit und Vorsatz (zB § 88 und § 83 Abs 1 StGB) nun auch im Schadenersatzrecht zu treffen ist, wenn ein Schadenersatzanspruch gegen Host-Provider zu prüfen ist.³⁴¹

Denkbar wäre etwa ein Online-Forum, in dem urheberrechtsverletzende Inhalte zur Verfügung gestellt werden (§ 18a UrhG) und gegen Entgelt an bestimmte Nutzer downloadbar sind (gewerbsmäßige Begehung ist gem § 91 Abs 2 UrhG mit bis zu zwei Jahren Freiheitsstrafe bedroht). Der Host-Provider hält es aufgrund von einzelnen Hinweisen (zB durch andere User) zwar ernstlich für möglich, dass derartige Dinge auf seinem Forum vor sich gehen, er vertraut aber darauf, dass schon keine rechtswidrigen Handlungen gesetzt werden und geht den Hinweisen daher nicht nach. Während er strafrechtlich jedenfalls haftungsfrei bleibt, weil er keine positive Kenntnis von einzelnen Verletzungshandlungen hat, verliert er sein Haftungsprivileg in Bezug auf Schadenersatzansprüche aber schon dadurch, dass ihm Umstände bewusst sind, aus denen eine rechtswidrige Tätigkeit in seinem Speicherbereich offensichtlich wird. Eine Schadenersatzklage wäre sohin nicht schon aufgrund von § 16 ECG abzuweisen, sondern es müsste der jeweilige Haftungstatbestand (hier § 18a iVm § 87 UrhG) geprüft werden (kein Umkehrschluss).³⁴² Der Host-Provider kann sich aber jedenfalls dann exkulpieren, wenn er die rechtswidrige Information unverzüglich entfernt, sobald er Kenntnis bzw Bewusstsein davon erlangt (§ 16 Abs 1 Z 2 ECG).

C.III.3. Anspruch auf Rechnungslegung

Rechtsgrundlagen: § 87a Abs 1 UrhG; § 55 MSchG iVm § 151 PatG

³⁴⁰ Zankl, E-Commerce-Gesetz Rz 241 f; Schanda, Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, *ecolex* 2001, 920 f.

³⁴¹ Dazu und mit Beispielen Zankl, E-Commerce-Gesetz Rz 241 f.

³⁴² Zankl, E-Commerce-Gesetz Rz 225 f.

C.III.3.a. Grundsätze

Da die genaue Bemessung von Genugtuungsansprüchen oft von den Aktivitäten und internen Unterlagen des Verletzers abhängt, ist der Verletzer dem Verletzten zur Rechnungslegung verpflichtet und dazu verpflichtet, deren Richtigkeit durch einen Sachverständigen prüfen zu lassen. Wenn sich dabei ein höherer Betrag als aus der Rechnungslegung ergibt, sind die Kosten der Prüfung vom Zahlungspflichtigen zu tragen. Im Urheberrecht ist der Anspruch auf Verletzungen, die Zahlungs- und Beseitigungspflichten auslösen, begrenzt. Wenn ein derartiges Hauptbegehren abgewiesen wird, ist auch das Begehren auf Rechnungslegung als bloßer Nebenanspruch abzuweisen.³⁴³

In § 87a Abs 1 letzter Satz UrhG wurde auch gesetzlich verankert, was in der Rsp als Grundsatz bereits anerkannt war: Wer zur Rechnungslegung verpflichtet ist, hat dem Anspruchsberechtigten darüber hinaus alle weiteren zur Rechtsverfolgung erforderlichen Umstände Auskunft zu erteilen. Art und Umfang richten sich nach den Erfordernissen des Einzelfalls.³⁴⁴

Der Rechnungslegungsanspruch wird prozessual im Zusammenhang mit Zahlungsbegehren durch eine Stufenklage (Art XLII EGZPO) geltend gemacht. Das Gericht führt zunächst ein Verfahren zum Bestehen und zum Umfang des Rechnungslegungsanspruches durch und erkennt darüber mit Teilurteil; erst nach dessen Rechtskraft hat der Kläger dann sein Zahlungsbegehren durch zahlenmäßige Angaben aufgrund der Rechnungslegung zu ergänzen.³⁴⁵

Der Anspruch auf Rechnungslegung ist ein Hilfsanspruch und dient der Erleichterung der Rechtsdurchsetzung.³⁴⁶ Besondere Fragestellungen im Zusammenhang mit dem Internet haben sich bisher, soweit ersichtlich, nicht ergeben.

C.III.4. Anspruch auf Urteilsveröffentlichung

Rechtsgrundlagen: § 85 UrhG; § 55 MSchG iVm § 149 PatG

C.III.4.a. Grundsätze

So auf Unterlassung oder Beseitigung geklagt wird, hat das Gericht der obsiegenden Partei auf Antrag die Befugnis zuzusprechen, das Urteil auf Kosten des Gegners zu veröffentlichen.

Unionsrechtlich ist dieser Anspruch in Art 15 Enforcement-RL normiert, wonach die Mitgliedstaaten sicherstellen, dass die Gerichte bei Verfahren wegen Verletzung von Rechten des geistigen Eigentums auf Antrag des Antragstellers und auf Kosten des Verletzers geeignete Maßnahmen zur Verbreitung von Informationen über die betreffende Entscheidung, einschließlich der Bekanntmachung und der vollständigen oder teilweisen Veröffentlichung,

³⁴³ Vgl RIS-Justiz RS0109113.

³⁴⁴ *Kucsko*, Geistiges Eigentum 1278 mwN.

³⁴⁵ *Schachter* in *Kucsko*, urheber.recht § 87a Pkt 6.

³⁴⁶ Vgl RIS-Justiz RS0077477.

anordnen können. Die Mitgliedstaaten können andere, den besonderen Umständen angemessene Zusatzmaßnahmen, einschließlich öffentlichkeitswirksamer Anzeigen, vorsehen. In Österreich hat diese Bestimmung zu keinem gesonderten Umsetzungsbedarf geführt.³⁴⁷

Voraussetzung für das Bestehen des Anspruchs ist der Nachweis eines berechtigten Interesses an der Veröffentlichung,³⁴⁸ was nicht dasselbe ist wie das Bestehen von Wiederholungsgefahr.³⁴⁹ Es ist vielmehr das Resultat einer Abwägung zwischen Notwendigkeit und Angemessenheit einer Veröffentlichung. Je ausgeprägter das Erinnerungsbild in der Öffentlichkeit ist, desto notwendiger ist die Veröffentlichung. Ein berechtigtes Interesse liegt somit insb dann vor, wenn die Rechtsverletzungen eine gewisse Publizität erlangt haben. Andererseits wird eine Veröffentlichung dann weniger bis gar nicht notwendig sein, wenn die Auswirkungen auf die Öffentlichkeit gering ausfallen.³⁵⁰

Insb bei der Verletzung von Immaterialgüterrechten tritt hinzu, dass die Veröffentlichung ein geeignetes Mittel zur Beseitigung jener Nachteile sein muss, die dem Rechteinhaber durch die Verletzung entstanden sind. Das folgt daraus, dass das Ziel der Veröffentlichung die Beseitigung falscher Eindrücke in Öffentlichkeit ist, und nicht die Befriedigung der menschlichen Neugier oder die Anprangerung der Rechtsverletzung; ebensowenig dient sie der Abschreckung Dritter.³⁵¹

Die Form der Urteilsveröffentlichung richtet sich nach Art und Umfang der Rechtsverletzung (Talionsprinzip). Da die Veröffentlichung idR die Öffentlichkeit von Immaterialgüterrechtsverletzungen informieren soll, hat sie in derselben Aufmachung wie die vorhergegangene Rechtsverletzung zu erfolgen. Wenn eine Veröffentlichung in gleicher Form nicht möglich oder zweckmäßig ist, so hat das Gericht auf Antrag jene Form zu bestimmen, die im Verhältnis zur Rechtsverletzung angemessen ist, um die Allgemeinheit zu informieren. Dabei wird idR auf Printmedien zurückgegriffen und je nach Ausmaß der Rechtsverletzung angeordnet, ob eine Veröffentlichung des Urteils in einer Fachzeitschrift, einer Tages- oder Wochenzeitung etc zu erfolgen hat.³⁵²

Da das Gesetz von „obsiegender Partei“ spricht, kann theoretisch auch die beklagte Partei eine Urteilsveröffentlichung zugesprochen bekommen, so sie berechtigtes Interesse daran nachweist.³⁵³

³⁴⁷ Vgl ErlRV 1423 BlgNR XXII. GP 4; ErlRV 1324 BlgNR XXII. GP 3.

³⁴⁸ RIS-Justiz RS0079737; RS0077300.

³⁴⁹ OGH 10.12.1974, 4 Ob 347/74 (Kopierdienst).

³⁵⁰ Vgl *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 174 f mwN; Rz 256.

³⁵¹ Vgl *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 213 f.

³⁵² *Tonninger* in Kucsko, urheber.recht § 85 Pkt 4.4 f.

³⁵³ *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 166.

C.III.4.b. Urteilsveröffentlichung im Internet

Dem Talionsprinzip entsprechend haben Urteilsveröffentlichungen im Internet zu erfolgen, wenn dort die Rechtsverletzung gesetzt und damit eine breitere Öffentlichkeit erreicht wurde. Auch hier gilt nämlich, dass Zweck der Urteilsveröffentlichung ist, das Publikum über einen Gesetzesverstoß aufzuklären, welcher auch in Zukunft noch nachteilige Auswirkungen besorgen lässt. Die Urteilsveröffentlichung soll damit auch einer Weiterverbreitung unrichtiger Ansichten entgegenwirken.³⁵⁴

In der höchstgerichtlichen Rsp wurde insb darüber diskutiert, in welcher Form eine Urteilsveröffentlichung im Internet erfolgen soll, um diese Zwecke zu erfüllen. Zunächst sprach der OGH aus, dass sich diese Entscheidung nach den technischen Gegebenheiten des Internets zu richten hat. 2002 erschien es daher zweckmäßig, das Urteil in einem Fenster zu veröffentlichen, das sich öffnet, wenn der Internetnutzer auf eine bestimmte Seite gelangt (Pop-up-Fenster). Was die Größe des Fensters betrifft, so sah der OGH es als angemessen an, wenn das Fenster ein Viertel der Bildschirmoberfläche bedeckt; zeitlich erschien ihm eine Veröffentlichungsdauer von 30 Tagen als angemessen.³⁵⁵

Wegen der mit dem technischen Fortschritt einhergehenden (gerichtsnotorischen) Verbreitung von „Pop-up-Blockern“ ging der OGH von dieser Rsp aber wieder ab. Eine Urteilsveröffentlichung im Internet ist nicht nur in einem Pop-up-Fenster, sondern direkt auf der Webseite des in Anspruch genommenen Rechteinhabers erforderlich, um die gebotene Aufklärung des Publikums zu ermöglichen; auch 60 Tage Dauer können dabei angemessen sein.³⁵⁶ Eine Veröffentlichung in einem Pop-up-Fenster ist daher heute nur mehr geboten, wenn auch die Rechtsverletzung in einem solchen erfolgt ist.³⁵⁷

Mit der zunehmenden Verbreitung von Web 2.0 – Diensten wie der Videoplattform YouTube und Social Networks wie Facebook erfolgen auch vermehrt Rechtsverletzungen in diesen Teilen des Internets. Dem Talionsprinzip entsprechend werden daher ebendort Urteilsveröffentlichungen vorzunehmen sein, wenn die betroffenen Rechteinhaber ein berechtigtes Interesse daran haben.³⁵⁸ Hierbei spielt die richtige Formulierung des Urteilsbegehrens eine entscheidende Rolle, um maximale Aufklärungswirkung zu erzielen.³⁵⁹

³⁵⁴ StRsp, vgl RIS-Justiz RS0079820.

³⁵⁵ OGH 15. 10. 2002, 4 Ob 174/02w (BOSS-Zigaretten IV).

³⁵⁶ OGH 12.6.2007, 4 Ob 57/07x (Pop-up Fenster II).

³⁵⁷ *Tonninger* in Kuesko, urheber.recht § 85 Pkt 4.5 mwN.

³⁵⁸ Für geschäftsschädigende Äußerungen auf einer Profilseite von Facebook wurde dies vom HG Wien zur GZ 39 Cg 75/10p bereits bejaht und eine Urteilsveröffentlichung ebendort angeordnet. Vgl *Kommenda*, Österreichisches Urteil auf Facebook, Rechtspanorama, Die Presse 22.11.2010 und *Hofmarcher*, Auch Social-Network Profile bieten Platz für Urteilsveröffentlichungen, e-center law survey 12/2010.

³⁵⁹ Anschauliche Bsp zur richtigen Formulierung des Begehrens finden sich bei *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 329 f.

D. RECHTSVERLETZENDES FILESHARING

Filesharing³⁶⁰ beschreibt das direkte Weitergeben von Dateien zwischen Internetusern unter Verwendung eines besonderen Programms, das den Zugang zu sog „Tauschbörsen“ herstellen kann. Dabei befinden sich die getauschten Daten nicht auf einem zentralen Rechner, sondern auf den Computern der einzelnen Teilnehmer. IdR empfangen die User Daten von fremden Rechnern (Download), während sie gleichzeitig anderen Usern Daten zusenden (Upload). Da das verwendete Programm lediglich die Verbindung zu dem Netzwerk herstellt und für die Koordination der Weitergabe zwischen den Usern sorgt, die Daten aber zwischen den einzelnen Teilnehmern („Peers“) übertragen werden, spricht man von Peer-to-Peer-Netzwerken („P2P“). Dabei können zentralisierte P2P-Netze, die von einer Zentralstelle aus Indexinformationen verteilen, und dezentralisierte P2P-Netze, bei denen die User ausschließlich untereinander kommunizieren und auf keinerlei zentralen Mittler angewiesen sind, unterschieden werden. Verbreitet sind auch Hybrid-Systeme, bei denen einer der Peers eine Verteilerfunktion übernimmt.

Terminologisch korrekt müsste es statt „Tauschbörse“ eigentlich „Kopierbörse“ heißen, weil die Daten nach Abschluss des Kopiervorganges beim Bereitsteller nicht wie beim herkömmlichen Tauschen verschwinden, sondern nach wie vor vorhanden sind. Der Begriff „Tauschbörse“ hat sich aber dennoch eingebürgert, insbesondere weil er den Charakter des Gebens und Nehmens in Filesharing-Netzwerken treffend beschreibt.

Als „Urvater“ des Filesharings bekannt wurde das Programm Napster, das noch selbst einen Index aller verfügbaren Inhalte erstellte, die von den Teilnehmern angeboten wurden. Zudem war pro Datei nur das Laden von einem einzelnen anderen User möglich. Nachdem Napster im Juli 2001 nach heftigen Rechtsstreitigkeiten geschlossen wurde, trat das eDonkey-System, insb bekannt durch das Programm eMule, seine Nachfolge an. Weiterhin erstellte ein zentraler Server einen Index über die bei den Usern gespeicherten und verfügbaren Daten. Eine wichtige Neuerung war die Möglichkeit, von mehreren anderen Peers gleichzeitig Teile derselben Datei zu beziehen und so die Ladezeit deutlich zu verkürzen.

Der eigentliche „Erbe“ Napsters in punkto Popularität und öffentlicher Aufmerksamkeit ist heute aber das BitTorrent-Protokoll, das auf einer hybriden P2P-Technologie basiert. Um den Download zu beginnen, benötigt ein Teilnehmer zunächst eine kleine Datei (Torrent), die die nötigen Koordinationsinformationen für den Download enthält. Zur Verfügung gestellt werden diese von Plattformen wie <ThePirateBay.org>. Torrents enthalten Metadaten über die jeweils gesuchten Inhalte, darunter deren Namen und Dateigröße und die Netzwerkadresse eines Teilnehmers, der als „Tracker“ fungiert. Jedes Torrent kann Metadaten über eine oder mehrere Dateien enthalten und steht idR jedem offen, der ein geeignetes Torrent-

³⁶⁰ Vgl Wikipedia, <de.wikipedia.org/wiki/Filesharing>.

Programm wie uTorrent besitzt, mit dem er sich zum Torrent verbinden kann. Der Tracker spielt die Rolle eines Kontaktvermittlers und stellt zwischen allen Peers, die an der Übertragung eines Torrent teilnehmen, eine Verbindung her, indem er dem neuen Peer die Netzwerkadresse der anderen Teilnehmer, die am Datenaustausch beteiligt sind, übermittelt.

Jeder Torrent ist daher ein separates Verteilungsnetzwerk für eine oder mehrere spezifische Dateien, wodurch im BitTorrent-System statt einem einzigen großen Filesharing-Netz, wie es zB Napster war, zahlreiche separate Verteilungsnetzwerke geschaffen werden. Das Besondere ist, dass alle teilnehmenden Computer sich bereits aktiv an der Verbreitung beteiligen, bevor die jeweilige Datei noch fertig heruntergeladen wurde. Dies ist durch die Aufteilung der Gesamtdatei in kleine Stücke (chunks) möglich, die durch eine eindeutige Prüfsumme (checksum) validiert werden. Dieses System ermöglicht hohe Redundanzen, große Flexibilität und starke Übertragungsraten, ist aber davon abhängig, dass viele Teilnehmer denselben Torrent finden und gleichzeitig darin eingewählt sind. Insb durch die verschiedenen Prozesse gegen die Betreiber von <ThePirateBay.org> rückte Filesharing mit dem BitTorrent-Protokoll, ebenso wie früher Napster, wieder in den Mittelpunkt öffentlicher Debatten.³⁶¹ Anders als Napster kann BitTorrent nicht durch Angriffe auf einen zentralen Betreiber unterbunden werden, weil es auf einem offenen Protokoll basiert und unzählige Torrent-Websites existieren.

Die User von Tauschbörsen treten – abgesehen vom Datenaustausch - untereinander idR nicht weiter in Kontakt. In den meisten Filesharing-Programmen werden heute auch keine Nicknames mehr verwendet. Jeder User kann aber die IP-Adressen der anderen Peers im Netzwerk sehen.

Bei älteren Filesharing-Programmen wie Napster war es noch üblich, dass die User sich aussuchen konnten, ob sie lediglich downloaden wollen oder auch selbst durch Freigabe der Upload-Funktion Daten und Bandbreite für das Netzwerk zur Verfügung stellen. Da das System einer Tauschbörse aber nur funktioniert, wenn die Teilnehmer auch selbst Daten zur Verfügung stellen, sind neuere Programme so gestaltet, dass Uploaden zumindest während des Downloads verpflichtend ist. Ebenfalls verbreitet ist, dass die User dem Programm bestimmte Bereiche der Festplatte freigeben müssen, aus denen Daten für den Upload bezogen werden können. Nach dem Abschluss eines Downloads kann man sich idR zwar dennoch dem Uploaden entziehen, indem man den freigegebenen Bereich leer lässt. Zumindest beim heute populärsten Filesharing-System BitTorrent ist man während des Downloads aber immer gleichzeitig auch Uploader.

Personen, die nur für den Bezug von Inhalten an Tauschbörsen teilnehmen und selbst kaum bis gar keine Inhalte bereitstellen, werden in der Community eher verächtlich als „Leecher“

³⁶¹ Zu alldem vgl *Berger*, Die neuen Archivare, in *Owning the Mind* 40 f.

(engl für „Blutsauger“) bezeichnet. Um diesen möglichst wenig der begehrten Übertragungsraten abzugeben, werden in neueren Filesharing-Systemen, insb solchen nach dem BitTorrent-System, sogenannte Anti-Leech-Tracker eingesetzt. Dabei handelt es sich um Tracker, deren Ziel es ist, ein zumindest annähernd ausgeglichenes Verhältnis zwischen Upload- und Downloadvolumen sicherzustellen. Dazu wird die Datenmenge des Uploads durch die des Downloads dividiert, was die „ratio“ ergibt. Wenn diese Rechnung zu weit gegen Null führt, also deutlich mehr heruntergeladen als „zurückgegeben“ wird, wird dem jeweiligen „Leecher“ die Zugangsberechtigung entzogen oder die Downloadrate gesenkt.³⁶²

Auf Tauschbörsen sind ua Musik, Software, Filme oder Dokumente in großer Zahl und schwankender Qualität im Umlauf. Die Teilnahme an den großen P2P-Netzwerken, bei denen idR Millionen Nutzer gleichzeitig verbunden sind, ist dennoch praktisch immer kostenlos. Während urheberrechtliche Probleme somit auf der Hand liegen, sind andere Immaterialgüterrechte dagegen nicht betroffen. Denkbar wäre höchstens eine Verletzung von Markenrechten. Dies scheidet aber ebenfalls aus, weil das Ausschließungsrecht des Markeninhabers (§ 10 f MSchG) auf Situationen beschränkt ist, in denen seine geschützte Marke von einem Dritten kennzeichenmäßig (§ 10a MSchG) verwendet wird. User von Tauschbörsen werden aber nur in krassen Ausnahmefällen fremde Marken dazu benutzen, eigene Waren oder Dienstleistungen zu kennzeichnen. Die rechtlichen Probleme mit Tauschbörsen beschränken sich daher weitgehend auf das Urheberrecht.

Die Frage, inwiefern das Downloaden von urheberrechtlich geschützten Werken rechtsverletzend ist, ist nicht geklärt. Zwar wird eindeutig in das Vervielfältigungsrecht des Urhebers eingegriffen, weil eine Kopie der heruntergeladenen Datei auf der Festplatte des Users hergestellt wird – es stellt sich aber die Frage, ob dies nicht durch die freie Werknutzung in § 42 Abs 4 UrhG gedeckt ist.³⁶³ Für die Zwecke dieser Arbeit kann dies offenbleiben, denn Filesharing mit geschützten Werken ist in seiner heutigen Form jedenfalls urheberrechtsverletzend – allerdings deshalb, weil Teilnehmer in Tauschbörsen stets auch Uploader sind und damit in das Zurverfügungstellungsrecht eingreifen, das nach § 18a Abs 1 UrhG dem Urheber vorbehalten ist.³⁶⁴ Diese Rechtsverletzung ist in § 91 Abs 1 UrhG auch strafrechtlich sanktioniert.

D.I. Informationsbeschaffung

Bei Filesharing greifen die gesetzlichen Offenlegungspflichten für Websites nicht. An Tauschbörsen kann auch ohne Identitätskontrolle, wie sie bei legalen Anbietern (zB dem iTunes-Store) nötig ist, teilgenommen werden. Für die Informationsbeschaffung über Filesharing sind daher technische Überwachungsmaßnahmen und (daran anschließend) die Mit-

³⁶² Berger, Die neuen Archivare, in *Owning the Mind* 48; Wikipedia, <de.wikipedia.org/wiki/Bittorrent>.

³⁶³ Zum Meinungsstand vgl FN 293.

³⁶⁴ IdS auch OLG Wien 12. 4. 2007, 5 R 193/06y (LSG/Tele2; nicht rk).

hilfe der Access-Provider von entscheidender Bedeutung. Diese befinden sich aber auch in einem Treueverhältnis zu ihren zahlenden Kunden und sind daher tendenziell nicht geneigt, Dritten bei der Durchsetzung ihrer Immaterialgüterrechte zu helfen, wenn sie dafür wider die Interessen ihrer Kunden handeln müssen. Zu prüfen ist daher, inwiefern die Rechtsordnung auch Auskunftspflichten für Access-Provider über die Aktivitäten ihrer Kunden kennt und wie diese zivil- und strafrechtlich durchgesetzt werden können. Der Zugang zu derartigen Daten ist dabei durch datenschutzrechtliche Bestimmungen nur in Ausnahmefällen gestattet.

D.I.1. Exkurs: Die Überwachung von BitTorrent-Filesharing

Zur Sicherung von Beweisen für Abmahnungen und Klagen auf Unterlassung und Schadenersatz setzen Rechteinhaber im Kampf gegen P2P-Urheberrechtsverletzer in zunehmenden Maße auf die Dienste von spezialisierten Agenturen, die den Datenverkehr in Filesharing-Netzen überwachen und protokollieren (im folgenden „Monitoring-Agenturen“). Für die Beurteilung der rechtlichen Validität der so erlangten Informationen ist ein Überblick über die dabei verwendeten Techniken unerlässlich, wobei sich die folgenden Ausführungen auf das heute primär verwendete BitTorrent-Verfahren beschränken.³⁶⁵ Zu unterscheiden sind indirekte und direkte Ermittlungsmethoden.

Indirekte Ermittlungsmethoden setzen daran an, dass der koordinierende Tracker aufgrund seiner Rolle als Kontaktvermittler über eine Liste aller Peers in einem Torrent verfügt und für die gegenseitige Vernetzung allen Teilnehmern zur Verfügung stellt. Wenn eine Monitoring-Agentur sich in einen Torrent einwählt, bekommt daher auch sie Zugriff auf die Peer-Liste des Trackers. Die Liste enthält IP-Adressen aller Peers, kann aber nur darüber Auskunft geben, wer sich in den Torrent eingewählt und beim Tracker um die Adressen der bereits verbundenen Peers angefragt hat. Der tatsächliche Datentransfer wird nicht mitprotokolliert, weil dies für das Funktionieren des Torrents nicht nötig ist – die Programmierung des BitTorrent-Protokolls sorgt schon dafür, dass die einzelnen chunks der Datei innerhalb des Torrents richtig verteilt werden. Somit kann diese indirekte Ermittlungsmethode nur Auskunft darüber geben, welche IP-Adresse beim Tracker um Teilnahme am Torrent angefragt hat, aber nicht, ob über diese IP-Adresse dann tatsächlich Daten gesendet und empfangen wurden, geschweige denn eine genaue Aufstellung des so bewegten Datenvolumens.

Zusätzliche Brisanz erhält diese Tatsache dadurch, dass manche Tracker-Implementierungen es dem anfragenden User erlauben, dem Tracker für seine Liste der Peers im Torrent eine andere IP-Adresse anzugeben als die, von der er gerade seine Anfrage sendet. Diese Möglichkeit soll die Verwendung von Proxy-Servern, die andere IP-Adressen als der jeweilige User verwenden, erleichtern. Mit dieser Methode kann aber zB auch ein zum Filesharing klarer-

³⁶⁵ Die Ergebnisse der umfassenden Studie der University of Washington von *Piatek/Kohno/Krishnamurthy*, *Challenges and Directions for Monitoring P2P File Sharing Networks*, dienen dabei als Grundlage.

weise unbrauchbarer Netzwerkdrucker mit eigener IP-Adresse oder gar der PC eines unschuldigen Dritten „vorgeschoben“ werden.³⁶⁶ Denkbar wäre auch, dass ein User in einem öffentlichen WLAN eine bestimmte IP-Adresse zugewiesen bekommt, an P2P-Filesharing teilnimmt und danach ohne eindeutige Abmeldung vom Tracker seinen Laptop herunterfährt. Der Tracker führt die IP-Adresse für eine bestimmte Zeit weiterhin auf seiner Liste, was dazu führen könnte, dass Monitoring-Agenturen diese IP-Adresse für Filesharing ermitteln, obwohl zu diesem Zeitpunkt bereits ein anderer Nutzer des öffentlichen WLANs die IP-Adresse zugewiesen bekommen hat.³⁶⁷

Direkte Ermittlungsmethoden gehen daher einen Schritt weiter und verbinden sich mit allen Peers, die vom Tracker an die Peers gemeldet werden. Da mit diesen Peers dann auch tatsächlich versucht wird, Daten auszutauschen, können „false positives“ vermieden werden. Aufgrund des dabei notwendigerweise bewegten Datenvolumens sind derartige Ermittlungsmethoden aber weit aufwendiger und kostenintensiver. Zudem bleibt, zumindest nach dem BitTorrent-Protokoll, selbst bei direkten Ermittlungsmethoden unklar, wer wem wieviel Daten geschickt hat.³⁶⁸ Weiters verwenden viele P2P-User Blacklist-Programme wie zB PeerGuardian, die IP-Adressen von bekannten Monitoring-Agenturen sammeln und Verbindungsversuche von diesen unterbinden.

Es zeigt sich daher, dass die von Monitoring-Agenturen ermittelten IP-Adressen, die für Identifizierungsanfragen an Access-Provider verwendet werden, nicht notwendigerweise tatsächlich von Filesharern stammen müssen. Eine genaue Prüfung im Einzelfall ist daher erforderlich, um Missbrauch auszuschließen.

³⁶⁶ *Piatek/Kohno/Krishnamurthy*, Challenges and Directions for Monitoring P2P File Sharing Networks 3; den Autoren der Studie ist es mittels dieser Verschleierung tatsächlich gelungen, einen Netzwerkdrucker der University of Washington mit eigener IP-Adresse des Filesharings „anzuschwärzen“, was eine Abmahnung dieses Druckers seitens einer Monitoring-Agentur nach sich gezogen hat.

³⁶⁷ Vgl dazu und zu weiteren möglichen Missbrauchsvarianten *Piatek/Kohno/Krishnamurthy*, Challenges and Directions for Monitoring P2P File Sharing Networks 4.

³⁶⁸ Für jeden Teilnehmer innerhalb eines Torrents steht lediglich offen, welche Teile er selbst von welchem Peer bezogen hat bzw welcher er welchem Peer geschickt hat, und wie der Gesamtfortschritt eines jeden Peers aussieht. Woher andere Peers ihre Daten bezogen haben, kann er aber nicht feststellen, sofern er nicht selbst die Quelle war. Rechteinhaber können somit zwar selbst am Datenaustausch über Torrents teilnehmen und erfahren, welche IP-Adresse innerhalb des Torrents welche Menge an Daten insgesamt bezogen hat, aber nicht ohne invasive Maßnahmen (insb ohne ein Eindringen in Computersysteme der einzelnen Peers) feststellen, wer die Quellen dieser Daten waren. Denkbar wäre allenfalls, dass Rechteinhaber bzw Monitoring-Agenturen selbst als Tracker auftreten, den darüber laufenden Datenverkehr überwachen und Filesharern damit eine „Falle“ stellen.

D.I.2. Zivilrechtlicher Auskunftsanspruch gegen Access-Provider

D.I.2.a. Problemstellung

Wenn ein Internetuser sich mit Benutzernamen und Passwort ins Internet einklinkt, wird ihm vom Remote Access Server (RAS) seines Access-Providers eine IP-Adresse zugewiesen. Meistens greift der Access-Provider dabei auf einen ihm zur Verfügung stehenden Pool aus IP-Adressen zu und vergibt diese nach dem Zufallsprinzip an seine Kunden. Es kann daher sein, dass ein und demselben Nutzer mehrmals nacheinander die gleiche IP-Adresse zugewiesen wird – er kann aber genauso jedes Mal eine andere erhalten. Daher spricht man hierbei von „dynamischen“ IP-Adressen.

Sollte dem Kunden im Nutzungsvertrag vom Access-Provider eine bestimmte IP-Adresse zugesichert worden sein, die er dem Kunden bei jeder Internetverbindung verbindlich zuweist, so ist das eine „statische“ IP-Adresse. In der Praxis geschieht dies aufgrund des hohen Verwaltungsaufwands allerdings selten.³⁶⁹ Die Differenzierung ist aber aus datenschutzrechtlichen Gründen relevant.

Durch eigenständige Recherche oder durch eine Monitoring-Agentur kann eine IP-Adresse ermittelt werden, die zumindest wahrscheinlich (siehe obigen Exkurs) an Filesharing teilgenommen hat. Über eine Whois-Abfrage³⁷⁰ (zB über <whois.net>) kann im Anschluss sehr einfach festgestellt werden, welchem Access-Provider diese IP-Adresse zugeordnet ist. Der Name und die Anschrift des konkreten Kunden des Access-Providers sind über einfache Recherche allerdings nicht feststellbar. Lediglich der Access-Provider selbst kann mittels Auswertung der Log-Dateien seines RAS herausfinden, aufgrund welcher Zugangsdaten (Benutzername und Passwort) die angegebene IP-Adresse in welchem Zeitraum vergeben wurde. Mittelbar kann so einem Kunden des Access-Providers eine IP-Adresse zugeordnet werden. Wer zum Zeitpunkt des Filesharings konkret hinter dem fraglichen PC gesessen ist, kann allerdings auch der Access-Provider nicht bestimmen. Freilich ist aber davon auszugehen, dass der Kunde zumindest darüber informiert ist, wer unter Verwendung seiner Zugangsdaten eine Internetverbindung herstellt.

Für Inhaber von Immaterialgüterrechten ist die beschriebene Vorgangsweise praktisch die einzig realistische Möglichkeit, die Identität von Rechtsverletzern festzustellen. Aus Effizienzgründen wäre es für Rechteinhaber besonders wünschenswert, ohne Zwischenschaltung eines Gerichtes gleichsam „auf Zuruf“ die begehrten Auskünfte von den Access-Providern zu erhalten.

³⁶⁹ *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (114).

³⁷⁰ Vgl dazu oben S 41.

Für Access-Provider wiederum ist die Herausgabe der Daten prima facie nicht durchführbar, ohne vertragliche Schutz- und Sorgfaltspflichten gegenüber ihren Kunden zu verletzen. Schließlich setzten sie letztere damit (zumindest potentiell) der zivil- und strafrechtlichen Verfolgung aus. Aus Sicht der Access-Provider wäre daher, so überhaupt ein Auskunftsanspruch bejaht wird, ein geregeltes gerichtliches Verfahren nötig, um Rechtssicherheit gegenüber ihren Kunden zu haben.

Weiters liegt auf der Hand, dass die beschriebene Verarbeitung von IP-Adressen und die Herausgabe von Name und Anschrift in die Privatsphäre der Kunden eingreift und damit auch datenschutzrechtlich problematisch ist.

Das im Folgenden behandelte Problem wurzelt daher in einer Abwägung der Interessen von Internetusern auf Schutz ihrer personenbezogenen Daten einerseits und der Interessen von Rechteinhabern an der Durchsetzung ihrer (meist) urheberrechtlichen Ansprüche andererseits. Der Access-Provider befindet sich dazwischen praktisch in einer „Zwickmühle“.³⁷¹

D.I.2.b. Europarechtliche Grundlagen

Zunächst ist zu prüfen, ob das Unionsrecht eine zivilrechtliche Auskunftspflicht von Access-Providern verbietet, sie gestattet oder gar zwingend anordnet. Dabei sind die Info-RL, die Telekom-Datenschutz-RL, die Enforcement-RL sowie die E-Commerce-RL von Bedeutung. Peripher ist auch die Vorratsdatenspeicherungs-RL zu beachten – eine ausführliche Untersuchung ist aber hier nicht nötig.³⁷²

D.I.2.b.1. E-Commerce-RL

Die E-Commerce-RL trifft keine besonderen Regelungen zur Frage von Auskunftsansprüchen gegenüber Access-Providern. Sie legt in Art 18 Abs 1 lediglich fest, dass die Mitgliedstaaten sicher zu stellen haben, dass die nach innerstaatlichem Recht verfügbaren Klagemöglichkeiten im Zusammenhang mit Diensten der Informationsgesellschaft es ermöglichen, dass rasch Maßnahmen, einschließlich vorläufiger Maßnahmen, getroffen werden können, um eine mutmaßliche Rechtsverletzung abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht. Zudem stellt Art 15 Abs 2 klar, dass die Mitgliedstaaten Anbieter von Diensten der Informationsgesellschaft dazu verpflichten können, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder den zuständigen Behörden auf Verlangen Informationen

³⁷¹ Vgl. *Raschhofer/Steinhofer*, Zwischen Urheber und Kunde: Provider in der Zwickmühle, Rechtspanorama, Die Presse 5.10.2009; eine "Zwickmühle" für Provider ortete bereits *Zankl*, E-Commerce-Gesetz Rz 274.

³⁷² Für weitergehende Informationen zur Vorratsdatenspeicherungs-RL vgl. *Liebwald*, The New Data Retention Directive, MR-Int 2006, 49.

zu übermitteln, anhand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.

Grds gilt aber gem Art 15 Abs 1, dass die Mitgliedstaaten Anbietern von Diensten im Sinne der Art 12, 13 und 14 (also Access und Host Providing sowie Caching) keine allgemeine Verpflichtung auferlegen dürfen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

Die RL lässt damit den Mitgliedstaaten einen weiten Ermessensspielraum bei ihrer Umsetzung und verpflichtet sie jedenfalls nicht dazu, einen zivilrechtlichen Auskunftsanspruch gegenüber Access-Providern vorzusehen.³⁷³

D.I.2.b.2. Info-RL

Zentrale Norm für das hier interessierende Problem ist der mit „Sanktionen und Rechtsbehelfe“ überschriebene Art 8 Info-RL.

Nach dessen Abs 1 haben die Mitgliedstaaten bei Verletzungen der in dieser RL festgelegten Rechte und Pflichten³⁷⁴ angemessene Sanktionen und Rechtsbehelfe vorzusehen und alle notwendigen Maßnahmen zu treffen, um deren Anwendung sicherzustellen. Die betreffenden Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Abs 2 leg cit hält fest, dass jeder Mitgliedstaat die erforderlichen Maßnahmen trifft, um sicherzustellen, dass Rechtsinhaber, deren Interessen durch eine in seinem Hoheitsgebiet begangene Rechtsverletzung beeinträchtigt werden, Klage auf Schadenersatz erheben und/oder eine gerichtliche Anordnung sowie gegebenenfalls die Beschlagnahme von rechtswidrigem Material sowie von Vorrichtungen, Erzeugnissen oder Bestandteilen zur Umgehung von wirksamen technischen (Kopierschutz-)Maßnahmen beantragen können.

Schließlich ordnet Abs 3 leg cit an, dass die Mitgliedstaaten sicherstellen, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Strittig war dabei lange, ob Access-Provider unter den Begriff „Vermittler“ fallen. Da der europäische Gesetzgeber mit Abschnitt 4 der E-Commerce-RL die „Verantwortlichkeit der Vermittler“ regeln wollte,³⁷⁵ und die einschlägige Regelung in deren Art 12, unter der Überschrift „Reine Durchleitung“, Access-Provider betrifft, ist es mE schon aus Gründen der

³⁷³ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 59.

³⁷⁴ Diese betreffen gem Art 1 der RL (nur) das Urheberrecht und die dazu verwandten Schutzrechte.

³⁷⁵ Dazu oben S 67; vgl weiters etwa *Stomper*, Europäische Union regelt E-Commerce Die EU-Richtlinie über den Elektronischen Geschäftsverkehr im Überblick, SWK 2000, W 59.

Einheitlichkeit der Rechtsordnung eindeutig, dass Access-Provider „Vermittler“ sind.³⁷⁶ Der EuGH kam zum selben Ergebnis.³⁷⁷

Insbesondere auf die Auslegung von Art 8 Abs 3 Info-RL wurde gestützt, dass das Unionsrecht einen Auskunftsanspruch gegen Access-Provider „ausdrücklich“ normiere.³⁷⁸ Dies ist mE nicht im Wortlaut der Bestimmung unterzubringen. Die Formulierung „gerichtliche Anordnungen“ lässt den Mitgliedstaaten vielmehr erneut einen breiten Ermessensspielraum für die Umsetzung in nationales Recht, weil sie eben nicht festlegt, welche „Anordnungen“ in den nationalen Rechtsordnungen genau vorzusehen sind.³⁷⁹ Der EuGH stellte folgerichtig in der Entscheidung „Promusicae“ auch fest, dass die Info-RL den Mitgliedstaaten nicht gebietet, im Hinblick auf einen effektiven Schutz des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.³⁸⁰

Art 9 Abs 1 sieht schließlich vor, dass die Info-RL ua Rechtsvorschriften im Bereich „Datenschutz und Schutz der Privatsphäre“ unberührt lässt.

D.I.2.b.3. Enforcement-RL

Art 3 Enforcement-RL legt fest, dass die Mitgliedstaaten Maßnahmen, Verfahren und Rechtsbehelfe vorsehen, die zur Durchsetzung der Rechte des geistigen Eigentums, auf die diese RL abstellt, erforderlich sind. Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen fair und gerecht sein, außerdem dürfen sie nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen. Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen darüber hinaus wirksam, verhältnismäßig und abschreckend sein und so angewendet werden, dass die Einrichtung von Schranken für den rechtmäßigen Handel vermieden wird und die Gewähr gegen ihren Missbrauch gegeben ist.

³⁷⁶ Ebenso *Schachter*, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz - Anlässe Promusicae und MediaSentry, jusIT 2008 H 2, 20; aA *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 115.

³⁷⁷ EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 43 f; vgl unten S 133.

³⁷⁸ *Schanda*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 215; ebenfalls eine unionsrechtliche Gebotenheit des Auskunftsanspruchs ordend *Daum*, Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug!, MR 2009, 249.

³⁷⁹ So auch *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 665.

³⁸⁰ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 70; der EuGH nennt in Rz 59 zwar nur Art 8 Abs 1 und 2 Info-RL, was aber im Zusammenhang mit der Vorlagefrage zu verstehen ist. Das spanische Vorlagegericht hatte nur auf diese beiden Absätze Bezug genommen und nach Abs 3 leg cit nicht ausdrücklich gefragt. Mit seinem Spruch stellte der EuGH aber indirekt klar, dass diese Auslegung auch für Abs 3 leg cit gelten muss.

Art 8 regelt den speziellen Anspruch auf Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen. Abs 1 lit c leg cit schreibt in diesem Zusammenhang vor, dass sichergestellt sein muss, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahren Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbracht.

Nach Art 8 Abs 3 lit a und e gilt diese Bestimmung unbeschadet anderer gesetzlicher Bestimmungen, die (a) dem Rechtsinhaber weiter gehende Auskunftsrechte einräumen bzw (e) den Schutz der Vertraulichkeit von Informationsquellen oder die Verarbeitung personenbezogener Daten regeln.

Der „Ursprung und die Vertriebswege von Waren, die ein Recht des geistigen Eigentums verletzen“ schließt bei Musikdateien, die über ein Filesharing-Programm getauscht werden, wohl auch die Identität des Inhabers des für den Tausch verwendeten Internetanschlusses ein.³⁸¹ Ein Access-Provider erbringt durch die Bereitstellung des Internetzugangs gegen Entgelt zudem eine Dienstleistung in gewerblichem Ausmaß.

Zumindest dem Wortlaut laut nach könnte der Bestimmung des Art 8 Abs 1 der RL daher unterstellt werden, die Offenlegung der Identität von Internetnutzern anzuordnen. Jedoch geht nach Auffassung des EuGH auch aus dieser Bestimmung vor dem Hintergrund der erwähnten Bestimmung des Art 8 Abs 3 lit e, die Datenschutzbestimmungen ausdrücklich unberührt lässt, letztlich nicht hervor, dass die Mitgliedstaaten verpflichtet wären, zur Sicherstellung eines effektiven Schutzes des Urheberrechts eine Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilgerichtlichen Verfahrens vorzusehen.³⁸²

D.I.2.b.4. Telekom-Datenschutz-RL

Die Telekom-Datenschutz-RL präzisiert und erweitert die „allgemeine“ Datenschutz-RL und gehört mit dieser gemeinsam in das System der Rahmen-RL. Ihr Anwendungsbereich erstreckt sich gem Art 3 auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft (Union), einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Access-Provider, die den Zugang zum Internet ermöglichen, stellen zweifellos elektronische Kommunikations-

³⁸¹ In diesem Sinn auch GA Kokott, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 110.

³⁸² EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 58.

dienste in öffentlichen Kommunikationsnetzen bereit.³⁸³ Weiters kann ein Access-Provider, wie bereits dargestellt, ein Auskunftsbeghen über die Identität von Internetusern nur dann erfüllen, wenn er eine IP-Adresse anhand seiner Log-Dateien mit einem bestimmten Nutzer verknüpft. Das ist somit ebenso zweifellos eine Verarbeitung personenbezogener Daten, weil die IP-Adressen in diesem Zusammenhang die indirekte Identifikation von natürlichen Personen ermöglichen.³⁸⁴

Die Zulässigkeit von Auskunftsansprüchen ist daher anhand der Telekom-Datenschutz-RL zu überprüfen. Deren Schutz erstreckt sich gem Art 5 Abs 1 auf mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten.³⁸⁵ Insbesondere untersagt Art 5 Abs 1 das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Art 15 Abs 1 Telekom-Datenschutz-RL gesetzlich dazu ermächtigt sind.

Der Einfachheit halber ist vorab festzuhalten, dass die üblichen dynamischen IP-Adressen jedenfalls Verkehrsdaten sind. Die selteneren statischen IP-Adressen fallen zusätzlich auch unter den (nur in Österreich gebräuchlichen) Begriff der Stammdaten³⁸⁶, weil sie aufgrund ihrer vertraglichen Zusicherung zur Abwicklung der Rechtsbeziehung zwischen Access-Provider und seinem Kunden erforderlich sind.³⁸⁷

Art 6 bestimmt, dass Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen

³⁸³ „Elektronische Kommunikationsdienste“ sind gem Art 2 lit c Rahmen-RL gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben.

³⁸⁴ „Personenbezogene Daten“ sind gem Art 2 lit a Datenschutz-RL alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

³⁸⁵ „Verkehrsdaten“ sind gem Art 2 lit b Telekom-Datenschutz-RL Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

³⁸⁶ Diese sind in § 92 Abs 3 Z 3 TKG definiert als alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind.

³⁸⁷ *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 671 mwN.

Kommunikationsdienstes verarbeitet und gespeichert werden, zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. Dies gilt jedoch unbeschadet der Ausnahmen in Abs 2, 3 und 5 leg cit und Art 15 Abs 1.

Die Ausnahmen in Art 6 Abs 2 und 3 der Telekom-Datenschutz-RL sind in Bezug auf die Speicherung von Verkehrsdaten für Auskünfte über die Identität von Urheberrechtsverletzern nicht einschlägig, weil sie nur Ausnahmen von der allgemeinen Löschpflicht für Verrechnungs- bzw Marketingzwecke aufstellen. Abs 5 bestimmt, dass Verkehrsdaten an Dritte weitergegeben werden können, wenn diese auf Weisung des Zugangsanbieters für bestimmte Zwecke, insbesondere für die Betrugsbekämpfung, Verkehrsdaten verarbeiten. ErwGr 29 stellt klar, dass mit Betrug die Nutzung elektronischer Kommunikationsdienste ohne entsprechende Bezahlung gemeint ist. Da Urheberrechtsverletzungen kein Betrug in diesem Sinn sind und Rechteinhaber nicht auf Weisung der Access-Provider agieren, ist auch diese Ausnahme von der allgemeinen Löschungspflicht nicht einschlägig.³⁸⁸

Art 15 Abs 1 sieht demgegenüber weitergehende Ausnahmen bei der Vertraulichkeit von Verkehrsdaten vor. Er legt fest, dass die Mitgliedstaaten Rechtsvorschriften³⁸⁹ erlassen können, die die Rechte und Pflichten gemäß Art 5 und Art 6 der Telekom-Datenschutz-RL beschränken, sofern eine solche Beschränkung gemäß Art 13 Abs 1 Datenschutz-RL für die nationale Sicherheit (dh die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Abs aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Abs genannten Maßnahmen müssen den allgemeinen Grundsätzen des Unionsrechts einschließlich den in Art 6 Abs 1 und 2 EUV niedergelegten Grundsätzen entsprechen. Zu beachten ist auch, dass diese Grundsätze gem Art 15 Abs 1a Telekom-Datenschutz-RL nicht für die Daten gelten, die aufgrund der Vorratsdatenspeicherungs-RL gespeichert werden.

Um eine Auskunftspflicht für Access-Provider über die Identität von Internetusern in einer nationalen Rechtsvorschrift vorsehen zu können, muss also eine Beschränkung des in Art 5 und 6 Telekom-Datenschutz-RL vorgesehen Schutzes von Verkehrsdaten in Einklang mit Art 15 derselben RL stehen. Andernfalls wäre ein Auskunftsanspruch wegen des Vorrangs des Unionsrechts unzulässig.

Ob sich eine Auskunftspflicht, die die Durchsetzung urheberrechtlicher Interessen im Blick hat, unter einen der Fälle des Art 15 Abs 1 Telekom-Datenschutz-RL subsumieren lässt, ist

³⁸⁸ Vgl GA Kokott, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 72.

³⁸⁹ Zur Auslegung dieses Begriffes vgl OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2).

nach dem Wortlaut der Bestimmung fraglich. Unklar ist weiters, wie der Verweis auf Art 13 Datenschutz-RL zu verstehen ist, insbesondere ob die dort genannten Ausnahmen auch für den Telekommunikationsbereich gelten oder ob Art 15 Abs 1 vielmehr eine abschließende Regelung darstellt.

Art 13 Abs 1 Datenschutz-RL lautet:

„Ausnahmen und Einschränkungen

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

a) die Sicherheit des Staates;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;

e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;

f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;

g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.“

Entscheidend ist daher vor allem, ob lit g auch im Telekommunikationsbereich gilt, weil sich unter die Formulierung „Schutz der Rechte anderer Personen“ auch die Ansprüche von Urheberrechtinhabern subsumieren lassen. Wären die in Art 15 Abs 1 Telekom-Datenschutz-RL genannten Gründe dagegen taxativ, müsste sich eine Ausnahme schon in diesem Art selbst finden.

Diese Fragen mussten durch den EuGH beantwortet werden. Er bekam anlässlich eines spanischen Falles („Promusicae“), in dem eine Verwertungsgesellschaft Auskunftsansprüche gegen einen Access-Provider geltend machen wollte, Gelegenheit dazu.

Die zuständige GA Kokott betonte in ihrem Schlussantrag zur Rs „Promusicae“, dass die Telekom-Datenschutz-RL sich in Art 15 Abs 1 konkret auf die personenbezogenen Daten beziehe, die im Rahmen der elektronischen Kommunikation anfallen. Daher beruhe sie auf einer vergleichsweise präzisen Einschätzung, wie stark eine Weitergabe personenbezogener Verkehrsdaten in das Grundrecht auf Datenschutz eingreift. Art 13 Abs 1 Datenschutz-RL dagegen sei verhältnismäßig allgemein gehalten, da er auf viele ganz unterschiedliche Situationen

Anwendung finden soll. Die differenzierte Regelung in Art 15 Abs 1 der Telekom-Datenschutz-RL beruhe daher auf einer bewussten Entscheidung im Gesetzgebungsverfahren, sodass der Schutz der Rechte und Freiheiten anderer Personen nach Art 13 Abs 1 lit g Datenschutz-RL die Weitergabe von personenbezogenen Verkehrsdaten nicht rechtfertigen könne.³⁹⁰

Unter den verbleibenden fünf Ausnahmetatbeständen, die in Art Abs 15 Telekom-Datenschutz-RL selbst zu finden sind, identifizierte die GA va eine mögliche Rechtfertigung für die Weitergabe von personenbezogenen Daten, nämlich den „unzulässigen Gebrauch von elektronischen Kommunikationssystemen“. Sie kam aber – in Einklang mit der Stellungnahme der Europäischen Kommission - zu dem Ergebnis, dass der unzulässige Gebrauch von elektronischen Kommunikationssystemen nur den systemwidrigen Gebrauch, nicht aber den Gebrauch zu unzulässigen Zwecken umfasse. Eine Ausnahme für den Gebrauch zu unzulässigen Zwecken, wie zB Urheberrechtsverletzungen, sei in ihrer Anwendung kaum vorhersehbar und würde das Recht auf Schutz personenbezogener Verkehrsdaten weitgehend entleeren. Weiters würden die übrigen vier Ausnahmetatbestände in Art 15 Telekom-Datenschutz-RL weitgehend ihrer praktischen Wirksamkeit beraubt, da Gefährdungen der nationalen Sicherheit, der öffentlichen Sicherheit und der Landesverteidigung sowie Straftaten durch den Gebrauch von elektronischen Kommunikationssystemen regelmäßig mit einem unzulässigen Zweck einhergehen.

GA *Kokott* zog daher mangels Ausnahmebestimmung den Schluss, dass das Unionsrecht eine Weitergabe von Useridentitäten für die Durchsetzung von Urheberrechten nicht zulässt. Sollte die Gemeinschaft (Union) einen weiter reichenden Schutz der Inhaber von Urheberrechten für notwendig erachten, so würde dies eine Änderung der Bestimmungen über den Datenschutz voraussetzen. Bislang habe der Gesetzgeber diesen Schritt allerdings noch nicht unternommen.³⁹¹

Dieser sehr differenzierten und überzeugenden Argumentation ist der EuGH allerdings nicht gefolgt.³⁹² Er hielt zwar analog zu den Ausführungen der GA fest, dass keine der Ausnahmen in Art 15 Abs 1 Telekom-Datenschutz-RL Situationen zu betreffen scheint, die die Erhebung einer zivilrechtlichen Klage erfordern. Der erkennende Senat gelangte jedoch zur Auffassung, dass Art 15 Abs 1 Telekom-Datenschutz-RL die Aufzählung der oben genannten Ausnahmen damit abschließe, dass er ausdrücklich auf Art 13 Abs 1 der (allgemeinen) Datenschutz-RL verweise. Nach dieser Vorschrift können die Mitgliedstaaten, wie oben erwähnt, ebenfalls Rechtsvorschriften erlassen, die die Pflicht zur Wahrung der Vertraulichkeit personenbezogener Daten beschränken, sofern eine solche Beschränkung ua für den Schutz der Rechte und

³⁹⁰ GA *Kokott*, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 85-89.

³⁹¹ GA *Kokott*, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 126.

³⁹² EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 53 f.

Freiheiten anderer Personen notwendig ist. Da diese Bestimmungen des Art 15 Abs 1 Telekom-Datenschutz-RL die betreffenden Rechte und Freiheiten nicht benennen, seien sie laut dem EuGH dahin auszulegen, dass sie den Willen des Gemeinschaftsgesetzgebers zum Ausdruck bringen, weder das Eigentumsrecht noch Situationen von ihrem Anwendungsbereich auszuschließen, in denen sich die Urheber im Rahmen eines zivilrechtlichen Verfahrens um diesen Schutz bemühen.

Aus dieser – methodisch durchaus kritikwürdigen – Auslegung folgert der EuGH ohne weitere Begründung, dass die (generelle) Ausnahme der Datenschutz-RL auch im (spezielleren) Anwendungsbereich der Telekom-Datenschutz-RL greift. Entgegen der Ansicht der GA *Ko-kott* kam er daher zu dem Ergebnis, dass die Telekom-Datenschutz-RL nicht die Möglichkeit der Mitgliedstaaten ausschließt, eine Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.³⁹³

Der Wortlaut des Art 15 Abs 1 Telekom-Datenschutz-RL kann dem EuGH zufolge jedoch auch nicht dahin ausgelegt werden, dass die Mitgliedstaaten in den in dieser Vorschrift aufgezählten Situationen gezwungen wären, eine solche Pflicht vorzusehen.³⁹⁴

D.I.2.b.5. Zwischenergebnis

Seit der Entscheidung „Promusicae“ ist, europarechtlich betrachtet, „die Tür auf“ für zivilrechtliche Auskunftsansprüche in den Rechtsordnungen der Mitgliedstaaten.³⁹⁵ Das Unionsrecht steht der Möglichkeit der Mitgliedsstaaten, eine Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen, nicht entgegen.

Der EuGH stellte in der genannten Entscheidung fest, dass die oben dargestellten RL es den Mitgliedstaaten nicht gebieten, in einer Situation wie der des Ausgangsverfahrens im Hinblick auf einen effektiven Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen.³⁹⁶ Die Mitgliedstaaten sind gemäß dem Unionsrecht jedoch dazu verpflichtet, sich bei der Umsetzung dieser Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien haben die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit diesen Richtlinien auszulegen, sondern auch darauf zu achten, dass

³⁹³ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 54.

³⁹⁴ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 55.

³⁹⁵ Dazu krit *Spindler*, „Die Tür ist auf“ –Urteilsanmerkung zu EuGH „Promusicae/Telefónica“, GRUR 2008, 574.

³⁹⁶ Insofern verfehlt *Daum*, Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug!, MR 2009, 249, der die Auskunft über Userdaten unter Verarbeitung von personenbezogenen Verkehrsdaten offenbar auch nach „Promusicae“ für unionsrechtlich geboten hält.

sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Unionsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert.³⁹⁷ Der Spielraum für die Mitgliedsstaaten ist damit aufgrund der vom EuGH gewählten Formulierung sehr weit.³⁹⁸

In einem weiteren Vorlageverfahren³⁹⁹, dem ein Streit zwischen der österreichischen Verwertungsgesellschaft LSG und dem Access-Provider Tele2 vorausging, bestätigte der EuGH auf Frage des OGH nochmals, dass das Unionsrecht einen Auskunftsanspruch weder vorschreibt noch ihm entgegensteht. Er wich aber von der Formulierung seines Spruchs in „Promusicae“ insofern ab, als er nicht mehr von einer „Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens“ sprach.⁴⁰⁰ Vielmehr hielt er fest, dass das Unionsrecht, insbesondere Art 8 Abs 3 Enforcement-RL iVm Art 15 Abs 1 Telekom-Datenschutz-RL, die Mitgliedstaaten nicht daran hindert, eine Verpflichtung zur Weitergabe personenbezogener Verkehrsdaten an private Dritte zum Zweck der zivilgerichtlichen Verfolgung von Urheberrechtsverstößen aufzustellen.⁴⁰¹ Das Erfordernis eines „zivilgerichtlichen Verfahrens“, aus dem viele ableiteten, dass ein Richtervorbehalt unionsrechtlich vorgegeben sei,⁴⁰² wurde damit nach Meinung des OGH aufgegeben.⁴⁰³

D.I.2.c. Nationale Rechtslage

Die dargestellten RL wurden in österreichisches Recht umgesetzt. Im österreichischen Immaterialgüterrecht finden sich daher an mehreren Stellen Regelungen über Auskunftsansprüche.

Die naheliegendste Anspruchsgrundlage bildet § 87b Abs 3 UrhG, der deshalb als erstes zu untersuchen ist. Weiters von Interesse sind auch § 87b Abs 1 UrhG und die beinahe wortgleichen Bestimmungen § 87b Abs 2 UrhG und § 55a MSchG.

³⁹⁷ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 70.

³⁹⁸ So auch *Barbist*, Auskunftspflicht: Streit Provider vs Musikindustrie Reloaded Das EuGH-Urteil in Sachen Promusicae, MR 2007, 416 f; *Walter*, Glosse zu OGH 13. 11. 2007, 4 Ob 141/07z, MR 2007, 443.

³⁹⁹ EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2).

⁴⁰⁰ Eigene Hervorhebung.

⁴⁰¹ EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 29.

⁴⁰² IdS *Barbist*, Auskunftspflicht: Streit Provider vs Musikindustrie Reloaded Das EuGH-Urteil in Sachen Promusicae, MR 2007, 416; *Schachter*, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz - Anlassfälle Promusicae und MediaSentry, jusIT 2008 H 2, 20; unklar *Walter*, Glosse zu 4 Ob 141/07z, MR 2007, 443; offen lassend *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25 (28).

⁴⁰³ OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2); aA *Raschhofer/Steinhofer*, § 87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig?, eolex 2010, 716 (718). Zur Frage der Erforderlichkeit eines Richtervorbehaltes noch ausführlich unten S 137 f.

D.I.2.c.1. § 87b Abs 3 UrhG

§ 87b. (3) Vermittler im Sinn des § 81 Abs. 1a haben dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. In die Begründung sind insbesondere hinreichend konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen.

Der selbständige Auskunftsanspruch nach § 87b Abs 3 UrhG wurde durch die UrhG-Novelle 2003,⁴⁰⁴ die ihrerseits die Info-RL umsetzte, eingeführt. Die Stammfassung lautete noch:

Vermittler im Sinne des § 81 Abs. 1a haben dem Verletzten Auskunft über die Identität des Verletzers (Name und Anschrift) zu geben.

Laut den Materialien⁴⁰⁵ sollte damit der in Art 8 Abs 3 Info-RL normierte und in § 81 Abs 1a UrhG umgesetzte Anspruch auf Unterlassung gegenüber einem „Vermittler“ ergänzt werden. Sein Anwendungsbereich, sein Ziel und seine Stellung in der Rechtsordnung sind dabei weder im Gesetzestext noch in den Materialien ausreichend erörtert worden, was durch die Novelle 2006⁴⁰⁶ zu korrigieren versucht wurde.

Der JA hielt damals fest, dass aus seiner Sicht die vorgesehenen Auskunftsansprüche gegen Vermittler der Bekämpfung des illegalen Uploads von Musik und Film im Internet und damit der Bekämpfung der Verbreitung illegaler Film- und Musikkraubkopien dienen. Dabei gehe es in erster Linie darum, dass die betroffenen Rechteinhaber die Personen identifizieren können, die Inhaber von Internetanschlüssen sind, die die Verletzten als Quelle illegaler Raubkopien durch Recherchen im Internet bereits festgestellt haben. Der Auskunftsanspruch sei daher erforderlich, um den Rechteinhabern die Möglichkeit zu geben, gegen eine solche eindeutig als rechtswidrig identifizierte Handlung gerichtlich vorzugehen.⁴⁰⁷

Durch die Novelle 2006 wurden weiters ein Schriftlichkeitsgebot und eine Aufwandsentschädigungspflicht für erteilte Auskünfte eingeführt. Auch sollten nur mehr ausreichend begründete Verlangen seitens der Rechteinhaber die Auskunftspflicht schlagend werden lassen. Um den Einwand abzuschneiden, es sei nicht sicher, ob der Inhaber des Anschlusses selbst die Urheberrechtsverletzung begangen habe, hat der Vermittler nun auch die zur Feststellung des Verletzers benötigten Auskünfte zu geben.⁴⁰⁸

⁴⁰⁴ BGBl I 32/2003.

⁴⁰⁵ ErlRV 40 BlgNR XXII. GP 44.

⁴⁰⁶ BGBl I 81/2006.

⁴⁰⁷ JAB 1508 BlgNR XXII. GP 2.

⁴⁰⁸ ErlRV 1324 BlgNR XXII. GP 4.

Das Grundproblem, nämlich das Verhältnis zum Datenschutzrecht, wurde seitens des Gesetzgebers aber nicht behandelt. Daher war für um Auskunft über Nutzerdaten ersuchte Access-Provider nicht klar, ob und unter welchen Umständen Daten zu speichern und herauszugeben sind. Mangels eindeutiger Regelung kam es zu Debatten in Lehre und Praxis, die vor allem um folgende Probleme kreisten:

D.I.2.c.1.1. Access-Provider als „Vermittler“ iSv § 87b Abs 3 UrhG

Fraglich war, ob Access-Provider „Vermittler“ iS des § 87b Abs 3 UrhG und damit für Auskunftsansprüche passivlegitimiert sind.

*Einzingler/Schubert/Schwabl/Wessely/Zykan*⁴⁰⁹ führten hierzu aus, dass Art 8 Abs 3 Info-RL verlange, dass Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, "deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden". Der Access-Provider ermögliche dem Nutzer jedoch nur den Zugang zum Netz, stelle ihm allerdings prinzipiell selbst keine Dienste (wie E-Mail, FTP oder eben insbesondere einen Filesharing-Dienst) zur Verfügung. In P2P-Netzwerken werde das "service" zwischen P2P-Applikationen (Filesharing-Software) aufgebaut und abgewickelt, der Access-Provider stelle nur den Verkehrsweg bis zum Internet-Backbone zur Verfügung und übe keinerlei rechtliche oder faktische Kontrolle über den verwendeten Dienst aus. Eine Einbeziehung der Access-Provider in den Begriff des Vermittlers würde also zu einem ähnlich absurden Ergebnis führen, als würde man einen Straßenerhalter zur Auskunft darüber verpflichten, wer die von ihm betriebene Straße benützt.

*Schanda*⁴¹⁰ als Vertreter der Gegenansicht argumentierte, dass es lediglich eines Nachlesens der Verweiskette in § 87b Abs 3 UrhG, der auf § 81 Abs 1a UrhG verweist, der wiederum ausdrücklich auf die §§ 13 - 17 ECG verweist, bedürfe. § 13 ECG beschreibe bekanntlich den Access-Provider. Auch die Info-RL, deren Umsetzung § 81 Abs 1a diene, beziehe sich auf "Vermittler" und meine damit alle Erbringer von Diensten der Informationsgesellschaft, also auch Access-Provider.

Der letzteren Ansicht ist der Vorzug zu geben, weil aus systematischer Interpretation nur dieses Ergebnis folgen kann (vgl auch oben die Ausführungen zur E-Commerce-RL).⁴¹¹ Mittlerweile wurde die Frage auch von der Judikatur in diesem Sinn gelöst. Anlässlich des Vora-

⁴⁰⁹ *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 115 f.

⁴¹⁰ *Schanda*, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 18.

⁴¹¹ Ebenfalls der systematischen Interpretation den Vorzug vor Schutzzwecküberlegungen gebend *Wiebe*, Auskunftsverpflichtung der Access Provider, MR 2005 Beilage H 4, 4 f; *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25 (27); *Schachter* in Kucsko, urheber.recht § 87b Pkt 3.2.; vgl auch die Materialien zur UrhG-Novelle 2003: ErlRV 40 BlgNR XXII. GP 42.

bentscheidungsverfahrens „LSG/Tele2“ legte der OGH dem EuGH die Frage vor, ob Access-Provider „Vermittler“ sind.

In seinem mit Gründen versehenen Beschluss⁴¹² erläuterte der EuGH zunächst, dass auch ein Access-Provider, der dem Kunden lediglich den Zugang zum Internet verschafft, ohne überhaupt weitere Dienste anzubieten oder eine rechtliche oder faktische Kontrolle über den genutzten Dienst auszuüben, einen Dienst bereitstellt, der von einem Dritten genutzt werden kann, um ein Urheberrecht oder ein verwandtes Schutzrecht zu verletzen, da er dem Nutzer zu der Verbindung verhilft, die diesem die Verletzung solcher Rechte ermöglicht.

Diese Auslegung stützte der Gerichtshof auch auf ErwGr 59 der Info-RL, wonach Rechteinhaber die Möglichkeit haben sollen, eine gerichtliche Anordnung gegen einen Vermittler zu beantragen, der die Rechtsverletzung eines Dritten in Bezug auf ein geschütztes Werk oder einen anderen Schutzgegenstand in einem Netz überträgt. Der Access-Provider ermögliche durch die Gewährung des Internetzugangs die Übertragung solcher Rechtsverletzungen zwischen einem Kunden und einem Dritten.

Zudem sei es die Zielsetzung der Info-RL, den effektiven rechtlichen Schutz des Urheberrechts und der verwandten Schutzrechte im Rahmen des Binnenmarkts sicherzustellen. Schlösse man einen Access-Provider, der als Einziger im Besitz der Daten ist, anhand deren die Nutzer, die solche Rechte verletzt haben, identifiziert werden können, vom Begriff des Vermittlers im Sinne des Art 8 Abs 3 Info-RL aus, würde der von der RL beabsichtigte Schutz wesentlich verringert.

Der EuGH kam daher zu dem Ergebnis, dass ein Access-Provider, der den Nutzern nur den Zugang zum Internet verschafft, ohne weitere Dienste wie insbesondere E-Mail, FTP oder Filesharing anzubieten oder eine rechtliche oder faktische Kontrolle über den genutzten Dienst auszuüben, „Vermittler“ im Sinne des Art 8 Abs 3 Info-RL ist.⁴¹³

D.I.2.c.1.2. IP-Adressen und ihre Verarbeitung

Fraglich ist, wie IP-Adressen und ihre Verarbeitung iS der Datenschutzvorschriften rechtlich zu beurteilen sind. Wie bereits oben erörtert, wird in Literatur und Judikatur einhellig zwischen dynamischen und statischen IP-Adressen unterschieden.⁴¹⁴ Erstere gehören nach hA

⁴¹² EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 43 f.

⁴¹³ EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 46.

⁴¹⁴ *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116); *Helmreich*, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? *ecolex* 2005, 379; OGH 26.7.2005, 11 Os 57/05z; OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2).

zu den Verkehrsdaten, letztere zu den Stammdaten.⁴¹⁵ Vertreten wurde auch, dass der Versuch einer Zuordnung der IP-Adressen zu Stamm- oder Verkehrsdaten im Wege der Interpretation nicht notwendig sei, weil der Gesetzgeber die Einordnung in Form der Unterkategorie „Zugangsdaten“⁴¹⁶ selbst vorgenommen habe.⁴¹⁷

Die Bedeutung der Unterscheidung liegt jedenfalls darin, dass Verkehrsdaten dem Kommunikationsgeheimnis gem § 93 TKG unterliegen und gem § 99 TKG außer in den gesetzlich geregelten Fällen nicht gespeichert werden dürfen, sondern vom Betreiber (Access-Provider) nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren sind. Diese Bestimmung ist Art 6 Abs 1 Telekom-Datenschutz-RL nachgebildet. Soweit dies für Zwecke der Verrechnung erforderlich ist, hat der Betreiber gem Abs 2 *leg cit* Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann.

Stammdaten unterliegen dagegen nicht dem Kommunikationsgeheimnis (e contrario aus § 93 TKG). Für sie besteht auch keine Löschungspflicht des Betreibers, weil dieser nur dann seine vertraglichen Pflichten erfüllen kann, wenn ihm die Stammdaten seiner Kunden bekannt sind und er sie ohne weiteres speichern und verarbeiten darf.

In der Entscheidung „LSG/Tele2“, die nach dem Vorabentscheidungsverfahren vor dem EuGH getroffen wurde, qualifizierte der OGH dynamische IP-Adressen in Einklang mit der herrschenden Ansicht als Verkehrsdaten und ließ mangels Relevanz für das Verfahren offen, ob statische IP-Adressen nun Stamm- oder Verkehrsdaten sind.⁴¹⁸ Weiters erklärte der OGH, dass das Problem weniger darin liege, ob Stammdaten zu Auskunftszwecken gespeichert werden können (das ist gem § 97 Abs 2 TKG zur Erfüllung gesetzlicher Pflichten gestattet), sondern darin, dass die begehrte Stammdatenauskunft nur möglich ist, wenn der Access-Provider dafür (intern) Verkehrsdaten verarbeitet.⁴¹⁹

⁴¹⁵ In diesem Sinn zB ErlRV 128 BlgNR XXII. GP 17 f; DSK 29.9.2006, K213.000/0005-DSK/2006; *Hasberger*, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23; *Helmreich*, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? *ecolex* 2005, 379; im Ergebnis auch *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116); differenzierend *Stomper*, Zur Auskunftspflicht von Internet-Providern, MR 2005, 118 (119); aA *Wiebe*, Auskunftsverpflichtung der Access Provider, MR 2005 Beilage H 4, 14.

⁴¹⁶ „Zugangsdaten“ sind gem § 92 Abs 3 Z 4a TKG jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

⁴¹⁷ *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116); vgl auch *Wiebe*, Auskunftsverpflichtung der Access Provider, MR 2005 Beilage H 4, FN 111.

⁴¹⁸ OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2).

⁴¹⁹ Dazu noch ausführlich unten bei Pkt 4. (Zulässigkeit der Verarbeitung).

D.I.2.c.1.3. **Speicherungspflicht von Access-Providern**

Unklar war lange, ob Access-Provider die Verbindungsdaten ihrer Kunden speichern müssen, damit sie ihrer Auskunftspflicht nachkommen können.

Weder im UrhG noch im TKG findet sich eine explizite gesetzliche Pflicht für Access-Provider, Daten ihrer Kunden für Auskunftsbegehren Dritter auf Vorrat zu speichern. Da Verkehrsdaten außer in den gesetzlich geregelten Fällen nicht gespeichert werden dürfen, müssen auch dynamische IP-Adressen nach Beendigung der Internetverbindung unverzüglich gelöscht werden.⁴²⁰

Die Gegenansicht⁴²¹, wonach aus § 87b Abs 3 UrhG zwar keine explizite, aber doch eine implizite Speicherungspflicht abzuleiten sei, wurde vor allem damit begründet, dass der Auskunftsanspruch ins Leere gehen würde, wenn Access-Provider die Verbindungsdaten nicht speichern müssten. Eine solche Absicht könne man dem Gesetzgeber aber nicht unterstellen.

Der OGH bezog anlässlich seiner Entscheidung „LSG/Tele2“ in dieser Diskussion klar Position. Zum einen lasse sich den Materialien der UrhG-Novellen 2003 und 2006 nicht entnehmen, dass dem Gesetzgeber die unionsrechtliche Problematik der Verarbeitung von Verkehrsdaten überhaupt bewusst war. Zum anderen könne die Annahme einer bloß impliziten Regelung dem unionsrechtlichen Erfordernis, wie sie in Art 15 Abs 1 Telekom-Datenschutz-RL formuliert ist, nämlich einer Anordnung durch „Rechtsvorschrift“ nicht genügen. Durch diesen formellen Gesetzesvorbehalt solle offenkundig Rechtssicherheit geschaffen werden, die bei Annahme einer bloß impliziten Anordnung, wie auch das vorliegende Verfahren beweist, nicht gegeben sei.⁴²² Dies schließe auch eine Analogie zur Füllung einer planwidrigen Lücke im TKG aus.

Dem Argument, dass dann der Auskunftsanspruch aus § 87b Abs 3 UrhG leer laufe, gab der OGH zwar Recht. Allerdings würde im umgekehrten Fall das allgemeine Speicherverbot in § 99 TKG ein ähnliches Schicksal erleiden, weil bei konsequenter Auslegung des § 87b Abs 3 UrhG im Sinne der vorher angeführten Ansicht sämtliche Verbindungsdaten dreißig Jahre lang gespeichert werden müssten – solange ist nämlich die Verjährungsdauer für Ersatzansprüche, die aus gewerblich begangenen Urheberrechtsverletzungen resultieren (§ 91 Abs 2a UrhG iVm § 1489 ABGB).

Diesen Normkonflikt löste der OGH mit einem Rückgriff auf höherrangiges Unionsrecht. Er führte unter Hinweis auf die Rechtsprechung des EuGH in der Sache „Promusicae“ aus, dass

⁴²⁰ Für viele: *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 671 mwN; DSK 29.9.2006, K213.000/0005-DSK/2006.

⁴²¹ *Schanda*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 215; *Schachter* in Kucsko, urheber.recht § 87b Pkt 3.4..

⁴²² AA *Bücheler*, Glosse zu 4 Ob 41/09x (LSG/Tele2), ÖBl 2010/18 (91).

mangels einer Pflicht der Mitgliedsstaaten, einen zivilrechtlichen Auskunftsanspruch vorzusehen, die ausdrückliche Lösungsverpflichtung in Art 6 Abs 1 Telekom-Datenschutz-RL Vorrang habe. Die Möglichkeit einer Einschränkung dieser Pflicht durch eine „Rechtsvorschrift“ iS von Art 15 Abs 1 Telekom-Datenschutz-RL habe der österreichische Gesetzgeber bisher nicht wahrgenommen.

D.I.2.c.1.4. Zulässigkeit der Verarbeitung bei vorhandenen Daten

Bleibt die Frage, ob Access-Provider dennoch eine Auskunft über die Identität ihrer Nutzer geben dürfen/müssen, wenn sie die benötigten Daten noch rechtskonform gespeichert haben, etwa für Verrechnungszwecke.

Der OGH erläuterte in der Entscheidung „LSG/Tele2“, dass bei Begehren auf Basis von § 87b Abs 3 UrhG nicht nur isoliert auf die Auskunft über Stammdaten, sondern vielmehr auf die dahinterliegende Verarbeitung von Verkehrsdaten abzustellen sei.

Aus dem Regelungszusammenhang von Art 6 Abs 1 Telekom-Datenschutz-RL sowie dessen Umsetzung in § 99 TKG schließt der OGH nämlich, dass eine Verarbeitung von - wenngleich unter Umständen nach den Abs 2, 3 und 5 rechtmäßig gespeicherten - Daten für andere Zwecke nicht zulässig ist. Denn die Löschungspflicht habe offenkundig den Zweck, eine unzulässige Nutzung der Daten zu verhindern. Dieser Zweck würde durch die Zulässigkeit der anderweitigen Nutzung rechtmäßig gespeicherter Daten unterlaufen, ohne dass dies durch die Wertung der jeweiligen Ausnahmestimmungen gedeckt wäre. Zudem verstieße eine solche Auffassung gegen den datenschutzrechtlichen Grundsatz der strikten Zweckbindung, wonach Daten, die für einen bestimmten Zweck gespeichert wurden, auch nur für diesen Zweck verarbeitet werden dürfen (Art 6 Abs 1 lit c Datenschutz-RL).

Der einfache Weg, allein auf die Bekanntgabe von Stammdaten abzustellen und die Vorgänge bei deren Ermittlung völlig auszublenden, sei damit unionsrechtlich nicht gangbar. Vielmehr sei anzunehmen, dass Art 6 Telekom-Datenschutz-RL und dessen Umsetzung in § 99 TKG der Verarbeitung von Verkehrsdaten für die Erteilung der begehrten Auskunft entgegensteht.

Interessant ist diese – in sich schlüssige – Argumentation des 4. Senats auch deswegen, weil der OGH in Strafsachen noch eine konträre Position bezogen hatte und eine formlose Bekanntgabe zuließ.⁴²³ Die Vorgänge „hinter“ der Herausgabe der begehrten Stammdaten, nämlich die Verarbeitung von Verkehrsdaten, klammerte der erkennende 11. Senat damit aus.⁴²⁴

⁴²³ OGH 26.7.2005, 11 Os 57/05z; siehe dazu noch ausführlich unten S 152 f.

⁴²⁴ Dazu krit *Hasberger*, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23 (24).

Zumindest zivilrechtlich ist seit der Entscheidung „LSG/Tele2“ aber klar, dass die isolierte Betrachtung, das Auskunftsbegehren stelle ja lediglich auf Stammdaten ab⁴²⁵, zu kurz greift.

Nach derzeitiger Rechtslage könne ein Auskunftsbegehren iSd § 87b Abs 3 UrhG nur aufgrund einer rechtswidrigen Verarbeitung von Verkehrsdaten erteilt werden, so der OGH in „LSG/Tele2“. Da Access-Provider nicht zu einem rechtswidrigen Verhalten verpflichtet werden können, wies der OGH das Klagebegehren im Anlassfall ab.

Aus den Ausführungen des OGH folgt ganz allgemein, dass die Durchsetzung eines Anspruchs nach § 87b Abs 3 UrhG derzeit daran scheitert, dass die begehrte Auskunft nur aufgrund einer rechtswidrigen Verarbeitung von Verkehrsdaten erteilt werden könnte.⁴²⁶

Der OGH hielt weiters fest, dass dies auch dann gilt, wenn ein Access-Provider diese Verarbeitung bereits durchgeführt haben sollte. Denn die Zulässigkeit der Weitergabe von Stammdaten könne nicht davon abhängen, ob das dafür erforderliche rechtswidrige Verarbeiten von Verkehrsdaten im Zeitpunkt der Anspruchserhebung oder der darüber ergehenden Entscheidung schon erfolgt war oder nicht.

D.I.2.c.1.5. Gerichtliche Vorabkontrolle oder direkte Weitergabe

Falls der Gesetzgeber eine Speicherpflicht schaffen und dadurch die bisher beschriebenen Hindernisse für eine Auskunftspflicht beseitigen würde, stellt sich die Frage, ob eine Auskunft über Nutzerdaten durch einen Access-Providers eine vorherige richterliche Genehmigung erfordert oder formlos und ohne Zwischenschaltung eines Gerichtes direkt an den Rechteinhaber ergehen kann.⁴²⁷

Nach Ansicht des OGH könne aus dem Beschluss des EuGH in „LSG/Tele2“ eindeutig abgeleitet werden, dass das Unionsrecht § 87b Abs 3 UrhG nicht entgegensteht.⁴²⁸ Falls der Mangel eines Richtervorbehalts dem Unionsrecht widerspräche, hätte der EuGH dies nach Ansicht des OGH zweifellos fest gehalten. Diese Schlussfolgerungen sind jedoch nicht zwingend. Hätte der EuGH ausgesprochen, dass das Unionsrecht einer direkten, also ohne gerichtliche Prüfung erfolgenden, Weitergabe personenbezogener Daten nicht entgegenstehe, käme keine andere Deutung als jene des OGH mehr in Frage. Der EuGH musste sich jedoch aufgrund der Formulierung der Vorlagefrage nicht festlegen, auch wenn die Begründung der Vorlageent-

⁴²⁵ So *Schanda*, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 18; *ders*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 214.

⁴²⁶ RIS-Justiz RS0124952.

⁴²⁷ Dieser Teil (Unterpunkt 5.) und der folgende Teil (Unterpunkt 6.) der vorliegenden Arbeit wurden in adaptierter Form in *Raschhofer/Steinhofer*, § 87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig?, *ecolex* 2010, 716, vorab veröffentlicht.

⁴²⁸ Ebenso *Guggenbichler* in Ciresa, Österreichisches Urheberrecht, § 87b UrhG Rz 15.

scheidung ein diesbezügliches Interesse des OGH erkennen lässt.⁴²⁹ Tatsächlich wiederholte der EuGH in „LSG/Tele2“ nur die in der Rs „Promusicae“ formulierten Prinzipien und betonte, dass zivilrechtliche Auskunftsansprüche zwar zulässig seien, jedoch bei der deren Auslegung die tangierten Grundrechte (insb Eigentum, Privatsphäre) in Einklang zu bringen und der Verhältnismäßigkeitsgrundsatz zu wahren sei. Der Beschluss in der Sache „LSG/Tele2“ brachte jedoch nichts Neues zur Frage des Richtervorbehalts. Daher können auch jene Stimmen, die zuvor aus dem Verhältnismäßigkeitsgrundsatz die Notwendigkeit einer richterlichen Prüfung ableiteten, nicht als obsolet betrachtet werden. Deshalb wird auch nach dem „LSG/Tele2“ noch immer über die unionsrechtliche Notwendigkeit eines Richtervorbehalts nachgedacht.⁴³⁰ Dass der EuGH das Fehlen einer richterlichen Kontrolle in § 87b Abs 3 UrhG nicht ausdrücklich als unionsrechtswidrig qualifizierte, kann vor dem Hintergrund seiner Kompetenzen im Verfahren gem Art 234 EGV (nunmehr Art 267 AEUV) nicht als klare Bestätigung der Unionsrechtskonformität verstanden werden. Im Vorabentscheidungsverfahren hat der EuGH nicht über die Vereinbarkeit nationalen Rechts mit EG-Recht abzusprechen, sondern lediglich eine abstrakte Auslegung der unionsrechtlichen Normen vorzunehmen.⁴³¹ Die Beurteilung, ob das nationale Recht mit dem vom EuGH ausgelegten Unionsrecht vereinbar ist, obliegt dagegen dem nationalen Richter.⁴³²

Zykan ist gleichfalls der Ansicht, dass die isolierte Aussage des EuGH in ihrem Kontext in den Entscheidungen „Promusicae“ und „LSG/Tele2“ zu sehen ist: Sie beziehe sich (nur) darauf, dass nach Ansicht des EuGH aus der Telekom-Datenschutz-RL kein prinzipielles Verbot einer Weitergabe von Daten im Rahmen eines zivilrechtlichen Auskunftsanspruches ableitbar ist. Ob eine konkrete innerstaatliche Umsetzung im Lichte des Unionsrechts zulässig ist, sei aber unter Abwägung der betroffenen grundrechtlich verbürgten Interessen (Schutz des Eigentums und effektiver Rechtsschutz einerseits und Achtung des Privatlebens auf der anderen Seite) unter Wahrung des Grundsatzes der Verhältnismäßigkeit zu prüfen. Daher hätte der OGH klären müssen, ob § 87b Abs 3 UrhG in seiner konkreten Ausgestaltung den geforderten Ausgleich gewährleistet und widrigenfalls die Bestimmung im Sinne des Anwendungsvorrangs des Unionsrechts allenfalls unangewendet lassen.⁴³³

⁴²⁹ *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 668.

⁴³⁰ *Büchle*, ÖBl 2010/18 (91); *ders*, Glosse zu EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2), ÖBl-LS 2009/233 (171); *Zerdick*, Europäisches Datenschutzrecht – neuere Rechtssprechung des EuGH, RDV 2009, 56 (59); vgl auch die Aussendung des BKA zum Beschluss des EuGH: BKA 2.8.2009, BKA-VA.C-557/07/0002-V/7/2009, abrufbar unter <austria.gv.at/DocView.axd?CobId=36104> (Stand April 2010).

⁴³¹ EuGH 15.7.1964 Rs C-6/64 (Costa/E.N.E.L.); dies übersehend *Daum*, Glosse zu EuGH 19. 2. 2009 Rs C-557/07 (LSG/Tele 2), MR 2009, 40 (43).

⁴³² *Fischer/Köck/Karollus*, Europarecht⁴ Rz 1433.

⁴³³ *Zykan*, Zum Verhältnis des Auskunftsanspruches gem § 87b Abs 3 UrhG zum Datenschutz, jusIT 2009 H 6, 208 f.

Die Auffassung, wonach ein Richtervorbehalt aus dem Unionsrecht abgeleitet werden kann, ist daher nach wie vor zulässig.

Unabhängig davon stellt sich die Frage, ob ein Richtervorbehalt aus nationalem österreichischem Verfassungsrecht ableitbar ist. Relevant ist hier erstens Art 8 EMRK (Recht auf Achtung des Privat- und Familienlebens). Eingriffe in dieses Grundrecht, das in Österreich in Verfassungsrang steht, müssen gesetzlich vorgesehen sein und der Eingriff muss in einer demokratischen Gesellschaft (unter anderem) zum Schutz der Rechte und Freiheiten anderer notwendig sein.

Primär von Bedeutung für die zu klärende Frage ist aber das Fernmeldegeheimnis in Art 10a StGG, das unter Richtervorbehalt steht. Die Offenlegung von bestimmten Daten, primär Inhaltsdaten von Kommunikationsvorgängen, darf demnach ohne richterlichen Befehl nicht erfolgen. Betrachtet man die Auskunft über Stammdaten eines Nutzers, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, als Eingriff in Art 10a StGG, wäre § 87b Abs 3 UrhG mangels Richtervorbehalts jedenfalls verfassungswidrig. Zwar ermöglicht diese Bestimmung nur die Bekanntgabe von Stammdaten, die keinesfalls dem Schutzbereich des Art 10a StGG zugehören. Jedoch müssen zur Erfüllung des Begehrens stets Verkehrsdaten verarbeitet werden.

Edthaler/Schmidt sehen – unter Berufung auf die herrschende strafrechtliche Judikatur und Literatur – auch Verkehrsdaten vom Schutzbereich des Fernmeldegeheimnisses umfasst. Die Autoren sind allerdings der Auffassung, dass nur ein „Vorgang mit Außenwirkung“ das Kommunikationsgeheimnis verletzen kann. Die bei dynamischen IP-Adressen beim auskunftspflichtigen Access-Provider intern erforderliche Ermittlung, Auswertung, Zuordnung, Abgleichung, Verwertung oder sonstige Verarbeitung von Verkehrsdaten sei davon nicht umfasst.⁴³⁴

Mangels Relevanz für den behandelten Anlassfall lies der OGH die Frage des Richtervorbehalts in seiner Entscheidung „LSG/Tele2“ offen – in einem obiter dictum beschäftigt sich das Höchstgericht dann aber doch mit den verfassungsrechtlichen Implikationen. Anknüpfend an die Argumentation von *Edthaler/Schmidt* hielt das Höchstgericht fest, dass gegen die verfassungsrechtliche Notwendigkeit eines Richtervorbehalts spreche, dass die Verarbeitung der sensiblen Verkehrsdaten intern erfolgt und nach außen nur Stammdaten bekanntgegeben werden. Der Verletzte will nicht Verkehrsdaten erfahren (welche Internetseiten hat ein bestimmter Nutzer wann besucht), sondern (umgekehrt) zu einer bereits bekannten Nutzung eines bestimmten Internetangebots Name und Anschrift des Nutzers erfahren.⁴³⁵

⁴³⁴ *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 221 f.

⁴³⁵ Vgl OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2) mwN zu Lit und deutscher Verfassungsjudikatur.

Folgt man der herrschenden Staatsrechtslehre, kommt man bereits einen Schritt früher zu dem Ergebnis, dass § 87b Abs 3 UrhG keinen Eingriff in das Fernmeldegeheimnis darstellt.⁴³⁶ Art 10a StGG schützt nach dieser Ansicht nämlich nur Kommunikationsinhalte, nicht aber Verkehrsdaten oder Stammdaten.⁴³⁷

Ordnet man allerdings mit einem Teil der Rsp⁴³⁸ und Lit⁴³⁹ Verkehrsdaten dem Schutzbereich des Art 10a StGG zu, dann wäre auch die Auskunft über Stammdaten unter Richtervorbehalt zu stellen, wenn dabei Verkehrsdaten verarbeitet werden müssen. So verstanden wäre der Zweck des Fernmeldegeheimnisses neben dem Schutz des Inhalts von Nachrichten auch der Schutz der Vertraulichkeit der Information, wem welche Verkehrsdaten zugeordnet sind. Diese Vertraulichkeit wird nicht nur durch die Erhebung der Verkehrsdaten einer bekannten Person beeinträchtigt, sondern auch durch die Ermittlung einer unbekannt Person anhand der bekannten, ihr zuordenbaren Verkehrsdaten.⁴⁴⁰

Die vor allem auf die Vorbildwirkung des Art 10 StGG – dieser schützt nur den Inhalt verschlossener Schriftstücke – gestützten historischen Argumente gegen eine Einbeziehung von Verkehrsdaten vermögen mE letztlich gegenüber den zahlreichen teleologischen Argumenten⁴⁴¹ für einen weiten Schutzbereich des Fernmeldegeheimnisses nicht zu überzeugen. Bei einem nahezu unentschiedenen Meinungsstand in der Lit wird jedoch nur der VfGH endgültige Klarheit verschaffen können. Sollte daher der OGH neuerlich mit der Auslegung von § 87b Abs 3 UrhG befasst werden und die oben dargelegten unionsrechtlichen Bedenken weiterhin nicht teilen, so müsste er wohl den VfGH mit der Klärung dieser Frage betrauen. Auch

⁴³⁶ *Wiederin* in Korinek/Holoubek, B-VG III, Art 10a StGG Rz 12 mwN; ebenso zB *Thiele* in Triffterer/Rosbaud/Hinterhofer, Sbg Kommentar zum StGB § 119 Rz 10.

⁴³⁷ Vgl *Wessely*, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, ÖJZ 1999, 491; *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 667; *Otto/Seitlinger*, Die "Spitzelrichtlinie", MR 2006, 227; OGH 26.7.2005, 11 Os 57/05z.

⁴³⁸ VwGH 27.5.2009, 2007/05/0280; OGH 6.12.1995, 13 Os 161/95.

⁴³⁹ *Zykan*, Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz, jusIT 2009, 206 (209); *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 (223 f); *Chadoian*, Stille Nacht, heimliche Macht, juridikum 2008, 130 (131); *Helmreich*, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen?, *ecolex* 2005, 379; *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 116; *Reindl-Krauskopf/Tipold/Zerbes* in Fuchs/Ratz, WK-StPO § 134 Rz 28 mwN; vgl auch die ErlRV 25 BlgNR XXI. GP 190.

⁴⁴⁰ Vgl auch *Hasberger*, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23 (24); *Kindt*, Grundrechtsschutz für Raubkopierer und Musikpiraten? MMR 2009, 147 (149) mwN; *Hoeren*, Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099 (3100).

⁴⁴¹ *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 13, hält einer Beschränkung von Art 10a StGG auf Inhaltsdaten zB entgegen, dass auch die zur Vermittlung verwendeten Daten zunehmend "informationell angereichert" würden. Da sich der Schutz des Fernmeldegeheimnisses auch auf die Kommunikationsbeziehungen richte, sei auch eine Einbeziehung der Verkehrsdaten geboten; ähnlich *Einzingler/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116).

deswegen wäre eine jedenfalls grundrechtskonforme Neugestaltung von § 87b Abs 3 UrhG, die nach dem Vorbild von § 101 dUrhG einen Richtervorbehalt vorsieht, der Rechtssicherheit zuträglich.⁴⁴²

Im Zusammenhang mit einer allfälligen gesetzliche Neuregelung wurden in der Lit nämlich zu Recht vor allem Argumente für die Implementierung eines Richtervorbehalts angeboten. Aus Gründen der Verhältnismäßigkeit und zur Wahrung der berührten Grundrechte sollte ein Zivilgericht vorab über die Rechtmäßigkeit des Auskunftsanspruchs entscheiden. Nur so kann das angemessene Gleichgewicht zwischen Datenschutz und effektiver Durchsetzung des Eigentumsrechts gewährleistet werden, weil Gerichte an Grundrechte, insbesondere an die Wahrung von Verfahrensgarantien und die Berücksichtigung von Umständen, die den einer Verletzung von Urheberrechten beschuldigten Nutzer entlasten, direkt gebunden sind.⁴⁴³

Der Richtervorbehalt wäre auch eine Möglichkeit, um zu verhindern, dass Provider mit Risiken bei der eigenen Beurteilung von mutmaßlichen Rechtsverletzungen und der Herausgabe von Daten belastet werden, wodurch Nutzerrechte auch besser vor etwaigen Missbrauchsfällen geschützt werden.⁴⁴⁴ Ein Gericht ist schließlich auch besser in der Lage, die zum Nachweis der Urheberrechtsverletzung vorgelegten Beweise zu würdigen. Dies ist vor allem vor dem Hintergrund der missbrauchsanfälligen Überwachung von Filesharing-Netzwerken besonders wichtig.⁴⁴⁵ Der betroffene Provider müsste zudem komplexe Rechtsfragen nicht selbst lösen, sondern hätte die Sicherheit einer gerichtlichen Entscheidung.⁴⁴⁶

Die Gegenseite hält dem, soweit ersichtlich, lediglich entgegen, dass eine Auskunft ohne Zwischenschaltung „aus Effizienzgründen“ zu bevorzugen wäre.⁴⁴⁷

*Daum*⁴⁴⁸ meinte differenzierend, es könne sinnvoll sein, die Auskunftserteilung im Rahmen eines geregelten Verfahrens über eine öffentliche Stelle vornehmen zu lassen. Anderenfalls würde etwa die Beurteilung, ob eine Rechtsverletzung durch die Nutzung einer bestimmten IP-Adresse ausreichend bescheinigt ist, alleine dem Vermittler überlassen. Allerdings plädiert er für ein möglichst vereinfachtes Verfahren, etwa im Sinne einer "Schlichtungsstelle". Dies hätte laut *Daum* auch den Vorteil, dass mit den Auskunftsanträgen nicht zwangsläufig bereits gerichtliche Verfahren gegen die bis dahin unbekanntem Nutzer in Gang gesetzt wer-

⁴⁴² Dazu *Raschhofer/Steinhofer*, Zwischen Urheber und Kunde: Provider in der Zwickmühle, Rechtspanorama, Die Presse 5.10.2009.

⁴⁴³ *Barbist*, Auskunftspflicht: Streit Provider vs Musikindustrie Reloaded Das EuGH-Urteil in Sachen Promusicae, MR 2007, 417 und FN 14.

⁴⁴⁴ *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25 (29).

⁴⁴⁵ Siehe den diesbezüglichen Exkurs oben S 118 f.

⁴⁴⁶ *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 669.

⁴⁴⁷ *Briem*, Urheberrecht: Politik unter Zugzwang, Rechtspanorama, Die Presse 28.9.2009.

⁴⁴⁸ *Daum*, Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug!, MR 2009, 250.

den müssten. Zur Entlastung der Justiz solle für jene Auskunftsbegehren, die von einer Verwertungsgesellschaft gestellt werden, allenfalls eine bestimmte Behörde mit der Durchführung des Verfahrens betraut werden. In Betracht käme dabei die Aufsichtsbehörde der österreichischen Verwertungsgesellschaften, die KommAustria, die von der Rundfunk & Telekom Regulierungs-GmbH (RTR) als Geschäftsstelle unterstützt wird.

Die von *Daum* geforderte Einrichtung eines möglichst vereinfachten Verfahrens trägt mE generell die Gefahr in sich, dass gerade im hier zu beurteilenden, äußerst grundrechtssensitiven Bereich nur rudimentär geprüft wird. Es kommt aber letztlich darauf an, wie ein derartiges Verfahren ausgestaltet würde – ein passendes Umfeld könnte etwa das bestehende und erprobte Provisorialverfahren nach § 87c UrhG sein.⁴⁴⁹ Dort wäre in einem neu zu schaffenden Absatz ein eigenes Regelwerk für Auskunftsansprüche zu schaffen, vergleichbar dem Abs 3 *leg cit*, der die Sicherung von Unterlassungs- und Beseitigungsansprüchen behandelt.

Jedenfalls zu weit geht mE aber das Ansinnen, die Beurteilung der Auskunftspflicht an eine Behörde auszulagern. Dagegen sprechen primär verfassungsrechtliche Argumente: Im Bereich der KommAustria besteht ein Weisungsrecht des Bundeskanzlers, sodass das Erfordernis eines „Tribunals“ für die Entscheidung über „civil rights“ iS von Art 6 EMRK nicht gegeben wäre. Zudem wäre es bei der KommAustria so, dass die Aufsichtsbehörde der Verwertungsgesellschaften auch direkt über rechtliche Ansprüche der von ihr zu beaufsichtigenden Gesellschaften zu befinden hätte. Das wäre vergleichbar einem Aufsichtsrat, der auch über Ansprüche des von ihm zu kontrollierenden Organs gegenüber Dritten zu entscheiden hat, und daher mE äußerst bedenklich.

Im Ergebnis sollte es daher den ordentlichen Gerichten überlassen bleiben, über die Zulässigkeit von Auskunftsansprüchen, die die Verarbeitung von personenbezogenen Verkehrsdaten voraussetzen, zu entscheiden.

D.I.2.c.1.6. Verhältnismäßigkeit von § 87b Abs 3 UrhG

Aufgrund der derzeitigen Ausgestaltung von § 87b Abs 3 UrhG stellt sich weiters die Frage, ob diese Regelung insgesamt unionsrechtlich zulässig ist, oder ob sie gegen das Prinzip der Verhältnismäßigkeit verstößt und daher nicht angewendet werden dürfte.

Im Beschluss zu „LSG/Tele2“ bekräftigte der EuGH lediglich, dass die unionsrechtlich geschützten Grundrechte und die allgemeinen Grundsätze des Unionsrechts, wie eben der Grundsatz der Verhältnismäßigkeit, bei der Umsetzung der oben dargestellten Richtlinien zu

⁴⁴⁹ Vgl dazu auch *Schachter*, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz - Anlassfälle Promusicae und MediaSentry, jusIT 2008 H 2, 21.

beachten sind.⁴⁵⁰ Sein Schweigen zu § 87b Abs 3 UrhG kann aber nicht als Bestätigung der Unionsrechtskonformität verstanden werden.⁴⁵¹

Der OGH ließ die Frage nach der Verhältnismäßigkeit von § 87b Abs 3 UrhG offen, weil schon aufgrund der oben genannten datenschutzrechtlichen Bestimmungen die Auskunftspflicht über Inhaber von dynamischen IP-Adressen bei Filesharing-Sachverhalten ins Leere geht.⁴⁵² Kursorisch behandelte der OGH aber dennoch, inwiefern sich eine gesetzliche Regelung am Unionsrecht messen lassen muss.

Zu beachten ist hierbei vor allem sein Argument, dass bei einer Speicherpflicht für Verkehrsdaten, die zur Verfolgung von urheberrechtlichen Ansprüchen dienen sollen, ein Wertungseinklang mit der Vorratsdatenspeicherungs-RL hergestellt werden muss. Nach dieser sind ua von den Access-Providern ua Verkehrsdaten für mindestens sechs Monate auf Vorrat zu speichern, um den Behörden das Verfolgen von „schwere Straftaten“ (Art 1 Abs 1 Vorratsdatenspeicherungs-RL) zu ermöglichen. Diese Speicherpflicht schließt, wie auch der OGH richtig feststellt, aber nicht zwingend andere Speicherpflichten, die nicht auf die Verfolgung von „schweren Straftaten“ abzielen, aus. Andernfalls wäre die Ausnahme in Art 15 Abs 1a Telekom-Datenschutz-RL, die die Vorratsdatenspeicherungs-RL im Verhältnis zum Datenschutz auf Unionsebene legitimiert, nicht erklärbar. Schließlich lässt sie die anderen Bestimmungen in Art 15 Abs 1 Telekom-Datenschutz-RL unberührt, sodass weiterhin auch Ausnahmen vom telekommunikationsrechtlichen Datenschutz denkbar sind, die nichts mit der Vorratsdatenspeicherungs-RL zu tun haben. Da nach der EuGH-Judikatur⁴⁵³ die Pflicht zur Wahrung der Vertraulichkeit personenbezogener Daten auch dann beschränkt werden kann, sofern eine solche Beschränkung für den Schutz der Rechte und Freiheiten anderer Personen notwendig ist, spricht unionsrechtlich somit nichts dafür, dass eine Speicherpflicht für Verkehrsdaten auf „schwere Straftaten“ beschränkt bleiben müsste.

Schwerer wiegt der Umstand, dass die Vorratsdatenspeicherungs-RL die Speicherdauer im Zusammenhang mit „schweren Straftaten“ zwischen sechs Monaten und zwei Jahren eingrenzt. Urheberrechtsdelikte sind nach § 91 UrhG lediglich mit einer Freiheitsstrafe von höchstens sechs Monaten bedroht, weswegen sie aus Wertungsgründen kein tauglicher Grund für eine ebenso lange Speicherung von Verkehrsdaten wie bei „schweren Straftaten“ sein können - um die Verhältnismäßigkeit zu wahren, müsste eine Speicherpflicht, die die Verfolgung von urheberrechtlichen Ansprüchen unterstützen soll, mE vielmehr entsprechend geringer ausfallen. Eine andere Möglichkeit wäre es, die Auskunftspflicht auf gewerbsmäßige

⁴⁵⁰ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 70.

⁴⁵¹ Vgl oben S 138 f; *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 669.

⁴⁵² OGH 14.7.2009, 4 Ob 41/09x (LSG/Tele2).

⁴⁵³ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 53 f.

Urheberrechtsverletzungen zu beschränken – letztere sind gem §91 Abs 2a UrhG mit einer Freiheitsstrafe von bis zu zwei Jahren zu bestrafen.

Hinsichtlich der Ausgestaltung derartiger Auskunftspflichten ist zunächst festzuhalten, dass § 87b Abs 3 UrhG in seiner jetzigen Form ein „austriacum“ darstellt und über den harmonisierten Bereich des Unionsrechts hinausgeht.⁴⁵⁴ Insb ergibt sich weder aus Art 8 Abs 1 und 3 Info-RL noch aus Art 8 Enforcement-RL, dass die Mitgliedstaaten zwingend die Pflicht zur Weitergabe personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorsehen müssten.⁴⁵⁵ Umso weniger kann eine direkte Weitergabe wie in § 87b Abs 3 UrhG, also ohne obligatorisches gerichtliches Verfahren, an private Dritte durch das Unionsrecht geboten sein.⁴⁵⁶ Dabei muss zudem bedacht werden, dass der EuGH die notwendige Beachtung des Verhältnismäßigkeitsgrundsatzes kaum betont hätte, wenn er jede Regelung, die eine Auskunftsverpflichtung auch bei geringsten Urheberrechtsverletzungen vorsieht, für verhältnismäßig hielte.⁴⁵⁷ Eine noch undifferenzierte Ausgestaltung eines Auskunftsanspruchs als § 87b Abs 3 UrhG in seiner derzeitigen Form ist aber nicht denkbar, weil weder nach der Schwere der Urheberrechtsverletzung differenziert wird noch eine Vorabkontrolle durch ein Gericht vorgesehen ist.

Das zur Verhältnismäßigkeit von § 87b Abs 3 UrhG von *Sofokleous/Mosing*⁴⁵⁸ gebrachte Argument, dass technisch kein gelinderes Mittel möglich sei, die anonymen Internetuser auszuforschen, mag zwar stimmen. Die Autoren übersehen freilich, dass es beim Kriterium der Notwendigkeit nicht darum geht, die technische Möglichkeit einer Maßnahme zu prüfen, sondern vielmehr darum, welches Vorgehen das am wenigsten invasive Mittel darstellt, um ein bestimmtes, im öffentlichen Interesse liegendes, Ziel zu erreichen. Hier muss man mE zum Ergebnis kommen, dass auch durch ein vorgeschaltetes gerichtliches Verfahren das Urheberrecht effektiv geschützt werden kann – der erhöhte Aufwand auf Seiten der Rechteinhaber ist vernachlässigbar, wenn man ihm auf der anderen Seite den deutlich erhöhten Rechtsschutzstandard für alle Beteiligten (insbes für die Access-Provider) gegenübergestellt.

⁴⁵⁴ Unter Hinweis auf die Entstehungsgeschichte der Bestimmung ebenso *Bücheler*, Glosse zu EuGH Rs C-557/07 (LSG/Tele2), ÖBl-LS 2009/233, 170 (171), der auch darauf hinweist, dass deswegen eine RL-konforme Auslegung nationalen Rechts nicht möglich und auch nicht zulässig sei.

⁴⁵⁵ EuGH 29.1.2008 Rs C-275/06 (Promusicae) Rz 58 f; *Spindler*, „Die Tür ist auf“ –Urteilsanmerkung zu EuGH „Promusicae/Telefónica“, GRUR 2008, 574 (576); das Unionsrecht steht einer solchen Weitergabe aber auch nicht prinzipiell entgegen: EuGH 19.2.2009 Rs C-557/07 (LSG/Tele2) Rz 29.

⁴⁵⁶ Insofern verfehlt *Daum*, Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug! MR 2009, 247 (249).

⁴⁵⁷ *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl 677.

⁴⁵⁸ *Sofokleous/Mosing*, Urheberrechtlicher Auskunftsanspruch gegen Access-Provider: ein "Pyrrhus-Anspruch"?! , ÖBl 2008/55, 268 (271).

Bei begründeten Ansprüchen wird gerade ein Gericht nicht entgegenstehen, dem Access-Provider die Auskunft aufzutragen. Schließlich wird zu Recht darauf hingewiesen, dass beim Filesharing bereits wenige Uploader genügen, um im Ergebnis ein massenhaftes Vervielfältigen und damit eine unzumutbare Beeinträchtigung der berechtigten Interessen der Rechteinhaber und der normalen Werkauswertung hervorzurufen.⁴⁵⁹ Der effektive Schutz des Urheberrechts ist somit auch und gerade mit einem sogenannten Richtervorbehalt zu erreichen, während auf diese Weise deutlich weniger stark vom Prinzip einer angemessenen Relation zwischen eingesetzten Mitteln und angestrebtem Zweck abgewichen wird.

Bei einer nochmaligen Befassung mit Auskunftsansprüchen aufgrund von Urheberrechtsverletzungen müsste der OGH daher mE die Vereinbarkeit von § 87b Abs 3 UrhG mit den Grundsätzen des Unionsrechts verneinen oder zumindest eine weitere Vorabentscheidung des EuGH in Gang setzen und seine Fragestellung präzisieren, um die zweifelhafte Verhältnismäßigkeit dieser Norm zu klären.

Das Unionsrecht bietet jedoch mit Art 8 Abs 1 Enforcement-RL eine passende Grundlage und ausreichend Orientierung für den nationalen Gesetzgeber, um unabhängig von einem weiteren Vorabentscheidungsverfahren eine verhältnismäßige legislatorische Abwägung zwischen den tangierten Grundrechten zu gestalten. Der „Ursprung und die Vertriebswege von Waren, die ein Recht des geistigen Eigentums verletzen“ schließt bei Musikdateien, die über ein Filesharing-Programm getauscht werden, nämlich auch die Identität des Inhabers des für den Tausch von Musikdateien verwendeten Internetanschlusses ein.⁴⁶⁰ Access-Provider erbringen durch die Bereitstellung des Internetzugangs gegen Entgelt auch eine Dienstleistung in gewerblichem Ausmaß. Ein Auskunftsanspruch mit der Zielrichtung von § 87b Abs 3 UrhG könnte daher auf diese Bestimmung gestützt werden.

Er müsste dann aber auch deren Wertungsmaßstab einhalten und deutlich größere Rücksicht auf die Abwägung der berührten Grundrechte nehmen als die bisherige, undifferenzierte Regelung. Bei näherer Betrachtung von Art 8 Abs 1 Enforcement-RL zeigt sich nämlich, dass der Unionsgesetzgeber die Auskunft über Herkunft und Vertriebswege von Waren und Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, äußerst behutsam regeln wollte („auf begründeten und die Verhältnismäßigkeit wahren Antrag des Klägers“) und zudem eine gerichtliche Prüfung dieser Maßnahmen vor Augen hatte („die zuständigen Gerichte [ordnen] im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des

⁴⁵⁹ *Daum*, EuGH zur Auskunftspflicht von Internetservice Providern, *ecolex* 2008, 200.

⁴⁶⁰ In diesem Sinn auch GA *Kokott*, SA 18.7.2007 Rs C-275/06 (*Promusicae*) Rz 110.

geistigen Eigentums [an]).⁴⁶¹ Dementsprechend vorsichtig hat der österreichische Gesetzgeber diesen Auskunftsanspruch in § 87b Abs 2 UrhG umgesetzt. Vorbilder für eine die Verhältnismäßigkeit wahrende Neuregelung von § 87b Abs 3 UrhG könnten daher die „Schwesterbestimmung“ in § 87b Abs 2 UrhG sowie der erwähnte § 101 Abs 9 dUrhG sein.

D.I.2.c.2. § 87b Abs 1 UrhG

§ 87b (1) Wer im Inland Werkstücke verbreitet, an denen das Verbreitungsrecht durch In-Verkehr-Bringen in einem Mitgliedstaat der Europäischen Gemeinschaft oder in einem Vertragsstaat des Europäischen Wirtschaftsraums erloschen ist (§ 16 Abs. 3), hat dem Berechtigten auf Verlangen richtig und vollständig Auskunft über Hersteller, Inhalt, Herkunftsland und Menge der verbreiteten Werkstücke zu geben. Anspruch auf Auskunft hat, wem das Recht, die Werkstücke im Inland zu verbreiten, im Zeitpunkt des Erlöschens zugestanden ist.

§ 87b Abs 1 UrhG bezieht sich auf Situationen, in denen gem § 16 Abs 3 UrhG ein Werkstück mit Einwilligung des Berechtigten durch Übertragung des Eigentums in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Europäischen Wirtschaftsraums in Verkehr gebracht worden ist. Eine Anwendbarkeit dieser Bestimmung auf Filesharing-Sachverhalte scheidet mE schon deswegen aus, weil eine digitale Datei (zB eine MP3-Datei, die ein urheberrechtlich geschütztes Musikstück beinhaltet) keine körperliche Festlegung eines Werkes und somit auch kein „Werkstück“ ist.⁴⁶²

D.I.2.c.3. § 87b Abs 2 UrhG; § 55a MSchG

§ 87b (2) Wer in einem auf dieses Gesetz gegründeten Ausschließungsrecht [§ 55a MSchG: „Wer in einer der ihm aus einer Marke zustehenden Befugnisse“] verletzt worden ist, kann Auskunft über den Ursprung und die Vertriebswege der rechtsverletzenden Waren und Dienstleistungen verlangen, sofern dies nicht unverhältnismäßig im Vergleich zur Schwere der Verletzung wäre und nicht gegen gesetzliche Verschwiegenheitspflichten verstoßen würde; zur Erteilung der Auskunft sind der Verletzer und die Personen verpflichtet, die gewerbsmäßig

- 1. rechtsverletzende Waren in ihrem Besitz gehabt,*
- 2. rechtsverletzende Dienstleistungen in Anspruch genommen oder*

⁴⁶¹ Auch vergleichbare Ansprüche und Rechtsbehelfe in E-Commerce-RL (vgl Art 14 Abs 3; Art 15 Abs 2) und Info-RL (vgl Art 8 Abs 3 iVm ErwG 59) sehen eine obligatorische Beteiligung staatlicher Einrichtungen vor; vgl auch *Bücheler*, Glosse zu EuGH Rs C-557/07 (LSG/Tele2), ÖBl-LS 2009/233, 170 (171); *ders*, Glosse zu 4 Ob 41/09x (LSG/Tele2), ÖBl 2010/18, 91..

⁴⁶² Auf die diesbezügliche Diskussion kann hier nicht näher eingegangen werden; vgl dazu *Anderl* in *Kucsko*, urheber.recht § 16 Pkt 2.2. und 4.5.

3. für Rechtsverletzungen genutzte Dienstleistungen erbracht haben.

(2a) Die Pflicht zur Auskunftserteilung nach Abs. 2 umfasst, soweit angebracht,

1. die Namen und Anschriften der Hersteller, Vertreiber, Lieferanten und der anderen Vorbesitzer der Waren oder Dienstleistungen sowie der gewerblichen Abnehmer und Verkaufsstellen, für die sie bestimmt waren,
2. die Mengen der hergestellten, ausgelieferten, erhaltenen oder bestellten Waren und die Preise, die für die Waren oder Dienstleistungen bezahlt wurden.

Die Auskunftsansprüche des § 87b Abs 2 UrhG und § 55a MSchG wurden jeweils in Umsetzung des Art 8 Abs 1 Enforcement-RL in das nationale Recht eingeführt.⁴⁶³ Die urheberrechtliche Bestimmung ist aufgrund ihres Wortlauts auch auf Filesharing-Sachverhalte anwendbar.⁴⁶⁴

Auch aus den Materialien ergibt sich, dass sich die Anwendungsbereiche der § 87b Abs 2 und 3 UrhG überschneiden können.⁴⁶⁵

Nach der bislang spärlichen einschlägigen Rsp⁴⁶⁶ ist der Auskunftsanspruch nach § 87 Abs 2 UrhG auf die Vertriebswege der im konkreten Fall rechtsverletzenden Ware beschränkt. Er umfasst insbesondere nicht die Bekanntgabe privater Endabnehmer. Die Pflicht zur Auskunftserteilung nach § 87b Abs 2a lit a UrhG erfasse nämlich nur Name und Anschrift der „gewerblichen“ Abnehmer. Das sei laut dem OGH folgerichtig, gehören doch nur Abnehmer, bei denen aufgrund ihrer gewerblichen Tätigkeit mit einer Weiterveräußerung zu rechnen ist, zu den „Vertriebswegen“ iSv § 87b Abs 2 UrhG. Anderes gelte für private Erwerber. Sie seien nicht Bestandteil der Vertriebswege, sondern stünden an deren Ende. Ein Auskunftsanspruch über die Identität von Endabnehmern bestehe daher nicht.⁴⁶⁷

Diese im Anlassfall schlüssige Argumentationslinie ist mE nicht auf Filesharing-Sachverhalte umlegbar. Wie bereits oben dargelegt, ist nämlich bei allen gängigen Tauschbörsen die Client-Software so programmiert, dass gleichzeitig down- und upgeloadet wird. Jeder einzelne Filesharer ist so gleichzeitig Abnehmer und Vertreiber von Daten. Diese Programmierung besteht nicht ohne Grund: Für das Funktionieren von Tauschbörsen ist es essentiell, dass die Teilnehmer nicht nur Daten von anderen Usern beziehen, sondern auch selbst ihre Inhalte und ihre Bandbreitenkapazität zur Verfügung stellen. Das unter Filesharern äußerst unbeliebte „Hit and Run“, bei dem ein Nutzer nur die von ihm begehrten Daten herunterlädt, oh-

⁴⁶³ BGBl I 81/2006 bzw BGBl I 96/2006; vgl auch § 151a PatG und § 21 HlSchG.

⁴⁶⁴ Vgl oben S 145 sowie GA Kokott, SA 18.7.2007 Rs C-275/06 (Promusicae) Rz 110.

⁴⁶⁵ ErlRV 1324 BlgNR XXII. GP 4.

⁴⁶⁶ RIS-Justiz RS0124719.

⁴⁶⁷ Zust Büchele, Glosse zu 4 Ob 34/09t, ÖBl 2010/17, 85.

ne selbst zum Bestehen des Systems beizutragen, wird durch das simultane Up- und Downloaden deutlich erschwert. Teilnehmer von Tauschbörsen sind daher (nicht nur) Endabnehmer, sondern selbst Glieder in der Vertriebskette.

Nach dem Wortlaut von § 87b Abs 2a Z 1 UrhG ist es für Vertreiber unerheblich, ob sie gewerblich agieren. Man könnte hier der Meinung sein, dass diese Eigenschaft bei Vertreibern notgedrungen vorausgesetzt werden muss und User von Tauschbörsen daher nur dann mittels dieser Bestimmung ausgeforscht werden dürfen, wenn sie zu gewerblichen Zwecken Daten austauschen. Dagegen spricht mE das systematische Argument, dass im UrhG Verletzungshandlungen idR unabhängig davon sanktioniert werden, ob sie unentgeltlich, entgeltlich oder gewerblich erfolgen. Selbiges gilt für das Markenrecht. Dort, wo eine Sanktion nur gewerbsmäßig agierende Akteure trifft, ordnet das Gesetz dies explizit an. Ein Hinweis darauf, dass dies beim Auskunftsanspruch in § 87 Abs 2 UrhG anders sein sollte, ergibt sich weder aus dem Wortlaut des Gesetzes noch aus den Materialien – insbesondere fehlt eine Definition des Begriffs „Vertreiber“. Die Klärung, was darunter zu verstehen ist, soll vielmehr der Rechtsprechung überlassen bleiben.⁴⁶⁸

Im Ergebnis ist somit festzuhalten, dass ein Auskunftsbegehren über die Identität von Tauschbörsennutzern gegenüber Access-Providern mE auch auf § 87 Abs 2 UrhG bzw auf § 55a MSchG gestützt werden kann. Durch den gesetzlichen Vorbehalt, dass eine Auskunft nur zu erteilen ist, sofern dies nicht unverhältnismäßig im Vergleich zur Schwere der Verletzung wäre, wird auch der unionsrechtlich gebotenen Verhältnismäßigkeitsprüfung Genüge getan.

De lege lata wird aber auch ein auf diese Gesetzesstelle gestützter Auskunftsanspruch scheitern.

Erstens gilt auch in diesem Zusammenhang, dass die für eine etwaige Auskunft benötigten Daten (dynamischen IP-Adressen) aufgrund der allgemeinen Löschungsverpflichtung gem § 99 TKG derzeit nicht gespeichert werden dürfen. Die oben dargestellte Situation, dass derzeit keine Art 15 Abs 1 Telekom-Datenschutz-RL genügende „Rechtsvorschrift“ besteht, die eine Speicherung von Verkehrsdaten für die Verfolgung von Immaterialgüterrechtsverletzungen gestattet, gilt selbstverständlich auch für § 87b Abs 2 UrhG bzw § 55a MSchG.

Zweitens ist nach dem Gesetzeswortlaut nur dann die begehrte Auskunft zu erteilen, wenn dies nicht gegen gesetzliche Verschwiegenheitspflichten verstoßen würde. Unter diese „gesetzlichen Verschwiegenheitspflichten“ lässt sich mE auch das allgemeine Weitergabeverbot des § 93 Abs 3 TKG subsumieren. Dieses umfasst zwar keine Stammdaten, jedoch dürfte auch in diesem Zusammenhang nicht ausgeklammert werden, dass für die Ermittlung der

⁴⁶⁸ ErlRV 1324 BlgNR XXII. GP 4.

begehrten Stammdaten zunächst rechtswidrig Verkehrsdaten in Form von dynamischen IP-Adressen verarbeitet werden müssten, was nach der Rsp unzulässig ist.⁴⁶⁹

De lege ferenda könnte § 87b Abs 2 UrhG aber als taugliche Anspruchsgrundlage dienen, sobald eine gesetzliche Grundlage für das Speichern und Verarbeiten von Verkehrsdaten zum Zweck der Verfolgung von Urheberrechtsverletzungen vorliegt. Die bei § 87b Abs 3 UrhG vorliegenden unionsrechtlichen Bedenken liegen hier nämlich nicht vor.⁴⁷⁰

D.I.2.d. Ergebnis

Sowohl nach § 87b Abs 2 und Abs 3 UrhG wie auch nach § 55a MSchG besteht nach derzeitiger Rechtslage keine Möglichkeit, die Identität von Verletzern von Immaterialgüterrechten im Internet, insbesondere in Filesharing-Plattformen, auszuforschen. Die einzigen, die Zugriff auf die entscheidenden Datensätze hätten und auch zur Auskunft darüber verpflichtet sind, sind die Access-Provider. Diese dürfen allerdings die (dynamischen) IP-Adressen, die zur Verknüpfung von Verletzungshandlung und Internetusern benötigt werden, aufgrund datenschutzrechtlicher Vorschriften weder für Auskünfte speichern noch verarbeiten.

Das Unionsrecht steht einem zivilrechtlichen Auskunftsanspruch nicht entgegen. Es schreibt andererseits aber auch nicht vor, dass die Mitgliedsstaaten einen derartigen Auskunftsanspruch vorsehen müssen.

Verfassungsrechtlich ist umstritten, ob die Ausgestaltung des § 87b Abs 3 UrhG problematisch ist, weil Auskünfte direkt an Rechteinhaber zu erteilen sind, ohne dass ein Gericht die Rechtmäßigkeit des Auskunftsbegehrens vorab prüft. Zwar sprechen bessere Argumente für eine Unzulässigkeit aufgrund des Fernmeldegeheimnisses – unabhängig davon sollte aber schon aus Gründen der Rechtssicherheit ein solcher Richtervorbehalt eingeführt werden.

Eine allfällige gesetzliche Neuregelung in Österreich müsste nach der Judikatur des EuGH auch ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten sicherstellen und auch die anderen Grundsätze des Unionsrechts, wie insbesondere den Grundsatz der Verhältnismäßigkeit, beachten. Ob die derzeitige Ausgestaltung von § 87b Abs 3 UrhG diesen Maßstab bereits erfüllt, ist höchst zweifelhaft.⁴⁷¹

Im Ergebnis harrt die Problematik einer ordentlichen gesetzlichen Regulierung. Denn die gerade im Internet wichtigen und richtigen Sorgen um den Datenschutz werden hier dadurch konterkariert, dass sich sogar gewerbsmäßig agierende Täter hinter einer durch die IP-

⁴⁶⁹ RIS-Justiz RSo124952.

⁴⁷⁰ Vgl oben S 146.

⁴⁷¹ Vgl auch *Schachter*, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz - Anlassfälle Promusicae und MediaSentry, jusIT 2008 H 2, 20.

Adresse begründeten Anonymität verstecken können.⁴⁷² Andererseits wäre es nach dem derzeitigen Wortlaut von § 87b Abs 3 UrhG möglich, jede kleinste Urheberrechtsverletzung zum Anlass für eine Verarbeitung personenbezogener Daten und damit einen Eingriff in den geschützten Persönlichkeitsbereich zu machen, ohne dass ein unabhängiger Richter dies genehmigen müsste. Zudem bestehen nicht zu vernachlässigende Missbrauchsgefahren bei den derzeit verwendeten Methoden, die zur Ermittlung von IP-Adressen verwendet werden. Auch dies spricht dafür, ein gegebenenfalls durch Sachverständige unterstütztes Gericht über die Freigabe von persönlichen Daten entscheiden zu lassen.

D.I.3. Auskunft über Inhaber von IP-Adressen im Strafverfahren

D.I.3.a. Problemstellung

Nach § 91 Abs 1 UrhG sind ua Eingriffe in § 18a UrhG mit bis zu 6 Monaten Freiheitsstrafe bedroht. Das Uploaden von geschützten Werken in Tauschbörsen ist daher strafbar, im Falle der Gewerbsmäßigkeit sind sogar bis zu zwei Jahre Freiheitsstrafe vorgesehen (§ 91 Abs 2a UrhG). Bei der Identifikation von Straftätern, die im Internet Urheberrechtsdelikte begehen und dabei über ihre IP-Adresse Spuren hinterlassen, stellen sich ähnliche Fragen wie im zivilrechtlichen Bereich. Hier begehren allerdings die öffentlichen Strafverfolgungsbehörden Auskunft über die Identität von Internetusern bei den Access-Providern. Die Zulässigkeit der Verarbeitung von IP-Adressen ist daher am Maßstab der StPO zu prüfen.

Wenn die Zulässigkeit im Hinblick auf die Ermittlungsbehörden bejaht wird, ist noch zu prüfen, ob sich Rechteinhaber tatsächlich auf dem Umweg über das Strafrecht die erwünschten Informationen beschaffen können. Fraglich ist dies insbesondere deshalb, weil Urheberrechtsverletzungen gem § 91 Abs 3 UrhG Privatanklagedelikte sind und es somit dem Rechteinhaber obliegt, einen Strafantrag einzubringen.

D.I.3.b. Europarechtliche Grundlagen

Das Unionsrecht determiniert das Strafrecht in weit geringerem Ausmaß als das Zivilrecht. Zu beachten sind aber selbstverständlich die Grundrechtecharta und die Vorgaben der EMRK. Zur Durchsetzung von Rechten des geistigen Eigentums sind Strafbestimmungen derzeit nicht unionsrechtlich vorgesehen, aber durchaus in Planung.

D.I.3.b.1. Enforcement-RL und IPRED²

Nach ErwGr 29 der Enforcement-RL stellen in geeigneten Fällen - zusätzlich zu den zivil- und verwaltungsrechtlichen Maßnahmen, Verfahren und Rechtsbehelfen, die in dieser RL vorgesehen sind - auch strafrechtliche Sanktionen ein Mittel zur Durchsetzung der Rechte des geistigen Eigentums dar. Der ursprüngliche Entwurf der Kommission vom 30. 1. 2003

⁴⁷² Vgl dazu auch *Schmidbauer*, Die Metamorphose der Auskunftspflicht, MR 2007, 241.

hatte auch noch Bestimmungen über strafrechtliche Sanktionen bei schwerwiegenden, vorsätzlichen, gewerblich motivierten Schutzrechtsverletzungen enthalten. Wegen Kompetenzunklarheiten und politischer Kritik wurden die strafrechtlichen Bestimmungen aber in der Endfassung nicht aufgenommen.⁴⁷³

Gem Art 3 lit c bleiben innerstaatliche Vorschriften der Mitgliedstaaten betreffend strafrechtliche Verfahren und Strafen bei Verletzung von Rechten des geistigen Eigentums von der Enforcement-RL allerdings unberührt. Gem Art 16 können die Mitgliedstaaten auch andere, in der RL nicht vorgesehene, angemessene Sanktionen vorsehen. Die Enforcement-RL lässt daher den Mitgliedstaaten bei der konkreten Ausgestaltung von Straftatbeständen und Prozessnormen, die der Verfolgung von Immaterialgüterrechtsdelikten dienen, weitgehend freie Hand.

Vorschläge der Kommission für die Schaffung einer ergänzenden RL zur Enforcement-RL, die unter dem Titel „IPRED2“ („Intellectual Property Rights Enforcement Directive 2“) bekannt wurde und auch drastische Strafsanktionen enthalten sollte⁴⁷⁴, wurden nicht weiter verfolgt, weil weiterhin Zweifel daran bestanden, ob die EG im Binnenmarkt Strafvorschriften erlassen kann. Dieses Problem wurde durch den Vertrag von Lissabon beseitigt, sodass mit neuerlichen Vorschlägen der Kommission in diese Richtung zu rechnen ist.⁴⁷⁵

D.I.3.c. Nationale Rechtslage

Die gerichtliche Erhebung von Daten einer Telekommunikation zum Zwecke der Strafverfolgung hat grds nach den Bestimmungen der StPO zu erfolgen. Die Ermittlungen der Strafverfolgungsbehörden unterliegen dabei den Regeln der StPO, die mit 1.1.2008 umfassend novelliert wurde.⁴⁷⁶ Die oben dargestellten Bestimmungen des TKG zu Kommunikationsgeheimnis und Datenschutz sind im Strafprozess nicht anwendbar, weil gem § 92 Abs 2 TKG die Bestimmungen der StPO unberührt bleiben.

D.I.3.c.1. § 135 Abs 2 StPO

§ 135. (2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie

⁴⁷³ Burgstaller, Die Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, MR 2004, 405.

⁴⁷⁴ Vgl Schöwerling, EU-Kommission schlägt europäische Strafvorschriften bei der Verletzung geistigen Eigentums vor, MR-Int 2005, 138.

⁴⁷⁵ Vgl heise online vom 19.12.2009, <heise.de/newsticker/meldung/EU-Vertreter-sehen-ACTA-als-notwendig-im-Kampf-gegen-Urheberrechtsverletzungen-an-890239.html>.

⁴⁷⁶ Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz) BGBl I 2004/19.

zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

§ 134. Im Sinne dieses Bundesgesetzes ist

[...]

2. "Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

3. "Überwachung von Nachrichten" das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden,

Noch vor Erlass der neuen StPO wurde der OGH mit der Frage befasst, ob die Identität von Personen, die unter Verwendung einer IP-Adresse im Internet Urheberrechtsdelikte begehen, nur unter den Voraussetzungen der sog Rufdatenrückerfassung nach §§ 149a f StPO aF (entspricht dem heutigen § 135 Abs 2 StPO) offengelegt werden darf.

Anlassfall war eine Nichtigkeitsbeschwerde zur Wahrung des Gesetzes, die aufgrund divergierender Rechtsmeinungen zweier Senate des OLG Wien ergangen war.⁴⁷⁷ Eine Verwertungsgesellschaft hatte in zwei Verfahren als Privatanklägerin beantragt, Name und Adresse jenes Nutzers zu ermitteln, dem im Zuge umfangreicher Filesharing-Aktivitäten eine bestimmte und bereits bekannte IP-Adresse zugewiesen war. Die Untersuchungsrichterin sollte

⁴⁷⁷ Vgl *Bergauer*, Auskunftspflicht der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, RdW 2005, 467.

den Access-Provider, bei dem der unbekannte Täter Kunde war, anweisen, die Daten zu ermitteln und bekannt zu geben. In beiden Verfahren wurde der Antrag abgewiesen, weil die Untersuchungsrichterin eine Rufdatenrückerfassung iSd § 149a Abs 1 Z 1 lit b StPO iVm Abs 2 Z 2 StPO (entspricht heute § 135 Abs 2 Z 3 StPO) ortete, die nur dann zulässig sei, wenn sie der Aufklärung einer vorsätzlich begangenen strafbaren Handlung diene, die mit mehr als einjähriger Freiheitsstrafe bedroht ist. Das gegenständliche Höchststrafmaß des § 91 Abs 1 UrhG liege jedoch bei einer Freiheitsstrafe von maximal sechs Monaten, weshalb die Voraussetzungen einer Überwachung der Telekommunikation nach § 149a StPO nicht erfüllt seien.

Gegen diese beiden Entscheidungen legte die Verwertungsgesellschaft als Privatanklägerin jeweils Beschwerde beim OLG Wien ein.

Der erste erkennende Senat kam zu dem Ergebnis, dass es nicht Ziel des Verfolgungsantrages sei, festzustellen, welche Teilnehmeranschlüsse Ursprung und Ziel einer Telekommunikation waren, weil der Teilnehmeranschluss des unbekanntes Täters der Einschreiterin bereits bekannt sei. Ziel der Vorerhebung sei bloß die Bekanntgabe der Stammdaten, wie Name und Anschrift des Anschlussinhabers, die für die Abwicklung der Rechtsbeziehungen zwischen Provider und Nutzer notwendig sind. Dies erfolge durch die Zuordnung der bereits bekannten IP-Adresse, die der Senat als Verkehrsdatum qualifizierte. Da Stammdaten aber nicht dem Fernmeldegeheimnis unterliegen, sondern nur dem Datenschutz (nach TKG), seien Auskünfte an Strafgerichte zur Bekanntgabe von Stammdaten zum Zweck der Aufklärung und Verfolgung einer bestimmten Straftat nicht den Regelungen der §§ 149a ff StPO unterworfen.⁴⁷⁸

Der zweite erkennende Senat des OLG Wien kam zu einem völlig konträren Ergebnis: Verkehrsdaten wie die gegenständliche dynamische IP-Adresse dürften, auch wenn sie der Einschreiterin bekannt seien, nach dem Wortlaut des § 93 Abs 1 TKG nicht ohne die Voraussetzungen des § 149a StPO für die Ausforschung von Stammdaten verwendet werden. Die Herausgabe von Stammdaten durch Herausfilterung und Individualisierung des relevanten Teilnehmeranschlusses aus Log-files gehe über ein bloßes Nachschlagen hinaus und besitze somit Verkehrsdatenwertigkeit. Da der erkennende Senat auch Verkehrsdaten dem Schutzbereich des Fernmeldegeheimnisses unterstellte, kam er zu dem Schluss, dass jedes Zulassen der Eruiierung eines Teilnehmers am Telekommunikationsverkehr über eine von ihm hergestellte oder gewährte Verbindung dem hohen grundrechtlichen Anliegen des Art 10a StGG zuwiderlaufen würde.⁴⁷⁹

⁴⁷⁸ OLG Wien 30.03.2005, 17 Bs 76/05h.

⁴⁷⁹ OLG Wien 28.02.2005, 20 Bs 27/05z; zust *Bergauer*, Auskunftspflicht der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, RdW 2005, 467.

Der durch den Generalprokurator angerufene OGH ließ letztere Auslegung für die alte Rechtslage nicht gelten und stellte für die Rechtslage nach neuer StPO fest, dass der Eingriffstatbestand der „Auskunft über Daten einer Nachrichtenübermittlung“ (§ 135 Abs 2 StPO) nicht vorliege. Denn nach der Legaldefinition des § 134 Z 2 StPO sei darunter (nur) die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs 3 Z 4 TKG), Zugangsdaten (§ 92 Abs 3 Z 4a TKG) und Standortdaten (§ 92 Abs 3 Z 6 TKG) ua eines Telekommunikationsdienstes zu verstehen. Das entscheidende Argument des OGH lag allerdings darin, dass eine bloße Ermittlung, Auswertung, Zuordnung, Abgleichung, Verwertung oder sonstige Verarbeitung im internen Bereich des Providers das Telekommunikationsgeheimnis nicht verletze, weil dies nur ein Vorgang mit Außenwirkung könne.

Da auch keine planwidrige Gesetzeslücke vorliege, könne somit eine Auskunft über einen Inhaber einer IP-Adresse formlos erfolgen und gegebenenfalls mit den Zwangsmaßnahmen der StPO durchgesetzt werden.⁴⁸⁰

Edthaler/Schmidt gaben zu bedenken, dass dies im Ergebnis aufgrund des entstandenen Rechtsschutzdefizits unbefriedigend sei, gestanden dem OGH allerdings zu, in der Sache korrekt entschieden zu haben. Die Auskunftserteilung seitens der Access Provider sei schlicht kein Anwendungsfall des § 134 Z 2 StPO, da gerade keine Auskunft „über“ Verkehrsdaten begehrt werde, sondern lediglich auf die Feststellung der Identität hinter einer IP-Adresse abgezielt werde. Dass dabei Verkehrsdaten (dynamische IP-Adressen) verarbeitet würden, sei zweifellos richtig, doch würden diese Daten weder offengelegt noch seien sie unbekannt und schutzbedürftig.⁴⁸¹

Die strafgerichtliche Praxis folgt der Ansicht des OGH bis heute und weist Einsprüche von Access-Providern, die gemäß § 106 Abs 1 Z 1 StPO eine Gesetzesverletzung durch die formlose Ermittlung der Daten ihrer Kunden rügen, regelmäßig ab.⁴⁸² Das Problem, dass auch die formlose Auskunft über Name und Adresse von Teilnehmern nach § 103 Abs 4 TKG und § 18 Abs 2 ECG ausdrücklich auf „Ersuchen bzw Anordnung eines Gerichtes“⁴⁸³ erfolgen muss, während nach dem neuen Vorverfahren die Kriminalpolizei unter Leitung der Staatsanwaltschaft ermittelt, löst die Judikatur dabei mit Analogien bzw teleologischen Reduktionen der erwähnten Gesetzesstellen.⁴⁸⁴ In der Praxis bedeutet dies, dass die Kriminalpolizei im Rahmen ihrer Ermittlungen selbstständig an die Access-Provider herantritt, weil ein spezielles Ersuchen der Staatsanwaltschaft nicht erforderlich ist.⁴⁸⁵

⁴⁸⁰ OGH 26.7.2005, 11 Os 57/05z.

⁴⁸¹ *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 (224).

⁴⁸² ZB OLG Wien 8.9.2009, 18 Bs 302/09g; OLG Linz 7. 1. 2010, 7 Bs 407/09s.

⁴⁸³ Eigene Hervorhebung.

⁴⁸⁴ Vgl OLG Wien 8.9.2009, 18 Bs 302/09g.

⁴⁸⁵ Dazu krit *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 (224).

Hasberger bezweifelt mit beachtlichen Argumenten, dass die beschriebene Rechtsansicht des 11. Senates des OGH auch nach dem Verfahren „LSG/Tele2“ und den damit verbundenen Erkenntnisgewinnen aufrecht erhalten werden kann. Die von den Strafgerichten versuchte Aufteilung in einen internen, rechtlich nicht zu berücksichtigenden, und externen Schutzbereich sei nicht möglich und mit dem Willen des Gesetzgebers des DSG 2000 auch nicht vereinbar.⁴⁸⁶

Die Ausführungen des OGH in der Rechtssache „LSG/Tele2“, die in der Feststellung gipfeln, dass der einfache Weg, allein auf die Bekanntgabe von Stammdaten abzustellen und die Vorgänge bei deren Ermittlung völlig auszublenden, unionsrechtlich nicht gangbar sei, bringen tatsächlich die bisherige Linie der Strafgerichte ins Wanken. Durch die Ausblendung der Vorgänge bei der Ermittlung wird nämlich der datenschutzrechtliche Grundsatz unterwandert, dass gespeicherte Daten strikt zweckgebunden sind und nur für den Zweck, für den sie ursprünglich angehäuft wurden, auch verarbeitet werden dürfen.

Daher stellt sich auch rechtspolitisch die Frage, ob die konkurrierenden Ansichten des 11. und 4. Senates des OGH in Straf- bzw Zivilsachen und die daran anschließende Praxis der Ermittlungsbehörden bzw gerichtlichen Unterinstanzen auf Dauer so gelebt werden können. Die strafrechtliche Sicht bietet betroffenen Internetusern im Moment praktisch keinerlei Rechtsschutz bei der Offenlegung ihrer Identität, weil die Kriminalpolizei über die Access-Provider formlos ermitteln kann, wer im Internet möglicherweise strafrechtlich relevante Handlungen gesetzt hat. Der einzige Grund, warum dieses Schlupfloch von Inhabern von Immaterialgüterrechten nach derzeitiger Rechtslage noch nicht genutzt werden kann, ist die derzeitige Situation im strafrechtlichen Privatanklageverfahren (dazu sogleich). Auf der anderen, zivilrechtlichen, Seite ist die Tür im Moment hingegen für Rechteinhaber gänzlich verschlossen, weil die Rsp (richtigerweise) davon ausgeht, dass Stammdaten nur offengelegt werden dürfen, wenn die dafür notwendige Verarbeitung von Verkehrsdaten gesetzlich gestattet ist.

Bei einer allfälligen gesetzlichen Neugestaltung müsste mE das Schutzniveau für Identitätsdaten im Internet aus einem Guss neu geregelt und deren Offenlegung einheitlich der Prüfung der unabhängigen Gerichte überantwortet werden.

D.I.3.c.2. § 71 StPO (Privatanklageverfahren)

§ 71. (1) Strafbare Handlungen, deren Begehung nur auf Verlangen des Opfers zu verfolgen sind, bezeichnet das Gesetz. Das Hauptverfahren wird in diesen Fällen auf Grund einer Anklage des Privatanklägers oder seines selbstständigen Antrags auf Erlassung vermögensrechtlicher Anordnungen nach § 445 durchgeführt; ein Ermittlungsverfahren findet nicht statt.

⁴⁸⁶ *Hasberger*, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23.

[...]

(3) Die Privatanklage ist beim zuständigen Gericht einzubringen. Sie hat den Erfordernissen einer Anklageschrift (§ 211) zu entsprechen. Die Berechtigung zur Privatanklage und allfällige privatrechtliche Ansprüche sind, soweit sie nicht offensichtlich sind, in der Begründung darzulegen. Für einen selbstständigen Antrag gilt Gleiches.

(4) Das Gericht hat den Antrag dem Angeklagten und den Haftungsbeteiligten mit der Information zuzustellen, dass sie berechtigt seien, sich dazu binnen 14 Tagen zu äußern. Danach hat das Gericht, soweit es nicht nach § 485 oder § 451 vorgeht, die Hauptverhandlung anzuberaumen.

(5) Der Privatankläger hat grundsätzlich die gleichen Rechte wie die Staatsanwaltschaft. Zwangsmaßnahmen zu beantragen ist er jedoch nur insofern berechtigt, als dies zur Sicherung von Beweisen oder vermögensrechtlichen Anordnungen erforderlich ist. Die Festnahme des Beschuldigten oder die Verhängung oder Fortsetzung der Untersuchungshaft zu beantragen ist er nicht berechtigt.

[...]

Im Rahmen der Reform der StPO mit 1. 1. 2008 wurde das Privatanklageverfahren an das neue Vorverfahren, das fortan nicht mehr vom Untersuchungsrichter, sondern der Staatsanwaltschaft geleitet wird, angepasst. Einerseits wurde die Verfolgung von mutmaßlichen Straftätern für Rechteinhaber erleichtert, weil die bisherige sechswöchige Frist für den Verfolgungsantrag ab Kenntnis der Tat und des Tatverdächtigen entfallen ist. Andererseits brachte die neue Regelung des § 71 StPO auch deutliche Verschlechterungen für Inhaber von Immaterialgüterrechten mit sich, weil ein Ermittlungsverfahren bei Privatanklagedelikten, wie es Immaterialgüterrechtsverletzungen sind, nicht mehr stattfindet. Während nämlich nach alter Rechtslage ein Antrag auf gerichtliche Vorerhebungen gegen unbekannte Täter gestellt werden konnte, steht dem Privatankläger nach neuem Recht diese Möglichkeit nicht mehr offen.⁴⁸⁷

Das Privatanklageverfahren kann nur auf zwei Arten eingeleitet werden: entweder bringt der Privatankläger die Anklage bzw den Strafantrag bei Gericht ein, oder er beantragt die Erlassung selbstständiger vermögensrechtlicher Anordnungen nach § 445 StPO.⁴⁸⁸ Sein Strafantrag muss gem § 211 Abs 1 Z 1 StPO den Namen des Angeklagten sowie weitere Angaben zu dessen Person enthalten und weiters die Stellung des Privatanklägers als Rechteinhaber nachweisen (zB Registerauszüge bei Markenrechten). Durch eine der beiden Möglichkeiten

⁴⁸⁷ Vgl *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220; *Horak*, StPO-Reform 2008 und Immaterialgüterrecht, *ecolex* 2007, 949; *Hinterhofer*, Aktuelle Entwicklungen im Urheberstrafverfahren, MR 2008, 152.

⁴⁸⁸ *Horak*, Das neue Privatanklageverfahren, *ÖJZ* 2009/24, 213.

wird sofort das Hauptverfahren begonnen, weil – wie erwähnt – ein Ermittlungsverfahren nicht stattfindet.⁴⁸⁹

In diesem Zusammenhang ist insb zu beachten, dass der Privatankläger gem § 71 Abs 5 StPO nur insofern berechtigt ist, Zwangsmaßnahmen zu beantragen, als dies „zur Sicherung von Beweisen oder vermögensrechtlichen Anordnungen erforderlich ist“. Diese Anträge muss er zeitgleich mit dem Strafantrag oder im Laufe der Hauptverhandlung einbringen.⁴⁹⁰ Die Festnahme des Beschuldigten oder die Verhängung oder Fortsetzung der Untersuchungshaft zu beantragen ist er (selbstverständlich) nicht berechtigt; Hausdurchsuchungen werden in der Praxis eher restriktiv gehandhabt.⁴⁹¹ Die theoretische Gleichstellung des Privatanklägers mit der Staatsanwaltschaft ist dadurch deutlich eingeschränkt.

Bei anonym agierenden Filesharern liegt das Problem somit auf der Hand: ohne Kenntnis von Name und Adresse des Rechtsverletzers kann der Rechteinhaber im Privatanklageverfahren keinen formgültigen Strafantrag stellen. Zunächst müsste er ermitteln, wer der bislang unbekannte Täter ist. Der bisherige Weg, einen Strafantrag gegen unbekannte Täter einzubringen und dabei gleichzeitig dessen Ausforschung zu beantragen, ist durch den Wegfall des Ermittlungsverfahrens aber nicht mehr möglich.

Die selbständigen vermögensrechtlichen Anordnungen nach § 445 StPO, mit deren Beantragung das Hauptverfahren ebenfalls eingeleitet werden kann, schaffen im Ergebnis ebenfalls keine Abhilfe. Sie umfassen (lediglich) die Abschöpfung der Bereicherung (§ 20 StGB), des Verfalls (§ 20b StGB) und der Einziehung (§ 26 StGB) und können dann angeordnet werden, wenn keine Möglichkeit zur Entscheidung darüber in einem Strafverfahren oder in einem auf Unterbringung in einem der in den §§ 21 - 23 StGB genannten Anstalten gerichteten Verfahren möglich ist. Wenn einem Rechteinhaber daher konkrete Gegenstände bekannt werden, die seine Rechte verletzen (zB gefälschte Markenartikel, kopierte Musik-CDs etc), könnte er auch ohne Kenntnis des Täters einen Antrag auf Einziehung dieser Gegenstände gem § 26 StGB einbringen. Dadurch würde das Hauptverfahren eröffnet, in dem dann weitere Beweise – im eingeschränkten Rahmen des § 71 Abs 5 StGB - erhoben werden könnten.⁴⁹² Um unbekannte Täter in Filesharing-Netzwerken auszuforschen, böte sich sodann § 118 StPO (Identitätsfeststellung) an. Dieser ermächtigt die Kriminalpolizei, zur Identitätsfeststellung die Namen einer Person, ihr Geschlecht, ihr Geburtsdatum, ihren Geburtsort, ihren Beruf und ihre

⁴⁸⁹ Horak, StPO-Reform 2008 und Immaterialgüterrecht, *ecolex* 2007, 950.

⁴⁹⁰ Diese Bestimmung führt zu Schwierigkeiten in der Praxis; vgl Horak, Das neue Privatanklageverfahren, *ÖJZ* 2009/24, 213 (215).

⁴⁹¹ Hinterhofer, Aktuelle Entwicklungen im Urheberstrafverfahren, *MR* 2008, 152 (154). Gegenteilig berichtet Horak, Erste Erfahrungen mit der StPO 2008 in Privatanklageverfahren, *ecolex* 2008, 211.

⁴⁹² Hinterhofer, Aktuelle Entwicklungen im Urheberstrafverfahren, *MR* 2008, 152 (153).

Wohnanschrift zu ermitteln. Zulässig ist dies ua dann, wenn auf Grund bestimmter Tatsachen angenommen werden kann, dass eine Person an einer Straftat beteiligt ist.

Nach der oben dargestellten Judikaturlinie der Strafgerichte wäre mE eine Ermittlung der Identität von Filesharern vom Gesetzeswortlaut gedeckt, weil die Kenntnis einer IP-Adresse, unter der zB Urheberrechtsverletzungen begangen wurden, bereits eine „bestimmte Tatsache“ ist, die die Annahme gestattet, dass der Inhaber des betreffenden Internetanschlusses zumindest mittelbar an der Straftat beteiligt war. Auch die Einschränkung in § 71 Abs 5 StPO auf Zwangsmaßnahmen, die der Sicherung von Beweisen dienen, schadet mE in diesem Zusammenhang nicht: Gerade die Ermittlung des Inhabers des Internetanschlusses ist ein wichtiges Beweisergebnis, das die Suche nach dem unmittelbaren Täter erst ermöglicht. Datenschutzrechtliche Bedenken stehen dem nach der dargestellten Rsp nicht entgegen (vgl oben zu § 135 Abs 2 StPO).

Das praktische Problem allerdings liegt darin, dass bei den typischen Filesharing-Sachverhalten keine körperlichen „Gegenstände“ vorliegen werden, auf die insb § 26 StGB abstellt. Eine Eröffnung des Hauptverfahrens durch einen selbstständigen Antrag ist allerdings nach dem Wortlaut von § 71 Abs 1 StPO nur dann durchzuführen, wenn er im Zusammenhang mit einer vermögensrechtliche Anordnung gem § 445 StPO steht.⁴⁹³ Wenn daher mangels „Gegenständen“ keine vermögensrechtlichen Anordnungen beantragt werden können und deswegen das Hauptverfahren nicht eröffnet wird, ist für Rechteinhaber auch der Umweg über § 118 StPO abgeschnitten. Für die Ausforschung unbekannter Täter in Filesharingnetzwerken ist also auch diese zweite Möglichkeit, ein Privatanklageverfahren zu eröffnen, wohl nur in Ausnahmefällen geeignet.

Die nach der Reform verbliebenen Berechtigungen für den Privatankläger sind vor allem in solchen Szenarien für weitere Beweiserhebungen geeignet, in denen dem Privatankläger Name und Adresse des Täters bereits bekannt sind.⁴⁹⁴ Daher bieten sie nicht die Möglichkeit, unbekannte Täter in Tauschbörsen auszuforschen, weil die zeitlich vorgelagerte Ausforschung des Täters im Ermittlungsverfahren stattfinden müsste, das in Privatanklageverfahren aber eben nicht stattfindet.⁴⁹⁵

D.I.3.c.3. § 110 StPO (Polizeiliche Hinweise von Amts wegen)

§ 110. (1) Sicherstellung ist zulässig, wenn sie

1. aus Beweisgründen,

2. zur Sicherung privatrechtlicher Ansprüche (§ 367) oder

⁴⁹³ So auch OLG Linz 8.5.2008, 9Bs 128/08z.

⁴⁹⁴ Horak, StPO-Reform 2008 und Immaterialgüterrecht, eolex 2007, 950.

⁴⁹⁵ Edthaler/Schmid, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220.

3. zur Sicherung der Abschöpfung der Bereicherung (§ 20 StGB), des Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung

erforderlich scheint.

(2) Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen.

(3) Die Kriminalpolizei ist berechtigt, Gegenstände (§ 109 Z 1 lit. a) von sich aus sicherzustellen,

(...)

4. in den Fällen des Artikels 4 der Verordnung (EG) Nr. 1383/2003 des Rates vom 22. Juli 2003 über das Vorgehen der Zollbehörden gegen Waren, die im Verdacht stehen, bestimmte Rechte geistigen Eigentums zu verletzen, und die Maßnahmen gegenüber Waren, die erkanntermaßen derartige Rechte verletzen (Amtsblatt Nr. L 196 vom 02/08/2003 S. 0007 - 0014).

Eine weitere Neuerung der Strafprozessreform war die Einführung einer Anknüpfung an die Produktpiraterie-VO in § 110 Abs 3 Z 4 StPO, mit der erstmals ausdrücklich klar gestellt wurde, dass die Kriminalpolizei von sich aus offensichtlich immaterialgüterrechtsverletzende Gegenstände sicherstellen kann.⁴⁹⁶ Bis zur Reform war die Berechtigung dazu fraglich, weil zuerst der Rechteinhaber als potentieller Privatankläger verständigt werden müsste, wodurch die Sicherstellung eher von der Initiative einzelner Beamter abhängig war.⁴⁹⁷

Nach der Sicherstellung hat die Kriminalpolizei den Rechteinhaber gem § 113 Abs 2 letzter Satz StPO iVm § 3 Abs 1 PPG zu informieren. Diese Verständigungspflicht soll es dem Rechteinhaber ermöglichen, das Privatanklageverfahren oder andere Schritte einzuleiten.⁴⁹⁸

Auf Filesharing-Sachverhalte wird sich diese neue Befugnis der Kriminalpolizei in der Praxis wohl kaum auswirken. Einerseits ist schon die Anwendbarkeit der Bestimmung fraglich, weil sowohl Gesetz wie auch VO klar auf körperliche „Waren“ abstellen. Bei sinngemäßer Anwendung auch im Online-Bereich wäre Rechteinhabern im Ergebnis aber idR ebenfalls wenig geholfen, weil das Auffinden von Vertriebswegen der Filesharer und die Feststellung, welche „Waren“ sie zur Verfügung stellen, nicht das Problem sind. Gerade über diese Informationen verfügen die Rechteinhaber idR bereits. Vielmehr ist die Zurechnung der digitalen Dateien zu

⁴⁹⁶ Nur dieses Auslegungsergebnis macht Sinn; die legistische Ausgestaltung der Bestimmung ist mit dem Verweis auf die Produktpiraterie-VO eher missglückt. Vgl dazu *Hinterhofer*, Aktuelle Entwicklungen im Urheberstrafverfahren, MR 2008, 154; *Horak*, Erste Erfahrungen mit der StPO 2008 in Privatanklageverfahren, *ecolex* 2008, 211.

⁴⁹⁷ Vgl *Horak*, StPO-Reform 2008 und Immaterialgüterrecht, *ecolex* 2007, 950.

⁴⁹⁸ *Hinterhofer*, Aktuelle Entwicklungen im Urheberstrafverfahren, MR 2008, 152 (154).

einem konkreten Täter die Schwierigkeit. Die Bestimmung ist daher für den Online-Bereich nicht weiter von Belang.

D.I.3.d. Ergebnis

Die strafrechtliche Judikatur sieht in der Ausforschung von Personen, die hinter IP-Adressen mutmaßlich Straftaten begehen, keinen Anwendungsfall von § 135 Abs 2 StPO. Entsprechende Auskünfte sind daher von den Access-Providern formlos an die Ermittlungsbehörden weiterzugeben und bedürfen keines richterlichen Beschlusses.

Inhaber von Immaterialgüterrechten können diese Befugnis der Strafverfolgungsbehörden aus prozessualen Gründen aber nicht praktisch nützen. Seit der Strafprozessreform findet im Privatanklageverfahren, wie es bei Immaterialgüterrechtsdelikten vorgesehen ist, nämlich kein Ermittlungsverfahren mehr statt. Da eine Anklage gegen unbekannte Täter prozessual nicht gestattet ist, können Rechteinhaber in Filesharingnetzwerken begangene Urheberrechtsverletzungen de facto nicht strafrechtlich verfolgen. Insbesondere ist es ihnen nicht möglich, die Identität der Täter zu ermitteln.

Der Hinweis des OLG Linz,⁴⁹⁹ dass Privatankläger zur Durchsetzung ihres Antrags einen Anspruch auf Auskunft nach § 87b Abs 3 UrhG haben, der allenfalls auch im Klagsweg durchgesetzt werden kann, ist rückblickend wohl kein Trost für Rechteinhaber – auch dieser Weg ist seit der Entscheidung „LSG/Tele2“ versperrt.

Diese unbefriedigende Situation hat zu Reformbestrebungen geführt.

D.I.3.e. Exkurs: Reformbestrebungen

Nach politischen Konsultationen wurde am 29.9.2008 ein Ministerialentwurf des BMJ in Begutachtung geschickt, der ua spürbare Änderungen am oben dargestellten System vorsieht.⁵⁰⁰ Insgesamt sollen die de lege lata sehr restriktiven Bestimmungen merklich abgeändert und die Position der betroffenen Privatankläger dadurch verbessert werden. Die wesentlichen Neuerungen, die der Entwurf für § 71 StPO vorsieht, sind folgende:⁵⁰¹

Erstens soll nach Abs 1 leg cit das Konzept, im Privatanklageverfahren kein Ermittlungsverfahren vorzunehmen, dadurch abgeschwächt werden, dass ein solches nur mehr „grundsätzlich“ nicht stattfindet. Dem Privatankläger soll jedoch die Möglichkeit gegeben werden, einen Antrag auf Anordnung oder Bewilligung von Ermittlungsmaßnahmen nach dem 8. Hauptstück der StPO zur Ausforschung des Beschuldigten oder zur Sicherung von Beweisen oder vermögensrechtlichen Anordnungen zu stellen, wenn die Voraussetzungen für eine Anklage oder einen Antrag auf Erlassung vermögensrechtlicher Anordnungen noch nicht vorliegen.

⁴⁹⁹ OLG Linz 8.5.2008, 9Bs 128/08z.

⁵⁰⁰ ME Strafgesetzbuch, Mediengesetz ua, Änderung 82/ME XXIV. GP 5.

⁵⁰¹ Vgl weiterführend *Horak*, Das neue Privatanklageverfahren, ÖJZ 2009/24, 215.

Rechteinhaber könnten auf diesem Weg insbesondere ermitteln, wer unter dem Schutz der Anonymität in Tauschbörsen urheberrechtlich geschützte Werke zum Download bereit stellt. Entsprechende Anträge können nach dem Formvorgaben für Beweisanträge (§ 55 StPO) gestellt werden.

Zweitens wird dem Privatankläger in Abs 5 leg cit des Entwurfs – konsequenterweise - gestattet, zusätzlich zu den bereits bisher möglichen auch solche Ermittlungsmaßnahmen zu beantragen, die zur Ausforschung des Beschuldigten erforderlich sind. Im Ergebnis bliebe damit nur mehr die Festnahme des Beschuldigten und die Verhängung der Untersuchungshaft, die dem Privatankläger jedenfalls verwehrt wären.

Drittens ist in Abs 4 leg cit des Entwurfs eine Klarstellung vorgesehen, wonach die Zustellung von Anträgen des Privatanklägers an den Beschuldigten vorerst unterbleiben kann, wenn besondere Umstände befürchten lassen, dass ansonsten der Zweck einer beantragten Beweisaufnahme gefährdet wäre.

Weiters soll auch die legislatisch missglückte Gestaltung von § 110 Abs 3 Z 4 StPO, der wie erwähnt eine Befugnis der Kriminalpolizei auf Sicherstellung immaterialgüterrechtsverletzender Gegenstände vorsieht, angepasst werden. Inhaltlich dürfte sich dadurch nichts ändern.

Der Entwurf wird wohl erst im Zuge der Umsetzung der Vorratsdatenspeicherungs-RL, im Sinne eines „Gesamtpakets“, umgesetzt werden. Die vorgesehenen Änderungen sind mE prozessual sachgerecht – Probleme werden sich aber in weiterer Folge daraus ergeben, dass die stRsp der Strafgerichte zur rechtlichen Qualifikation von Ermittlungsvorgängen, die die Erhebung der Identität von Internetusern zum Gegenstand haben, aus heutiger Sicht wohl nicht mehr aufrechtzuerhalten ist (siehe oben zu § 135 Abs 2 StPO).

D.II. Unterbindung der Verletzungshandlung

Zentrales Mittel, um Verletzungshandlungen zu unterbinden, ist der immaterialgüterrechtliche Unterlassungsanspruch. Dessen Grundsätze sowie seine Anwendbarkeit auf Gehilfen des unmittelbaren Täters wurden bereits oben auf S 58 bzw S 70 behandelt. Um Wiederholungen zu vermeiden, beschränken sich die folgenden Ausführungen daher auf besondere Probleme im Zusammenhang mit Filesharing.

D.II.1. Anspruch auf Unterlassung gegen Filesharer

D.II.1.a. Grundsätze

So ein einzelner Filesharer überhaupt ermittelbar ist, kann er idR auf Unterlassung in Anspruch genommen werden, weil er selbst unmittelbarer Täter ist. Zwar ist umstritten, ob das Downloaden von urheberrechtlich geschützten Werken aus Tauschbörsen rechtswidrig ist, das simultan erfolgende Uploaden ist es aber jedenfalls. Entscheidend ist dabei nach dem

Wortlaut des Gesetzes nicht, ob oder wieviel andere User der Tauschbörse tatsächlich vom jeweiligen Filesharer laden, sondern alleine der Umstand, dass dieser der Öffentlichkeit urheberrechtlich geschütztes Material zur Verfügung stellt und bereits damit in das Zurverfügungstellungsrecht des Urhebers eingreift (§ 18a UrhG).⁵⁰²

Das Begehren hat sich daher darauf zu richten, es in Zukunft zu unterlassen, bestimmte Werke der Öffentlichkeit drahtgebunden oder drahtlos in einer Weise zur Verfügung zu stellen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist.

D.II.1.b. Anspruch auf Unterlassung gegen Computerinhaber

Fraglich könnte sein, ob nicht nur die physische Person, die an Filesharing teilnimmt, sondern auch der von (dieser verschiedene) Inhaber des benutzten Computers bzw. Internetanschlusses als Täter infrage kommt. In der Rsp⁵⁰³ wurde in diesem Zusammenhang darauf hingewiesen, dass das bloße Bereitstellen eines Computers mit Internetzugang noch keine bewusste Förderung einer Urheberrechtsverletzung darstellt, wenn keine besonderen Umstände hinzutreten, wegen derer der Inhaber des Computers mit Rechtsverletzungen durch den jeweiligen Benutzer des Computers rechnen müsste. Die Funktionsweise von Internettauschbörsen und Filesharing-Systemen könne bei Erwachsenen nämlich nicht als allgemein bekannt vorausgesetzt werden. Der OGH ortete insoweit auch keinen Verstoß seitens des Computerinhabers, der die Vermutung der Wiederholungsgefahr begründen würde, wenn vom fraglichen Computer Filesharing betrieben wurde. Eine Erstbegehungsgefahr lag im Anlassfall, in dem die Tochter des beklagten Vaters von dessen Computer Filesharing betrieben hatte, ebenfalls nicht vor. Der Beklagte hatte nämlich nach Erhalt des Aufforderungsschreibens für die Entfernung des Filesharing-Systems gesorgt, indem er seine Tochter angewiesen hatte, das Programm zu löschen und sie dieser Aufforderung nachkam. Es wurde damit jenes Instrument beseitigt, das Voraussetzung weiterer Eingriffe in Verwertungsrechte sein könnte. Der beklagte Vater, dessen Tochter Filesharing betrieben hatte, blieb daher haftungsfrei.

D.II.2. Anspruch auf Unterlassung gegen Access-Provider

D.II.2.a. Problemstellung

Beim Filesharing entstehen auch auf den Routern, die der Access-Provider verwendet, um für seine Kunden Datenströme durch das Internet zu leiten, Vervielfältigungen von idR urheber-

⁵⁰² Vgl dazu auch *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 1.

⁵⁰³ OGH 22.1.2008, 4 Ob 194/07v (Limewire).

rechtlich geschützten Werken.⁵⁰⁴ Ein Rechteinhaber könnte daher daran denken, den Access-Provider selbst nach § 81 Abs 1 UrhG als unmittelbaren Täter oder zumindest als Gehilfen des unmittelbaren Täters in Anspruch zu nehmen.

D.II.2.b. Europarechtliche Grundlagen

Mit der E-Commerce-RL, der Info-RL und der Enforcement-RL wurde der besonderen Rolle der Internetprovider in der Informationsgesellschaft Rechnung getragen. Die dabei relevanten Bestimmungen wurden bereits oben bei C.II.2.b. (S 67 f) behandelt, worauf an dieser Stelle verwiesen werden kann.

D.II.2.c. Nationale Rechtslage

Unabhängig davon, ob er als unmittelbarer Täter oder Gehilfe zur Haftung herangezogen werden soll, kann sich der Access-Provider jedenfalls nicht auf die Haftungsprivilegien des ECG (insb § 13 ECG) berufen, weil diese gem § 19 Abs 1 ECG nicht für gesetzliche Vorschriften gelten, die einen Unterlassungsanspruch einräumen.⁵⁰⁵

Eine Haftung als unmittelbarer Täter, die aufgrund der technisch notwendigen Vervielfältigungen im Serverbereich des Access-Providers angedacht werden könnte, scheidet jedoch von vorneherein aus, weil ein Access-Provider sich erfolgreich auf das einschlägige freie Werknutzungsrecht des § 41a UrhG berufen kann.⁵⁰⁶

Es kommt daher mangels Erfüllung des Unterlassungstatbestands in § 81 Abs 1 UrhG nur eine Haftung als Gehilfe des unmittelbaren Täters, also des jeweiligen Filesharers, in Betracht.⁵⁰⁷ Auch hier ist das oben entwickelte Prüfschema zu beachten, wonach der Access-Provider nur subsidiär zu den unmittelbaren Tätern und nur dann haftet, wenn er einen Beitrag zu einer offenkundigen Rechtsverletzung in seinem Netzbereich leistet, er davon Kenntnis hat, ihm ein Alternativverhalten zumutbar wäre und er dieses dennoch nicht setzt. Zusätzlich muss er aufgrund der Sonderregelung in § 81 Abs 1a Satz 2 UrhG jedenfalls vor Klagseinbringung abgemahnt werden.⁵⁰⁸

Ähnlich wie bei rechtsverletzenden Websites leistet der Access-Provider einen Beitrag zu Rechtsverletzungen im Wege des Filesharings, indem er die entsprechende technische Infrastruktur bereitstellt. Da das Phänomen von Tauschbörsen und die damit verbundenen Rechtsverletzungen mittlerweile allgemein bekannt sind, ist dieser Beitrag auch adäquat, weil

⁵⁰⁴ Access-Provider verwenden zahlreiche vernetzte Router, die die Weiterleitung von Datenpaketen besorgen. Vgl *Malhotra*, IP Routing 6. Damit ein Router derartige Datenpakete weiterleiten kann, muss er diese in seinen Arbeitsspeicher kopieren und somit vervielfältigen.

⁵⁰⁵ OGH 21.12.2006, 6 Ob 178/04a (Online-Gästebuch); vgl oben FN 189 f.

⁵⁰⁶ Siehe oben S 99 bzw FN 289.

⁵⁰⁷ Zur Möglichkeit, aus § 81 Abs 1a UrhG eine Haftung als unmittelbarer Täter abzuleiten, siehe oben S 76 f.

⁵⁰⁸ Zur Begründung dieses Prüfschemas vgl oben S 97 f.

die damit verbundenen Gefahren für den Provider vorhersehbar und beherrschbar sind. Die Offenkundigkeit der begangenen Rechtsverletzung wird idR ebenso leicht erkennbar sein, weil auch juristische Laien nicht davon ausgehen können, dass mit hohem wirtschaftlichem Aufwand produzierte Werke wie Kinofilme kostenfrei in Tauschbörsen abrufbar sind.

Fraglich ist jedoch, zu welchem Alternativverhalten der Access-Provider verpflichtet werden kann. Da bei Filesharing keine Domainnamen bzw stationären Server mit eindeutigen IP-Adressen verwendet werden, auf denen die Daten längerfristig liegen und abrufbar sind, werden die im Zusammenhang mit Websites diskutierten DNS- und Proxy-Sperrmaßnahmen nicht sinnvoll angewendet werden können. Technisch könnte der Access-Provider Filesharing in seinem Netz somit lediglich dadurch unterbinden, dass er die von entsprechenden Programmen dafür verwendeten Ports sperrt.

Ports sind, vereinfacht gesagt, Türen zwischen einem Netzwerk wie dem Internet und einem einzelnen PC. Programme, die einen Internetzugang benötigen, um richtig zu funktionieren, müssen ihre Datenströme dabei durch einen Port leiten. Manche dieser Programme verwenden einheitlich festgelegte und weithin bekannte Ports. So nutzen zB alle Webbrowser (Internet Explorer, Firefox etc) Port 80, um Webbrowsing im Internet zu ermöglichen, Mailprogramme (Outlook, Thunderbird) verwenden Port 110, um auf die weit verbreiteten POP3 E-Mail-Konten zuzugreifen. Wichtig ist dabei, dass Daten auf ihrem Weg durch das Internet durch zahlreiche verschiedene Router geleitet werden, die teils durch den Anbieter der Daten (Serverbetreiber), teils durch den Access-Provider und teils durch den Endnutzer (insb mittels Firewalls) kontrolliert werden können. Daraus folgt insb, dass die benötigten Ports auf allen beteiligten Routern und Firewalls offen sein müssen, weil der Datenstrom sonst sein Ziel nicht erreichen kann.

Da es abgesehen von den standardisierten Ports zehntausende weitere Ports gibt, die zT für beliebige Zwecke verwendet werden können, sind aus Sicherheitsgründen bei den meisten PCs und Routern durch Firewalls alle Ports gesperrt, soweit sie nicht für Standardanwendungen oder bestimmte verwendete Programme geöffnet sein müssen.

Während ältere Filesharing-Programme wie Napster bestimmte, festgesetzte Ports verwendeten, können neuere Programme wie uTorrent die von ihnen verwendeten Ports wechseln oder machen dies nach Wunsch automatisch.⁵⁰⁹ Von Userseite ist dafür lediglich das Ändern einer Zahl im Einstellungsmenü bzw das Setzen eines Häkchens sowie ein Neustart des Filesharing-Programms erforderlich. Eine vollkommene Unterbindung der Filesharing-Datenströme ist dessen, dass überhaupt kein Filesharing mehr stattfinden könnte, ist folglich technisch nicht möglich, sofern man nicht eine komplette Unterbindung des Datenverkehrs

⁵⁰⁹ Zu diesem Problem auch *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 6; *Einzigger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (115).

und damit eine gänzliche Sperre des Internetzugangs fordert.⁵¹⁰ Ein entsprechendes Begehren dürfte daher mE ähnlich wie bei Websitesperren lediglich darauf lauten, dass der Access-Provider es zu unterlassen hat, Nutzern den Zugang zum Internet zu ermöglichen, ohne gleichzeitig die Verwendung von Filesharing-Programmen durch diese Nutzer durch technische Maßnahmen (Port-Sperren) zu erschweren.

Fraglich ist allerdings, ob derartige Portsperren aus grundrechtlicher Perspektive verhältnismäßig und damit dem Access-Provider und anderen betroffenen Personen zumutbar sind. Ebenso wie bei „Sperren“ von Websites sind hier wirtschaftliche Interessen der Rechteinhaber einerseits und die des jeweiligen Access-Providers andererseits abzuwiegen. Dabei ist bei Ersteren nur der Entgang von Lizenzgebühren (§ 86 UrhG) zu berücksichtigen, der durch eine Portsperre voraussichtlich unterbunden werden kann.⁵¹¹ Zu bedenken ist weiters, dass vielfach nur kleine Teile von urheberrechtlich geschützten Werken an andere User der Tauschbörse versandt werden, weil der jeweilige User idR mit tausenden anderen Nutzern verbunden ist und von jedem daher nur ein kleines Stück der Gesamtdatei benötigt. Daher bestehen Zweifel an der Werkqualität dieser übertragenen Teilstücke⁵¹², was zwar zunächst nichts am Eingriff in § 18a UrhG ändert, der nicht auf ein- oder mehrmaligen Abruf des jeweiligen Werks, sondern lediglich auf die öffentliche Zurverfügungstellung abstellt.⁵¹³ Der konkrete quantitative „Beitrag“ des jeweiligen Tauschbörsennutzers, soweit er überhaupt nachweisbar ist, wird aber in die Bemessung der wirtschaftlichen Interessen der Rechteinhaber einfließen müssen.⁵¹⁴

Auf Seiten der Access-Provider ist zunächst festzuhalten, dass sie –ebenso wie bei Websites – im Rahmen des „klassischen Geschäftsmodells“ lediglich einen technischen-mittelbaren Bei-

⁵¹⁰ Derartige Maßnahmen würden freilich massive grundrechtliche Bedenken entgegenstehen, insb im Zusammenhang mit der Informationsfreiheit (Art 10 EMRK; vgl dazu FN 314) und der Erwerbsfreiheit (Art 6 StGG). Zudem muss jeder Endnutzer im Rahmen des Universaldienstes Zugang zu einem funktionalen Internetzugang haben (§ 26 Abs 2 Z1 TKG); vgl auch *Parschalk*, Provider-Haftung für Urheberrechtsverletzungen Dritter, *ecolex* 1999, 834 (836).

⁵¹¹ Dies folgt aus einer grundrechtlichen Kosten-Nutzen-Überlegung; vgl mit ähnlichem Ergebnis zu DNS-Sperren von Websites LG Hamburg 12.11.2008, 308 O 548/08 (DNS-Sperren I): „Denn je geringer die Eignung ist, umso weniger wird vom Access-Provider unter Berücksichtigung des dargestellten zusätzlichen Aufwandes die Einrichtung einer solchen Sperre verlangt werden können.“

⁵¹² *Gutman*, Abruf im Internet von unbekanntem und offensichtlich urheberrechtlich unrechtmäßigen Werken, *MMR* 2003, 706; *Dillenz/Gutman*, UrhG & VerwGesG² § 41a UrhG Rz 13.

⁵¹³ Vgl *Dillenz/Gutman*, UrhG & VerwGesG² § 18a UrhG Rz 5.

⁵¹⁴ In OLG Köln 23.7.2010, 6 U 31/10, wurde etwa das Zurverfügungstellen eines „wesentlichen Teils“ eines Softwareprogramms in einer Tauschbörse für ausreichend befunden und der Erstinstanz dahin Recht gegeben, dass als fiktive Lizenzgebühr für die am Markt unstrittig zu einem vierstelligen Preis angebotene Software wegen der nicht kontrollierbaren Zahl möglicher Tauschbörsenteilnehmer ein Vielfaches des Entgelts für eine Einzellizenz angemessen erscheint.

trag leisten. Dementsprechend eng sind die Zumutbarkeitsgrenzen zu ziehen.⁵¹⁵ Jedoch können Portsperrern prima facie ohne großen wirtschaftlichen Aufwand gesetzt werden, weil lediglich einzelne Werte in der Software der Router geändert werden müssen. Nur eine ständige Aktualisierung der gesperrten Ports zur Unterbindung von dynamischen Portwechseln durch Filesharing-Programme ist äußerst aufwendig und erfordert umfassende Scans des Datenverkehrs. Solange daher nur das Setzen von spezifischen Ports begehrt wird, die nicht für Standardanwendungen benötigt werden, ist mE eine Portsperrern nicht von vorneherein ein unverhältnismäßiger Eingriff in das Recht auf Unversehrtheit des Eigentums bzw auf Freiheit der Erwerbsbetätigung und somit potentiell zumutbar. Mangels technischer Alternativen werden Portsperrern auch das gelindeste Mittel sein.

Ähnlich wie bei DNS-Sperrern ist jedoch zu beachten, dass Portsperrern leicht umgangen werden können und entsprechende Anleitungen dafür im Internet binnen Minuten auffindbar sind. Dementsprechend gering wird das wirtschaftliche Interesse der betroffenen Rechteinhaber an derartigen Sperrmaßnahmen einzustufen sein.

Zu berücksichtigen sind zudem die Grundrechte weiterer Personen, die uU nichts mit der Urheberrechtsverletzung in Tauschbörsen zu tun haben, aber dennoch durch Portsperrern bzw deren Anordnung beeinträchtigt werden. Hier könnte im Einzelfall eine Unverhältnismäßigkeit vorliegen, weil die Sperrern von Ports (und umso mehr das Sperrern des gesamten Internetzugangs) die Funktionstüchtigkeit zulässiger Programme und die Erreichbarkeit legaler Inhalte beeinträchtigen kann und somit in das Eigentum, die Erwerbstätigkeit oder die Informationsfreiheit dieser Personen eingreift, ohne dass die Leidtragenden einen Anlass dafür gesetzt hätten.⁵¹⁶

Eine abschließende Beurteilung der Zumutbarkeit von Portsperrern wird somit im Ergebnis dem konkreten Einzelfall überlassen bleiben.

Die in der Entscheidung „Online-Gästebuch“ angedachte Figur der besonderen Überwachungspflicht wird in Filesharing-Sachverhalten mE jedenfalls keine Anwendung finden können, selbst wenn der Access-Provider mit weiteren ähnlich gearteten Rechtsverletzungen rechnen muss. Ihm fehlen im Vergleich zum Host-Provider die Möglichkeiten, entsprechenden Rechtsverletzungen vorzubeugen, weil nur eine Überwachung des Datenverkehrs des jeweiligen Users Aufschluss darüber geben könnte, ob dieser weiterhin Urheberrechtsverletzungen in Tauschbörsen begeht. Würde dem Access-Provider eine derartige Pflicht auferlegt, würde aber nicht nur § 18 Abs 1 ECG ad absurdum geführt, sondern auch unverhältnismäßig

⁵¹⁵ Vgl oben S 102 mwN.

⁵¹⁶ Siehe auch die Fallbeispiele bei *Wiebe*, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 6; *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (115).

in das Fernmeldegeheimnis eingegriffen, das die Vertraulichkeit von Kommunikation schützt.

D.II.2.d. Ergebnis

Filesharing ist aus Sicht der Rechteinhaber schwerer zu unterbinden als rechtsverletzende Websites, weil es bei heute üblichen Programmen keine zentralen Server mehr gibt, sondern vielmehr dezentral zwischen den einzelnen Usern Daten getauscht werden. Somit gibt es auch keinen Host-Provider, auf den gegriffen werden könnte.

Da Filesharer schwer ermittelbar sind, könnten Klagen gegen Access-Provider in den Mittelpunkt des Interesses rücken. Access-Provider sind jedoch aufgrund ihres Geschäftsmodells weit von der Quelle der Rechtsverletzung entfernt und können aufgrund technischer Unzulänglichkeiten die Verwendung von Filesharing durch ihre Kunden zudem nicht völlig unterbinden, sondern lediglich erschweren. Die dafür in Frage kommenden Portsperren sind leicht zu umgehen und bergen zudem Gefahren für die Grundrechte unbeteiligter Dritter, was idR zu einer Unzumutbarkeit einer Sperre führen wird.

D.III. Genugtuung

Durch die rapide Verbreitung von urheberrechtlich geschütztem Material in Tauschbörsen kommt der Genugtuung für Rechteinhaber im Zusammenhang mit Filesharing große Bedeutung zu. Die Grundsätze der einzelnen Ansprüche wurden bereits im Zusammenhang mit rechtsverletzenden Websites (S 107 f) behandelt, worauf an dieser Stelle verwiesen werden kann.

D.III.1. Anspruch auf angemessenes Entgelt

So Filesharer ermittelbar sind, besteht gegen sie aufgrund ihres Eingriffs in das dem Urheber vorbehaltene Verwertungsrecht (§ 18a UrhG) ein Anspruch auf angemessenes Entgelt. Sie profitieren objektiv nämlich je nach der Art ihrer Teilnahme auf verschiedene Weise von diesem Eingriff. Sollten sie parallel zum Uploaden eines bestimmten Werkes gerade dasselbe Werk herunterladen (was aufgrund der starken Stückelung der einzelnen Datenpakete im heute üblichen BitTorrent-Protokoll gang und gäbe ist), liegt die Bereicherung im kostenfreien Bezug dieses Werkes. Wenn sie dagegen ein Werk ohne vorheriges Downloaden quasi „neu“ in den Kreislauf der Tauschbörse einführen und anderen Teilnehmern zur Verfügung stellen, profitieren sie zumindest durch die Verbesserung ihrer Download/Upload-Rate, was ihnen die fortgesetzte Teilnahme am Filesharing ermöglicht.⁵¹⁷

⁵¹⁷ Schon aufgrund dessen sind Argumente, wonach Filesharer in keiner Weise von der Zurverfügungstellung fremder Werke profitieren und es deswegen an der notwendigen Bereicherung fehlt, von vorneherein verfehlt.

Nach der Rsp ist jenes Entgelt angemessen, das üblicherweise für eine gleichartige im Voraus eingeholte Einwilligung des Urhebers gezahlt werden muss, somit der Marktpreis. Bei Standardsoftware ist dies nach der Lit der „Verkaufspreis“, der als einmalige Lizenzgebühr für die dauernde Nutzung der Software entrichtet wird.⁵¹⁸ Dieser Gedanke ist auch auf Musik- oder Filmdateien übertragbar, weil sich hierfür durch legale Angebote wie den iTunes-Store bereits ein Markt gebildet hat. Dementsprechend muss mE auch die Zahl der Uploads des jeweiligen geschützten Werks eine Rolle bei der Bemessung des angemessenen Entgelts spielen. Ob dieser Wert aber überhaupt nachvollziehbar zu ermitteln ist, ist nach derzeitigem Stand der Technik fraglich und wird im Einzelfall geklärt werden müssen.⁵¹⁹

Access-Providern droht keine Pflicht zur Zahlung von angemessenem Entgelt für Filesharing ihrer Kunden, weil sie durch ihre Haftungsprivilegien (§ 13 ECG) grds freigestellt sind und zudem als Gehilfen keinen Nutzen aus dem Ersparen der Lizenzgebühr ziehen.⁵²⁰

D.III.2. Anspruch auf Schadenersatz und Herausgabe des Gewinns

Für Schadenersatzansprüche kann das Problem, das konkrete Ausmaß der Rechtsverletzungen zu ermitteln, durch die Regelung in § 87 Abs 3 UrhG stark entschärft werden. Rechteinhaber können aufgrund dieser Bestimmung das Doppelte des gebührenden Entgelts begehren, ohne dass ein „Grundscha-den“ nachgewiesen werden müsste. Der Nachweis, dass das Werk auf eine dem Urheber vorbehaltene Art genutzt wurde und dafür ein bestimmtes Entgelt angemessen ist, genügt.⁵²¹

Im Einzelfall problematisch könnte der Nachweis des notwendigen Verschuldens sein, weil nicht bei allen Nutzern als bekannt vorausgesetzt werden kann, dass bei modernen Filesharing-Programmen ab dem ersten geladenen Dateistück sofort an alle anderen Nutzer, die dieses Stück noch benötigen, Daten upgeloadet werden.⁵²² Wenn die Umstände des Einzelfalls daher dafür sprechen, dass dem Nutzer nur am Bezug des Werkes gelegen war, er aber nicht wusste und auch nicht wissen musste, dass er dieses auch anderen zur Verfügung stellt, wird es beim (verschuldensunabhängigen) Anspruch auf angemessenes Entgelt zu bleiben haben.

Da Access-Provider gem § 13 ECG selbst dann ein Haftungsprivileg besitzen, wenn sie positive Kenntnis von Rechtsverletzungen in ihrem Leitungsbereich haben, scheiden Schadenersatzansprüche wegen Filesharings gegen sie aus.

⁵¹⁸ Höller, Software-Urheberrechtsverletzungen im Konkurs, *ecolex* 2003, 922.

⁵¹⁹ Vgl oben S 118 und FN 368.

⁵²⁰ Siehe oben S 107 f.

⁵²¹ RIS-Justiz RS0111242.

⁵²² Vgl OGH 22.1.2008, 4 Ob 194/07v (Limewire).

D.III.3. Anspruch auf Urteilsveröffentlichung

Das für jeden Anspruch auf Urteilsveröffentlichung notwendige berechtigte Interesse wird bei Filesharing-Sachverhalten idR nicht vorliegen. Insb ist idZ das Argument verfehlt, dass durch „abschreckende“ Veröffentlichungen bekannt würde, dass Filesharing durchaus verfolgt und „bestraft“ wird, und Internetnutzer deswegen vermehrt davon Abstand nehmen würden. Nach stRsp darf der Anspruch auf Urteilsveröffentlichung nämlich nicht so verstanden werden, dass eine Veröffentlichung primär andere Personen von gleichartigen Gesetzesverstößen abschrecken sollen.⁵²³ Ziel dieser Maßnahme ist vielmehr allein die Aufklärung der Öffentlichkeit über einen bestimmten Gesetzesverstoß, dessen Publizität auch noch in Zukunft nachteilige und durch Unterlassungsgebot gegen den Beklagten nicht hintanzuhaltende Folgen befürchten lässt.⁵²⁴

Da Filesharing unter informierten Gleichgesinnten und weitgehend unter Ausschluss der Öffentlichkeit stattfindet, droht kein Umsichgreifen von unrichtigen Meinungen à la „Der Künstler XY bietet seine Musik jetzt kostenlos zum Download an“ in der Bevölkerung, die durch eine Urteilsveröffentlichung beseitigt werden könnten.⁵²⁵ Bei der Suche nach einem geeigneten Medium für eine Veröffentlichung bestünde zudem das Problem, dass die Teilnehmer an Tauschbörsen idR über die gesamte Erde verstreut sind, und eine Veröffentlichung des Urteils in landesspezifischen Medien nicht mit der notwendigen Wahrscheinlichkeit aufklärerische Wirkung entfalten könnte.⁵²⁶ Daher wird die gerichtliche Abwägung zwischen Notwendigkeit und Angemessenheit der Urteilsveröffentlichung idR dazu führen, dass kein berechtigtes Interesse vorliegt.

Falls es im Einzelfall dennoch zu bejahen ist, müsste vom Talionsprinzip notgedrungen abgewichen werden, weil eine Veröffentlichung in einem Torrent oder Filesharingprogramm unmöglich ist. In diesem Fall muss daher eine Veröffentlichung in anderen Medien (Zeitungen, Websites etc) und so erfolgen, dass das Verhältnis zwischen Veröffentlichungsform und Verletzungshandlung angemessen ist.⁵²⁷

⁵²³ RIS-Justiz RS0077305.

⁵²⁴ OGH 8.5.1984, 4 Ob 329/84 (Linzer Torte).

⁵²⁵ Zum Erfordernis der Beseitigungseignung vgl *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 213 f.

⁵²⁶ *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 224.

⁵²⁷ Vgl *Heidinger*, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht 166.

E. RECHTSVERLETZENDES KEYWORD-ADVERTISING

Keyword-Advertising ist eine weit verbreitete Form von Online-Werbung. Dabei werden auf Websites stichwortbezogene Werbeeinschaltungen angezeigt, die sich an den Eingaben des Internetusers oder dem Kontext der besuchten Site orientieren. Die entsprechenden Stichwörter können von den Werbenden gegen Entgelt vom jeweiligen Anbieter erworben werden. Die Abrechnungsmodelle sind dabei idR so ausgestaltet, dass der Werbende nur für jeden tatsächlich erfolgten Klick auf die Werbeeinschaltung, die durch einen Link auf die Website des Werbenden führt, eine Gebühr an den Anbieter abzuführen hat (cost per click).

Der weltweit mit großem Abstand führende Anbieter von Keyword-Advertising ist der Suchmaschinenbetreiber Google mit seinen Diensten „AdWords“ und „AdSense“. Das Geschäftsmodell mit AdWords basiert auf stichwortbezogenen Anzeigen, die auf den Ergebnisseiten der kostenlosen Suchmaschinen (insb <google.com>) oberhalb und seitlich der eigentlichen (im Fachjargon: „natürlichen“) Suchergebnisse auftauchen, wenn die Nutzer der Suchmaschine nach gebuchten Wörtern suchen. Der Werbebereich ist dabei durch das Wort „Anzeigen“ und abweichende Farbgestaltung (oberer Anzeigenbereich) bzw einen Trennstrich (seitlicher Anzeigenbereich) von den natürlichen Suchergebnissen getrennt.⁵²⁸

The screenshot shows a Google search for 'Rechtsberatung'. The search bar contains the text 'Rechtsberatung' and the search button is labeled 'Suche'. Below the search bar, it indicates 'Ungefähr 1.790.000 Ergebnisse (0,12 Sekunden)'. The main search results are listed below, starting with an advertisement for 'Rechtsberatung Online' which states '6 Anwälte sind gerade online. Stellen Sie jetzt Ihre Frage! JustAnswer.de/Anwalt'. Below the ad are several organic search results, including 'Ihre Rechte-Dr. Januschke', 'Rechtsberatung - Wikipedia', 'Erste Auskunft - Willkommen bei der Rechtsanwaltskammer Wien', 'Sozialinfo Wien - Rechtsberatung', 'HELP.gv.at - Soziales und Notfälle - Rechtsberatung für ...', 'Rechtsberatung', 'Rechtsberatung - ÖAMTC - Der Österreichische Automobil, Motorrad ...', and 'rechtsberatung.at - Internet-Portal für Rechtsberatung'. On the right side of the page, there is a section for 'Anzeigen' (Advertisements) with several legal service ads, including 'Organisation & Führung', 'RA Mardetschläger /Schulz', 'Harmonie und Zukunft', 'Rechtsberatung', 'Strafverteidigung', 'Rechtsanwalt Grasl - Wien', 'Rechtsanwalt Scheer', and 'Familienrecht'.

⁵²⁸ Zur Funktionsweise von AdWords weiterführend *Dichlberger*, Markenrechtliche Risiken bei Keyword-Advertising, *ecolex* 2008, 1032; die obenstehende Grafik dokumentiert eine Suchanfrage vom 19.12.2010.

Die Anzeigen werden über ein Online-Formular geschaltet. Darin legt der Werbekunde fest, bei welchen Suchworten die Anzeige erscheinen soll. Google bietet zusätzlich an, auch bei weitgehend passenden Keywords bestimmte Werbungen anzuzeigen (zB wird so auch bei der Suche nach "Rechtsanwalt" eine Anzeige für das Keyword "Rechtsberatung" angezeigt). Wenn mehrere Werbekunden dasselbe Keyword gebucht haben, legt Google die Reihenfolge fest, in der die Anzeigen aufscheinen. Dabei spielen vor allem das Budget, das die Werbekunden für jedes Keyword festlegen können, und die entsprechende Nachfrage eine Rolle.

Besonders Gattungsbegriffe wie „Rechtsberatung“ sind wertvolle AdWords, die nur gegen entsprechend höhere Bezahlung erworben werden können. Auch Kombinationen aus mehreren Wörtern, wie zB „kostenlose Rechtsberatung“ sind als AdWords buchbar. Für Werbende ist AdWords besonders attraktiv, weil aufgrund der enormen Nutzerzahlen zahlreiche Suchanfragen über die Suchmaschine von Google gesetzt werden und dementsprechend häufig gebuchte Wörter eingegeben werden, die potentielle Kunden auf die Anzeigen und damit das Onlineangebot der Werbenden aufmerksam machen können. Außerhalb der Google-Suchmaschinen profitiert Google zudem vom Dienst AdSense, welcher kontextsensitive Werbeeinschaltungen auf den Websites von Dritten erzeugt. Ein automatisiertes Scannprogramm („Crawler“) prüft den Inhalt der Website, deren Betreiber sich bei AdSense registriert hat, und erzeugt dazu passende Anzeigen (auf Websites, die sich mit Computern beschäftigen, entstehen zB Links zu PC-Händlern). Den Text der Anzeigen und die damit verbundenen Keywords bezieht Google aus dem Fundus seines AdWords-Dienstes. Einen Teil der so generierten Einnahmen gibt Google an die Betreiber der an AdSense teilnehmenden Websites weiter.

Rechtliche Probleme im Zusammenhang mit Keyword-Advertising stellen sich insb durch eine mögliche unlautere oder markenrechtsverletzende Nutzung fremder Kennzeichen als Keywords. Aufgrund des immaterialgüterrechtlichen Fokus dieser Arbeit beschränken sich die folgenden Ausführungen vor allem auf das Markenrecht.⁵²⁹

Während bei anderen Rechtsverletzungen im Internet oftmals das Kernproblem in der Ausforschung der Täter liegt, sind bei Diensten wie AdWords die handelnden Personen idR leicht auszumachen, weil sie bei der Buchung des jeweiligen Keywords dieses durch einen Link mit ihrer eigenen Website verknüpfen. Aus rechtlicher Sicht bereitet vielmehr das Unterbinden der Verletzungshandlung Probleme, weil keine „lupenreine“ Nutzung fremder Marken vorliegt, wie es bei gefälschten offline-Markenartikeln, die mit fremden Kennzeichen geschmückt werden, der Fall ist. Überprüfenswert ist zudem die Rolle des Anbieters von

⁵²⁹ Ansprüche aus beiden Rechtsgebieten (Marken- bzw Wettbewerbsrecht) sind separat zu prüfen, werden im Rahmen eines funktionalen und wettbewerbsbezogenen Verständnisses der Markenfunktionen aber zu ähnlichen Ergebnissen führen; vgl *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (282).

Keyword-Advertising-Diensten, weil dieser sich– wie zB Google – zwar durch Einnahmen aus diesen Diensten finanziert, die AdWords aber grds weder selbst auswählt noch die Gestaltung der Anzeigen bestimmt.

E.I. Informationsbeschaffung

Die Betreiber von Keyword-Advertising-Diensten bieten idR ein eigenes Compliance-Verfahren an, mit dem problematische Anzeigen auf ihre markenrechtliche Konformität geprüft und gegebenenfalls entfernt werden können.⁵³⁰ Falls dieses aber nicht fruchtet oder über die Unterlassung hinausgehende Ansprüche geltend gemacht werden sollen, kann die Ausforschung des jeweiligen Anzeigekunden samt seiner klagsfähigen Anschrift notwendig werden.

Da die mit Keyword-Anzeigen verbundenen Links idR zum Online-Auftritt des Anzeigekunden führen, dient dessen Website als Anknüpfungspunkt für die weitere Informationsbeschaffung. Die dabei in Frage kommenden rechtlichen und technischen Mittel wurden bereits oben bei C.I. (S 41 f) behandelt, worauf in diesem Zusammenhang verwiesen werden kann.

E.II. Unterbindung der Verletzungshandlung

Der markenrechtliche Unterlassungsanspruch gem § 51 MSchG, dessen grundlegende Tatbestandselemente oben unter C.II.1. (S 58) besprochen wurden, ist das zentrale Mittel zur Unterbindung von potentiellen Markenverletzungen im Zusammenhang mit Keyword-Advertising.

E.II.1. Anspruch auf Unterlassung gegen Keyword-Advertiser

E.II.1.a. Problemstellung

Eine im Markt gut eingeführte und bekannte Marke ist oftmals ein wesentliches Verkaufsargument gegenüber potentiellen Käufern. Sie dient insb dazu, die Waren und Dienstleistungen verschiedener Anbieter unterscheidbar zu machen und gibt somit gewisse Sicherheiten im immer stärkeren Wettbewerb. Daran hat auch der zunehmende Vertrieb von Markenartikeln über das Internet grds nichts geändert.

Ebenso wie offline besteht daher auch online die Tendenz, sich an den Erfolg von prominenten Markenprodukten „anzuhängen“ und die Käufer durch plumpe Fälschungen oder – subtiler – durch gezielte Irreführung vom Anbieter der tatsächlichen Ware abzulenken und zum eigenen Konkurrenzangebot zu locken. Für Letzteres sind die Mechanismen des Keyword-Advertising wie geschaffen, weil es durch die Buchung von fremden Markennamen oder –

⁵³⁰ Im Falle von Google AdWords besteht ein eigenes Markenbeschwerdeverfahren, bei dem Rechteinhaber mittels eines Formulars die Überprüfung bestimmter Werbeanzeigen beantragen können; abrufbar unter <https://services.google.com/inquiry/aw_tmcomplaint?hl=de>.

bestandteilen möglich ist, interessierte Käufer durch geschickt gestaltete Anzeigen vom eigentlich gesuchten fremden Internetauftritt auf den eigenen zu lenken. Ob diese Vorgangsweise eine rechtswidrige Nutzung einer fremden Marke ist oder doch in den Bereich zulässiger Werbung fällt, stellt das zentrale Problem im Zusammenhang mit Keyword-Advertising dar.

E.II.1.b. Europarechtliche Grundlagen

Das Markenrecht wurde innerhalb der EU durch die Marken-RL bereits 1989 weitgehend harmonisiert. Durch die Marken-VO besteht seit 1994 zudem eine eigene Rechtsgrundlage für unionsweit gültige Gemeinschaftsmarken.

E.II.1.b.1. Marken-RL

Die Marken-RL findet gem Art 1 auf Individual-, Kollektiv-, Garantie- und Gewährleistungsmarken für Waren oder Dienstleistungen Anwendung, die in einem Mitgliedstaat oder beim Benelux-Amt für geistiges Eigentum eingetragen oder angemeldet oder mit Wirkung für einen Mitgliedstaat international registriert worden sind. Als Marke kommen alle Zeichen infrage, die sich grafisch darstellen lassen, insb Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen und die Form oder Aufmachung der Ware, soweit solche Zeichen geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden (Art 2). Art 3 und 4 regeln Eintragungshindernisse und Ungültigkeitsgründe, die bestimmte Zeichen von der Eintragung oder der weiteren Verwendung als Marke ausschließen.

Art 5 Abs 1 ordnet an, dass eine eingetragene Marke ihrem Inhaber ein ausschließliches Recht gewährt. „Dieses Recht gestattet es dem Inhaber, Dritten zu verbieten, ohne seine Zustimmung im geschäftlichen Verkehr a) ein mit der Marke identisches Zeichen für Waren oder Dienstleistungen zu benutzen, die mit denjenigen identisch sind, für die sie eingetragen ist; b) ein Zeichen zu benutzen, wenn wegen der Identität oder der Ähnlichkeit des Zeichens mit der Marke und der Identität oder Ähnlichkeit der durch die Marke und das Zeichen erfassten Waren oder Dienstleistungen für das Publikum die Gefahr von Verwechslungen besteht, die die Gefahr einschließt, dass das Zeichen mit der Marke gedanklich in Verbindung gebracht wird.“

Art 5 Abs 2 schützt darüber hinaus bekannte Marken vor unlauterer Ausnutzung oder Beeinträchtigung ihrer Unterscheidungskraft oder Wertschätzung durch identische oder ähnliche Zeichen, die für Waren oder Dienstleistungen benutzt werden, die nicht denen ähnlich sind, für die die Marke eingetragen ist. Nach der Rsp des EuGH ist dieses Recht über den Wortlaut von Art 5 Abs 2 hinaus auszulegen, weil auch die Systematik und die Ziele der Regelung, zu der die Bestimmung gehört, zu berücksichtigen sind. Somit betrifft sie nicht nur die Fälle, in denen ein Dritter ein mit einer bekannten Marke identisches oder ihr ähnliches Zeichen für

Waren oder Dienstleistungen benutzt, die denjenigen nicht ähnlich sind, für die diese Marke eingetragen ist, sondern auch die Fälle, in denen ein solches Zeichen für Waren oder Dienstleistungen benutzt wird, die mit denjenigen identisch oder ihnen ähnlich sind, für die diese Marke eingetragen ist.⁵³¹ Es bleibt allerdings aufgrund der bloßen Ermächtigung in Art 5 Abs 2 den Mitgliedsstaaten überlassen, ob sie dem Inhaber der bekannten Marke ein weitergehendes Ausschließungsrecht einräumen oder nicht.

So die Voraussetzungen in Art 5 Abs 1 oder Abs 2 erfüllt sind, kann der Markeninhaber gem Art 5 Abs 3 insb verbieten, dass Dritte ohne seine Zustimmung das Zeichen auf Waren oder deren Aufmachung anbringen, unter dem Zeichen Waren anbieten, sie in den Verkehr bringen oder zu diesen Zwecken besitzen, sie einführen oder ausführen. Für Dienstleistungen kann dementsprechend verboten werden, sie unter dem Zeichen anzubieten oder zu erbringen. Abs 3 lit d *leg cit* ordnet schließlich an, dass das Verbot auch umfassen kann, das Zeichen in den Geschäftspapieren und in der Werbung zu benutzen.

Die Grenzen der Wirkung der Marke werden in Art 6 und 7 gezogen. Die Marke gewährt ihrem Inhaber demzufolge (Art 6) „nicht das Recht, einem Dritten zu verbieten, a) seinen Namen oder seine Anschrift, b) Angaben über die Art, die Beschaffenheit, die Menge, die Bestimmung, den Wert, die geografische Herkunft oder die Zeit der Herstellung der Ware oder der Erbringung der Dienstleistung oder über andere Merkmale der Ware oder Dienstleistung, c) die Marke, falls dies notwendig ist, als Hinweis auf die Bestimmung einer Ware, insbesondere als Zubehör oder Ersatzteil, oder einer Dienstleistung, im geschäftlichen Verkehr zu benutzen, sofern die Benutzung den anständigen Gepflogenheiten in Gewerbe oder Handel entspricht.“ Das Recht aus der Marke erschöpft sich zudem (Art 7 Abs 1) bei Waren, die unter dieser Marke von ihrem Inhaber oder mit seiner Zustimmung in der Gemeinschaft in den Verkehr gebracht worden sind. Ausnahmen bestimmt Abs 2 *leg cit*.

Der EuGH hatte in einem Vorabentscheidungsverfahren ("Google France"), das auf Rechtsstreitigkeiten zwischen verschiedenen französischen Markeninhabern und Google zurückging, zu klären, inwieweit durch Keyword-Advertising bei Googles AdWords in fremde Markenrechte eingegriffen werden kann.⁵³² Ähnliche Probleme stellten sich auch in einem österreichischen Anlassfall ("Bergspechte").⁵³³ Zentrale Fragestellung war da wie dort, ob durch die Buchung von fremden Marken oder verwechselbar ähnlichen Begriffen als AdWords eine „Benutzung“ dieser Marken im geschäftlichen Verkehr iSv Art 5 Abs 1 lit a und b Marken-RL vorliegt, die der Markeninhaber dem Werbenden oder dem Suchmaschinenbetreiber verbieten kann.

⁵³¹ EuGH 9.1.2003 Rs C-292/00 (Davidoff) Rz 24-30; 10.4.2008 Rs C-102/07 (adidas und adidas Benelux) Rz 37.

⁵³² EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea).

⁵³³ EuGH 25.3.2010 Rs C-278/08 (Bergspechte).

Anknüpfend an seine stRsp erklärte der EuGH zunächst, ein mit der Marke identisches Zeichen werde „im geschäftlichen Verkehr“ benutzt, wenn die Benutzung im Zusammenhang mit einer auf einen wirtschaftlichen Vorteil gerichteten kommerziellen Tätigkeit und nicht im privaten Bereich erfolgt. Hinsichtlich des mit Adwords Werbenden stellte der EuGH fest, dass eine Nutzung iSd dieser Rsp vorliegt, weil nämlich aus Sicht des Werbenden mit der Auswahl des mit der Marke identischen Schlüsselworts bezweckt und bewirkt wird, dass ein Werbelink zu der Website gezeigt wird, auf der er seine Waren und Dienstleistungen anbietet. Da das als Schlüsselwort ausgewählte Zeichen der Auslöser für das Erscheinen dieser Werbung ist, sei im Ergebnis unbestreitbar, dass der Werbende es im Zusammenhang mit seiner kommerziellen Tätigkeit und nicht im privaten Bereich benutzt.⁵³⁴

Im Anschluss klärte der Gerichtshof die Frage, ob durch die Verwendung fremder Marken als Keywords auch eine Nutzung „für Waren und Dienstleistungen“ iS der genannten Bestimmungen erfolgt. Google hatte dem insb deswegen widersprochen, weil das Zeichen selbst nicht im Text der inkriminierten Werbeanzeigen vorgekommen war, und somit keiner der dem Markeninhaber in Art 5 Abs 3 Marken-RL vorbehaltenen Benutzungsformen vorliege. Der EuGH widersprach dem unter Hinweis auf die nicht taxative, sondern bloß exemplarische Aufzählung in Abs 3 leg cit (arg: „insbesondere“), die zudem erstellt wurde, als der elektronische Geschäftsverkehr und die Werbung in diesem Rahmen noch nicht richtig zur Entfaltung gekommen waren; die Anwendung von Informationstechnik könne daher zu anderen als den aufgezählten Benutzungsformen führen.⁵³⁵

Inhaltlich führte der EuGH aus, der Werbende ziele durch die Auswahl des mit einer Marke identischen Zeichens als Schlüsselwort darauf ab, dass die Internetnutzer, die dieses Wort als Suchbegriff eingeben, nicht nur auf die vom Inhaber dieser Marke herrührenden angezeigten Links klicken, sondern auch auf den Werbelink des Werbenden. Diese Situation verglich der Gerichtshof mit der von vergleichender Werbung (bei der er eine „Benutzung“ bereits früher bejaht hatte), weil der Mitbewerber eines Markeninhabers ein mit der Marke identisches Zeichen als Schlüsselwort ausgewählt habe, um den Internetnutzern eine Alternative zu den Waren oder Dienstleistungen dieses Markeninhabers vorzuschlagen. Somit handelt es sich bei Keyword-Advertising um eine „Benutzung für Waren oder Dienstleistungen“ des Werbenden, wenn dieser ein mit der Marke eines Mitbewerbers identisches Zeichen benutzt, um zu erreichen, dass der Internetnutzer nicht nur die von diesem Mitbewerber angebotenen Waren oder Dienstleistungen, sondern auch die seinen wahrnimmt.⁵³⁶

⁵³⁴ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 50-52 mwN; zur Entwicklung der diesbezüglichen Rsp des EuGH vgl *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (274 f).

⁵³⁵ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 66.

⁵³⁶ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 65-71 mwN.

Das gilt im Übrigen auch dann, wenn der Werbende dem Internetuser nicht seine Waren und Dienstleistungen als Alternative zu dem gesuchten Markenartikel präsentieren will, sondern das Ziel verfolgt, die Internetnutzer über die Herkunft seiner Waren oder Dienstleistungen in die Irre zu führen, indem er sie zu der Annahme verleitet, dass sie vom Markeninhaber oder einem wirtschaftlich mit ihm verbundenen Unternehmen stammen.⁵³⁷

Diese Überlegungen treffen allesamt auch dann zu, wenn lediglich ein der Marke ähnliches Zeichen als AdWord gebucht wird. Auch hier liegt eine Benutzung im geschäftlichen Verkehr für Waren oder Dienstleistungen vor.⁵³⁸

Entscheidend ist aber der folgende Schritt, wonach der Markeninhaber einer solchen Benutzung nur widersprechen kann, wenn (Variante A) bei identischen Zeichen durch die Benutzung in eine der Funktionen der Marke eingegriffen wird bzw (Variante B) bei ähnlichen Zeichen Verwechslungsgefahr iSv Art 5 Abs 1 lit b Marken-RL besteht.⁵³⁹

Die Begründung für Variante A, die dem Wortlaut von Art 5 Abs 1 lit a Marken-RL nicht direkt entnehmbar ist, liegt laut EuGH darin, dass das dort niedergelegte ausschließliche Recht gewährt wurde, um dem Markeninhaber den Schutz seiner spezifischen Interessen als Inhaber dieser Marke zu ermöglichen, dh um sicherzustellen, dass diese Marke ihre Funktionen erfüllen kann. Die Ausübung dieses Rechts müsse daher auf Fälle beschränkt bleiben, in denen die Benutzung des Zeichens durch einen Dritten die Funktionen der Marke beeinträchtigt oder beeinträchtigen könnte.⁵⁴⁰ Zu diesen „Funktionen“ der Marke zählen die Gewährleistung der Herkunft der Ware oder Dienstleistung gegenüber den Verbrauchern (herkunftshinweisende Funktion), welche die Hauptfunktion ist, und zudem die Gewährleistung der Qualität oder die Kommunikations-, Investitions- oder Werbefunktion.⁵⁴¹

Als relevant für Keyword-Advertising mit der Marke identen Zeichen beurteilte der EuGH idZ die herkunftshinweisende Funktion und die Werbefunktion. Ob erstere als Hauptfunktion der Marke durch die beschriebene Anzeige eines Dritten beeinträchtigt wird, hänge davon ab, wie die Anzeige gestaltet ist. Eine Beeinträchtigung liege dann vor, wenn aus der Anzeige für einen normal informierten und angemessen aufmerksamen Internetnutzer nicht oder nur schwer zu erkennen ist, ob die in der Anzeige beworbenen Waren oder Dienstleistungen vom

⁵³⁷ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 72 mwN.

⁵³⁸ Vgl EuGH 25.3.2010 Rs C-278/08 (Bergspechte) Rz 17-19.

⁵³⁹ Die Beschränkungen in Art 6 und 7 Marken-RL, die Dritten die Nutzung der Marke unter bestimmten Umständen freistellen, gelten freilich unabhängig davon.

⁵⁴⁰ EuGH 25.3.2010 Rs C-278/08 (Bergspechte) Rz 29; vgl auch EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 75-76 mwN.

⁵⁴¹ Vgl EuGH 18.6.2009 Rs C-487/07 (L'Oréal ea) Rz 58; weiterführend zu den verschiedenen Markenfunktionen vgl *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (277 f) mwN; *Fercher*, Markenrecht, in Wettbewerbs- und Immaterialgüterrecht 80 f.

Markeninhaber oder einem mit ihm wirtschaftlich verbundenen Unternehmen oder vielmehr von einem Dritten stammen. Zur Untermauerung dieses Befundes verwies der EuGH neben älterer Rsp noch auf ErwGr 29 der E-Commerce-RL, wonach aus Gründen des Verbraucherschutzes und der Lauterkeit im Geschäftsverkehr kommerzielle Kommunikation bestimmten Transparenzerfordernissen genügen muss, die in Art 6 E-Commerce-RL auch aufgestellt werden. Daraus folgt im Ergebnis, dass der Markeninhaber eine Buchung seiner Marke als (identen) Keyword und die damit verbundenen Anzeigen nur dann verbieten kann, wenn diese von den Internetnutzern fälschlich als von ihm stammend aufgefasst werden könnten. Darunter fällt auch eine Anzeige, die das Bestehen einer wirtschaftlichen Verbindung zwischen Markeninhaber und Werbendem zwar nicht suggeriert, aber hinsichtlich der Herkunft der fraglichen Waren oder Dienstleistungen so vage gehalten ist, dass der erwähnte durchschnittliche Internetnutzer auf Grundlage des Werbelinks und der ihn begleitenden Werbebotschaft nicht erkennen kann, ob der Werbende mit dem Markeninhaber wirtschaftlich verbunden ist oder nicht.⁵⁴²

Eine Beeinträchtigung der Werbefunktion der Marke durch Googles AdWords-Dienst verneinte der EuGH dagegen pauschal, weil die Werbe-Website des Markeninhabers ohnehin in der Liste der natürlichen Suchergebnisse erscheine, wenn der Internetnutzer den Namen einer Marke als Suchwort eingibt, und zwar normalerweise an einer der vordersten Stellen dieser Liste. Infolge dieser Anzeige, die im Übrigen unentgeltlich ist, sei die Sichtbarkeit der Waren oder Dienstleistungen des Markeninhabers für den Internetnutzer gewährleistet, unabhängig davon, ob es dem Markeninhaber gelingt, eine Anzeige auch in der Rubrik „Anzeigen“ unter den Ersten zu platzieren.⁵⁴³ Dieses Argument des EuGH ist freilich stark verallgemeinernd, weil idR nur solche Unternehmen tatsächlich unter den ersten Suchergebnissen aufscheinen, die in Suchmaschinenoptimierung investiert haben. Zudem lässt es alle Markeninhaber außen vor, die keine eigene Website betreiben.⁵⁴⁴

Eine Benutzung von der Marke ähnlichen Zeichen ist nach dem EuGH trotz der unterschiedlichen Rechtsgrundlagen in Art 5 Abs 1 Marken-RL (lit a für idente bzw lit b für ähnliche Zeichen) im Ergebnis gleich zu behandeln: Die für Variante B notwendige Verwechslungsgefahr liegt nach stRsp nämlich dann vor, wenn das Publikum glauben könnte, dass die betreffenden Waren oder Dienstleistungen aus demselben Unternehmen oder gegebenenfalls aus wirtschaftlich miteinander verbundenen Unternehmen stammen.⁵⁴⁵ Somit konnte der EuGH auch bei der Verwendung von ähnlichen Zeichen die zur herkunftshinweisenden Funktion

⁵⁴² Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 81-90.

⁵⁴³ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 91-98.

⁵⁴⁴ Daher zu Recht krit *Schubert/Ott*, Die Google France Entscheidung des EuGH, jusIT 2010/36, 85 (87).

⁵⁴⁵ EuGH 22.6.1999 C-342/97 (Lloyd Schuhfabrik Meyer) Rz 17; 6.10.2005 C-120/04 (Medion) Rz 26; 10.4.2008 C-102/07 (adidas ea) Rz 28 etc.

der Marke gewonnenen Erkenntnisse heranziehen und antworten, dass der Markeninhaber einem Werbenden verbieten darf, anhand eines mit der Marke identischen oder ihr ähnlichen Schlüsselworts, das dieser Werbende ohne Zustimmung des Markeninhabers im Rahmen eines Internetreferenzierungsdienstes ausgewählt hat, für Waren oder Dienstleistungen, die mit denjenigen identisch sind, für die die Marke eingetragen ist, zu werben, wenn aus dieser Werbung für einen Durchschnittsinternetnutzer nicht oder nur schwer zu erkennen ist, ob die in der Anzeige beworbenen Waren oder Dienstleistungen von dem Inhaber der Marke oder einem mit ihm wirtschaftlich verbundenen Unternehmen oder vielmehr von einem Dritten stammen.⁵⁴⁶

Eine Auskunft darüber, ob sich an diesen Grundsätzen irgendetwas ändert, wenn die inkriminierte Anzeige nicht in einer von den natürlichen Suchergebnissen getrennten und mit „Anzeigen“ gekennzeichneten Rubrik aufscheint, verweigerte der EuGH im Fall "Bergspechte" allerdings. Diese Frage sei für die Lösung des anlassgebenden Rechtsstreits nicht von Nutzen, weil hier die anlassgebende Anzeige unstreitig in einer solchen Rubrik gezeigt wurde.

Ebensowenig ließ sich der EuGH auf nähere Ausführungen dazu ein, welche Gesichtspunkte bei der Buchung von fremden Zeichen, die einer besonders geschützten bekannten Marke iSv 5 Abs 2 Marken-RL entsprechen, erfüllt sein müssen, um die Werbefunktion der Marke zu beeinträchtigen.⁵⁴⁷ Freilich besteht kein Grund, bei Keyword-Advertising von der gefestigten Rsp des EuGH abzuweichen, wonach die bloße Nennung der bekannten Marke dafür nicht ausreicht, sondern erst die Übertragung des Rufs und der Merkmale der bekannten Marke auf Waren oder Dienstleistungen eines Dritten zur rechtswidrigen Rufausbeutung führt.⁵⁴⁸

Der EuGH hat seine in den Verfahren "Google France" und "Bergspechte" erarbeitete, recht allgemein gehaltene Rechtsprechungslinie zum Keyword-Advertising auch in den Anlassfällen "Bananababy" und "Portokabin" beibehalten.⁵⁴⁹ Es bleibt dadurch bei beträchtlichen Ermessensspielräumen für die nationalen Gerichte, wann eine Beeinträchtigung der Herkunftsfunktion der Marke bzw Verwechslungsgefahr zwischen zwei Zeichen vorliegt.⁵⁵⁰

Google hat aufgrund der Entscheidungen des EuGH seine eigene Markenrichtlinie angepasst. Die Buchung fremder Marken als Keywords ist für die EU seit 14.9.2010 grds zulässig.⁵⁵¹

⁵⁴⁶ EuGH 25.3.2010 Rs C-278/08 (Bergspechte) Rz 41; EuGH 23.3.2010 (Google France ea) Rz 99.

⁵⁴⁷ EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 100 f.

⁵⁴⁸ Grundlegend EuGH 18. 6. 2009, Rs C-487/07 (L'Oréal/Bellure) Rz 41 f; dazu vgl auch *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (280 f).

⁵⁴⁹ EuGH 26.3.2010 Rs C-91/09 (Bananababy); EuGH 8.7.2010 Rs C-558/08 (Portokabin). Zu "Bananababy" vgl *Splittgerber*, Google France und Google – Klärung bei Markenrechtsverletzungen, NJW 2010, 2014 (2015 f).

⁵⁵⁰ Zu den damit verbundenen Risiken für die Rechtssicherheit vgl *Heidinger*, Keyword-Advertising: Nutzung fremder Kennzeichen als Schlüsselwörter, MR 2010, 119 (120).

⁵⁵¹ *Wukoschitz*, Keyword Advertising - "Bergspechte" - nun vom OGH entschieden, ecolex 2010, 972 (974).

E.II.1.b.2. Marken-VO

Die Marken-VO soll den Unternehmen eine unbehinderte Wirtschaftstätigkeit im gesamten Binnenmarkt ermöglichen, wofür Marken erforderlich sind, die einem einheitlichen, unmittelbar in allen Mitgliedstaaten geltenden Unionsrecht unterliegen (ErwGr 2). Das gemeinschaftliche Markenrecht tritt zwar nicht an die Stelle der nationalen Markenrechte (ErwGr 6), weil nicht alle Unternehmen gemeinschaftsweiten Schutz benötigen; es soll aber vermieden werden, dass sich in Rechtsstreitigkeiten voneinander abweichende Gerichtsurteile aus einer Gemeinschaftsmarke und aus parallelen nationalen Marken ergeben (ErwGr 17).

Dementsprechend wurden die wesentlichen Regelungen zum Recht aus der Gemeinschaftsmarke, seinen Beschränkungen und seiner Erschöpfung parallel zu den oben dargestellten Bestimmungen in der Marken-RL getroffen (vgl Art 9 Abs 1 lit a-c sowie Abs 2, Art 12 und Art 13 Marken-VO).

Der EuGH hat daher in seiner Vorabentscheidungen zum Anlassfall „Google France“ die für die Marken-RL gewonnenen Erkenntnisse ausdrücklich auch auf die Marken-VO erstreckt.⁵⁵²

E.II.1.c. Nationale Rechtslage

Das österreichische MSchG wurde in Umsetzung der Marken-RL in den §§ 10 – 10b den europarechtlichen Vorgaben angepasst (BGBl I 1999/111).

Bereits vor den einschlägigen Vorabentscheidungen des EuGH hatte der OGH einen genuin österreichischen Anlassfall aus dem Bereich des Weinhandels im Hinblick auf eine Verwendung fremder Marken als Keywords zu entscheiden.⁵⁵³

E.II.1.c.1. Die Entscheidung „Wein & Co“

Die Klägerin betrieb (und betreibt noch immer) unter dem Firmenschlagwort „Wein & Co“ das gleichnamige Weinhandelsunternehmen mit einem Filialnetz zum Vertrieb von Qualitätsweinen, eine Weinbar, eine Bar mit angeschlossenen Restaurant und unter der Internetadresse <weinco.at> auch einen entsprechenden Onlineshop. Die Bezeichnung „Wein & Co“ hatte sie sich mittels zweier Wortbildmarken markenrechtlich schützen lassen.

Das beklagte Unternehmen Interspar war (und ist) im selben Marktsegment tätig, insb auch mit einem unter <weinwelt.at> betriebenen Onlineshop. Es hatte beim Suchmaschinenbetreiber Google insgesamt 815 AdWords gebucht, darunter auch „Wein“ „Rotwein“ und „Wein & Co“, und damit erreicht, dass bei Eingabe eines dieser Suchbegriffe bezahlte Werbeanzeigen für seine Website <weinwelt.at> oberhalb und seitlich der natürlichen Suchergebnisse aufschienen. Die Anzeige der Beklagten war dabei so gestaltet, dass als Überschrift

⁵⁵² EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 49 f.

⁵⁵³ OGH 20.3.2007, 17 Ob 1/07g (Wein & Co).

„Wein & Co“ und darunter - wesentlich kleiner - „www.weinwelt.at“ erschien und im Werbetext daneben „tolle Weine für Sie oder Ihre Freunde: Geschenk-Pakete bestellen“ zu lesen war. Dem Dienst AdWords entsprechend waren beide Anzeigenrubriken mit dem Wort „Anzeigen“ gekennzeichnet (vgl die Abbildung oben S 170).

Der OGH wendete für die Fallprüfung § 10 Abs 1 Z 2 MSchG an, wonach eine Markenverletzung vorliegt, wenn ein mit der Marke gleiches oder ähnliches Zeichen für gleiche oder ähnliche Waren oder Dienstleistungen benutzt wird und dies die Gefahr von Verwechslungen begründet. Zwar waren die angebotenen Waren beider Unternehmen gleich, die Beklagte nutzte aber lediglich den Wortbestandteil der Wortbildmarke der Klägerin und damit laut dem OGH ein mit dieser Marke (lediglich) ähnliches Zeichen als Suchwort und zur Kennzeichnung ihres eigenen Angebots. Somit war in einem nächsten Schritt die Verwechslungsgefahr zu prüfen. Der OGH hätte mE aber ohne weiteres auch auf eine Verwendung eines mit der Marke gleichen Zeichens iSv § 10 Abs 1 Z 1 MSchG schließen können, weil die Wortbildmarke der Klägerin sich vom verwendeten Keyword nur durch die hinzutretende Farbgestaltung und die Schreibweise in Blockbuchstaben unterschied und nach hA und Rsp eine vollkommene Identität der Zeichen nicht erforderlich ist, weil ein Durchschnittsverbraucher nur selten die Möglichkeit haben wird, die Zeichen unmittelbar miteinander zu vergleichen. Auch bei geringen Unterschieden sind die Zeichen daher als gleiche Zeichen zu behandeln, wodurch eine Prüfung der Verwechslungsgefahr nicht mehr erforderlich ist.⁵⁵⁴

Die Gefahr von Verwechslungen war im Anlassfall freilich ohnedies offenkundig, weil die Beklagte ihre Anzeige mit einem der Marke zumindest hochgradig ähnlichen Zeichen überschrieb. Verwechslungsgefahr wurde laut OGH jedoch auch dadurch begründet, dass bei Eingabe des Suchworts der Hinweis auf die Website der Beklagten in der Trefferliste noch vor dem Hinweis auf die Website der Klägerin aufscheint oder besonders hervorgehoben wird.⁵⁵⁵ Die Vorreihung lasse ebenso wie die Hervorhebung den Eindruck eines besonderen Zusammenhangs zwischen dem Suchwort und dem Angebot der Beklagten entstehen, was wiederum den Eindruck wirtschaftlicher oder organisatorischer Nahebeziehungen zwischen der Klägerin und Beklagten entstehen lasse. Eine Verletzung der Markenrechte der Klägerin wurde daher bejaht, aufgrund ohnedies aufrechter Wiederholungsgefahr ließ der OGH allerdings offen, ob dies auch bei Werbeanzeigen in der Anzeigenrubrik rechts der natürlichen Suchergebnisse zutrifft.

⁵⁵⁴ *Kucsko*, Geistiges Eigentum 392; *Fercher*, Markenrecht, in Wettbewerbs- und Immaterialgüterrecht 98; EuGH 10.5.2003 C-291/00 (LTJ Diffusion) Rz 52.

⁵⁵⁵ Diese Formulierung ist missverständlich, weil der Link zur Website des Werbenden bei AdWords eben nicht in der Trefferliste der natürlichen Suchergebnisse aufschien, sondern vielmehr in einer eigenen, farblich markierten Anzeigenrubrik oberhalb der natürlichen Treffer. Ebendies dürfte der OGH aber gemeint haben; vgl auch *Noha*, Keyword Advertising - Verwendung von Kennzeichen Dritter als Suchwort, *ecolex* 2007, 616 (617).

Eine Differenzierung zwischen diesen beiden Ausprägungen der Werbung auf Google AdWords ist mE auch im Lichte der (freilich später ergangenen) Rsp des EuGH aber sachlich nicht indiziert, weil eine Abgrenzung von den natürlichen Suchergebnissen durch die Gestaltung (farbliche Markierung bzw Trennstrich) der Ergebnisseite da wie dort eindeutig erfolgt.⁵⁵⁶ Entscheidend ist alleine, ob ein normal informierter und angemessen aufmerksamer Internetnutzer durch die Gestaltung der Anzeige darüber irren kann, ob die mit dem Keyword verknüpfte Werbeanzeige vom Markeninhaber bzw einem mit ihm wirtschaftlich verbundenen Unternehmen oder von einem Dritten stammt. Da dies im Fall „Wein & Co“ zweifellos gegeben war, ist sie mE auch vom heutigen Wissenstand aus als europarechtskonform zu beurteilen.⁵⁵⁷

E.II.1.c.2. Die Entscheidung „Bergspechte“

Der bereits erwähnte zweite österreichische Keyword-Advertising-Fall drehte sich um die Wortbildmarke „BERGSPECHTE Outdoor Reisen und Alpenschule Edi Koblmüller“.⁵⁵⁸

Die Klägerin trat im geschäftlichen Verkehr unter dem Firmenschlagwort „Die BergSpechte“ auf und war Inhaberin der Domain <bergspechte.at>. Ihr Tätigkeitsbereich lag in Outdoor-Reisen, wie Trekking-, Abenteuer-, Berg- und Mountainbike- Reisen. Die Zweitbeklagte sowie ihr erstbeklagter Geschäftsführer waren ebenfalls auf diesem Markt aktiv und bewarben ihr Angebot unter der Domain<trekking.at>.

Bei mehreren Eingaben des Suchbegriffs „Edi Koblmüller“ in die Suchmaschine Google erschien die verlinkte Werbeanzeige der Zweitbeklagten unter der Überschrift „Trekking- und Naturreisen“ unmittelbar oberhalb der natürlichen Suchergebnisse in der beschrifteten Anzeigenrubrik. Bei der Eingabe von „Bergspechte“ erschien eine Werbeeinschaltung der Zweitbeklagten mit der Überschrift „Äthiopien mit dem Bike - Traumreise durch den Norden mit viel Kultur, sechzehn Tage ab 20. 10.“. Dieser Anzeigentext befand sich unter der Überschrift „Anzeige“ am rechten oberen Seitenrand, rechts neben der Trefferliste. Unmittelbar darüber, gleichfalls unter der Bezeichnung „Anzeigen“, fand sich die Werbeeinschaltung ei-

⁵⁵⁶ Vgl dazu auch *Anderl*, Glosse zu 17 Ob 1/07g (Wein & Co), MMR 2007, 497 (499). Dessen Einschätzung, dass durchschnittliche User in der farblichen Hinterlegung idR nur die Hervorhebung des relevantesten Treffers, nicht aber den Hinweis auf eine Werbeeinschaltung vermuten, ist mE nicht generell zuzustimmen; vgl auch *Büchle*, Glosse zu 17 Ob 3/08b (Bergspechte I), ÖBl 2009/15 (87) mwN. Bei Anzeigen oberhalb der natürlichen Suchergebnisse wird aber noch größere Aufmerksamkeit auf die Formulierung der Werbetexte zu legen sein, um Verwechslungsgefahr auszuschließen, weil diese sich optisch näher an der Suchleiste und damit am gesuchten Markenbegriff befinden.

⁵⁵⁷ Ebenso *Anderl*, Glosse zu EuGH Rs C-278/08 (Bergspechte), *ecolex* 2010/171 (477); *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (282).

⁵⁵⁸ OGH 20.5.2008, 17 Ob 3/08b (Bergspechte I); OGH 21.6.2010, 17 Ob 3/10f (Bergspechte II).

nes weiteren Anbieters. Klickte man auf die Anzeigenüberschrift „Äthiopien mit dem Bike“, so gelangte man zur Website der Zweitbeklagten.

Die Marke oder ihr ähnliche Zeichen schienen in keiner der beiden Anzeigen auf. Dieser signifikante Unterschied zur Entscheidung „Wein & Co“ veranlasste den OGH, sich zunächst näher mit der Rsp des EuGH zur Auslegung der Marken-RL zu befassen. Ob die Verwendung einer Marke oder eines ihr ähnlichen Zeichens als Keyword in der Online-Werbung auf den Trefferseiten von Suchmaschinen als eine dem Markeninhaber vorbehaltene „Benutzung“ iSv § 10a MSchG der Marke zu werten ist, konnte nach der damals bekannten Rsp des EuGH nicht eindeutig beantwortet werden, zumal die Verwendung – wie im Anlassfall – häufig „unsichtbar“ erfolgt, dh die Marke scheint im Anzeigentext selbst nicht auf, sondern ist aufgrund der Eingabe durch den Internetnutzer lediglich in der Suchleiste und gegebenenfalls in der Liste der natürlichen Suchergebnisse zu sehen. Der OGH leitete daher ein Vorabentscheidungsverfahren gem Art 234 EGV (heute Art 267 AEUV) ein.

Nach der oben erläuterten Antwort des EuGH auf die ihm vorgelegten Auslegungsfragen konnte der OGH eine dieser Auslegung entsprechende Endentscheidung treffen.⁵⁵⁹ Beide von den Beklagten verwendeten Keywords beurteilte er zutreffend als der geschützten Marke ähnliche Zeichen iSv § 10 Abs 1 Z 2 MSchG. In Einklang mit der Rsp des EuGH führte er weiters aus, dass beim Keyword-Advertising eine markenmäßige Nutzung des fremden Kennzeichens durch den werbenden Dritten erfolgt, und zwar unabhängig davon, ob die Marke in der so generierten Anzeige des Wettbewerbers sichtbar ist oder nicht.⁵⁶⁰ Da es sich bei den Keywords lediglich um der Marke ähnliche Zeichen handelte, war in weiterer Folge Verwechslungsgefahr zu prüfen.

Da keiner der beiden Anzeigentexte die vom Internetnutzer gesuchten Wörter enthielt, die angebotenen Dienstleistungen von Klägerin und Beklagten gleich waren und im Link „www.trekking.at“ lediglich ein beschreibender Gattungsbegriff aufschien, der keine Zuordnung des Online-Angebots zu einem bestimmten Unternehmen erkennen lässt, war für einen normal informierten und angemessen aufmerksamen Internetnutzer nicht zu erkennen, dass die Anzeigen von einem Anbieter stammen, der mit der Klägerin in keiner Weise wirtschaftlich verbunden ist. Es lag laut OGH für ihn vielmehr nahe, das Gegenteil zu vermuten, weil beide Suchworte ein hohes Maß an Originalität aufweisen und die angebotenen Dienstleistungen nicht einmal ansatzweise beschreiben. Der dadurch gegebenen Verwechslungsgefahr hätten die Beklagten durch entsprechende Gestaltung der Anzeigen, wie etwa durch Auf-

⁵⁵⁹ Eine Vorabentscheidung des EuGH bindet nach stRsp sowohl das vorlegende Gericht als auch alle anderen Gerichte, die in derselben Sache zu entscheiden haben. Die Entscheidung in der anhängigen Rechtsache ist so zu treffen, dass die vom EuGH vorgegebene Auslegung der fraglichen unionsrechtlichen Norm übernommen wird; RIS-Justiz RS0111726.

⁵⁶⁰ Vgl EuGH 25.3.2010 Rs C-278/08 (Bergspechte) Rz 19.

nahme eines aufklärenden Hinweises, entgegenwirken können. Da sie dies aber nicht taten, wurde dem Unterlassungsbegehren der Klägerin insoweit stattgegeben, als aus den konkreten Anzeige nicht oder nur schwer erkennbar war, dass zwischen der Klägerin und der Zweitbeklagten keine wirtschaftliche Verbindung besteht. Wie ein solcher aufklärender Hinweis gestaltet werden hätte müssen, sagte der OGH freilich nicht. In der Praxis wird eine kennzeichnungskräftige Domain, die in der Anzeige genannt wird, aber weder die fremde Marke selbst im Text enthält, noch sonst ein Naheverhältnis zum Markeninhaber suggeriert, bereits ausreichen, um eine Zuordnungsverwirrung beim angesprochenen Publikum zu vermeiden.⁵⁶¹

Im Anlassfall wurde der Beklagten daher im Endeffekt nur zur Unterlassung verpflichtet, weil die Nutzer der Suchmaschine aus der Adresse "www.trekking.at" keine aufklärende Information gewinnen konnten. Das Mehrbegehren, den Beklagten ganz allgemein zu untersagen, im geschäftlichen Verkehr auf Trefferlisten-Seiten von Internet-Suchmaschinen zu den Suchworten „Edi Koblmüller“ und/oder „Bergspechte“ mit einem Link auf die Homepage der Zweitbeklagten zu verweisen, lehnte der OGH dagegen als zu weitgehend ab.

E.II.1.d. Ergebnis

Durch die Verwendung einer Marke (eines Markenbestandteils) als Keyword für generierte Online-Werbung eines Dritten wird in die Rechte des Markeninhabers laut dem OGH nur dann nicht eingegriffen, wenn aus dieser Werbung für einen normal informierten und angemessen aufmerksamen Internetnutzer leicht zu erkennen ist, dass die in der Anzeige beworbenen Waren oder Dienstleistungen weder vom Inhaber der Marke noch von einem mit ihm wirtschaftlich verbundenen Unternehmen stammen. Ansonsten besteht ein Unterlassungsanspruch des Markeninhabers.

Aufgrund dieser Rsp ist es weiters im Ergebnis nicht entscheidend, ob ein zur Marke identisches oder nur ähnliches Zeichen als Keyword für die Bewerbung gleicher Waren oder Dienstleistungen verwendet wird, weil in beiden Fällen bereits ausreicht, wenn die Gefahr der wirtschaftlichen Zuordnungsverwirrung beim angesprochenen Marktpublikum besteht. Bei identischen Zeichen wird dies im Rahmen der Herkunftsfunktion der Marke geprüft, bei ähnlichen Zeichen dagegen führt das Vorliegen der Zuordnungsverwirrung zur Bejahung der für eine Markenverletzung ausreichenden Verwechslungsgefahr im weiteren Sinn.⁵⁶² Ganz allgemein besteht dadurch zwischen den Voraussetzungen für markenrechtlichen Schutz ge-

⁵⁶¹ Vgl *Wukoschitz*, Keyword Advertising - "Bergspechte" - nun vom OGH entschieden, *ecolex* 2010, 972 (973).

⁵⁶² Vgl *Schumacher* in *Kucsko*, *marken.schutz* 208.

gen identische Zeichen einerseits bzw bloß ähnliche Zeichen andererseits de facto kein Unterschied mehr.⁵⁶³

Im Übrigen hat der OGH in seiner "Bergspechte"-Entscheidung die Vorgaben des EuGH ("für einen Durchschnittsinternetnutzer nicht oder nur schwer zu erkennen") semantisch umgedreht ("für einen normal informierten und angemessen aufmerksamen Internetnutzer leicht zu erkennen"). Die österreichische Auslegung ist tendenziell restriktiver, weil die beiden Begriffe nicht komplementär sind, sondern die beiden entgegengesetzten Enden einer ganzen Skala repräsentieren, wie bereits *Wukoschitz* erkannt hat.⁵⁶⁴ Aufgrund des Vorrangs des Unionsrechts wird der OGH aber dem (zumindest sprachlich) liberaleren Ansatz des EuGH zu folgen haben und bereits ab einer "mittelschweren" Zuordenbarkeit die jeweilige Werbung zulassen müssen.

E.II.2. Anspruch auf Unterlassung gegen Suchmaschinenbetreiber

E.II.2.a. Problemstellung

Suchmaschinen spielen eine bedeutende Rolle im Zusammenhang mit Keyword-Advertising, weil sie für die meisten User die erste Anlaufstelle bei der Durchforstung der zahlreichen Angebote des Internets sind und sich zudem durch Werbeanzeigen – wie Googles AdWords – finanzieren. Da ihnen somit keine gänzlich neutrale Rolle im Keyword-Advertising-Geschäft zukommt, könnten Rechteinhaber daran denken, Suchmaschinenbetreiber in ihrer Funktion als Referenzierungsdiensteanbieter für Markenrechtsverletzungen durch Werbende in die Pflicht zu nehmen.

E.II.2.b. Europarechtliche Grundlagen

E.II.2.b.1. Marken-RL/VO

Auch bei Suchmaschinenbetreibern stellt sich die Frage, ob sie im Zuge ihrer Geschäftstätigkeit rund um Keyword-Advertising fremde Marken im geschäftlichen Verkehr und für Waren und Dienstleistung auf eine dem Markeninhaber vorbehaltene Art „benutzen“, indem sie Dritten erlauben, diese Marken oder ihre Bestandteile als Keywords zu buchen.

Der EuGH hatte daher auch in diesem Zusammenhang Art 5 Abs 1 lit a Marken-RL sowie Art 9 Abs 1 lit a Marken-VO auszulegen. Dabei stellte er zwar fest, dass der Anbieter des Referenzierungsdienstes eine kommerzielle Tätigkeit ausübt und einen wirtschaftlichen Vor-

⁵⁶³ Ebenso *Knaack/Venor*, Gerichtshof der Europäischen Union: Markenrecht und elektronischer Geschäftsverkehr, GRUR Int 2010, 385 (397); *Schubert/Ott*, Die Google France Entscheidung des EuGH, jusIT 2010/36, 85 (86). Für einen selbstständigen Anwendungsbereich beider Bestimmungen aber *Schuhmacher*, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, wbl 2010, 273 (278).

⁵⁶⁴ *Wukoschitz*, Keyword Advertising - "Bergspechte" - nun vom OGH entschieden, ecolex 2010, 972 (973).

teil anstrebt, wenn er für bestimmte seiner Kunden mit Marken identische Zeichen als Schlüsselwörter speichert und dafür sorgt, dass anhand dieser Schlüsselwörter Werbeanzeigen erscheinen. Die technischen Voraussetzungen für die Benutzung eines Zeichens zu schaffen und sich diese Dienstleistung vergüten zu lassen, bedeutet aber nach dem EuGH nicht, dass deren Erbringer dieses Zeichen selbst benutzt. Soweit er seinem Kunden eine solche Benutzung ermöglicht hat, sei seine Rolle gegebenenfalls nach anderen Rechtsvorschriften als nach den genannten Bestimmungen der Marken-RL und -VO zu beurteilen. Seitens des Erbringers von Referenzierungsdiensten liege daher keine Benutzung im Geschäftsverkehr vor, wodurch sich die weitere Prüfung, ob eine Benutzung „für Waren oder Dienstleistungen vorliegt, erübrigte.⁵⁶⁵ Dieses Auslegungsergebnis gilt auch dann, wenn der Erbringer des Referenzierungsdienstes – im Anlassfall also Google – es zulässt, dass Werbende Zeichen, die mit bekannten Marken wie „Louis Vuitton“ identisch sind, kombiniert mit Ausdrücken wie „Imitat“ oder „Kopie“ buchen und entsprechende Anzeigen erscheinen.⁵⁶⁶

E.II.2.b.2. E-Commerce-RL

Der EuGH wurde im Fall „Google France“ weiters gefragt, ob Art 14 E-Commerce-RL (dazu oben S 67) dahin auszulegen ist, dass ein Internetreferenzierungsdienst einen Dienst der Informationsgesellschaft darstellt, der in der Speicherung von durch den Werbenden eingegebenen Informationen besteht, so dass diese Daten Gegenstand von „Hosting“ im Sinne dieses Artikels sind und die Verantwortlichkeit des Anbieters des Referenzierungsdienstes nicht geltend gemacht werden kann, solange er von dem rechtswidrigen Verhalten dieses Werbenden keine Kenntnis hat. Die Verfahrensgegner von Google hatten argumentiert, dass AdWords kein Dienst der Informationsgesellschaft und die E-Commerce-RL somit insgesamt nicht anwendbar sei.

Die Definition des Begriffs „Dienst der Informationsgesellschaft“, der Dienstleistungen umfasst, die im Fernabsatz mittels Geräten für die elektronische Verarbeitung und Speicherung von Daten auf individuellen Abruf eines Empfängers und in der Regel gegen Entgelt erbracht werden, erfasst laut EuGH aber einen Dienst wie AdWords sehr wohl. Zudem speichert der Anbieter eines Referenzierungsdienstes dem Bild des Host-Providers entsprechend Informationen des Nutzers dieses Dienstes, nämlich des Werbenden, wie zB die vom Werbenden ausgewählten Schlüsselwörter, den Werbelink und die diesen begleitende Werbebotschaft sowie die Adresse der Website des Werbenden.⁵⁶⁷

Dennoch wollte der EuGH sich bei der konkreten Beurteilung nicht festlegen und führte aus, dass Google mit AdWords nur dann unter Art 14 E-Commerce-RL fällt, wenn sein Verhalten

⁵⁶⁵ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 53-59.

⁵⁶⁶ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 104.

⁵⁶⁷ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 14-15; 110-114.

auf das eines „Vermittlers“ in dem vom Gesetzgeber im Rahmen des Abschnitts 4 der E-Commerce-RL gewollten Sinn beschränkt bleibt. IdZ ergibt sich aus deren ErwGr 42, dass die hinsichtlich der Verantwortlichkeit festgelegten Ausnahmen nur die Fälle erfassen, in denen die Tätigkeit des Anbieters von Diensten der Informationsgesellschaft „rein technischer, automatischer und passiver Art“ ist, was bedeutet, dass der Anbieter „weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt“. Die Feststellung darüber, ob die Rolle von Google bei AdWords in diese Kategorie fällt, überließ der EuGH den nationalen Gerichten.⁵⁶⁸

Als Anhaltspunkte sollen dabei beachtet werden, dass Google mittels der von ihm entwickelten Programme die von den Werbenden eingegebenen Daten verarbeitet und dass als Ergebnis unter Voraussetzungen, die Google kontrolliert, Anzeigen gezeigt werden. So bestimmt Google die Reihenfolge der Anzeigen ua nach der von den Werbenden gezahlten Vergütung.

Der bloße Umstand, dass der Referenzierungsdienst entgeltlich ist, dass die Vergütungsmodalitäten von Google festgelegt werden und dass Google seinen Kunden Auskünfte allgemeiner Art erteilt, kann laut dem EuGH nicht zur Verneinung der Eigenschaft als neutralpassiver Host-Provider führen. Ebenso wenig reicht die Übereinstimmung zwischen dem ausgewählten Schlüsselwort und dem von dem Internetnutzer eingegebenen Suchbegriff aus für die Annahme, dass Google die Daten kennt oder kontrolliert, die von den Werbenden in sein System eingegeben und auf seinem Server gespeichert werden.

Dagegen ist für die genannte Prüfung von Bedeutung, welche Rolle Google bei der Abfassung der den Werbelink begleitenden Werbebotschaft oder bei der Festlegung oder der Auswahl der Schlüsselwörter gespielt hat. Hier könnte insb das Angebot Googles von Bedeutung sein, auch "weitgehend passende Keywords" für die Generierung von Werbeanzeigen heranzuziehen, und somit Nutzern der Suchmaschine auch dann die problematischen Werbeanzeigen zu zeigen, wenn sie eigentlich nur nach Variationen oder Oberbegriffen der Markennamen suchen.⁵⁶⁹

Das Auslegungsergebnis hinsichtlich Art 14 E-Commerce-RL lautete daher, dass die darin aufgestellte Regel auf den Anbieter eines Internetreferenzierungsdienstes Anwendung findet, wenn dieser keine aktive Rolle gespielt hat, die ihm eine Kenntnis der gespeicherten Daten oder eine Kontrolle über sie verschaffen konnte. Hat dieser Anbieter keine derartige Rolle

⁵⁶⁸ Vgl EuGH 23.3.2010 verb Rs C-236/08 bis C-238/08 (Google France ea) Rz 119.

⁵⁶⁹ Zur Funktionsweise *Dichlberger*, Markenrechtliche Risiken bei Keyword-Advertising, *ecolex* 2008, 1032; zur Frage, ob diese Funktion dazu führt, dass Google nicht mehr neutraler Vermittler ist vgl *Jaeschke*, EuGH: Gemeinschaftsrechtskonforme Möglichkeit zum Kauf von den Marken von Mitbewerbern entsprechenden Marken, *EuZW* 2010, 419 (427); *Anderl*, Glosse zu EuGH Rs C-278/08 (Bergspechte), *ecolex* 2010/171 (478); *Noha*, Glosse zu EuGH Rs C-278/08 (Bergspechte), *MR* 2010, 177 (180); *Schubert/Ott*, Die Google France Entscheidung des EuGH, *jusIT* 2010/36, 85 (88).

gespielt, kann er für die Daten, die er auf Anfrage eines Werbenden gespeichert hat, nicht zur Verantwortung gezogen werden, es sei denn, er hat die Informationen nicht unverzüglich entfernt oder den Zugang zu ihnen gesperrt, nachdem er von der Rechtswidrigkeit dieser Informationen oder Tätigkeiten des Werbenden Kenntnis erlangt hat.⁵⁷⁰

E.II.2.c. Nationale Rechtslage

Noch vor dem europäischen Verfahren „Google France“ wurde der österreichische OGH mit der Frage der Verantwortlichkeit von Google für seinen Dienst AdWords konfrontiert. Es stellt sich die Frage, ob die damals entworfene Rechtsprechungslinie mit den jüngeren europarechtlichen Vorgaben kompatibel ist.

E.II.2.c.1. Die Entscheidung „Glucochondrin“

Die Klägerin in diesem Rechtsstreit⁵⁷¹ war Inhaberin der Gemeinschaftswortmarke „Glucochondrin“ für pharmazeutische Erzeugnisse. Bei Eingabe des Suchbegriffs „Glucochondrin“ in die Suchmaschine <google.at> erschienen zu verschiedenen Zeitpunkten auf der ersten Seite der Trefferliste, oberhalb des ersten Treffers, als Anzeige gekennzeichnete Einschaltungen und auf dem rechten Bildschirmrand diverse Anzeigen, darunter eine mit dem Hinweis „Glucosamine Plus Extra“, samt einem Link zur entsprechenden Website. In den Anzeigen kam der Begriff „Glucochondrin“ nicht vor. Sie stammten allesamt nicht von der Klägerin, sondern von Konkurrenten, und führten zu deren Online-Angeboten.

Da Google einer Unterlassungsaufforderung nicht nachkam, klagte die Markeninhaberin auf Unterlassung. Der OGH erinnerte in seiner rechtlichen Beurteilung an seine stRsp im Zusammenhang mit der Haftung von Diensteanbietern für Rechtsverletzungen im Internet, wonach ein Diensteanbieter nur dann für Rechtsverletzungen seiner Kunden in Anspruch genommen werden kann, wenn ihm eine bewusste Förderung des Täters zum Vorwurf gemacht werden kann. Dies setzt voraus, dass die Rechtsverletzungen auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig sind.⁵⁷²

Für die Haftung eines Suchmaschinenbetreibers und damit für die Haftung der Beklagten für (angebliche) Rechtsverletzungen durch Keyword-Advertising könne nichts anderes gelten. Mit der Annahme von Werbeeinschaltungen, die bei Eingabe bestimmter Suchbegriffe aufgerufen werden, ermögliche Google zwar damit allenfalls verbundene Rechtsverletzungen; es habe aber mit der Auswahl der Suchworte nichts zu tun. Google stelle lediglich das Formular zur Verfügung, in das der Werbekunde die Suchworte einträgt, deren Eingabe die Werbeein-

⁵⁷⁰ Vgl. EuGH 23.3.2010 verb. Rs C-236/08 bis C-238/08 (Google France ea) Rz 116-120.

⁵⁷¹ OGH 19.12.2005, 4 Ob 194/05s und 4 Ob 195/05p (Glucochondrin).

⁵⁷² Siehe dazu oben S 61 f mwN.

schaltung aufrufen soll. Eine allfällige Rechtsverletzung durch die Verknüpfung des Suchworts mit einer Werbeeinschaltung sei idR nicht offenkundig.

Google ist somit nicht verpflichtet, die von Werbekunden verwendeten Suchworte ohne vorherige Abmahnung auf allfällige Markenverletzungen oder Wettbewerbsverstöße zu überprüfen. Eine Pflicht zum Handeln läge nur dann vor, wenn die Rechtsverletzung auch für einen juristischen Laien offenkundig wäre.

Ob eine offenkundige Rechtsverletzung zumindest nach der Abmahnung durch den Markeninhaber vorliegt, ließ der OGH im Anlassfall mangels Relevanz offen. Hier ist mE an die nunmehr vorliegende Rsp des EuGH anzuknüpfen – dieser hatte ja betont, dass der Markeninhaber einem Werbenden verbieten darf, anhand eines mit der Marke identischen oder ihr ähnlichen Schlüsselworts für Waren oder Dienstleistungen, die mit denjenigen identisch sind, für die die Marke eingetragen ist, zu werben, wenn aus dieser Werbung für einen Durchschnittsinternetnutzer nicht oder nur schwer zu erkennen ist, ob die in der Anzeige beworbenen Waren oder Dienstleistungen von dem Inhaber der Marke oder einem mit ihm wirtschaftlich verbundenen Unternehmen oder vielmehr von einem Dritten stammen.

Eine Beurteilung, ob ein solcher Fall vorliegt, wird für den Suchmaschinenbetreiber dann möglich sein, wenn er vom Markeninhaber darauf hingewiesen wurde, dass nicht von ihm stammende Werbeanzeigen mit seinen geschützten Marken verknüpft wurden. Sofern durch die Gestaltung der Anzeige suggeriert wird, der damit verknüpfte Online-Shop stamme vom Markeninhaber oder von einem mit ihm wirtschaftlich verbundenen Unternehmen, obwohl er in Wirklichkeit von einem Dritten stammt, wird mE eine offenkundige Markenrechtsverletzung durch den Werbenden vorliegen, die durch den Suchmaschinenbetreiber technisch ermöglicht wird.⁵⁷³ Google ist ein Alternativverhalten – dh die Löschung der betreffenden Anzeige – zumutbar, weil es keinerlei nennenswerte Aufwendungen verursacht und zudem in hohem Maße effektiv ist, weil danach die Anzeige nicht mehr neben den Suchergebnissen aufscheint. In einem solchen Fall muss daher mE eine Löschung der Anzeige erfolgen, will sich Google nicht einer bewussten Förderung der Markenrechtsverletzung schuldig machen. Im Weigerungsfall besteht ein Unterlassungsanspruch des Markeninhabers.

E.II.2.c.2. Zur Rolle von Art 14 E-Commerce-RL und § 14 ECG

Der vom EuGH gewählte allgemeine Ansatz, dass die in Art 14 E-Commerce-RL aufgestellte Regel auf den Anbieter eines Internetreferenzierungsdienstes Anwendung findet, wenn dieser keine aktive Rolle gespielt hat, die ihm eine Kenntnis der gespeicherten Daten oder eine Kontrolle über sie verschaffen konnte, legitimiert unionsrechtlich die vom OGH entworfene verschuldensabhängige Gehilfenhaftung für Unterlassungsansprüche. Da die Entscheidung,

⁵⁷³ Freilich können auch hier schwierige Abgrenzungsfragen auftreten: vgl *Noha*, Glosse zu EuGH Rs C-278/08 (Bergspechte), MR 2010, 177 (181).

wann eine Rechtsverletzung überhaupt vorliegt, den nationalen Gerichten überlassen bleibt, kann von einer Notwendigkeit, diese österreichische stRsp zu ändern, keine Rede sein. Eben- sowenig unterliegen Unterlassungsansprüche dadurch nun den Haftungsprivilegien der E- Commerce-RL oder des ECG.⁵⁷⁴

Das Ergebnis der Sache "Google France" unterstreicht vielmehr die oben auf S 83 f vertretene Position, dass die in der E-Commerce-RL und im ECG statuierten Haftungsprivilegien für Vermittler im Zusammenhang mit immaterialgüterrechtlichen Unterlassungsansprüchen keine Rolle spielen.⁵⁷⁵ So die materiellen Voraussetzungen für den Unterlassungsanspruch des Host-Providers vorliegen, sind die Haftungsprivilegien nicht mehr anwendbar und vice versa.

Aus diesem Grund konnte der OGH auch in der Entscheidung „Glucoschondrin“ davon abse- hen, Google überhaupt einer der Providerkategorien zuzuweisen, ohne gegen Unionsrecht zu verstoßen. Insofern ist die Entscheidung dieses Rechtsstreits durch den OGH auch aus heuti- ger Sicht unionsrechtlich gangbar.

Weiters wird in der österreichischen Lit gelegentlich vertreten, dass der EuGH in der Ent- scheidung "Google France" die Bestimmungen zu Host-Providern (analog) auslegen musste, weil die E-Commerce-RL im Gegensatz zum österreichischen ECG keine Haftungsbeschrän- kung für Suchmaschinen vorsieht.⁵⁷⁶ Diese Ansicht ist doppelt verfehlt: Erstens wäre, wenn überhaupt, die Regelung des Art 13 E-Commerce-RL zu Access-Providern analog auszulegen, weil diese von ihrer Tätigkeit her am ehesten einem Suchmaschinenbetreiber entsprechen (Vermittlung des Zugangs zu fremden Inhalten, ohne diese zu speichern). Zweitens ist die Tätigkeit eines Diensteanbieters stets funktional zu beurteilen, sodass auch in Österreich die Regelung des § 14 ECG nicht anzuwenden wäre, soweit nicht reine Suchmaschinenleistun- gen, sondern Dienste wie AdWords betroffen sind. Schließlich geht es bei Keyword- Advertising nicht um das Betreiben einer Suchmaschine, sondern um das Speichern und Ver- linken fremder Werbeanzeigen, also um Host-Providing und Linksetzung. Dass dabei mit Google "zufällig" der führende Suchmaschinenbetreiber auch führender Keyword- Advertising-Anbieter ist, darf im Rahmen einer funktionalen Betrachtungsweise keinen Un- terschied machen.

⁵⁷⁴ Offenb aA *Heidinger*, Keyword-Advertising: Nutzung fremder Kennzeichen als Schlüsselwörter, MR 2010, 119 (122), unter Berufung auf *Stadler*, EuGH: Google verletzt mit AdWords keine Markenrechte, MMR-Aktuell 2010, 301002.

⁵⁷⁵ Auch *Schubert/Ott*, Die Google France Entscheidung des EuGH, jusIT 2010/36, 85 (88) kommen zum Ergeb- nis, dass die Haftungsprivilegien im Zusammenhang mit Keyword-Advertising praktisch nicht relevant sind.

⁵⁷⁶ So *Noha*, Glosse zu EuGH Rs C-278/08 (Bergspechte), MR 2010, 177 (180); vgl auch *Schubert/Ott*, Die Google France Entscheidung des EuGH, jusIT 2010/36, 85 (87) mwN aus der deutschen Lit.

E.II.2.d. Ergebnis

Internetreferenzierungsdienstbetreiber wie Google mit seinem Dienst AdWords „benutzen“ fremde Marken nicht dadurch im geschäftlichen Verkehr für Waren und Dienstleistungen, dass sie Dritten ihre Buchung für Keyword-Advertising gestatten.

Ob sie idZ die Haftungsprivilegien eines Host-Providers iSv Art 14 E-Commerce-RL genießen, hängt nach dem EuGH davon ab, ob sie aktive Rolle gespielt haben, die ihnen eine Kenntnis der gespeicherten Daten oder eine Kontrolle über sie verschaffen konnte.

Für das österreichische Recht kann diese Frage dahingestellt bleiben, weil sich die Voraussetzungen für das entsprechende Haftungsprivileg in § 16 ECG und die materiellrechtlichen Voraussetzungen für einen Unterlassungsanspruch gegen Gehilfen decken. Keyword-Advertising-Dienstleister wie Google haften daher lediglich dann für Markenrechtsverletzungen ihrer Kunden, wenn sie diese bewusst fördern, was nur beim Vorliegen von offenkundigen Rechtsverletzungen und der Weigerung, diese zu entfernen, zu bejahen sein wird.

E.III. Genugtuung

IdR wird für Rechteinhaber die Unterbindung von markenrechtsverletzendem Keyword-Advertising im Mittelpunkt stehen. Darüber hinaus besteht auch die Möglichkeit zur Genugtuung. Die Grundsätze der dabei in Frage kommenden Ansprüche wurden bereits oben auf S 107 f behandelt, worauf hier verwiesen werden kann.

E.III.1. Anspruch auf angemessenes Entgelt

Gegen einen Werbenden, der eine Marke unbefugt im Rahmen von Keyword-Advertising benutzt, besteht gem § 53 Abs 1 MSchG ein Anspruch auf angemessenes Entgelt. Die Bereicherung liegt in der unbefugten und kostenfreien Ausnutzung des guten Rufs einer fremden Marke für eigene Werbezwecke.

Als angemessen ist jenes Entgelt zu beurteilen, das unter redlichen und vernünftigen Parteien üblicherweise für eine im Voraus eingeholte vertragliche Lizenz bezahlt hätte werden müssen. Dabei ist vor allem die allgemeine wirtschaftliche Bedeutung des Rechts zu berücksichtigen und es sind die Vor- und Nachteile abzuwägen, die der Verletzer gegenüber einem Lizenznehmer hat. Die Lizenz wird üblicherweise als Stücklizenz berechnet. Sie beträgt im Regelfall zwischen ein bis fünf Prozent des Bruttoerlöses; bei sehr bekannten Marken mit überragender Bedeutung für den Absatz kann die Lizenz bis zu fünfzehn Prozent betragen.⁵⁷⁷

Dem Betreiber des Keyword-Advertising-Dienstes (zB Google) droht idR keine Pflicht zur Zahlung von angemessenem Entgelt für Markenrechtsverletzungen ihrer Kunden, weil er als Gehilfe keinen Nutzen aus dem Ersparen der Lizenzgebühr zieht und somit nicht bereichert

⁵⁷⁷ OGH 30.11.2006, 3 Ob 222/06b mwN.

wird. Insofern ist es aus seiner Sicht auch unproblematisch, dass er sein uU gegebenes Haftungsprivileg als Host-Provider ab Kenntniserlangung verliert.⁵⁷⁸

E.III.2. Anspruch auf Schadenersatz und Herausgabe des Gewinns

Anstelle des angemessenen Entgelts kann der Verletzte bei schuldhafter Markenverletzung Schadenersatz einschließlich des ihm entgangenen Gewinns oder die Herausgabe des Gewinnes, den der Verletzer durch die Markenverletzung erzielt hat, verlangen (§ 53 Abs 2 Z 1 und 2 MSchG). Neben dem Markeninhaber selbst können nach der Rsp auch Lizenznehmer Schadenersatzansprüche geltend machen, weil die Rechtsordnung auch für das bloß abgeleitete Recht eine (quasi-)dingliche, dh von jedermann zu beachtende Wirkung der Kennzeichenrechte annimmt.⁵⁷⁹

Bei Beweisschwierigkeiten kann unabhängig vom Nachweis eines „Grundschadens“ das Doppelte des angemessenen Entgelts als Schadenersatz begehrt werden (§ 53 Abs 3 MSchG). Der hierbei notwendige erhöhte Verschuldensgrad (grobe Fahrlässigkeit oder Vorsatz) wird bei der Benutzung von fremden und bekannten Marken als Keywords idR zu bejahen sein, weil der Werbende oftmals ein Konkurrent des Markeninhabers sein wird und sich folglich kaum erfolgreich auf den Standpunkt stellen kann, die benutzte Marke nicht gekannt zu haben.

Keyword-Advertising-Anbieter dagegen können sich aufgrund dieser Regelung wohl im Regelfall aus der drohenden Haftung entziehen, sofern sie nach Abmahnung die inkriminierten Anzeigen entfernen. Ein „normaler“ (nicht pauschalierter) Vermögensschaden, der bereits ab dem Vorliegen von leichter Fahrlässigkeit zu ersetzen wäre, welche bei der Zulassung von Keyword-Kombinationen wie „Kopie“ oder „Imitat“ im Zusammenhang mit bekannten Marken zumindest denkbar erscheint, wird nämlich idR nicht nachweisbar sein. Das den Anbietern wie Google uU ebenfalls zustehende Haftungsprivileg aus § 16 ECG verlieren diese im Zusammenhang mit Schadenersatzansprüchen ebenfalls erst ab dem Vorliegen von bewusst grober Fahrlässigkeit (§ 16 Abs 1 Z 1 ECG).⁵⁸⁰

E.III.3. Anspruch auf Urteilsveröffentlichung

Das für den Anspruch auf Urteilsveröffentlichung notwendige berechtigte Interesse wird bei Markenrechtsverletzungen im Zusammenhang mit Keyword-Advertising-Diensten idR vorliegen, weil die rechtswidrige Werbung mit fremden Marken bei Anbietern wie Google große Publizität hervorruft. Die Aufklärung der Öffentlichkeit über einen derartigen Gesetzesverstoß wird mE auf zwei Arten notwendig sein:

⁵⁷⁸ Dazu oben S 107.

⁵⁷⁹ OGH 24.2.2008, 17 Ob 34/08m.

⁵⁸⁰ Siehe dazu weiterführend S 110.

Zum Einen ist das Urteil auf der Website des Werbenden zu veröffentlichen, weil Internetnutzer sich die Adresse des durch die Anzeige beworbenen Online-Shops merken oder in ihrem Browser speichern können und somit ohne erneuten Aufruf der Suchmaschine das rechtswidrig beworbene Online-Angebot des Werbenden weiterhin besuchen können. Dabei werden sie weiterhin die ursprünglich gesuchte Marke gedanklich mit dem fremden Angebot in Verbindung bringen, wodurch weiterhin die Gefahr der Zuordnungsverwirrung besteht. Durch das Gebot alleine, die Benutzung der fremden Marke für Werbeanzeigen in Zukunft zu unterlassen, kann diese aus Sicht des Markeninhabers nachteilige Folge nicht verhindert werden. Eine Aufklärung der Internetuser auf der mit der Anzeige verknüpften Website des Werbenden liegt daher im berechtigten Interesse des betroffenen Markeninhabers.

Darüber hinaus ist es mE auch denkbar und sinnvoll, dem Markenrechtsverletzer im Sinne des Talionsprinzips zusätzlich aufzutragen, innerhalb des Keyword-Advertising-Dienstes in seinen mit der Marke verknüpften Anzeigentext einen Hinweis auf die erfolgte und in Zukunft verbotene Rechtsverletzung aufzunehmen und diesen Text durch einen Link mit seiner Website zu verbinden, wo der Volltext der Urteilsveröffentlichung zu finden wäre. Diese Pflicht müsste freilich zeitlich begrenzt werden, wofür sich die für Websites angemessene Frist von 30 Tagen anbietet. Da dem Werbenden damit etwas aufgetragen wird (die Verknüpfung der fremden Marke mit einem Text in seiner Werbeanzeige), was ihm durch ein zu allgemeines Unterlassungsgebot gleichzeitig untersagt würde, müsste im Begehren und dem daran anknüpfenden Urteilsspruch eine entsprechende Ausnahme für die Urteilsveröffentlichung vorgesehen werden.

Somit würden Nutzer der Suchmaschine, die dort nach der geschützten Marke suchen, seitlich oder oberhalb der Suchergebnisse auch einen Link zur Urteilsveröffentlichung finden. Zwar würden auch so nicht alle Nutzer aufgeklärt, die durch das ursprüngliche rechtswidrige Keyword-Advertising erreicht wurden, und zudem bisher uninformierte Nutzer von den Rechtsverletzungen überhaupt erst erfahren. Dennoch sichert die beschriebene Vorgehensweise mE am ehesten die Äquivalenz zwischen dem Ausmaß der Rechtsverletzung und der deswegen gebotenen Aufklärung. Die beschriebenen Nachteile sind dabei in Kauf zu nehmen.⁵⁸¹

⁵⁸¹ Dazu *Ciresa*, Handbuch der Urteilsveröffentlichung³ Rz 224; 266 f.

F. RESÜMEE & AUSBLICK

Die gute Nachricht aus Sicht der Inhaber von Immaterialgüterrechten ist, dass das Internet nicht nur theoretisch, sondern im zunehmenden Maße auch praktisch kein rechtsfreier Raum ist. Viele Probleme, die sich durch den technologischen Fortschritt ergeben haben, konnten durch Weiterentwicklungen der Rsp oder der Gesetzeslage bereits in den Griff bekommen werden. Dies zeigt sich besonders schön im Zusammenhang mit Informationspflichten auf Websites, neuen Formen der Urteilsveröffentlichung oder der Anwendung bewährter Konzepte der Gehilfenhaftung auf die Tätigkeit der Internetprovider. Zwar sind auch hier noch einige Fragen offen, wie zB bei urheberrechtlichen Sperransprüchen gegen Access-Provider - es besteht aber nur mehr ein Maß an Rechtsunsicherheit, das rechtswissenschaftlich annehmbar ist, weil eine Lösung anhand vorhandener Rechtsnormen und bestehender Leitlinien in der Rsp möglich ist.

Andernorts bestehen starke Defizite, die derzeit nicht auf rechtspolitisch vertretbare Weise zu bewältigen sind. Besonders eindrücklich zeigt sich dies beim Komplex Filesharing, wo seitens des Gesetzgebers das Grundproblem, nämlich das Verhältnis zum Datenschutzrecht, auf geradezu haarsträubende Weise vernachlässigt wurde. Das hat in diesem Bereich zum einen dazu geführt, dass den typischerweise betroffenen Inhabern von Urheberrechten eine Durchsetzung ihrer Ansprüche faktisch verwehrt ist. Zum anderen wurde dadurch provoziert, dass die österreichische Rsp im Zivil- und Strafbereich trotz gleicher Fragestellungen grundsätzlich verschiedene Wege eingeschlagen hat, was den Schutz personenbezogener Daten im Internet betrifft. Da dies auf Dauer unhaltbar ist, harrt die Materie einer ordentlichen Neuregulierung durch die Politik. Leider ist zum Zeitpunkt der Fertigstellung dieser Arbeit lediglich feststellbar, dass eine Lösung dieser und anderer vergleichbarer Probleme blockiert ist, weil grundsätzliche Differenzen über die Rolle der Privatsphäre im Internet bestehen. Dies zeigt sich insb an der Debatte um die Umsetzung der Vorratsdatenspeicherungs-RL, mit der das weitere Schicksal des Urheberrechts im Internet wohl oder übel verknüpft wurde.

Vielleicht besteht idZ aber auch die Möglichkeit, dass Praktiker und Politiker mit der Unterstützung von Think Tanks und akademischer Lehre neue Wege für eine zeitgemäße Verbindung von neuen Technologien und Urheberrecht finden. Das heute (noch) vorherrschende „Stufensystem zur mittelbaren Erfassung des Endverbrauchers“⁵⁸², in dem zwischen Künstler und Nutzer viele verschiedene Werkvermittler aktiv sind (insb Verleger, Produzenten, Tonträgerhersteller etc), hört bereits seit Jahren auf, richtig zu funktionieren, weil Nutzer direkten und unkomplizierten Zugang zu geschützten Werken schätzen und wollen. Das ist dem Gesetzgeber seit Jahren bekannt, und er hat mit der Einführung von indirekten Vergütungsansprüchen wie der Leerkassettenvergütung auch darauf reagiert. Ein ähnlicher Mechanis-

⁵⁸² *Walter*, Österreichisches Urheberrecht Rz 523.

mus wird über kurz oder lang auch für die neuen und direkten Werknutzungen im Internet eingeführt werden müssen, will man sich nicht mit der Situation abfinden, dass die urheberrechtlichen Ausschließungsrechte trotz stetiger Verschärfung im zunehmenden Maße nutzlos werden. Zwischen neuen und erfolgreichen Vertriebsformen wie Apples iTunes-Store und radikalen Umbrüchen wie der Einführung einer Kulturflatrate bei gleichzeitiger Preisgabe der urheberrechtlichen Ausschließungsrechte muss ein gangbarer Mittelweg gefunden werden, der die negativen Auswüchse der Internetrevolution für Kreative und Kulturschaffende begrenzt – vollkommen verhindern lassen sie sich ohnehin nicht mehr.

Für weiterhin viel Diskussionen wird auch ein Bereich sorgen, in dem „Vermittler“ nach wie vor im Zentrum des Geschehens stehen: die Haftung der Internetprovider. Wie in den Kapiteln zum Keyword-Advertising und den rechtsverletzenden Websites gezeigt, bestehen auch heute durchaus Instrumentarien, um die Durchsetzung von Immaterialgüterrechten mit der Hilfe von Providern zu erleichtern. Es besteht daher keine Veranlassung dafür, dass in Europa durch die E-Commerce-RL vorgezeichnete System aus Haftungsbeschränkungen und reduzierten Handlungspflichten grundlegend dahin zu verändern, dass Internetprovider in Zukunft für fremde Daten auf ihren Servern oder in ihren Leitungen unbeschränkt haften sollen. Trotz des rasanten Fortschritts in den vergangenen Jahren ist die Architektur des Internets nämlich nach wie vor auf die wichtigen und wertvollen Dienste dieser Anbieter angewiesen. Aus Sicht der Internetprovider wäre es aber schon aus Gründen des Selbstschutzes angezeigt, noch mehr Energie und auch Geld darin zu investieren, ihre Systeme missbrauchsicher zu machen und mit Rechteinhabern zusammenzuarbeiten– Google geht hier mit AdWords und dem damit verbundenen Compliance-System zB bereits einen guten Weg, ähnliches zeichnet sich auch bei eBay im Zusammenhang mit markenrechtsverletzenden Produkten in Online-Versteigerungen ab. Die Tendenz geht hier also in Richtung einer außergerichtlichen Rechtsdurchsetzung, die auf Kooperation statt auf Konfrontation zwischen Rechteinhabern und Vermittlern basiert.

Nicht zuletzt liegt es aber auch bei der Rechtswissenschaft, den seit Jahrhunderten bestehenden grundlegenden Gegensatz zwischen freier Verbreitung von Geisteswerken einerseits und der Entlohnung der Schöpfer dieser Werke andererseits in einem für die moderne Kommunikationsgesellschaft fruchtbringenden und gerechten Weg zu gestalten. Für Juristen bietet die zukünftige Entwicklung somit die Chance, an der Schnittstelle von Immaterialgüter- und Internetrecht weiterhin neue Fragen zu beantworten, die gleichermaßen Verständnis für die technologischen Neuerungen und ein gehöriges Maß an Phantasie erfordern.

G. LITERATURVERZEICHNIS

<p><i>Adrian</i>, Technikentwicklung und Patentrecht, in <i>Adrian/Nordemann/Wandtke</i> (Hg), <i>Josef Kohler und der Schutz des geistigen Eigentums in Europa</i> (1996) 31</p> <p>zitiert als: <i>Adrian</i>, Technikentwicklung und Patentrecht, in <i>Josef Kohler und der Schutz des geistigen Eigentums in Europa</i></p>
<p><i>Anderl</i>, Das neue Mediengesetz, <i>ecolex</i> 2005, 701</p>
<p><i>Anderl</i>, Glosse zu 17 Ob 1/07g (Wein & Co), <i>MMR</i> 2007, 497</p>
<p><i>Anderl</i>, Glosse zu EuGH Rs C-278/08 (Bergspechte), <i>ecolex</i> 2010/171 (477)</p>
<p><i>Anduleit</i>, Die Rechtsdurchsetzung im Markenrecht (2001)</p>
<p><i>Barbist</i>, Auskunftspflicht: Streit Provider vs Musikindustrie Reloaded Das EuGH-Urteil in Sachen Promusicae, <i>MR</i> 2007, 415</p>
<p><i>Bergauer</i>, Auskunftspflicht der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, <i>RdW</i> 2005, 467</p>
<p><i>Berger</i>, Die neuen Archivare: Philosophische Implikationen moderner Filesharing-Technologien, in <i>Ferstl/Wedrac</i> (Hg), <i>Owning the Mind Beiträge zur Frage geistigen Eigentums</i> (2010), 37</p> <p>Zitiert als: <i>Berger</i>, Die neuen Archivare, in <i>Owning the Mind</i></p>
<p><i>Berka</i>, RichterInnen als GrundrechtswahrerInnen: Grundrechte und Rechtsprechung der ersten Instanz, <i>RZ</i> 2008, 114</p>
<p><i>Brenn</i>, E-Commerce-Gesetz (ECG) Kurzkommentar (2002)</p> <p>zitiert als: <i>Brenn</i>, ECG</p>
<p><i>Büchele</i>, Glosse zu 17 Ob 3/08b (Bergspechte I), <i>ÖBl</i> 2009/15 (87)</p>
<p><i>Büchele</i>, Glosse zu 4 Ob 34/09t, <i>ÖBl</i> 2010/17, 83</p>
<p><i>Büchele</i>, Glosse zu 4 Ob 41/09x (LSG/Tele2), <i>ÖBl</i> 2010/18, 90</p>
<p><i>Büchele</i>, Glosse zu EuGH Rs C-557/07 (LSG/Tele2), <i>ÖBl-LS</i> 2009/233, 170</p>
<p><i>Burgstaller</i>, Beugestrafen zur Durchsetzung von Zivilurteilen, <i>ÖJZ</i> 2000, 134</p>
<p><i>Burgstaller</i>, Die Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, <i>MR</i> 2004, 405</p>
<p><i>Burgstaller/Minichmayr</i>, E-Commerce-Gesetz Praxiskommentar (2002)</p> <p>zitiert als: <i>Burgstaller/Minichmayr</i>, ECG</p>
<p><i>Chadoian</i>, Stille Nacht, heimliche Macht, <i>juridikum</i> 2008, 130</p>
<p><i>Ciresa</i>, Handbuch der Urteilsveröffentlichung³ (2006)</p>
<p><i>Ciresa</i>, Österreichisches Urheberrecht (13. Lfg 2010)</p>

Zitiert als: <i>Verfasser</i> in Ciresa, Österreichisches Urheberrecht
<i>Ciresa</i> , Urheberrecht aktuell - Wegweiser durch das österreichische Urheber- und Leistungsschutzrecht für die Praxis (1997) zitiert als <i>Ciresa</i> , Urheberrecht aktuell
<i>Dalus</i> , Der Download aus Filesharingbörsen, <i>ecolex</i> 2009, 1066
<i>Daum</i> , EuGH zur Auskunftspflicht von Internetservice Providern, <i>ecolex</i> 2008, 200
<i>Daum</i> , Providerauskunft und Urheberrecht - der Gesetzgeber ist am Zug!, <i>MR</i> 2009, 247
<i>Dichlberger</i> , Markenrechtliche Risiken bei Keyword-Advertising, <i>ecolex</i> 2008, 1032
<i>Dillenz</i> (Hg), Materialien zum österreichischen Urheberrecht (1986)
<i>Dillenz/Gutman</i> , Praxiskommentar zum Urheberrecht; österreichisches Urheberrechtsgesetz und Verwertungsgesellschaftengesetz ² (2004) zitiert als: <i>Dillenz/Gutman</i> , <i>UrhG & VerwGesG</i> ²
<i>Dittrich</i> , Geistiges Eigentum – ein Versuch einer grundlegenden Untersuchung aus österreichischer Sicht, in <i>Dittrich</i> (Hg), Beiträge zum Urheberrecht VIII (2005) 35 zitiert als: <i>Dittrich</i> , Geistiges Eigentum, in Beiträge zum Urheberrecht VIII
<i>Dittrich</i> , Setzt die Vervielfältigung zum eigenen Gebrauch voraus, dass sie mit Hilfe eines rechtmäßig erworbenen und rechtmäßig hergestellten Werkstücks erfolgt?, in <i>Dittrich</i> (Hg), Beiträge zum Urheberrecht VIII (2005) 1 Zitiert als <i>Dittrich</i> , Vervielfältigung zum eigenen Gebrauch, in Beiträge zum Urheberrecht VIII
<i>Dreier</i> , TRIPS und die Durchsetzung von Rechten des geistigen Eigentums, <i>GRUR Int</i> 1996, 205.
<i>Dudenverlag</i> , Duden – Deutsches Universalwörterbuch ⁶ (2007) zitiert als: Duden ⁶ , Wort
DWDS/Berlin-Brandenburgische Akademie der Wissenschaften (Hg), Das Digitale Wörterbuch der deutschen Sprache des 20. Jahrhunderts, <dwds.de> zitiert als: DWDS, Wort
<i>Edthaler/Schmid</i> , Auskunft über IP-Adressen im Strafverfahren, <i>MR</i> 2008, 220
<i>Einzinger/Schubert/Schwabl/Wessely/Zykan</i> , Wer ist 217.204.27.214? Access-Provider im Spannungsfeld zwischen Auskunftsbegehr(lich)keiten der Rechteinhaber und Datenschutz, <i>MR</i> 2005, 113 zitiert als: <i>Einzinger/Schubert/Schwabl/Wessely/Zykan</i> , Wer ist 217.204.27.214?, <i>MR</i> 2005, 113
<i>Fercher</i> , Markenrecht, in <i>Wiebe</i> (Hg), Wettbewerbs- und Immaterialgüterrecht (2010) 77 zitiert als <i>Fercher</i> , Markenrecht, in Wettbewerbs- und Immaterialgüterrecht

<p><i>Fischer/Köck/Karollus</i>, Europarecht⁴ Recht der EU/EG, des Europarates und der wichtigsten anderen europäischen Organisationen (2002)</p> <p>zitiert als: <i>Fischer/Köck/Karollus</i>, Europarecht⁴</p>
<p><i>Fuchs</i>, Die marken- und wettbewerbsrechtliche Zulässigkeit von kontextabhängiger Suchmaschinenwerbung (Keyword Advertising) Zugleich eine Anmerkung zu OGH 20. 3. 2007, 17 Ob 1/07g - Wein & Co, wbl 2007, 414</p> <p>Zitiert als: <i>Fuchs</i>, Zulässigkeit von kontextabhängiger Suchmaschinenwerbung, wbl 2007, 414</p>
<p><i>Fuchs/Ratz</i> (Hg), Wiener Kommentar zur Strafprozessordnung (2009)</p> <p>Zitiert als: <i>Verfasser</i> in <i>Fuchs/Ratz</i>, WK-StPO</p>
<p><i>G. Korn</i>, Glosse zu 3 Ob 261/03h, MR 2005, 95</p>
<p><i>Gamerith</i>, Der vorbeugende Unterlassungsanspruch, ÖBl 2005/13</p>
<p><i>Griss</i>, Haftung für Dritte im Wettbewerbsrecht und im allgemeinen Zivilrecht, JBl 2005, 69</p>
<p><i>Gutman</i>, Abruf im Internet von unbekanntem und offensichtlich urheberrechtlich unrechtmäßigen Werken, MMR 2003, 706</p>
<p><i>Gutman</i>, Urheberrecht im Internet in Österreich, Deutschland und der EU (2003)</p> <p>zitiert als: <i>Gutman</i>, Urheberrecht im Internet</p>
<p><i>Handig</i>, Die Nutzung des World Wide Web aus urheberrechtlicher Sicht Rechtslage nach der UrhG-Nov 2003, ÖBl 2004, 196</p>
<p><i>Handig</i>, Geistiges Eigentum nach dem Vertrag von Lissabon, ecolex 2010, 171</p>
<p><i>Hasberger</i>, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23</p>
<p><i>Hasberger</i>, Glosse zu 4 Ob 66/04f, MR 2004, 274 (277)</p>
<p><i>Hasberger/Semrau-Deutsch</i>, Host –Provider als Richter?, ecolex 2005, 197</p>
<p><i>Heidinger</i>, Keyword-Advertising: Nutzung fremder Kennzeichen als Schlüsselwörter, MR 2010, 119</p>
<p><i>Heidinger</i>, Rechtsdurchsetzung im Immaterialgüterrecht, in Wiebe (Hg), Wettbewerbs- und Immaterialgüterrecht (2010) 163</p> <p>zitiert als: <i>Heidinger</i>, Rechtsdurchsetzung im Immaterialgüterrecht, in Wettbewerbs- und Immaterialgüterrecht</p>
<p>Heise Online, <heise.de></p>
<p><i>Helmreich</i>, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? ecolex 2005, 379</p>
<p><i>Hinterhofer</i>, Aktuelle Entwicklungen im Urheberstrafverfahren, MR 2008, 152</p>
<p><i>Hoeren</i>, Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099</p>

<i>Hofmarcher</i> , Auch Social-Network Profile bieten Platz für Urteilsveröffentlichungen, e-center law survey 12/2010
<i>Höller</i> , Software-Urheberrechtsverletzungen im Konkurs, ecolex 2003, 922.
<i>Horak</i> , Das neue Privatanklageverfahren, ÖJZ 2009/24, 212
<i>Horak</i> , Erste Erfahrungen mit der StPO 2008 in Privatanklageverfahren, ecolex 2008, 211
<i>Horak</i> , StPO-Reform 2008 und Immaterialgüterrecht, ecolex 2007, 949
<i>Hubmann/Götting</i> , Gewerblicher Rechtsschutz ⁶ : Patent-, Gebrauchsmuster-, Geschmacksmuster-, Marken- und Wettbewerbsrecht (1998) zitiert als <i>Hubmann/Götting</i> , Gewerblicher Rechtsschutz ⁶
<i>Hubmann/Rehbinder</i> , Urheber- und Verlagsrecht ⁸ (1995)
<i>Jaeschke</i> , EuGH: Gemeinschaftsrechtskonforme Möglichkeit zum Kauf von den Marken von Mitbewerbern entsprechenden Marken, EuZW 2010, 419
<i>Jänich</i> , Geistiges Eigentum – eine Komplementäerscheinung zum Sacheigentum? (2002) zitiert als <i>Jänich</i> , Geistiges Eigentum
<i>Kahlert</i> , Urheberrecht kontra Datenschutz, ELR 2008, 78
<i>Kamlah</i> , Müssen Access-Provider den Zugang ins Internet filtern?, MR-Int 2005, 97
<i>Kasper</i> , Die privatrechtliche Haftung des Host-Providers in der Judikatur des OGH, jusIT 2009 H 1, 1
<i>Keiler/Bezemek</i> , leg cit (2009)
<i>Kindt</i> , Grundrechtsschutz für Raubkopierer und Musikpiraten? MMR 2009, 147
<i>Klicka</i> , Zum Umfang der Unterlassungsexekution nach § 355 EO - Aktuelle Abgrenzungsfragen zwischen Handlungs- und Unterlassungsexekution bei Beseitigungsansprüchen, wbl 2003, 260 Zitiert als: <i>Klicka</i> , Zum Umfang der Unterlassungsexekution nach § 355 EO, wbl 2003, 260
<i>Knaack/Venor</i> , Gerichtshof der Europäischen Union: Markenrecht und elektronischer Geschäftsverkehr, GRUR Int 2010, 385
<i>Kodek</i> , Die Wahrung von Grundrechten durch die Gerichtsbarkeit. Bilanz – Probleme – Perspektiven, ÖJZ 2008, 216
<i>Kohler</i> , Das Immaterialgüterrecht und seine Gegner (1887)
<i>Korinek/Holoubek</i> (Hg), Österreichisches Bundesverfassungsrecht Bd I bis IV (1999) Zitiert als: <i>Verfasser</i> in <i>Korinek/Holoubek</i> , B-VG
<i>Koziol/Welser</i> , Grundriss des Bürgerlichen Rechts Bd I ¹³ (2006) + II ¹³ (2007) zitiert als: <i>Koziol/Welser</i> , Bürgerliches Recht I ¹³

<i>Kresbach</i> , E-Commerce ² (2003)
<i>Kucsko</i> (Hg), marken.schutz - systematischer kommentar zum markenschutzgesetz (2006) zitiert als: <i>Verfasser</i> in <i>Kucsko</i> , marken.schutz
<i>Kucsko</i> (Hg), urheber.recht - systematischer kommentar zum urheberrechtsgesetz (2008) zitiert als: <i>Verfasser</i> in <i>Kucsko</i> , urheber.recht
<i>Kucsko</i> , Geistiges Eigentum ; Markenrecht, Musterrecht, Patentrecht, Urheberrecht ; [eine Expedition durch den unsichtbaren Dschungel des Immaterialgüterrechts] (2003) zitiert als: <i>Kucsko</i> , Geistiges Eigentum
<i>Laimer/Thiele</i> , Die Privatkopie nach der Urheberrechtsnovelle 2003, ÖBl 2004, 52
<i>Liebwald</i> , The New Data Retention Directive, MR-Int 2006, 49
<i>Liu/Albitz</i> , DNS and BIND ⁵ (2006)
<i>Malhotra</i> , IP Routing (2002)
<i>Marberth-Kubicki</i> , Der Beginn der Internet-Zensur - Zugangssperren durch Access-Provider, NJW 2009, 1792
<i>Neubauer</i> , Zur Haftung und Auskunftspflicht von Providern Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-Int 2008, 25 Zitiert als: <i>Neubauer</i> , Zur Haftung und Auskunftspflicht von Providern, MR-Int 2008, 25
<i>Noha</i> , Glosse zu EuGH Rs C-278/08 (Bergspechte), MR 2010, 177
<i>Noha</i> , Keyword Advertising - Verwendung von Kennzeichen Dritter als Suchwort, ecolex 2007, 616
<i>Otto/Seitlinger</i> , Die "Spitzelrichtlinie" Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227 zitiert als: <i>Otto/Seitlinger</i> , Die "Spitzelrichtlinie", MR 2006, 227
<i>Parschalk</i> , Provider-Haftung für Urheberrechtsverletzungen Dritter, ecolex 1999, 834
<i>Piatek/Kohno/Krishnamurthy</i> , Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice, Department of Computer Science and Engineering, University of Washington; abrufbar unter <dmca.cs.washington.edu/dmca_hotsec08.pdf> zitiert als <i>Piatek/Kohno/Krishnamurthy</i> , Challenges and Directions for Monitoring P2P File Sharing Networks
<i>Pichler</i> , Besondere Kontrollpflicht für Host-Provider, ecolex 2007, 189
<i>Plasser</i> , Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007?, ÖBl 2008/40
<i>Raschhofer</i> , Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in Feiler/Raschhofer (Hg), Innovation und internationale Rechtspraxis Praxisschrift für Wolfgang Zankl (2009) 661

<p>zitiert als: <i>Raschhofer</i>, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access Provider, in PS Zankl</p>
<p><i>Raschhofer/Steinhofer</i>, § 87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig?, <i>ecolex</i> 2010, 716</p>
<p><i>Raschhofer/Steinhofer</i>, Zwischen Urheber und Kunde: Provider in der Zwickmühle, <i>Rechtspanorama</i>, Die Presse 5.10.2009</p>
<p><i>Rechberger/Oberhammer</i>, Exekutionsrecht⁴ (2005)</p>
<p><i>Rechberger/Simotta</i>, Grundriss des österreichischen Zivilprozessrechts⁷ (2009)</p> <p>zitiert als: <i>Rechberger/Simotta</i>, Zivilprozessrecht⁷ Rz</p>
<p><i>Rummel</i> (Hg), Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch³ (2007)</p> <p>zitiert als: <i>Verfasser</i> in Rummel³</p>
<p><i>Schachter</i>, Umsetzung der Enforcement-Directive in Österreich, <i>ecolex</i> 2006, 810</p>
<p><i>Schachter</i>, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz - Anlassfälle Promusicae und MediaSentry, <i>jusIT</i> 2008 H 2, 19</p>
<p><i>Schanda</i>, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, <i>MR</i> 2005, 18</p>
<p><i>Schanda</i>, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, <i>MR</i> 2007, 213</p>
<p><i>Schanda</i>, Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, <i>ecolex</i> 2001, 920</p>
<p><i>Schmidbauer</i>, Die Metamorphose der Auskunftspflicht, <i>MR</i> 2007, 239</p>
<p><i>Schneider</i>, Sperren und Filtern im Internet, <i>MMR</i> 2004, 18</p>
<p><i>Schönherr</i>, Gewerblicher Rechtsschutz und Urheberrecht – Grundriß – Allgemeiner Teil (1982)</p> <p>zitiert als: <i>Schönherr</i>, Gewerblicher Rechtsschutz und Urheberrecht Rz</p>
<p><i>Schönherr</i>, Zur Begriffsbildung im Immaterialgüterrecht, in Brügger (Hg), <i>Homo Creator – Festschrift für Alois Troller</i> (1976) 57</p> <p>zitiert als: <i>Schönherr</i>, Zur Begriffsbildung im Immaterialgüterrecht, in FS Troller</p>
<p><i>Schöttle</i>, Sperrverfügungen im Internet: Machbar und verhältnismäßig? <i>K&R</i> 2007, 366</p>
<p><i>Schubert/Ott</i>, Mehr Fragen als Antworten – die Google France Entscheidung des EuGH zum Keyword Advertising, <i>jusIT</i> 2010/36, 85</p> <p>Zitiert als: <i>Schubert/Ott</i>, Die Google France Entscheidung des EuGH, <i>jusIT</i> 2010/36, 85</p>
<p><i>Schuhmacher</i>, Keyword advertising und eine vorsichtige Neubestimmung der Markenfunktionen, <i>wbl</i> 2010, 273</p>
<p><i>Sieber/Nolde</i>, Sperrverfügungen im Internet: Nationale Rechtsdurchsetzung im globalen Cyberspace? (2008)</p>

Zitiert als: <i>Sieber/Nolde</i> , Sperrverfügungen im Internet
<i>Sofokleous/Mosing</i> , Urheberrechtlicher Auskunftsanspruch gegen Access-Provider: ein "Pyrrhus-Anspruch"?! , ÖBl 2008/55, 268
<i>Spindler</i> , „Die Tür ist auf“ – Europarechtliche Zulässigkeit von Auskunftsansprüchen gegenüber Providern Urteilsanmerkung zu EuGH „Promusicae/Telefónica“, GRUR 2008, 574 zitiert als: <i>Spindler</i> , „Die Tür ist auf“ –Urteilsanmerkung zu EuGH „Promusicae/Telefónica“, GRUR 2008, 574
<i>Spittgerber</i> , Google France und Google – Klärung bei Markenrechtsverletzungen, NJW 2010, 2014
<i>Stadler</i> , EuGH Google verletzt mit AdWords keine Markenrechte, MMR-Aktuell 2010, 301002
<i>Steinhofer/Feiler</i> , Urheberrechtliche Ansprüche auf die Sperrung von Websites durch Access-Provider, MR 2010,322
<i>Stepan</i> , Ökonomie des Urheberrechts Ein Überblick, juridikum 2007, 35
<i>Stomper</i> , Auskunftsansprüche gegen Internet-Provider nach österreichischem Recht, MR-Int 2005, 99
<i>Stomper</i> , Die Folgen der Megasex-Entscheidung -Mitverantwortlichkeit und Auskunftspflicht von Diensteanbietern, RdW 2005, 284 zitiert als: <i>Stomper</i> , Die Folgen der Megasex-Entscheidung, RdW 2005, 284
<i>Stomper</i> , Europäische Union regelt E-Commerce Die EU-Richtlinie über den Elektronischen Geschäftsverkehr im Überblick, SWK 2000, W 59
<i>Stomper</i> , Zur Auskunftspflicht von Internet-Providern, MR 2005, 118
<i>Straube</i> (Hg), Fachwörterbuch zum Handels- und Gesellschaftsrecht (2005) zitiert als: <i>Verfasser</i> , Begriff, in Fachwörterbuch Handelsrecht
<i>Thaler</i> , Immaterialgüterrechte und gewerblicher Rechtsschutz, in Österreichisches Patentamt (Hg), Festschrift 75 Jahre Österreichisches Patentamt 1899 – 1974 (1974) 246 zitiert als: <i>Thaler</i> , Immaterialgüterrechte und gewerblicher Rechtsschutz, in FS 75 Jahre Österreichisches Patentamt
<i>Thiele</i> , Urheberrecht und Erben, in Bogendorfer/Ciresa (Hg) Urheberrecht; Werbung – Telekommunikation – Internet (2009) 51 zitiert als: <i>Thiele</i> , Urheberrecht und Erben, in Urheberrecht
<i>Triffterer/Rosbaud/Hinterhofer</i> , Salzburger Kommentar zum Strafgesetzbuch (22. Lfg 2010) zitiert als: <i>Verfasser</i> in Triffterer/Rosbaud/Hinterhofer, Sbg Kommentar zum StGB
<i>Troller</i> , Immaterialgüterrecht Bd I ² (1959) und Bd II ² (1962), zitiert als: <i>Troller</i> , Immaterialgüterrecht I ²
<i>Walter</i> , Glosse zu 4 Ob 141/07z, MR 2007, 437
<i>Walter</i> , Glosse zu 4 Ob 238/03h, MR 2004, 123

<p><i>Walter</i>, Österreichisches Urheberrecht: Handbuch I. Teil, Materielles Urheberrecht, Leistungsschutzrecht, Urhebervertragsrecht (2008)</p> <p>zitiert als: <i>Walter</i>, Österreichisches Urheberrecht</p>
<p><i>Walter</i>, Schadenersatz, angemessenes Entgelt und Verletzergegnung bei Urheberrechtsverletzungen, MR 1995, 2</p>
<p><i>Walter</i>, Urheberrechtsgesetz – UrhG-Novelle 2003 (2003); zitiert als <i>Walter</i>, UrhGNov 2003</p>
<p><i>Wessely</i>, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, ÖJZ 1999, 491</p>
<p><i>Wiebe</i>, Auskunftspflichtung der Access Provider [-] Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen [-] Gutachten im Auftrag der Internet Service Providers Austria (ISPA), MR 2005, Beilage zu Heft 4, 1</p> <p>zitiert als: <i>Wiebe</i>, Auskunftspflichtung der Access Provider, MR 2005 Beilage H 4, 1</p>
<p>Wikipedia, Die freie Enzyklopädie, <de.wikipedia.org/></p>
<p><i>Wiltschek</i>, UWG - Gesetz gegen den unlauteren Wettbewerb samt Durchführungsverordnungen, Zuständigkeitsvorschriften, Lebensmittelkennzeichnungsverordnung, Nahversorgungsgesetz und einschlägigen EG-Richtlinien ; mit Anmerkungen und Entscheidungen⁷ (2003)</p> <p>zitiert als: <i>Wiltschek</i>, UWG⁷</p>
<p><i>Wukoschitz</i>, Keyword Advertising - "Bergspechte" - nun vom OGH entschieden, ecolex 2010, 972</p>
<p><i>Zankl</i>, Bürgerliches Recht Kurzlehrbuch⁵ (2010); zitiert als <i>Zankl</i>, Bürgerliches Recht⁵</p>
<p><i>Zankl</i>, E-Commerce-Gesetz; Kommentar und Handbuch (2002); zitiert als: <i>Zankl</i>, E-Commerce-Gesetz</p>
<p><i>Zankl</i>, Glosse zu 6 Ob 190/03i (Online-Archiv II), ecolex 2004/319</p>
<p><i>Zankl</i>, Haftung und Haftungsbefreiung im E-Commerce, ecolex 2005, 202</p>
<p><i>Zankl</i>, Online-Archiv: Dritte OGH-Entscheidung zum E-Commerce-Gesetz, ecolex 2004, 524</p>
<p><i>Zankl</i>, Online-Privilegien für Unterlassungsansprüche, ecolex 2004, 361</p>
<p><i>Zankl</i>, Proxy, Cache und Unterlassung, ecolex 2004, 941</p>
<p><i>Zankl</i>, Unterwegs zum Überwachungsstaat, Rechtspanorama, Die Presse 15.5.2007</p> <p>abrufbar unter < diepresse.com/home/recht/rechtallgemein/304039/index.do? ></p>
<p><i>Zerdick</i>, Europäisches Datenschutzrecht – neuere Rechtsprechung des EuGH, RDV 2009, 56</p>
<p><i>Zykan</i>, Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz: OGH 14.7. 2009, 4 Ob 41/09x - Keine Auskunft über die Identität von Inhabern dynamischer IP-Adressen, jusIT 2009 H 6, 206</p> <p>zitiert als: <i>Zykan</i>, Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz, jusIT 2009 H 6, 206</p>

ABSTRACT

Der Titel „Aktuelle Probleme der Durchsetzung von Immaterialgüterrechten im Internet“ umreißt bereits hinreichend klar, worum es in der vorliegenden Arbeit geht. Aufbauend auf Erkenntnissen, die das Immaterialgüterrecht und seine zentralen Regelungsmechanismen teilweise bereits seit mehr als hundert Jahren prägen, liegt der Fokus der Darstellung auf drei sowohl aktuellen wie auch wissenschaftlich ergiebigen Problembereichen an der Schnittstelle von Immaterialgüter- und Internetrecht: rechtsverletzende Websites, rechtsverletzendes Filesharing und rechtsverletzendes Keyword-Advertising. Dabei wird weniger danach gefragt, wann in diesem Zusammenhang eine Verletzung von Immaterialgüterrechten, insbesondere von Urheber- oder Markenrechten, vorliegt, sondern vielmehr, welche Fragen sich bei der Durchsetzung dieser Rechte, also bei Informationsbeschaffung, Unterbindung von Verletzungshandlungen und Genugtuung, für Rechteinhaber stellen.

Während in Teilbereichen bereits deutliche Fortschritte erkennbar sind, zeigt sich dennoch klar, dass die technologischen Neuerungen der Entwicklung des Rechts stark voraneilen. So wurde zB zwar in Europa durch umfangreiche Informationspflichten für Website-Betreiber und subsidiäre Auskunftsansprüche dafür Sorge getragen, dass betroffene Rechteinhaber nachvollziehen können, an wen sie sich bei Rechtsverletzungen auf Websites zu wenden haben. Sofern sich die Website-Betreiber aber außerhalb Europas befinden, sind sie de facto kaum greifbar. Host- und Access-Provider sind daher für Rechteinhaber attraktive Ziele für Unterlassungs- oder Schadenersatzansprüche, weil sie idR einfach ermittelt und geklagt werden können. In der vorliegenden Arbeit wird zunächst die bisherige Rechtsprechung zur Haftung von Host-Providern einer kritischen Würdigung unterzogen, insbesondere was die Frage von Haftungsprivilegien und „besonderen Überwachungspflichten“ angeht. Es zeigt sich dabei, dass manchen Themen in Schrifttum und Judikatur bisher unnötig breiter Raum eingeräumt wurde, während wichtigere Fragen noch offen sind.

So ist etwa die Unterlassungshaftung von Access-Providern aus urheberrechtlicher Perspektive bisher kaum erforscht worden. Bei der Suche nach diesbezüglichen Anspruchsgrundlagen und Bewertungskriterien beschreitet die Arbeit daher weitgehend Neuland. Wie sich zeigt, sind sogenannte „Sperransprüche“, die sich auf die Sperrung des Zugangs zu bestimmten, rechtsverletzenden Websites richten, nach geltendem Recht im Regelfall nicht durchsetzbar. Aufgrund der bloß mittelbar-technischen Rolle des Access-Providers bestehen nämlich grundrechtlich eng determinierte Zumutbarkeitsgrenzen. Ähnliches zeigt sich auch bei derartigen Ansprüchen im Zusammenhang mit Filesharing.

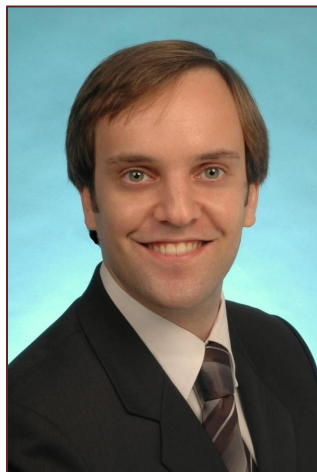
Beim Filesharing-Themenkreis liegt ein weiterer besonderer Fokus auf den datenschutzrechtlichen Implikationen. Hier wird anhand bisher ergangener nationaler und europäischer Rechtsprechung gezeigt, dass der österreichische Gesetzgeber durch ungenaue und wenig

durchdachte Regelungen im Urheberrecht bewirkt hat, dass Zivil- und Strafgerichte bei der Beurteilung des Schutzes von IP-Adressen zu markant unterschiedlichen Ergebnissen kommen. Das führt im Ergebnis dazu, dass de lege lata weder die Durchsetzbarkeit von Urheberrechten noch der Schutz der Privatsphäre von Internetusern ausreichend gewährleistet ist und zudem massive unionsrechtliche Bedenken gegen die derzeitige Rechtslage bestehen. Hier ist der Gesetzgeber gefordert, durch adäquate Regelungen, wie sie in der Arbeit vorgezeichnet werden, Abhilfe zu schaffen.

Im Bereich Genugtuung konzentriert sich die Untersuchung primär auf die Haftungssituation der Internetprovider und zeigt, etwa beim Stichwort Urteilsveröffentlichungen bei Markenverletzungen durch Keyword-Advertising, auch neue Ansatzpunkte für die Weiterentwicklung der bisherigen Rechtsprechung auf. Zum Keyword-Advertising findet sich zudem eine ausführliche Darstellung der bisherigen Judikatur und eine dogmatische Untersuchung, inwieweit die bisherigen Leitlinien sich in österreichisches Recht der Gehilfenhaftung und das E-Commerce-Gesetz einordnen lassen.

Im Ergebnis zeigt sich, dass gerade aufgrund der offenen Regelungstechnik des Immaterialgüterrechts viele Probleme auf Basis des geltenden Rechtsbestandes lösbar sind, wenngleich sich dadurch im Einzelnen schwierige Abwägungsfragen ergeben können. Neben punktuellen Anpassungen der Rechtslage wird in Zukunft aber vor allem die Kooperation von Rechteinhabern und Providern gefragt sein, um die Durchsetzbarkeit von Immaterialgüterrechten im Internet zu gewährleisten, ohne gleichzeitig die Privatsphäre der Nutzer preiszugeben.

LEBENS LAUF



Mag. Stephan Steinhofer

office@stephansteinhofer.at

www.stephansteinhofer.at

BERUF SERFAHRUNG

Seit 1/11	Dorda Brugger Jordis	Wien, Österreich
	<ul style="list-style-type: none">▪ Rechtsanwaltsanwärter im Litigation Team	
7/10-9/10	Alston & Bird LLP	New York City, USA
	<ul style="list-style-type: none">▪ Dreimonatiges Internship in führender US-Wirtschaftskanzlei mit Schwerpunkt Copyright und Trademark Law	
10/09-06/10	Oberlandesgericht Wien	Wien,
	<ul style="list-style-type: none">▪ Rechtspraktikant bei Staatsanwaltschaft Wien, BG Leopoldstadt und Handelsgericht Wien (UWG/UrhG-Abteilung)	
03/09-06/09	Magna International Europe AG	Oberwaltersdorf
	<ul style="list-style-type: none">▪ Legal Intern im Europäischen HQ (Teilzeit)	
09/08	Wolf Theiss Rechtsanwälte GmbH	Wien
	<ul style="list-style-type: none">▪ Summer Internship in der Practice Group IP & IT	
09/07	Small and Medium Entrepreneurs Union	Brüssel, Belgien
	<ul style="list-style-type: none">▪ Projektmanager beim Wirtschaftsbund der EVP (SME Union)	
09/07-12/10	Europäisches Zentrum für E-Commerce & Internetrecht Wien	
	<ul style="list-style-type: none">▪ Wissenschaftlicher Mitarbeiter und ab 6/08 Unternehmenssprecher▪ Veröffentlichungen zu Urheber-, Verfassungs- und IT-Recht	
09/06-06/08	Gruber & Partner Kommunikation GmbH	Wien
	<ul style="list-style-type: none">▪ Konzepte im Kommunikationsbereich	
04/06-09/08	Rechtsanwalt Dr. Johann Gelbmann	Wien
	<ul style="list-style-type: none">▪ Juristischer Mitarbeiter (Teilzeit)	

AUSBILDUNG

Seit 03/09	Universität Wien	Wien
	<ul style="list-style-type: none">▪ Doktoratsstudium der Rechtswissenschaften	
10/05-01/09	Universität Wien	Wien
	<ul style="list-style-type: none">▪ Diplomstudium der Rechtswissenschaften▪ „Best of the Best“ 2008 und 2009▪ Leistungsstipendien 2007, 2008 und 2009	
Seit 10/08t	Universität Wien	Wien
	<ul style="list-style-type: none">▪ Bachelor-Studium der Philosophie	
08/08	Universitäten Innsbruck/Passau/Salzburg	Alpbach, Österreich
	<ul style="list-style-type: none">▪ Hochschulkurs zur Europäischen Integration (Europarecht)	
10/04-05/06	Politische Akademie der ÖVP	Wien
	<ul style="list-style-type: none">▪ Ausbildung zum Diplomierten Seminartrainer (Rhetorik, Führung)	
09/04-05/05	Österreichisches Bundesheer	Eisenstadt, Österreich
	<ul style="list-style-type: none">▪ Grundwehrdienst als Heereskraftfahrer	
09/96-06/04	Gymnasium der Diözese	Eisenstadt
	<ul style="list-style-type: none">▪ Matura 2004 mit Auszeichnung	

PUBLIKATIONEN

Beiträge in Fachzeitschriften und -büchern

- „Urheberrechtliche Ansprüche auf die Sperrung von Websites durch Access-Provider“, Medien und Recht, 2010, 322 (gemeinsam mit Lukas Feiler)
- „§87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig?“, ecolex 2010, 716 (gemeinsam mit Maximilian Raschhofer)
- „Die Stellung des Laien im österreichischen Rechtsleben“, Praxisschrift für Wolfgang Zankl (2009)
- „Zwischen Urheber und Kunde: Provider in der Zwickmühle“, Die Presse, Rechtspanorama 2009/41/05 vom 5.4.2009

Essays

- „Urheberrecht: So gehts weiter“, computerwelt 02/2010
- „E-Voting: Ungute Verfassung?“, Output 04/2009, 19
- „Urheberrecht: Three Strikes Out?“, Output 10/2008, 14

Sonstiges

- Zahlreiche Beiträge für die Studenten-Magazine "Juristl" und "JusReport"
- Broschüren: „AbsolventInnenbroschüre 2011“; „Sozialrecht für Studierende“; „Alles rund ums junge Wohnen“; „Schulrecht für Schülervertreter“
- Interviews für Zeitungen und Online-Medien