Filesharing und Abmahnwesen

Inaugural-Dissertation
zur Erlangung der Doktorwürde
der Hohen Juristischen Fakultät
der Ludwig-Maximilians-Universität zu München

vorgelegt von
Lars-Oliver Eggersdorfer
2021

Referentin: Prof. Dr. Dr. h.c. Annette Kur

Korreferent: Prof. Dr. Matthias Leistner

Tag der mündlichen Prüfung: 26. Oktober 2020

Vorwort

Die vorliegende Arbeit wurde von November 2016 bis Juli 2019 am Max-Planck-Institut für Innovation und Wettbewerb angefertigt. Die rechtlichen und tatsächlichen Entwicklungen bis einschließlich März 2021 wurden berücksichtigt.

Ein eigenständig entwickeltes Thema eines extern Promovierenden stellt für eine Betreuerin stets ein großes Wagnis dar. Besonderer Dank gilt daher meiner Doktormutter Frau Professorin Annette Kur, die sich hierauf eingelassen hat und mir mit Ratschlägen und weiterführenden Hinweisen zur Seite stand.

Herrn Professor Matthias Leistner danke ich für die Anfertigung des Zweitgutachtens sowie die darin enthaltenen Impulse für die Veröffentlichung, Herrn Professor Ansgar Ohly für die Abnahme der mündlichen Prüfung.

Weiterhin bedanke ich mich bei Herrn Professor Clement Petersen und Herrn Rechtsanwalt Pauli Sortti für die Erläuterungen zur Rechtslage in Dänemark bzw. Finnland.

Caterina Schürch verdanke ich den letzten Schliff bei der Setzung der Arbeit in Latex.

Meiner Frau Cora Stuhrmann für alles zu danken, würde den Rahmen des Vorworts sprengen. Ich beschränke mich daher auf Ihren Beitrag zur formalen Fertigstellung und Einreichung.

Ihr und unserer Tochter Mathilda ist die vorliegende Arbeit gewidmet.

Lars Eggersdorfer
München, den 30. Juni 2021

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA andere Auffassung

AcP Archiv für die civilistische Praxis

AEUV Vertrag über die Arbeitsweise der Europäischen Union

AG Amtsgericht

Ausschussdrs. Ausschussdrucksache

AW3P Abmahnwahn-Dreipage

Az. Aktenzeichen

BDSG Bundesdatenschutzgesetz

BeckRS Beck-Rechtsprechung

BEP BitTorrent Enhancement Proposal

Berkeley Tech. L. J. Berkeley Technology Law Journal

BGB Bürgerliches Gesetzbuch

BGH Bundesgerichtshof

BPatG Bundespatentgericht

BTGO Geschäftsordnung des Deutschen Bundestages

BT-Drs. Bundestagsdrucksache

BGBl. Bundesgesetzblatt

BVerfG Bundesverfassungsgericht

BVerfGG Bundesverfassungsgerichtsgesetz

bzw. beziehungsweise

Cato Sup. Ct. Rev. Cato Supreme Court Review

ccTLD Country Code Top-Level Domain

CG-NAT Carrier-grade Network Address Translation

Chap. L. Rev. Chapman Law Review

Colum. J. Asian L. Columbia Journal of Asian Law

CR Computer und Recht

CRi Computer Law Review International

DatenschutzRL 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

d.h. das heißt

DDoS Distributed Denial of Service

DHT Distributed Hash Table

DNS Domain Name System

DPI Deep Packet Inspection

DRM Digital Rights Management

DSRITB Tagungsband Deutsche Stiftung für Recht und Informatik

DS-GVO Datenschutz-Grundverordnung

ECommerceRL Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt

EGMR Europäischer Gerichtshof für Menschenrechte

EnforcementRL Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums

EuGH Europäischer Gerichtshof

EUIPO Amt der Europäischen Union für geistiges Eigentum

EUR Euro

FD-GewRS Fachdienst Gewerblicher Rechtsschutz

Fordham Intell. Prop. Media & Ent. L. J. Fordham Intellectual Property, Media & Entertainment Law Journal

FTP File Transfer Protocol

Geo. L. J. Georgetown Law Review

GG Grundgesetz

GRC Charta der Grundrechte der Europäischen Union

GRUR Gewerblicher Rechtsschutz und Urheberrecht

GRUR Int. GRUR International

GRUR-Prax Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht

GRUR-RS Gewerblicher Rechtsschutz und Urheberrecht, Rechtsprechung

Harv. L.J. & Tech. Harvard Journal of Law & Technology

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IANA Internet Assigned Numbers Authority

ICANN Internet Corporation for Assigned Names and Numbers

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Taskforce

IGGDAW Interessengemeinschaft gegen den Abmahnwahn

IIC International Review of Intellectual Property and Competition Law

IMAP Internet Message Access Protocol

InfoSocRL 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

Iowa L. Rev. Iowa Law Review

IP Internetprotokoll

IP-Adresse Internetprotokolladresse

ISP Internet Service Provider

iVm in Verbindung mit

JA Juristische Arbeitsblätter

J. Marshall J. Info. Tech. & Privacy L. The John Marshall Journal of Information Technology & Privacy Law

JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht

K&R Kommunikation & Recht

LAN Local Area Network

LG Landgericht

MAC Media Access Control

MDR Monatsschrift für Deutsches Recht

Mitt. Mitteilungen der deutschen Patentanwälte

MMR Zeitschrift für IT-Recht und Recht der Digitalisierung

MPAA Motion Picture Association of America

MPI Max-Planck-Institut für Innovation und Wettbewerb

NAT Network Address Translation

NJW Neue Juristische Wochenschrift

NRWE Rechtsprechungsdatenbank Nordrhein-Westfalen

OLG Oberlandesgericht

PEX Peer Exchange

POP3 Post Office Protocol

P2P peer-to-peer

Rechtstheorie Zeitschrift für Logik und Juristische Methodenlehre, Allgemeine Rechts- und Staatslehre, Kommunikations-, Normen- und Handlungstheorie, Soziologie und Philosophie des Rechts

Rechtswissenschaft Zeitschrift für rechtswissenschaftliche Forschung

RIAA Recording Industrie Association of America

RIR Regional Internet Registry

SHA-1 Secure Hash Algorithm 1

SMTP Simple Mail Transfer Protocol

SPI Shallow Packet Inspection

SVR Straßenverkehrsrecht

Syracuse Sci. & Tech. L. Syracuse Journal of Science & Technology Law

TCP Transmission Control Protocol

TKG Telekommunikationsgesetz

TLD Top-Level-Domain

TRIPS Agreement on Trade-Related Aspects of Intellectual Property Rights

UDP User Datagram Protocol

URL Uniform Resource Locator

USPTO United States Patent and Trademark Office

Vgl. Vergleiche

VorratsdatenspeicherungsRL Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher

Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

VPN Virtual Private Network

vzvb Verbraucherzentrale Bundesverband

Wash. U. Global Stud. L. Rev. Washington University Global Studies Law Review

WLAN Wireless Local Area Network

WWW World Wide Web

ZfPW Zeitschrift für die gesamte Privatrechtswissenschaft

ZGE Zeitschrift für Geistiges Eigentum

ZJS Zeitschrift für das Juristische Studium

ZPO Zivilprozessordnung

ZUM Zeitschrift für Urheber- und Medienrecht

2. TMGÄndG Zweitens Gesetz zur Änderung des Telemediengesetzes

3. TMGÄndG Drittes Gesetz zur Änderung des Telemediengesetzes

Einleitung

Keine juristische Arbeit kommt ohne bestimmte Axiome aus, also diejenigen Grundannahmen, auf denen die Arbeit aufbaut, deren Geltung jedoch nicht weiter in Frage gestellt werden.

Diese wären vorliegend:

1. Geistigem Eigentum im Allgemeinen und dem Urheberrecht und den Leistungsschutzrechten im Besonderen wird in einer marktwirtschaftlichen Ordnung grundsätzlich derselbe, durch die Grundrechte gewährte, Schutz zu Teil wie verkörpertem Eigentum und anderen Rechten.

2. Darauf aufbauend hat jeder Inhaber von geistigem Eigentum das Recht, aus diesem den ihm größtmöglichen Profit zu erzielen und muss sich nicht auf eine ihm planwirtschaftlich zugeteilte Quote verweisen lassen.

Der erste Punkt klingt und ist banal, Punkt zwei ist im rechtspolitischen Diskurs aber spätestens seit dem Jahr 2004 keine Selbstverständlichkeit mehr, als der US-amerikanische Juraprofessor *William W. Fisher III* ein alternatives Kompensationssystem für immaterielle Güter erdachte.[1]

Seine Idee verbreitete sich im deutschen Sprachraum unter dem Schlagwort *Kulturflatrate*[2] innerhalb kurzer Zeit und wird nach wie vor – in verschie-

---

[1] *Fisher III*, Promises to keep: Technology, law, and the future of entertainment, Chapter VI, S. 1 - 66.

[2] Siehe zu den verschiedenen Begrifflichkeiten *Amini*, Digitale Kultur zum Pauschaltarif?, S. 27f.

denen Spielarten – rezipiert.[3] Vereinfacht gesagt wird unter Kulturflatrate verstanden, dass die nicht-gewerbsmäßige Weitergabe digital verkörperter Werke schrankenlos erlaubt ist, umgekehrt jedoch hierfür ein Pauschaltarif zu leisten ist, beispielsweise pro Internetanschluss.[4] Warum aber sollte der *status quo* nicht genügen? Handelt es sich bei der Kulturflatrate nur um eine akademische Spielerei? Mitnichten. Aus dem Blick gerät bisweilen, dass eine reale, technische Entwicklung den Anstoß dafür gegeben hat, das Urheberrecht neu zu denken: *filesharing*.[5] Während aber die Urheberrechtswissenschaft sich Zeit nehmen konnte und kann, völlig neue Konzepte zu entwickeln, sah sich die Urheberrechtsindustrie zum sofortigen Handeln gezwungen. Das als Bedrohung empfundene *filesharing* sollte nach ihrem Willen mit den Mitteln des Rechts bezwungen werden. Nach zwei Dekaden und unzählbaren Verfahren gegen die verschiedensten Akteure des *filesharing*-„Ökosystems", fällt eine Begebenheit in Deutschland ins Auge, die weltweit in vielerlei Hinsicht einzigartig ist: das massenhafte Vorgehen gegen die Inhaber von Internetanschlüssen, über die urheberrechtsverletzendes *filesharing* betrieben wurde; ein Vorgehen, das auf Grund zahlreicher Besonderheiten als Abmahnwesen bezeichnet werden kann.

Die zweite Entwicklung die das *filesharing* angestoßen hat, ist also gleichsam die Kehrseite der Idee der Kulturflatrate, denn während diese als rigorose Preisgabe des Urheberrechts zu deuten wäre, so bedeutet das Abmahnwesen seine überschießende Durchsetzung. Das *filesharing* hat also mit der Kulturflatrate und dem Abmahnwesen zwei gesellschaftliche Entwicklungen angestoßen, von denen die erste im Falle ihrer Durchsetzung nicht weniger als eine Revolution des Urheberrechts wäre, die zweite durch ihr – jedenfalls im öffentlichen Diskurs – anrüchiges Bild an dessen Legitimität nagen kann. Welche Zukunft das Urheberrecht im weiteren rechtspolitischen

[3] Konsens scheint zu sein, dass eine Kulturflatrate in tatsächlicher Hinsicht umsetzbar wäre, ihr aber insbesondere gegenwärtig das europäische Sekundärrecht im Weg stünde, siehe *Amini*, Digitale Kultur zum Pauschaltarif?, S. 323ff.; *Spindler*, Rechtsprobleme und wirtschaftliche Vertretbarkeit einer Kulturflatrate, S. 163ff.; *Zwengel*, Kulturflatrates, S. 277; *Jandt*, Kulturflatrate - eine zulässige Gestaltung der Medienverbreitung?, S. 93, 103. Siehe auch *Braun*, Grundeinkommen statt Urheberrecht?, S. 95ff.

[4] *Spindler*, Rechtsprobleme und wirtschaftliche Vertretbarkeit einer Kulturflatrate, S. 29.

[5] *Fisher III*, Promises to keep: Technology, law, and the future of entertainment, Chapter VI, S. 10f., 24.

Diskurs haben wird, hängt nach Auffassung des Verfassers in nicht unerheblichem Maße davon ab, wie bestimmte dogmatische Fragen, die das *filesharing* im bisherigen Ordnungsrahmen aufwirft, beantwortet wurden und werden. Harmonieren die Antworten mit dem Rechtsgefühl der Adressaten, so lässt sich das Urheberrecht (in diesem Punkt) auch in seiner bisherigen Form verteidigen. Lässt sich mit keiner rechtswissenschaftlichen Methode ein ausgewogenes Ergebnis erreichen, so sind die Möglichkeiten *de lege ferenda* auszuloten. Ausgehend von den soeben vorgestellten Prämissen ist aufzuzeigen, dass ein „großer Wurf", eine Revolution wie die Kulturflatrate, schon gar nicht notwendig ist, sondern dass bereits das Drehen an kleinen Stellschrauben ausreichen kann.

Die vorliegende Arbeit möchte also das *filesharing*, und insbesondere die Haftung des Anschlussinhabers, aus technischer, rechtstatsächlicher, rechtsvergleichender und rechtsdogmatischer Perspektive beleuchten. Sie versteht sich damit als Beitrag zum Urheberrecht im Internetzeitalter.

Die Arbeit knüpft dabei an den bisherigen Forschungsstand an, der mittlerweile veraltet ist oder sich spezifischen Teilbereichen dieses Themenkomplexes widmet – was allein dessen dynamischen Entwicklung geschuldet ist. Die Monographien von[6] *Brinkel*, *Wenzl*, *Engelhardt*, *Freiwald* und *Mayer* wurden in den 2000er-Jahren veröffentlicht und haben entsprechend die für die rechtliche Bewertung des *filesharing* maßgeblichen Entwicklungen insbesondere ab 2010 nicht zum Gegenstand. Die Monographie von *Köhler* betrachtet vorrangig die Nutzung eines Internetanschlusses im familiären Kontext, diejenigen von *Schäufele* und *Reinbacher* strafrechtliche Fragen. Die Monographien von *Brüggemann*, *Stein*, *Nietsch*, *Sandor* und *Wick* haben den Auskunftsanspruch zum Gegenstand, allerdings nicht mit Fokus auf das *filesharing*.

An einer Gesamtdarstellung und dogmatischen Bewertung der Rechtsentwicklung bezüglich *filesharing* insbesondere ab 2010 fehlte es bisher, ebenso an einer umfassenden Untersuchung des hieraus entstandenen Abmahnwesens sowie einer hierauf bezogenen Rechtsvergleichung. Ebenso fehlte bislang eine Gesamtdarstellung der relevanten technischen Tatsachenfragen sowie in rechtlicher Hinsicht die Erörterung der möglichen Konzepte *de lege ferenda* sowie der Entwicklungsmöglichkeiten *de lege lata*.

[6] Siehe hierzu jeweils das Literaturverzeichnis.

Die vorliegende Arbeit möchte diese Lücken füllen.

Überblick und Gang der Darstellung

Die Arbeit ist in fünf Teile gegliedert.

1. Im ersten Teil werden die für das juristische Verständnis notwendigen technischen Kenntnisse vermittelt.

2. Im zweiten Teil werden deskriptiv die Entwicklung und der gegenwärtige Stand der Rechtslage im Bezug auf Urheberrechtsverletzungen über *filesharing*-Systeme geschildert, mit besonderem Schwerpunkt auf die Rechtslage den Inhaber des hierzu verwendeten Internetanschlusses betreffend.

3. Im dritten Teil wird erörtert, wie aus der Entwicklung der Rechtslage eine Rechtspraxis entstanden ist, die als Abmahnwesen – ein in diesem Teil entwickelter Begriff – zu bezeichnen ist. Diese Rechtspraxis wird sodann nach hiesiger Anschauung als rechtspolitisch unerwünscht eingestuft und einem internationalen Vergleich unterzogen.

4. Im vierten Teil wird anschließend die gegenwärtige Rechtslage auf ihre rechtsdogmatische Stimmigkeit hin überprüft. Es wird aufgezeigt, dass insbesondere die Rechtsprechung des BGH in vielen Punkten dogmatische Mängel aufweist und die bisher in weiten Teilen noch nicht ausjudizierte, spezifisch mit Blick auf das *filesharing* ergangene Gesetzgebung gesetzgebungstechnisch mangelhaft ist.

5. Nachdem im dritten Teil dargelegt wurde, dass die als Abmahnwesen zu bezeichnende Rechtspraxis rechtspolitisch unerwünscht, und im vierten Teil dargelegt wurde, dass die gegenwärtige Rechtslage dogmatisch mangelhaft ist, werden im fünften und letzten Teil schließlich zu Letzterer Alternativen *de lege ferenda* entwickelt und *de lege lata* Entwicklungsmöglichkeiten der Rechtsprechung aufgezeigt.

§ 1 Technische Vorfragen

I. Zum Begriff *filesharing*

1. Einleitung

filesharing ist in der Informatik – anders als viele andere Begriffe auf diesem Feld – kein eindeutig definierter Begriff, da er von keiner Instanz eine bestimmte inhaltliche Zuschreibung erfahren hat, sondern im Laufe der Entwicklung der Computertechnologie von den damit befassten Personen auf ein breites technisches Sachverhaltsspektrum mit Bezug zur Datenübertragung angewandt wurde.[1] Im weitesten Sinne ist daher unter *filesharing* jede Übermittlung einer Datei oder Bruchteilen davon von einer Partei zu einer anderen Partei über ein beliebiges Medium zu verstehen.

In diesem weitesten Sinne ist er jedoch für die Zwecke dieser Arbeit unbrauchbar. Er ist deshalb in drei Schritten einzugrenzen.

2. Erste Eingrenzung auf das Internet als Übermittlungsmedium

Zunächst lässt sich der Begriff in einer ersten Weise dahingehend einengen, dass die Dateiübermittlung über tragbare Speichermedien wie DVDs, USB-Sticks und dergleichen außer Acht gelassen wird, da kaum mehr ein besonderes öffentliches, rechtswissenschaftliches oder rechtspraktisches Interesse hieran fortbesteht. Stattdessen ist eine Dateiübermittlung für den Zweck dieser Arbeit nurmehr dann von Interesse, wenn Übermittlungsmedium das Internet ist.

Als Internet bezeichnet man den Zusammenschluss elektronisch selbstständ-

[1] *John*, Critical Studies in Media Communication, Nr. 3, Bd. 31, 2014, S. 198, 204.

diger Systeme mittels technisch standardisierter Netzwerkprotokolle.[2]

Elektronisch selbstständig, also autonom, sind alle Systeme, die in ihrer Funktion nicht von einem anderen Element abhängig sind, mithin Endgeräte wie PCs, Smartphones, Tablets etc. sowie dezidierte Server. Ein Server ist zunächst nur ein Programm, das einen Dienst anbietet. Das Gegenstück dazu ist der Client, also ein Programm, das einen Dienst abfragt.[3] Folglich können Endgeräte sowohl Client als auch Server sein.[4] Für das Internet typisch ist aber, dass die Funktionen eines Servers auf eigens hierfür vorgesehene selbstständige Rechner ausgelagert sind, die selbst keine Dienste abrufen. Auf diesen sind die im Internet angebotenen Applikationen und Speicherplätze vorhanden. Solche Server werden als dezidierte Server bezeichnet.[5] Örtlich werden diese meist in „Serverfarmen“ konzentriert.

Netzwerkprotokolle sind ein Unterfall der allgemeinen Kategorie der Kommunikationsprotokolle.[6] Ein Protokoll ist in der Informatik wiederum eine definierte Menge von Regeln, die einen bestimmten Vorgang betreffen. Kommunikationsprotokolle sind also definierte Mengen von Regeln, die Herstellung und Ablauf einer Kommunikation, mithin die Dateiübertragung zwischen zwei oder mehr Parteien betreffen.[7] Diejenigen Netzwerkprotokolle, die den als Internet bezeichneten Zusammenschluss von selbstständigen Systeme bewirken, werden als die Internetprotokollfamilie bezeichnet.[8]

Die Internetprotokollfamilie wird (unter anderem) von der *Internet Engineering Task Force* (IETF) entwickelt[9] und (neben anderem) in den sogenannten *Requests for Comments* (RCF) festgehalten[10].

Plastisch ausgedrückt ermöglicht das Internet also den Nutzern der oben genannten Endgeräte, von dezidierten Servern oder von den Endgeräten anderer Nutzer Applikationen oder Dateien abzufragen, und das unabhängig

---

2 *Internet*, in: Oxford English Dictionary, abrufbar unter http://www.oed.com/view/Entry/248411 - Zugriff am 31.03.2021.

3 *Forouzan*, TCP/IP protocol suite, S. 544.

4 Und bei der für diese Arbeit relevante Form des *filesharing* sind sie das auch, siehe dazu unten Kapitel § 1 I.4.

5 https://de.wikipedia.org/wiki/Server#Dedizierte_Server - Zugriff am 31.03.2021.

6 https://de.wikipedia.org/wiki/Netzwerkprotokoll - Zugriff am 31.03.2021.

7 *Holtkamp*, Einführung in TCP/IP, S. 5; *Forouzan*, TCP/IP protocol suite, S. 7.

8 https://de.wikipedia.org/wiki/Internetprotokollfamilie - Zugriff am 31.03.2021.

9 https://www.ietf.org/about/ - Zugriff am 31.03.2021.

10 https://www.ietf.org/rfc.html - Zugriff am 31.03.2021.

davon, auf welche Art und Weise die Verbindung letztlich physisch hergestellt wird – sei es Kabel, Funk oder Satellit – und durch welches Betriebssystem – sei es Windows, Linux oder MacOS – das Endgerät gesteuert wird.

3. Zweite Eingrenzung auf die unmittelbare Dateiübermittlung von Endnutzer zu Endnutzer

a) Die Strukturierung der Internetprotokolle

Zur Reduzierung von Komplexität werden Protokollfamilien in Schichten organisiert, d.h. einer Schicht werden bestimmte Aufgaben zugewiesen, deren Lösung für die nächsthöhere Schicht bereit gestellt wird, ohne dass sie von dieser selbst nachvollzogen werden muss.[11] Derart geschichtete Protokolle werden als Protokollstapel bezeichnet.[12] Diese Art zu schichten entspricht der allgemeinen Vorgehensweise in der Informatik.[13] Sie ist im sogenannten OSI-Schichtenmodell (bestehend aus sieben Schichten) der *International Organisation for Standardisation* (ISO) in der ISO-Norm 7489 festgehalten.[14] Die Schichtung der Internetprotokollfamilie wird jedoch typischerweise mit dem älteren, vierschichtigen[15] TCP/IP-Referenzmodell beschrieben (dessen Schichten jedoch auf diejenigen des OSI-Modells aufgeteilt bzw. mit diesen in Entsprechung gebracht werden können).[16]

Diese vier Schichten sind (aufsteigend) die Netzzugangs-, die Internetzwerk-, die Transport- und die Anwendungsschicht.[17]

aa) Die Netzzugangsschicht

Die Netzzugangsschicht betrifft die Verbindung eines Endgeräts mit einem lokalen Netzwerk sowie die Koordinierung des Datenpaketstroms mehrerer Endgeräte innerhalb desselben lokalen Netzwerks.[18] Ihr sind keine Protokol-

[11] *Tanenbaum/ Wetherall*, Computer networks, S. 29.
[12] https://bit.ly/2Kk2bNI - Zugriff am 31.03.2021.
[13] *Tanenbaum/ Wetherall*, Computer networks, S. 29.
[14] BT-Drs. 17/12541, S. 10.
[15] Jedenfalls nach RFC 1122; es werden aber auch andere Beschreibungen wie zum Beispiel eine fünfschichtige vorgeschlagen, vgl. Überblick unter https://en.wikipedia.org/wiki/Internet_protocol_suite#Layer_names_and_number_of_layers_in_the_literature - Zugriff am 31.03.2021.
[16] *Forouzan*, TCP/IP protocol suite, S. 28f.
[17] *Severance*, Introduction to Networking, S. 13.
[18] *Severance*, Introduction to Networking, S. 14f.

le der Internetprotokollfamilie zugeordnet. Letztere betreffen erst die Frage, wie verstreute lokale Netzwerke verbunden werden, greifen also erst ab deren als Router bezeichneten[19] Verbindungsgeräten. Als Router kommen für den Heimgebrauch derzeit typischerweise WLAN-Router, zum Beispiel aus der *Fritz!Box*-Serie des Herstellers AVM zum Einsatz. WLAN, also *Wireless Local Area Network*, ist ein mit der IEEE 802.11-Norm bezeichneter Industriestandard für Funknetzwerke.[20] Umgangssprachlich wird hierfür häufig auch der Begriff *WiFi* verwendet.[21] Wer also zum Beispiel in einem Café oder am Flughafen mit seinem Smartphone „über *WiFi* ins Internet geht", stellt tatsächlich (zunächst) eine WLAN-Verbindung zu einem Router her. Die Netzzugangsschicht betrifft diese Verbindung.[22]

Sie stellt also das Bindeglied zwischen den über ihr liegenden Schichten der TCP/IP-Protokollschicht und der unter ihr liegenden physischen Schicht (also der Verbindungshardware[23]) dar. Dies bewerkstelligt sie, indem sie Signale aus der physischen Schicht einkapselt und somit als Pakete vorbereitet.[24] Das Prinzip der Datenkapselung wird dann auf den höheren Schichten fortgetragen, d.h. auf jeder Schicht werden dem Paket als *Header* bezeichnete, schichtbezogene Metainformationen vorangestellt, was letztlich die Auflösung des Pakets am Zielort ermöglicht (*Zwiebelstruktur*).[25] Den eigentlichen Inhalt eines Paktes bezeichnet man als *Payload*.[26] Diese – also den eigentlichen Inhalt – enthält aber erst die Anwendungsschicht bzw. erfolgt deren Zuweisung dort (hierzu sogleich).[27]

Die Verbindungsreichweite von Routern ist relativ betrachtet sehr beschränkt. Zwei sehr weit voneinander entfernte Endgeräte können sich also

---

19 *Forouzan*, TCP/IP protocol suite, S. 25.

20 https://de.wikipedia.org/wiki/IEEE_802.11 - Zugriff am 31.03.2021. Die IEEE ist ein weltweiter Berufsverband von Ingenieuren.

21 Im eigentlichen Sinne handelt es sich hierbei um ein Firmenkonsortium, das Geräte zertifiziert, die dem gerade genannten Industriestandard entsprechen, siehe https://de.wikipedia.org/wiki/Wi-Fi - Zugriff am 31.03.2021.

22 So auch festgehalten in RFC 1122.

23 Da die Verbindungshardware sehr unterschiedlicher Natur sein kann, gehört auch eine entsprechende Vielzahl von Protokollen zur Netzzugangsschicht.

24 *Stalla-Bourdillon/Papadaki/Chown*, 30 CLSR 670, 671 (2014).

25 *Mahlmann/Schindelhauer*, Peer-to-Peer-Netzwerke: Algorithmen und Methoden, S. 13f.

26 https://en.wikipedia.org/wiki/Payload_(computing) - Zugriff am 31.03.2021.

27 *Stalla-Bourdillon/Papadaki/Chown*, 30 CLSR 670, 672 (2014).

nicht zum selben Router verbinden, mithin nicht allein über denselben sogenannten *hop*[28]; die Kommunikation zwischen diesen Endgeräten muss also über zwei oder mehrere Router, mithin über zwei oder mehrere *hops* bewerkstelligt werden.[29] Wenn hier von Routern die Rede ist, so sind regelmäßig nur der Router des Ursprungs- und der des Zielnetzwerkes der oben erwähnten handelsüblichen Natur.[30] Die übrigen Geräte sind auf den Hochleistungsbetrieb der technischen Infrastruktur des Internets abgestimmt. Diese umfasst je nach Entfernung mehrere Ebenen. Ist das Ursprungsnetzwerk zum Beispiel in Deutschland und das Zielnetzwerk in den USA, so wird das Signal zunächst typischerweise über eine Koaxialverbindung[31] über Verteilerstellen in den sogenannten *backbone* (eine Struktur aus Glasfaserleitungen[32]) des *Internet Service Providers* (ISP) geleitet, sodann über sogenannte *Internet Exchange Points* (IXP) in die Leitungen anderer ISP auf dem europäischen Festland weitergegeben[33] und schließlich per Tiefseekabel[34] an eine analog konzipierte Struktur in den USA übergeben.[35] Dabei nimmt das Signal nicht selten bis zu 20 *hops*.[36]

Mit dem Begriff *Internet Service Provider* sind in dieser Arbeit nur solche Anbieter gemeint, die den Zugang zu der gerade genannten technischen Infrastruktur aus terrestrischen Leitungen und/oder Mobilfunknetzwerken bereitstellen, entweder weil diese ihnen selbst gehören oder sie jene zu diesem Zwecke anmieten. Als ISP könnte man auch viele andere Anbieter verstehen, beispielsweise Anbieter von Inhalten oder den Inhaber eines Internetanschlusses, der anderen Personen seinen Anschluss zur Verfügung stellt. Um Begriffsverwirrungen vorzubeugen, wird hiervon in dieser Arbeit jedoch

28 *Forouzan*, TCP/IP protocol suite, S. 31.

29 *Severance*, Introduction to Networking, S. 16.

30 Technisch möglich ist aber auch das Anschließen mehrerer handelsüblicher Router an das Netzwerk eines anderen handelsüblichen Routers, wodurch die angeschlossenen Router nur noch als *Repeater* in einem vergrößerten Netzwerk fungieren. Dieser Zusammenschluss ist eine Idee, auf der die sogenannte Freifunk-Gemeinde basiert, siehe https://freifunk.net/worum-geht-es/technik-der-community-netzwerke/ - Zugriff am 31.03.2021.

31 *Tanenbaum/ Wetherall*, Computer networks, S. 97f.; wobei für diese sogenannte letzte Meile auch immer mehr Glasfaser-Verbindungen verlegt werden.

32 *Tanenbaum/ Wetherall*, Computer networks, S. 100.

33 *Tanenbaum/ Wetherall*, Computer networks, S. 480.

34 Vgl. http://www.submarinecablemap.com - Zugriff am 31.03.2021.

35 *Bleich*, c't, Nr. 7, 2005, S.88-93.

36 *Severance*, Introduction to Networking, S. 16.

Abstand genommen.

Zuletzt darf zudem nicht außer Acht gelassen werden, dass die Verbindung zu einem Router nicht nur mittels des WLAN-Standards hergestellt werden kann, sondern auch kabelgestützt[37] im Rahmen des Ethernet-Standards[38]. Zwar wird für mobile Geräte (Smartphones, Tablets, Laptops) typischerweise eine WLAN-Verbindung verwendet, die kabelgestützte Verbindung ist aber nach wie vor weit verbreitet. Erstens im Heimgebrauch, da WLAN für bestimmte Anwendungen (insbesondere Online-Gaming und Streaming) bisher nicht sonderlich gut oder gegenüber einer kabelgestützten Verbindung weniger gut geeignet ist und zudem mit WLAN noch nicht die volle Bandbreite eines Anschlusses für Downloads und Uploads ausgeschöpft werden kann. Zweitens in gewerblichen Betrieben, da neben den Geschwindigkeitsaspekt dort noch der Sicherheitsaspekt hinzutritt, da in ein rein kabelgebundenes Netzwerk weniger leicht eingedrungen werden kann als in ein funkbasiertes Netzwerk.

bb) Die Internetzwerkschicht

Die Internetzwerkschicht ist nun damit befasst, die verschiedenen Router, die „durchquert“ werden müssen, zu adressieren und die Wegfindung zwischen ihnen zu ermöglichen.[39] Mittels den der Internetzwerkschicht zugeordneten Protokollen kommunizieren die Router untereinander[40] und etablieren dabei, was jeweils die schnellsten Wege zwischen ihnen sind; dies wird als *dynamisches Routing* bezeichnet[41]. Das Resultat der Wegfindung wird auf den Routern in sogenannten *Routing-Tabellen* festgehalten.[42]

Hinsichtlich der Adressierung ist zwischen der physikalischen und der logischen Adressierung zu unterscheiden. Die physikalische Adresse (gemeinhin als *MAC-Adresse* bezeichnet) ist hardwareseitig und damit unveränderbar in einem Gerät (zum Beispiel einem Endgerät oder Router) hinterlegt. Die logische Adresse ist nicht hardware-, sondern protokollseitig. Im Rahmen der

---

37 Siehe https://de.wikipedia.org/wiki/Patchkabel - Zugriff am 31.03.2021.

38 https://de.wikipedia.org/wiki/Ethernet#Kabel - Zugriff am 31.03.2021.

39 *Zisler*, Computer-Netzwerke, S. 184.

40 *Schreiner*, Computer-Netzwerke, S. 77.

41 *Zisler*, Computer-Netzwerke, S. 184.

42 *Mahlmann/Schindelhauer*, Peer-to-Peer-Netzwerke: Algorithmen und Methoden, S. 18.

Internetprotokollfamilie wird also der physikalischen Adresse des Routers – und damit also dem gesamten Netzwerk, das dieser Router repräsentiert[43] – eine logische Adresse „übergestülpt".[44] Die Zuteilung der logischen Adressen an die verschiedenen Netzwerke, die als Internet zusammengeschlossen werden sollen, bedarf einer übergeordneten Instanz, da die Adresse eines jeden Netzwerks zur Vermeidung von Adresskonflikten singulär sein muss.[45] Diese übergeordnete Instanz ist die *Internet Corporation for Assigned Names and Numbers* (ICANN).[46]

In der Internetprotokollfamilie heißt die logische Adresse *Internetprotokoll-Adresse* (IP-Adresse)[47] und ist Gegenstand des für die gesamte Familie namensgebenden[48] *Internetprotokolls* (IP).[49]

Das IP ist aber darüber hinaus auch mit der Datenübertragung befasst.[50] Die Übertragung findet mittels Paketen statt, die auch als Datagramme bezeichnet werden.[51] Jene beinhalten unter anderem die Ziel-IP-Adresse. Die Pakete werden dann von den Routern auf den in den Routing-Tabellen festgehaltenen Wegen solange weitergeleitet (*Packet Forwarding*), bis sie die Zieladresse erreicht haben.[52]

cc) Die Transportschicht

Die Transportschicht erfüllt mehrere Zwecke. Einige dieser Zwecke betreffen die Zuverlässigkeit des Datentransports; denn auf dem Sendungsweg von mehreren Datagrammen, die eigentlich zusammen gehören, können einzelne verloren gehen.[53] Das zur Transportschicht gehörende *Transmission Con-*

---

43 *Kozierok*, The TCP/IP Guide, S. 320.
44 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 85f.
45 *Kozierok*, The TCP/IP Guide, S. 320.
46 Siehe hierzu https://de.wikipedia.org/wiki/Internet_Corporation_for_Assigned_Names_and_Numbers - Zugriff am 31.03.2021.
47 Siehe hierzu genauer Kapitel § 1 IV. 2.
48 Zusammen mit dem TCP, hierzu sogleich.
49 *Kozierok*, The TCP/IP Guide, S. 318.
50 Anders als der Name vermuten lässt, ist also nicht erst die Transportschicht mit der Datenübertragung befasst.
51 *Forouzan*, TCP/IP protocol suite, S. 187.
52 *Mahlmann/Schindelhauer*, Peer-to-Peer-Netzwerke: Algorithmen und Methoden, S. 18.
53 *Severance*, Introduction to Networking, S. 18f.

trol Protocol (TCP) stellt sicher, dass dies nicht passieren kann.[54] Folglich bezeichnet man das TCP als verbindungsorientiertes, das IP als verbindungsloses Protokoll.[55] Es existiert aber auch ein verbindungsloses Protokoll auf Ebene der Transportschicht, das *User Datagram Protocol* (UDP).[56] Dieses hat gegenüber dem TCP wegen seiner Verbindungslosigkeit die damit verbundenen Nachteile, hat aber umgekehrt auch einige Vorteile.[57]

Letztlich ist aber eine weitere Vertiefung der Unterschiede zwischen verbindungsorientierten und verbindungslosen Protokollen für die Zwecke dieser Arbeit nicht relevant. Wichtig ist dagegen eine Gemeinsamkeit von TCP und UDP, nämlich die Funktion der Adressierung eines bestimmten Prozesses mittels *Ports*. Da auf Endgeräten wie PCs und Smartphones mehrere Prozesse gleichzeitig ausgeführt werden können, müssen die auf dem Endgerät eingehenden Datagramme auch an den richtigen Prozess adressiert werden. Während Netzzugangs- und Internetzwerkschicht also nur ermöglichen, dass ein Datagramm das richtige Endgerät erreicht, sorgen die Protokolle der Transportschicht dafür, dass das Datagramm auch den richtigen Prozess auf dem Endgerät erreicht.[58]

Für jeden Prozess gibt es also einen oder mehrere „Kanäle“, die als Ports bezeichnet werden.[59] RFC 6335 bestimmt, dass die Zuweisung von Ports im Rahmen der Funktion der *Internet Assigned Numbers Authority* (IANA)[60] ausgeübt wird. Diese Zuweisung ist online einsehbar.[61] Ports können aber auch ohne Zuweisung inoffiziell verwendet werden.[62]

---

54 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 69ff.

55 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 42f.

56 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 43.

57 *Holtkamp*, Einführung in TCP/IP, S. 40; *Schreiner*, Computer-Netzwerke, S. 113; *Kozierok*, The TCP/IP Guide, S. 945

58 *Forouzan*, TCP/IP protocol suite, S. 26.

59 *Zisler*, Computer-Netzwerke, S. 211.

60 Siehe hierzu https://de.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority - Zugriff am 31.03.2021. Es handelt sich um eine Abteilung der ICANN.

61 https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml - Zugriff am 31.03.2021.

62 Siehe eine Übersicht bei https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports - Zugriff am 31.03.2021.

dd) Die Anwendungsschicht

Wie unter aa) festgehalten wurde, rufen die Protokolle der oberen Schichten die Dienste der unteren Schichten ab und müssen deren Schritte nicht selbst nachvollziehen. Während sich vereinfacht gesagt also die unteren drei Schichten damit befassen, wie Daten von einem Endgerät zu einem anderen Endgerät gebracht werden können und dort zu einem bestimmten Prozess, betrifft die Anwendungsschicht nur noch diesen Prozess selbst, also die Anwendungen im eigentlichen Sinne.

Beispielsweise betreffen die Protokolle *SMTP*, *POP3* und *IMAP* das Versenden, Speichern und Abrufen eindeutig adressierter elektronischer Nachrichten, also den *Email*-Verkehr.[63] Möchte ein Entwickler diese Protokolle für sich nutzbar machen, so ist ihm dies ohne weiteres möglich, da er zwar die Regeln dieser Protokolle programmiertechnisch in einem Anwendungsprogramm implementieren, aber – aufbauend auf den bereits vorhandenen Betriebssystemen – nur noch die Transportschicht ansprechen muss, sich also mit den darunter liegenden Schichten nicht zu befassen braucht. Die dynamische Entwicklung des Internet basiert darauf, dass nicht nur die programmiertechnische Umsetzung der vorhandenen Protokolle für jeden Entwickler möglich ist, sondern diese auch ihre eigenen Protokolle auf Ebene der Anwendungsschicht definieren und umsetzen können.[64]

Bekannte Email-Programme wie *Mozilla Thunderbird* oder *Microsoft Office Outlook* sind also (neben ihren Zusatzfunktionen) programmiertechnische Umsetzungen der die elektronischen Nachrichten betreffenden Protokolle. In der bereits präsentierten Terminologie werden diese Programme als Clients bezeichnet, da sie von Email-Servern Dienste abfragen (Abholen und Versenden von Emails), aber selbst keine anbieten.[65]

Wie oben festgehalten[66], wird auf der Anwendungsschicht dem Paket erst der eigentliche Inhalt, also die Payload hinzugefügt. Auf Ebene der Anwendungsschicht hat ein Paket also einen Header des Anwendungsprotokolls und eine Payload. Auf Ebene der Transportschicht hat das Paket dann einen Hea-

---

63 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 239ff.

64 *Severance*, Introduction to Networking, S. 21.

65 https://de.wikipedia.org/wiki/Client#Clientseitige_Anwendungen - Zugriff am 31.03.2021.

66 Siehe Kapitel § 1 I. 3. a) aa).

der des Transportprotokolls (beispielsweise TCP) und eine Payload, die aus dem Header der Anwendungsschicht und deren Payload besteht. Auf Ebene der Internetzwerkschicht hat ein Paket schließlich einen IP-Header und eine Payload, die aus allen gerade genannten Teilen besteht.[67] Um einer terminologischen Verwirrung vorzubeugen, ist mit der Payload in den weiteren Ausführungen dieser Arbeit nur die Payload der Anwendungsschicht gemeint.

b) Dateiübertragung auf Ebene der Anwendungsschicht

Ausgehend von dem soeben entwickelten Verständnis, existieren verschiedene Möglichkeiten, eine Dateiübertragung von einem Endgerät auf ein anderes Endgerät über das Internet zu realisieren. Wie sie realisiert wird, hängt von demjenigen Protokoll ab, das auf Ebene der Anwendungsschicht verwendet wird. Bekannte Protokolle dieser Art sind zum Beispiel das *File Transfer Protocol* (FTP)[68] oder das besonders für den Abruf von *HTML*-Dateien (die zur Darstellung von Webseiten benutzt werden) verwendete *Hypertext Transfer Protocol* (HTTP)[69] bzw. die verschlüsselte Variante hiervon, das *Hypertext Transfer Protocol Secure* (HTTPS)[70].

Eine Dateiübertragung von Endgerät zu Endgerät kann nun dergestalt vonstattengehen, dass ein Dritter als Intermediär zwischengeschaltet wird. Dies ist ein Server, der Speicherplatz bereitstellt, auf den dann die betroffene Datei vom ersten Endgerät (zum Beispiel mittels HTTP) hochgeladen und vom anderen Endgerät (wiederum mittels HTTP) heruntergeladen wird. In praktischer Hinsicht funktionieren *Sharehosting*-Seiten[71] wie die mittlerweile nicht mehr existenten Seiten *megaupload* oder *Rapidshare* auf diese Weise. Da diesen keine Dateiübertragung *unmittelbar* von Endgerät zu Endgerät zu Grunde liegt, sind sie folglich nur insoweit Gegenstand der Dissertation, als sie einen direkten Bezug zum hier behandelten *filesharing* aufweisen. Gleiches gilt für sogenannte *Streaming*-Seiten[72] wie der nicht mehr existierenden

---

67 http://blog.boson.com/bid/102793/The-Seven-Layers-of-Networking-Part-II - Zugriff am 31.03.2021.

68 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 216ff.

69 *Lienemann/Larisch*, TCP/IP Grundlagen und Praxis, S. 229ff.

70 https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure - Zugriff am 31.03.2021.

71 Siehe hierzu auch Kapitel § 3 IV. 3.

72 Siehe hierzu auch Kapitel § 3 IV. 2.

Seite *kino.to* oder der gegenwärtigen Seite *kinox.to*. Mit Streaming wird das gleichzeitige Empfangen und Abspielen von Video- und/oder Audiodateien bezeichnet.[73] Zwar ist dies auch im Wege des *filesharing* möglich[74]; regelmäßig wird mit dem Begriff Streaming aber der Abruf der genannten Dateien von einem Speicherplatz, der von einem Dritten bereitgestellt wird, ohne dass ein Datenaustausch zwischen Endgeräten stattfindet, assoziiert. Typischerweise verlinken Streaming-Seiten zu Videodateien, die auf Sharehosting-Seiten gespeichert sind.[75] Folglich ist auch das Streaming in diesem Sinne nur insoweit Gegenstand der Dissertation, als es einen direkten Bezug zum hier behandelten *filesharing* aufweist.[76] Das *UseNet* basiert auf der Anwendungsebene zwar nicht auf dem HTTP-Protokoll[77], funktioniert praktisch aber ähnlich wie Sharehosting-Seiten[78], bleibt also ebenfalls weitestgehend außer Betracht.

Der für diese Arbeit verwendete Begriff des *filesharing* ist mithin zumindest auf eine Dateiübertragung *unmittelbar* von einem Endgerät zu einem anderen Endgerät einzugrenzen. Das Kriterium der Unmittelbarkeit ist jedoch noch nicht geeignet, den für diese Arbeit benötigten Begriff ausreichend einzugrenzen. So ist es zum Beispiel möglich, auf einem Endgerät einen FTP-Server einzurichten, d.h. ein Endgerät, das einen FTP-Client aufweist, kann eine Datei unmittelbar von ersterem Endgerät erhalten – ohne den Umweg über einen Intermediär.[79] Zwar liegt in der Terminologie der Informatik hier ein Client-Server-Paradigma vor[80], dies ist jedoch für das Vorhandensein von *filesharing* unschädlich. Stattdessen gehört es zum Wesen des *filesharing*, dass ein solches Paradigma vorhanden ist (hierzu sogleich). Das Vorhandensein eines solchen Paradigmas ist also für das Vorliegen von *filesharing* unschäd-

---

73 *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 28.

74 Siehe hierzu Kapitel § 3 XI. 2. a).

75 *Ibosiola* et al., CoRR, Bd. abs/1804.02679, 2018, S. 1.

76 Ausführlichere Erläuterung der tatsächlichen Ausgestaltung von Sharehosting- und Streamingdiensten bei *Rehbinder*, ZUM 2013, 241, 248ff.

77 https://en.wikipedia.org/wiki/Usenet - Zugriff am 31.03.2021.

78 Mit dem Unterschied, dass im UseNet-System die Betreiber von UseNet-Servern Daten nur für einen bestimmten Zeitraum vorrätig halten, dafür aber ihren Datenbestand untereinander spiegeln, siehe OLG Hamburg, Urteil vom 9. Januar 2014, Az. 5 U 52/10, Rz. 4 – juris.

79 Zur Veranschaulichung siehe beispielsweise https://www.howtogeek.com/140352/how-to-host-an-ftp-server-on-windows-with-filezilla/ - Zugriff am 31.03.2021.

80 *Forouzan*, TCP/IP protocol suite, S. 543.

lich.

4. Dritte und letzte Eingrenzung auf das *peer-to-peer filesharing*

Folglich ist drittens und letztens zur Eingrenzung des für diese Arbeit verwendeten Begriffs des *filesharing* der bisher gefundenen Definition ein *Komfortelement* hinzuzufügen, das das *peer-to-peer filesharing* gegenüber Formen, die nicht als *peer-to-peer* (P2P) zu bezeichnen sind, bietet. Denn die oben aufgezeigte Möglichkeit erfordert nicht nur (für den durchschnittlichen Computeranwender) einigen Aufwand, sondern es ist – dem Dateiaustausch vorgelagert – schon fraglich, wie die beiden Parteien überhaupt für diesen Austausch zusammenfinden sollen. Letztlich wäre eine individuelle Absprache erforderlich. Es ist offensichtlich, dass ein solches Vorgehen kaum praktikabel wäre und ein Datenaustausch über das Internet unmittelbar von Endgerät zu Endgerät jedenfalls als Massenphänomen nicht existieren würde. Dass er als solches *doch* existiert, ist dem P2P zu verdanken.

Wie schon für den Begriff *filesharing*, existiert in der Informatik auch keine allgemein anerkannte Definition des Begriffs P2P.[81] Verbreitet ist beispielsweise die Definition, dass ein P2P-System ein selbstorganisierendes System ist, das – unter Vermeidung zentralisierter Dienste – aus gleichgestellten, autonomen, untereinander verbundenen Einheiten (*peers*) besteht, die ihre vorhandenen Ressourcen untereinander teilen.[82]

Eine solche Definition ist für die Zwecke dieser Arbeit aber nicht brauchbar, da sie Dienste aus dem Begriff P2P ausscheiden würde, die in der Rechtspraxis üblicherweise hiermit assoziiert werden. Beispielsweise wird vereinzelt postuliert, das Kriterium „gleichgestellt“ bedeute, dass im P2P die Einteilung nach Client und Server aufgehoben sei.[83] Dann könnte aber kein gemeinhin als *filesharing*-Dienst bezeichnetes Programm vollständig P2P sein, da auf Ebene der Dateiübertragung ein *peer* Dateien überträgt, ein anderer Dateien empfängt (typischerweise nach modifizierten Regeln des HTTP), mithin also das Client-Server-Paradigma vorliegt.[84] Aus Sichtweise der Informatik könn-

[81] *Saroiu/ Gummadi/ Gribble*, SPIE Proceedings, Bd. 4673, 2002, S. 1.

[82] *Steinmetz/ Wehrle*, Peer-to-Peer Systems and Applications, S. 10.

[83] *Pfitzmann/ Köpsell/ Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 31.

[84] *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 16.

te man dann nur die Zusammenführung der *peers* als P2P bezeichnen, nicht aber die Dateiübertragung. Selbst dies würde aber nicht uneingeschränkt gelten, da alle Dienste für die Zusammenführung eine im Mindestmaß zentralisierte Infrastruktur benötigen – was nach obiger Definition nicht als P2P gilt.[85]

Es zeigt sich daher: für die juristische Betrachtungsweise ist in Bezug auf P2P die Begriffsfindung der Informatik ungeeignet, da sie Elemente, die für erstere begrifflich zusammengehören, voneinander trennt. Folglich erscheint es näherliegend, Dienste, die in ihren *Auswirkungen* im Wesentlichen ähnlich sind, einheitlich als P2P zu bezeichnen, und erst auf nachgelagerter Ebene dort Unterscheidungen zu treffen, wo sich rechtliche Unterschiede ergeben (können).

Für den in dieser Arbeit verwendeten Begriff des P2P soll also – der juristischen Betrachtungsweise geschuldet – nicht das hierunter verstandene technische Paradigma entscheidend sein; vielmehr sind diejenigen technischen Voraussetzungen als P2P zu bezeichnen, die Dateiübertragungen unmittelbar von Endgerät(en) zu Endgerät(en) als Massenphänomen ermöglichen. Diese sind: das effiziente und anwenderfreundliche Zusammenführen derjenigen Personen, die eine bestimmte Datei suchen und eine ebenso effiziente und anwenderfreundliche Gestaltung des Vorgangs der Dateiübertragung, wobei es unschädlich ist, wenn für Ersteres ein gewisses Maß an zentraler Infrastruktur vorhanden ist.

Damit fällt durch die dritte Eingrenzung das *Darknet*, soweit hiermit ein manuell hergestelltes P2P-Netz bezeichnet wird[86], aus dem *filesharing*-Begriff dieser Arbeit heraus, da der Zugang zu diesem sich für den durchschnittlichen Anwender als zu schwierig gestalten dürfte, nicht jedoch sogenannte *Private Börsen*[87], da diese noch ausreichend anwenderfreundlich sind und daher auch hohe Teilnehmerzahlen aufweisen.

---

85 *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 37.

86 https://de.wikipedia.org/wiki/Darknet - Zugriff am 31.03.2021.

87 Siehe hierzu Kapitel § 1 II. 5. c).

5. Abschließende Definition des Begriffs *filesharing*

Abschließend für dieses Kapitel ist *filesharing* mithin als ein Vorgang zu definieren, bei dem eine Dateiübertragung über das Internet unmittelbar von Endgerät(en) zu Endgerät(en) dergestalt stattfindet, dass diejenigen Nutzer, die eine bestimmte Datei abrufen und/oder anbieten möchten, effizient und anwenderfreundlich zusammengeführt werden, insbesondere durch in den für den Datentausch benutzten Programmen integrierte oder auf das *World Wide Web* (WWW) ausgelagerte Suchmechanismen, und die Dateiübertragung ebenfalls effizient und anwenderfreundlich gestaltet ist.

6. Zu den verschiedenen Begrifflichkeiten

In der juristischen Literatur und Rechtsprechung wird zum Teil der Begriff „Tauschbörse“ verwendet. Gemeint ist damit ganz regelmäßig ein *filesharing*-System im Sinne dieser Arbeit. Die Begriffe können also synonym verwendet werden.

II. Unterschiede zwischen verschiedenen *filesharing*-Systemen

1. Einleitung

Wie schon beim Begriff P2P, gibt es auch hinsichtlich der verschiedenen *filesharing*-Systeme informatische Besonderheiten, die für eine abschließende juristische Erörterung nur teilweise von Bedeutung sind. Folglich sollen diese Besonderheiten kurz erläutert, sodann aber ausschließlich Oberbegriffen, die für die juristische Erörterung relevant sind, zugeteilt werden.

Die informatische Einteilung ist insbesondere schon deshalb für eine juristische unbrauchbar, weil über Erstere kein Konsens besteht. Beispielsweise wird eine Einteilung nach Generationen vorgenommen, wobei für die erste Generation unstrukturierte, zentralisierte Systeme wie *Napster*, für die zweite Generation unstrukturierte, dezentralisierte Systeme wie *Gnutella* und für die dritte Generation anonyme Systeme wie *freenet* und strukturierte Systeme wie *Kad* vorgeschlagen werden.[88] Diese Einteilung ist aber in technischer

[88] *Buford/ Yu*, Peer-to-Peer Networking and Applications: Synopsis and Research Directions, S. 3, 10.

Hinsicht zu grobschlächtig und begrifflich auch unpräzise, da die jeweils nachfolgenden Generationen ihre Vorgänger nicht abgelöst haben, sondern Systeme jeden Generationentyps nach wie vor (bei weitem aber nicht in gleichem Maße[89]) benutzt werden.[90]

Eine andere Einteilung differenziert detailliert nach der Art, wie Daten im P2P-Netzwerk aufgefunden werden. Damit ergeben sich als Oberbegriffe „strukturierte“ und „unstrukturierte“ (sowie die hier nicht weiter relevanten hybriden und hierarchischen) Systeme.[91] Unstrukturierte Systeme lassen sich wiederum in zentralisierte, dezentralisierte und hybride Systeme unterteilen.[92] Bei unstrukturierten, dezentralisierten Systemen wiederum kann nach der Art, wie Suchanfragen verarbeitet werden, differenziert werden.[93] Gleiches gilt für strukturierte Systeme. Strukturierte Systeme unterscheiden sich von unstrukturierten dadurch, dass sie – ähnlich der Funktionsweise von Routern auf Ebene der Internetzwerkschicht – Routing-Tabellen über den Speicherort von Daten anlegen und somit die entsprechenden Daten schneller aufgefunden werden können.[94] Die Speicherorte werden in einem sogenannten *Distributed Hash Table* (DHS), also einer verteilten Hashtabelle, festgehalten.[95] Bei unstrukturierten Systemen, bei denen der Speicherort nicht indexiert wird, muss der Speicherort der Datei hingegen jedes mal von neuem aufgefunden werden.

Eine weitergehende, vertiefte technische Differenzierung der verschiedenen Systeme ist allerdings nicht weiter erforderlich. Denn: für die juristische Erörterung reichen für die Einordnung der Funktionsweisen betreffend der Aufgabenstellung, wie derjenige, der eine Datei anfragt und derjenigen/diejenigen, die die Datei anbieten können, zusammengeführt werden, zwei Obergruppen von Funktionsweisen aus, die sich vom bisher technisch Analysiertem abstrahieren lassen. Diese beiden Obergruppen betreffen also die Verbindungsher-

89 Siehe hierzu Kapitel § 1 II. 4. f) und § 3 II.

90 *Buford/ Yu*, Peer-to-Peer Networking and Applications: Synopsis and Research Directions, S. 3, 10.

91 *Buford/ Yu*, Peer-to-Peer Networking and Applications: Synopsis and Research Directions, S. 3, 10.

92 *Danielis*, Peer-to-Peer-Technologie in Teilnehmerzugangsnetzen, S. 23.

93 *Buford/ Yu*, Peer-to-Peer Networking and Applications: Synopsis and Research Directions, S. 3, 12.

94 *Buford/ Yu*, Peer-to-Peer Networking and Applications: Synopsis and Research Directions, S. 3, 13.

95 *Danielis*, Peer-to-Peer-Technologie in Teilnehmerzugangsnetzen, S. 22.

stellung, von denen die eine im Folgenden als zentralisiert, die andere als dezentralisiert bezeichnet wird.

Hinsichtlich der Dateiübertragung, die stattfindet, sobald eine Verbindung zwischen den Parteien der Übertragung hergestellt wurde, kann wiederum unterscheiden werden, nämlich zwischen der zweiseitigen und der mehrseitigen Dateiübertragung.

2. Unterschiede bei der Verbindungsherstellung

Als zentralisiert im Sinne dieser Arbeit sind mithin alle *filesharing*-Systeme zu bezeichnen, bei denen die Verbindungsherstellung zwischen den Parteien einer Vermittlungshandlung gleich welcher Art durch einen Dritten in Form einer zentral erreichbaren Stelle bedarf.

Als dezentralisiert im Sinne dieser Arbeit sind mithin alle *filesharing*-Systeme zu bezeichnen, bei denen es für die Verbindungsherstellung keiner Vermittlungshandlung durch einen Dritten in Form einer zentral erreichbaren Stelle bedarf und daher außer dem Client (also der programmiertechnischen Implementierung eines *filesharing*-Protokolls) keine weiteren Hilfsmittel erforderlich sind.

3. Unterschiede bei der Dateiübertragung

Beide Arten der Dateiübertragung haben gemein, dass die Zieldatei bruchstückhaft, also Stück für Stück übertragen wird. Bei Vorhandensein aller Bruchstücke wird die Zieldatei am Zielort wieder zusammengesetzt.

Als zweiseitig bezeichnet man einen Dateitransfer, bei dem die Zieldatei nur von einer Quelle bezogen wird, also nur von dem Endgerät *eines* anderen Nutzers, der diese anbietet.

Beim mehrseitigen Dateitransfer kann die Datei von mehreren Quellen gleichzeitig bezogen werden.[96] D.h. es werden von den Endgeräten *mehrerer* Nutzer jeweils verschiedene Bruchstücke bezogen.

[96] *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 16.

4. Beispiele für *filesharing*-Systeme

Für diese verschiedenen Funktionsweisen sollen zur Veranschaulichung fünf Beispiele gegeben werden.

a) Napster

Wohl mit das bekannteste *filesharing*-System im Sinne dieser Arbeit, weil das erste dieser Art, ist *Napster*, das im Juni 1999 für die Öffentlichkeit zugänglich wurde.[97] Nutzer hatten nun erstmals die Möglichkeit, ohne größeres Wissen in der Computeranwendung Dateien über das Internet zu tauschen. Außer dem Download und der Installation des Napster-Client waren keine weiteren Schritte nötig. Im Napster-Client konnte dann zum einen ein Dateiordner freigegeben werden, in dem sich die Dateien befinden, die der betreffende Nutzer anderen Nutzern von Napster zur Verfügung stellen wollte, zum anderen über eine Suchmaske nach einer gewünschten Datei gesucht werden. Typischerweise gab man also den Namen eines Songtitels ein, den man suchte, in der Hoffnung, dass andere Nutzer eine Datei freigegeben hatten, die das entsprechende Lied beinhaltete und mit dessen Namen bezeichnet war. War die Suche erfolgreich, konnte das Lied dann in einem zweiseitigen Dateitransfer direkt von dem Endgerät, das der Fundort war, bezogen werden. Die Suchfunktion funktionierte deshalb, weil auf einem zentralen Napster-Server alle Dateien indexiert wurden, die die Nutzer freigegeben hatten. Die Nutzer konnten also eine Datei auch dann auffinden, wenn der betreffende Anbieter gerade nicht online war (wobei der Download natürlich erst dann initiiert werden konnte, wenn er wieder online war).[98]

Nach informatischer Klassifizierung war Napster also ein zentralisierter, unstrukturierter *filesharing*-Dienst und nach der hier verwendeten Klassifizierung ein zentralisierter *filesharing*-Dienst mit zweiseitiger Dateiübertragung.

Die gewählte Form der Zentralisierung war aber auch zugleich seine große Schwachstelle. Denn ohne die Indexierung an einer einzigen Zentralstelle konnte er nicht funktionieren. Folglich hörte er auf zu existieren, als auf rechtliches Vorgehen der Unterhaltungsindustrie hin der Napster-Server im Juli 2001 abgeschaltet wurde.[99]

---

97 *Allen-Robertson*, Digital Culture Industry, S. 44.
98 *Allen-Robertson*, Digital Culture Industry, S. 47.
99 *Tschmuck*, 10 Jahre Napster - Ein Rückblick (Teil 5).

b) Gnutella

Ein anderes Beispiel für ein *filesharing*-System ist das *Gnutella*-Protokoll. Es wurde samt einem quelloffenen Entwurf eines implementierenden Clients im März 2000 im Internet veröffentlicht.[100] Folglich war die Implementierung des Protokolls auch für andere Entwickler im Rahmen eigener Projekte möglich, sodass im August 2000 ein Entwicklerteam den Client *LimeWire* der Öffentlichkeit zur Verfügung stellte. Dieser avancierte schnell zum einem der beliebtesten Clients für *filesharing* überhaupt[101]; seine Verbreitung wurde jedoch 2010 gerichtlich verboten.[102] Ein weiterer bekannter Client, der auf dem Gnutella-Protokoll basierte, war *BearShare*[103], der auch dem gleichlautenden, bedeutenden BGH-Urteil[104] zu Grunde lag.

In der Informatik[105] wird Gnutella gemeinhin als dezentralisiertes *filesharing*-System bezeichnet; dies ist nach der hier gefundenen Definition aber nicht der Fall. Suchanfragen werden in Clients auf Gnutella-Basis von Nutzer zu Nutzer weitergeleitet, bis entweder die Suchanfrage verfällt oder ein Treffer erzielt wird.[106] Um einen Sprung von Nutzer zu Nutzer zu ermöglichen, muss für jeden Sprung aber die IP-Adresse des Ziels bekannt sein. D.h. die Suchanfrage kann nur an einen „bekannten“ Nutzer (die Nutzer des Netzwerkes werden in diesem Zusammenhang als *nodes* bezeichnet) weitergeleitet werden, und auch dieser kann wiederum die Suchanfrage nur an die Nutzer geben, die er kennt. Um also in das Gnutella-Netzwerk initiiert zu werden, bedarf es eines ersten Einstiegspunkts. Diese Art der Initiierung wird als *bootstrapping* bezeichnet.[107] Der Einstiegspunkt ließe sich zum Beispiel manuell durch Absprache herstellen.[108] Ein solches Vorgehen wäre aber höchst unkomfortabel – und folglich auch nicht mehr *filesharing* im Sinne

---

100 *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 1: KaZaA und Grokster.

101 *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 2: LimeWire.

102 Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481 (2010) – h2o.law.harvard.edu.

103 https://de.wikipedia.org/wiki/BearShare - Zugriff am 31.03.2021.

104 Siehe Kapitel § 2 IV. 3.

105 Und auch in der Rechtswissenschaft, siehe zum Beispiel *Heckmann/Paschke* in: Heckmann, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 3.2, Rz. 15.

106 *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 17ff.

107 *Karbhari* et al., Bootstrapping in Gnutella: A Measurement Study, S. 22.

108 *Allen-Robertson*, Digital Culture Industry, S. 68.

dieser Arbeit. Zur Abhilfe existierten für das Gnutella-System daher zentrale „Sammelstellen“ in Form von Servern, die Nutzer indexierten, um so eine möglichst breite Streuung der Suchanfragen zu ermöglichen; ohne diese Server wäre das Gnutella-System in seiner Ausbreitung nicht denkbar gewesen.[109]

Die Dateiübertragung war wie in Napster zweiseitig.

Gnutella war/ist also nach informatischer Klassifizierung ein unstrukturiertes, dezentralisiertes *filesharing*-System und nach der hier verwendeten Klassifizierung ein zentralisierteres *filesharing*-System mit zweiseitiger Dateiübertragung.

c) FastTrack

Gnutella[110] hat/hatte also gegenüber Napster den Vorteil, dass es keiner zentralen Stelle bedurfte, an der alle im Netzwerk vorhandenen Dateien indexiert wurden, sondern lediglich eine Mehrzahl an Sammelstellen, die als Anlaufpunkte dienten, um die Nutzer des Dienstes zusammenzuführen. Jedoch verlangsamte die Datei-Suchmethode, nämlich die Flutung des Netzwerks mit einer Suchanfrage, das System mit seinem Anwachsen erheblich.[111] Auch die zweiseitige Dateiübertragung bildete nach wie vor einen Flaschenhals; schließlich sind die *Upload*-Raten eines handelsüblichen Internetanschlusses erheblich geringer als seine *Download*-Raten. In einer zweiseitigen Dateiübertragung kann also der Empfänger nicht das volle Potential seines Anschlusses ausschöpfen.

Das *FastTrack*-Protokoll stellte demgegenüber eine erhebliche Verbesserung dar. Anders als Gnutella war das FastTrack-Protokoll, und seine zunächst

[109] *Weekly*, Gnutella and the state of P2P.

[110] Zumindest in seiner ursprünglichen Version 0.4; spätere Versionen wie 0.6 und Gnutella2 waren in ihrer Funktionalität stark verbessert.

[111] *Lipowski*, Struktur, Aufbau und Funktionalität des P2P-Netzwerkprotokolls FastTrack, S. 8.

einzige programmiertechnische Implementierung, der *KaZaA*-Client[112], der im März 2001 veröffentlicht wurde[113], jedoch proprietär.[114] Mithin blieb die Anzahl der auf FastTrack basierten Clients gering. Das bekannteste weitere Beispiel für einen FastTrack-Client ist der aus der US-amerikanischen Rechtsprechung bekannte Client *Grokster*.[115]

Die technische Betrachtung ist dadurch erschwert, dass FastTrack und KaZaA proprietär waren und ein *reverse engineering* nur begrenze Einsichten brachte.[116] Die Funktionsweise ist damit nicht restlos geklärt. Offen bleibt insbesondere, ob es zum Zwecke des *bootstrapping* einen zentralen Server gab. In dem australischen Gerichtsverfahren gegen die Entwickler von KaZaA konnte dies nicht bestätigt werden.[117] Der Verdacht liegt daher nahe, dass der Einstieg ins Netzwerk über *supernodes* bewerkstelligt wurde, die mit dem Rechner des Einsteigenden bereits eine Verbindung aufwiesen.[118]

Als *nodes* (auf Deutsch: Knoten) bezeichnet man die einzelnen Rechner der Teilnehmer in Gnutella und FastTrack. Als sogenannte *supernodes* fungierten im FastTrack-System Rechner mit besonders hoher Bandbreite und starker Rechnerleistung.[119] Theoretisch konnte jedem Rechner die Funktion einer *supernode* zugewiesen werden; die meisten Clients waren so eingestellt, dass ein Opt-out erforderlich war.[120] Auf Grund der programmiertechnischen Randomisierung des Auswahlprozesses[121] war jedoch wegen der genannten

[112] Bekannt aus dem Gerichtsverfahren in den Niederlanden, in dem die Entwickler von Urheberrechtsverletzungen freigesprochen wurden, siehe Urteil des obersten Gerichtshofs der Niederlande vom 19. Dezember 2003, AN7253 Case no.: C02/186HR – englische Übersetzung abrufbar unter https://www.muddlawoffices.com/RIAA/cases/Netherlands.pdf - Zugriff am 31.03.2021 ; in Australien hingegen wurden sie vom dortigen obersten Gerichtshof zur Leistung von Schadensersatz verurteilt, siehe Universal Music Australia Pty Ltd et al. v. Sharman License Holdings Ltd et al., [2005] FCA 1242 – jade.io.

[113] *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 1: KaZaA und Grokster.

[114] *Ding/Nutanong/Buyya*, Peer-to-Peer Networks for Content Sharing, S. 28, 56.

[115] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) – supreme.justia.com.

[116] *Ding/Nutanong/Buyya*, Peer-to-Peer Networks for Content Sharing, S. 56.

[117] Universal Music Australia Pty Ltd et al. v. Sharman License Holdings Ltd et al., [2005] FCA 1242, Rz. 195ff – jade.io.

[118] *Strowel*, Peer-to-peer file sharing and secondary liability in copyright law, S. 211.

[119] *Pauly*, Zentrale und dezentrale Peer-to-Peer-Filesharing-Systeme im Vergleich, S. 10.

[120] *Sachs* et al., Securing IM and P2P Applications for the Enterprise, S. 348.

[121] *Sachs* et al., Securing IM and P2P Applications for the Enterprise, S. 335.

Auswahlkriterien nicht verwunderlich, dass viele Universitätsrechner als *supernodes* fungierten.[122]

Supernodes waren jeweils für die ihnen räumlich naheliegenden *nodes* zuständig und dienten ihnen ähnlich wie der Napster-Server dem gesamten Napster-System gedient hatte, indem sie alle auf diesen angebotenen Dateien und diese selbst indexierten.[123] Suchanfragen mussten damit nicht mehr wie in (der ursprünglichen Version von) Gnutella durch das gesamte System geschickt werden, sondern nur noch von *supernode* zu *supernode*; die jeweilige *supernode* konnte die Anfrage dann mit ihrem Index abgleichen.[124]

Mithin ist offensichtlich, dass das FastTrack-Netzwerk ohne *supernodes* nicht funktioniert[125], wie auch das Gnutella-Netzwerk *de facto* nicht ohne Server auskam. In der Informatik wird FastTrack folglich wegen der *supernodes* als unstrukturiertes, hybrides System bezeichnet.[126] Da allerdings zum Funktionieren des Netzwerks stets vermittelnde Dritte (die *supernodes*) erforderlich sind, ist FastTrack nach der hier verwendeten Terminologie hinsichtlich der Verbindungsherstellung als zentralisiertes *filesharing*-System zu bezeichnen.

Bezüglich der Dateiübertragung boten FastTrack-Clients nicht nur die Möglichkeit, abgebrochene Downloads wieder aufzugreifen, sondern auch, sofern die gesuchte Datei von mehreren anderen Nutzern angeboten wurde, diese auch (bzw. verschiedene Teile dieser) gleichzeitig von jenen zu beziehen.[127]

FastTrack war also nach informatischer Klassifizierung ein unstrukturiertes, hybrides *filesharing*-System und nach der hier verwendeten Klassifizierung ein zentralisierteres *filesharing*-System mit mehrseitiger Dateiübertragung.

d) eDonkey

Das *eDonkey*-Protokoll könnte man hinsichtlich seines Modus der Verbindungsherstellung zwischen (dem ursprünglichen) Gnutella und FastTrack

[122] Universal Music Australia Pty Ltd et al. v. Sharman License Holdings Ltd et al., [2005] FCA 1242, Rz. 347 – jade.io.

[123] *Sachs* et al., Securing IM and P2P Applications for the Enterprise, S. 335.

[124] *Allen-Robertson*, Digital Culture Industry, S. 78.

[125] *Hadaller/Regan/Russell*, The Necessity of Supernodes, S. 1.

[126] *Ding/Nutanong/Buyya*, Peer-to-Peer Networks for Content Sharing, S. 28, 55; *Pauly*, Zentrale und dezentrale Peer-to-Peer-Filesharing-Systeme im Vergleich, S. 10

[127] *Lipowski*, Struktur, Aufbau und Funktionalität des P2P-Netzwerkprotokolls FastTrack, S. 21.

einordnen. Wie bei Ersterem sind Server erforderlich, um die Nutzer des Systems zusammen zu führen; darüber hinaus indexieren die Server jedoch auch die Dateien, die die Nutzer jeweils anbieten. Anders als die *supernodes* bei FastTrack müssen die Server allerdings über einen eigenen Client aufgesetzt werden, d.h. von einem von dem für die Nutzung des Systems reguläre verwendeten Client unabhängigen Programm. Folglich kann das System auch beschrieben werden als ein Napster, das statt einem viele verteilte Server verwendet.[128] Grundsätzlich ist es auch jedem regulären Internetnutzer möglich, einen eDonkey-Server aufzusetzen. Dennoch existieren derzeit nur noch einige wenige eDonkey-Server.[129]

eDonkey wird in der Informatik mithin wie FastTrack als unstrukturiertes, hybrides System klassifiziert[130], ist aber nach der hier verwendeten Klassifizierung hinsichtlich der Verbindungsherstellung wiederum als zentralisiertes System einzuordnen.

Eine Besonderheit des eDonkey-Systems, die die Verbindungsherstellung in Bezug auf die gewünschte Datei erleichtert, ist die Verwendung sogenannter *eD2k*-Links. Es handelt sich hierbei um elektronische Verweise ähnlich einem Hyperlink, also einer Abfolge von Buchstaben, Sonderzeichen und Zahlen. Neben eD2k-Links, die auf Server verweisen, gibt es solche, die auf Dateien verweisen. Sie enthalten insbesondere den sogenannten *Hashwert* der entsprechenden Datei.[131] Mittels einer Hash-Funktion lassen sich Dateien beliebiger Größe auf eine Zeichenfolge von bestimmter, einheitlicher Größe abbilden.[132] Der Hashwert identifiziert also eine Datei unabhängig von ihrem Dateinamen.[133]

eD2k-Links können und werden auf Webseiten gelistet und erhöhen dadurch die Funktionalität des eDonkey-Systems enorm, da Nutzer so erstens schneller Server auffinden und ihre Server-Liste im Client erweitern können, zweitens durch die Links auf Dateien ohne den Umweg einer manuellen Suche

[128] *Heckmann* et al., The eDonkey FileSharing Network, S. 2.
[129] Siehe Statistiken zum eDonkey-System auf http://edk.peerates.net – Zugriff am 31.03.2021. Zum Niedergang verschiedener *filesharing*-Systeme siehe Kapitel § 1 II. 4. f).
[130] *Heckmann* et al., The eDonkey FileSharing Network, S. 2.
[131] *Ahmad*, Grundlagen über Peer-to-Peer, S. 11.
[132] *Forouzan*, TCP/IP protocol suite, S. 837.
[133] *Heckmann* et al., The eDonkey FileSharing Network, S. 2.

sofort von den ihnen bekannten Servern abfragen können, ob diese eine Datei mit dem entsprechenden Hashwert gelistet haben. Eine solche Webseite war zum Beispiel Gegenstand der bekannten BGH-Entscheidung den Anspruch auf Netzsperren gegen ISPs betreffend.[134]

Die Dateiübertragung ist beim eDonkey-Protokoll wie bei FastTrack mehrseitig, d.h. eine Datei kann – wenn bei mehreren Nutzern vorhanden – auch von diesen gleichzeitig bezogen werden. Darüber hinaus können aber *chunks* einer Datei bereits wieder anderen Nutzern angeboten werden, noch bevor die Datei vollständig heruntergeladen wurde.[135]

Die bekannteste und beliebteste programmiertechnische Implementierung des eDonkey-Protokolls ist der *eMule*-Client[136], der erstmals im Mai 2002 veröffentlicht wurde.[137]

eDonkey ist also nach informatischer Klassifizierung ein unstrukturiertes, hybrides *filesharing*-System und nach der hier verwendeten Klassifizierung ein zentralisierteres *filesharing*-System mit mehrseitiger Dateiübertragung.

e) Kad

Das *Kad*-Netzwerk ist eine für *filesharing* modifizierte Variante des *Kademlia*-Protokolls, dessen bekannteste Implementierung (wie schon beim eDonkey-Netzwerk) das Programm eMule ist.[138] Es handelt sich hierbei nach informatischer Beschreibung um ein strukturiertes System, da DHT – also eine verteilte Hashtabelle – zum Einsatz kommt. In einem strukturierten System erhalten nicht nur Dateien einen Hashwert, sondern auch die Nutzer des Systems. Diese sind dann für diejenigen Daten verantwortlich, deren Hashwert dem ihren ähnlich ist. Suchanfragen werden von Nutzer zu Nutzer weitergeleitet und dabei möglichst an denjenigen Nutzer, dessen Hashwert dem der gesuchten Datei ähnlich ist. Zum Zwecke der Weiterleitung werden bei den Nutzern jeweils Routing-Tabellen (ähnlich denen im IP[139]) angelegt, in denen die Kontaktinformationen einiger anderer Nutzer (also deren Has-

[134] BGH, Urteil vom 26. November 2015, Az. I ZR 174/14 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.
[135] *Heckmann/Bock*, The eDonkey 2000 protocol, S. 4.
[136] *Heckmann* et al., The eDonkey FileSharing Network, S. 2.
[137] https://en.wikipedia.org/wiki/EMule - Zugriff am 31.03.2021.
[138] *Wang* et al., Attacking the Kad network, S. 1.
[139] Siehe Kapitel § 1 I. 3. a) bb).

hwert) vorrätig gehalten werden. Diese Kontaktinformationen müssen aber erst einmal erhalten werden. Ist der Nutzer bereits in das Kad-Netzwerk initiiert, kann er über den Austausch bereits bekannter Kontakte automatisch neue Kontakte erhalten oder alte aktualisieren.[140]

Wie in anderen Systemen auch, geht die Initiierung in das Netzwerk jedoch nicht ohne Mithilfe vonstatten. Der Austausch mit anderen Kontakten ist erst möglich, wenn solche vorhanden sind. Ein Beispiel für eine solche Mithilfe im Kad-Netzwerk ist eine zentral auf einer Website angebotene, regelmäßig aktualisierte Datei, die einige Kontakte enthält bzw. vermittelt und somit die nötige Multiplikator-Funktion erfüllt, die das Kad-Netzwerk erst zum massentauglichen Phänomen und damit zu *filesharing* im Sinne dieser Arbeit macht.[141] Kad mag also im informatischen Sinne ein strukturiertes System sein; im Sinne dieser Arbeit gilt es als zentralisiert, da es ohne Mithilfehandlungen wie der eben Genannten auf keine ökonomisch relevante Größe anwachsen würde.

Die Dateiübertragung geht beim Kad-Protokoll wie beim eDonkey-Protokoll vonstatten.

Kad ist also nach informatischer Klassifizierung ein strukturiertes *filesharing*-System und nach der hier verwendeten Klassifizierung ein zentralisierteres *filesharing*-System mit mehrseitiger Dateiübertragung.

f) Zusammenfassung

Abgesehen vom Modus der Dateiübertragung, wo eine mehrseitige Dateiübertragung bei gleichzeitiger Einbindung des Downloaders als Weiterverteiler (wie bei eDonkey und Kad) anderen Formen überlegen ist, bestehen bei den verschiedenen Modi der Verbindungsherstellung jeweils Vor-und Nachteile. Je zentralisierter (im informatischen Sinne) ein Netzwerk verwaltet wird, desto leichter lassen sich Suchanfragen beantworten, desto höher ist jedoch auch der Ressourcenaufwand für die zentralen Verwaltungseinheiten. Zudem ist die Ausfallsicherheit des Netzwerks an sich geringer. Je dezentralisierter ein Netzwerk dagegen ist, desto weniger effizient ist die Bearbeitung

[140] *Danielis*, Peer-to-Peer-Technologie in Teilnehmerzugangsnetzen, S. 26ff.

[141] Ein Beispiel für eine solche Webseite ist zum Beispiel http://www.nodes-dat.de - Zugriff am 31.03.2021.

von Suchanfragen.[142] Allen Systemen gemein ist das Problem des sogenannten *free riding*.[143] Hinzu kommen weitere speziellere Vor-und Nachteile eines Systems wie zum Beispiel seine Anfälligkeit für die Flutung mit korrumpierten oder nutzlosen Dateien. Zuletzt treten natürlich die einzelnen Systeme gegeneinander in Konkurrenz um die Aufmerksamkeit potentieller Nutzer.

An Hand dieser Merkmale lassen sich die Entwicklungslinien der *filesharing*-Systeme verstehen:

Napster endete 2001 zwangsweise mit der Schließung des zentralen Servers. Gnutella büßte mit Anwachsen des Netzwerks an Funktionalität ein, weshalb der Datenverkehr in diesem System ab 2002 rapide abnahm. FastTrack dominierte im Hinblick auf die Menge an Datenverkehr bis Mitte 2003.[144] Sein schneller Niedergang ist sicher auch dadurch bedingt, dass Teile der Urheberrechtsindustrie das Netzwerk mit nutzlosen, aber als brauchbar erscheinenden Dateien fluteten und somit für Frustration bei den Nutzern sorgten.[145] Auffällig ist aber, dass das Abnehmen des FastTrack-Datenstroms mit dem Anwachsen des Datenstroms eines (damals) relativ neuen Systems zusammenfällt: *BitTorrent*.[146] Die erste Implementierung des BitTorrent-Protokolls wurde am 2. Juli 2001 veröffentlicht[147] und vom heutigen Standpunkt aus betrachtet lässt sich berechtigterweise sagen, dass der Begriff *filesharing* fast zu einem Synonym für BitTorrent geworden ist. Nach Auskunft eines Analyseunternehmens hatte BitTorrent beispielsweise in einem zweimonatigen Beobachtungszeitraum im Jahr 2007 bereits nahezu einen Anteil von 70 Prozent am gesamten *filesharing*-bezogenen Datenverkehr in Deutschland, wobei das eDonkey-Netzwerk weit abgeschlagen auf Platz 2 lag mit nur knapp 30 Prozent und andere Systeme folglich kaum mehr eine Rolle spielten.[148] In der Analyse für die Jahre 2008 und 2009 setzte sich der Trend fort und BitTorrent baute seinen Vorsprung weiter aus.[149] Nach den Angaben eines anderen Ana-

142 *Danielis*, Peer-to-Peer-Technologie in Teilnehmerzugangsnetzen, S. 32ff.
143 Siehe hierzu Kapitel § 1 II. 5. c).
144 *Steinmetz/ Wehrle*, Peer-to-Peer Systems and Applications, S. 21.
145 *Idris/ Altmann*, A Market-Managed Topology Formation Algorithm for Peer-to-Peer File Sharing Networks, S. 61, 63.
146 *Steinmetz/ Wehrle*, Peer-to-Peer Systems and Applications, S. 21.
147 Siehe die Originalmeldung bei https://groups.yahoo.com/neo/groups/decentralization/conversations/topics/3160 - Zugriff am 31.03.2021.
148 *Schulze/ Mochalski*, ipoque Internet Study 2007, S. 2–4.
149 *Schulze/ Mochalski*, ipoque Internet Study 2008/2009, S. 6.

lyseunternehmens betrug 2011 der Anteil der über das BitTorrent-System ausgesandten Daten fast 60 Prozent an der Gesamtmenge aller von Europa aus ins Internet ausgesandten Daten, der Anteil von eDonkey hieran nicht einmal mehr 2 Prozent.[150] In aktuellen Analysen wird der Anteil von *filesharing*-Systemen am gesamten Datenstrom im Internet abgesehen von BitTorrent gar nicht mehr gesondert ausgewiesen.[151] Andere *filesharing*-Systeme werden also kaum noch benutzt oder sind allenfalls in Nischen relevant.[152]

Wichtig ist dennoch, deren Funktionsweise zu kennen, da erstens somit die Funktionsweise von BitTorrent leichter nachvollzogen werden kann, und zweitens weil sich die Rechtsprechung des BGH zum Teil (jedenfalls implizit) auf die Funktionsweise anderer Systeme bezieht, sich aus der Funktionsweise von BitTorrent jedoch auch für die rechtliche Betrachtung relevante Unterschiede ergeben.[153]

5. Besonderheiten des BitTorrent-Systems

Folglich lohnt eine gesonderte Betrachtung des BitTorrent-Protokolls. Diese wird zwar einerseits dadurch erschwert, dass es nicht *das* BitTorrent-Protokoll gibt, sondern – dank seiner offenen Entwicklung – verschiedene Versionen des Protokolls, wobei die Vielzahl der existierenden Clients auch zum Teil verschiedene Versionen des Protokolls implementiert[154]; andererseits wird die Betrachtung dadurch erleichtert, dass BitTorrent ein Amalgam aus einigen der Prinzipien der bereits erläuterten *filesharing*-Systeme darstellt, mithin auf das hierzu bereits Erörterte aufgebaut werden kann.

---

150 *Sandvine*, Global Internet Phenomena Report Spring 2011, S. 14.

151 Zu den aktuellen Zahlen die BitTorrent-Nutzung betreffend siehe Kapitel § 3 II.

152 Beispielsweise das technisch ähnlich wie eine Mischung aus Napster und FastTrack ausgestaltete *Soulseek*, das noch eine nennenswerte Nutzerbasis aufweist und überwiegend zum Tausch von seltenen Musiktiteln verwendet wird, siehe *Menegus*, Download Utopia: A 17-Year-Old File-Sharing Program Is Still the Best Place to Find Obscure Music; zur Nutzung anonymer Systeme siehe Kapitel § 1 IV. 6. a).

153 Siehe Kapitel § 4 II. 3., 4. und § 4 VIII. 3. d) und § 5 IV. 4. sowie § 5 VII.

154 Einen umfassenden, wenn auch in Teilen veralteten Überblick über das BitTorrent-„Ökosystem“ gibt *Zhang, Chao* et al., Unraveling the BitTorrent Ecosystem, IEEE Transactions on Parallel and Distributed Systems, 22 2011 Nr. 7.

a) Modi der Verbindungsherstellung

aa) .torrent-Dateien und Tracker

In seiner ursprünglichen (und nach wie vor benutzten) Fassung bewerkstelligte BitTorrent die Verbindungsherstellung mittels *.torrent*-Dateien und *Trackern*. Eine .torrent-Datei beinhaltet alle für den Dateitransfer notwendigen Informationen, also insbesondere den Hashwert der Zieldatei und die Adresse eines Trackers. Die .torrent-Datei wird von einem Anbieter, regelmäßig einer Webseite, bezogen. Webseiten dieser Art werden fortan als *Indexseiten* bezeichnet. Die Anbieter solcher Indexseiten (darunter beispielsweise die bekannteste Indexseite *The Pirate Bay*) stellen die .torrent-Dateien regelmäßig nicht selbst zur Verfügung. Stattdessen werden sie von Nutzern hochgeladen, die Webseite katalogisiert diese dann (in der Regel automatisch), sodass sie über eine Suchmaske aufgefunden werden können.[155]

Eine .torrent-Datei wird mit einem Client, der das BitTorrent-Protokoll implementiert, geöffnet, woraufhin der Client eine Verbindung zu dem oder den in der Datei benannten Tracker(n) vornimmt. Als Tracker bezeichnet man eine Registrierungsstelle, die regelmäßig als Modul eines Servers implementiert ist. Der Tracker führt alle Nutzer, die eine Datei mit demselben Hashwert nachfragen, zusammen. Die Nutzer übermitteln hierzu dem Tracker ihre IP-Adressen und den Status ihres Downloads.

Der Tracker verbindet dann die Nutzer randomisiert mit anderen Nutzern untereinander.[156] Es wird dabei regelmäßig eine Verbindung zu etwa 50 anderen Nutzern aufgebaut.[157] Die maximale Anzahl an Verbindungen kann in Clients typischerweise manuell definiert werden, ist aber standardmäßig auf 50 eingestellt.[158] Clients achten regelmäßig darauf, dass die Zahl der Verbindungen nicht unter 20 fällt; geschieht dies doch, werden neue Verbindungen angefragt.[159] Die Menge an bestehenden Verbindungen wird als *peer*

---

155 Vgl. EuGH, Urteil vom 14. Juni 2016, Rs. C-610/15, Rz. 10 – ECLI:EU:C:2017:456 - „The Pirate Bay“.

156 *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 37f.

157 *Xu*, CoRR, Bd. abs/1311.1195, 2013, S. 1, 3; *Izal* et al., Dissecting BitTorrent: Five Months in a Torrent's Lifetime, S. 1, 2.

158 http://blog.libtorrent.org/2012/12/swarm-connectivity/ - Zugriff am 31.03.2021.

159 *Legout/Urvoy-Keller/Michiardi*, Rarest First and Choke Algorithms Are Enough, S. 213, 215.

set bezeichnet.[160]

Tracker werden zum Teil von Indexseiten betrieben, viele Indexseiten bieten aber keinen Tracker (mehr) an. Beispielsweise schaltete die Indexseite *The Pirate Bay* ihren Tracker im Jahr 2009 ab.[161] Es ist aber auch ohne weiteres möglich, einen von einer Indexseite unabhängigen Tracker aufzusetzen[162], der dann aber wiederum – sofern öffentlich[163] – von den Indexseiten in ihren .torrent-Dateien referenziert werden kann.

Soweit zur ursprünglichen Funktionsweise des BitTorrent-Systems. Das BitTorrent-Protokoll wird jedoch zusammen mit einem Referenz-Client[164] ständig fortentwickelt. Die Entwicklungen des Protokolls werden von der Firma *Rainberry*, die früher *BitTorrent Inc.* hieß und auf Grund eines Besitzerwechsels umbenannt wurde[165], auf der Webseite *www.bittorrent.org* in sogenannten *BitTorrent Enhancement Proposals* (BEP), also ähnlich den RFCs der IETF, festgehalten.[166] Insbesondere kamen drei neue Modi der Verbindungsherstellung hinzu, nämlich DHT/Verteilte Hashtabelle (BEP 5), *magnet links* (BEP 9) und *peer exchange*/PEX (BEP 11).

bb) DHT

Die Funktionsweise einer verteilten Hashtabelle wurde bereits im Rahmen der Darstellung des Kad-Netzwerkes erklärt.[167] Im BitTorrent-System existieren zwei verschiedene, miteinander inkompatible DHTs; zum einen die ursprünglich im Referenz-Client implementierte *Mainline DHT*, zum anderen die im konkurrierenden Client *Vuze* implementierte *Azureus DHT*[168], wobei jedoch Letztere bei Vergleich der Nutzerzahlen relativ unbedeutend

[160] *Legout/Urvoy-Keller/Michiardi*, Rarest First and Choke Algorithms Are Enough, S. 213, 214.

[161] *Maxwell*, The Pirate Bay Tracker Shuts Down for Good.

[162] Siehe als Beispiel *Maxwell*, Running a Torrent Tracker For Fun Can Be a Headache.

[163] Zu privaten Trackern siehe Kapitel § 1 II. 5. c).

[164] Früher *BitTorrent Mainline*, heute *uTorrent*; BitTorrent Mainline wurde zunächst quelloffen entwickelt, der Quellcode von uTorrent ist jedoch proprietär. Siehe zum Ganzen https://en.wikipedia.org/wiki/MTorrent#Ownership_change - Zugriff am 31.03.2021.

[165] *Van Der Sar*, BitTorrent Is Reportedly Selling for $ 140 Million (Update).

[166] http://www.bittorrent.org/beps/bep_0001.html - Zugriff am 31.03.2021.

[167] Siehe Kapitel § 1 II. 4. e).

[168] *Jünemann*, Confidential Data-Outsourcing and Self-Optimizing P2P-Networks: Coping with the Challenges of Multi-Party Systems, S. 85.

ist[169]. Zum *bootstrapping* muss wie auch im Kad-Netzwerk auf einen externen Mechanismus zurückgegriffen werden. Für das Mainline DHT stellt beispielsweise Rainberry selbst einen solchen unter *router.bittorrent.com* zur Verfügung. Im Rahmen der DHT wird ein Tracker nicht benötigt, da die Verbindungsherstellung bereits durch das strukturierte Overlay ermöglicht wird; mithin fungiert jeder Nutzer in der Hashtabelle als Tracker.[170] Für die Suche einer Datei muss lediglich deren Hashwert (hierzu sogleich) in der Hashtabelle „weitergereicht" werden. Da zum *bootstrapping* aber externe Hilfe erforderlich ist, sind im Rahmen dieser Arbeit auch die verteilten Hashtabellen des BitTorrent-Systems als zentralisierte Modi der Verbindungsherstellung zu bezeichnen.

Im Vergleich der Nutzerzahlungen zwischen Trackern einerseits und DHT andererseits wurde in einer Untersuchung mit dem Untersuchungszeitraum 2010 ermittelt, dass 40 Prozent der BitTorrent-Nutzer – zumindest im untersuchten Schwarm[171] – exklusiv DHT verwenden.[172]

cc) *magnet links*

Magnet links sind Zeichenfolgen ähnlich wie eD2k-Links.[173] Ein *magnet link* kann dieselben Informationen enthalten wie eine .torrent-Datei[174], d.h. den Hashwert der Zieldatei und, sofern ein Tracker benutzt werden soll, dessen IP-Adresse. Folglich wird der Umweg über den Download einer .torrent-Datei gespart. *magnet links* sind auf Grund ihres im Vergleich zu solchen Dateien verschwindend geringen Speicherbedarfs außerordentlich beliebt. *The Pirate Bay* stieg im Jahr 2012 beispielsweise vollständig auf *magnet links* um, wodurch ihr gesamtes Archiv nur noch 90 MB umfasste; dies gab ihr im internationalen „Katz-und-Maus-Spiel" mit der Urheberrechtsindustrie den entscheidenden Vorsprung, da ein „Serverumzug" nun ohne größeren Aufwand möglich wurde.[175] In der Rechtsprechung tauchen *magnet links* beispiels-

[169] *Wang/Kangasharju*, Measuring large-scale distributed systems: case of BitTorrent Mainline DHT, S. 1, 2.
[170] http://www.bittorrent.org/beps/bep_0005.html - Zugriff am 31.03.2021.
[171] Siehe zu diesem Begriff Kapitel § 1 II. 5. a) ee).
[172] *Varvello/Steiner*, Traffic Localization for DHT-Based BitTorrent Networks, S. 40, 51f.
[173] Siehe hierzu Kapitel § 1 II. 4. d).
[174] http://www.bittorrent.org/beps/bep_0009.html - Zugriff am 31.03.2021.
[175] https://bit.ly/2M2OOE0 - Zugriff am 31.03.2021.

weise im Urteil des EuGH die Netzsperre eben diese Indexseite betreffend auf.[176]

dd) PEX

Die Nutzer von Clients, die PEX implementiert haben, können – einmal verbunden, beispielsweise durch einen Tracker – Kontaktinformationen anderer Nutzer, die dem Gegenüber der Verbindung noch unbekannt sind, untereinander austauschen. Dies dient vor allem dazu, die Arbeitslast eines Trackers zu reduzieren, da ihm dessen Hauptaufgabe, die Nutzer untereinander zu verbinden, nun teilsweise von diesen abgenommen werden kann. Zum Zwecke des *bootstrapping* bleibt der Tracker aber notwendig.[177]

ee) Zusammenfassung

Tracker, DHT und PEX sind untereinander kompatibel.[178] Lädt also ein Nutzer beispielsweise einen *magnet link*, der einen Verweis auf einen Tracker enthält, in seinem BitTorrent-Client[179], so tauscht dieser über die durch Tracker vermittelten Kontakte per PEX Kontaktinformationen über andere Nutzer aus, während er zugleich über die DHT ebenfalls nach Nutzern suchen kann, die als Quelle für die Zieldatei in Frage kommen.

Alle Nutzer, die sich in Bezug auf eine bestimmte Datei verbinden möchten, werden in der BitTorrent-Terminologie unabhängig davon, auf welche der oben genannten Weisen sie verbunden wurden, als *swarm*, also *Schwarm* bezeichnet.[180] Auf Grund der mengenmäßigen Begrenzung dahingehend, mit wie vielen anderen Nutzern man gleichzeitig verbunden sein kann, also das *peer set*, könnte man als Schwarm auch alle Nutzer bezeichnen, die in Bezug auf eine bestimmte Datei in einem *peer set* angeordnet werden möchten, mithin alle koordinierten *peer sets*[181] plus gegebenenfalls Nutzer aus der DHT.

---

176 EuGH, Urteil vom 14. Juni 2017, Rs. C-610/15, Rz. 11 – ECLI:EU:C:2017:456 - „The Pirate Bay“.

177 *Wu* et al., Understanding Peer Exchange in BitTorrent Systems, S. 1.

178 *Van Der Sar*, BitTorrent's Future? DHT, PEX and Magner Links Explained.

179 Der eine entsprechende Kompatibilität vorsehen muss.

180 *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 311, 313.

181 *Legout/Urvoy-Keller/Michiardi*, Rarest First and Choke Algorithms Are Enough, S. 213, 215.

Ein Schwarm kann also beispielsweise die Form annehmen, dass mehrere Tracker zur selben Zeit Nutzer in Bezug auf eine Zieldatei koordinieren und auch zwei Nutzer, die nicht denselben Tracker ansteuern, über die DHT oder PEX dennoch miteinander verbunden werden. Schwärme können somit bisweilen zu beachtlicher Größe anwachsen, ohne dass dies jedoch bedeutet dass alle Nutzer sich untereinander verbinden oder gar an der Dateiübertragung beteiligt sind.[182] Die Größe eines Schwarms lässt sich auf Grund der soeben dargestellten möglichen Schwarmstruktur sowie dem ständigen Bei-und Austritt von Nutzern nur grob schätzen.[183]

b) Modus der Dateiübertragung

BitTorrent greift – wie beispielsweise auch eDonkey[184] – auf die eindeutige Identifizierung von Dateien mittels eines Hashalgorithmus zurück. Zu tauschende Dateien erhalten also einen individuellen Hashwert. In BitTorrent kommt der *Secure Hash Algorithm 1* (SHA-1) zum Einsatz[185], der einen 160 Zeichen langen Binärcode generiert, der aber regelmäßig in Hexadezimalen wiedergegeben wird, also einer Kette aus 40 Zeichen.[186]

BitTorrent „zerteilt" eine zu tauschende Datei in jeweils 256 KB große *pieces*, die wiederum in 16 KB große Untereinheiten, *chunks* genannt, „zerteilt" werden. Beginnt ein Nutzer den Download der Zieldatei, lädt er zunächst alle *chunks* eines *pieces* herunter. *chunks* und *pieces* können auch als Dateifragmente bezeichnet werden. Der Client berechnet nach erfolgter Zusammensetzung von *chunks* zu einem *piece* aus dem *piece* einen Hashwert, also einen Teilwert des Hashwerts der Gesamtdatei. Dieser wird mit dem Hashwert, der in der .torrent-Datei oder dem *magnet link* enthalten war, abgeglichen. Wurden alle *pieces* heruntergeladen, ergibt der Abgleich, dass beide Werte identisch sind. Der Client stellt den Download dann ein.[187]

Die Dateiübertragung bei BitTorrent ist mehrseitig. Mit Erhalt des ersten *chunks* kann ein Nutzer bereits an anfragende andere Nutzer Kopien des-

[182] Siehe hierzu sogleich Kapitel § 1 II. 5. b).
[183] *Lareida/Hoßfeld/Stiller*, The BitTorrent Peer Collector Problem, S. 449.
[184] Siehe Kapitel § 1 II. 4. d).
[185] Ein Umstieg auf eine aktuellere Version ist jedoch geplant, siehe https://www.quora.com/Does-bittorrent-support-SHA-2-256-512-or-future-SHA-3 - Zugriff am 31.03.2021.
[186] https://en.wikipedia.org/wiki/SHA-1 - Zugriff am 31.03.2021.
[187] *Xu*, CoRR, Bd. abs/1311.1195, 2013, S. 1, 4.

selben an diese senden.[188] Solange dieser Nutzer selber noch herunterlädt, wird er in der BitTorrent-Terminologie als *leecher* bezeichnet.[189] Hat er die Datei vollständig heruntergeladen, kann er sie aus der Liste seines Clients entfernen oder den Client beenden, wodurch er das Hochladen von *chunks* an andere Nutzer stoppt. Tut er dies nicht, wird er als *seeder* bezeichnet.[190] Damit es aber überhaupt *leecher* und *seeder* geben kann, muss die Zieldatei ursprünglich bei einer Person vollständig vorhanden gewesen sein. Diese Person nennt man *initial seeder* oder *first seeder*.[191]

Im Rahmen der Dateiübertragung ist von der Zahl der bloßen Verbindungen[192] die Zahl der Upload-Verbindungen zu unterscheiden. Der Nutzer lädt, egal ob er *leecher* oder *seeder* ist, nicht zeitgleich an alle anderen Nutzer hoch, mit denen er verbunden ist. Tatsächlich ist letztere Zahl deutlich niedriger als erstere. Überhaupt lädt ein Nutzer an andere Nutzer nur hoch, soweit er eine Anfrage nach einem *chunk* erhält und dieser Anfrage auch entsprechen kann.[193] Zunächst sind alle Verbindungen *choked*, also „abgewürgt"; erst wenn eine Verbindung *unchoked* wird, werden Daten übertragen. Vom Erfinder des BitTorrent-Protokolls, *Bram Cohen*, wird empfohlen, maximal vier *unchoked*-Verbindungen zuzulassen.[194] Dieser Wert wird auch in anderen Publikationen neueren Datums genannt.[195] Er ist in BitTorrent-Clients folglich standardmäßig voreingestellt; er lässt sich zwar in einigen Clients manuell verändern[196], was allerdings nicht empfohlen wird. Es daher davon auszugehen, dass die allermeisten Nutzer nie an mehr als vier Personen

[188] https://www.techworm.net/2017/03/seeds-peers-leechers-torrents-language.html - Zugriff am 31.03.2021.

[189] *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 311, 313.

[190] *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 311, 313.

[191] *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 311, 313. Zudem muss eine Person, die nicht notwendigerweise mit dem *initial seeder* identisch ist, für die Zieldatei eine .torrent-Datei oder einen *magnet link* erstellt und diesen im Internet zugänglich gemacht haben. Erst dann kann sich um die Zieldatei ein Schwarm bilden.

[192] Typischerweise um die 50, siehe Kapitel § 1 II. 5. a).

[193] Zu den zu Grunde liegenden technischen Vorgängen siehe *Straube*, Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, S. 44ff.

[194] *Cohen*, Incentives Build Robustness in BitTorrent, S. 4.

[195] Beispielsweise *Xu*, CoRR, Bd. abs/1311.1195, 2013, S. 1, 4.

[196] Siehe beispielsweise http://dev.deluge-torrent.org/wiki/UserGuide/BandwidthTweaking - Zugriff am 31.03.2021.

gleichzeitig hochladen.[197] Jedoch werden diese Vier regelmäßig neu evaluiert: alle zehn Sekunden werden drei neue *unchoke*-Verbindungen bestimmt, alle 30 Sekunden eine neue sogenannte *optimistic unchoke*-Verbindung. Die Wahl der *unchoke*-Verbindungen fällt auf diejenigen Nutzer, die dem Anfragenden die höchste Download-Geschwindigkeit zur Verfügung gestellt haben; die der neuen *optimistic unchoke*-Verbindung wird nach dem Zufallsprinzip getroffen.[198] Bleibt die angebotene Downloadgeschwindigkeit konstant, ändern sich also die drei Nutzer, an die im Rahmen der *unchoke*-Verbindungen hochgeladen wird, nicht. Da sich die Uploadraten einer Internetverbindung auch dynamisch ändern können, ist jedoch mit einem gelegentlichen Austausch der Empfänger von *chunks* im Rahmen der *unchoke*-Verbindungen zu rechnen.[199] Zudem werden regelmäßig nicht lediglich drei Nutzer alle aus Sicht des hochladenden Nutzers benötigten *chunks* haben. Dann kommen sie nicht mehr als Bezugsquelle und mithin auch nicht mehr als Empfänger in Frage. Auch dann findet ein Wechsel der Empfänger statt.

Der Nutzerwechsel wiederum ist aber auf die im *peer set* vorhandenen Nutzer beschränkt[200], kann jedoch gegebenenfalls auf Nutzer in der DHT erweitert werden.

Auf Basis des Vorausgesagten lässt sich also – von außen beobachtet – nicht mit Sicherheit sagen, an wie viele andere Nutzer im Falle der Teilnahme an einem Schwarm *chunks* hochgeladen werden. Es kommt primär auf die Beständigkeit des *peer sets*, die Größe des Schwarms und die Dauer der Teilnahme am Schwarm sowie gegebenenfalls auf Querverbindungen über die DHT an.[201] Jedenfalls aber lassen sich damit zu hoch gegriffene Schätzungen als haltlos zurückweisen. Behauptungen wie, dass ein Zugänglichmachen an ein Millionenpublikum stattfinden würde[202], ist angesichts der Tatsache, dass nur an den Bruchteil der Teilnehmer eines Schwarms überhaupt hochgeladen

197 *Laoutaris/Carra/Michiardi*, Uplink Allocation Beyond Choke/Unchoke: Or How to Divide and Conquer Best, S. 1.

198 *Oechsner* et al., Pushing the performance of Biased Neighbor Selection through Biased Unchoking, S. 301, 303.

199 *Ngiwlay/Intanagonwiwat/Teng-amnuay*, Bittorrent Peer Identification Based on Behaviors of a Choke Algorithm, S. 65, 68.

200 *Legout/Urvoy-Keller/Michiardi*, Rarest First and Choke Algorithms Are Enough, S. 213, 214.

201 *Lareida/Hoßfeld/Stiller*, The BitTorrent Peer Collector Problem, S. 449, 450.

202 So aber *Koch*, jurisPR-ITR 14/2015, Anm. 3.

wird und selbst der bekannteste (bisher) größte Schwarm auf – geschätzt – maximal 193.000 Teilnehmer anwuchs[203], schlicht abwegig. Vielmehr weisen – zumindest nach einer Erhebung aus dem Jahr 2011 – mehr als 80 Prozent der Schwärme nicht mehr als 10 Teilnehmer auf; nur eine handvoll Schwärme kommen auf mehr als 10.000 Teilnehmer.[204]

Weiterhin ist hinsichtlich der übertragenen Daten*menge* die Zahl der Datenempfänger irrelevant, da Erstere in jedem Fall auf die Upload-Geschwindigkeit des übertragenden Internetanschlusses begrenzt ist und weiter durch die Menge an abgefragten Daten begrenzt werden kann. Diejenigen Nutzer, an die hochgeladen wird, teilen sich also die vorhandene Bandbreite untereinander auf. Typischerweise dauert es im BitTorrent-System mindestens zweimal so lange, Daten hochzuladen wie die gleiche Datenmenge herunterzuladen.[205]

Zudem kann in BitTorrent-Clients regelmäßig eingestellt werden, welche Uploadrate maximal zur Verfügung gestellt werden soll.[206]

c) Private Börsen

Öffentlich zugängliche *filesharing*-Systeme weisen bestimmte organisatorische Gemeinsamkeiten auf: die Nutzer kennen sich nicht untereinander und haben dasselbe – und damit technisch gegensätzliche – Interesse, nämlich Dateien zu bekommen. Es gibt keinen Anreiz, dem System Dateien bzw. Dateifragmente beizusteuern. Bezüglich urheberrechtlich geschützter Dateien gilt vielmehr das Gegenteil: die Gefahr rechtlicher Konsequenzen schreckt eher davon ab, etwas beizutragen.[207] Der Vorgang, aus einem System einen Nutzen zu ziehen ohne zum System beizutragen, wird in der informatischen, ökonomischen und sozialwissenschaftlichen Literatur als *free riding* bezeichnet. Naheliegenderweise tritt dieses Phänomen in öffentlich zugänglichen *filesharing*-Systemen häufig auf und ist für den oben geschilderten Niedergang

[203] *Van Der Sar*, Game of Thrones Sets New Torrent Swarm Record.

[204] *Zhang* et al., IEEE Transactions on Parallel and Distributed Systems, Nr. 7, Bd. 22, 2011, S. 1164, 1171f.

[205] *Izal* et al., Dissecting BitTorrent: Five Months in a Torrent's Lifetime, S. 1, 10.

[206] Siehe beispielsweise *Cohen*, uTorrent Pro Tips: Faster Download & Upload Rates. Eine Reduzierung auf null ist jedoch bei den meisten Clients nicht möglich, siehe hierzu sogleich Kapitel § 1 II. 5. c).

[207] *Harris*, Journal of Institutional Economics, Nr. 5, Bd. 14, 2018, S. 901, 904f.

einiger anderer Systeme[208] mitverantwortlich.[209]

Im BitTorrent-System soll der *tit-for-tat*-Mechanismus dem *free riding* entgegenwirken. Durch diesen Mechanismus soll gesichert werden, dass ein Nutzer grundsätzlich an diejenigen Nutzer bevorzugt *chunks* hochlädt, die ihm selbst wiederum *chunks* mit der größten Upload-Geschwindigkeit zur Verfügung gestellt haben.[210] Theoretisch sind somit alle Nutzer angehalten, in ihrem Client eine möglichst hohe Upload-Rate einzustellen. Tatsächlich aber erreicht der Mechanismus das erwünschte Ziel aus technischen Gründen nicht uneingeschränkt. Stattdessen können in bestimmten Konstellationen Nutzer mit geringen Uploadraten schnellere Downloadraten haben als solche mit hohen Uploadraten.[211] Darüber hinaus kann der Mechanismus auch nicht verhindern, dass ein Nutzer den Upload einstellt, sobald er die gewünschte Datei vollständig heruntergeladen hat (er also nicht zum *seeder* wird).[212] Zuletzt existieren auch Clients wie *BitThief*, bei denen der Mechanismus „ausgetrickst" wird und ein Upload überhaupt nicht erfolgt.[213]

Die zwei genannten Probleme öffentlich zugänglicher BitTorrent-Netzwerke – geringer oder kein Upload und Vermeidung der Rolle als Seeder – können durch *private Börsen*[214] gelöst werden.

Private Börsen umfassen eine private Indexseite, einen (regelmäßig vom Inhaber der Indexseite betriebenen) privaten Tracker und .torrent-Dateien, die mit einem individuellen *passkey* präpariert sind. In Bezug auf die Indexseite heißt „privat", dass ein Zugriff auf die dort zur Verfügung gestellten .torrent-Dateien erst nach einer Registrierung auf der Seite möglich wird, die wiederum regelmäßig nur auf Einladung eines bereits registrierten Nutzers erlaubt wird. Der individuelle *passkey* ist mit dieser Registrierung verknüpft. In Bezug auf den Tracker heißt „privat", dass er einen Nutzer nur dann mit

208 Siehe Kapitel § 1 II. 6.

209 *Harris*, Journal of Institutional Economics, Nr. 5, Bd. 14, 2018, S. 901, 902f.

210 *Neglia* et al., A Network Formation Game Approach to Study BitTorrent Tit-for-Tat, S. 13.

211 *Pang/Guo*, Single-Hop Friends Recommendation and Verification Based Incentive for BitTorrent, S. 703, 704.

212 *Harris*, Journal of Institutional Economics, Nr. 5, Bd. 14, 2018, S. 901, 904.

213 *Locher* et al., Free Riding in BitTorrent is Cheap, S. 85.

214 Diese werden auch als *BitTorrent darknets* bezeichnet, was jedoch in dieser Arbeit auf Grund der anderweitigen Bedeutung des Begriffs *darknet* im allgemeinen *filesharing*-Kontext vermieden wird, siehe Kapitel § 1 I. 4.

anderen Nutzern zusammenführt, wenn dieser den Tracker mit einem gültigen *passkey* ansteuert.[215] Das System bleibt auf diese Weise geschlossen, ein Austausch mit Fremden beispielsweise über DHT oder PEX findet (idealerweise) nicht statt.[216] Um die Nutzer dazu zu bewegen, ihre Uploadrate nicht zu drosseln und als *seeder* im Schwarm zu verbleiben, kommt der als *Sharing Ratio Enforcement* (SRE) bezeichnete Mechanismus zum Einsatz: über den Tracker wird mit dem Account des Nutzers die Information verknüpft, welche Datenmenge er herunter- und welche er hochgeladen hat. Fällt dieses Verhältnis unter einen bestimmten Wert, wird er sanktioniert, beispielsweise durch Sperrung für weitere Downloads oder Ausschluss aus der privaten Börse.[217]

Die Erstellung privater Börsen wurde mit Einführung des BEP 27[218] möglich. Das Aufsetzen einer privaten Börse ist ohne vertiefte Informatik-Kenntnisse möglich, da standardisierte, quelloffene Software hierfür vorhanden ist.[219]

Aus der Rechtspraxis bekannte private Börsen sind beispielsweise *OiNK*[220] und *What.CD*[221], die im Jahr 2007 durch Vorgehen der englischen und holländischen Behörden respektive im Jahr 2016 durch Vorgehen der französischen Behörden geschlossen wurden. Seit 2020 versuchen in den USA Rechteinhaber durch Auskunftsbegehren gegen *Cloudflare* die Identität der Betreiber eines privaten Trackers herauszufinden.[222] Weniger bekannt sind Beispiele aus Deutschland: das polizeiliche Vorgehen gegen den Tracker *Quorks*[223] sowie die Verurteilung der Betreiber der Börse *The Independence Tracker* durch das AG Lüneburg[224].

---

215 *Liu* et al., Understanding and Improving Ratio Incentives in Private Communities, S. 610, 611.

216 *Zhang* et al., BitTorrent Darknets, S. 1, 2.

217 *Jia* et al., Fast download but eternal seeding: The reward and punishment of Sharing Ratio Enforcement, S. 280; *Liu* et al., Understanding and Improving Ratio Incentives in Private Communities, S. 610, 611.

218 http://www.bittorrent.org/beps/bep_0027.html - Zugriff am 31.03.2021.

219 *Zhang* et al., BitTorrent Darknets, S. 1, 2.

220 https://en.wikipedia.org/wiki/Oink%27s_Pink_Palace - Zugriff am 31.03.2021.

221 https://en.wikipedia.org/wiki/What.CD - Zugriff am 31.03.2021.

222 *Van Der Sar*, New MPA Subpoena Targets Private BitTorrent Tracker & Locally Significant Pirate Sites.

223 https://winfuture.de/news,51871.html - Zugriff am 31.03.2021.

224 AG Lüneburg, Strafbefehl, undatiert, Az. 14 Cs 7104 Js 30363/08 – unveröffentlicht; dem Verfasser auf ein Auskunftsbegehren hin zur Verfügung gestellt.

6. Zusammenfassung

Bei den vorgestellten *filesharing*-Systemen handelt es sich um die aus rechtspraktischer Sicht einzig relevanten Systeme, wobei – wie dargestellt – ein besonderes Augenmerk auf das BitTorrent-System zu legen ist. Zwar gibt es in Bezug auf die technische Funktionsweise der Verbindungsherstellung Gemeinsamkeiten und Unterschiede, sie unterfallen jedoch alle der in dieser Arbeit formulierten Kategorie „Zentralisiert". Auch Systeme wie Gnutella, Kad oder die Mainline DHT von BitTorrent müssen die einzelnen Nutzer in das Netzwerk initiieren, d.h. mit anderen Nutzern zusammenzuführen. Zumindest um das *bootstrapping* zu ermöglichen, kommt ein *filesharing*-System also nicht um eine zentral erreichbare Stelle herum.[225] Zwar existieren in der Informatik Ansätze, die auch zentral erreichbare Stellen jedenfalls für Systeme auf Basis verteilter Hashtabellen überflüssig machen könnten (beispielsweise das „Erraten" von möglicherweise ansprechbaren IP-Adressen[226]), diese wurden jedoch soweit ersichtlich bisher nicht implementiert oder sind jedenfalls nicht in nennenswertem Umfang in Benutzung.

Es mag zunächst künstlich wirken, zwei Kategorien zu bilden und dann einer der Kategorien keinen einzigen Anwendungsfall zuzuschreiben. Dieses Vorgehen ist jedoch – der rechtlichen Betrachtung vorgreifend – berechtigt: damit steht fest, dass über jedem Endnutzer von *filesharing* eine organisatorische Ebene steht, in die eingegriffen werden kann, um das jeweils genutzte System ganz oder jedenfalls partiell auszuschalten oder dessen Benutzung zu erschweren.[227]

III. Anwendungsfelder des *filesharing*

Bisher wurde in dieser Arbeit die Funktion des *filesharing* lediglich allgemein als Ermöglichung des Austauschs von Dateien beschrieben. Das ist nicht falsch, aber unpräzise, weil eine Datei im informatischen Sinne zunächst nur die Aneinanderreihung von Bits ist, die erst durch die Zuordnung

[225] *Jünemann*, Confidential Data-Outsourcing and Self-Optimizing P2P-Networks: Coping with the Challenges of Multi-Party Systems, S. 84, 123.

[226] *Dinger/ Waldhorst*, Decentralized Bootstrapping of P2P Systems: A Practical View, S. 703, 705; *GauthierDickey/ Grothoff*, Bootstrapping of Peer-to-Peer Networks, S. 205f.

[227] Für die rechtlichen Implikationen siehe Kapitel § 4 VIII. 3. d).

zu einem bestimmten Dateiformat (zum Beispiel .pdf, .mp3 oder .avi) von einem dafür ausgerichteten Anwendungsprogramm als Text-, Ton- oder Bildfolge interpretiert wird[228] und damit nichts über die Art ihrer Speicherung gesagt ist. Grob lassen sich in einem nächsten Schritt die Anwendungsfelder von *filesharing* in drei Kategorien aufteilen: in der ersten Kategorie soll eine Datei dauerhaft auf dem Rechner eines Nutzers gespeichert werden, in der zweiten Kategorie nur temporär. Als dritte Kategorie ließe sich verteiltes Speichern ansehen, d.h. statt eine Datei zu erlangen, soll umgekehrt eine bereits vorhandene Datei in Einzelteile zerlegt und auf verschiedenen Rechnern gespeichert werden.[229] Da für den im Rahmen dieser Arbeit verwendeten Begriff des *filesharing* jedoch nur die Erlangung neuer Dateien relevant ist, wird diese Kategorie nur am Rande beachtet.[230]

Einziges Anwendungsfeld aller vorgestellten *filesharing*-Systeme außer BitTorrent ist/war die erste Kategorie. Nutzer laden also Dateien zur dauerhaften Speicherung herunter. Musik in Audioformaten, typischerweise *mp3*, Videos in Videoformaten wie beispielsweise *avi*. Software wie Anwendungsprogramme und Videospiele sind typischerweise in sogenannten *ISO-Containern* (Dateiendung .iso) enthalten. Hierbei handelt es sich um eine virtuelle CD oder DVD, also ein virtuelles Abbild eines physischen Datenträgers.[231] Größere Dateien oder eine Vielzahl von Dateien sind häufig in Archivdateien wie *zip* oder *rar* „verpackt“[232], oft auch auf mehrere Archivteile aufgesplittet, die erst zusammengesetzt werden müssen, bevor das gesamte Archiv „entpackt“ und auf die Zieldatei(en) zugegriffen werden kann. Nicht archivierte Musik- und Videodateien können regelmäßig bereits dann zumindest teilweise abgespielt werden, wenn einzelne Bruchteile erlangt wurden; ISO-Container und Archivdateien sind hingegen „Datenmüll“, wenn sie nicht vollständig erlangt werden.[233]

Auch die meisten Clients, die das BitTorrent-Protokoll implementieren[234], sind für den Zweck der Übertragung der eben genannten Dateien ausgelegt.

[228] https://de.wikipedia.org/wiki/Datei - Zugriff am 31.03.2021.
[229] https://en.wikipedia.org/wiki/Cooperative_storage_cloud - Zugriff am 31.03.2021.
[230] Siehe Kapitel § 3 XI. 2. b).
[231] https://de.wikipedia.org/wiki/ISO-Abbild - Zugriff am 31.03.2021.
[232] *Heckmann/Nordmeyer*, CR 2014, 41, 42f.
[233] *Heckmann/Nordmeyer*, CR 2014, 41, 42f.
[234] Eine Übersicht findet sich unter https://en.wikipedia.org/wiki/Comparison_of_BitTorrent_clients - Zugriff am 31.03.2021.

Es existieren aber auch gänzlich andere Anwendungsmöglichkeiten für das Protokoll, wie beispielsweise der Messenger *Bleep* beweist, der anders als der bekannte Messenger *WhatsApp* keiner zentralen Speicherung der übertragenen Nachrichten bedarf.[235]

BitTorrent wurde auch für die zweite Kategorie nutzbar gemacht: Der (mittlerweile wieder eingestellte Dienst) *BitTorrent Live* hat gezeigt, dass die BitTorrent-Technologie das Live-Streaming von Events an eine Zahl von Personen ermöglichen könnte, von der klassische Server-basierte Lösungen überfordert wären.[236] Generell könnte die BitTorrent-Technologie für datenintensive Streamingdienste nutzbar gemacht werden.[237]

Weitere Beispiele mit absehbarer, zukünftiger Relevanz in Bezug auf Urheberrechtsverletzungen und Abmahnungen finden sich in Kapitel § 3 XI. Abgesehen hiervon gibt es jedoch auch – neben den bereits Genannten – zahlreiche legale Anwendungsgebiete für BitTorrent.[238]

IV. Die Ermittlung von Teilnehmern in einem *filesharing*-System

1. Einleitung

Grundlage der Kommunikation im Internet ist die auf Grundlage des Interprotokolls[239] vergebene IP-Adresse. In diesem Abschnitt wird zunächst erörtert, welche Information sich von außen betrachtet – d.h. aus der Warte einer Person, die nicht denjenigen Router verwaltet, auf den die entsprechende IP-Adresse zurückzuführen ist – aus einer IP-Adresse ablesen lässt. Sodann wird auf die Ermittlung der IP-Adresse in einem *filesharing*-Sytem und die darauf folgende Zuordnung der IP-Adresse zu einem konkreten Internetanschluss, mithin einem Anschlussinhaber[240] und dessen Name und Anschrift, eingegangen. Anschließend wird aufgezeigt, wie die Ermittlung der IP-Adresse vereitelt werden kann und welche Fehler bei der Ermittlung

235 *Fadaie*, Building An Engine for Decentralized Communications.
236 *Vincent*, BitTorrent unveils new live-streaming platform for peer-to-peer broadcasts.
237 *Brodkin*, BitTorrent: Netflix should defeat ISPs by switching to peer-to-peer.
238 Siehe beispielsweise nur *Hoffmann*, 8 Legal Uses for BitTorrent: You'd Be Surprised.
239 Siehe hierzu Kapitel § 1 I. 3. a) bb).
240 Gemeint ist/sind derjenige/diejenigen, der/die bezüglich der Leistung der Internetversorgung Gläubiger eines entsprechenden Providervertrages mit einem ISP ist/sind.

passieren können.

2. Die IP-Adresse

a) IPv4

Wie in Kapitel § 1 I. 3. a) bb) gezeigt, erhält auf Ebene der Internetzwerkschicht ein Netzwerk durch das IP eine logische Adresse, mittels der es von anderen Netzwerken adressiert werden kann.

Diese logische Adresse ist die IP-Adresse. Nach dem gegenwärtig überwiegend benutzten *IPv4*-Standard ist die Adresse 32 bit lang. In Dezimalstellen wiedergegeben bedeutet dies, dass sie aus vier Blöcken besteht, die jeweils den Wert 0 bis 255 einnehmen können. Vom Wert 0.0.0.0 bis 255.255.255.255 sind also alle Kombinationen möglich, insgesamt damit knapp 4,3 Milliarden. Dieser Wert wird als *Adressraum* bezeichnet.[241] Jedes am Internet teilnehmende Netzwerk erhält eine einzigartige Adresse.[242] Zwar erhalten auch die Geräte *innerhalb* eines Netzwerkes eine IP-Adresse; mit dieser Adresse können sie aber nicht außerhalb ihres Netzwerkes „auftreten".[243] Folglich treten alle Geräte eines Netzwerkes mit anderen Netzwerken nur über die IP-Adresse ihres Netzwerkes in Kontakt. Bewerkstelligt wird dies durch den Mechanismus der *Network Adress Translation* (NAT), der im Router eines Netzwerkes zum Einsatz kommt. Verkehr von der privaten Adresse wird dazu in die öffentliche Adresse, also die IP-Adresse des Netzwerks, „übersetzt", eingehender Verkehr umgekehrt von der öffentlichen in die private.[244] Dieses Prozedere verringert die benötigte Anzahl an IP-Adressen erheblich, da für die im Internet zu vermeidenden Adresskonflikte nur die öffentliche IP-Adresse relevant ist.

Die öffentliche IP-Adresse ist in der Regel dynamisch. Das bedeutet, dass sie für jede neue Einwahl des Routers ins Internet oder nach einer bestimmten Zeit (regelmäßig 24 Stunden)[245] vom jeweils zuständigen ISP neu vergeben wird. Dieser wiederum hat für seine Geschäftstätigkeit von einer *Regional Internet Registry* (RIR) einen Block aus dem oben genannten Adressraum

241 *Forouzan*, TCP/IP protocol suite, S. 115f.
242 *Forouzan*, TCP/IP protocol suite, S. 115.
243 https://de.wikipedia.org/wiki/Private_IP-Adresse - Zugriff am 31.03.2021.
244 *Kurose/Ross*, Computer Networking: A Top-Down Approach, S. 349ff.
245 *Aschermann*, Dynamische und statische IP-Adressen: Das sind die Unterschiede.

erhalten, der wiederum ein Bruchteil des Blocks ist, den die RIR von der IANA/ICANN erhalten hat.[246] Durch diese gestufte Vergabe wird sichergestellt, dass keine IP-Adresse zweimal vergeben wird.

Da alle Geräte eines Netzwerkes mit anderen Netzwerken nur über die IP-Adresse ihres Netzwerkes in Kontakt treten, lässt sich von außen nicht ermitteln, von welchem Gerät aus diesem Netzwerk bestimmte Datenpakete übermittelt wurden bzw. an dieses übermittelt wurden.

b) IPv6

Soweit ersichtlich, wird sich hieran (also der fehlenden Möglichkeit, aus einer IP-Adresse über den Internetanschluss hinaus Rückschlüsse ziehen zu können) auch mit der schrittweise stattfindenden Einführung des *IPv6*-Standards nicht ändern. Dieser Standard soll die – trotz NAT und CG-NAT[247] bestehende – Adressknappheit des IPv4-Standards[248] kommt aber noch nicht vollumfänglich zum Einsatz.[249] Für eine vollständige Ablösung des IPv4-Standards wären insbesondere auf Seiten der ISPs und IXPs weitreichende Änderungen an der Router-Hardware vorzunehmen, die noch ausstehen.[250]

Da Netzwerke, die nur eine IPv6-Adresse haben, nicht mit Netzwerken kommunizieren können, die eine IPv4-Adresse aufweisen, existieren zum Zwecke der Kommunikation solcher Netzwerke untereinander die Mechanismen *Dual Stack*, *Dual Stack Lite* sowie für den Mobilfunk *464XLAT*, was einen parallelen Betrieb von IPv6 und IPv4 bedeutet.[251]

IP-Adressen nach IPv6 sind 128 bit lang, was theoretisch 2^{128} Kombina-

[246] https://de.wikipedia.org/wiki/IP-Adresse#Vergabe_von_IP-Adressen_und_Netzbereichen - Zugriff am 31.03.2021.

[247] Siehe zu Letzterem Kapitel § 1 IV. 5. d).

[248] *Richter*, Empirical Analysis of the Effects and the Mitigation of IPv4 Address Exhaustion, S. 16; RIRs handeln aus diesem Grund bereits untereinander in großem Umfang mit IPv4-Adressblöcken, siehe *Livadariu/Elmokashfi/Dhamdhere*, Computer Communications, Bd. 111, 2017, S. 105, 108.

[249] In Deutschland gegenwärtig zu ca. 52 Prozent, siehe https://www.google.de/ipv6/statistics.html#tab=per-country-ipv6-adoption - Zugriff am 31.03.2021.

[250] *Richter*, Empirical Analysis of the Effects and the Mitigation of IPv4 Address Exhaustion, S. 109.

[251] https://www.elektronik-kompendium.de/sites/net/2010211.htm - Zugriff am 31.03.2021.

tionsmöglichkeiten ergibt, womit eine Erschöpfung an Adressen praktisch ausgeschlossen ist.[252] Die ersten 64 bit (der vordere Teil) werden dabei ISP-seitig vergeben, die zweiten 64 bit (der hintere Teil) werden auf Basis der MAC-Adresse des jeweils verwendeten Geräts gebildet.[253]

Wie stark die Privatsphäre unter diesem Standard betroffen sein kann und wird, ist in der informatischen und juristischen Debatte nach wie vor ein Streitpunkt.[254] Gegenstand in diesem Zusammenhang sind insbesondere die Fragen nach der Verwendung der NAT sowie der Art des Adressaufbaus.

Hinsichtlich NAT ist umstritten, ob es im Rahmen von IPv6 noch zum Einsatz kommen soll.[255] Das Problem der Adressknappheit existiert bei IPv6 nicht. Es werden jedoch verschiedene technische Gründe angeführt, warum ein Festhalten an NAT bei IPv6 dennoch Sinn machen kann.[256] Ohne NAT hätte jedes Gerät eine eigene öffentliche IP-Adresse. Es ist aber nicht davon auszugehen, dass deswegen von außen betrachtet der von einem Internetanschluss ausgehende Datenverkehr einem bestimmten Gerät zuortbar sein wird. Es ist wie gesagt auch noch nicht entschieden, ob und inwieweit NAT zum Einsatz kommen wird.

Ebenfalls ist noch nicht gesichert, wie die Adressvergabe in Bezug auf den vorderen Teil in Zukunft von statten gehen wird. Kernstreit ist die Frage, ob der Adressteil statisch oder – jedenfalls in Teilen – dynamisch vergeben wird.[257] Anders als beim IPv4-Standard ist eine dynamische Vergabe aus Rücksicht auf die Adressknappheit bei IPv6 wegen der praktisch unbegrenzten Anzahl an Adressen nicht nötig.[258] Allerdings haben in Deutschland einige ISPs angekündigt, auch IPv6-Adressen dynamisch zu vergeben. Darüber hinaus ist zudem denkbar, den unter IPv4 in Verbindung mit der NAT geltenden Grundsatz „eine IP-Adresse für mehrere Geräte“ umzuwandeln in „mehrere Adressen pro Gerät“[259]; ein Gerät könnte beispielsweise für verschiedene Adressaten verschiedene Adressen verwenden.

[252] *Forouzan*, TCP/IP protocol suite, S. 772.
[253] https://de.wikipedia.org/wiki/IPv6#Adressaufbau_von_IPv6 - Zugriff am 31.03.2021.
[254] *Kaps*, Datenschützer besorgt über IPv6; *Freund/Schnabel*, MMR 2011, 495, 495ff.
[255] *Ermert*, Gretchenfrage: NAT oder nicht NAT für IPv6?
[256] *Thoma*, IPv6 ist noch nicht genügend getestet.
[257] *Donnerhacke*, Der Mythos von der dynamischen IP-Adresse.
[258] *Kleinz*, Das Internet-Protokoll 6 verändert die Spielregeln.
[259] *Sullivan*, IPv6 will allow them to track you down. Not!

Das Problem bei der Art der Adressbildung des hinteren Teils ist, dass derjenige, der ein Datenpaket erhält, über die MAC-Adresse des aussendenden Geräts informiert wird. Betriebssysteme wie Windows sehen aber bereits die in RFC 4941 festgehaltenen *Privacy Extensions* vor, die die Adresse derart modifizieren, dass die Auslesbarkeit der MAC-Adresse verhindert werden soll.[260] Es ist daher damit zu rechnen, dass von außen betrachtet auch aus dem hinteren Teil einer IPv6-Adresse keine Rückschlüsse auf das verwendete Endgerät gezogen werden können.[261]

c) Zusammenfassung

Für den Zweck dieser Arbeit ist im Ergebnis davon auszugehen, dass – von außerhalb eines Netzwerks betrachtet – eine IP-Adresse gemäß dem IPv6-Standard keinen Mehrgehalt an Informationen verrät als eine IP-Adresse gemäß dem IPv4-Standard.[262]

Folglich kann – von außen betrachtet – sowohl gegenwärtig als auch in Zukunft nicht nur nicht ermittelt werden, welche konkrete Person ein Datenpaket ausgesendet hat, sondern auch nicht, von welchem Gerät innerhalb eines Netzwerkes dieses ausgesandt wurde. Lediglich der verwendete Internetanschluss ist als Quelle identifizierbar.[263]

3. Arten des Betriebs eines WLAN

An dem Vorgesagten ändert auch die Art, wie das WLAN betrieben wird, nichts. Ein WLAN kann geschlossen, offen oder als *Hotspot* betrieben wer-

[260] https://www.elektronik-kompendium.de/sites/net/1601271.htm - Zugriff am 31.03.2021.

[261] Anders kann es jedoch sein, wenn auf einem Gerät die *Privacy Extension* nicht aktiviert ist und hierbei wiederum insbesondere dann, wenn dem Gerätehersteller bekannt ist, welchen seiner Kunden welche MAC-Adresse zugeordnet ist, was insbesondere bei mobilen Geräten der Fall sein kann, siehe *Wegener/Heidrich*, CR 2011, 479, 483f.

[262] Diese Aussage kann jedoch im Lichte zukünftiger tatsächlicher Entwicklungen und Erkenntnisse unter Umständen zu korrigieren sein.

[263] *Liberatore* et al., Digital Investigation, Bd. 7, 2010, S. 95, 98; *Mackey/Schoen/Cohn*, Unreliable Informants: IP Addresses, Digital Tips and Police Raids, S. 10ff.

den.[264]

Der Betrieb des WLANs ist geschlossen, wenn ein Gerät zwar Signale des entsprechenden Routers empfängt, diese jedoch verschlüsselt sind, mithin für den Zugang ein Passwort erforderlich ist, das entweder werkseitig im Router hinterlegt ist oder vom Betreiber vergeben wird. Die Passwortauthentifizierung baut auf einem Sicherheitsmechanismus auf, der regelmäßig werkseitig bereits im Router implementiert ist. Gegenwärtig ist eine Sicherung nach dem WPA2-Protokoll üblich.[265]

Der Betrieb ist offen, wenn ein Passwortzugang nicht erforderlich ist, mithin bei Verbindung mit dem Router insbesondere eine über diesen vermittelte Internetverbindung benutzt werden kann. Offen betriebene WLANs sind in Deutschland im Vergleich zu anderen Industrieländern nur sehr selten anzutreffen.[266]

Der Betrieb eines WLAN als Hotspot ist in seinen Auswirkungen ähnlich dem geschlossenen Betrieb. Die Verbindung zum Netzwerk ist zwar anders als beim geschlossenen möglich; es ist aber regelmäßig so konfiguriert, dass die Nutzung einer über das WLAN vermittelten Internetverbindung erst möglich ist, wenn über den Webbrowser eine Authentifizierung mittels Eingabe der Einwahldaten eines Benutzerkontos erfolgt ist. Die Authentifizierung wird für jeweils eine bestimmte MAC-Adresse, also ein bestimmtes Gerät, vermerkt. Der Betrieb eines Hotspot erleichtert gegenüber dem geschlossenen Betrieb insbesondere das gewerbliche Anbieten einer Internetverbindung im öffentlichen Raum, da einem Benutzerkonto bestimmte Datenkontingente zugewiesen werden können und somit eine Abrechnung vereinfacht und automatisiert erfolgen kann. Zudem können die Benutzerkonten auch an einer Zentralstelle verwaltet werden, sodass für die Abrechnung irrelevant ist, über welchen Router eine Internetverbindung genutzt wurde (falls der gewerbliche

[264] Eine kabelgestützte Verbidung zu einem Netzwerk ist prinzipiell als geschlossen zu bezeichnen, da ein Internetanschlussinhaber letztlich in jedem Einzelfall die Verfügungsgewalt darüber hat, welche Kabelverbindungen zu seinem Router er zulässt und welche nicht, eine kabelgestützte Verbindung also im Ergebnis wie eine passwortgeschützte WLAN-Verbindung zu bewerten ist. Eine rein kabelgestützte Verbindung würde man als *Local Area Network* (LAN) bezeichnen, siehe https://de.wikipedia.org/wiki/Local_Area_Network - Zugriff am 31.03.2021.

[265] https://de.wikipedia.org/wiki/WPA2 - Zugriff am 31.03.2021.

[266] Siehe Nachweise bei *Mantz/Sassenberg*, CR 2015, 298, 298; *Grigorjew*, CR 2016, 701, 701.

Anbieter mehrere Router betreibt).[267]

Da bei allen drei Betriebsvarianten von außen betrachtet nur die IP-Adresse des Netzwerks in Erscheinung tritt, ergibt sich für die Ermittlung (von außen) kein Unterschied, welche Betriebsvariante tatsächlich vorliegt. Unterschiede können sich aber in der rechtlichen Bewertung ergeben.[268]

4. Die Ermittlung der IP-Adresse in einem *filesharing*-System

Wer in einem nicht-anonymen *filesharing*-System[269] eine Verbindung zu einem anderen Nutzer aufbaut, offenbart dabei zwangsläufig seine IP-Adresse.

In älteren *filesharing*-Systemen war es möglich und üblich, eine Datei nur herunterzuladen, ohne sie nach vollständigem Download anderen Nutzern anzubieten.[270] Die Ermittlung in diesen Systemen war folglich nur in eingeschränktem Umfang möglich, also nur insoweit als dort Nutzer auch Dateien anboten, was lediglich auf den geringeren Teil der Nutzer zutraf.[271] Wollte man auch Nutzer ermitteln, die nur herunterladen, mussten die Ermittler hierzu selbst Dateien anbieten, also als Lockvogel oder „Honeypot" agieren.[272] Da bei eDoneky und insbesondere BitTorrent jeder Nutzer ganz regelmäßig auch Fragmente der Zieldatei hochlädt[273], stellt sich dieses Problem dort nicht mehr.

In der Praxis sind spezialisierte Ermittlungsfirmen damit beauftragt, die IP-Adressen von Nutzern, die urheberrechtlich geschützte Dateien abrufen und/oder anbieten, in Erfahrung zu bringen und zu speichern. Im Rahmen des BitTorrent-Systems kann der Ermittler dabei insbesondere gezielt nach Anbietern und Nachfragern einer Datei mit einem bestimmten Hashwert suchen[274], die bereits als urheberrechtsverletzend identifiziert wurde, sodass die namentliche Bezeichnung der Datei ignoriert werden kann. Typischer-

267 https://de.wikipedia.org/wiki/Hot_Spot_(WLAN) - Zugriff am 31.03.2021.
268 Siehe insbesondere Kapitel § 5 V. 3. a).
269 Zu anonymen Systemen siehe Kapitel § 1 IV. 6. a).
270 Insbesondere Napster, Gnutella und FastTrack, siehe die Kapitel § 1 II. 4. a), b) und c).
271 Aus Sicht der Nutzer also ein Problem des *free riding*, siehe Kapitel § 1 II. 5. c).
272 Siehe hierzu *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 175ff.
273 Siehe hierzu Kapitel § 1 II. 4. d) und § 1 II. 5. b).
274 Zum Hashwert siehe Kapitel § 1 II. 4. d).

weise beteiligt sich der Ermittler dann mittels eines modifizierten Clients an dem Schwarm, der auf diese Datei bezogen ist und loggt die IP-Adressen derjenigen Nutzer, die sich mit ihm verbinden, automatisch mit. Nach Abschluss der Ermittlung werden die IP-Adressen gelistet und an eine Rechtsanwaltskanzlei übersandt.[275]

Laut einer Studie aus dem Jahr 2012 wird ein Großteil der IP-Adressen der Nutzer, die eine aktuell populäre Datei tauschen, auch ermittelt.[276]

5. Der Rückschluss aus der IP-Adresse auf den Inhaber eines Internetanschlusses

a) IPv4

Aus einer IP-Adresse kann nicht unmittelbar der Rückschluss auf einen Namen und eine Anschrift gezogen werden. Dies kann nur der ISP, der die IP-Adresse vergeben hat. Er kann speichern, welche IP-Adresse er welchem Kunden zugeteilt hat. Ein Rückschluss aus der IP-Adresse auf den ISP, der sie vergeben hat, ist jedoch möglich. Bewerkstelligen lässt sich dies in Deutschland durch eine Abfrage bei *RIPE*, dem – unter anderem – für Deutschland zuständigen RIR, da dieser IP-Blöcke an die ISPs verteilt.[277]

Der ISP erteilt dann Auskunft über Name und Anschrift des Anschlussinhabers, dem die IP-Adresse zuzuordnen ist, freiwillig oder wird durch rechtliche Mittel hierzu gezwungen.[278] Einzige technische Voraussetzung für die Erteilung der Auskunft ist, dass der ISP die Information über die Zuordnung der IP-Adresse zu einem bestimmten Kunden für den abgefragten Zeitpunkt oder Zeitraum gespeichert hat. Dies ist technisch möglich (jedoch, je nach betriebenem Umfang, mit einigem Aufwand für die ISP verbunden[279]); in Deutschland existieren hierzu gesetzlich vorgeschriebene, aber gegenwärtig umstrittene Speicherfristen.[280]

---

275 *Lutz*, DuD 2012, 584, 584f; *Morgenstern*, CR 2011, 203, 205f.

276 *Chothia* et al., The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent, S. 185, 199ff.

277 https://www.ripe.net - Zugriff am 31.03.2021.

278 Siehe hierzu Kapitel § 2 III. 1. b).

279 *Briegleb*, Vorratsdatenspeicherung: Provider warnen vor dem „Mittelstandskiller".

280 Siehe hierzu Kapitel § 2 III. 1. e).

b) IPv6

Wegen der prinzipiell ähnlichen Adressvergabe im Rahmen von IPv6[281], ergeben sich hinsichtlich des Vorgehens bei der Ermittlung des Anschlussinhabers keine Unterschiede zu IPv4.

D.h. aus einer IPv6-Adresse wird sich auch in Zukunft nicht auf Name und Anschluss eines Internetanschlusses ohne Mithilfe des entsprechenden ISP schließen lassen. Zwar wurden zu Testzwecken registrierte, *statische* IP-Adressen samt Zuordnung zu einem Inhaber in öffentlichen Registern geführt[282]; es ist jedoch nicht anzunehmen, dass dies bei gewöhnliche Endverbrauchern der Regelfall sein wird, auch dann, wenn IPv6-Adressen generell statisch vergeben werden sollten.[283]

Unterschiede ergeben sich mithin bei der Zuordnung nicht.

c) Reseller

Eine Besonderheit ist die Auskunft durch einen *Reseller*. Ein Reseller ist ein ISP, der keine eigene technische Infrastruktur betreffend die Datenübermittlung hat, sondern diese nur von einem anderen ISP mit Infrastruktur anmietet, um selbst Endkundenanschlüsse anbieten zu können.[284] In Deutschland hat beispielsweise die *Deutsche Telekom* eigene Infrastruktur (ist also Netzbetreiber), das Unternehmen *1&1* ist dagegen ein Reseller, der sich der Infrastruktur der Deutschen Telekom bedient. Für einen Ermittler erscheint eine IP-Adresse also zum Netz der Deutschen Telekom zugehörig, auch wenn für den Endkundenanschluss 1&1 zuständig ist. Name und Anschrift des entsprechenden Anschlussinhabers kann letztlich jedoch nur der Reseller mitteilen.[285] Die Auskunftserteilung muss also, wenn der betroffene Internetanschluss von einem Reseller zur Verfügung gestellt wird, zweistufig erfolgen, d.h. der Netzbetreiber teilt mit, von welchem Reseller der Anschluss zur Verfügung gestellt wird (mittels einer Anschlusskennung), der Reseller nennt Name und Anschrift des Anschlussinhabers, dem die jeweilige Anschlusskennung zugeordnet ist.

---

281 https://de.wikipedia.org/wiki/IPv6#Adresszuweisung - Zugriff am 31.03.2021.

282 Die öffentlich einsehbare Zuordnung ist in den Geschäftsbedingungen von RIPE vorgegeben, siehe *Meyerdierks*, MMR 2015, 705, 706.

283 *Schneider*, Wie IPv6 das Medienrecht verändern wird.

284 BVerwG, Urteil vom 3. Dezember 2003, Az. 6 C 20.02, Rz. 45 – juris.

285 *Zimmermann*, K&R 2015, 73, 73.

d) Carrier-grade NAT

Um der Adressknappheit im Rahmen des IPv4-Standards zu entkommen, wird der Mechanismus der NAT[286] nicht nur auf Ebene des Endkundenanschlusses genutzt, sondern auch auf Ebene des ISP.[287] Das bedeutet, dass der ISP eine öffentliche IP-Adresse mehreren Endkundenanschlüssen zuteilt, also auch die Endkundenanschlüsse selbst nur eine private IP-Adresse haben. Verkehr zwischen dem Endkundenanschluss und dem Internet muss also von der privaten in die öffentliche Adresse (mittels Port-Adressierung[288]) „übersetzt" werden und umgekehrt. Diesen Mechanismus bezeichnet man als *Carrier-grade NAT* (CG-NAT).[289] Nach einer Erhebung aus dem Jahr 2016 setzen 90 Prozent der Mobilfunkanbieter und 38 Prozent der „klassischen" ISPs das CG-NAT ein.[290] Eine andere Untersuchung stellte für den Zeitraum von 2014 bis 2016 fest, dass knapp ein Viertel aller ISPs CG-NAT nutzen.[291] *Europol* hat diesen Umstand als ein Hindernis für die Strafermittlungsbehörden bezeichnet; 80 Prozent der befragten Ermittler seien in ihrer Ermittlungstätigkeit durch CG-NAT schon einmal aufgehalten oder vollständig behindert worden.[292] In Schweden scheiterte in einem Fall die Durchsetzung des urheberrechtlichen Auskunftsanspruchs an der Verwendung von CG-NAT durch den Beklagten ISP.[293]

Rein technisch betrachtet verhindert jedoch auch ein CG-NAT nicht den Rückschluss auf einen bestimmten Endkundenanschluss aus einer öffentlichen IP-Adresse. Es müssen „lediglich" über die IP-Adresse hinaus weitere, im Rahmen der CG-NAT erforderliche Daten gespeichert werden.[294] Die

[286] Siehe hierzu Kapitel § 1 IV. 2. a).

[287] *Doyle*, Can Large Scale NAT Save IPv4?

[288] *Doyle*, Can Large Scale NAT Save IPv4?

[289] https://www.elektronik-kompendium.de/sites/net/2010221.htm - Zugriff am 31.03.2021.

[290] *Richter* et al., CoRR, Bd. abs/1605.05606, 2016, S. 1, 2.

[291] *Livadariu* et al., Inferring Carrier-Grade NAT Deployment in the Wild, S. 2249.

[292] https://bit.ly/2yDviCI - Zugriff am 31.03.2021.

[293] *Maxwell*, IP Address Fail: ISP Doesn't Have to Hand 'Pirates' Details to Copyright Trolls.

[294] Nach Angabe eines ISP im Rahmen des Verfahrens betreffend der Aussetzung der Vorratsdatenspeicherung sind diese Daten die interne IP-Adresse und interne Port-Nummer, die zugeordnete externe IP-Adresse und externe Port-Nummer, die jeweilige Ziel-IP-Adresse und Ziel-Port-Nummer sowie der präzise Zeitstempel der Zuordnung; siehe hierzu VG Köln, Beschluss vom 25. Januar 2017, Az. 9 L 1009/16, Rz. 132 – juris.

Speicherung dieser Daten ist für ISPs technisch möglich.[295] Ob die Daten auch gespeichert werden, ist mithin eine rein rechtliche Frage.

6. Anonyme und anonymisierende Dienste

Die Ermittlung der IP-Adresse kann unmöglich gemacht oder jedenfalls erschwert werden. Die Ermittlung der IP-Adresse kann auch möglich, aber nicht unmittelbar zielführend sein, weil das Netzwerk, von dem eine *filesharing*-Aktivität ausgeht, hinter der IP-Adresse eines anderen Netzwerks „verborgen“ ist.

a) Anonyme Dienste

Anonyme Dienste im Sinne dieser Arbeit sind *filesharing*-Systeme, die an sich bereits darauf ausgelegt sind, die Ermittlung der IP-Adresse unmöglich zu machen. Beispiele sind das bereits erwähnte *freenet* oder *RetroShare* sowie *I2P*. Zwar gibt es wenig empirische Hinweise auf den Nutzungsumfang anonymer Systeme im Hinblick auf *filesharing*; er dürfte aber bei wenigen tausend Personen liegen.[296] Ein wichtiger Grund hierfür dürfte folgendes sein: Der technischen Erzeugung der Anonymität ist geschuldet, dass anonyme Dienste in der Datenübertragung sehr langsam und in der Bedienung wenig benutzerfreundlich sind.[297] Abgesehen davon also, dass die Nutzerbasis anonymer Systeme (bisher) im Vergleich zu BitTorrent ohnehin relativ unbedeutend ist, kann schon bezweifelt werden, ob sie überhaupt als *filesharing* im Rahmen der in dieser Arbeit gefundenen Definition anzusehen sind. Sie werden folglich nur am Rand behandelt.[298]

b) Anonymisierende Dienste

Anonymisierende Dienste hingegen ermöglichen es, ein eigentlich nichtanonymes System wie BitTorrent zu benutzen und dabei die IP-Adresse

[295] *Clayton*, Online traceability: who did that? Technical expert report on collecting robust evidence of copyright infringement through peer-to-peer filesharing, S. 16.

[296] Wenn auch die Tendenz nach oben geht und insbesondere die Zahl der Personen, die anonyme Systeme außerhalb von *filesharing* nutzen, stark steigt, siehe *O'Neill*, Tor and the rise of anonmyity networks.

[297] *Skogh* et al., Fast Freenet: improving Freenet performance by preferential partition routing and file mesh propagation, S. 8, 11.

[298] Siehe Kapitel § 3 XI. 2. d).

des Netzwerkes, von dem eine *filesharing*-Aktivität ausgeht, zu „verschleiern“ oder die Aktivität gleich ganz auszulagern. Die vier wichtigsten Dienste dieser Art sind *Virtual Private Networks* (VPN), *seedboxes*, das *Tor*-Netzwerk und *IP-Blocker*.[299]

aa) VPN

Ein VPN ermöglicht den Zutritt zu einem privaten Netzwerk über das Internet.[300] Beispielsweise lässt sich ein Heimnetzwerk so einrichten, dass auf dieses über das Internet von außerhalb zugegriffen werden kann. Für einen Außenstehenden erscheint der Internetverkehr, der von dem Nutzer eines VPN erzeugt wird, von dem entsprechenden VPN statt dessen eigenem Netzwerk auszugehen. Ein Ermittler in einem BitTorrent-Netzwerk kann also den über ein VPN ausgehenden Verkehr auch nur dem VPN zuordnen, nicht aber – ohne Mithilfe des VPN-Anbieters – demjenigen Netzwerk, von dem der Verkehr ursprünglich ausging. VPNs werden in der Regel von gewerblichen Anbietern betrieben. Bei diesen kann ein Benutzerkonto eingerichtet und der Datenverkehr über das Internet dann über deren Netzwerk abgewickelt werden.

Einem VPN sehr ähnlich sind auch *SOCKS5 proxies*[301], die häufig von gewerblichen VPN-Anbietern zur Verfügung gestellt werden; im Unterschied zu einem VPN wird hier nur der Verkehr einer bestimmten Anwendung über ein anderes Netzwerk umgeleitet. Wenig überraschend gibt es also speziell auf BitTorrent zugeschnittene *SOCKS5 proxies*. Das Resultat der Nutzung ist aus der Sicht eines Ermittlers das gleiche wie bei einem VPN: er kann den ermittelten Verkehr nur dem Anbieter des *SOCKS5 proxy* zuordnen.

bb) *seedbox*

Auf eine *seedbox* kann der Betrieb des *filesharing* ganz ausgelagert werden. Der Nutzer betreibt also das *filesharing* gar nicht auf seinem eigenen Gerät und über sein eigenes Netzwerk, sondern gibt lediglich der *seedbox* Anweisungen. Ist der Download auf die *seedbox* abgeschlossen, lädt er die Zieldatei über eine bloß zweiseitige Verbindung – beispielsweise mittels HTTP – von der

[299] *Caraway*, International Journal of Communication, Bd. 6, 2012, S. 564, 576.
[300] https://en.wikipedia.org/wiki/Virtual_private_network - Zugriff am 31.03.2021.
[301] https://en.wikipedia.org/wiki/SOCKS - Zugriff am 31.03.2021.

seedbox auf seinen Rechner herunter.[302] Ein Ermittler in einem BitTorrent-Netzwerk kann also dem über eine *seedbox* ausgehenden Verkehr auch nur dieser zuordnen, mithin ohne Mithilfe des Betreibers derselben nicht den Anweisenden herausfinden. Die Betreiber sind meist gewerbliche Anbieter, die die *seedbox* auf einem eigenen oder angemieteten Server ausführen.[303] Zugriff auf die *seedbox* erhält man durch Einrichtung eines Benutzerkontos.

cc) Tor-Netzwerk

Das Tor-Netzwerk soll Anonymität gewährleisten, indem der Verkehr eines Internetnutzers zunächst durch dieses Netzwerk getunnelt wird und dann erst nach außen tritt. Im Tor-Netzwerk passiert der Verkehr typischerweise drei Router (jeder reguläre Internetanschluss kann als Tor-Router sowie als *exit node*, also als Austrittspunkt aus dem Netzwerk, fungieren[304]); erst dann tritt der Verkehr unverschlüsselt nach außen. Bei Eintritt in und Bewegung innerhalb des Netzwerks ist er verschlüsselt.[305] BitTorrent-Clients können häufig so eingestellt werden, dass sie den Datenverkehr über das Tor-Netzwerk abwickeln. Sofern die Anonymisierung nicht fehlgeht, kann ein Ermittler nur die IP-Adresse der *exit node* in Erfahrung bringen.

dd) IP-Blocker

IP-Blocker sind Programme wie *PeerBlock* oder *PeerGuardian*, die man nebenher bei Nutzung eines *filesharing*-Client aktivieren kann und die verhindern, dass im *filesharing*-System eine Verbindung zu IP-Adressen aufgebaut wird, die verdächtigt werden, zu einem Ermittlungsdienst im Sinne von Kapitel § 1 IV. 4. zu gehören. Die Programme halten hierzu eine (aktualisierbare) Liste mit entsprechenden IP-Adressen vor.[306] So soll verhindert werden, dass die IP-Adresse des entsprechenden Nutzers vom Ermittlungsdienst geloggt wird.

---

302 *Caraway*, International Journal of Communication, Bd. 6, 2012, S. 564, 576.
303 https://en.wikipedia.org/wiki/Seedbox - Zugriff am 31.03.2021.
304 https://blog.torproject.org/tips-running-exit-node - Zugriff am 31.03.2021.
305 *McCoy* et al., Shining Light in Dark Places: Understanding the Tor Network, S. 63, 64f.
306 https://en.wikipedia.org/wiki/PeerBlock - Zugriff am 31.03.2021.

7. Fehler und Defizite bei der Ermittlung

a) Annahme der Zuverlässigkeit der Ermittlung

Eine Ermittlung ist im Sinne dieser Arbeit als zuverlässig zu anzusehen, wenn der Ermittler bzw. dessen Software eine IP-Adresse so aufzeichnet, wie sie sich ihm präsentiert hat.

Diese zunächst banal erscheinende Erkenntnis ist wichtig, da der Begriff „zuverlässig“ teils anders gebraucht wird. Beispielsweise spricht das AG Köln unter Berufung auf die Staatsanwaltschaft Köln in einem Urteil davon, dass die „Zuverlässigkeit“ der dort eingesetzten Ermittlungssoftware nicht ausreichend gesichert sei.[307] Gemeint ist jedoch, dass für eine Verurteilung des beklagten, vermeintlichen *filesharers* keine ausreichende Gewähr dafür bestehe, dass die ermittelte IP zum behaupteten Verletzungszeitpunkt auch dem behaupteten Anschluss zugeordnet war – was aber unabhängig von der Frage ist, welche IP-Adresse sich dem Ermittler bzw. der Ermittlungssoftware präsentiert hat und wie diese aufgezeichnet wurde. Tatsächlich wurde also der Beweiswert der Ermittlung, nicht jedoch deren Zuverlässigkeit angezweifelt.

Den folgenden Ausführungen[308] ist zu Grunde zu legen, dass die Aussage eines Ermittlers im Sinne von Kapitel § 1 IV. 4., dass er das Angebot/die Nachfrage einer Datei mit einem bestimmten Hashwert von einer bestimmten IP-Adresse aus beobachtet habe bzw. das hierfür eingesetzte automatisierte Programm eine zuverlässige Beobachtung gemacht habe, wahrheitsgemäß ist, mithin zuverlässig ermittelt wird.

Dies entspricht auch der üblichen Handhabung in der Rechtspraxis.[309] Das Bestreiten der Zuverlässigkeit führt ganz regelmäßig nicht zum Erfolg. Umgekehrt wurde stattdessen bereits in einem bekannt gewordenen Gerichtsverfahren von einem gerichtlichen Sachverständigen eine Ermittlungssoftware

[307] AG Köln, Urteil vom 22. April 2013, Az. 125 C 602/09, Rz. 25 – juris.

[308] Wegen der Dominanz des BitTorrent-Systems über andere Systeme beziehen sie sich auch auf dieses. Nicht alle nachfolgend genannten Punkte müssen nicht in jedem *filesharing*-System problematisch sein.

[309] Siehe beispielsweise exemplarisch LG Köln, Urteil vom 27. Januar 2010, Az. 28 O 241/09, Rz. 23ff. – juris; demnach genügt unqualifiziertes Bestreiten der Aussage des Ermittlers, er habe die einschlägige IP-Adresse zuverlässig ermittelt, sowie der Richtigkeit des entsprechend vorgelegten Ausdrucks der Log-Datei der Ermittlungssoftware, nicht.

überprüft und festgestellt, dass deren Überwachungsaufzeichnung im konkreten Fall authentisch ist, da eine Manipulation der entsprechenden Daten sofort aufgefallen wäre.[310] Diese Feststellung ist natürlich über den konkreten Fall hinaus nicht auf die entsprechende Ermittlungssoftware oder gar sämtliche im Einsatz befindliche Varianten von Ermittlungssoftware generell übertragbar. Ältere Gutachten mit gleichem Ergebnis wurden vom IT-Sachverständigen *Morgenstern* hinsichtlich Nichteinhaltung fachlicher Standards bemängelt.[311] Dies ist beispielsweise auch dem AG Köln bekannt.[312] Selbst von diesem aber wurde nicht die Konsequenz der Einordnung von Ermittlungen als unzuverlässig gezogen. Stattdessen wurde „nur" festgehalten, dass lediglich die Mehrfachermittlung[313] als ausreichendes Beweismittel für die Zuordnung einer Verletzung zu dem vom Rechteinhaber behaupteten Anschluss angesehen wird.[314] Tatsächlich ist mit wenigen Ausnahmen[315] kein Fall ersichtlich, in dem das Bestreiten der Zuverlässigkeit im eingangs definierten Sinne erfolgreich war. Immerhin: das OLG Köln hat postuliert, dass die Zuverlässigkeit von Ermittlungssoftware generell in regelmäßigen Abständen durch einen gerichtlich beauftragten Sachverständigen bestätigt werden muss.[316]

Im Ergebnis ist nach Vorgesagtem die eingangs postulierte Annahme als Arbeitshypothese gerechtfertigt (wenn sie *in praxi* natürlich durchaus in Zweifel gezogen werden kann[317]). Sie ist zudem auch nötig, da die Zuverlässigkeit der Ermittlung notwendige Bedingung für ihren positiven Beweiswert ist. Die Annahme der Zuverlässigkeit der Ermittlung ist also Grundbedingung der rechtlichen Erörterung der Ermittlung.

---

310 AG München, Urteil vom 29. Juni 2015, Az. 155 C 27136/12 – waldorf-frommer.de.

311 *Morgenstern*, CR 2011, 203, 206ff.

312 AG Köln, Hinweisbeschluss vom 22. Oktober 2014, Az. 125 C 410/14 – juris.

313 Siehe hierzu Kapitel § 5 III. 2.

314 AG Köln, Hinweisbeschluss vom 22. Oktober 2014, Az. 125 C 410/14 – juris.

315 Beispielsweise LG Frankenthal, Urteil vom 30. September 2014, Az. 6 O 518/13, Rz. 35 – juris; dem lag aber die besondere Konstellation zu Grunde, dass eine veraltete Version einer Ermittlungssoftware eingesetzt wurde. Ein anderes Beispiel ist LG Berlin, Urteil vom 3. Mai 2011, Az. 16 O 55/11, Rz. 45 – juris, bei dem von der erfassten IP-Adresse kein Upload ausging.

316 OLG Köln, Beschluss vom 20. Januar 2012, Az. 6 W 242/11, Rz. 6 – juris; OLG Köln, Beschluss vom 20. April 2016, Az. I-6 W 37/16, 6 W 37/16, Rz. 10ff. – juris.

317 Siehe ausführlicher *Bleich*, c't, Bd. 5, 2010, S. 50, 51

b) Annahme der aktiven Ermittlung

Um einen Download zu ermitteln, muss der Ermittler selbst hochladen, um einen Upload zu ermitteln, muss er selbst herunterladen.[318] Download und Upload werden nur durch eine *aktive* Ermittlung festgestellt. Bei einer *indirekten* Ermittlung werden hingegen (im Falle von BitTorrent) die in einem *peer set* vorhandenen IP-Adressen erfasst.[319] Die Beteiligung in einem *peer set* sagt aber noch nichts darüber aus, ob auch *chunks* hoch-oder heruntergeladen wurden; dies ist allenfalls wahrscheinlich, aber nicht zwingend (beispielsweise wird nichts hochgeladen, wenn ein entsprechender Client eingesetzt wird[320]). Zudem sind manche Tracker bewusst so ausgelegt, dass sie auch falsche IP-Adressen ausgeben, also solche, die gar nicht am Schwarm beteiligt sind.[321]

Eingesetzt werden laut einer Untersuchung aus dem Jahr 2012 wohl beide Ermittlungsmethoden.[322] Ob dies auch auf die für Deutschland benutzten Ermittlungsprogramme zutraf und zutrifft, kann mangels öffentlicher Informationen hierzu nicht bewertet werden.[323] Soweit ersichtlich, wurde jedenfalls vor Gericht bisher von Beklagtenseite nicht angeführt, dass zwar eine Beteiligung im *peer set* zutreffe, aber keine *chunks* hoch-oder herunter geladen wurden.

Folglich ist den Ausführungen in dieser Arbeit auch zu Grunde zu legen, dass eine Ermittlung nicht nur zuverlässig ist, sondern auch das Hoch-und Herunterladen von *chunks* beweist.[324]

---

[318] *Clayton*, Online traceability: who did that? Technical expert report on collecting robust evidence of copyright infringement through peer-to-peer filesharing, S. 20.

[319] *Chothia* et al., The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent, S. 185, 186.

[320] Siehe hierzu Kapitel § 1 II. 5. c).

[321] http://opentracker.blog.h3q.com/2007/02/12/perfect-deniability/ - Zugriff am 31.03.2021.

[322] *Chothia* et al., The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent, S. 185, 186.

[323] Anders in den USA, wo in einigen Fällen der Verdacht besteht, dass zwar die Anwendung aktiver Ermittlung behauptet wird, tatsächlich aber eine indirekte Ermittlung stattfindet, siehe *Hunter*, 31 J. Marshall J. Info. Tech. & Privacy L. 105, 127 (2014).

[324] Was jedoch nichts darüber aussagt, ob beispielsweise alle für die Zieldatei benötigten *pieces* heruntergeladen wurden; es sagt auch nichts darüber aus, an wie viele Personen welche Menge von *chunks* hochgeladen wurde. Siehe zu diesen Punkten Kapitel § 1 IV. 7. c) dd).

c) Technischer Beweiswert der Ermittlung

Eine absolute Gewissheit dafür, dass die *filesharing*-Aktivität über den vom ISP der IP-Adresse zugeordneten Internetanschluss betrieben wurde, bietet die Ermittlung jedoch typischerweise auch dann nicht, wenn sie – wie angenommen – zuverlässig und aktiv war. Auch sagt eine zuverlässige und aktive Ermittlung noch nichts über den Umfang der *filesharing*-Aktivität aus, die von einem ermittelten Anschluss aus betrieben wurde.

aa) Schwierigkeiten der Rekonstruierbarkeit einer *filesharing*-Aktivität

Im Nachhinein – und die rechtliche Aufarbeitung findet nur im Nachhinein statt – lässt sich normalerweise[325] nicht mit absoluter Gewissheit rekonstruieren, ob von der genannten IP-Adresse tatsächlich die genannte Datei angeboten und/oder nachgefragt wurde. Dies wäre nur in dem Sonderfall möglich, wenn im Rahmen des BitTorrent-Systems ein Tracker benutzt wurde, der Tracker die eingehenden Verbindungsdaten loggt, die Logdaten vom Tracker erlangt werden können und sich herausstellt, dass der Tracker – mit den Angaben des Ermittlers übereinstimmend – festgehalten hat, dass von der genannten IP-Adresse tatsächlich die genannte Datei angeboten und/oder nachgefragt wurde.

Sollte sich beispielsweise im Rahmen einer Hausdurchsuchung herausstellen, dass ein aufgefundenes Gerät eine Datei gespeichert hat, deren Hashwert dem des vom Ermittler genannten Wertes entspricht, wäre dies nicht einmal ein eindeutiger Beweis der Täterschaft des Inhabers des Geräts. Denn die Datei könnte theoretisch auch anders als über den Internetanschluss, der der genannten IP-Adresse zuzuordnen ist, erlangt worden sein. Eine Bestätigung des Ermittlungsergebnisses wäre ausnahmsweise nur dann möglich, wenn eine Analyse der Festplatte des betreffenden Geräts die behauptete *filesharing*-Aktivität zu Tage fördert, was aber nur möglich ist, soweit entsprechende „Residuen“ auf der Festplatte vorhanden sind.[326] Selbst aber dann wäre noch denkbar, dass eine andere Person als der Inhaber das Gerät für *filesharing* verwendet hat.

Soweit ersichtlich, existiert kein praktischer Fall der Verifizierung durch Log-

[325] Siehe zur Ausnahme in Kapitel § 1 V. 1. a).

[326] *Ieong* et al., Forensic Investigation of Peer-to-Peer Networks, S. 355, 365.

daten eines Trackers und/oder der Analyse des für die *filesharing*-Aktivität genutzten Geräts. Umgekehrt wurde eine Rekonstruktion auf Grund der genannten, im konkreten Fall unüberwindbaren Schwierigkeiten abgelehnt.[327]

bb) Wechsel bzw. Neuvergabe der IP-Adresse

Dynamische IP-Adressen werden regelmäßig alle 24 Stunden neu vergeben.[328] Gibt der Ermittler also lediglich einen einzigen Zeitpunkt an, an dem *filesharing* über die betroffene IP-Adresse ermittelt werden soll, ist eine zutreffende Auskunft des ISP nicht einmal mehr dann gesichert, wenn der betroffene Zeitpunkt eine Sekunde lang ist und der ISP seine Auskunft auch für diese Sekunde erteilen kann. Denn bereits innerhalb dieser Sekunde könnte die IP-Adresse neu vergeben worden sein.[329] Dieser Fall mag noch unwahrscheinlich erscheinen, ausgeschlossen ist er jedoch nicht. Ohnehin aber fallen der Zeitpunkt, für den Auskunft gegeben wird und der Zeitpunkt, der ermittelt wurde, regelmäßig auseinander. Dann ist die Neuvergabe schon wahrscheinlicher. Dass eine Neuvergabe ausgeschlossen erscheint, kann mithin nur durch eine Mehrfachermittlung bejaht werden.[330]

cc) Missbräuchliche Verwendung der IP-Adresse

Als *IP spoofing* bezeichnet man den Vorgang, bei dem jemand den Datenverkehr aus seinem Netzwerk mit der IP-Adresse eines anderen Netzwerks tarnt, sodass es von außen so erscheint, als käme der Datenverkehr aus Letzterem.[331] Möglich ist dies auf Grund des Routing-Mechanismus im Rahmen der Internetzwerkschicht, da die einzelnen *hops* nicht die Authentizität der IP-Adresse eines Datagramms verifizieren können.[332]

Nach Auffassung des OLG Köln sei IP *spoofing* in *filesharing*-Systemen ausgeschlossen.[333] Das ist nachweislich falsch. In einer wissenschaftlichen Untersuchung aus den USA wurde mittels – absichtlich zu diesem Zweck betriebe-

[327] Siehe beispielsweise LG Stuttgart, Urteil vom 28. Juni 2011, Az. 17 O 39/11, Rz. 24 – juris; AG Frankenthal, Urteil vom 24. April 2015, Az. 3a C 253/14, Rz. 54 – juris.

[328] Siehe oben Kapitel § 1 IV. 2. a).

[329] *Gietl/Mantz*, CR 2008, 810, 815.

[330] Siehe hierzu Kapitel § 5 III. 2.

[331] *Forouzan*, TCP/IP protocol suite, S. 210f.

[332] *Mathew/Cheshire*, Risky Business: Social Trust and Community in the Practice of Cybersecurity for Internet Infrastructure, S. 2341, 2343.

[333] OLG Köln, Beschluss vom 22. November 2012, Az. 6 W 217/12 – waldorf-frommer.de

nen – IP *spoofing* erreicht, dass die durchführenden Forscher hunderte *DMCA takedown notices*[334] erhielten, deren Basis die „gespooften" IP-Adressen waren – über diejenigen Geräte, die tatsächlich originär im Internet mit diesen Adressen kommunizierten, wurde jedoch erwiesenermaßen gar kein *filesharing* betrieben.[335]

IP spoofing verbleibt auch nach gegenwärtigem Forschungsstand ein nach wie vor nicht vollständig gelöstes Problem.[336] Belastbare Zahlen dazu, wie häufig im Rahmen von *filesharing*-System „gespoofte" IP-Adressen vorhanden sind, existieren nicht und lassen sich wohl auch nicht ermitteln.[337] Jedenfalls ist ein beachtlicher Anteil an IP-Adressen generell tauglich dafür, „gespooft" zu werden, d.h. er ist nicht durch Sicherungsmaßnahmen geschützt.[338]

dd) Fehlende Informationen in den Ermittlungsergebnissen

Schlussendlich ist auch der Aussagewert einer zuverlässigen, aktiven und auch im Übrigen fehlerlosen Ermittlung begrenzt. In der Regel weisen Ermittlungsdienste die Teilnahme eines BitTorrent-Nutzers an einem Schwarm nur im Umfang von wenigen Sekunden nach. Auf Grund des *tit-for-tat*-Mechanismus[339] ist vom gegenwärtigen Erkenntnisstand her auch davon auszugehen, dass eine weitergehende Ermittlung – zum Beispiel dahingehend, wie lange ein Nutzer ab Ermittlungsbeginn insgesamt im Schwarm verbleibt – nicht möglich ist. Offen ist lediglich, ob Ermittlungsdienste bewusst nach wenigen Sekunden abbrechen oder eine einmal hergestellte Verbindung zumindest solange aufrecht erhalten, wie das System erlaubt. Ist Ersteres der Fall, bestünden in der Praxis jedenfalls noch Möglichkeiten, die Ermittlung zu verbessern.

Weiterhin ist nicht davon auszugehen, dass für die ermittelte Dauer der Teilnahme am Schwarm der Umfang der Download- und Uploadaktivität des ermittelten Nutzers feststellbar ist, da der Ermittler keinen Einblick in die

[334] Vereinfacht gesagt ein ähnliches Instrument wie die Abmahnung in Deutschland.

[335] *Piatek/Kohno/Krishnamurthy*, Challenges and Directions for Monitoring P2P File Sharing Networks - or: Why My Printer Received a DMCA Takedown Notice, S. 1, 3.

[336] *Ehrenkranz/Li*, ACM Trans. Internet Technol., Nr. 2, Bd. 9, 2009, S. 1, 26; *Baker* et al., Addressing the challenge of IP spoofing, S. 1, 2.

[337] *Leicht*, VuR 2009, 346, 349.

[338] https://spoofer.caida.org/summary.php - Zugriff am 31.03.2021.

[339] Siehe hierzu Kapitel § 1 II. 5. c).

sonstigen Verbindungen hat, die das System zwischen dem ermittelten Nutzer und anderen Nutzern herstellt. Es lassen sich bei BitTorrent allerdings zumindest aus dem *bitfield* bestimmte Annahmen ableiten. Stellen zwei Nutzer eine Verbindung her, teilen sich diese gegenseitig ihr *bitfield* mit, d.h. eine Liste von den *pieces* der vollständigen Datei, die gegenwärtig bei den jeweiligen Nutzern vorhanden sind.[340] Aus dem *bitfield* lässt sich also ableiten, ob der ermittelte Nutzer bereits die vollständige Datei hat oder welchen Bruchteil hiervon. Da in BitTorrent nach bisherigen Erkenntnissen der Upload einer bestimmten Dateimenge ungefähr doppelt soviel Zeit in Anspruch nimmt wie deren Download[341], kann also als dem *bitfield* die hochgeladene Menge an Dateien geschätzt werden[342], auch wenn die Empfänger weiterhin unbekannt bleiben. Ist das *bitfield* vollständig, kann hieraus zudem gefolgert werden, dass der Nutzer kein *leecher* mehr ist, sonder bereits ein *seeder*.[343]

Nach Kenntnisstand des Verfassers ist es in Deutschland bisher nicht üblich, dass Ermittlungsdienste das *bitfield* ermitteln; zumindest wird es in Abmahnungen nicht angegeben.

ee) Zusammenfassung

Selbst also wenn man von einer zuverlässigen und aktiven Ermittlung ausgeht und eine Neuvergabe der ermittelten IP-Adresse ausschließt, verbleibt eine möglicherweise „gespoofte“ IP-Adresse als Fehlerquelle. Auch andere, unbekannte Fehlerquellen lassen sich nicht ausschließen.

Mithin ist es nicht verwunderlich, dass Praktiker von einer Fehlerquote von 1–2 Prozent ausgehen[344], d.h. von 100 Abmahnungen sind 1–2 deswegen unberechtigt, weil vom Anschluss des Abgemahnten ganz sicher keine *filesharing*-Aktivität ausgegangen ist. Auch das AG Köln ist der Überzeugung, dass Abmahnungen an Personen versandt wurden, die kein *filesharing* be-

340 *Hunter*, 31 J. Marshall J. Info. Tech. & Privacy L. 105, 110 (2014). Zwar ist es grundsätzlich möglich, das *bitfield* zu fälschen, siehe *Liogkas* et al., Exploiting BitTorrent For Fun (But Not Profit), S. 1, 3; es ist jedoch nicht davon auszugehen, dass der durchschnittliche BitTorrent-Nutzer hierzu fähig ist.

341 *Izal* et al., Dissecting BitTorrent: Five Months in a Torrent's Lifetime, S. 10.

342 Ist also eine Datei zum Beispiel 100 MB groß und weist das *bitfield* aus, dass die Hälfte aller *pieces* vorhanden sind, kann davon ausgegangen werden, dass der Nutzer 25 MB hochgeladen hat.

343 *Hunter*, 31 J. Marshall J. Info. Tech. & Privacy L. 105, 110 (2014).

344 *Stadler*, Filesharing: Wie zuverlässig ist die Ermittlung des Anschlussinhabers?

trieben haben.[345]

Somit ist im Ergebnis zu konstatieren, dass auch bei Anwendung größtmöglicher Sorgfalt im Rahmen der Ermittlung Fehler nicht vollständig ausgeschlossen sind. Zudem lässt sich der Ermittlungsvorgang im Nachhinein – d.h. im Prozess – nicht mehr rekonstruieren. Zuletzt weist auch eine fehlerlose Ermittlung Defizite hinsichtlich ihres Inhalts auf.

V. Überwachung und Prävention von *filesharing*-Nutzung

1. Übersicht

a) Überwachung

Überwachung heißt im Kontext dieser Arbeit die nachträgliche Zuordnung einer *filesharing*-Aktivität zu einem bestimmten Gerät und idealerweise einer bestimmten Person. Von Interesse ist im Rahmen dieser Arbeit dabei nur, welche technischen Möglichkeiten dem Inhaber eines Internetanschlusses zur Verfügung stehen, d.h. inwieweit er feststellen kann, ob eine *filesharing*-Aktivität von einem bestimmten Gerät ausgeht bzw. ausging, das zum Zugriff auf das Internet über seinen Anschluss verwendet wurde.

b) Prävention

Prävention bedeutet im Kontext dieser Arbeit, welche technischen Möglichkeiten zur Verfügung stehen, *filesharing*-Aktivitäten generell zu verhindern oder einzudämmen oder den Fortgang gerade stattfindender *filesharing*-Aktivitäten abzustellen. Präventive Maßnahmen können an der Internetzwerk-, Transport- und Anwendungsschicht ansetzen.[346]

Typische Präventionsmaßnahmen sind *IP-Sperren*, *Port-Sperren*, *DNS-Sperren*, *URL-Sperren* sowie *Traffic-Drosselungen / Datenmengenbegrenzungen*. Diese kommen vor allem auf Ebene des Anschlussinhabers und des ISP in Betracht. Zu den Präventionsmöglichkeiten anderer Akteure siehe Kapitel § 1 V. 4.

[345] AG Köln, Hinweisbeschluss vom 22. Oktober 2014, Az. 125 C 410/14 – juris.
[346] Siehe zu den Schichten Kapitel § 1 I. 3. a).

aa) IP-Sperren

Mittels einer IP-Sperre werden Daten, die von einer bestimmten oder einer Gruppe von IP-Adressen eingehen oder an diese ausgehen sollen, blockiert.[347] Über die zu blockende bzw. die zu blockenden Adressen muss eine Auswahl getroffen werden, d.h. die Sperre „unerwünschter" Adressen kann nicht einfach automatisiert werden.

Webseiten sind in der Regel auf Servern gespeichert, denen eine statische IP-Adresse zugewiesen ist. Möglich ist aber auch für Server die dynamische Adressvergabe.[348] Bei Endkundenanschlüssen ist Letztere ohnehin üblich.[349] Ist das zu sperrende Ziel unter einer dynamisch vergebenen Adresse erreichbar, so muss die Sperre mit jeder Neuvergabe aktualisiert werden.

Und für den Anbieter einer Webseite muss auch die Blockierung der statischen IP-Adresse, unter der der Server, auf dem seine Webseite gespeichert ist, zu erreichen ist, kein großes Hindernis sein. Beispielsweise ermöglichte im Jahr 2012 *The Pirate Bay* den Zugang zu ihrer Webseite einfach unter einer zusätzlichen statischen IP-Adresse und machte somit auf einen Schlag mehrere Gerichtsurteile in verschiedenen Ländern, die dort jeweils ISPs aufgetragen hatten, die bisherige statische IP-Adresse, die zu der Webseite führte, für ihre Kunden zu blockieren, wirkungslos.[350]

IP-Sperren sind also bereits für den Dienst, der sich hinter einer gesperrten IP verbirgt, ohne größeren Aufwand auszuhebeln. Zudem können auch die Personen, die eine gesperrte IP-Adresse ansteuern möchten, die Sperre durch VPNs oder das Tor-Netzwerk[351] umgehen.[352]

Umgekehrt besteht sowohl bei der Sperre von statischen als auch – besonders – bei der Sperre von dynamischen IP-Adressen das Risiko des *overblocking*, also dass Unbeteiligte oder rechtmäßige Dienste betroffen sind.[353] Für beide Arten der Adressvergabe gilt: im Rahmen der IP-Sperre ist eine Differenzierung nach Art der Daten nicht möglich. Geblockt werden also alle Websei-

[347] https://en.wikipedia.org/wiki/IP_address_blocking - Zugriff am 31.03.2021.
[348] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 55.
[349] Siehe hierzu Kapitel § 1 IV. 2. a) und zu den Besonderheiten bei IPv6 Kapitel § 1 IV. 2. b).
[350] *Van Der Sar*, Pirate Bay Simplifies Circumvention of ISP Blockades.
[351] Siehe hierzu Kapitel § 1 IV. 6. b) cc).
[352] *Keßler*, Wie Netzsperren umgangen werden können.
[353] Zum rechtlichen Begriff des *overblocking* siehe Kapitel § 4 VIII. 3. e) bb).

ten und Dienste, die unter der oder den geblockten IP-Adressen angeboten werden.[354] Das Angebot mehrerer Webseiten unter der selben IP-Adresse ist möglich.[355] Bei dynamischen Adressen kommt hinzu, dass – wegen dem oben geschilderten Erfordernis der ständigen Aktualisierung – die Sperrung einer Adresse nicht zielführend ist, sondern ein ganzer Adressbereich gesperrt werden muss.

Hierzu ein Beispiel: denkbar wäre es, dass ein Ermittler, der einen BitTorrent-Schwarm überwacht, alle im Schwarm ermittelten IP-Adressen einem ISP mitteilt. Der ISP sperrt diese Adressen dann für seine Kunden. Diese können dann, sofern sie auch am Schwarm teilnehmen möchten, zunächst keine Verbindungen mit anderen Teilnehmern mehr herstellen. Dies ändert sich jedoch, sobald diese manuell oder automatisch eine neue IP-Adresse erlangen. Der Praktikabilität halber müsste der ISP also einen Adressbereich wählen, der die neu vergebenen Adressen mit einschließt. Dann könnten seine Kunden aber auch keine Verbindungen zu Nutzern aufbauen, die sich gar nicht am Schwarm beteiligen. Zudem wäre auch das Aufbauen einer Verbindung zu anderen Zwecken als dem *filesharing* mit keiner der gesperrten Adressen möglich.

Zusammengefasst sind IP-Sperren also technisch möglich, jedoch sowohl von Seiten des Zugreifenden als auch des Gesperrten leicht zu umgehen, müssen ständig aktualisiert werden und tragen – vor allem beim Sperren von Adressbereichen, aber auch schon bei der Sperre einzelner Adressen – das Risiko des *overblocking*, also einer inhaltlich überschießenden Sperrung, in sich.[356]

Sie sind daher allenfalls zur Sperrung statischer IP-Adressen praktikabel, um den Kunden eines ISP den Zugang zu den beispielsweise für das BitTorrent-System wichtigen Indexseiten und Trackern zumindest vorübergehend zu versperren.

bb) Port-Sperren

Bei Port-Sperren werden bestimmte Portnummern des TCP oder UDP generell gesperrt, sodass über diese kein Datenverkehr abgewickelt werden kann.

[354] *Murdoch/Anderson*, Tools and Technology of Internet Filtering, S. 57, 59.
[355] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 54f.
[356] Zum rechtlichen Begriff des *overblocking* siehe Kapitel § 4 VIII. 3. e) bb).

Für Anwendungen sind bestimmte Ports offiziell reserviert[357] oder werden inoffiziell durch diese verwendet.

Dem BitTorrent-System sind beispielsweise offiziell keine Portnummern zugewiesen. Es werden typischerweise die TCP-Nummern 6881-6900 verwendet, sowie für Tracker die TCP-Nummer 6969.[358] Im Rahmen der DHT werden verschiedene UDP-Nummern verwendet[359], die aber ebenfalls nicht offiziell zugewiesen sind.

Dass diese Portnummern typischerweise für BitTorrent benutzt werden, heißt nicht, dass keine Daten mehr über BitTorrent erlangt werden können, sobald diese Portnummern gesperrt sind. Denn der BitTorrent-Datenverkehr (und der anderer *filesharing*-Systeme) kann auch über andere Portnummern abgewickelt werden. Viele *filesharing*-Clients suchen sich im Falle einer Portsperre automatisch einen anderen Port, über den sie den Datenverkehr abwickeln oder lassen sich zumindest manuell so einrichten[360]; die manuelle Einrichtung ist auch für wenig versierte Nutzer ohne weiteres möglich.[361] Zudem sind Clients in der Lage, Ports zu benutzen, die eigentlich für andere Prozesse offiziell reserviert sind, beispielsweise TCP-Port 80, der eigentlich für HTTP reserviert ist.[362] Laut einer Untersuchung aus dem Jahr 2003 wickelten bereits damals mehrere *filesharing*-Systeme einen beträchtlichen Anteil ihres Datenverkehrs über zufällig ausgewählte oder eigentlich für andere Prozesse vorgesehene Ports ab.[363]

Letztlich können Portsperren also *filesharing* nur vollständig verhindern,

[357] Siehe oben Kapitel § 1 I. 3. a) cc).

[358] https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports - Zugriff am 31.03.2021.

[359] https://wiki.wireshark.org/BitTorrent - Zugriff am 31.03.2021.

[360] *Hofmeister*, Technische Durchführbarkeit der Blockierung von Filesharing-Diensten und Hindernisse bei der Beweisführung bei Urheberrechtsverletzungen, S. 3.

[361] http://www.easytins.com/2014/09/how-to-change-listening-port-on.html - Zugriff am 31.03.2021.

[362] *Hofmeister*, Technische Durchführbarkeit der Blockierung von Filesharing-Diensten und Hindernisse bei der Beweisführung bei Urheberrechtsverletzungen, S. 3; *Delaney*, Tunnelling Bittorrent Over Port 80 - How to Detect Activity on Your Network; zur technischen Funktionsweise *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 50.

[363] *Karagiannis* et al., File-sharing in the Internet: A characterization of P2P traffic in the backbone, S. 10f.; die dortige Angabe, dass BitTorrent nicht auf andere Ports ausweiche, ist mittlerweile veraltet.

wenn alle Ports gesperrt werden – dies käme praktisch allerdings einer Internet-Sperre gleich.[364]

Und selbst eine Begrenzung auf die beispielhaft genannten Ports könnte zu *overblocking* führen, da über BitTorrent auch rechtlich unbedenklicher Datenverkehr abgewickelt werden kann und abgewickelt wird.[365] Die technische Beratungsgruppe *BITAG*[366] empfiehlt, Portsperren sehr restriktiv einzusetzen bzw. so weit wie möglich zu vermeiden.[367] Bei der Verwendung des Begriffs *overblocking* muss im Rahmen von Portsperren jedoch umgekehrt darauf geachtet werden, dass keinen Anwendungen ein Blockier-Risiko zugeschrieben wird, bei denen ein solches gar nicht besteht. Beispielsweise wird darauf hingewiesen, dass auch legale Anwendungen wie Software-Updates von *Windows 10* über *filesharing* verteilt werden.[368] Das ist zunächst richtig. Jedoch gibt es wie dargestellt keinen allgemeinen *filesharing*-Port, sondern nur verschiedene, von *filesharing*-Protokollen genutzte Portnummern. *Microsoft* setzt für den erwähnten Update-Dienst ein eigenes Protokoll ein, das nicht die oben erwähnten (typischen) BitTorrent-Ports benutzt.[369] Damit soll das *overblocking*-Risiko jedoch nicht heruntergespielt werden; es ist auch dann groß genug, sofern beispielsweise nur die genannten typischen BitTorrent-Portnummern blockiert werden.

Während Portsperren bisher eher ein Nischendasein im juristischen Diskurs fristeten, steht zu erwarten, dass diese in Zukunft im Rampenlicht stehen werden, weil das 3. TMGÄndG in seiner Gesetzesbegründung Portsperren ausdrücklich als mögliche Sperrmaßnahme vorsieht.[370] Zudem hat das LG Düsseldorf die Störerhaftung eines Anschlussinhabers, der eine Tor-Exitnode[371] betrieben hatte, darauf gestützt, dass er keine Exit-Policy eingesetzt hätte, die BitTorrent sperrt, obwohl dies technisch angeblich möglich

364 *Hofmeister*, Technische Durchführbarkeit der Blockierung von Filesharing-Diensten und Hindernisse bei der Beweisführung bei Urheberrechtsverletzungen, S. 3.

365 Zum Verhältnis zwischen urheberrechtsverletzendem und nicht-verletzendem Verkehr siehe Kapitel § 3 II. 3.

366 https://icannwiki.org/BITAG - Zugriff am 31.03.2021.

367 *BITAG*, Port Blocking, S. 21ff.

368 Ausschussdrs. 18(9)1280, 23. Juni 2017, Stellungnahme Mantz, S. 10

369 https://www.wintotal.de/windows-10-p2p-update-verteilung-deaktivieren/ - Zugriff am 31.03.2021.

370 Siehe Kapitel § 4 VIII. 3. e) ff).

371 Siehe hierzu Kapitel § 1 IV. 6. b) cc).

gewesen wäre[372]; „Exit-Policy“ meint dabei nichts anderes als die Definition derjenigen Ports, die der Betreiber einer Exitnode für den Verkehr zwischen dem Tor-Netzwerk und dem offenen Internet sperrt bzw. offen lässt. Das LG Düsseldorf[373] gibt dabei als Belegstelle für die technische Möglichkeit einen Aufsatz aus der MMR an, der wiederum jedoch keine Belegstelle für die Behauptung, dass eine vollständige Blockierung möglich wäre, nennt.[374] Eine Belegstelle hätte sich zwar auf der Webseite des Tor-Projekts finden lassen; dort wird unter Berufung auf Einzelfälle angegeben, dass eine *Reduced Exit Policy*, also die Freigabe nur einiger weniger Ports, den BitTorrent-Verkehr über die entsprechen Exitnodes komplett geblockt hätte.[375] Allerdings kommen wissenschaftliche Untersuchungen zu dem Ergebnis, dass eine Exit-Policy, mithin Portsperren, egal welchen Umfangs den BitTorrent-Datenverkehr nur teilweise reduzieren kann.[376] Zudem ist hinsichtlich des geblockten BitTorrent-Datenverkehrs eine Differenzierung zwischen legalen und illegalen Inhalten bei Portsperren nicht möglich.

Zusammengefasst sind Portsperren also technisch möglich, können jedoch durch automatische oder manuelle Einstellungen im *filesharing*-Client umgangen werden und bergen, soweit sie nicht umgangen werden können, ein erhebliches *overblocking*-Risiko.

cc) DNS-Sperren

DNS-Sperren beziehen sich auf das *Domain Name System* (DNS). Das DNS ist ein Protokoll auf Ebene der Anwendungsschicht. Grund für seine Implementierung ist, dass IP-Adressen schwer zu merken sind. Ein weiteres Problem ist der Serverwechsel oder der Wechsel der IP-Adresse: speichert eine Firma oder ein Institut ihre Webseite auf einem neuen Server (ohne dabei die alte statische IP-Adresse für den neuen Server verwenden zu können) oder wechselt die statische IP-Adresse des Servers, wird sie von Personen auch dann nicht aufgefunden, wenn diese sich die alte Adresse merken konnten

[372] LG Düsseldorf, Urteil vom 13. Januar 2016, Az. 12 O 101/15, Rz. 27 – juris.

[373] Der BGH hat in der Revisionsentscheidung „Dead Island“ die Feststellungen des LG Düsseldorf zu Grunde gelegt, aber richtigerweise angedeutet, dass diese Feststellungen für andere Verfahren nicht zwingend sind, siehe BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 52 – GRUR 2018, 1044 - „Dead Island“.

[374] Vgl. *Thiesen*, MMR 2014, 803, 803.

[375] https://blog.torproject.org/tips-running-exit-node - Zugriff am 31.03.2021.

[376] *Hansen*, Analysis of Client Anonymity in the Tor Network, S. 27f.

oder gespeichert haben.[377]

Durch das DNS kann eine Webseite immer unter dem gleichen Namen erreicht werden, auch wenn sich die Ziel-IP-Adresse geändert hat. Beispielsweise wird die als *Domain* bezeichnete Adresse *www.ip.mpg.de* gegenwärtig zur IP-Adresse 193.174.132.100 aufgelöst. Ändert sich die IP-Adresse und wird dies vom Webseitenbetreiber entsprechend hinterlegt, kann auch die neue IP-Adresse unter derselben Domain erreicht werden.[378]

Die Auflösung einer Domain in eine IP-Adresse vollzieht sich vereinfacht dargestellt[379] in folgenden Schritten:

Wird in die Adresszeile eines Webbrowsers eine Domain eingegeben, wird eine auf diese Domain bezogene Anfrage an einen *DNS-Resolver* gesendet. Ein DNS-Resolver ist ein Programm, das für den Webbrowser die zur Auflösung benötigte Information, mithin die Ziel-IP-Adresse, aus dem DNS besorgt.[380] Typischerweise ist der Router eines Netzwerks so vorkonfiguriert, dass die Anfrage an den DNS-Resolver des für den betroffenen Anschluss zuständigen ISP gesendet wird.[381]

Sofern die richtige Auflösung der Domain auf Grund frührer Anfragen nicht in einem Cache zwischengespeichert ist[382], schickt der DNS-Resolver eine Anfrage an die hierarchisch oberste Stelle des DNS, die *Root-Zone*. Die Aufsicht über die Root-Zone hat die ICANN inne, die technische Verwaltung erfolgt durch den US-amerikanischen ISP *VeriSign*; die Root-Zone wird verteilt auf 13, zum Teil unterschiedlichen Organisationen zugehörigen, Server-Clustern betrieben, die sich überwiegend auf US-amerikanischem Staatsgebiet befinden.[383]

---

377 *Tanenbaum/ Wetherall*, Computer networks, S. 611.

378 Die Domain ist nicht mit der URL zu verwechseln, siehe hierzu sogleich Kapitel § 1 V. 1. b) dd).

379 Siehe eine umfangreichere Darstellung beispielsweise bei https://www.elektronik-kompendium.de/sites/net/0901141.htm - Zugriff am 31.03.2021 31.03.2021 und bei https://de.wikipedia.org/wiki/Domain_Name_System#Beispiel_Namensaufl.C3.B6sung - Zugriff am 31.03.2021.

380 https://www.elektronik-kompendium.de/sites/net/0901141.htm - Zugriff am 31.03.2021.

381 *Ng*, DNS Lookup: How a Domain Name is Translated to an IP Address.

382 *Karrenberg*, The Internet Domain Name System Explained for Non-Experts.

383 *Wander/ Boelmann/ Weis*, Domain Name System without Root Servers.

Die Root-Zone selbst kann keine Auskunft über die Ziel-IP-Adresse geben, sie kann jedoch auf den für die *Top Level Domain* (TLD) zuständigen *Nameserver* verweisen.[384] TLDs sind der hinterste Bestandteil einer Domain, also beispielsweise *.de* oder *.com*. Als *country code TLD* (ccTLD) werden TLDs bezeichnet, die für Staaten reserviert sind[385], also beispielsweise .de oder .at; als *generic TLD* werden TLDs bezeichnet, die nicht-staatlichen Akteuren zugewiesen sind, beispielsweise .com, .info, .org, .net oder .biz.[386].[387]

Die Nameserver für die .de-TLD zum Beispiel werden von der DENIC betrieben.[388] Die Root-Zone teilt dem DNS-Resolver also die IP-Adressen dieser Nameserver mit, wenn sich die Anfrage des DNS-Resolvers auf eine .de-Domain bezog. Die Ziel-IP-Adresse ist dann entweder in Nameservern der DENIC hinterlegt, d.h. der DNS-Resolver bekommt dann von diesen die Ziel-IP-Adresse mitgeteilt. Alternativ ist die Ziel-IP-Adresse wiederum auf einem Nameserver eines anderen Anbieters hinterlegt.[389] Dann verweisen die Nameserver der DENIC den DNS-Resolver auf diesen Nameserver (*subsidiärer Nameserver)*. Wurde die Ziel-IP-Adresse mitgeteilt, kann die Domain schlussendlich aufgelöst, der Ziel-Server angesteuert und die Ziel-Webseite aufgerufen werden.

Unter einer DNS-Sperre wird typischerweise – und auch in dieser Arbeit – die Sperre der Namensauflösung entweder auf Ebene des Routers beim Endkundenanschluss oder auf Ebene des DNS-Resolvers (und auf diese bezogen wiederum typischerweise nur solche bei ISPs) verstanden. Im ersteren Fall wird also die Domain-Anfrage nicht an den DNS-Resolver weitergeleitet, im letzteren Fall vom DNS-Resolver nicht aus dem Cache abgefragt und auch nicht an die Root-Zone weitergeleitet. Rein technisch ist eine Sperre der Namensauflösung auf Ebene der Root-Zone – soweit ersichtlich – nur für eine

384 *Ng*, DNS Lookup: How a Domain Name is Translated to an IP Address.

385 https://en.wikipedia.org/wiki/Country_code_top-level_domain - Zugriff am 31.03.2021.

386 https://en.wikipedia.org/wiki/Generic_top-level_domain - Zugriff am 31.03.2021.

387 Die *Second Level Domain* ist der Domain-Bestandteil nach der TLD (von rechts nach links gelesen), im obigen Beispiel also *mpg*. Die Bestandteile *ip* und *www* sind *Lower Level Domains*. Mit deren Auflösung ist die Root-Zone nicht befasst, folglich muss besagte Weiterleitung der Anfrage erfolgen.

388 https://www.denic.de/service/nameservice/ - Zugriff am 31.03.2021.

389 https://www.denic.de/domains/de-domains/registrierung/nameserver-und-nsentry-eintraege/ - Zugriff am 31.03.2021.

TLD insgesamt, nicht aber für eine spezifische Domain möglich; auf Ebene der Nameserver beispielsweise der DENIC oder subsidiärer Nameserver kann die Auflösung für eine spezifische Domain aber blockiert werden. Dies ist jedoch nicht mehr als DNS-Sperre zu bezeichnen.[390]

DNS-Sperren werden in der technischen Fachwelt eher kritisch gesehen. Die ICANN verweist darauf, dass DNS-Sperren technische Nachteile für das gesamte „Ökosystem“ des DNS haben können.[391] Konkret wird beispielsweise die mangelnde Kompatibilität mit Mechanismen, die einem Missbrauch des DNS vorbeugen sollen, angeführt.[392]

Auf Ebene des Endnutzers sind DNS-Sperren relativ leicht zu umgehen. Sollte die Sperre auf Ebene des DNS-Resolvers beim ISP erfolgen, kann der Endnutzer seinen Computer so konfigurieren, dass er einen anderen DNS-Resolver ansteuert (die es zahlreich gibt[393]).[394] Das LG Hamburg wies in einer Entscheidung exemplarisch darauf hin, dass es der Kammer ohne Vorkenntnisse gelungen sei, innerhalb weniger Minuten einen neuen DNS-Resolver zu konfigurieren.[395] Ist dem Endnutzer die Ziel-IP-Adresse bekannt, kann er diese auch direkt ohne Eingabe der Domain ansteuern (sofern die IP-Adresse nicht geblockt ist). Der von der DNS-Sperre betroffene Anbieter kann sich zudem ohne weiteres einfach eine neue Domain registrieren, die dann wieder gesperrt werden müsste.

Die Gefahr des *overblocking* ist überdies auch bei DNS-Sperren gegeben, da eine Webseite viele Ressourcen aufweisen kann (also Unterseiten und verschiedene, zum Download bestimmte Dateien), von denen nur ein Bruchteil rechtlich bedenklich ist; bei der Sperrung der Domain ist aber die gesamte Webseite nicht mehr erreichbar und damit sind auch die rechtlich unbedenklichen Teile gesperrt.[396]

---

390 Siehe zu Maßnahmen auf dieser Ebene Kapitel § 1 V. 4. c).

391 *SSAC*, DNS Blocking: Benefits Versus Harms, S. 5.

392 *CDT*, The Perils of Using the Domain Name System to Address Unlawful Internet Content, S. 3f.

393 https://www.lifewire.com/free-and-public-dns-servers-2626062 - Zugriff am 31.03.2021.

394 *Keßler*, Wie Netzsperren umgangen werden können.

395 LG Hamburg, Urteil vom 12. November 2008, Az. 308 O 548/08, Rz. 41 – juris.

396 *CDT*, The Perils of Using the Domain Name System to Address Unlawful Internet Content, S. 2f.

In Bezug auf das *filesharing* können DNS-Sperren nur den Zugang zu Indexseiten verhindern; die eigentliche Verbindung der Nutzer untereinander zum Datentausch findet mittels IP-Adressen statt und kann daher durch DNS-Sperren von vornherein nicht blockiert werden.

dd) URL-Sperren

Als *Uniform Resource Locator* (URL)[397] bezeichnet man eine Zeichenfolge, die auf eine eindeutige Ressource verweist.[398] Typischster Anwendungsfall von URLs sind Verweise auf *Hypertext-Dokumente*, also den Grundbaustein des WWW. Hypertext-Dokumente sind Dateien im *.html* oder *.htm*-Format, also Dateien, die Befehle der *Hypertext Markup Language* (HTML) enthalten (eine Auszeichnungssprache, die auf Darstellung von Texten, Bildern und sonstigen Darstellungsinhalten ausgelegt ist[399]). Über das Internet erreichbare Hypertext-Dokumente werden als Webseiten bezeichnet. Als Webseiten im Sinne dieser Arbeit sind alle Hyptertext-Dokumente eines einheitlichen Internetauftritts gemeint. Webseiten lassen sich untergliedern in Startseiten und von diesen aus über *Verlinkungen* erreichbare Unterseiten.

Beispielsweise löst die Eingabe der URL *www.uni-muenchen.de/index.html* in die Adresszeile eines Browsers zunächst den oben geschilderten Prozess der Namensauflösung auf, da Bestandteil der URL eine Domain ist. Wurde die Ziel-IP-Adresse aufgerufen, wird die konkrete Ressource *index.html* angesteuert, über das HTTPS übertragen und schließlich im Browser dargestellt. Letztere stellt zugleich die Startseite des Internetauftritts der LMU dar. Außerdem ist die Domain *www.uni-muenchen.de* so konfiguriert, dass nicht nur die Ziel-IP-Adresse des Servers, auf dem die Webseite der LMU gespeichert ist, angesteuert, sondern zugleich auch die Ressource *index.html* aufgerufen wird.[400]

Auf der Startseite der LMU wiederum finden sich Verlinkungen auf andere Ressourcen, mithin Unterseiten; beispielsweise wird über den Menüreiter *Über die LMU* die Ressource *https://www.uni-muenchen.de/ueber_die_*

[397] Typischerweise spricht man aber von der URL in der weiblichen Form, also *eine* URL.
[398] https://de.wikipedia.org/wiki/Uniform_Resource_Locator - Zugriff am 31.03.2021.
[399] https://de.wikipedia.org/wiki/Hypertext_Markup_Language - Zugriff am 31.03.2021.
[400] Die Domain verhindert also nicht nur, dass man sich eine bestimmte IP-Adresse merken muss, sondern auch, dass man sich eine bestimmte URL merken muss.

lmu/index.html aufgerufen.

Eine Sperre letzterer URL bewirkt also, dass nur die konkrete Ressource nicht mehr aufgerufen werden kann. Die Namensauflösung der Domain der LMU ist dann aber weiterhin möglich, ebenso wie das Aufrufen sämtlicher sonstiger Unterseiten. Mit URL-Sperren lässt sich also deutlich spezifischer als mit DNS-Sperren der Zugang zu bestimmten Inhalten sperren.

URL-Sperren sind technisch jedoch deutlich aufwendiger als IP-, Port- und DNS-Sperren. Das hängt mit dem gekapselten Aufbau der Pakete der Internetprotokollfamilie zusammen.[401] Es ist in der Infrastruktur des Internets normalerweise nicht vorgesehen, dass der Inhalt der Anwendungsschicht während des Transports – außer beispielsweise beim DNS – ausgelesen wird. Die Information eine URL betreffend ist aber in dieser Schicht enthalten. Um einem Paket zu entnehmen, ob es eine und wenn ja welche URL enthält, muss es also über einen *Proxyserver* geleitet werden[402], d.h. einen eigens zu diesem Zwecke eingerichteten Dienst.[403] Erst dort kann das Paket hinsichtlich seiner Anwendungsschicht ausgelesen werden.

Mit Verweis auf die englische Rechtsprechung findet sich in der deutschen juristischen Literatur die Auffassung, dass hierbei nur das Auslesen des HTTP-Headers, nicht aber der Payload erforderlich sei, da sich die Bezeichnung der URL im Header und nicht in der Payload befände.[404] Folglich reiche für URL-Sperren eine sogenannte *Shallow Packet Inspection* (SPI) statt der invasiveren[405] *Deep Packet Inspection*[406], bei der auch die Payload ausgelesen wird, aus.

Hierzu gibt es von englischer Seite eine gegenteilige Ansicht.[407] Demnach müsse für URL-Sperren sehr wohl die Payload der Anwendungsschicht mittels DPI analysiert werden. Aus dem mit dem HTTP befassten RFC 2616 lässt sich jedoch ableiten, dass die Auffassung in der deutschen juristischen

401 Siehe oben Kapitel § 1 II. 3. a).
402 *Leistner/Grisse*, GRUR 2015, 19, 24.
403 Siehe genauer zur Funktionsweise eines solchen Dienstes https://www.elektronik-kompendium.de/sites/net/1101221.htm - Zugriff am 31.03.2021.
404 *Leistner/Grisse*, GRUR 2015, 19, 24.
405 http://itlaw.wikia.com/wiki/Shallow_packet_inspection - Zugriff am 31.03.2021.
406 Siehe hierzu Kapitel § 1 V. 1. b) ee).
407 *Stalla-Bourdillon*, Cartier et al v Sky et al 2014: what if the ISPs' blocking systems did not implement Shallow Packet Inspection technologies?

Literatur zutreffend ist.[408]

Auf das *filesharing* bezogen lässt sich mit URL-Sperren lediglich erreichen, dass der Zugang zu Indexseiten gesperrt wird. Der Unterschied zu DNS-Sperren ist, dass sich spezifisch bestimmte Unterseiten einer Webseite sperren lassen. Der *filesharing*-Vorgang an sich lässt sich mit URL-Sperren nicht blockieren. Allerdings sind URL-Sperren für den Betreiber einer Webseite leicht auszuhebeln, da nur der Name der betroffenen HTML-Datei oder ihr Speicherverzeichnis geändert werden muss, um die Sperre wirkungslos zu machen.[409]

Zuletzt kommt noch ein weiterer Umstand hinzu: die Filterung einer URL lässt sich beim HTTPS, das seinen unverschlüsselten „Vorgänger" HTTP nach und nach ablöst[410] nur mit höherem Aufwand implementieren.[411] Entsprechende Filterprogramme existieren zwar, diese müssen aber vor dem Auslesen des Headers das entsprechende Datagramm erst entschlüsseln.[412] Der Betrieb einer solchen Filterung dürfte damit ungleich aufwändiger sein als die Filterung von bloßem HTTP-Verkehr.[413]

URL-Sperren sind mithin im Ergebnis von ihrer Wirkung her ähnlich wie DNS-Sperren, jedoch präziser und tragen damit ein geringeres *overblocking*-Risiko als Letztere. Sie können jedoch wie diese leicht umgangen werden und sind zudem – gerade wegen HTTPS – schwieriger zu implementieren.

ee) Traffic-Drosselung/Datenmengenbegrenzung

Als Trafficdrosselung oder Datenmengenbegrenzung[414] wird ein Vorgang bezeichnet, bei dem die Geschwindigkeit, mit der Daten durch eine Verbin-

[408] https://tools.ietf.org/html/rfc2616 - Zugriff am 31.03.2021 31.03.2021 ; siehe dort 4.5, 5.1.2 und 3.2.2. Möglicherweise basieren die unterschiedlichen Auffassungen auf einer terminologischen Verwirrung darüber, was mit DPI und SPI jeweils gemeint ist.

[409] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 54.

[410] Siehe https://en.wikipedia.org/wiki/HTTPS#Usage_in_websites - Zugriff am 31.03.2021 31.03.2021 , zum steigenden Nutzungsumfang.

[411] *Riordan*, The Liability of Internet Intermediaries, S. 472.

[412] Siehe beispielsweise https://github.com/e2guardian/e2guardian/wiki/MITM---Filtering-HTTPS - Zugriff am 31.03.2021.

[413] In der Praxis werden beispielsweise in Südkorea solche Filtermaßnahmen rechtmäßig durchgeführt, siehe *Van Der Sar*, South Korea Expands Site Blocking Efforts with SNI Eavesdropping.

[414] Im Fortgang der Arbeit wird nur noch der Begriff Datenmengenbegrenzung benutzt.

dung geleitet werden, gegenüber der eigentlich möglichen Geschwindigkeit verringert wird oder wenn die Menge aller Daten, die über eine Verbindung durchgeleitet werden kann, für bestimmte Zeitabschnitte kontingentiert ist; denkbar ist auch eine Kombination dieser beiden Arten der Datenmengenbegrenzung.

Soll nicht nach dem Inhalt der Daten differenziert werden, ist eine oder sind beide Arten der Datenmengenbegrentung technisch in der Regel ohne weiteres machbar. Anders ist es hingegen, wenn nach dem Inhalt der Daten differenziert werden soll. Auf *filesharing* bezogen würde eine Differenzierung bedeuten, dass entweder auf Ebene des ISP oder auf Ebene des Routers des Endkundenanschlusses *filesharing*-bezogene eingehende und ausgehende Daten nicht oder nur in begrenztem Umfang (also nur mit einer bestimmten Geschwindigkeit und/oder begrenzt auf eine bestimmte Datenmenge innerhalb eines definierten Zeitraums) weitergeleitet werden.

Um eine Datenmengenbegrenzung zu ermöglichen, die nicht unterschiedslos für alle Arten von Daten wirkt, sondern spezifisch auf *filesharing* abzielt, müssen Daten inhaltlich kategorisiert werden. Hierfür existieren verschiedene Methoden, insbesondere portbasierte, statistische und heuristische sowie Payload[415]-basierte.[416] Die Payload-basierte Methode wird als *Deep Packet Inspection* (DPI) bezeichnet.[417] DPI ist nach den hierzu verfügbaren Untersuchungen nicht nur die überwiegend eingesetzte Methode, sondern wird von ISPs auch benutzt, um BitTorrent-Datenverkehr zu blockieren.[418]

Die Einsicht in die Payload der Anwendungsschicht eines Datenpakets während seines Versandes ist nur mittels einer „Inspektion“ möglich, da in der Internetprotokollfamilie die Offenbarung der Payload – wie beim Postversand eines Briefes auch – erst beim Empfänger vorgesehen ist.[419] Da *filesharing*-Protokolle, und insbesondere das BitTorrent-Protokoll, nicht zu den Standard-Internetprotokollen gehören, reicht anders als bei URL-Sperren[420] die Analyse des Headers der Anwendungsschicht nicht aus, um ein Daten-

[415] Siehe zum Begriff *Payload* Kapitel § 1 I. 3. a) dd).
[416] *Bhatia/Rai*, Peer-to-Peer Networking and Applications, Nr. 5, Bd. 10, 2017, S. 1182, 1186ff.
[417] *Gomes* et al., ACM Computing Surveys, Nr. 3, Bd. 45, 2013, S. 1, 9.
[418] *Dischinger* et al., Detecting Bittorrent Blocking, S. 3, 6.
[419] Siehe Kapitel § 1 V. 1. b) dd).
[420] Siehe Siehe Kapitel § 1 V. 1. b) dd).

paket mit Sicherheit einem *filesharing*-Protokoll zuordnen zu können; daher genügt für diese Zuordnung eine SPI nicht, sonder es ist stattdessen eine DPI erforderlich.[421]

Im Ergebnis ist es technisch also zunächst problemlos möglich, Datenmengenbegrenzungen einzusetzen, sofern nicht nach dem Inhalt der Daten differenziert werden soll. Soll nach dem Inhalt differenziert werden, so ist die technisch aufwendige DPI einzusetzen.[422]

2. Möglichkeiten des Anschlussinhabers

a) Möglichkeiten der Überwachung

Zunächst ergibt sich aus den unterschiedlichen Betriebsarten eines WLAN[423] für die Möglichkeit der Überwachung kein Unterschied. Keine der Betriebsarten erlaubt für sich genommen den Rückschluss von einer *filesharing*-Aktivität auf ein bestimmtes Gerät. Typischerweise legen die meisten Router *Logfiles* an, aus denen hervorgeht, welche Geräte, d.h. welche MAC-Adressen, zu welcher Zeit mit dem Router verbunden waren. Der Abgleich des Logs mit dem beispielsweise in einer Abmahnung angegebenen Ermittlungszeitpunkts bietet dem Anschlussinhaber nur ein Indiz, da mehr als die Verbindung an sich nicht geloggt wird. Wird zudem das WLAN offen betrieben, könnte auch das Gerät einer dem Anschlussinhaber nicht bekannten Person als „Tatgerät" in Frage kommen. Auch im geschlossenen Betrieb ist der Rückschluss von einem Gerät auf eine Person nur dann möglich, wenn der Anschlussinhaber entweder weiß, welches Gerät welchem seiner von ihm zugelassenen Mitnutzer des Anschlusses gehört[424] oder jene ihm dies mitteilen. Einzig in dem Fall, in dem das WLAN als Hotspot betrieben wird, lässt sich einrichten, dass im Rahmen eines Log auch die Zuordnung der MAC-Adresse zu einer bestimmten Benutzerkennung und damit idealerweise zu einer bestimmten

421 *Zuozhi/ Yue/ Yunlang*, The Research of Protocol Identification Based on Traffic Analysis, S. 172, 173.

422 Siehe als Beispiel dafür, wie auf Ebene eines ISP die DPI in der Praxis eingesetzt wird High Court of Ireland, EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd, [2010] IEHC 377, Rz. 23ff. – bailii.org.

423 Siehe oben Kapitel § 1 IV. 3.

424 Beispielsweise weil er das WLAN so eingerichtet hat, dass nur vorher genehmigte MAC-Adressen sich mit dem Router verbinden können, siehe *Seemann*, WLAN-Gastzugang einrichten - so geht's.

Person möglich ist. Letztlich kann aber auch dies nicht absoluter Gewissheit sicherstellen, ob der konkrete Benutzer das *filesharing* betrieben hat, da auch eine andere Person als er selbst auf seine Nutzerdaten und das eingesetzte Gerät Zugriff gehabt haben könnte.

Zuletzt müsste auch zur Erhärtung der aus dem Log gewonnenen Indizien die einschlägigen Geräte forensisch untersucht werden. Aus der forensischen Untersuchung eines Geräts lässt sich im Nachhinein aber nicht zwingend ermitteln, ob von dem entsprechenden Gerät auch die in Frage stehende *filesharing*-Aktivität begangen wurde.[425]

Die einzige Möglichkeit, eine *filesharing*-Aktivität mit absoluter Gewissheit einem bestimmten Gerät zuzuordnen ist, den gesamten Datenverkehr, der über den Router abgewickelt wird, mitzuschneiden, mithin „abzuhören". Dies lässt sich technisch durch die Einrichtung eines *WLAN-Sniffers* bewerkstelligen.[426]

Die Zuordnung einer *filesharing*-Aktivität zu einer bestimmten Person ist aber auch in diesem Fall nicht möglich, wenn das betroffene Gerät von mehreren Personen benutzt wird oder benutzt werden konnte. Sofern auf dem betroffenen Gerät betriebssystemseitig Benutzerkonten eingerichtet wurden, kann aber die Benutzung eines bestimmten Benutzerkontos – sofern hierüber auf dem entsprechenden Gerät eine Logdatei angelegt wird – ein Indiz für den Täter liefern.

b) Möglichkeiten der Prävention

Hinsichtlich der Prävention gilt dasselbe wie für die Überwachung: die Art, wie das WLAN betrieben wird – ob offen, geschlossen oder als Hotspot –, hat auf die Prävention zunächst keinen Einfluss. Die Einrichtung eines Passworts oder ein Registrierungserfordernis per Benutzerkennung ändern nichts daran, dass nach erfolgter Passworteingabe oder Registrierung *filesharing* betrieben werden kann.

Von den erwähnten Präventionsmaßnahmen sind für den Anschlussinhaber IP-, Port- und DNS-Sperren an sich leicht zu ergreifen[427], da die zu blockie-

[425] Siehe oben Kapitel § 1 IV. 7. c) aa).

[426] https://www.pcwelt.de/ratgeber/So-entlarven-Sie-WLAN-Schnueffler-7685086.html - Zugriff am 31.03.2021.

[427] *Sassenberg/Mantz*, WLAN und Recht, Rz. 229ff.

renden IP-Adressen, Portnummern und Domainnamen typischerweise in eine Eingabemaske des Steuerungsmenüs des Routers eingegeben werden können[428]. Die im Router somit hinterlegten Sperrungen werden als *blacklist* bezeichnet. Auf Ebene des Endkundenanschlusses eingerichtete *blacklists* sind – soweit ersichtlich – nur sehr schwer zu umgehen, soweit kein VPN eingesetzt oder das Tor-Netzwerk benutzt wird.[429] Allerdings weisen nicht alle handelsüblichen Router die Funktion auf, eine *blacklist* anzulegen oder weisen eine mengenmäßige Begrenzung der möglichen Einträge auf.[430]

Die Sperrung von einschlägigen Ports auf Ebene des Routers ist von vornherein nicht geeignet, *filesharing* zu verhindern, wenn hierzu eine *seedbox* verwendet wird.[431] Denn bei einer *seedbox* läuft der BitTorrent-Datenverkehr auf einem externen Server; nur die vollständige Datei wird anschließend – regelmäßig über HTTP, also TCP-Port 80 – heruntergeladen. Mithin fehlt es an einem technischen Berührungspunkt mit typischen *filesharing*-Portnummern. Auch wenn *filesharing* direkt über einen Anschluss betrieben werden soll, an dem entsprechende Ports gesperrt sind, hindert Letzteres den *filesharing*-Vorgang in aller Regel nicht.[432]

Einen ähnlichen Effekt wie Portsperren haben *Software-Firewalls*, also Programme, die dem Gerät, auf dem sie installiert sind, Verkehr auf bestimmten Ports nicht erlauben.[433] Da sie aber auf einem Gerät zunächst installiert werden müssen, erscheinen sie für den Anschlussinhaber noch weniger zielführend als die anderen Sperrmechanismen, da das für ihn relevante *filesharing* in der Regel von einem anderen Gerät als seinem eigenen betrieben wird, und bleiben daher im Rahmen dieser Arbeit weitgehend außer Betracht; ohnehin wären sie technisch auch nicht effektiver als Portsperren.

URL-Sperren und die Begrenzung oder Blockierung von *filesharing*-Daten erfordern den Einsatz von Filter-Technologien (SPI, DPI) und daher speziell hierauf ausgerichtete Router mit wiederum speziell hierfür ausgerichteter und

[428] Siehe als Beispiel für Domainsperren http://praxistipps.chip.de/router-blacklist-zugriff-auf-bestimmte-webseiten-sperren_35684 - Zugriff am 31.03.2021.

[429] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access-Provider, S. 54f.

[430] *Sesing/Baumann*, MMR 2017, 583, 588.

[431] *Alcock/Nelson*, Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users, S. 551, 554.

[432] Siehe Kapitel § 1 V. 1. b) bb).

[433] *Sassenberg/Mantz*, WLAN und Recht, Rz. 230.

konfigurierter Software.[434] Die Implementierung solcher Maßnahmen dürfte daher die Fähigkeiten und Möglichkeiten von Anschlussinhabern im privaten Bereich oder im Kleingewerbe regelmäßig übersteigen.

Datenmengenbegrenzungen, die allgemein wirken, dürften regelmäßig auch auf handelsüblichen Routern und ohne besondere IT-Kenntnisse implementierbar sein, nicht jedoch Datenmengenbegrenzungen, die nur betreffend bestimmter Personen bzw. bestimmter Geräte greifen.[435]

3. Möglichkeiten des ISP

Während bei Routern auf Ebene des Endkundenanschlusses die Einrichtung der genannten Präventivmaßnahmen nicht zwingend möglich sein muss oder nur in begrenztem Umfang möglich sein kann (je nach Router-Modell), können auf Ebene des ISP alle der genannten Präventionsmaßnahmen ergriffen werden, wie sich betreffend IP-, DNS- und URL-Sperren der Entscheidung „Störerhaftung des Access-Providers“ des BGH entnehmen lässt.[436] Weiterhin können ISPs auch Portsperren sowie Daten(mengen)begrenzungen mittels DPI vornehmen.[437]

Die Ausführungen zur Wirksamkeit von Portsperren und die Möglichkeiten der Umgehung der übrigen Sperrmaßnahmen gelten aber auch im Verhältnis zu ISPs.

4. Möglichkeiten anderer Akteure

a) ICANN und RIRs

ICANN und RIRs können keine der genannten oder andere Präventivmaßnahmen implementieren.

IP-Sperren sind für diese Akteure nicht möglich, weil sie nur IP-Adressblöcke vergeben, nicht aber einzelne IP-Adressen einem Endkundenanschluss zuordnen; dies tun erst ISPs. Theoretisch könnten ICANN und RIRs die Vergabe

[434] Vgl. *Patterson*, Deep packet inspection: The smart person's guide.
[435] *Mantz*, GRUR 2017, 969, 974.
[436] BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 61 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“. In Rz. 68 wird auch ausgeführt, dass URL-Sperren eine Analyse des Datenverkehrs erfordern.
[437] *Dischinger* et al., Detecting Bittorrent Blocking, S. 3, 6.

bestimmter Blöcke verweigern, würden damit aber ganze geographische Regionen vom Internet abschneiden.

Port-Sperren, URL-Sperren und andere Präventivmaßnahmen mittels DPI sind ihnen ebenfalls nicht möglich, da sie keinen Datenverkehr im Internet befördern. Die ICANN könnte lediglich im Rahmen der Ausübung der IANA-Funktion bestimmte Ports nicht reservieren oder Reservierungen rückgängig machen.[438] Dies würde aber nichts daran ändern, dass über die betroffenen Ports dennoch von jeder Anwendung Datenverkehr abgewickelt werden könnte.[439]

RIRs können DNS-Sperren schon deswegen nicht umsetzen, weil sie keine Funktionen im DNS übernehmen. Die ICANN verwaltet zwar die Root-Zone; auf Ebene der Root-Zone können aber nur TLDs generell gesperrt werden, nicht spezifische Domains (also auch nicht konkrete Second- und Lower Level Domains).[440]

Im Ergebnis haben die ICANN und RIRs keine technischen[441] Möglichkeiten, präventiv gegen *filesharing* tätig zu werden.

b) Alternative DNS-Resolver

Wie in Kapitel § 1 V. 1. b) cc) erwähnt, werden DNS-Resolver nicht nur von ISPs betrieben, sondern auch von anderen Akteuren angeboten. Rein technisch wäre es denkbar, dass auch diese die Namensauflösung für spezifische Domains sperren. 2020 hat in Deutschland erstmals das LG Köln die Möglichkeit der Störerhaftung eines alternativen DNS-Resolvers angenommen.[442]

c) Registries, Registrare und subsidiäre Nameserver

Als *Registry* bezeichnet man im DNS den Verwalter einer oder mehrerer TLDs. Wie bereits in Kapitel § 1 V. 1. b) cc) erwähnt, verwaltet beispielsweise die DENIC die .de-TLD.

438 Siehe hierzu RFC 6335 8.1 und 8.2
439 Siehe Kapitel § 1 V. 1. b) bb).
440 Siehe Kapitel § 1 V. 1. b) cc).
441 Zu den rechtlichen siehe *Bridy*, 74 J. Wash. & Lee L. Rev. 1345, 1359ff. (2017).
442 LG Köln, Urteil vom 30. Januar 2020, Az. 14 O 171/19, Rz. 9, 118ff. – GRUR-RS 2020, 1797.

Registries können aber die Zuständigkeit für die Registrierung und Abrechnung einer Domain auch delegieren. Die Delegaten bezeichnet man als *Registrare*.[443] Die DENIC nimmt diese Tätigkeit sowohl selbst wahr[444] als auch durch Registrare[445].

Möchte ein Rechteinhaber gegen eine Domain vorgehen, beispielsweise weil unter der Domain eine BitTorrent-Indexseite erreichbar ist, können ihm DNS-Sperren unzureichend erschienen, da diese lediglich die Namensauflösung der Domain nur für die Nutzer der Endkundenanschlüsse, in deren Router eine DNS-Sperre eingerichtet ist und nur für die Kunden derjenigen ISPs, die in ihren DNS-Resolvern entsprechende Einträge gemacht haben, verhindern. Dies ändert nichts an der generellen Erreichbarkeit der Domain. Nun könnte er versuchen, über eine WHOIS-Abfrage den Inhaber der Domain in Erfahrung zu bringen und direkt gegen diesen vorzugehen. Dies kann sich aber aus praktischen Gründen schwierig gestalten oder WHOIS-Einträge sind nicht vorhanden oder der Inhaber ist durch einen Service für *WHOIS privacy* geschützt.[446]

Der Rechteinhaber könnte dann in Betracht ziehen, gegen die Registry

443 *Haertel*, Registry, Registrar, Registrant: Die große Domainbegriffssammlung Teil 3.

444 https://www.denic.de/domains/de-domains/registrierung/ - Zugriff am 31.03.2021.

445 Eine Liste findet sich auf https://www.denic.de/ueber-denic/mitglieder/liste/ - Zugriff am 31.03.2021.

446 Mit einer WHOIS-Anfrage können Informationen über den Inhaber einer Domain wie Name und Anschrift erfragt werden, siehe https://de.wikipedia.org/wiki/Whois - Zugriff am 31.03.2021. Die ICANN schreibt in ihren Verträgen mit Registries vor, dass diese Daten erhoben und zum öffentlichen Abruf bereit gehalten werden müssen. Im Zuge des Inkrafttretens der DS-GVO ist dies nunmehr allerdings nur noch eingeschränkt möglich, vgl. https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf - Zugriff am 31.03.2021. Insbesondere hat die ICANN keinen rechtlichen Anspruch auf Einhaltung ihrer Vertragsbedingungen, da die Regeln der DS-GVO insoweit vorgehen, siehe LG Bonn, Beschluss vom 29. Mai 2018, Az. 10 O 171/18 – juris; bestätigt durch OLG Köln, Beschluss vom 3. September 2018, Az. 19 W 32/18 – juris. Wie es mit dem WHOIS in Zukunft weitergehen wird, ist noch unklar. Aber schon vor Inkrafttreten der DS-GVO war es häufig schwierig, den Inhaber einer Domain in Erfahrung zu bringen, da viele TLDs *WHOIS privacy* erlaubten, d.h. als Inhaber der Domain konnte ein Strohmann eingetragen werden, vgl. https://en.wikipedia.org/wiki/Domain_privacy - Zugriff am 31.03.2021. Allerdings ist auch gegen Anbieter solcher Dienste ein gerichtliches Vorgehen denkbar; siehe als Beispiel *Van Der Sar*, RIAA Orders WhoisGuard to Identify Torrent Site Owner.

und/oder – soweit vorhanden – den Registrar vorzugehen. Da Indexseiten typischerweise nicht unter .de-Domains betrieben werden[447], ist aus deutscher Perspektive insbesondere das Vorgehen gegen Registrare auf deutschem Boden interessant. Beispielsweise verurteilte das LG Saarbrücken[448], einen in Deutschland ansässigen Registrar, der unter anderem .com-Domains „vertreibt", dazu, die Domain *h33t.com*[449] eines seiner Kunden zu dekonnektieren; ein neueres Beispiel aus der Rechtsprechung ist ein Urteil des LG Köln, mit dem ein Registrar verpflichtet wurde, mehrere Domians von *The Pirate Bay* zu dekonnektieren.[450] Die grundsätzliche Störerhaftung des Registrars ist mittlerweile vom BGH bestätigt worden.[451]

Mit Dekonnektierung ist gemeint, dass der Registrar eine DNS-Anfrage nicht mehr auf den Nameserver[452], den sein Kunde angegeben hat, verweist.[453] Damit führen DNS-Anfragen, egal von welchem DNS-Resolver aus sie kommen, nicht mehr zum Ziel, d.h. eine Namensauflösung kann global nicht mehr erfolgen.[454]

Stichwort Nameserver: Sie sind zwar letztes Glied in der Kette der Namensauflösung, aber ein Hindernis an dieser Stelle verhindert eine Namensauflösung zunächst ebenso global wie eine Dekonnektierung bei der Registry oder dem Registrar, auch wenn der Domaininhaber natürlich einen neuen Nameserver angeben kann, sofern er die Inhaberschaft der Domain behalten hat.

Besonders interessant sind in diesem Zusammenhang die Anbieter *verteilter*

[447] Im internationalen Vergleich wird hierfür (und für andere strukturell urheberrechtsverletzende Angebote) regelmäßig die .to-Domain verwendet. Deren Registry sieht sich in neuerer Zeit daher häufiger Auskunftsbegehren ausgesetzt, siehe *Maxwell*, ACE Obtains DMCA Subpoena to Unmask Operators of Major Pirate Sites.

[448] LG Saarbrücken, Urteil vom 15. Januar 2014, Az. 7 O 82/13 – juris. Bestätigt durch OLG Saarbrücken, Urteil vom 22. Oktober 2014, Az. 1 U 25/14 – MMR 2015, 120.

[449] Die Domain einer früher sehr bekannten BitTorrent-Indexseite.

[450] LG Köln, Urteil vom 5. Dezember 2017, Az. 14 O 125/16 – juris. Bestätigt durch OLG Köln, Urteil vom 31. August 2018, Az. 6 U 4/18 – juris.

[451] BGH, Urteil vom 15. Oktober 2020, Az. I ZR 13/19 – GRUR 2021, 63 - „Störerhaftung des Registrars".

[452] Siehe hierzu Kapitel § 1 V. 1. b) cc).

[453] https://de.wikipedia.org/wiki/Domain-Registrierung#Konnektierung - Zugriff am 31.03.2021.

[454] *Murdoch/Anderson*, Tools and Technology of Internet Filtering, S. 64.

Nameserver wie *Cloudflare*.[455] Hoch frequentierte Seiten benötigen für eine zuverlässige und stabile Erreichbarkeit ihrer Seiten einen solchen Dienst, um die mit einer hohen Zahl von Seitenzugriffen verbundene Nutzlast zu „managen". Da die Anzahl der Anbieter solcher Nameserver nicht unbegrenzt ist, deren Dienste aber für hoch frequentierte Seiten notwendig sind, bietet sich hier für Rechteinhaber ein attraktiver Angriffspunkt. Folglich wird auch gegenwärtig in US-amerikanischen Gerichtsverfahren von *Cloudflare* verlangt, unter anderen der Indexseite *The Pirate Bay* keinen verteilten Nameserver anzubieten.[456] 2020 wurde der Dienst zudem in einem einstweiligen Verfügungsverfahren erstmals in Deutschland erfolgreich auf Grundlage der Störerhaftung dahingehend in Anspruch genommen, bestimmten Indexseiten seine Nameserver-Dienste nicht mehr anzubieten.[457]

d) .onion-Domains und Tor-Proxies

.onion-Domains sind Adressen, die auf sogenannte *hidden services* innerhalb des Tor-Netzwerkes[458] verweisen. Ein *hidden service* kann auch eine Webseite sein. Als sogenannte *Special Use*-TLDs sind .onion-Domains nicht Teil des DNS. Reguläre Webbrowser können eine entsprechende Adresse daher nicht auflösen.[459] Beispielsweise bietet *Facebook* einen Zugriff auf seine Dienste unter der Adresse *facebookcorewwwi.onion* an. Die Ansteuerung der Webseite gelingt aber grundsätzlich nur, wenn man die Adresse in die Adresszeile eines Browsers eingibt, der für das Tor-Netzwerk ausgelegt ist.[460]

Da sie nicht Teil des DNS sind, können .onion-Domains auch nicht durch Maßnahmen wie DNS-Sperren und Dekonnektierung erreicht werden. Diesen Umstand machen sich natürlich Indexseiten wie *The Pirate Bay* zu Nutze und unterhalten .onion-Domains.

Ein gezielter Zugriff auf .onion-Domains ist also nicht möglich, daher verbleibt für Anschlussinhaber und ISPs nur die Blockierung des gesamten Tor-

[455] https://de.wikipedia.org/wiki/Cloudflare#Domain_Name_Server - Zugriff am 31.03.2021.

[456] *Van Der Sar*, Cloudflare Faces Lawsuit For Assisting Pirate Sites.

[457] LG Köln, Urteil vom 30. Januar 2020, Az. 14 O 171/19 – GRUR-RS 2020, 1797.

[458] Siehe hierzu Kapitel § 1 IV. 6. b) cc).

[459] *McCarthy*, It's official: Tor's .onion domains must be kept off the public internet.

[460] Zum Beispiel https://www.torproject.org/projects/torbrowser.html.en - Zugriff am 31.03.2021.

Netzwerks durch Sperrung der IP-Adressen der Eintritts-und Austrittspunkte.

Nur wenig gezieltere Sperrungen sind bezüglich *Tor-Proxies* möglich. Solche Dienste ermöglichen den Zugriff auf .onion-Domains, ohne dass hierfür ein Tor-Browser erforderlich ist, beispielsweise die Webseite *http://onion.plus*. Fügt man der Eingabe einer .onion-Domain in die Adresszeile eines regulären Browsers also die TLD *.plus* hinzu, wird die Webseite aus dem Tor-Netzwerk in diesem Browser angezeigt. Da DNS-Resolver aber bei der Namensauflösung nur bis zum Adressteil *onion.plus* beteiligt sind, kann eine DNS-Sperre sich nur auf die Webseite *onion.plus* insgesamt beziehen; gleiches gilt für eine Dekonnektierung.

Der Zugriff auf .onion-Domains kann daher im Ergebnis nur durch erhebliches *overblocking* vereitelt werden.

Anders als zum Teil noch landläufige Meinung, können jedoch die *hidden services* selbst mittlerweile enttarnt und abgeschaltet werden, wie das Beispiel des Dienstes *Silk Road* zeigt.[461] Der materielle Aufwand ist gegenüber dem Abschalten von Diensten im „offenen“ Internet gegenwärtig freilich noch ungleich höher.

e) Suchmaschinen und sonstige Suchhilfen

Mit Suchmaschinen lassen sich Indexseiten auffinden, aber auch konkrete Verweise auf .torrent-Dateien und *magnet links*.[462] Marktbeherrscher *Google* sieht sich daher immer wieder mit *DMCA takedown requests* konfrontiert, beispielsweise wurden Ende 2017 über drei Milliarden URLs moniert (wobei jedoch davon nur ein Teil BitTorrent-Indexseiten betroffen haben dürfte).[463] Rechteinhaber beklagen allerdings, dass dieser Prozess letztlich zwecklos sei, da die entfernten Inhalte in neuem Gewand wieder in den Suchergebnissen auftauchen. Google sieht sich technisch nicht dazu in der Lage, hierauf automatisch zu reagieren.[464] Die Entfernung von nicht-spezifisch verletzenden Inhalten wie beispielsweise Domains von Indexseiten generell (die zunächst

[461] *Feilner*, iX, Bd. 7, 2017, S. 86, 87.
[462] Siehe hierzu *Greenberg*, Why Google Is The New Pirate Bay
[463] *Van Der Sar*, Google Asked to Remove 3 Billion „Pirate“ Search Results.
[464] *Van Der Sar*, Google Says It Can't Filter Pirated Content Proactively.

nur auf die Startseite der Indexseite führen), verweigert Google.[465]

Als sonstige Suchhilfen sind zum einen Webseiten zu bezeichnen, die auf Indexseiten verlinken. Beispielsweise stellt der *filesharing*-Blog *torrentfreak.com* regelmäßig die wichtigsten aktuellen Indexseiten für BitTorrent vor.[466] Sonstige Suchhilfen sind zum anderen Metasuchmaschinen. Zum Beispiel kann über die Webseite *torrentz2.eu* auf mehreren BitTorrent-Indexseiten gleichzeitig nach einem bestimmten Werk gesucht und das Suchergebnis einheitlich auf einer Seite wiedergegeben werden, sodass eine Suche nach und auf den einzelnen Indexseiten erspart bleibt.

Suchmaschinen und sonstige Suchhilfen sind somit als Einstiegstor in das *filesharing* enorm wichtig, da ohne sie zumindest Indexseiten und auch konkrete *magnet links* oder .torrent-Container schwerer aufzufinden wären.

f) Hostserver

Wie unter Kapitel § 1 II. 6. dargestellt, kommt kein *filesharing*-System ohne eine zentrale Instanz aus. Bei BitTorrent sind dies beispielsweise in seiner klassischen Funktion Indexseiten und Tracker; in der DHT sind zentrale Anlaufstellen für das *bootstrapping* nötig.[467] Alle diese Dienste müssen also auf irgendeinem Server gespeichert sein. Solche Server sind als *Hostserver* zu bezeichnen.

Zunächst kann es sein, dass dem Anbieter des Dienstes der Server selbst gehört. Dann ist der Hostserver kein eigenständiger Akteur, gegen den vorgegangen werden könnte. Sehr häufig aber werden Hostserver angemietet, um die Dienste darauf zu betreiben. Der Fremdanbieter hat es dann in der Hand, diese Dienste von seinen Hostservern zu entfernen. Beispielsweise erreichte es der *Bundesverband der Musikindustrie*, einen Anbieter von Hostservern dazu zu bewegen, einige BitTorrent-Tracker, die auf seinen Servern betrieben wurden, zu entfernen.[468] Indexseiten speichern ihre Inhalte mittlerweile weit überwiegend bei Fremdanbietern.[469]

---

[465] *Van Der Sar*, Google Categorically Refuses to Remove The Pirate Bay's Homepage.

[466] *Van Der Sar*, Top 10 Most Popular Torrent Sites of 2017.

[467] Siehe oben Kapitel § 1 II. 5. a) bb).

[468] http://www.urheberrecht.org/news/5408/ - Zugriff am 31.03.2021.

[469] *The Pirate Bay* beispielsweise speichert ihre Inhalte bei mehreren Anbietern verteilt, *Van Der Sar*, The Pirate Bay Runs on 21 „Raid-Proof" Virtual Machines.

Fallen Diensteanbieter-Eigenschaft und Inhaberschaft des Hostservers in einer Person zusammen oder erklärt sich der Anbieter eines Hostservers nicht bereit, den Dienst abzuschalten, kann der Dienst einfach durch physische Entfernung des Servers eingestellt werden.[470] Beispielsweise wurden beim polizeilichen Vorgehen gegen die Indexseite *The Pirate Bay* im Jahr 2006 die (damals noch in Eigenregie betriebenen) Hostserver beschlagnahmt und die Seite damit – wenn auch nur vorübergehend – abgeschaltet.[471]

g) Umgehungshilfen bei DNS-Sperren und Dekonnektierungen von Domains

Wie unter Kapitel § 1 V. 1. b) cc) erwähnt, sind DNS-Sperren wirkungslos, wenn demjenigen, der die betroffene Domain ansteuern wollte, stattdessen die Ziel-IP-Adresse des gewünschten Servers bekannt ist. Gleiches gilt für Domain-Dekonnektierungen: auch diese verhindern nicht, dass eine IP-Adresse direkt angesteuert werden kann. Als beispielsweise der Seite *Sci-Hub*, die wissenschaftliche Publikationen urheberrechtswidrig öffentlich zugänglich macht, nach einem Gerichtsurteil aus den USA von Seiten der zuständigen Registries gleich mehrere Domains dekonnektiert wurden, veröffentlichte der populäre Blog *torrentfreak.com* einfach die aktuellen IP-Adressen der Sci-Hub-Server.[472] Von *Sci-Hub* neu registrierte Domains sind auf der englischen Wikipedia gelistet[473] oder lassen sich über *Google* finden.

Um Domain-bezogene Eingriffe überhaupt einigermaßen wirksam zu machen, müssten also theoretisch auch solche Umgehungshilfen angegriffen werden.

h) TLS-Zertifizierungsstellen

Wie in Kapitel § 1 I. 3. a) dd) und Kapitel § 1 V. 1. b) dd) erläutert, ist das HTTPS eine verschlüsselte Version des HTTP und wird in zunehmenden Maße mehr als Letzteres verwendet. Die durchschnittlich am meisten frequentierten Webseiten benutzen allesamt HTTPS. Damit sichergestellt ist, dass eine Domain, die über HTTPS angesteuert wird, auch tatsächlich sicher

[470] *Murdoch/Anderson*, Tools and Technology of Internet Filtering, S. 64.
[471] https://en.wikipedia.org/wiki/The_Pirate_Bay_raid#Execution - Zugriff am 31.03.2021.
[472] *Van Der Sar*, Sci-Hub Loses Domain Names, But Remains Resilient.
[473] https://en.wikipedia.org/wiki/Sci-Hub - Zugriff am 31.03.2021.

ist, muss diese zertifiziert sein.[474] Da HTTPS für die Verschlüsselung das *Transport Layer Protocol* (TLS) verwendet, benötigt der Webseitenbetreiber also ein TLS-Zertifikat. Solche Zertifikate werden von Zertifizierungsstellen herausgegeben, die hierzu wiederum von Betriebssystem- und Webbrowserherstellern autorisiert wurden.[475] In Webbrowsern sind diese Zertifizierungsstellen vermerkt. Möchte der Benutzer eines Webbrowsers eine Domain mit HTTPS ansteuern und die Webseite kann kein Zertifikat eines der im Browser vermerkten Zertifizierungsstellen ausweisen, verweigern Webbrowser in der Regel das Ansteuern der Webseite.

Dieser Umstand kann dazu genutzt werden, Zertifizierungsstellen dazu zu bringen, für bestimmte Webseiten ein Zertifikat zu widerrufen. Beispielsweise wurde 2018 eine Zertifizierungsstelle gerichtlich dazu gezwungen, Zertifikate für einige der Domains der Webseite *Sci-Hub* zu widerrufen.[476] Jedoch konnte die Webseite umgehend Zertifikate von einer anderen Stelle erlangen (schon nach Stand 2013 gab es über 1600 Zertifizierungsstellen[477]). Theoretisch müsste also – sollten sich die Zertifizierungsstellen, auf die ausgewichen wurde, weigern, für die einschlägigen Webseiten die Zertifikate zu widerrufen und auch ein hierauf gerichtetes Gerichtsverfahren keinen Erfolg haben – erreicht werden, dass solchen Zertifizierungsstellen der Status als Zertifizierungsstelle entzogen wird.

Auf *filesharing* übertragen bedeutet dieser Komplex, dass Zertifizierungsstellen, die BitTorrent-Indexseiten (die HTTPS verwenden) zertifiziert haben, theoretisch dazu gebracht werden könnten, die entsprechenden Zertifikate zu widerrufen. Im Ergebnis wäre die Auswirkung hiervon ähnlich wie von DNS-Sperren und Domainkonnektierungen. Ein *filesharing*-Vorgang selbst kann hiermit nicht aufgehalten werden.

i) Routerseitige *blacklists*

Die von Seiten des Anschlussinhabers bisher vorgestellten Präventionsmöglichkeiten basieren darauf, dass er sie freiwillig oder auf Grund von Zwang implementiert, jedenfalls aber eigenhändig. Denkbar wäre stattdessen jedoch auch, dass in den für Endkundenanschlüsse verwendeten Routern werkseitig

[474] RFC 2818 Zif. 3.1.
[475] *Durumeric* et al., Analysis of the HTTPS Certificate Ecosystem, S. 291, 292.
[476] *Maxwell*, Sci-Hub 'Pirate Bay For Science' Security Certs Revoked by Comodo.
[477] *Durumeric* et al., Analysis of the HTTPS Certificate Ecosystem, S. 291.

bereits *blacklists* implementiert sind, die gegebenenfalls durch automatisierte Updates aktualisiert werden, der Anschlussinhaber also gar keine Wahl hat, welche IP-Adressen und/oder Domains gesperrt sind.

Rein technisch wäre es möglich, werkseitig bestimmte Konfigurationen vorzugeben. Dies spiegelt sich beispielsweise in Art. 3 Abs.3 lit. i) RL 2014/53/EU[478] wider, die vorschreibt, dass auf WLAN-Routern bestimmte Software werkseitig nicht installiert werden darf. Theoretisch ließe sich also auch umgekehrt festlegen, welche Konfigurationen ein Router positiv aufweisen muss.

Hinsichtlich des Inhalts der *blacklists* und dessen Aktualisierung könnte beispielsweise ein Modell übertragen werden, wie es gegenwärtig in Kanada im Gespräch ist: dabei gibt ein Interessenverband aus Rechteinhabern den ISPs vor, was sie zu blockieren haben.[479] Ähnliche Überlegungen gibt es in Frankreich.[480] Entsprechend könnten also auch Rechteinhabern den Routerherstellern vorgeben oder vorschlagen, welche *blacklist*-Inhalte mittels automatischer Updates zu implementieren sind.

j) Protokoll-Ebene und Client-Ebene

Technische Voraussetzung zum Betrieb von *filesharing* ist, wie unter Kapitel § 1 II. 6. dargestellt, neben einem zentralen Verwaltungselement stets ein Client; typischerweise stellt der Client die Implementierung allgemeiner Regeln, mithin eines Protokolls dar.

Die bisher dargestellten Eingriffsebenen für präventive Maßnahmen haben in ihrer praktischen Anwendung primär die Funktion, entweder den Zugriff auf Suchmechanismen wie Indexseiten oder die Abwicklung des *filesharing*-Datenverkehrs zu verhindern.

Rein theoretisch denkbar wäre aber auch, an der Wurzel anzusetzen und die Verbreitung eines *filesharing*-Protokolls oder eines Clients zu verbieten; technisch würde man dies durch IP, DNS und URL-Sperren oder Serverab-

[478] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG.

[479] *Van Der Sar*, ISPs and Movie Industry Prepare Canadian Pirate Site Blocking Deal.

[480] *Van Der Sar*, French Minister of Culture Calls For Pirate Streaming Blacklist.

schaltungen gegen Webseiten umsetzen, die weiterhin das betroffene Protokoll erläutern oder den betroffenen Client anbieten, rechtlich begleitet von Sanktionen gegen die Anbieter. Dass einem solchem Vorgehen die Gefahr des *overblocking* noch mehr inhärent ist als allen anderen Präventionsmaßnahmen, steht auf einem anderen Blatt.

Rein praktisch und chronologisch waren Client-Verbote noch vor allen anderen Präventionsmaßnahmen prominent, wie beispielsweise die gerichtlichen Verbote der Clients Napster, KaZaA und Limewire beweisen.[481] Client-Verbote sind gegenwärtig „außer Mode gekommen", was primär damit zusammen hängt, dass *filesharing* seit einiger Zeit fast ausschließlich über das BitTorrent-System betrieben wird und die Entwickler des BitTorrent-Protokolls und des Referenzclients uTorrent sowie sonstige Entwickler von BitTorrent-Clients bisher von gerichtlichem Vorgehen verschont geblieben sind. Dass sich dies aber in Zukunft auch ändern könnte, deutet ein Schreiben des Interessenverbandes RIAA an BitTorrent Inc. (die Entwickler des Protokolls und des Referenzclients, die nunmehr *Rainberry* heißen) vom 30. Juli 2015 hin, in dem auf die umfangreiche Nutzung des BitTorrent-Systems für Urheberrechtsverletzungen hingewiesen wird und Konsequenzen gefordert werden.[482]

Dies dürfte für die Urheberrechtsindustrie nun umso dringlicher werden, da *Rainberry* über eine 2018 initiierte Erweiterung des BitTorrent-Protokolls bezahltes Uploaden ermöglicht, indem *leecher* im Gegenzug für die Zahlung von Kryptowährung, nämlich des eigens hierfür eingeführten *BitTorrent token* (BTT), von Uploadern bessere Downloadgeschwindigkeiten erkaufen können; diese Funktion wird als *BitTorrent Speed* bezeichnet.[483] Unternehmensintern hatte dies bereits zu Streitigkeiten über die urheberrechtliche

[481] Siehe hierzu Kapitel § 1 II. 4. a), b) und c) sowie Kapitel § 1 V. 4. j).

[482] *Maxwell*, RIAA Asks BitTorrent Inc. to Block Infringing Content.

[483] *Van Der Sar*, BitTorrent Unveils New Token to Pay for Faster Downloads. Siehe Erläuterungen zur Funktionsweise direkt auf der Webseite von *Rainberry*, abrufbar unter https://www.bittorrent.com/de/token/bittorrent-speed/ - Zugriff am 31.03.2021.

Zulässigkeit von *BitTorrent Speed* geführt.[484]

k) Peer-Ebene

Ein Eingriff auf *Peer-Ebene* im Sinne dieser Arbeit bedeutet, dass das Auffinden von gewünschten Zieldateien oder der Dateiübertragungsvorgang in einem *filesharing*-System durch einen externen Eingriff derart gestört werden kann, dass die betroffenen Endnutzer ihre gewünschte Zieldatei nicht oder nur unter erschwerten Umständen erlangen können und somit auf lange Sicht betrachtet das betroffene *filesharing*-System aus Frustration nicht mehr nutzen. Ist ein solcher Eingriff systematisch durchführbar, kann auf diese Weise ein gesamtes *filesharing*-System „zu Fall" gebracht werden. Wie bereits in Kapitel § 1 II. 4. f) erwähnt, waren solcherlei disruptive Eingriffe in *filesharing*-Systeme wie FastTrack, Gnutella und eDonkey durch die Urheberrechtsindustrie mitverantwortlich für deren Nutzerschwund. Wissenschaftliche Untersuchung haben aufgezeigt, dass diese Systeme besonders anfällig für „Verschmutzungs"-Angriffe waren, mithin mit *fake*-Dateien geflutet wurden.[485] Das BitTorrent-System, das gegenwärtig den *de facto*-Standard für *filesharing* darstellt[486], ist jedoch gegenüber disruptiven Eingriffen auf Peer-Ebene nahezu unempfindlich. Beispielsweise hatten Rechteinhaber versucht, durch Einsätze von „Agenten" in BitTorrent-Schwärmen den Datenaustausch durch verschiedene Mechanismen zu stören – mit nur sehr geringem Erfolg.[487]

Für Rechteinhaber kommen technische Maßnahmen auf Peer-Ebene daher nicht in ernsthaft in Betracht, sodass sie im Weiteren außer Betracht bleiben können.

---

[484] Siehe *Maxwell*, BitTorrent Owner Accused of Profiting From Movie Piracy. Unter Geltung des Grokster-Standards dürfte diese nach US-amerikanischer Rechtslage in der Tat problematisch sein, vgl. *Giblin*, IEEE Internet Computing, Nr. 3, Bd. 16, 2012, S. 92, 94. Siehe zum Grokster-Standard *Post/Sandefur*, 2004-2005 Cato Sup. Ct. Rev. 235, 253ff. (2005). In Deutschland ist die Rechtslage ähnlich, da der BGH schon in der „Cybersky"-Entscheidung geurteilt hat, dass eine Störerhaftung für den Betrieb eines *filesharing*-Systems in Betracht kommt, wenn die Möglichkeit dessen Nutzung für Rechtsverletzungen aktiv beworben wird, siehe BGH, Urteil vom 15. Januar 2009, Az. I ZR 57/07, Rz. 33 – GRUR 2009, 841 - „Cybersky".

[485] *Liang* et al., Pollution in P2P file sharing systems, S. 1174, 1185; *Christin/Weigend/Chuang*, Content Availability, Pollution and Poisoning in File Sharing Peer-to-peer Networks, S. 68.

[486] Siehe oben Kapitel § 1 II. 6.

[487] *Dhungel* et al., A Measurement Study of Attacks on BitTorrent Leechers, S. 1, 8.

l) Zahlungsdienste und Werbetreibende

Keine technische, aber ökonomische Maßnahme der Prävention ist, Zahlungsdiensten und Werbetreibenden die Zusammenarbeit mit urheberrechtsverletzenden Diensten wie Indexseiten zu verbieten oder entsprechende freiwillige Vereinbarungen zu treffen.[488] Eine Haftung Werbetreibender ist zwar bisher weder in Deutschland noch international höchstgerichtlich anerkannt[489], wäre aber mindestens in Deutschland denkbar.[490] Auch international wird wohl mit entsprechenden Verfahren zu rechnen sein. Betreffend Zahlungsdiensten wurde beispielsweise *PayPal* im Jahr 2018 in den USA dazu verurteilt, die Konten von Betreibern urheberrechtsverletzender Angebote einzufrieren.[491]

5. Zusammenfassung

Als Ergebnis lässt sich festhalten, dass Überwachungsmaßnahmen für den Anschlussinhaber möglich sind, aber der damit verbundene Aufwand extrem hoch ist, wenn sie einigermaßen lückenlos sein sollen.

Präventionsmaßnahmen stehen grundsätzlich hinsichtlich (fast) aller Ebenen des *filesharing*-Vorgangs zur Verfügung. Auf das – hinsichtlich des Nutzungsumfangs maßgebliche[492] – BitTorrent-System bezogen, bedeutet dies, dass theoretisch an folgenden Stellen eingegriffen werden kann:

1. die Veröffentlichung von Vorschlägen das Protokoll betreffend, mithin die BEPs
2. die Veröffentlichung von Clients, die das BitTorrent-Protokoll programmiertechnisch implementieren
3. Domains und Hosting-Server von Indexseiten (öffentliche wie private), die .torrent-Dateien oder *magnet links* anbieten
4. Tracker, öffentliche wie private
5. Server, die das *bootstrapping* in die DHT ermöglichen

[488] Siehe hierzu auch das Schlusswort dieser Arbeit.
[489] Vgl. *Nordemann/ Waiblinger*, MMR 2017, 211, 212; *Goldman*, Ad Network Defeats Secondary Copyright Claims - ALS Scan v. JuicyAds.
[490] *Nordemann/ Waiblinger*, MMR 2017, 211, 212.
[491] *Van Der Sar*, Court Orders PayPal to Restrain Pirate Site Funds.
[492] Siehe Kapitel § 1 II. 6. und Kapitel § 3 II.

6. Ausweichmechanismen wie .onion-Domains und andere Umgehungshilfen
7. Suchmaschinen und sonstige Suchhilfen
8. nicht in technischer, aber wirtschaftlicher Hinsicht, Bezahldienste und Vermittler von Werbung, die mit Indexseiten zusammenarbeiten

Lediglich die Peer-Ebene scheidet bei BitTorrent als Ebene für Präventionsmaßnahmen aus, hier bleiben Rechteinhaber auf Ermittlungsmaßnahmen[493] beschränkt. Bei anderen *filesharing*-Systemen kann die Peer-Ebene ein potentielles Angriffsziel sein[494], dafür können andere potentielle Ziele entfallen, beispielsweise die Indexseiten, die es in vergleichbarer Form sonst nur bei eDonkey gibt. Wie aufgezeigt[495] muss nach gegenwärtigem Stand ein *filesharing*-System aber mindestens zwei Elemente aufweisen, einen Client und einen zentralen Anlaufpunkt fürs *bootstrapping*. Sollte Letzterer in Zukunft durch eine technische Neuerung überflüssig werden[496], verbliebe jedenfalls noch der Client als Angriffspunkt sowie Webseiten, auf denen ein Client zum Download angeboten wird.

Zugleich muss im Bewusstsein bleiben, dass, wie aufgezeigt, eine vollständige Prävention von *filesharing* nicht möglich ist. Zwischen Rechteinhabern und *filesharing*-Nutzern- und Anbietern findet vielmehr ein „Katz-und-Maus-Spiel“ statt[497], das – solange es gespielt wird – den Rechteinhabern (nach deren Wahrnehmung) ein gewisses Maß an Abhilfe schafft, nämlich indem *filesharing* zumindest erschwert und verkompliziert wird. Das Recht darf dabei allerdings nicht vergessen, dass seine Spielregeln Kollateralschäden in Form von *overblocking* und übermäßigen Sanktionen ermöglichen können. Es muss daher die Interessen aller Akteure im Internet im Blick behalten und zu einem gerechten Ausgleich bringen, der im Laufe der gesellschaftlichen und technischen Entwicklungen immer wieder neu zu verhandeln sein wird.

493 Siehe hierzu Kapitel § 1 IV.
494 Siehe Kapitel § 1 V. 4. k).
495 Siehe Kapitel § 1 II. 6.
496 Siehe Kapitel § 1 II. 6.
497 *Bilton*, Internet Pirates Will Always Win.

§ 2 Die Behandlung des *filesharing* in der Praxis der Rechtsprechung und der Gesetzgebung

I. Einleitung

Wollte man die Entwicklung der Rechtsprechung und der Gesetzgebung zum *filesharing* grob gliedern, so ließe sie sich in zwei Phasen aufteilen, von denen die erste im Jahr 2000 mit dem Bekanntwerden des ersten *filesharing*-Systems Napster beginnt und mit der Einführung des zivilrechtlichen, nichtakzessorischen Drittauskunftsanspruches zum 1. September 2008 durch das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums[1] endet, während die sich hieran anschließende zweite Phase mit der BGH-Entscheidung „Konferenz der Tiere“[2] bzw. den Konsequenzen hieraus ihr Ende gefunden haben könnte; dies ist jedoch noch nicht mit Gewissheit abzusehen.

Relativ betrachtet zeichnet sich die erste Phase durch viel Literatur, aber wenig Rechtsprechung, die zweite Phase durch viel Rechtsprechung, aber wenig Literatur aus, insbesondere dann, wenn man die rein die Rechtsprechung und Gesetzgebung begleitende Aufsatzliteratur auslässt.

Diese Verteilung dürfte dem Umstand geschuldet sein, dass Anfang der 2000er Jahre *filesharing* ein neues Phänomen war und dementsprechend gesellschaftliche und nachfolgend rechtswissenschaftliche Aufmerksam-

[1] BGBl. 2008 I, S. 1191.
[2] Siehe Kapitel § 2 XI. 5.

keit auf sich zog. Durch die Zunahme der Geschwindigkeit von Internet-Endkundenanschlüssen blieb es nicht beim Tausch von Musik im mp3-Format, wie es noch bei Napster der Fall war; Filme, Software, Videospiele, Hörbücher und eBooks kamen hinzu. Das BitTorrent-Protokoll perfektionierte schließlich die technische Effizienz des *filesharing*, der Tausch über physische Datenträger verschwand. Als dann 2008 der zivilrechtliche Auskunftsanspruch eingeführt wurde, war *filesharing* aus rechtswissenschaftlicher Perspektive wohl bereits „ein alter Hut“, während es als gesellschaftliches und technisches Phänomen gerade erst in seine Hochphase eintrat. Dabei waren die entscheidenden rechtlichen Fragen von der Rechtsprechung noch gar nicht beantwortet worden. Zwar hatte es bereits einige – vergleichsweise zu später sehr wenige – Klagen gegeben, doch der Instanzenzug blieb regelmäßig aus und der Grad der rechtlichen Auseinandersetzung mit dem Sachverhalt in den Urteilsbegründungen niedrig.

Dies ist zum Zeitpunkt der Fertigstellung dieser Arbeit nicht mehr der Fall. *Filesharing* ist – in den zeitlichen Dimensionen der Entwicklung der Informationstechnologie betrachtet – ein altes Phänomen, will aber einfach nicht verschwinden. Die Rechtsprechung hatte folglich durch den nach 2008 stattfindenden, massiven Anstieg der Klagezahlen die Gelegenheit, eine Vielzahl an Sachverhaltskonstellationen zu beurteilen; der Gesetzgeber ist in Reaktion hierauf aktiv geworden und hat mehrere Reformen durchgeführt.

In diesem Kapitel wird daher die umfassende Tätigkeit von Rechtsprechung und Gesetzgebung dargestellt und zusammengefasst. Da eine deskriptive Beschreibung der gegenwärtigen Rechtslage angestrebt ist, wird im Rahmen dieses Kapitels die Instanzrechtsprechung weitestgehend außer Acht gelassen, mithin also eine faktische Geltung der Rechtsprechung der obersten Gerichtsinstanzen angenommen.

Um die Entwicklung verständlich nachzuzeichnen, wird vorwiegend chronologisch verfahren. Ausnahme ist der Auskunftsanspruch des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums und die hierzu gehörende Rechtsprechung sowie die zugehörige Frage der Speicherpflichten, da dies ein eigener, thematisch geschlossenen Bereich ist.

II. Die Entwicklung von 2000 bis 2008

Die ersten deutschen juristischen Publikationen zum *filesharing* erschienen in Reaktion auf das Napster-Verfahren in den USA[3] ab dem Jahr 2000. Es wurde überwiegend problematisiert, ob *filesharing* seitens der Endnutzer – und zwar sowohl der Upload- als auch der Downloadvorgang – im Rahmen der damaligen Rechtslage überhaupt eine Urheberrechtsverletzung darstellen konnte. Hinsichtlich des Downloadvorgangs wurde eine Vervielfältigung im Sinne von § 16 UrhG a.F. vorwiegend noch bejaht, die Urheberrechtswidrigkeit aber wegen § 53 UrhG a.F., dem zu diesem Zeitpunkt noch der ausdrückliche Ausschluss der offensichtlich rechtswidrigen Vorlagen fehlte, als kritisch angesehen.[4] Die klare Einordnung des Uploadvorgangs als urheberrechtswidrige Handlung scheiterte schon an der noch fehlenden Normierung der öffentlichen Zugänglichmachung; bei anderen Verwertungshandlungen wie der öffentlichen Wiedergabe nach § 15 Abs.2 UrhG a.F. oder der Vervielfältigung nach § 16 UrhG stellte sich wiederum die Schrankenproblematik, also insbesondere die Frage der Anwendbarkeit der §§ 52 und 53 UrhG a.F.[5]

Mit der Umsetzung der InfoSocRL[6] ins deutsche Recht zum 13. September 2003 durch das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft[7] (Erster Korb) verblieben zwar noch letzte Zweifel, ob der Downloadvorgang trotz der Änderung des Wortlauts des § 53 UrhG a.F.

---

3 Siehe Kapitel § 1 II. 4. a).

4 *Ahrens*, ZUM 2000, 1029, 1036; *Hänel*, JurPC WebDok. 245/2000, Abs. 16ff.; *Kreutzer*, ITRB 2001, 136, 137; *Kreutzer*, GRUR 2001, 193, 199ff.; *Bosak*, CR 2001, 176, 181; *Braun*, GRUR 2001, 1106, 1107f.; *Spindler*, JZ 2002, 60, 61f.; *Mayer*, Urheber- und haftungsrechtliche Fragestellungen bei peer-to-peer-Tauschbörsen, S. 43ff.; *Wenzl*, Musiktauschbörsen im Internet, S. 92f.

5 *Ahrens*, ZUM 2000, 1029, 1030ff.; *Hänel*, JurPC WebDok. 245/2000, Abs. 9ff.; *Kreutzer*, ITRB 2001, 136, 137; *Kreutzer*, GRUR 2001, 193, 201f.; *Braun*, GRUR 2001, 1106, 1108f.; *Spindler*, JZ 2002, 60, 63ff.; *Mayer*, Urheber- und haftungsrechtliche Fragestellungen bei peer-to-peer-Tauschbörsen, S. 24ff.; *Wenzl*, Musiktauschbörsen im Internet, S. 66ff.

6 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.

7 BGBl. 2003 I, S. 1774.

nicht doch privilegiert sein könnte[8]; der Uploadvorgang bzw. das Bereithalten einer Datei auf der eigenen Festplatte zum Abruf durch andere Nutzer eines *filesharing*-Systems war nun aber nach einhelliger Meinung unter den neuen § 19a UrhG betreffend die öffentliche Zugänglichmachung zu subsumieren, ohne dass hiergegen eine Schrankenregelung in Stellung gebracht werden könnte.[9]

Der akademischen Klärung stand jedoch an anderer Stelle ein praktisches Problem gegenüber: die technischen Möglichkeiten der Ermittlung[10] existierten, aber es fehlte an einem normierten zivilrechtlichen Auskunftsanspruch[11] gegen die ISPs bezüglich der Zuordnung der ermittelten IP-Adressen zu Endkundenanschlüssen und freiwillig teilten die ISPs – soweit ersichtlich – keine Daten ihrer Nutzer mit[12]. Daher blieb den Rechteinhabern nur der Weg über das Strafverfahren. Die Verfältigung war schon seit jeher nach § 106 UrhG strafbar gewesen, und die nun neu eingeführte öffentliche Zugänglichmachung fiel – als Form der öffentlichen Wiedergabe nach § 15 Abs.2 Nr.2 UrhG – ebenfalls unter diese Norm. Die Urheberrechtswidrigkeit einer Handlung führte (und führt[13]) also automatisch zu ihrer Strafbarkeit.[14] Leitete die Staatsanwaltschaft auf Anzeige eines von einem *filesharing*-Vorgangs betrof-

---

8 *Nordemann/Dustmann*, CR 2004, 380, 381; *Bäumer/Rendell/Pühler*, CRi 2004, 129, 132f.; *Freiwald*, Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, S. 142ff.; *Wenzl*, Musiktauschbörsen im Internet, S. 87ff.; *Brinkel*, Filesharing, S. 112ff.; *Engelhardt*, Die rechtliche Behandlung von Urheberrechtsverletzungen in P2P-Netzwerken nach US-amerikanischem und deutschem Recht, S. 176f.; diese Unsicherheit wurde durch die weitere Änderung des § 53 UrhG a.F. durch den Zweiten Korb beseitigt.

9 *Nordemann/Dustmann*, CR 2004, 380, 380; *Bäumer/Rendell/Pühler*, CRi 2004, 129, 131f.; *Wenzl*, Musiktauschbörsen im Internet, S. 73; *Brinkel*, Filesharing, S. 87ff.

10 Siehe hierzu Kapitel § 1 IV.

11 Zwar konstruierten einige Gerichte einen solchen Anspruch, diese Entscheidungen machten aber keine Schule und waren heftiger Kritik der Literatur ausgesetzt; siehe mit umfangreichen Nachweisen hierzu *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 128f.

12 Die freiwillige Mitteilung wäre auch nach damaliger Rechtslage straf-und datenschutzrechtlich nicht zulässig gewesen; so jedenfalls *Brinkel*, Filesharing, S. 212ff. sowie *Abdallah/Gercke*, ZUM 2005, 368, 371.

13 Die Einführung einer gesetzlichen Bagatellgrenze wurde beim Entwurf des Zweiten Korbs erwogen, aber wieder verworfen; Bagatellen werden allerdings strafprozessual durch Verfahrenseinstellung berücksichtigt, siehe *Sternberg-Lieben* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 106 UrhG, Rz. 3.

14 *Heghmanns*, MMR 2004, 14, 18; *Frank*, K&R 2004, 576, 580.

fenen Rechteinhabers hin ein Strafverfahren gegen Unbekannt ein, konnte sie auf Basis der – regelmäßig im Auftrag des Rechteinhabers ermittelten und der Staatsanwaltschaft zur Verfügung gestellten[15] – IP-Adressen gemäß den Ermächtigungsgrundlagen der §§ 100a ff. StPO a.F. und § 113 TKG a.F. die einschlägigen ISPs zur Herausgabe von Name und Anschrift des (vermeintlichen) Täters oder der (vermeintlichen) Täter zwingen.[16] Der Rechteinhaber konnte sodann versuchen, durch Berufung auf § 406e StPO a.F. Einsicht in die Strafakten zu erhalten, um anschließend auf zivilrechtlichem Wege gegen den oder die Täter vorzugehen.

Filesharing-Nutzer, die eine große Zahl an geschützten Werken zum Download zur Verfügung stellten, mussten auch strafrechtliche Konsequenzen befürchten. Nach den ersten Hausdurchsuchungen im Jahr 2004 wurde ein Nutzer, der 272 Lieder über FastTrack angeboten hatte, vom AG Cottbus zu einer Geldstrafe verurteilt.[17] Im Herbst 2005 wurden über 40.000 Anzeigen gegen *filesharer* eines Videospiels erstattet, jedoch die Verfahren wegen geringer Schuld überwiegend eingestellt.[18] Mitte 2006 wurde in einer anderen Sache gegen rund 24.000 Personen ermittelt und von den 6000, die aus Deutschland kamen, konnten 3500 identifiziert werden. Bei 130 Personen, die in sehr großem Umfang Dateien getauscht hatten, kam es zu Hausdurchsuchungen.[19] Wie die Verfahren ausgingen, ist jedoch – soweit ersichtlich – nicht öffentlich bekannt. Die breite Masse der „kleinen“ Nutzer wurde allerdings augenscheinlich ganz überwiegend nicht strafrechtlich belangt. Dazu dürfte beigetragen haben, dass die Gerichte der Staatsanwaltschaft bei nur in kleinem Umfang betriebenen *filesharing* teilweise kein Auskunftsrecht gegen

[15] *Solmecke*, MMR 2006, XXIII, XXIII.

[16] *Reinbacher*, Die Strafbarkeit der Vervielfältigung urheberrechtlich geschützter Werke zum privaten Gebrauch nach dem Urheberrechtsgesetz, S. 318ff.; *Abdallah*, JurPC WebDok. 149/2006, Abs. 4.

[17] AG Cottbus, Urteil vom 6. Mai 2004, Az. 95 DS 1653 JS 15556/04 (57/04) – juris; siehe hierzu auch *Patalong*, Deutscher KaZaA-Nutzer muss 8000 Euro zahlen.

[18] *Solmecke*, MMR 2006, XXIII, XXIII.

[19] *Solmecke*, MMR 2006, XXIII, XXIII; http://www.spiegel.de/netzwelt/web/massenrazzia-fahnder-nehmen-3500-deutsche-edonkey-nutzer-ins-visier-a-417619.html - Zugriff am 31.03.2021.

die ISPs zubilligten.[20]

Auch zum Erfolg des damaligen zivilrechtlichen Vorgehens stehen wenige Informationen zur Verfügung. Problematisch dürfte hierbei gewesen sein, dass die Akteneinsicht oft verweigert wurde.[21]

Soweit Auskunft erteilt wurde, versandten die jeweiligen Rechteinhaber vor einem gerichtlichen Vorgehen Abmahnungen, in denen sie regelmäßig mehrere tausend Euro Schadensersatz für die außergerichtliche Beilegung des Streits verlangten.[22] Die gerichtliche Geltendmachung des Schadensersatzes scheiterte aber zunächst. An der Rechtslage auf Rechtsfolgenseite lag dies nicht. Zwar war und ist eine konkrete Bezifferung des Schadens, der durch den *filesharing*-Vorgang entsteht, im Wege der Differenzhypothese nicht möglich[23], jedoch konnte der Schaden stattdessen auch auf Grundlage der Lizenzanalogie berechnet werden, die als Rechtsinstitut schon vor der ausdrücklichen Normierung durch das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums gewohnheitsrechtlich bzw. richterrechtlich anerkannt war.[24] Allerdings monierten die Zivilgerichte auf Tatbestandsseite, dass der Nachweis der Tatsache, dass eine *filesharing*-Aktivität von einem bestimmten Anschluss ausgegangen war, keinen Beweis für die Täterschaft des Anschlussinhabers begründet. Zwar treffe den Anschlussinhaber eine sekundäre Darlegungslast über die Nutzungssituation seines Anschlusses; wenn er aber vortragen könne, dass andere Personen seinen Anschluss mitbenutzen, sei der Vorwurf der Täterschaft entkräftet.[25] In der Literatur wurde dieser Ansatz der Gerichte nicht kritisiert.[26] Ob der Anschlussinhaber jedenfalls als Störer auf Unterlassung der Urheberrechtsverletzung in Anspruch genommen werden kann und wenn ja, in welchen Konstellationen, wurde von

---

[20] Beispielsweise AG Offenburg, Beschluss vom 20. Juli 2007, Az. 4 Gs 442/07 – juris. Ohnehin spielt die strafrechtliche Verfolgung der Endnutzer seit der Einführung des zivilrechtlichen Auskunftsanspruches keine Rolle mehr, jedenfalls sind seitdem keine entsprechenden Fälle mehr bekannt geworden.

[21] *Kondziela*, MMR 2009, 295, 300, mit einer Übersicht der Rechtsprechung.

[22] *Röhl/Bosch*, NJOZ 2008, 1197, 1198.

[23] *Röhl/Bosch*, NJOZ 2008, 1197, 1209; siehe hierzu auch Kapitel § 4 IX. 1.

[24] *Ernicke*, ZGE 2016, 84, 86.

[25] LG Mannheim, Urteil vom 29. September 2006, Az. 7 O 62/06, Rz. 11ff. – juris; LG Mannheim, Urteil vom 29. September 2006, Az. 7 O 76/06, Rz. 4 – juris; LG Mannheim, Urteil vom 30. Januar 2007, Az. 2 O 71/06, Rz. 19 – juris.

[26] Vergleiche beispielsweise *Ernst/Seichter*, ZUM 2007, 513, 514

der Instanzrechtsprechung unterschiedlich beurteilt.[27]

Die Haftung des Anschlussinhabers änderte sich jedoch durch die nachfolgende BGH-Rechtsprechung grundlegend.[28]

III. Das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums

1. Der zivilrechtliche Auskunftsanspruch

a) Die Enforcement-Richtlinie

Der Umweg zur Auskunft über das Strafverfahren schien mit Inkrafttreten der EnforcementRL[29] kein hinnehmbarer Rechtszustand mehr zu sein, da Art. 8 Abs.1 lit. c) EnforcementRL Rechteinhabern nach einer zum Teil vertretener Auffassung einen materiellen, zivilrechtlichen Anspruch gegen denjenigen zubilligte, der „*nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte.*“.[30] Die Norm war dazu intendiert, ISPs zu erfassen[31] und ihr Wortlaut leistet dies auch offensichtlich.

Ob sie jedoch auch einen *zivilrechtlichen* Auskunftsanspruch gebietet, blieb zunächst unklar. Als diese Frage Gegenstand des Vorabentscheidungsverfahrens „Promusicae“[32] wurde, machte die zuständige Generalanwältin die Antwort in ihren Schlussanträgen an der Überlegung fest, wie der Auskunftsanspruch mit dem Datenschutzrecht in Einklage zu bringen sei. Der dem Verfahren zu Grunde liegende Sachverhalt war eine klassische *filesharing*-Konstellation, die sich in Spanien zugetragen hatte. Spanische Internetnutzer hatten über ihren Anschluss urheberrechtlich geschützte Lieder über Fast-Track/KaZaA angeboten. Deren IP war geloggt und der zuständige ISP zur Auskunft über Name und Anschrift der Nutzer aufgefordert worden. Vor Gericht verteidigte er sich mit dem Hinweis auf eine spanische Rechtsvorschrift,

---

27 Übersicht bei *Ernst/Seichter*, ZUM 2007, 513, 515

28 Siehe hierzu Kapitel § 2 IV.

29 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums.

30 *McGuire*, GRUR Int. 2005, 15, 16.

31 *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 140.

32 EuGH, Rs. C-275/06, ECLI:EU:C:2008:54 - „Promusicae“.

die eine solche Auskunft nur im Rahmen strafrechtlicher Untersuchungen oder anderer wichtiger öffentlicher Belange erlaubte.[33] Die Generalanwältin war der Auffassung, dass eine solche Einschränkung nach Art. 13 Abs.1 DatenschutzRL[34] iVm Art. 15 E-DatenschutzRL[35] zulässig sei.[36] Die Angabe darüber, zu welchem Zeitpunkt eine bestimmte IP-Adresse einem bestimmten Anschluss zugeordnet war, sei ein personenbezogenes Datum im Sinne von Art. 2 lit. a) DatenschutzRL, sodass Datenschutzrecht auch Anwendung finde.[37] Da Art. 2 lit. a) EnforcementRL die Geltung des Datenschutzrechts insgesamt unbeschadet lasse, folge aus dessen Wertungen – auch angesichts der Tatsache, dass nicht gesichert sei, wie schwer die Unterhaltungsindustrie durch privates, also nicht-gewerbliches *filesharing* betroffen sei – dass Art. 8 Abs.1 lit. c) EnforcementRL keinen zivilrechtlichen Anspruch gegen ISPs fordere, wenn die entsprechende Rechtsverletzung durch *filesharing* mit nicht-gewerblichem Zweck erfolgt war.[38] Und nicht nur das: tatsächlich müsse der europäische Gesetzgeber sogar erst das Datenschutzrecht ändern, um einen Auskunftsanspruch in dieser Konstellation europarechtskonform zu machen.[39]

Ein solches Verständnis der EnforcementRL hätte im Ergebnis an der bisherigen deutschen Rechtslage nichts geändert. Rechteinhaber hätten mithin weiter auf das Strafverfahren verwiesen werden müssen. Denn von Endnutzern wird *filesharing* praktisch ausschließlich privat, also ohne gewerblichen Hintergrund, betrieben. Jedoch trug der EuGH in seiner Entscheidung diese letzte Konsequenz nicht mit. Die Datenschutzrichtlinien seien in Bezug auf die streitgegenständliche Frage zu allgemein gehalten, als dass sich hieraus

[33] Schlussanträge vom 18. Juli 2007, Rs. C-275/06, Rz. 81 – ECLI:EU:C:2007:454 - „Promusicae"; zur Änderung der Rechtslage in Spanien siehe Kapitel § 3 XII. 3. d).

[34] 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.

[35] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002.

[36] Schlussanträge vom 18. Juli 2007, Rs. C-275/06, Rz. 80 – ECLI:EU:C:2007:454 - „Promusicae".

[37] Schlussanträge vom 18. Juli 2007, Rs. C-275/06, Rz. 61 – ECLI:EU:C:2007:454 - „Promusicae".

[38] Schlussanträge vom 18. Juli 2007, Rs. C-275/06, Rz. 106ff – ECLI:EU:C:2007:454 - „Promusicae".

[39] Schlussanträge vom 18. Juli 2007, Rs. C-275/06, Rz. 126 – ECLI:EU:C:2007:454 - „Promusicae"; diese Lesart auch bei *Schoene*, FD-GewRS 2007, 238454.

konkrete Ableitungen treffen ließen; folglich müssten die Mitgliedstaaten bei der Umsetzung der EnforcementRL selbst darauf achten, einen angemessenen Ausgleich zwischen den betroffenen Belangen herzustellen. Die EnforcementRL spreche im Ergebnis also zwar kein Gebot aus, einen zivilrechtlichen Auskunftsanspruch gegen ISPs bei privatem *filesharing* zu implementieren, würde einen solchen Anspruch aber auch nicht verbieten.[40]

Etwas mehr als ein Jahr später bekräftigte der EuGH in einer gleich gelagerten Konstellation diese Entscheidung in der Rechtssache „Tele2".[41]

b) Die Umsetzung der EnforcementRL in § 101 UrhG n.F.

Die Umsetzung der EnforcementRL erfolgte durch das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums.[42]

In der EnforcementRL ist auf Grund des Wortlauts in Art. 8 Abs.1 – „*im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums*" – die Akzessorietät des Auskunftsanspruches zu einem Verfahren gegen den Verletzer angeordnet. Die wortgetreue Umsetzung der Richtlinie hätte dazu geführt, dass von ISPs keine Auskunft über *filesharer* hätte erlangt werden können, da gegen Letztere zuerst ein Verfahren hätte eingeleitet werden müssen, Klagen gegen Unbekannt – entsprechend dem im angelsächsischen Rechtskreis bekannten Institut der *John Doe* - Klage – jedoch wegen des Erfordernisses der identifizierbaren Bezeichnung der Prozessparteien gemäß § 253 Abs.2 Nr.1 1.Alt ZPO in Deutschland nicht möglich sind.[43]

Dieser Umstand wurde im Gesetzesentwurf berücksichtigt, indem stattdessen ein nicht-akzessorischer Auskunftsanspruch gegen ISPs bei einer „*offensichtlichen Rechtsverletzung*" aufgenommen wurde; die europarechtliche Zulässigkeit dieser Abweichung von der Richtlinie wurde auf Grund Art. 8 Abs.3 lit. a) EnforcementRL angenommen, da nach dieser Norm die Absätze 1 und 2 unbeschadet weiterer gesetzlicher Auskunftsrechte gelten, also andere Aus-

[40] EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 54ff., 67ff. – ECLI:EU:C:2008:54 - „Promusicae".

[41] EuGH, Beschluss vom 19. Februar 2009, Rs. C-557/07, Rz. 25, 41ff. – ECLI:EU:C:2009:107 - „Tele2".

[42] BT-Drs. 16/5048, S. 1.

[43] Siehe hierzu auch Kapitel § 3 XII. 6.

kunftsrechte grundsätzlich möglich sind.[44]

Ein zivilrechtlicher, nicht-akzessorischer Drittauskunftsanspruch gegen ISPs wurde daher in § 101 Abs.2 Satz 1 Nr.3 UrhG implementiert.[45] Dieser ist gemäß § 101 Abs.9 UrhG mit einem Richtervorbehalt versehen[46], sofern die Auskunft nur mittels Verkehrsdaten im Sinne des § 3 Nr.30 TKG erteilt werden kann. Verkehrsdaten nach § 3 Nr.30 TKG sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden; dynamische IP-Adressen fallen unter diese Definition.[47] Weil die Auskunft auch nur unter Verwendung der dynamischen IP-Adresse erteilt werden kann – da diese einem Anschluss zugeordnet werden muss – kommt der Richtervorbehalt in *filesharing*-Konstellationen immer zur Anwendung.

Eine Gestattungsanordnung nach § 101 Abs.9 UrhG darf nur ergehen, wenn der Auskunftsanspruch materiell besteht.[48] Zudem muss gemäß § 101 Abs.2 Satz 1 UrhG die einschlägige Rechtsverletzung offensichtlich sein und gemäß § 101 Abs.4 UrhG der Grundsatz der Verhältnismäßigkeit berücksichtigt werden, wobei aktuell ungeklärt ist, in welchen Fällen diese Voraussetzungen nicht gegeben sind; bisher wurden sie nicht problematisiert.[49] Eine positive Gestattungsanordnung wirkt gestaltungsrechtlich dahingehend, dass dem ISP erlaubt wird, die vom Rechteinhaber begehrte Auskunft zu erteilen.[50] Eine ohne Gestattungsanordnung erteilte Auskunft wäre also im Prozess gegen den Verletzer kein verwertbares Beweismittel. Umgekehrt ist die auf Grundlage einer Gestattungsanordnung erteilte Auksunft von demjenigen Gericht,

44 BT-Drs. 16/5048, S. 29, 38f.

45 In der Ausschussempfehlung wurde zur Kenntnis genommen, dass durch das mittlerweile ergangene Urteil des EuGH in der Rs. C-275/06 – ECLI:EU:C:2008:54 - „Promusicae“ nunmehr geklärt sei, dass die Festschreibung des Auskunftsrechts in einem zivilrechtlichen Auskunftsverfahren nicht notwendig sei. Man sei aber dennoch überzeugt, dass dies rechtspolitisch vorzugswürdig sei, siehe BT-Drs. 16/8383, S. 44, 46f.

46 Da der Richtervorbehalt kein Erfordernis der EnforcementRL ist, war er in der Diskussion über das Umsetzungsgesetz heftig umstritten, siehe *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 318.

47 *Braun* in: Geppert/Schütz, BeckTKG, 4. Aufl. 2013, § 96 TKG, Rz. 7.

48 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 24 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“, mit weiteren Nachweisen.

49 Siehe hierzu Kapitel § 5 IV. 3.

50 Vgl. BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 25 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“; *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 331f.

das im Nachgang über das Verletzungsverfahren zu entscheiden hat, nicht zwingend als Beweismittel zu berücksichtigen. Es kann die Auskunft als nicht verwertbares Beweismittel ansehen.[51]

Des Weiteren führt auch eine rechtskräftige Gestattungsanordnung[52] nicht dazu, dass der ISP zur Auskunft verpflichtet ist. Weigert er sich also auch nach Erteilung der Gestattungsanordnung, die Auskunft zu erteilen, muss der Rechteinhaber diese in einem weiteren Verfahren einklagen.[53] Das Verfahren über die Erteilung der Gestattungsanordnung wird gemäß § 101 Abs.9 Satz 4 UrhG nach den Regeln des FamFG durchgeführt, die Durchsetzung des Auskunftsanspruches findet regulär im Rahmen der ZPO statt.[54]

Allerdings wird – soweit ersichtlich – von Seiten der ISPs spätestens nach Rechtskraft der Gestattungsanordnung die Auskunft ganz regelmäßig auch erteilt, meistens aber schon unmittelbar nach Mitteilung über die erstinstanzlich erteilte Gestattung. Zu einer gerichtlichen Durchsetzung des Auskunftsanspruches kommt es daher in der Regel nicht.

c) Zum Erfordernis eines „gewerblichen Ausmaßes“

Auf Seiten der Rechteinhaber hatten sämtliche Entwürfe eines Umsetzungsgesetzes der EnforcementRL nicht nur wegen des Richtervorbehalts für Unmut gesorgt. Erwägungsgrund 14 der EnforcementRL sieht vor, dass ein Auskunftsrecht bei Rechtsverletzungen im gewerblichen Ausmaß gewährt werden muss, bei Fehlen des gewerblichen Ausmaßes jedoch fakultativ ist. Der Referentenentwurf zum Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom Januar 2006 hob ausdrücklich hervor, dass man von dieser fakultativen Möglichkeit keinen Gebrauch machen wolle.[55] Zwar ging der Entwurf davon aus, dass ein „gewerbliches Ausmaß“ nicht erst bei kommerziellem Handeln erreicht sei, sondern schon dann, wenn das Maß des „*üblichen Konsums*“ überschritten ist[56]; allerdings, so monierte ein von einem Interessenvertreter in der ZUM veröffentlichter Aufsatz, würde ein solches

[51] Siehe hierzu Kapitel § 2 III. 1. d).

[52] Die erstinstanzliche Gestattungsordnung kann noch mit der Beschwerde angegriffen werden, § 101 Abs.9 Satz 6 UrhG.

[53] *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 332.

[54] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 27 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[55] Referentenentwurf, S.78f.

[56] Referentenentwurf, S.78f.

Kriterium die Rechteinhaber vor unüberwindliche Beweisprobleme stellen.[57] Dennoch hielt auch der Regierungsentwurf daran fest, dass die Rechtsverletzung über einen im privaten Gebrauch üblichen Nutzungsumfang hinausgehen müsse.[58] In der Anhörung im Rechtsausschuss hielten die Vertreter der Unterhaltungsindustrie im Gegenzug ihre Einwände aufrecht[59], jedoch ohne Erfolg; in seiner Beschlussempfehlung änderte der Rechtsausschuss die Gesetzesbegründung in diesem Punkt nicht.[60]

Eine streng an der – soeben dargelegten – Gesetzesbegründung orientierte Auslegung hätte nach manchen Befürchtungen[61] dazu geführt, dass eine Gestattungsanordnung mangels Nachweisbarkeit des gewerblichen Ausmaßes in *filesharing*-Fällen niemals erteilt worden wäre. Den Rechteinhabern drohte vermeintlich abermals – wie zuletzt vor dem EuGH –, auf den Ermittlungsweg über das Strafverfahren zurückgeworfen zu werden.

Einigermaßen überraschend und entgegen zahlreicher gegenteiliger Entscheidungen der unteren Instanzen[62] befand der BGH jedoch im Beschluss „Alles kann besser werden“, dass die Gesetzesbegründung unbeachtlich sei, da sie – was zutrifft – im Gesetzeswortlaut des § 101 Abs.2 UrhG keinen ausdrücklichen Niederschlag gefunden habe.[63] Auf das Erfordernis eines gewerblichen Ausmaßes könne folglich verzichtet werden. Die Entscheidung wurde später noch dreimal bestätigt.[64]

Zwar war von einigen Instanzgerichten schon vor den BGH-Beschlüssen auch in Fällen nicht-gewerblichen Ausmaßes die Auskunftserteilung rege gestattet

---

57 *Zombik*, ZUM 2006, 450, 455.

58 BT-Drs. 16/5048, S. 49.

59 http://webarchiv.bundestag.de/archive/2010/0203/presse/hib/2007_06/2007_171/03.html - Zugriff am 31.03.2021.

60 BT-Drs. 16/8783.

61 Diese sind jedoch nach gegenwärtiger Sachlage unbegründet, siehe hierzu Kapitel § 5 IV. 4.

62 Siehe die Übersicht bei BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 10 – GRUR 2012, 1026 - „Alles kann besser werden“.

63 BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 27ff. – GRUR 2012, 1026 - „Alles kann besser werden“.

64 BGH, Beschluss vom 25. Oktober 2012, Az. I ZB 13/12, Rz. 11 – ZUM 2013, 38; BGH, Beschluss vom 5. Dezember 2012, Az. I ZB 48/12, Rz. 30 – GRUR 2013, 536 - „Heiligtümer des Todes“; BGH, Beschluss vom 16. Mai 2013, Az. I ZB 44/12, Rz. 8 – BeckRS 2013, 13001.

worden[65], diese Praxis war nun aber höchstgerichtlich abgesegnet. Grundsätzlich waren damit alle auf Grund einer Erstattungsanordnung erteilten Auskünfte im anschließenden Verfahren gegen den Anschlussinhaber ein zulässiges Beweismittel.

Der Inanspruchnahme der Anschlussinhaber war folglich auch für die Zukunft der Weg geebnet, sodass sich nunmehr primär nur noch die Frage stellte, inwieweit sie haften würden.

d) Die Auskunft in Reseller-Konstellationen

Der BGH musste sich im Anschluss nur noch ein weiteres Mal mit dem Auskunftsanspruch in Bezug auf *filesharing* auseinandersetzen, nämlich in einer Reseller-Konstellation[66], allerdings nicht im Rahmen eines Gestattungsverfahrens nach § 101 Abs.9 UrhG, sondern inzident im Rahmen eines Verletzungsprozesses gegen einen Anschlussinhaber.

Grund dafür war Folgendes: das Auskunftsbegehren in Reseller-Konstellationen kann sich zunächst nur gegen den Netzbetreiber richten. Dieser kann die dynamische IP-Adresse jedoch keinem Namen und keiner Anschrift zuordnen, sondern nur der sogenannten Anschlusskennung, einer Zeichenfolge, die von außen betrachtet nicht geeignet ist, eine Person zu identifizieren.[67] Der Netzbetreiber kann dem Rechteinhaber allerdings mitteilen, welcher Reseller für die Anschlusskennung zuständig ist. Es wurde übliche Praxis, dass die Rechteinhaber sich mit dem Gestattungsbeschluss nach Mitteilung der Anschlusskennung durch den jeweiligen Netzbetreiber an die jeweils zuständigen Reseller wandten und diese sodann freiwillig mitteilten, welcher Kunde sich hinter der Anschlusskennung verbirgt.

Einige Instanzgerichte befanden jedoch[68], dass die Auskunft der Reseller ebenfalls nur auf Grund einer Gestattungsanordnung nach § 101 Abs.9 UrhG hätte erteilt werden dürfen. Wenn eine solche – wie in der Regel der Fall – nicht eingeholt worden war, würden die entsprechenden Auskünfte im Verletzungsprozess einem Beweisverwertungsverbot unterliegen. Dem widersprach

[65] Zu den Abmahnzahlen ab 2008 siehe Kapitel § 3 V.

[66] Zum technischen Hintergrund siehe Kapitel § 1 IV. 5. c).

[67] Anschlusskennungen werden aber auch von ISPs generell – also unabhängig von dem Vorliegen einer Reseller-Konstellation – verwendet.

[68] Beispielsweise AG Augsburg, Endurteil vom 22. Juni 2015, Az. 16 C 3030/14 – juris; AG Koblenz, Urteil vom 9. Januar 2015, 411 C 250/14 – juris.

der BGH in der Entscheidung „Benutzerkennung“: eine Gestattungsanordnung sei für die Auskunft des Resellers nicht erforderlich, da dieser für die Auskunft nur die Anschlusskennung heranziehen müsse, auf die § 101 Abs.9 UrhG allerdings keine Anwendung finde.[69] Folglich sei gegenüber Resellern keine Gestattungsanordnung erforderlich, wenn bereits gegenüber dem Netzbetreiber eine solche ergangen sei; mithin ergebe sich auch kein Beweisverwertungsverbot, wenn Reseller ohne eine sie betreffende Gestattungsanordnung Auskunft erteilen.

e) Die Sicherung des Auskunftsanspruchs

Damit die Auskunft überhaupt erteilt werden kann, muss die Zuordnung der IP-Adresse zu der Anschlusskennung eines bestimmten Endkunden beim jeweiligen ISP, dessen Netz für eine Urheberrechtsverletzung genutzt wurde, gespeichert worden sein. Über die Speicherung kommt es immer wieder zu Streit, der sich vor allem an der Vorratsdatenspeicherung entzündet.

Vorratsdatenspeicherung ist kein gesetzlich normierter Begriff. Allgemein meint Vorratsdatenspeicherung die Speicherung personenbezogener Daten, die IP-Vorratsdatenspeicherung spezifisch die Speicherung der Zuordnung einer dynamischen IP-Adresse zu einer bestimmten Anschlusskennung zu einem bestimmten Zeitpunkt, ohne dass ein konkreter Anlass für die Speicherung besteht. Diese kann freiwillig oder verpflichtend erfolgen, seit dem Erlass der VorratsdatenspeicherungsRL[70] wird der Begriff aber typischerweise mit einer Speicher*pflicht* assoziiert, da die Richtlinie eine solche vorschrieb.

Bis zum Inkrafttreten des entsprechenden Umsetzungsgesetzes in Deutschland am 1. Januar 2008 war ein Speicherrecht der Provider grundsätzlich anerkannt, eine Speicherpflicht jedoch nicht vorhanden.[71] Die Vorschriften des Umsetzungsgesetzes wurden vom BVerfG im Wege des Eilverfahrens für nur eingeschränkt anwendbar[72] und später schließlich für verfassungswidrig

69 BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16, Rz. 15ff. – GRUR 2018, 189 - „Benutzerkennung“.

70 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

71 *Marberth-Kubicki* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 43, Rz. 306ff.

72 BVerfG, Beschluss vom 11. März 2008, Az. 1 BvR 256/08 – bverfg.de.

erklärt.[73] Die Richtlinie selbst befand der EuGH im Jahr 2014 für nichtig.[74] 2016 entschied er zudem im Rahmen eines Vorabentscheidungsverfahrens, dass das EU-Recht einer allgemeinen und anlasslosen Vorratsdatenspeicherung auch auf nationaler Ebene entgegenstünde.[75] In Deutschland war ein Jahr zuvor eine bundesgesetzliche Einführung der Vorratsdatenspeicherung beschlossen worden, die bezüglich ISPs ab dem 1. Juli 2017 greifen sollte.[76] Die große Koalition sah sich nach Verkündung des EuGH-Urteils dennoch nicht veranlasst, das Gesetz nachzubessern oder aufzuheben.[77] Allerdings begehrte ein ISP im Wege des einstweiligen Rechtsschutzes festzustellen, dass die Speicherpflicht (unter anderem für IP-Adressen) nach § 113b Abs.3 TKG n.F. vorläufig auf ihn keine Anwendung finde und hatte damit vor dem OVG NRW Erfolg, da dieses die Vereinbarkeit der Regelung mit dem EU-Recht – insbesondere im Lichte der EuGH-Entscheidungen zur Vorratsdatenspeicherung – kritisch sah.[78] Die (mit der Überwachung der Einhaltung der Speicherpflichten betraute) Bundesnetzagentur verkündete daraufhin, bis zum Abschluss des Hauptsacheverfahrens die Speicherpflicht nach § 113b Abs.3 TKG nicht durchsetzen zu wollen.[79] Zahlreiche ISPs kündigten in Folge an, dass sie die neuen Vorschriften zur Vorratsdatenspeicherung vorerst nicht befolgen werden.[80]

Eine ausdrücklich normierte Speicherpflicht (hinsichtlich dynamischer IP-Adressen) besteht deshalb in Deutschland gegenwärtig faktisch nicht.

Die Urheberrechtsindustrie versuchte in der Zwischenzeit jedoch über das Speicher*recht* der ISPs aus dem TKG eine Speicherpflicht zu konstruieren.

---

73 BVerfG, Urteil vom 2. März 2010, Az. 1 BvR 256/08 – bverfg.de.

74 EuGH, Urteil vom 8. April 2014, Rs. C-594/12 – ECLI:EU:C:2014:238 - „Digital Rights Ireland Ltd".

75 EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15, C-698/15 – ECLI:EU:C:2016:970 - „Tele2 Sverige".

76 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl. 2015 I, S. 2218.

77 *Braun*, Grundrechtswidrig bleibt grundrechtswidrig - Reaktionen zum zweiten EuGH-Urteil zur Vorratsdatenspeicherung.

78 OVG NRW, Beschluss vom 22. Juni 2017, Az. 13 B 238/17 – juris. Gegenwärtig anhängig beim BVerwG, Az. 6 C 12.18.

79 https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html - Zugriff am 31.03.2021.

80 *Reuter*, Vorratsdatenspeicherung: Große Provider speichern erstmal nicht.

Grundlage des Speicherrechts ist die Vorschrift des § 96 TKG. Zwar dürfen ISPs IP-Adressen grundsätzlich „erheben“, da diese unter § 96 Abs.1 Satz 1 Nr.1 TKG fallen.[81] „Erheben“ bezieht sich dabei auf eine datenschutzrechtliche Begrifflichkeit, mithin § 3 BDSG, demgemäß eine Erhebung jedwede Datenbeschaffung ist[82]; eine „Verwendung“ der IP-Adressen, also insbesondere deren Speicherung[83] ist allerdings nur soweit zulässig, wie dies für diejenigen Zwecke erforderlich ist, auf die § 96 Abs.1 Satz 2 TKG verweist. Im Übrigen sind sie unverzüglich zu löschen, § 96 Abs.1 Satz 3 TKG.

Nach Auffassung der Rechteinhaber folge nun aus § 96 Abs.1 Satz 2 TKG iVm § 101 Abs.2 und Abs.9 UrhG eine generelle, anlasslose[84] Speicherpflicht, jedenfalls aber eine Speicherpflicht hinsichtlich konkret benannter IP-Adressen auf Zuruf. Die Instanzrechtsprechung bewertete dies sehr unterschiedlich, teils wurde die abstrakte Speicherpflicht bejaht, teils verneint, teils die konkrete bejaht, teils verneint.[85] Als der BGH schließlich mit einem Fall betreffend die konkrete Speicherpflicht betraut wurde, konnte er entsprechend das Bestehen einer abstrakten Speicherpflicht offenlassen.[86] Eine konkrete Speicherpflicht auf Zuruf zur Vorbereitung des Auskunftsanspruchs hinsichtlich genau benannter Adressen bejahte er jedoch – realisiert dadurch, dass Rechteinhaber einen Anspruch auf Unterlassung dahingehend haben, dass ISPs bei IP-Adressen, die ihnen „zugerufen“ wurden, nicht die Zuordnung zum Endkunden löschen dürfen, bis ein hierauf gerichtetes Auskunftsverfahren beendet ist; löschen sie nach Zuruf dennoch, steht eine Schadensersatzpflicht im Raum.[87] Die gerichtliche Durchsetzung dieses Anspruchs findet regulär im

---

81 *Braun* in: Geppert/Schütz, BeckTKG, 4. Aufl. 2013, § 96 TKG, Rz. 7 mit umfangreichen Nachweisen.

82 *Eckhardt* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 96 TKG, Rz. 1.

83 Wiederum wird die datenschutzrechtliche Begrifflichkeit – hier § 3 Abs.5 und Abs.4 BDSG a.F. – referenziert.

84 Bzw. Anlass kann bereits sein, dass eine Urheberrechtsverletzung abstrakt drohen kann.

85 Siehe mit Nachweisen bei BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 26, 54 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

86 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 54 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

87 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 59, 47 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

Rahmen der ZPO statt.[88] Schlagendes Argument für diese Speicherpflicht sei laut BGH, dass die EnforcementRL bezwecke, den Rechteinhabern diejenigen Beweismittel zu sichern, die sie für die Geltendmachung ihrer Ansprüche benötigen. Folgerichtig ergebe sich auch eine Pflicht von ISPs zur Speicherung, da andernfalls der in der EnforcementRL vorgesehene Auskunftsanspruch vereitelt werde.[89]

Als plausibler (ungeschriebener) wirklicher Grund für die Entscheidung erscheint hingegen eine praktische Überlegung, die der BGH angestellt haben dürfte, nämlich dass die Rechteinhaber ohne eine Speicherpflicht darauf angewiesen gewesen wären, dass ISPs freiwillig speichern. Zwar ist die freiwillige Speicherung – soweit ersichtlich – ganz überwiegende Praxis[90]; allerdings gibt es auch ISPs, die *nicht* speichern.

Dies hat folgenden Hintergrund: Der BGH entschied in einem Streit zwischen einem ISP und einem seiner Kunden im Jahr 2011, dass § 96 Abs.1 Satz 2 TKG iVm § 100 Abs.1 TKG grundsätzlich ein siebentägiges, generelles und anlassloses Speicherrecht für IP-Adressen gewähre: bestimmte missbräuchliche Nutzungen eines Internetanschlusses wie beispielsweise Spam-Emails, Hackerangriffe oder DDoS-Attacken würden eine Störung oder Fehler an Telekommunikationsanlagen im Sinne der Norm darstellen.[91] Vom Berufungsgericht waren aber nicht diejenigen Tatsachen festgestellt worden, die erforderlich gewesen wären, um zu subsumieren, ob die Speicherung der IP-Adressen auch im Sinne der Norm erforderlich sei, um diese Störungen zu erkennen, einzugrenzen oder zu beseitigen. Die Sache wurde also zurück verwiesen. Das Berufungsgericht bejahte nach Einholung eines Sachverständigengutachtens schließlich die Erforderlichkeit der Speicherung.[92] Die hiergegen erneut eingelegte Revision wurde 2014 zurückgewiesen.[93]

[88] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 27 – GRUR 2017, 1236 - „Sicherung der Drittauskunft".

[89] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 30, 61ff. – GRUR 2017, 1236 - „Sicherung der Drittauskunft".

[90] Vergleiche hierzu den (unvollständigen) Überblick bei http://wiki.vorratsdatenspeicherung.de/Speicherdauer - Zugriff am 31.03.2021.

[91] BGH, Urteil vom 13. Januar 2011, Az. III ZR 146/10, Rz. 18ff. – MMR 2011, 341 - „Speicherung dynamischer IP-Adressen".

[92] Auch in anderen späteren instanzgerichtlichen Verfahren wurde die Erforderlichkeit sachverständig bestätigt, beispielsweise OLG Köln, Urteil vom 14. Dezember 2015, Az. 12 U 16/13, Rz. 44ff. – NRWE.

[93] BGH, Urteil vom 3. Juli 2013, Az. III ZR 391/13 – NJW 2014, 2500.

Nach Erfahrung des Verfassers können Rechteinhaber regelmäßig innerhalb weniger Tage nach der Ermittlung die Auskunft über die Identität des Anschlussinhabers erlangen. Typischerweise genügt ihnen daher eine siebentägige Speicherfrist. Allerdings hilft ihnen ein freiwillig ausübbares Speicherrecht nicht, wenn – wie es in Deutschland der Fall ist – nicht alle ISPs von diesem Recht Gebrauch machen.[94] Denn dann hängt der Erfolg des Auskunftsbegehrens vom Glück ab, nämlich ob der ISP, den der in einem *filesharing*-System ermittelte Nutzer benutzt hat, speichert oder nicht; darüber hinaus könnten sich *filesharing*-Nutzer für ihren Internetanschluss auch gerade solche ISPs aussuchen, die nicht speichern. Zudem ist gegen das Urteil des BGH betreffend das siebentägige Speicherrecht gegenwärtig noch eine Verfassungsbeschwerde anhängig, die der Entscheidung harrt.[95] Sollte das BVerfG dem BGH widersprechen, erscheint auch das generelle Speicherrecht der ISPs fragwürdig. Dann könnte es passieren, dass die ISPs nicht nur verschiedene Speicherpraxen haben, sondern gar nicht mehr auf Grundlage des § 96 Abs.1 TKG iVm § 100 Abs.1 TKG speichern.

Es erscheint nicht unplausibel, dass der BGH dem durch die Entscheidung „Sicherung der Drittauskunft“ vorbeugen wollte, indem er eine konkrete Speicherpflicht auf Zuruf konstituierte und somit den Auskunftsanspruch der Rechteinhaber sichert, ohne dass diese auf die freiwillige Speicherung der ISPs auf Grundlage des § 96 Abs.1 TKG iVm § 100 Abs.1 TKG angewiesen sind.

f) Die Sicherung des Auskunftsanspruchs bei CG-NAT und dem IPv6-Standard

Verwendet der ISP die CG-NAT, genügt die Speicherung der Zuordnung der IP-Adresse allein nicht, um einen bestimmten Kunden zu identifizieren, sondern es müssen weitere Metadaten gespeichert werden.[96] Es ist nicht bekannt, inwieweit dies auch geschieht. Da aber Strafermittler schon durch CG-NAT in ihren Ermittlungen behindert wurden[97], erscheint es plausibel

[94] Diese ungleiche Praxis wurde in einer späteren instanzgerichtlichen Entscheidung auch nicht als Argument gegen das Speicherrecht an sich akzeptiert, siehe OLG Köln, Urteil vom 14. Dezember 2015, Az. 12 U 16/13, Rz. 48 – NRWE.

[95] BVerfG, Az. 1 BvR 2370/14 – bverfg.de.

[96] Siehe hierzu Kapitel § 1 IV. 5. d).

[97] Siehe hierzu Kapitel § 1 IV. 5. d).

anzunehmen, dass die entsprechenden Metadaten nur von einem Teil der ISPs gespeichert werden.

Ob das Urteil des BGH „Sicherung der Drittauskunft“ auch für diese Metadaten gilt, ist bisher nicht geklärt.[98] Hinsichtlich des IPv6-Standards ist jedoch davon auszugehen, dass das Urteil des BGH „Sicherung der Drittauskunft“[99] auch auf IPv6-Adressen Anwendung finden kann.

Im Ergebnis kann die Sicherung des Auskunftsanspruches bei CG-NAT nach der bisherigen Rechtslage unzulässig sein, bei IPv6-Adressen ist bzw. bleibt sie höchstwahrscheinlich zulässig.

g) Kosten der Sicherung des Auskunftsanspruches und des Auskunftsverfahrens

Ob ISPs Erstattung derjenigen Kosten, die ihnen für die Sicherung des Auskunftsanspruches – also die Speicherung der Zuordnung einer IP-Adresse zu einem bestimmten Anschlussinhaber im Verletzungszeitpunkt – entstehen, von demjenigen Rechteinhaber, der die Sicherung begehrt hat, verlangen können, ist gerichtlich bisher nicht ausdrücklich entschieden. Diese Frage hat der BGH in seinem Urteil über den Sicherungsanspruch[100] nicht angeschnitten. Nach älterer Instanzrechtsprechung zum Sicherungsanspruch können ISPs diese Kosten über § 101 Abs.2 Satz 3 UrhG von Rechteinhabern heraus verlangen.[101] Welche Kosten dies genau betrifft, ist jedoch unklar. Zum Vergleich: im Rahmen der gesetzlichen Vorratsdatenspeicherung[102] müssen ISPs die allgemeinen Infrastrukturkosten der Speicherung gemäß § 113 Abs.5 TKG selbst tragen, während hingegen einzelne Auskunftsbegehren der Behörden einen Entschädigungsanspruch nach § 23 JVEG auslösen können.[103] Da zu dieser Frage keine einschlägige Rechtsprechung bekannt ist, scheinen Rechteinhaber die von den ISPs geltend gemachten Kosten freiwillig zu tragen und diese sodann – mit Billigung des BGH – im Rahmen des Kostenfestsetzungsverfahrens gegen erfolgreich verklagte Anschlussinhaber an letztere

98 Siehe hierzu Kapitel § 5 IV. 1.

99 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

100 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“

101 LG Hamburg, Urteil vom 11. März 2009, Az. 308 O 75/09, Rz. 58 – juris.

102 Siehe Kapitel § 2 III. 1. e).

103 *Graf* in: Graf, BeckOK StPO, 39. Ed. 2021, § 113 TKG, Rz. 43-43.1.

„weiterzureichen“ (hierzu sogleich).

Das Auskunftsbegehren selbst bzw. der Antrag auf Erteilung einer Gestattungsanordnung kostet EUR 200.[104] Die Kosten trägt der Antragsteller, also der Rechteinhaber, § 101 Abs.9 Satz 5 UrhG. In der Instanzrechtsprechung zu dieser Norm ist unstreitig, dass die Zusammenfassung mehrerer IP-Adressen (also potentiell mehrerer Anschlussinhaber) in einem Antrag die Gebühr nicht erhöht[105]; strittig ist nur, ob die EUR 200 pro im Antrag geltend gemachten Werk anfallen oder in einem Antrag mehrere Werke zusammengefasst werden können, ohne dass dies die Kosten erhöht.[106] Sofern der Rechteinhaber (wie üblich) für die Antragstellung einen Rechtsanwalt heranzieht, so hat er dessen Kosten zunächst selbst zu tragen.[107]

Im Ergebnis trägt also der Rechteinhaber anfänglich alle mit dem Auskunftsverfahren verbundenen Kosten selbst. Diese kann er jedoch sämtlich anteilig[108] gegen erfolgreich verklagte Anschlussinhaber geltend machen. Der BGH hat insoweit in dem Beschluss „Deus Ex“ entschieden, dass diese Kosten notwendige Kosten im Sinne des § 91 Abs.1 ZPO und damit im Kostenfestsetzungsverfahren festsetzbar sind.[109] Folglich kann dahinstehen, ob diese Kosten – wenn sie nicht über § 91 Abs.1 ZPO erlangt werden könnten – im Rahmen eines materiellen Anspruches geltend gemacht werden könnten.[110]

---

104 Früher § 128e Abs.1 Nr.4 KostO, nunmehr Zif. 15213 der Anlage 1 des GNotKG.

105 Vgl. OLG Köln, Beschluss vom 11. Februar 2014, Az. 2 Wx 307/13 – juris.

106 *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 101 UrhG, Rz. 20.

107 *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 101 UrhG, Rz. 20.

108 Da mit einem Auskunftsbegehren in der Regel Auskunft über mehrere IP-Adressen begehrt wird, mithin auch potentiell über mehrere Anschlussinhaber.

109 BGH, Beschluss vom 15. Mai 2014, Az. I ZB 71/13 – ZUM 2014, 967 - „Deus Ex“; in einer späteren Entscheidung hat der BGH zudem bestätigt, dass auch die Kosten eines Rechtsanwalts für den Antrag auf Erteilung einer Gestattungsanordnung erstattungsfähig sind, siehe BGH, Beschluss vom 26. April 2017, Az. I ZB 41/16 – GRUR 2017, 854 - „Anwaltskosten im Gestattungsverfahren“.

110 Bejahend OLG Hamburg, Beschluss vom 4. September 2013, Az. 8 W 17/13, Rz. 16, 18 – juris. Problematisch ist jedoch, dass als materieller Anspruch nur ein Schadensersatzanspruch in Frage käme und hierbei wiederum nur die Berechnungsmethode der Differenzhypothese. Da im Verletzungsverfahren die Rechteinhaber jedoch die Berechnungsmethode der Lizenzanalogie wählen, dürfte der Ersatz der Rechtsverfolgungskosten dann ausgeschlossen sein, da nicht mehrere Berechnungsmethoden miteinander kombiniert werden dürfen, aA *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 97 UrhG, Rz. 109.

2. Begrenzung der Abmahngebühren

Ein Nebenaspekt des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums war die Normierung eines Ersatzanspruches für die rechtsanwaltlichen Gebühren einer vorgerichtlichen Abmahnung, angelehnt an die entsprechende Regelung in § 12 UWG.[111] Früher – und in manchen Gebieten wie im Patentrecht noch heute – waren ausdrückliche Regeln zur Abmahnung in den Gesetzen betreffend den gewerblichen Rechtsschutz und das geistige Eigentum nicht vorhanden. Anspruchsgrundlage für die Gebühren war die Geschäftsführung ohne Auftrag nach den §§ 677ff. BGB sowie Schadensersatzansprüche, die Höhe bestimmte sich nach der auf Grundlage des Streitwerts berechneten Geschäftsgebühr nach RVG.[112] Den Streitwert konnten die Gerichte im Prozess autonom bestimmen. Dies führte dazu, dass nicht nur der zu leistende Schadensersatz hunderte von Euro betrug, sondern auch der pro Abmahnung zu leistende Gebührenersatz.[113]

Mit dem nun eingeführten § 97a UrhG wurde der Ersatzanspruch (in § 97a Abs.1 Satz 2 UrhG) ausdrücklich normiert, zugleich seiner Höhe nach aber für „*einfach gelagerte Fällen mit einer nur unerheblichen Rechtsverletzung außerhalb des geschäftlichen Verkehrs*“ auf EUR 100 begrenzt. Der Gesetzgeber hatte jedoch keine Anhaltspunkte dafür gegeben, ob er mit dieser Formulierung die typischen *filesharing*-Konstellationen von der Beschränkung der Gebührenhöhe ausschließen oder in diese einbeziehen wollte. Die Pressemitteilung des BGH zur Entscheidung „Sommer unseres Lebens“[114] deutete darauf hin, dass der BGH in Zukunft (für diese Entscheidung spielte die Norm noch keine Rolle, da die dort behandelte *filesharing*-Nutzung vor dem Inkrafttreten des § 97a UrhG stattgefunden hatte) sich für Ersteres entscheiden werde.[115] Überraschenderweise schloss sich der BGH jedoch, als er schließlich über die Frage zu entscheiden hatte, der Instanzrechtsprechung[116] an, die sich gegen die Anwendung der Beschränkung auf *filesharing*

[111] BT-Drs. 16/5048, S. 35f.
[112] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 11f. – GRUR 2014, 657 - „BearShare“.
[113] Siehe hierzu Kapitel § 3 VI.
[114] Siehe hierzu Kapitel § 2 IV. 1.
[115] BGH, Pressemitteilung Nr. 101/2010.
[116] Mit einem Überblick hierzu siehe *Faustmann/Ramsperger*, MMR 2010, 662, 663.

entschieden hatte.[117]

Mit dem am 9. Oktober 2013 in Kraft getretenen Gesetz gegen unseriöse Geschäftspraktiken[118] wurde § 97a UrhG allerdings ohnehin reformiert und eine andere Beschränkung der Gebührenhöhe eingeführt. § 97a UrhG a.F. ist mithin nur noch für Altfälle relevant. Da diese in der Praxis jedoch mittlerweile überwiegend abgewickelt worden sein dürften[119], ist § 97a UrhG a.F. im Übrigen nicht mehr Gegenstand dieser Arbeit.

3. Dreifache Schadensberechnung

In § 97 Abs.2 UrhG wurde die dreifache Schadensberechnung aufgenommen; diese war jedoch ohnehin bereits zuvor gewohnheitsrechtlich bzw. richterrechtlich anerkannt.[120]

4. Zusammenfassung

Mit dem Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums wurde im Ergebnis also ein – nach der Rechtsprechung des EuGH europarechtlich zulässiger – zivilrechtlicher, nicht-akzessorischer Drittauskunftsanspruch eingeführt, der mit der Rechtsprechung des BGH nicht auf Verletzungen eines bestimmten Ausmaßes beschränkt ist. Mithin kann nach gegenwärtiger Rechtslage bei jeder Urheberrechtsverletzung vom hierfür genutzten ISP Auskunft über den Verletzer erlangt werden. Die hierfür notwendigen Daten muss der ISP, sofern er diese nicht ohnehin schon freiwillig speichert, auf Zuruf sichern.

Die mit dem Gesetz ebenfalls eingeführte Begrenzung der Abmahngebühren wurde mittlerweile durch eine neue Regel ersetzt und ist daher nicht mehr relevant.

---

[117] BGH, Urteil vom 12. Mai 2016, Az. I ZR 1/15, Rz. 48ff. – GRUR 2016, 1275 - „Tannöd“; BGH, Urteil vom 12. Mai 2016, Az. I ZR 272/14, Rz. 55ff. – ZUM 2016, 1037.

[118] Siehe hierzu Kapitel § 2 V.

[119] Siehe hierzu Kapitel § 3 XI. 1. sowie *Reuther*, MMR 2018, 433, 436.

[120] Siehe Kapitel § 2 II.

IV. BGH - „Sommer unseres Lebens“, „Morpheus“, „BearShare“

1. „Sommer unseres Lebens“

Die erste Entscheidung des BGH zur Haftung des Anschlussinhabers für eine Urheberrechtsverletzung durch *filesharing* „Sommer unseres Lebens“[121] erging im Jahr 2010, betraf aber einen im Vergleich zu den später üblichen Sachverhalten atypischen Fall. Denn der beklagte Anschlussinhaber behauptete *unbestritten*, dass er seinen Internetanschluss anderen Personen nicht zur Verfügung stelle, sein PC zum Verletzungszeitpunkt ausgeschaltet und er selbst urlaubsabwesend gewesen sei.[122] Unstreitig war jedoch auch, dass die WLAN-Funktion seines Routers eingeschaltet gewesen sein musste und dieser nicht marktüblich – also nur mit dem werkseitigen, nicht aber mit einem ausreichend langen und persönlichen Passwort[123] – gesichert war.[124] Die Urheberrechtsverletzung musste daher von einem unbekannten Dritten begangen worden sein, der sich unberechtigt von außen auf das WLAN Zugriff verschafft hatte.[125]

Auch wenn dieser Sachverhalt nicht typisch ist – typisch ist ein potentieller Täterkreis aus einer eingrenzbaren Zahl berechtigter Mitnutzer des Anschlusses – ist die Entscheidung „Sommer unseres Lebens“ für das *filesharing* von größter Bedeutung, da sie bezüglich drei Rechtsinstituten die entscheidenden Weichen setzte, nämlich bezüglich der tatsächlichen Vermutung der Täterschaft und der sekundären Darlegungslast des Anschlussinhabers sowie seiner – bei Erfüllung der sekundären Darlegungslast und (ggf.) Widerlegung der tatsächlichen Vermutung greifenden – Haftung als Störer.

---

[121] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08 – GRUR 2010, 633 - „Sommer unseres Lebens“; die dem Fall zu Grunde liegende Auskunft wurde noch auf Grundlage eines Strafverfahrens erteilt, siehe hierzu Kapitel § 2 II.

[122] Siehe hierzu die Vorinstanz OLG Frankfurt a.M., Urteil vom 1. Juli 2008, Az. 11 U 52/07, Rz. 27 – juris; BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 11 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[123] Seine Auffassung bezüglich der werkseitigen Sicherung hat der BGH mittlerweile geändert, siehe Kapitel § 2 XI. 2.

[124] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 34 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[125] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 6 – GRUR 2010, 633 - „Sommer unseres Lebens“.

Die Geltung der tatsächlichen Vermutung statuierte der BGH apodiktisch ohne Begründung.[126] Auch die vom ihm als Beleg referenzierte Rechtsprechung von Instanzgerichten liefert eine solche nicht.[127] Aus der tatsächlichen Vermutung folge eine sekundäre Darlegungslast, die die Vermutung nur entkräfte, wenn ihr ausreichend nachgekommen werde.[128] In dem zu entscheidenden Sachverhalt sei dies der Fall, da die Nichtvornahme der Tathandlung durch den Beklagten unstreitig feststünde.[129]

Er hafte aber jedenfalls als Störer auf Unterlassung (und damit auch auf Ersatz der Rechtsanwaltsgebühren für die vorgerichtliche Abmahnung). Die Geltung der Störerhaftung war in einigen Gebieten des gewerblichen Rechtsschutzes und des geistigen Eigentums für verschiedene Sachverhaltskonstellationen auf Grundlage des § 1004 Abs.1 BGB analog seit vielen Jahren anerkannt[130]; unter Berufung auf einige entsprechende Präjudizien übertrug sie der BGH nun auch auf den Inhaber eines Internetanschlusses.[131] Als Störer hafte generell, wer in irgendeiner Weise willentlich[132] und adäquat-kausal zur Verletzung des geschützten Rechts beiträgt und dabei Prüfpflichten, deren Umfang sich nach der Zumutbarkeit für den in Anspruch genommenen bestimme, verletze.[133] Der adäquat-kausale Beitrag liege im streitigen Fall

[126] Vgl. BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[127] Vgl. OLG Köln, Beschluss vom 11. September 2009, Az. 6 W 95/09, Rz. 7 – juris sowie OLG Köln, Urteil vom 23. Dezember 2009, Az. 6 U 101/09, Rz. 8 – juris; letztere Entscheidung spricht im Übrigen auch nur von einer sekundären Darlegungslast, keiner tatsächlichen Vermutung. Der BGH hat in seiner *filesharing*-Rechtsprechung später selbst die Anwendung der tatsächlichen Vermutung geändert und in Bezug zu der sekundären Darlegungslast nach § 138 Abs.2 ZPO gesetzt.

[128] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[129] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[130] Siehe mit einer Übersicht beispielsweise *Gärtner*, GRUR 2009, 1142, 1147f.

[131] Die Rechtsprechung des BGH zu diesem Punkt ist durch die „Abschaffung“ der Störerhaftung für Anschlussinhaber durch das Dritte Gesetz zur Änderung des Telemediengesetzes mittlerweile in ihren Rechtsfolgen obsolet, allerdings in ihrer dogmatischen Begründung im Zusammenspiel mit der sekundären Darlegungslast weiterhin relevant. Siehe hierzu Kapitel § 4 VII. 3. b).

[132] Dieses Kriterium unterschlägt der BGH aber bei seiner Subsumtion im Folgenden.

[133] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 19 – GRUR 2010, 633 - „Sommer unseres Lebens“.

im Betrieb eines nicht ausreichend gesicherten WLANs[134], die Verletzung einer Prüfpflicht sei in der mangelnden Untersuchung des Routers auf die Qualität seiner Sicherung hin zu sehen.[135] Dass insoweit – anders als bei der Störerhaftung gewerblicher Plattformbetreiber – eine präventive Sicherungspflicht auferlegt werde, d.h. bereits bei der ersten Rechtsverletzung über den Anschluss die Störerhaftung greifen könne, sei für den Anschlussinhaber zumutbar, da mit dem Betreiben des Anschlusses kein Geschäftsmodell verfolgt werde.[136]

2. „Morpheus“

Der Sachverhalt, der der Entscheidung „Morpheus“[137] zu Grunde lag, war ein im Vergleich zu „Sommer unseres Lebens“ ganz typischer *filesharing*-Sachverhalt insoweit, als dass der Anschluss zum Zeitpunkt der Verletzung bewusst und gewollt mehreren Personen – hier der Familie des Anschlussinhabers – grundsätzlich zugänglich war. Er war allerdings in einem Punkt auch eher untypisch, nämlich insoweit, als dass als Täter der Urheberrechtsverletzung einer der minderjährigen Söhne des Beklagten *unstreitig* feststand.[138] Grund dafür ist, dass sich der streitgegenständliche Sachverhalt vor dem 1. September 2008 zutrug, gegen den Beklagten also zunächst staatsanwaltlich ermittelt worden war[139] und sämtliche als Täter in Betracht kommenden Personen verhört worden waren. In späteren Fällen fand auf Grund der rein zivilrechtlich stattfindenden Ermittlung keine polizeiliche Vernehmung der potentiellen Täter mehr statt, sodass sich der wahre, aus dem Kreis der Mitnutzer des Internetanschluss stammende Täter in der Regel nicht frei-

134 BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 20 – GRUR 2010, 633 - „Sommer unseres Lebens“.

135 BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 23 – GRUR 2010, 633 - „Sommer unseres Lebens“.

136 BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 24 – GRUR 2010, 633 - „Sommer unseres Lebens“.

137 BGH, Urteil vom 15. November 2012, Az. I ZR 74/12 – GRUR 2013, 511 - „Morpheus“; für die Namensgebung seiner *filesharing*-Urteile wählt der BGH manchmal – wie zum Beispiel bei „Sommer unseres Lebens“ – die streitgegenständlichen Werke und manchmal – wie eben bei „Morpheus“ – den zur Verletzung verwendeten *filesharing*-Client.

138 BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 4ff., 34 – GRUR 2013, 511 - „Morpheus“.

139 Siehe Kapitel § 2 II.

willig stellte und damit der wahre Täter regelmäßig bis zum Abschluss der entsprechenden Verfahren unbekannt blieb.

Der BGH stellte in „Morpheus“ klar, dass der bisherigen Prüfungsreihenfolge, nach der zuerst zu prüfen war, ob der Anschlussinhaber als Täter der Urheberrechtsverletzung durch eigenes Handeln vermutet werden könne und nach Entkräftung der Vermutung seine Haftung als Störer zu prüfen war, ein anderer Prüfungspunkt voranzustellen sei, nämlich ob der Anschlussinhaber für Schadensersatz und Unterlassung täterschaftlich *aus einem anderen Grund* als der Vornahme der Urheberrechtsverletzung durch *eigenes* Handeln haften könne. Als Haftungsgrundlage hierfür komme zwar nicht schon der Betrieb eines Internetanschlusses an sich – unter dem Gesichtspunkt „Eröffnung einer Gefahrenquelle“ – in Betracht, stattdessen aber § 832 Abs.1 BGB, also die Verletzung der Aufsichtspflicht im Hinblick auf minderjährige Kinder.[140] Im konkreten Fall hätten die Eltern ihrer Aufsichtspflicht genügt, weil sie das minderjährige Kind, das das *filesharing* betrieben hatte, zuvor schon darüber belehrt hatten, dass ihm solches verboten sei; die Durchsuchung des PC des Kindes und andere Überwachungsmaßnahmen würden erst dann Teil der Aufsichtspflicht, wenn die Eltern Kenntnis von einer Urheberrechtsverletzung erlangen.[141]

Weiterhin gelte im nächsten Prüfungsschritt streitgegenständlich auch die tatsächliche Vermutung der Täterschaft des Anschlussinhabers als entkräftet, da die Täterschaft eines Dritten positiv feststehe.[142] Zuletzt hafte der Anschlussinhaber hier auch nicht als Störer. Zwar sei die Störerhaftung grundsätzlich auch in Fällen anwendbar, in denen der Anschlussinhaber einen ausreichend gesicherten Anschluss Dritten zur Benutzung zur Verfügung stelle; soweit die Mitnutzer minderjährige Kinder seien, seien die Prüfpflichten aber mit der Aufsichtspflicht des § 832 Abs.1 BGB identisch.[143] Da dieser entsprochen worden war, haftete der Beklagte also auch nicht als Störer.

[140] BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 38, 13ff. – GRUR 2013, 511 - „Morpheus“. Siehe zur Frage der Neubewertung der täterschaftlichen Haftung *de lege lata* Kapitel § 5 II. 1.

[141] BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 16ff., 29 – GRUR 2013, 511 - „Morpheus“.

[142] BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 32ff. – GRUR 2013, 511 - „Morpheus“.

[143] BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 41ff. – GRUR 2013, 511 - „Morpheus“.

3. „BearShare“

Der in „BearShare“[144] zu entscheidende Sachverhalt entsprach grundsätzlich dem aus „Morpheus“, mit dem Unterschied, dass nicht ein minderjähriger Sohn des Anschlussinhabers als Täter feststand, sondern ein volljährige Stiefsohn der Tat verdächtig war, die Täterschaft aber nicht positiv feststand.[145]

Für Beobachter aus der Praxis reichlich verwirrend[146] schrieb der BGH nun aber – unter Berufung auf „Sommer unseres Lebens“ (!) – dass gar keine tatsächliche Vermutung der Täterschaft des Anschlussinhabers gelte, wenn andere Personen zum Zeitpunkt der Verletzung den Anschluss benutzen konnten.[147] Unabhängig davon bestünde jedoch eine sekundäre Darlegungslast des Anschlussinhabers darüber, ob und gegebenenfalls welche anderen Personen selbstständigen Zugang zu dem Internetanschluss hatten und damit als Täter der Rechtsverletzung in Betracht kommen; in diesem Umfang sei der Anschlussinhaber im Rahmen des Zumutbaren zu Nachforschungen verpflichtet.[148] Könne der Anschlussinhaber der sekundären Darlegungslast nicht genügen, gelte er – so der BGH also implizit – als Täter der Urheberrechtsverletzung.

Im konkreten Fall hätte der Anschlussinhaber aber seiner sekundären Darlegungslast dadurch genügt, dass er vorgetragen hatte, dass sein Stiefsohn der Täter sei[149] – offensichtlich unabhängig davon, dass nicht positiv feststand, ob der Stiefsohn auch der Täter war. Auf Grund der Beweislastverteilung sei der Anschlussinhaber jedenfalls nicht als Täter anzusehen.[150]

Hinsichtlich der Störerhaftung ergänzte der BGH seine bisherige Rechtsspre-

144 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12 – GRUR 2014, 657 - „BearShare“.

145 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 1f., 4 – GRUR 2014, 657 - „BearShare“.

146 Vgl. *Forch*, GRUR-Prax 2015, 49, 49

147 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 15 – GRUR 2014, 657 - „BearShare“.

148 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 18 – GRUR 2014, 657 - „BearShare“. Der BGH verweist dabei auf seine entsprechende Rechtsprechung zum Transportrecht, nämlich BGH, Urteil vom 11. April 2013, Az. I ZR 61/12, Rz. 31 – BeckRS 2013, 18833, mit weiteren Nachweisen.

149 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 1f., 4 – GRUR 2014, 657 - „BearShare“.

150 BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 20 – GRUR 2014, 657 - „BearShare“.

chung: bei der im Rahmen der Ermittlung der Prüfungspflichten zu bewertenden Zumutbarkeit sei die Eigenverantwortung desjenigen, der die rechtswidrige Beeinträchtigung selbst unmittelbar vorgenommen hat oder jedenfalls als Täter in Betracht kommt, zu berücksichtigen. Volljährige (quasi-[151]) Familienangehörige müssten – anders als minderjährige – ohne konkrete Anhaltspunkte dafür, dass sie an Internettauschbörsen teilnehmen, nicht über den erlaubten Nutzungsumfang des Internets belehrt werden.[152] Zur Begründung berief sich der BGH zudem auf den mittelbar durch Art. 6 GG vermittelten Schutz des Vertrauensverhältnisses innerhalb der Familie, das insofern die zu Gunsten des Inhabers der verletzten Urheberrechte wirkende Schutzwirkung des Art. 14 GG überwiege.[153] Ob diese Auslegung des Zumutbarkeitskriteriums auch auf Personen, die nicht familiär verbunden sind, übertragen werden kann, lies der BGH jedoch ausdrücklich offen.[154]

V. Das Gesetz gegen unseriöse Geschäftspraktiken

Dem Gesetzgeber war mittlerweile bekannt geworden, dass seit 2008 massenhaft Abmahnungen wegen *filesharing* versandt worden waren.[155] Der Gesetzesentwurf über das Gesetz gegen unseriöse Geschäftspraktiken ging hierauf ausdrücklich ein. Insbesondere wurde angedeutet, dass der ursprüngliche Zweck der Abmahnungen, Rechtsverletzungen zu unterbinden, in den Hintergrund trete gegenüber dem Ziel, eine Gewinnquelle zu erschließen.[156] Dieser Punkt wurde in den Parlamentsdebatten über den Entwurf besonders hervorgehoben.[157]

Er wurde aber nicht weiter vertieft. Stattdessen wurde betont, es müsse weiterhin wie bisher möglich sein, abzumahnen, nur gegen Missbrauch der Abmahnung solle vorgebeugt werden.[158] Allerdings wurde nicht präzise her-

[151] „Quasi“ da hier nicht ein Sohn, sondern ein Stiefsohn als Täter im Raum stand.
[152] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 22, 24 – GRUR 2014, 657 - „BearShare“.
[153] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 27, 29 – GRUR 2014, 657 - „BearShare“.
[154] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 28 – GRUR 2014, 657 - „BearShare“.
[155] Genaueres hierzu siehe Kapitel § 3 V.
[156] BT-Drs. 17/13057, S. 10f.; siehe hierzu ausführlich Kapitel § 3 VI.
[157] Plenarprotokoll 17/234, S. 29279ff.
[158] Plenarprotokoll 17/234, S. 29282.

ausgearbeitet, worin genau der Missbrauch nun liegt. Es hatte mit der Feststellung sein Bewenden, dass jedenfalls die Abmahngebühren zu hoch und die Abmahnungen zum Teil zu unsauber oder ungenau formuliert seien.[159]

Nach Beschlussempfehlung des Rechtsausschusses[160] trat das Gesetz gegen unseriöse Geschäftspraktiken am 9. Oktober 2013[161] in Kraft und änderte in Bezug auf das Urheberrecht folgende vier Dinge:

- Die alte Gebührenbegrenzung auf EUR 100 wurde ersetzt durch § 97a Abs.3 UrhG n.F. mit einer Begrenzung auf die gesetzlichen Gebühren nach RVG aus einem Streitwert von EUR 1000, also EUR 124. Die Begrenzung gilt nun ausdrücklich immer dann, wenn Abgemahnter eine natürliche Person ist, die nicht kommerziell handelt. Allerdings ist die Begrenzung mit einem Generalklauselvorbehalt der Billigkeit versehen, was ihre Geltung für nicht-kommerzielle Verletzungen wieder unsicher macht.

- Die Abmahnung muss bestimmte inhaltliche (jedoch sehr leicht zu befolgende und eigentlich selbstverständliche) Voraussetzungen erfüllen, um wirksam zu sein, § 97a Abs.2 UrhG n.F. Der Ersatzanspruch greift nur, wenn die Abmahnung wirksam und berechtigt ist, also der geltend gemachte Anspruch materiell besteht.

- Abgemahnte haben nun einen Anspruch auf Ersatz der Kosten ihrer Rechtsverteidigung, wenn die Abmahnung unwirksam oder – für den Abmahnenden erkennbar – unberechtigt ist, § 97a Abs.4 UrhG n.F., wobei die Kostendeckelung nach § 97a Abs.3 UrhG n.F. hier entsprechend gilt.[162]

- Bei nicht-kommerziell handelnden natürlichen Personen gilt nicht der fliegende, sondern der allgemeine Gerichtsstand, § 104a UrhG n.F.

Es soll schon an dieser Stelle angedeutet werden, dass diese Gesetzesreform den Abgemahnten zwar ein Stück weit entgegen kam, jedoch der eigentlich springende Punkt des ganzen Komplexes, die Änderung des ursprünglichen Zwecks der Abmahnung von der Unterbindung von Rechtsverstößen hin zur

[159] Plenarprotokoll 17/234, S. 29282.
[160] BT-Drs. 17/14192.
[161] BGBl. 2013 I, S. 3714.
[162] *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 97a UrhG, Rz. 32.

Erschließung einer Gewinnquelle, nicht tangieren konnte. Hierzu hätten zwei der eigentlichen Säulen des Abmahnwesens angegangen werden müssen: die sekundäre Darlegungslast und die tatsächliche Vermutung der Täterschaft des Anschlussinhabers sowie die übliche Praxis der Berechnung der fiktiven Lizenz.[163] Abmahnungen und Gerichtsverfahren in großer Zahl gab es mithin auch nach 2013.[164]

VI. BGH - Tauschbörse I - III

Nachdem der BGH zwischen 2010 und 2014 „nur“ dreimal zur Haftung eines Anschlussinhabers für *filesharing* zu entscheiden hatte, sollte sich die Frequenz nun deutlich erhöhen. Am 11. Juni 2015 verkündete der BGH gleich drei Entscheidungen hierzu.[165]

1. „Tauschbörse I“

Die Entscheidung „Tauschbörse I“[166] beantwortet primär Fragen, die der Prüfung der Haftung vorgelagert sind, nämlich solche zur Aktivlegitimation, dem Vorliegen einer urheberrechtlich relevanten Verwertungshandlung angesichts der technischen Besonderheiten des *filesharing*, zur Beweiskraft der Ermittlung und zur Beweiskraft der Zuordnung der IP-Adresse zu einem Anschluss durch den ISP, allerdings auch Fragen zur Vermutung der Täterschaft und zur Berechnung des lizenzanalogen Schadens.

Die Eintragung des Klägers in einschlägige Datenbanken des Handels als Rechteinhaber der streitgegenständlichen Werke sei laut BGH grundsätzlich ausreichendes Indiz für seine tatsächliche Rechteinhaberschaft, sofern keine gegenteiligen konkreten Anhaltspunkte vorliegen.[167]

Unerheblich für die Frage der Verletzung sei, ob die streitgegenständlichen Dateien, in denen die streitgegenständlichen Lieder verkörpert waren, voll-

[163] Siehe hierzu Kapitel § 3 VII.

[164] Siehe hierzu Kapitel § 3 V.

[165] In den Urteilen werden zum Teil identische Rechtsfragen beantwortet. Auf solche Rechtsfragen wird bei der Zusammenfassung der Urteile nur bei denjenigen Urteilen eingegangen, bei denen sie – der numerischen Reihenfolge nach – als erstes auftauchen.

[166] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14 – GRUR 2016, 176 - „Tauschbörse I“.

[167] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 20ff. – GRUR 2016, 176 - „Tauschbörse I“.

ständig auf dem PC des Beklagten vorhanden waren. Der BGH ging hierbei nicht auf die Reichweite des Werkschutzes ein, sondern stütze sich allein auf das Leistungsschutzrecht des Tonträgerherstellers nach § 85 Abs.1 Satz 1 UrhG, das die unternehmerische Leistung schützt und sich damit auf den gesamten Tonträger erstrecke, mithin auch auf jedes Dateifragment.[168] Unerheblich sei zudem auch, ob die betroffenen Dateien jeweils vollständig an andere Nutzer der Tauschbörse hochgeladen wurden. Ausreichend sei, dass generell eine Zugriffsmöglichkeit eröffnet worden war, also implizit auch eine Zugriffsmöglichkeit auf bloße Dateifragmente.[169]

Die Tatsache, dass streitgegenständliche Dateien von einer streitgegenständlichen IP-Adresse aus zugänglich gemacht wurden, sei regelmäßig nicht anzuzweifeln, wenn die Mitarbeiter des Ermittlungsdienstes den Ermittlungsvorgang nachvollziehbar schildern könnten.[170]

Von der richtigen Zuordnung einer IP-Adresse zum Inhaber eines Anschlusses beim ISP sei regelmäßig auszugehen und könne nur durch konkrete Anhaltspunkte erschüttert werden.[171]

Weiterhin erteilte der BGH allen Versuchen eine Absage, die Vermutung der Täterschaft des Anschlussinhabers durch Vortrag zu entkräften, der nicht auf die Nutzungsmöglichkeit des Anschlusses durch *andere* Personen als ihm selbst bezogen ist. Konkret seien also Eigenheiten in der Person des Anschlussinhabers[172] unbeachtlich.[173] Auch sei unbeachtlich, ob der Anschlussinhaber zum Tatzeitpunkt persönlich auf den Internetanschluss zugreifen konnte, da *filesharing*-Programme auch bei persönlicher Abwesenheit laufen

[168] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 26f. – GRUR 2016, 176 - „Tauschbörse I“.

[169] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 28 – GRUR 2016, 176 - „Tauschbörse I“.

[170] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 33ff. – GRUR 2016, 176 - „Tauschbörse I“.

[171] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 38ff. – GRUR 2016, 176 - „Tauschbörse I“.

[172] In der Sache wurde vorgetragen, die streitgegenständliche Musik höre er nicht und für ihn sei es als als IT-Fachmann unwahrscheinlich, dass er *filesharing* betreibe, da er das damit verbundene Risiko kenne. Außerdem habe er bisher noch keine weiteren Abmahnungen erhalten, was eigentlich hätte eintreten müssen.

[173] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 49ff. – GRUR 2016, 176 - „Tauschbörse I“.

können.[174]

Die Schadensberechnung bei *filesharing* erfolge zu Recht auf Basis der Lizenzanalogie und dabei – da es keine Vergleichslizenzsätze bezüglich dem öffentlichen Zugänglichmachen eines Werkes in einer Tauschbörse gibt – auf Basis einer fiktiven Lizenz.[175] Dem Tatrichter sei bei der Bemessung des fiktiven Lizenzsatzes gemäß § 287 ZPO ein weites Ermessen eingeräumt, das durch die Revision nur eingeschränkt überprüft werden könne, nämlich nur darauf hin, ob Rechtsgrundsätze der Schadensbemessung verkannt, wesentliche Bemessungsfaktoren außer Acht gelassen oder der Schätzung unrichtige Maßstäbe zu Grunde gelegt wurden.[176]

Spiegelbildlich zur Verletzungshandlung sei es für die Berechnung irrelevant, wie oft die angebotenen Dateien tatsächlich abgerufen wurden, sondern nur, welche Zahl an Abrufen theoretisch möglich war; die Schätzung auf 400 mögliche Abrufe sei dabei mit Verweis auf die Gesamtgröße der streitgegenständlichen Tauschbörse mit ca. 340.000 Teilnehmern nicht unvertretbar.[177]

Weiterhin äußerte der BGH ausdrücklich, dass er die Problematik der Überkompensation[178] nicht übersehe.[179] Dieses Verbot – also das Verbot der Bereicherung mittels des Schadensrechts – sei aber nicht tangiert, da die relevante Verletzungshandlung in der Eröffnung der Zugriffsmöglichkeit für Dritte liege und nicht im Absenden und Empfangen eines Dateifragments. Die Eröffnung der Zugriffsmöglichkeit sei demgegenüber eine eigene Verwertungshandlung. Aber auch bei Annahme einer einheitlichen Verletzungshandlung könne auf Grund der wegen der §§ 830, 840 BGB entsprechend anwendbaren Regeln der Gesamtschuld der Beklagte auch dann vollständig in Anspruch genommen werden, wenn seine Verwertungshandlung und die Verwertungshandlungen der Empfänger der Dateien als einheitlich zu betrachten wä-

[174] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 51 – GRUR 2016, 176 - „Tauschbörse I“.

[175] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 57, 65 – GRUR 2016, 176 - „Tauschbörse I“.

[176] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 57 – GRUR 2016, 176 - „Tauschbörse I“.

[177] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 60f. – GRUR 2016, 176 - „Tauschbörse I“.

[178] Siehe hierzu Kapitel § 4 IX. 2. b).

[179] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 63 – GRUR 2016, 176 - „Tauschbörse I“.

ren.[180]

Eine Einschränkung des Schadensersatzes sei allerdings denkbar, wenn sehr viele Musiktitel streitgegenständlich seien und pro Titel eine Lizenzgebühr von mehr als EUR 200 veranschlagt werde, da ein vernünftig denkender, privater Musiknutzer bei vielen Titeln keine Lizenzgebühr von EUR 200 und mehr pro Titel vereinbaren würde.[181] Im konkreten Fall konnte der BGH dies jedoch dahinstehen lassen, da nur 15 Titel geltend gemacht wurden und sich somit ein Gesamtschadensbetrag von „nur“ EUR 3000 ergab (EUR 0,50 pro Titel mal 400 Abrufmöglichkeiten pro Titel mal 15 Titel). Die Summe von EUR 0,50 pro Titel je Abruf entspreche nach den instanzgerichtlichen Feststellungen den üblichen Lizenzsätzen für legale Abrufe und wurde jedenfalls von der Revision nicht angegriffen.[182]

Die Ausführungen des BGH zu den Abmahngebühren[183] sind wegen der Neuregelung derselben in § 97a UrhG gegenstandslos.[184]

Ausdrücklich nicht Gegenstand der Revision war wegen § 559 Abs.1 ZPO, ob die fehlende Mehrfachermittlung[185] im Rahmen der Beweiswürdigung zu Lasten des Klägers gehe, mithin dem Verletzungsnachweis entgegenstünde.[186]

Aus demselben Grund war ebenfalls nicht Gegenstand der Revision, ob die Leistungsfähigkeit des Internetanschlusses bei der Schadensberechnung zu berücksichtigen ist.[187]

---

[180] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 60f. – GRUR 2016, 176 - „Tauschbörse I“.

[181] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 65. – GRUR 2016, 176 - „Tauschbörse I“.

[182] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 58 – GRUR 2016, 176 - „Tauschbörse I“.

[183] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 66ff. – GRUR 2016, 176 - „Tauschbörse I“.

[184] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 60f. – GRUR 2016, 176 - „Tauschbörse I“. Sie können allenfalls im Rahmen von § 97a Abs.3 Satz 3 UrhG eine Rolle spielen, siehe hierzu Kapitel § 4 X.

[185] Siehe hierzu Kapitel § 5 III. 2.

[186] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 36 – GRUR 2016, 176 - „Tauschbörse I“.

[187] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 62 – GRUR 2016, 176 - „Tauschbörse I“.

2. „Tauschbörse II“

Die Entscheidung „Tauschbörse II“[188] führt im Wesentlichen die Rechtsprechung aus „Morpheus“[189] weiter und macht zudem einige Aussagen zur Berechnung des Schadensersatzes.

Die Belehrungspflicht hinsichtlich minderjähriger Kinder über die Rechtswidrigkeit der Nutzung von Tauschbörsen wird bekräftigt. Eine generelle Ermahnung zu rechtmäßigem Verhalten genüge dieser nicht.[190] Da eine Belehrung im konkreten Fall nicht erteilt worden war, hafteten die Eltern nach § 832 Abs.1 BGB. Im Rahmen von § 832 BGB finde für die Berechnung des Schadensersatzes die dreifache Schadensberechnung, mithin auch die Lizenzanalogie Anwendung, wenn der Rechtsverstoß des Kindes, der Gegenstand der Aufsichtspflichtverletzung ist, eine Urheberrechtsverletzung ist.[191]

Hinsichtlich der Berechnung der Summe der fiktiven Lizenzgebühr komme es nicht darauf an, ob der Beklagte generell bereit gewesen wäre, einen Lizenzvertrag zu schließen.[192] Auch sei hinsichtlich der möglichen Zugriffszahlen unerheblich, in welcher Sprache der Musiktitel sei.[193] Die Veranschlagung von EUR 0,50 pro Titel je Abruf werde nicht dadurch in Zweifel gezogen, dass bei Angeboten wie *Spotify* niedrigere Lizenzsätze veranschlagt werden, da es sich hierbei nach Einschätzung der Vorinstanzen um Streaming- und nicht um Downloaddienste und folglich um ein anderes Geschäftsmodell handle; diese Einschätzung sei nicht erfahrungswidrig, mithin der gegenteilige Vortrag der Revision unbeachtlich.[194]

Die Ausführungen zu der Höhe der Abmahngebühren[195] sind wegen der Neu-

---

188 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14 – GRUR 2016, 184 - „Tauschbörse II“.

189 Siehe hierzu Kapitel § 2 IV. 2.

190 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 32, 38 – GRUR 2016, 184 - „Tauschbörse II“.

191 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 42 – GRUR 2016, 184 - „Tauschbörse II“.

192 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 41 – GRUR 2016, 184 - „Tauschbörse II“.

193 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 47 – GRUR 2016, 184 - „Tauschbörse II“.

194 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 52 – GRUR 2016, 184 - „Tauschbörse II“.

195 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 56ff. – GRUR 2016, 184 - „Tauschbörse II“.

regelung derselben in § 97a UrhG wiederum gegenstandslos.[196] Inhaltlich sei die Forderung auf Ersatz der Abmahngebühren nicht rechtsmissbräuchlich, da nicht erkennbar sei, dass die Abmahnung hier – und insoweit übertragbar auf die allermeisten Abmahnfälle – primär den Zweck verfolge, eine möglichst hohe Geldforderung zu realisieren.[197] Auch sei nicht erkennbar, dass die Klägerin der Prozessbevollmächtigten eine niedrigere Gebühr für die Rechtsvertretung zahle, als im Rahmen der Abmahnung eingefordert werde. Hierfür müssten konkrete Zweifel geltend gemacht werden, wofür – und insoweit ebenfalls übertragbar auf die allermeisten Abmahnfälle – ein allgemeiner Verdacht, auch wenn er begründet ist, nicht ausreichend sei.[198]

3. „Tauschbörse III“

Die Entscheidung „Tauschbörse III“[199] bekräftigt im Wesentlichen die Rechtsprechung aus „BearShare“[200], beantwortet aber auch Fragen zum Schadensersatz und zum Gebührenersatzanspruch.

Anders als in „BearShare“, wo der Beklagte vorgetragen hatte, sein Stiefsohn sei Täter gewesen, trug der Beklagte in „Tauschbörse III“ vor, zum Tatzeitpunkt seien er und seine ganze Familie urlaubsabwesend und der einzige PC im Haushalt so wie der Router vom Stromnetz genommen gewesen. Der Vortrag zur Urlaubsabwesenheit wurde jedoch als höchst unglaubwürdig bewertet.[201] Der Beklagte hatte sich durch diesen Vortrag weitere Verteidigungsmöglichkeiten abgeschnitten: der BGH wollte den Hilfsvortrag[202] dahingehend, dass jedenfalls die Möglichkeit bestand, dass seine Kinder – anders als zunächst vorgetragen und von diesen bezeugt – heimlich vor Abreise den PC und Router ans Stromnetz angeschlossen hätten und während der Urlaubsabwesenheit das *filesharing*-Programm laufen ließen, nicht gelten las-

196 Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 60f. – GRUR 2016, 176 - „Tauschbörse I“.

197 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 70 – GRUR 2016, 184 - „Tauschbörse II“.

198 BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 56ff. – GRUR 2016, 184 - „Tauschbörse II“.

199 BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14 – GRUR 2016, 191 - „Tauschbörse III“.

200 Siehe hierzu Kapitel § 2 IV. 3.

201 BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 31ff. – GRUR 2016, 191 - „Tauschbörse III“.

202 Wohl angesichts des als Lüge entlarvten Erstvortrags.

sen.[203] Ein Beklagter muss sich im Rahmen seiner sekundären Darlegungslast also an seinem eigenen Vortrag messen lassen; wird dieser im Rahmen einer Beweisaufnahme als unrichtig angesehen, kann es ihm nicht zu Gute kommen, wenn dann ein im Umkehrschluss stattdessen naheliegender Sachverhalt (hier also die Anwesenheit seiner gesamten Familie zum Tatzeitpunkt) ebenfalls gegen die Vermutung seiner Täterschaft gesprochen hätte (unbeachtliche Schutzbehauptung).[204] Im Ergebnis bestand daher – da auf Grund der Verschlüsselung des WLAN die Täterschaft eines unbekannten Dritten ausgeschlossen werden konnte[205] – die bloß abstrakt-theoretische Zugriffsmöglichkeit eines Dritten, die zur Entkräftung der tatsächlichen Vermutung nicht genügt.[206] Dies gilt auch dann, wenn besagter Dritter im Haushalt des Anschlussinhabers lebt.[207]

Die Sachverhaltskonstellation in „Tauschbörse III“ ist relativ untypisch, da Anschlussinhaber regelmäßig nicht die Abwesenheit aller potentiellen Mitnutzer zum Tatzeitpunkt behaupten und sich somit nicht durch ihren Vortrag selbst schaden. Aus dem Urteil folgt allerdings, dass einem Anschlussinhaber, der keine potentiellen Mitnutzer zum Tatzeitpunkt nennen kann, die Entkräftung der tatsächlichen Vermutung seiner Täterschaft regelmäßig verwehrt bleibt.[208]

Der BGH klärt damit das Verhältnis zwischen sekundärer Darlegungslast und tatsächlicher Vermutung: aus der Behauptung des Klägers, der beklagte Anschlussinhaber sei Täter, trifft Letzteren eine sekundäre Darlegungslast darüber, welche Personen statt seiner als Täter der Urheberrechtsverletzung

[203] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 40 – GRUR 2016, 191 - „Tauschbörse III“.

[204] Im konkreten Fall kam jedoch noch hinzu, dass selbst bei der Annahme der Anwesenheit aller Familienangehörigen der Anschlussinhaber nicht exkulpiert gewesen wäre, da nach seinem eigenen Vortrag unbeaufsichtigt niemand außer ihm den einzigen PC im Haushalt nutze, siehe BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 41 – GRUR 2016, 191 - „Tauschbörse III“.

[205] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 46 – GRUR 2016, 191 - „Tauschbörse III“.

[206] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 31ff. – GRUR 2016, 191 - „Tauschbörse III“.

[207] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 42 – GRUR 2016, 191 - „Tauschbörse III“.

[208] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 37 – GRUR 2016, 191 - „Tauschbörse III“.

in Betracht kommen. Genügt er dieser nicht, wird seine Täterschaft vermutet.[209] Diese rein tatsächliche Vermutung ist dann theoretisch rein rechtlich betrachtet noch widerlegbar, faktisch aber nicht.

Außerdem wiederholt der BGH die aus „BearShare“ bekannte Nachforschungspflicht, ohne diese inhaltlich weiter zu definieren.[210] Zusätzlich fügt er geräuschlos eine weitere Pflicht ein, nämlich die Pflicht der Mitteilung aller Kenntnisse, die der Anschlussinhaber über die Verletzungshandlung gewonnen hat (Mitteilungspflicht).[211]

Bezüglich der Berechnung des Schadensersatzes bestätigte der BGH die Selbstverständlichkeit, dass es im Rahmen der Lizenzanalogie nicht auf einen nachweisbar kausal entstandenen entgangenen Gewinn (konkret: die streitgegenständlichen Lieder wären käuflich erworben worden, wenn der Beklagte keinen Zugriff durch *filesharing* auf diese ermöglicht hätte) ankommt.[212] Nicht Gegenstand der Revision wurde jedoch die Frage, ob bei Minderjährigen die Berechnung der Lizenzanalogie sich unter Umständen anders gestalten kann als bei Volljährigen.[213]

Ersatz der Abmahngebühren kann auch dann verlangt werden, wenn der Unterlassungsanspruch nur in der Abmahnung, nicht aber – bei Unterbleiben der Abgabe einer strafbewehrten Unterlassungserklärung – im Klageverfahren geltend gemacht wird.[214]

VII. Sechsmal BGH

Am 12. Mai 2016 verkündete der BGH gleich sechs Entscheidungen zur Haftung des Inhabers eines Internetanschlusses für *filesharing*. Die Entschei-

[209] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 48, 37 – GRUR 2016, 191 - „Tauschbörse III“.

[210] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 37 – GRUR 2016, 191 - „Tauschbörse III“.

[211] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 42 – GRUR 2016, 191 - „Tauschbörse III“.

[212] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 54 – GRUR 2016, 191 - „Tauschbörse III“.

[213] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 55 – GRUR 2016, 191 - „Tauschbörse III“.

[214] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 61f. – GRUR 2016, 191 - „Tauschbörse III“.

dungen haben nur teilweise einen Namen. Sie werden daher für die Zwecke dieser Arbeit nach Aktenzeichen aufsteigend (zusätzlich) als „Tauschbörse“ bezeichnet.[215]

1. Tauschbörse IV - VII

Das Urteil „Tauschbörse IV“[216] enthält nur Ausführungen zum Gegenstandswert der Unterlassung, auf Grundlage dessen die Abmahngebühren zu berechnen sind, und § 97a UrhG a.F. Es ist damit für die heutige Rechtslage gegenstandslos. Da in *filesharing*-Prozessen ganz regelmäßig nur der Schadensersatz und die Abmahngebühren, nicht jedoch die Unterlassung der Rechtsverletzung geltend gemacht wird bzw. wegen abgegebener Unterlassungserklärungen nicht geltend gemacht werden kann, ist der Gegenstandswert auch für die Berechnung der Prozesskosten irrelevant.[217] Relevant werden kann der Gegenstandswert daher nur[218] noch bei Verstoß gegen die Unterlassungserklärung, da in diesem Fall die Gebührenbegrenzung wegen § 97a Abs.2 Satz 2 Nr.2 UrhG nicht greift.[219] Die *filesharing*-Fälle aber, in denen gegen eine Unterlassungserklärung verstoßen wurde, sind so selten[220], dass hierauf in der Arbeit nicht weiter eingegangen wird. Die Berechnung des Gegenstandswerts bei *filesharing*-Fällen wird im Ergebnis in dieser Arbeit insgesamt nicht weiter untersucht.

Für die Urteile „Tauschbörse V / Tannöd“[221], „Tauschbörse VI“[222] und „Tauschbörse VII“[223] gilt inhaltlich dasselbe wie für „Tauschbörse IV“.

---

[215] In den Urteilen werden zum Teil identische Rechtsfragen beantwortet, sowohl im Vergleich untereinander als auch im Vergleich zu Tauschbörse I-III. Auf solche Rechtsfragen wird bei der Zusammenfassung der Urteile nur bei denjenigen Urteilen eingegangen, bei denen sie – der numerischen Reihenfolge nach – als erstes auftauchen.

[216] BGH, Urteil vom 12. Mai 2016, Az. I ZR 272/14 – ZUM 2016, 1037.

[217] Siehe hierzu auch Kapitel § 4 II. 2. c).

[218] Siehe zu einer weiteren, zukünftigen Möglichkeit Kapitel § 5 XI.

[219] Siehe hierzu beispielsweise OLG Schleswig, Teilversäumnis- und Schlussurteil vom 25. Januar 2017, Az. 6 U 9/16 – aw3p.de sowie OLG Schleswig, Urteil vom 5. Oktober 2017, Az. 6 U 47/16 – aw3p.de.

[220] Neben den genannten Fällen des OLG Schleswig ist dem Verfasser nur eine einzige Entscheidung bekannt, die eine solche Konstellation zum Gegenstand hatten, siehe LG Flensburg, Urteil vom 13. Juni 2018, Az. 8 O 25/16 – aw3p.de.

[221] BGH, Urteil vom 12. Mai 2016, I ZR 1/15 – GRUR 2016, 1275 - „Tannöd“.

[222] BGH, Versäumnisurteil vom 12. Mai 2016, Az. I ZR 43/15 – ZUM-RD 2017, 25.

[223] BGH, Versäumnisurteil vom 12. Mai 2016, Az. I ZR 44/15 – ZUM-RD 2017, 30.

2. „Tauschbörse VIII / Every time we touch“

In „Tauschbörse VIII / Every time we touch“[224] präzisierte der BGH seine – leicht missverständlichen – Aussagen aus „Tauschbörse III“ zur sekundären Darlegungslast. Der Vortrag über die Mitnutzer müsse sich auf die Nutzungssituation im Verletzungszeitpunkt beziehen. Zudem müsse zum Nutzungsverhalten, den Kenntnissen und den Fähigkeiten der Mitnutzer vorgetragen werden – also um solche Mitnutzer als mögliche Täter auszuschließen, die auf Grund persönlicher Eigenschaften nicht als Täter in Betracht kommen.[225] Im konkreten Fall wurde jedenfalls der Vortrag des Beklagten auf Grund der Zeugenaussagen seiner Familienmitglieder als unplausibel zurückgewiesen, da die anderen Familienmitglieder nach Würdigung ihrer Aussagen nicht als Täter in Betracht kämen.[226] Implizit legte der BGH damit auch fest, dass es also nicht nur auf die Darlegungen des Anschlussinhabers ankommt, sondern auch darauf, ob diese angesichts der Zeugenaussagen der Mitnutzer plausibel erscheinen. In „BearShare“ hatte es zur Erfüllung der sekundären Darlegungslast ausgereicht, dass der Anschlussinhaber seinen Stiefsohn als Täter benannt hatte, obwohl diese Tatsache strittig war. Nunmehr[227] ist nach „Tauschbörse VIII / Every time we touch“ davon auszugehen, dass sowohl die Darlegung der Umstände der Anschlussnutzung als auch die Nennung eines konkreten Täters nicht ausreichen, sondern sich entweder das eine oder das andere nach tatrichterlicher Würdigung der entsprechend gehörten Zeugen als plausibel darstellen muss, wobei nur in letzterem Falle die Täterschaft des Anschlussinhabers definitiv ausgeschlossen ist. Erscheint nur sein Vortrag zur Nutzungssituation plausibel oder trägt er nur hierzu vor, kann er immer noch als Täter angesehen werden, wenn die übrigen Nutzer im Anschluss an ihre Zeugenvernehmung nach tatrichtlicher Würdigung nicht als Täter in Betracht kommen.

---

[224] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15 – GRUR 2016, 1280 - „Every time we touch“.

[225] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 34, 50 – GRUR 2016, 1280 - „Every time we touch“. In Bezug auf familiär verbundene Mitnutzer revidierte der BGH diese Aussage in einem späterem Urteil jedoch, siehe Kapitel § 2 XI. 1.

[226] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 36ff. – GRUR 2016, 1280 - „Every time we touch“.

[227] Wobei zu berücksichtigen ist, dass die Zeugenaussagen nach einer später erfolgten Klarstellung des BGH erst im Rahmen der Beweiswürdigung, nicht schon bei der sekundären Darlegungslast zu bewerten sind, siehe Kapitel § 2 XI. 4.

Weiterhin urteilte der BGH zum Schadensersatzanspruch, dass dieser zwar gemäß § 102 Satz 1 UrhG iVm §§ 195, 199 BGB der regelmäßigen Verjährungsfrist von drei Jahren unterliege, der lizenzanaloge Schaden auf Basis einer fiktiven Lizenz aber auch als ungerechtfertigte Bereicherung gemäß § 102 Satz 2 UrhG iVm § 852 Satz 1 BGB innerhalb der zehnjährigen Verjährungsfrist verlangt werden könne (sogenannter Restschadensersatzanspruch).[228]

3. „Tauschbörse IX / Silver Linings Playbook“

In „BearShare“ hatte der BGH noch offen gelassen, welche Prüfpflichten den Anschlussinhaber im Rahmen der Störerhaftung treffen, wenn die Mitnutzer (jedenfalls teilweise) nicht familiär verbundene volljährige Personen sind. Dass gegenüber volljährigen Familienangehörigen ohne konkrete Anhaltspunkte für deren Fehlverhalten keine Belehrungspflichten bestehen, hatte der BGH erstens auf deren Eigenverantwortung und zweitens auf eine Abwägung der Grundrechte Art. 6 und Art 14 GG miteinander gestützt. In der Entscheidung „Tauschbörse IX / Silver Linings Playbook“[229] stellte der BGH volljährige nicht familiär verbundene Personen, also insbesondere Mitbewohner einer Wohnungsgemeinschaft, Gäste und Besucher den volljährigen Familienangehörigen gleich.[230] Die Argumentation war im Grundsatz dieselbe wie bei „BearShare“. Bei Volljährigen könne man sich grundsätzlich auf deren Eigenverantwortung verlassen.[231] Zur Begründung berief sich der BGH darauf, dass der Zugang zum Internet nach den heutigen gesellschaftlichen Verhältnissen eine übliche Gefälligkeit darstelle; zudem berief er sich auf seine Präjudizien zur Überlassung von Telefon, Kraftfahrzeug oder Wohnung, in denen ebenfalls ohne konkreten Anlass keine Belehrung über den Umgang mit dem überlassenen Gegenstand als erforderlich erachtet worden

[228] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 92ff. – GRUR 2016, 1280 - „Every time we touch“. Später noch einmal bestätigt durch BGH, Beschluss vom 23. Januar 2017, Az. I ZR 265/15 – ZUM 2017, 596.

[229] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15 – GRUR 2016, 1289 - „Silver Linings Playbook“.

[230] Die täterschaftliche Haftung des beklagten Anschlussinhabers schied aus, weil die von ihm genannten Mitnutzer die Tat eingeräumt hatten, siehe BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 3 – GRUR 2016, 1289 - „Silver Linings Playbook“.

[231] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 18f. – GRUR 2016, 1289 - „Silver Linings Playbook“.

war.[232] Die Grundrechtsabwägung erweiterte der BGH um die europäische Dimension. Den Eigentumsgrundrechten von Art. 17 Abs. GRC und Art. 14 GG stellte er die Grundrechte auf Informationsfreiheit nach Art. 11 GRC und Art. 5 Abs.1 Satz 1 GG sowie das Recht auf Freiheit und Achtung des Privatlebens nach Art. 6, 7 GRC und Art. 2 Abs.1 GG gegenüber.[233] In der Abwägung gab er Letzteren den Vorzug, da erstens empirisch betrachtet nicht festgestellt sei, dass von der streitgegenständlichen Form der Anschlussteilung Urheberrechtsverletzungen in nennenswertem Umfang begangen würden, und zweitens, dass Rechteinhaber durch die Rechtsprechung des BGH zur sekundären Darlegungslast ausreichend abgesichert seien.[234]

Zuletzt würde sich auch in richtlinienkonformer Auslegung nach Art. 9 Abs.1 lit.a) EnforcementRL und Art. 8 InfoSoc nichts anderes ergeben, da sich diesen keine anlasslose Belehrungspflicht für volljährige Personen entnehmen lasse (diese Normen mithin zu allgemein seien, als dass sich hieraus derart konkrete Pflichten ableiten ließen).[235]

VIII. Zweites Gesetz zur Änderung des Telemediengesetzes

Lange Zeit wurde von den meisten Gerichten die Frage ignoriert, ob die Privilegierungen des Telemediengesetzes (TMG) auf Anschlussinhaber Anwendung finden können. Der BGH hatte in „Sommer unseres Lebens“ lediglich mit wenigen Worten festgehalten, dass das Hostprovider-Privileg nach § 10 TMG nicht einschlägig sei.[236] Dies dürfte aber ohnehin völlig unstreitig sein,

[232] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 21f. – GRUR 2016, 1289 - „Silver Linings Playbook“.

[233] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 26 – GRUR 2016, 1289 - „Silver Linings Playbook“.

[234] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 27f. – GRUR 2016, 1289 - „Silver Linings Playbook“.

[235] BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 24f. – GRUR 2016, 1289 - „Silver Linings Playbook“.

[236] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 24 – GRUR 2010, 633 - „Sommer unseres Lebens“.

da Anschlussinhaber keine Daten ihrer Mitnutzer speichern[237], sondern nur durchleiten. Fraglich wäre also allein gewesen, ob und wenn ja, inwieweit, das Accessprovider-Privileg nach § 8 TMG Anwendung finden kann. Hierzu hätte geklärt werden müssen, ob ein Anschlussinhaber ein „*Diensteanbieter*“ im Sinne von § 2 Satz 1 Nr.1 TMG und § 8 TMG sein kann, wie „*nicht verantwortlich*“ in § 8 Abs.1 Satz 1 TMG auszulegen ist und wie dabei jeweils die Art. 2, 14 der ECommerceRL[238], die mit den genannten Vorschriften des TMG umgesetzt werden, zu berücksichtigen sind.

In vereinzelten Entscheidungen widmeten sich ab 2014 immerhin einige Instanzgerichte der Anwendbarkeit des TMG und bejahten diese.[239] In der Literatur war diese Frage dagegen bereits seit 2002 diskutiert und bejaht worden.[240] Öffentliches Bekanntheit erlangte diese Frage aber erst mit der Vorlage des LG München I an den EuGH in der Sache „McFadden“[241], mit der mehrere Fragen der Auslegung des TMG im Zusammenhang mit der ECommerceRL beantwortet werden sollten.[242]

Parallel dazu wurde jedoch der Gesetzgeber aktiv und wollte die Entscheidung des EuGH nicht abwarten. Im Koalitionsvertrag der großen Koaliti-

[237] Eine Speicherung findet in technischer Hinsicht bei Einsatz eines WLAN-Sniffers statt, siehe Kapitel § 1 V. 2. a). Die Frage, ob auf diese gespeicherten Daten § 10 TMG Anwendung findet, ist jedoch praktisch irrelevant, da der Anschlussinhaber diese Daten nicht dem Zugriff der Öffentlichkeit aussetzt.

[238] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“).

[239] Beispielsweise AG Hamburg, Urteil vom 10. Juni 2014, Az. 25b C 431/13 – juris und AG Hamburg, Urteil vom 24. Juni 2014, Az. 25b C 924/13 – juris für Hotels bzw. Ferienwohnungen; für Freifunk AG Charlottenburg, Urteil vom 17. Dezember 2014, Az. 217 C 121/14 – juris. Der BGH hat dem nunmehr ebenfalls zugestimmt, siehe BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 18 – GRUR 2018, 1044 - „Dead Island“. Da aber 2016 und 2017 das TMG in diesem Punkt reformiert worden ist, ist die Entscheidung nur noch für Altfälle relevant.

[240] Zur Vorgängervorschrift im TDG: *Röhrborn/Katko*, CR 2002, 882, 887; *Mantz*, MMR 2006, 763, 765f.; *Roggenkamp*, jurisPR-ITR 12/2006, Anm. 3. Zum TMG: *Gietl*, MMR 2006, 630, 631; *Mantz*, Rechtsfragen offener Netze, S. 46ff., 291f.; *Stang/Hühner*, GRUR-RR 2008, 273, 275; *Mantz/Gietl*, MMR 2008, 603, 608; *Borges*, NJW 2010, 2624, 2627; *Mantz*, MMR 2011, 401, 403; *Kirchberg*, ZUM 2012, 544, 549; *Mantz*, GRUR-RR 2013, 497, 498; *Borges*, NJW 2014, 2305, 2309f.

[241] LG München I, EuGH-Vorlage vom 18. September 2014, Az. 7 O 14719/12 – juris.

[242] Siehe hierzu Kapitel § 2 IX.

on von 2013 war vereinbart worden, dass die Haftung von Betreibern eines WLAN klargestellt werden soll.[243] Der Koalitionsvertrag bezog sich aber auf das bisher mangelnde Vorhandensein offener Netze im öffentlichen Raum. Gemeint war also wohl der Zugriff aufs Internet mittels mobiler Geräte auf eher weniger bandbreitenintensive Anwendungen (mobiles Surfen, soziale Netzwerke, Messengerdienste und ähnliches). Zur Haftung von Betreibern geschlossener WLANs oder der kabelgestützten Anschlussteilung[244] (beides insbesondere im Heimbereich anzutreffen) war jedoch nicht die Rede. Entsprechend war als Zielsetzung des nachfolgenden Gesetzesentwurfes auch lediglich formuliert, frei verfügbares WLAN im öffentlichen Raum zu fördern.[245] Zum Problem der Abmahnungen gerade auch im Heimbereich verhielt sich der Gesetzesentwurf jedoch gerade nicht. Es wurde dort aber auch nicht ausdrücklich ausgeschlossen, dass die – dem Wortlaut nach eher offen gehaltenen – Ergänzungen des TMG auf entsprechende Sachverhalte Anwendung finden können. In der Sache sollte dem § 8 TMG ein Absatz 3 zugefügt werden, demgemäß Diensteanbieter auch sei, wer Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellt – mithin die in der Literatur ohnehin schon herrschende Auffassung über die Anwendbarkeit auf Anschlussinhaber deklaratorisch klargestellt werden. Ausweislich des Entwurfs sollte hierbei egal sein, ob das Zur-Verfügung-Stellen einen kommerziellen Hintergrund hat oder nicht.[246] Die eher technisch formulierte Definition des „drahtlosen lokalen Netzwerkes“ in dem neuen § 2 Satz 1 Nr.2a TMG sollte lediglich klarstellen, dass hiermit der WLAN-Standard und nicht etwa Mobilfunk-oder Bluetoothnetze oder Satellitenkommunikation gemeint sei.[247]

Da nach der Rechtsprechung des BGH die Formulierung „*nicht verantwortlich*“ in § 8 Abs.1 Satz 1 TMG sich bisher nicht auf Beseitigungs-und Unterlassungsansprüche erstreckte[248], war zudem ein Absatz 4 für § 8 TMG geplant gewesen, demgemäß diese beiden Ansprüche ausscheiden, wenn der An-

[243] „Deutschlands Zukunft gestalten“, Koalitionsvertrag zwischen CDU, CSU und SPD für die 18. Legislaturperiode, S. 9, 35.
[244] Siehe Kapitel § 1 3. a) aa) und Kapitel § 1 IV. 3.
[245] BT-Drs. 18/6745, S.1, 7f.
[246] BT-Drs. 18/6745, S. 8.
[247] BT-Drs. 18/6745, S. 17.
[248] *Paal/Hennemann* in: Gersdorf/Paal, BeckOK InfoMedienR, 31. Ed. 2021, § 7 TMG, Rz. 54.

schlussinhaber bestimmte Sicherungsmaßnahmen ergreift[249] – diese zielten ihrem Wortlaut nach wohl auf einen Hotspotbetrieb des WLAN ab.[250] Dieser Teil des Entwurfs wurde jedoch von der EU-Kommission im Rahmen des nach der RL (EU) 2015/1535 durchzuführenden Notifizierungsverfahrens bemängelt[251], weil die im Entwurf angedachten Sicherungsmaßnahmen womöglich dasjenige überstiegen, was nach ECommerceRL und EU-Grundrechten von einem Anschlussinhaber gefordert werden könne.[252]

Entsprechend wurde mittels eines Änderungsantrages die Streichung des Absatzes 4 beantragt, wobei die ausdrücklich in Absatz 4 formulierte Geltung der Haftungsprivilegierung für Beseitigungs-und Unterlassungsansprüche implizit weitergelten solle.[253] Die Änderung wurde in der Beschlussempfehlung des zuständigen Ausschusses angenommen, wobei auch dort davon ausgegangen wurde, dass die Privilegierung für den Unterlassungs-und Beseitigungsanspruch bzw. die Störerhaftung gelte.[254] In der 2. Beratung über den Gesetzesentwurf wurde jedoch von der Opposition zu Recht darauf hingewiesen, dass nach der Rechtsprechung des BGH Erwägungen des Gesetzgebers in Gesetzesentwürfen nicht zu berücksichtigen seien, wenn sie keinen ausdrücklichen Niederschlag im Gesetzeswortlaut gefunden hätten.[255]

Dennoch trat der Entwurf mit den dargestellten Ergänzungen (außer eben § 8 Abs.4 TMG) als Zweitens Gesetz zur Änderung des Telemediengesetzes (2. TMGÄndG)[256] am 27. Juli 2016 in Kraft.

IX. EuGH - „McFadden“

Anders als andere Instanzgerichte[257] sah sich das LG München I (berechtigterweise) nicht in der Lage, die Anwendbarkeit des TMG auf Anschlussinhaber sowie gegebenenfalls die Reichweite der Haftungsprivilegierungen ohne

[249] BT-Drs. 18/6745, S. 6.
[250] Siehe dazu Kapitel § 1 IV. 3.
[251] Notifizierungsnummer 2015/305/D.
[252] *Beckedahl*, EU-Kommission kritisiert Gesetz-Entwurf zur Verschlimmbesserung der Störerhaftung.
[253] Ausschussdrs. 18(9)822.
[254] BT-Drs. 18/8645, S. 10.
[255] Plenarprotokoll 18/173, S. 17058; siehe dazu auch Kapitel § 4 IV. 1. d).
[256] BGBl. 2016 I, S. 1766.
[257] Siehe Kapitel § 2 VIII.

Vorlage an den EuGH zu beantworten. In der Sache „McFadden“[258] hatte der Anschlussinhaber seinen WLAN-Anschluss zum Zeitpunkt der Verletzung offen betrieben. Das WLAN trug zwar nicht zum Verletzungszeitpunkt, aber ansonsten die meiste Zeit als Bezeichnung[259] den Namen seiner Webseite, mit dem er Personen auf sein Geschäft aufmerksam machen wollte, von dem aus er das WLAN betrieb.[260] Die Nutzung des WLAN war auch nicht kostenpflichtig.[261] Der Anschlussinhaber bestritt seine Täterschaft, das LG München I ging in Folge dessen davon aus, diesen nach Beantwortung der europarechtlichen Fragen gegebenenfalls nur als Störer verurteilen zu können.[262]

In seinem Urteil[263] stimmte der EuGH weit überwiegend mit den Schlussanträgen überein: Zunächst könne ein WLAN-Betreiber Diensteanbieter im Sinne der ECommerceRL wegen des Entgelterfordernisses[264] nur sein, wenn der Betrieb einen wirtschaftlichen Bezug aufweise. Dies sei aber schon dann der Fall, wenn der Betrieb Werbezwecken dient.[265] Ein Anpreisen des WLANs selbst sei ebenfalls nicht erforderlich, ausreichend sei, dass rein tatsächlich die Zugangsmöglichkeit besteht.[266] Weiterhin sei auch das Accessproviderprivileg keinen Anforderungen außer den in Art. 12 ECommerceRL ausdrücklich Genannten unterworfen[267]; insbesondere könnten Tatbestandsvoraussetzungen anderer Providerprivilegien wie dem Hostproviderprivileg aus Art. 14 ECommerceRL nicht in den Tatbestand des Art. 12 ECommer-

[258] LG München I, EuGH-Vorlage vom 18. September 2014, Az. 7 O 14719/12 – juris.

[259] Also der Name, der sich Personen, die mit ihrem Gerät nach WLAN-Anschlüssen suchen, präsentiert.

[260] LG München I, EuGH-Vorlage vom 18. September 2014, Az. 7 O 14719/12, Rz. 52f. – juris.

[261] Bei einem offenen Betrieb lässt sich eine Begrenzung der Nutzer auf nur solche, die dafür gezahlt haben, technisch ohnehin nicht bewerkstelligen.

[262] LG München I, EuGH-Vorlage vom 18. September 2014, Az. 7 O 14719/12, Rz. 75ff. – juris.

[263] EuGH, Urteil vom 15. September 2016, Rs. C-484/14 – ECLI:EU:C:2016:689 - „McFadden“.

[264] Aus der Verweisung in Art. 2 lit.a) ECommerceRL auf Art. 1 Nr.2 RL (EG) 98/34.

[265] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 42f. – ECLI:EU:C:2016:689 - „McFadden“.

[266] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 51ff. – ECLI:EU:C:2016:689 - „McFadden“.

[267] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 71 – ECLI:EU:C:2016:689 - „McFadden“.

ceRL hineingelesen werden.[268] Hinsichtlich der Reichweite der Privilegierung verbiete Art. 12 Abs.1 ECommerceRL, dass gegen einen Accessprovider Schadensersatz geltend gemacht werden könne sowie damit verbundene Abmahn- und/oder Gerichtskosten.[269] Wegen Art. 12 Abs.3 ECommerceRL sei es den Mitgliedstaaten aber nicht verboten, dass gegen einen WLAN-Anbieter die Unterlassung einer Rechtsverletzung geltend gemacht wird sowie die damit verbundenen Abmahn- und/oder Gerichtskosten.[270]

Der EuGH wich von den Schlussanträgen nur in deren letztem Punkt ab: diesem zu Folge sollten WLAN-Anbieter keine der drei angedachten technischen Maßnahmen – Filterung/Auswertung der über den Anschluss laufenden technischen Kommunikation, Stilllegung des Anschlusses, Sicherung des Anschlusses mittels eines Passworts (also Umstellung vom offenen Betrieb auf den geschlossenen Betrieb) – zugemutet werden dürfen.[271] Dem folgte der EuGH nur im Hinblick auf die ersten beiden Maßnahmen. Dem Erlass einer Anordnung einer Passwortsperre (wobei das Passwort nur an Personen herausgegeben werden dürfe, die dem Betreiber ihre Identität offenbaren) stünden Art. 12 Abs.1 und Abs.3 ECommerceRL nicht entgegen.[272]

In Folge bestand Verwirrung darüber[273], ob Mitgliedstaaten nun Unterlassungsordnungen gegen WLAN-Betreiber ermöglichen müssen oder lediglich ermöglichen dürfen. Gleiches gilt für die Passwortsperre.[274] Zudem war nicht eindeutig, wo diese dogmatisch im deutschen Rechtssystem unterzubringen sei. Das LG München I begnügte sich im Endurteil in der Sache „McFadden“ mit der Feststellung, dass jedenfalls aus der BGH-Entscheidung „Sommer unseres Lebens“ die Pflicht zur Passwortsicherung folge[275] und der Anschluss-

[268] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 65 – ECLI:EU:C:2016:689 - „McFadden“.

[269] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 74f. – ECLI:EU:C:2016:689 - „McFadden“.

[270] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 77ff. – ECLI:EU:C:2016:689 - „McFadden“.

[271] Schlussanträge vom 16. März 2016, Rs. C-484/14, Rz. 127ff. – ECLI:EU:C:2016:170 - „McFadden“.

[272] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 101 – ECLI:EU:C:2016:689 - „McFadden“.

[273] Siehe hierzu Kapitel § 2 VIII. und X.

[274] Dies hat der BGH mittlerweile geklärt, siehe Kapitel § 2 XI. 6.

[275] Mithin die Frage, ob diese europarechtlich geboten oder nur erlaubt ist, dahinstehen könne.

inhaber im konkreten Fall wegen des offenen WLAN-Betriebs also als Störer hafte.[276]

Offen blieb darüber hinaus, ob ein WLAN-Betreiber auch dann Diensteanbieter im Sinne der ECommerceRL ist, wenn der WLAN-Betrieb keinen wirtschaftlichen Bezug aufweist (also im Heimbereich oder Öffnung des Anschluss aus altruistischen Motiven, zum Beispiel beim Freifunk). Laut den Schlussanträgen war diese Frage vom Vorlagenverfahren ausdrücklich ausgeklammert.[277] Dabei wäre darüber hinaus auch zu fragen, ob – wenn diese nicht unter den Anwendungsbereich der ECommerceRL fallen – diesen auf Grund einer nationalstaatlichen Regelung dieselben oder größere Privilegien eingeräumt werden können als Diensteanbietern im Sinne der ECommerceRL.[278]

In der Berufung gegen das Urteil des LG München I kritisierte der Kläger, dass der EuGH die Passwortsperre nur als zulässige Sperrmaßnahme angesehen habe, weil die dem EuGH zur Prüfung vorgelegten Alternativen nicht die Bandbreite des technisch möglichen abgeschöpft hätten.[279] Das Berufungsgericht entschied jedoch, dass es hierauf im konkreten Fall nicht ankäme, weil der Beklagte jedenfalls auch keine andere Sperrmaßnahme ergriffen hätte, also die Passwortsperre zumindest vorliegend gerechtfertigt sei.[280] Die Revision hatte keinen Erfolg.[281]

X. Drittes Gesetz zur Änderung des Telemediengesetzes

Unklar ist, wieso genau der Gesetzgeber sich veranlasst sah, das 2. TMGÄndG nachzubessern. Ausweislich des Gesetzesentwurfes für ein Drittes Gesetz zur Änderung des Telemediengesetzes[282] nahm er an, dass das nach Inkrafttreten des 2. TMGÄndG ergangene Urteil des EuGH in der Rechtssache „McFadden“ für Rechtsunsicherheit gesorgt hätte; insbe-

[276] LG München I, Urteil vom 20. April 2017, Az. 7 O 14719/12, Rz. 55ff. – juris.
[277] Schlussanträge vom 16. März 2016, Rs. C-484/14, Rz. 50 – ECLI:EU:C:2016:170 - „McFadden“.
[278] Siehe hierzu Kapitel § 2 VIII. und X.
[279] OLG München, Urteil vom 15. März 2018, Az. 6 U 1741/17, Rz. 48 – juris.
[280] OLG München, Urteil vom 15. März 2018, Az. 6 U 1741/17, Rz. 82f. – juris.
[281] BGH, Urteil vom 7. März 2019, Az. I ZR 53/18 – GRUR 2019, 947 - „Bring mich nach Hause“.
[282] BT-Drs. 18/12202.

sondere sei WLAN-Betreibern nicht klar, ob sie ihr WLAN vom offenen in den geschlossenen oder den Hotspot-Betrieb wechseln müssten.[283] In der 1. Beratung wurde hierzu weiter ausgeführt, dass gegen WLAN-Betreiber möglicherweise eine entsprechende gerichtliche Anordnung ergehen könnte.[284] Gemeint war wohl § 7 Abs.2 Satz 2 TMG a.F. bzw. § 7 Abs.3 TMG n.F.[285]

Ein weiterer Umstand, der den Gesetzgeber zur Reform veranlasst haben könnte, ist die angesichts Art. 3 EnforcementRL und Art. 8 InfoSocRL im Raum stehende Europarechtswidrigkeit des TMG in der Fassung des 2. TMGÄndG; schließlich sollte nach Vorstellung des Gesetzgebers ein Anschlussinhaber wegen § 8 TMG a.F. gar nicht mehr in Anspruch genommen werden können.[286]

Folglich wurde zwar vorgeschlagen, ausdrücklich in den Gesetzeswortlaut aufzunehmen, dass Access-Provider, die nach § 8 Abs.1 Satz 1 TMG nicht verantwortlich sind, nach § 8 Abs.1 Satz 2 TMG n.F. weder auf Schadensersatz *noch* auf Unterlassung haften, gegen WLAN-Anbieter nach § 8 Abs.3 TMG jedoch als Ausgleich bei Verletzung des geistigen Eigentums ein Sperranspruch nach § 7 Abs.4 Satz 1 TMG n.F. besteht. Voraussetzung hierfür ist, dass keine andere Möglichkeit besteht, der Verletzung des Rechts abzuhelfen.[287] Der Inhalt des Sperranspruches wurde nicht abschließend definiert, nach § 7 Abs.4 Satz 2 TMG n.F. muss er lediglich zumutbar und verhältnismäßig sein; jedoch schlägt die Gesetzesbegründung Port-Sperren und Datenmengenbegrenzungen sowie Webseitensperren, also wohl IP-, DNS- und

[283] BT-Drs. 18/12202, S. 1.

[284] Plenarprotokoll 18/237, S. 24283.

[285] Diese Norm verweist jedoch lediglich auf die allgemeinen Gesetze, mithin die Störerhaftung nach § 1004 BGB analog, siehe *Paal/Hennemann* in: Gersdorf/Paal, BeckOK InfoMedienR, 31. Ed. 2021, § 7 TMG, Rz. 54. Es sei hier nur nebenbei bemerkt, dass auf Grundlage der Störerhaftung die Verschlüsselung eines WLAN oder die Registrierung seiner Nutzer nicht verlangt werden kann, da es sich hierbei um Handlungspflichten und nicht um Beseitigungs- oder Unterlassungspflichten handelt.

[286] Was selbst bei Anwendung des § 8 TMG a.F. auf den Unterlassungsanspruch gar nicht der Fall gewesen wäre, da immer noch – insoweit vom Gesetzgeber wohl übersehen – eine täterschaftliche Haftung durch Nichterfüllung der sekundären Darlegungslast sowie die Haftung auf Grund kollusiven Handelns nach § 8 Abs.1 Satz 2 TMG a.F. möglich gewesen wären.

[287] Vorgeschlagen wird, dass der Rechteinhaber zunächst etwa gegen den „eigentlichen Verletzer“ oder den „Hostanbieter“ vorgehen müsse, siehe BT-Drs. 18/12202, S. 12.

URL-Sperren vor[288], mithin das bisher gesamte derzeit verfügbare Spektrum an Präventionsmaßnahmen.[289] Hingegen soll der WLAN-Betreiber nach § 8 Abs.4 Satz 1 TMG n.F. nicht verpflichtet werden können, das WLAN vom offenen in den geschlossenen oder Hotspot-Betrieb umzustellen oder das WLAN abzuschalten. Freiwillig soll ihm dies alles aber weiterhin möglich sein, § 8 Abs.4 Satz 2 TMG n.F. Wird der Anschlussinhaber auf Grundlage von § 7 Abs.4 Satz 1 TMG n.F. in Anspruch genommen, kann keine Erstattung der Kosten für dessen vor-und außergerichtliche Geltendmachung verlangt werden – gemeint ist der Anspruch aus § 97a Abs.3 UrhG. Die Regelung des § 91 ZPO über die Prozesskosten bleibt jedoch unberührt.[290]

Der Bundesrat sah in seiner Stellungnahme den Sperranspruch kritisch.[291] Auch die vor dem federführenden Ausschuss für Wirtschaft und Energie angehörten Sachverständigen zeigten sich von dem Entwurf – wenn überhaupt – nur in Teilen überzeugt.[292] Die große Koalition konnte sich zunächst nicht über den Entwurf einigen, sodass seine Umsetzung mit dem Ablauf der 18. Legislaturperiode zu scheitern drohte. Überraschend gelang eine Einigung jedoch gerade noch vor der Sommerpause[293], sodass das 3. TMGÄndG[294] am 30. Juni 2017 verabschiedet wurde und schließlich nach Billigung durch den Bundesrat am 13. Oktober 2017 in Kraft trat.

XI. Weitere Rechtsprechung des BGH

1. „Afterlife“ und das Vorlageverfahren „Bastei Lübbe“

Die Entscheidung „Afterlife“[295] betrifft die sekundäre Darlegungslast und die tatsächliche Vermutung.

Zunächst präzisiert und bekräftigt der BGH seine Dogmatik zu diesem Komplex: Auf die Behauptung hin, der Anschlussinhaber sei Täter der Urheberrechtsverletzung, muss dieser – da der Verletzte keine Einsicht in die Interna der Anschlussnutzung hat – zu der Nutzungssituation des Anschlusses vor-

[288] BT-Drs. 18/12202, S. 12.
[289] Vgl. Kapitel § 1 V. 1. b).
[290] BT-Drs. 18/12202, S. 13.
[291] BT-Drs. 18/12496, S. 2.
[292] Siehe Ausschuss für Wirtschaft und Energie, Protokoll-Nr. 18/118.
[293] MMR-Aktuell 2017, 392815.
[294] BGBl. 2017 I, S. 3530.
[295] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15 – GRUR 2017, 386 - „Afterlife“.

tragen. Nicht aber gelte schon auf Grund der Behauptung seiner Täterschaft eine generelle Vermutung dahingehend, dass diese Behauptung auch richtig sei. Dies wäre nur dann zutreffend, wenn es einen Anscheinsbeweis für die Täterschaft des Anschlussinhabers gäbe. Für die Annahme eines Anscheinsbeweises bedürfe es aber einen Erfahrungssatz dahingehend, dass der Inhaber eines Internetanschlusses in aller Regel auch der Täter einer Urheberrechtsverletzung ist, die über diesen Anschluss begangen wird. Da ein solcher Erfahrungssatz offensichtlich nicht existiere, gebe es auch keine generelle Vermutung der Täterschaft des Anschlussinhabers. Ihn treffe also zunächst nur eine sekundäre Darlegungslast; die Vermutung seiner Täterschaft folge erst, wenn er dieser nicht genüge.[296]

Erstmals berücksichtigt der BGH auch die mittelbare Drittwirkung der Grundrechte bei der Bestimmung der Reichweite der sekundären Darlegungslast[297]; außerdem geht er von der Notwendigkeit einer richtlinienkonformen Auslegung derselben aus und stellt in die Abwägung daher auch Art. 8 Abs.1 InfoSocRL und Art. 3 Abs.2 EnforcementRL ein, denen zu Folge Rechteinhabern wirksame, verhältnismäßige und abschreckende Rechtsbehelfe zur Verfügung stehen müssen.[298] Zudem rückt der BGH von der noch in „BearShare“ vertretenen Heranziehung transportrechtlicher Grundsätze für die Bestimmung der sekundären Darlegungslast ab, da die Handlungspflichten von Kaufleuten nicht einfach auf Privatleute übertragen werden könnten.[299]

Im Ergebnis sei daher in familiären Kontexten ausreichend, wenn der Anschlussinhaber allgemein dazu vortrage, welche Familienmitglieder seinen Anschluss mitbenutzen. Vortrag zur Nutzungssituation im Verletzungszeitpunkt und zu den Nutzungsgewohnheiten der Mitnutzer sei nicht erforder-

---

296 BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 17ff. – GRUR 2017, 386 - „Afterlife“.

297 Bei der Bestimmung der Prüfungspflichten im Rahmen der Störerhaftung bereits seit „BearShare“.

298 BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 22f. – GRUR 2017, 386 - „Afterlife“. Zur mittelbaren Drittwirkung der EU-Grundrechte siehe BVerfG, Beschluss vom 6. November 2019, Az. 1 BvR 276/17, Rz. 96f., 107 – bverfg.de - „Recht auf Vergessen II“, mit Nachweisen der Rechtsprechung des EuGH.

299 BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 26 – GRUR 2017, 386 - „Afterlife“.

lich; nur den eigenen PC müsse er auf *filesharing*-Software untersuchen.[300] Hinsichtlich der ersten beiden Punkte entscheidet der BGH damit komplett gegenteilig zu seiner früheren Rechtsprechung in „Tauschbörse VIII / Every time we touch“.[301]

Allerdings ist auch nach „Afterlife“ nach wie vor entscheidend, was die als Mitnutzer benannten Personen vor Gericht als Zeugen aussagen. In „Tauschbörse VIII / Every time we touch“ war der Anschlussinhaber verurteilt worden, weil nach den Aussagen der Mitnutzer zur Überzeugung des Tatrichters stand, dass diese nicht als Täter in Betracht kommen. In „Afterlife“ hatte die einzige Mitnutzerin – die Ehefrau des Beklagten – zwar ausgesagt, dass sie nicht Tätern sei; dies hatte jedoch das Berufungsgericht als nicht glaubhaft gewürdigt, weil nach dessen Auffassung die Ehefrau zwar angegeben hatte, kein *filesharing* zu betreiben und den streitgegenständlichen Film nicht heruntergeladen zu haben, es aber nicht davon auszugehen sei, dass sie die Tat eingeräumt hätte, falls sie tatsächlich die Täterin gewesen wäre.[302] Der BGH hatte an dieser Auffassung des Berufungsgerichts nichts zu bemängeln. Er bleibt damit zumindest seiner Linie treu, dass der Anschlussinhaber nicht positiv darlegen muss, wer statt seiner der „wahre Täter“ ist. In Folge erachtete der BGH in „Afterlife“ die sekundäre Darlegungslast als erfüllt, da die Ehefrau glaubwürdig den Vortrag des Beklagten zu der Tatsache, dass sie

[300] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 26f. – GRUR 2017, 386 - „Afterlife“. Andere Lesart bei *Kuntz*, JurPC Web-Dok. 162/2018, Abs. 53 und *Köhler*, ZUM 2018, 861, 863, die – entgegen den eindeutigen Ausführungen in Rz. 26 des Urteils – davon ausgehen, dass laut BGH im Rahmen der sekundären Darlegungslast weiterhin Vortrag zur Nutzung des Anschlusses durch Familienangehörige zu einem konkreten Zeitpunkt oder zu deren Nutzungsgewohnheiten- und Fähigkeiten verlangt werden könne.

[301] Der BGH lässt in Randziffer 26 zudem *obiter dictum* offen, ob die Ermittlung der Internetnutzung zum Verletzungszeitpunkt generell von Anschlussinhabern – also jedenfalls in nicht-familiären Kontexten – verlangt werden könne. Er deutet damit eventuell grundsätzlich eine Abkehr von seiner bisherigen Rechtsprechung zur Reichweite der sekundären Darlegungslast an. Zum Vergleich: in „BearShare“ hatte er offen gelassen, ob nicht-familiären Kontexte im Rahmen der Störerhaftung genauso zu privilegieren sind wie familiäre und sich dann in „Tauschbörse IX / Silver Linings Playbook“ dafür entschieden.

[302] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 29, 32 – GRUR 2017, 386 - „Afterlife“.

den Anschluss *allgemein* mitbenutze, bestätigen konnte.[303]

Die Anhörungsrüge (§ 321a ZPO) des Klägers gegen das Urteil war erfolglos.[304] Jedoch war das LG München I der Auffassung, dass der BGH mit „Afterlife“ die sekundäre Darlegungslast im Hinblick auf Art. 8 Abs.1 und 2 InfoSocRL sowie Art. 3 Abs.1 und 2 EnforcementRL, denen zu Folge Rechteinhabern wirksame, verhältnismäßige und abschreckende Rechtsbehelfe zur Verfügung stehen müssen, möglicherweise zu eng fasse.[305] Es hatte daher dem EuGH die Frage vorgelegt, ob dieses Verständnis der sekundären Darlegungslast, das im Ergebnis bei Erfüllung derselben den Schadensersatzanspruch der Rechteinhaber gegen den Anschlussinhaber – und faktisch auch insgesamt, da er den wahren Täter nicht ermitteln können wird – mit den genannten Normen vereinbar ist.[306] In dem Vorlageverfahren, das als „Bastei Lübbe“ bezeichnet wird, befand der EuGH die „Afterlife“-Rechtsprechung des BGH als mit dem Europarecht unvereinbar.[307] Er stützt diese Entscheidung primär auf eine Grundrechtsabwägung sowie Art. 6 Abs.1 EnforcementRL.[308]

2. „WLAN-Schlüssel“

Die Entscheidung „WLAN-Schlüssel“[309] knüpft an „Sommer unseres Lebens“ an. Auch der ersterer Entscheidung zu Grunde liegende Sachverhalt ist untypisch, da dort unstreitig war, dass ein unbekannter Dritter sich unberech-

303 BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 29, 33ff. – GRUR 2017, 386 - „Afterlife“.

304 BGH, Beschluss vom 18. Mai 2017, Az. I ZR 154/15 – ZUM-RD 2018, 3.

305 Es lässt sich darüber streiten, ob in dem Fall, über den das LG München I zu entscheiden hatte, eine Vorlage überhaupt nötig war. Denn bereits nach dem eigenen Vortrag des Anschlussinhabers dort schieden seine Mitnutzer als mögliche Täter aus, siehe LG München I, Beschluss vom 17. März 2017, Az. 21 S 24454/14, Rz. 35 – juris. Folglich hätte die tatsächliche Vermutung seiner Täterschaft ohne weiteres Anwendung gefunden. Für die Vorlage ist dies jedoch letztlich irrelevant, denn es ist nicht Aufgabe des EuGH zu prüfen, ob das nationale Recht eine Vorlage tatsächlich erforderlich macht, siehe EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 24 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

306 LG München I, Beschluss vom 17. März 2017, Az. 21 S 24454/14 – juris.

307 EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

308 EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 39ff. – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

309 BGH, Urteil ist 24. November 2016, Az. I ZR 220/15 – GRUR 2017, 617 - „WLAN-Schlüssel“.

tigten Zugriff auf das WLAN des Beklagten verschafft und die Rechtsverletzung begangen haben muss.[310] Normalerweise wird eine solche Behauptung bestritten, kann vom Anschlussinhaber nicht bewiesen werden und ist – seit „Tauschbörse III“ unzweifelhaft – nicht zur Erfüllung der sekundären Darlegungslast geeignet.

In „Sommer unseres Lebens“ hatte der BGH (ohne tatsächliche Feststellungen hierzu durch die Vorinstanzen) geurteilt, dass – zum dortigen Tatzeitpunkt im September 2006 – die Sicherung eines Routers mit dem damaligen WPA-Standard nicht ausreichend sei, wenn nur das werkseitig voreingestellte, zufällig generierte 16-stellige Passwort verwendet werde. Eine solche Sicherung sei „nicht marktüblich“, stattdessen müsse ein persönliches, ausreichend langes und sicheres Passwort gewählt werden, um der Prüfpflicht im Rahmen der Störerhaftung zu genügen; eine Sicherung mit dem damals noch neuen WPA2-Standard sei hingegen nicht erforderlich.[311] Da bei WPA primär nur *brute force*-Attacken im Raum standen, mit denen das Passwort erraten wird[312], hätte der BGH eigentlich erklären müssen, warum die werkseitig erzeugten Passwörter gegenüber persönlich gewählten Passwörtern weniger Schutz gegen solche Attacken bieten, was er aber nicht tat. Stattdessen befand er in „WLAN-Schlüssel“ nunmehr, dass eine Sicherung mit dem WPA2-Standard (zum Tatzeitpunkt im Dezember 2012) ausreichend sei, auch dann, wenn das werkseitig vergebene 16-stellige Passwort verwendet werde.[313] Die Kehrtwende gegenüber „Sommer unseres Lebens“ erklärte der BGH nicht. Er zitiert lediglich Instanzrechtsprechung und Literatur, nach der das werkseitig voreingestellte Passwort nicht weniger sicher sei als ein persönlich eingestelltes Passwort. Wahrscheinlich war er in „Sommer unseres Lebens“ davon ausgegangen, dass alle Router des dort streitgegenständlichen Typs mit demselben Passwort versehen waren.[314] Dies dürfte wohl erklären, warum der BGH in „WLAN-Schlüssel“ umfangreich ausführt, dass der Anschlussinhaber zwar sekundär zu dem von ihm verwendeten Routertyp und

[310] BGH, Urteil ist 24. November 2016, Az. I ZR 220/15, Rz. 2 – GRUR 2017, 617 - „WLAN-Schlüssel“.

[311] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 33f. – GRUR 2010, 633 - „Sommer unseres Lebens“.

[312] https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access - Zugriff am 31.03.2021.

[313] BGH, Urteil ist 24. November 2016, Az. I ZR 220/15, Rz. 12 – GRUR 2017, 617 - „WLAN-Schlüssel“.

[314] So *Mantz*, MMR 2010, 568, 569.

Passwort vortragen müsse, der Rechteinhaber aber darlegungs-und beweisbelastet dafür sei, dass alle Router dieses Typs mit demselben Passwort versehen sind.[315]

Zur Anwendbarkeit des TMG äußerte sich der BGH nicht. Zwar fand die streitgegenständliche Urheberrechtsverletzung noch vor Inkrafttreten des 2. TMGÄndG in Kraft, allerdings war auch nach alter Rechtslage die Anwendbarkeit des TMG diskutiert worden[316], sodass eine Auseinandersetzung hiermit nahegelegen hätte.

Das Urteil schließt mit der Feststellung, dass die Prüfungspflichten anders zu bewerten sein könnten, wenn nachträglich neue Sicherheitslücken bekannt werden.[317] Dies ist in Bezug auf WPA2 mittlerweile eingetreten.[318] Jedoch findet die Störerhaftung seit Inkrafttreten des Dritten Gesetzes zur Änderung des Telemediengesetzes auf Anschlussinhaber ohnehin keine Anwendung mehr.[319]

3. „Loud“

In den Fällen, über die der BGH bisher zu entscheiden gehabt hatte, war dem Anschlussinhaber (jedenfalls nach dessen Vortrag) der eigentliche Täter der Urheberrechtsverletzung entweder unbekannt oder er hatte die Person, die er für den Täter hielt, dem klagenden Rechteinhaber genannt.[320] Im Sachverhalt der Entscheidung „Loud“[321] hatte den beklagten Eltern eines ihrer drei volljährigen Kinder seine Täterschaft gestanden. Dies trugen die Eltern auch im Prozess vor. Sie waren aber nicht bereit mitzuteilen, welches ihrer Kinder geständig gewesen war.[322] In „Tauschbörse III“ hatte der BGH bereits festgelegt, dass der Anschlussinhaber alle Umstände mitteilen müsse,

[315] BGH, Urteil ist 24. November 2016, Az. I ZR 220/15, Rz. 12 – GRUR 2017, 617 - „WLAN-Schlüssel“.

[316] Siehe Kapitel § 2 VIII.

[317] BGH, Urteil ist 24. November 2016, Az. I ZR 220/15, Rz. 22 – GRUR 2017, 617 - „WLAN-Schlüssel“.

[318] *Schirrmacher*, Details zur KRACK-Attacke: WPA2 ist angeschlagen, aber nicht gänzlich geknackt.

[319] Siehe Kapitel § 2 X.

[320] Was für sich allein aber noch nicht zur Erfüllung der sekundären Darlegungslast genügt, wenn die Täterschaft des genannten Dritten bestritten wird, siehe Kapitel § 2 VII. 2.

[321] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16 – GRUR 2017, 1233 - „Loud“.

[322] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 5 – GRUR 2017, 1233 - „Loud“.

die er über eine Rechtsverletzung in Erfahrung gebracht hatte. „Afterlife“ schränkte nur die Nachforschungspflicht (im familiären Kontext) ein, eine Einschränkung der Mitteilungspflicht ist dieser Entscheidung aber nicht zu entnehmen. Folglich stellte sich dem BGH lediglich noch die Frage, ob er von diesem Grundsatz auf Basis einer Grundrechtsabwägung – die er im Rahmen der sekundären Darlegungslast erstmals in der Entscheidung „Afterlife“ vorgenommen hatte – abrücken würde.

Dies trat jedoch nicht ein. Der BGH sah auf Grund der Nichtmitteilung der Identität des Kindes, das sich seien Eltern gegenüber als Täter bekannt hatte, die sekundäre Darlegungslast der anschlussinhabenden Eltern als nicht erfüllt an, weshalb diese als Täter hafteten.

In der Grundrechtsabwägung sei laut BGH in dieser Konstellation den Rechteinhabern der Vorzug zu geben. Erstens könnten sich die Eltern aussuchen, ob sie Auskunft erteilen oder selbst haften. Im letzteren Fall wären sie in keiner anderen rechtlichen Position als jede andere prozessual ungenügend vortragende Partei auch. Anders als Zeugen, die nach §§ 383f. ZPO ein Zeugnisverweigerungsrecht haben können, sei die Wahrheitspflicht nach § 138 Abs.1 ZPO nur insoweit begrenzt, als ein Angehöriger einer Straftat oder Unehrenhaftigkeit bezichtigt werden müsste.[323] Der Familienfrieden sei also nicht über Gebühr beeinträchtigt.[324] Zweitens bliebe bei einer Entscheidung zu Gunsten der Eltern die Identität des Verletzers ungeklärt und damit das europarechtliche Gebot der Möglichkeit der effektiven Rechtsverfolgung nicht ausreichend berücksichtigt.[325]

Das BVerfG hat die gegen die Entscheidung „Loud“ eingelegte Verfassungsbeschwerde nicht zur Entscheidung angenommen. Laut dessen Begründung habe der BGH Art. 6 GG und Art. 14 GG in nicht zu beanstandender Weise gegeneinander abgewogen.[326]

---

[323] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 26f. – GRUR 2017, 1233 - „Loud“. Der BGH übersieht dabei allerdings, dass auch nicht-kommerziell betriebenes *filesharing* materiell eine Straftat ist, siehe Kapitel § 2 II.

[324] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 26f. – GRUR 2017, 1233 - „Loud“.

[325] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 28 – GRUR 2017, 1233 - „Loud“.

[326] BVerfG, Nichtannahmebeschluss vom 18. Februar 2019, Az. 1 BvR 2556/17, Rz. 15ff. – bverfg.de.

4. „Ego-Shooter-Spiel“

In den Fällen, über die der BGH bisher zu entscheiden hatte, war im Rahmen der sekundären Darlegungslast immer relevant gewesen, was das Ergebnis der Zeugenvernehmung der Mitnutzer ist. Nur wenn auf Grund dieser der Vortrag des Anschlussinhabers plausibel erscheint, war seine Haftung ausgeschlossen. Jedoch kann im Zivilprozess nach § 383 ZPO aus persönlichen und nach § 384 ZPO aus sachlichen Gründen das Zeugnis verweigert werden. Da ein familiärer Kontext in *filesharing*-Prozessen regelmäßig gegeben ist, machten die als Mitnutzer benannten und als Zeugen geladenen Familienmitglieder von ihrem Zeugnisverweigerungsrecht regen Gebrauch. In der Instanzrechtsprechung war die Ausübung des Zeugnisverweigerungsrecht teilweise zu Lasten des Anschlussinhabers bewertet worden; schließlich kann dann sein sekundärer Vortrag nicht bestätigt werden.[327] Als der BGH in der Sache „Ego-Shooter-Spiel“[328] mit dieser Frage befasst wurde[329], entschied er, dass eine Zeugnisverweigerung grundsätzlich nicht zu Lasten einer Partei gewertet werden könne, da die Parteien keinen rechtlichen Einfluss auf die Ausübung desselben haben. Daher sei nach erfolgter Verweigerung nach Beweislast zu entscheiden. Ausnahmsweise könne eine Verweigerung nur zu Lasten einer Partei gewertet werden, wenn die Verweigerung aus sachlichen (§ 384 ZPO) statt persönlichen (§ 383 ZPO) Gründen erfolge und zudem besondere, konkret festgestellte Indizien eine solche Wertung rechtfertigen.[330] Zugleich stellte er (gegenüber der früheren Rechtsprechung, die in dieser Frage stets im Vagen verblieben war) klar, dass die Würdigung der Zeugenaussagen dogmatisch nicht im Rahmen der sekundären Darlegungslast stattzufinden hat, sondern mit der Erfüllung der Pflichten aus der sekundären Darlegungslast dieser auch genügt ist, folglich die Würdigung der Zeugenaussagen zur Beweiswürdigung gehört.[331]

---

[327] Beispielsweise AG Leipzig, Urteil vom 9. Februar 2017, Az. 100 C 5611/16 – waldorf-frommer.de.

[328] Dies ist kein offizieller Name der Entscheidung, er wird aber in der Literatur verwendet, siehe *Reuther*, MMR 2018, 433, 434.

[329] BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16 – MMR 2018, 311 - „Ego-Shooter-Spiel“.

[330] BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16, Rz. 28 – MMR 2018, 311 - „Ego-Shooter-Spiel“.

[331] BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16, Rz. 22ff. – MMR 2018, 311 - „Ego-Shooter-Spiel“. Siehe hierzu genauer Kapitel § 4 VII. 4. a).

In *filesharing*-Fällen im familiären Kontext kommt als Folge des Urteils eine Zeugnisverweigerung immer dem Anschlussinhaber zu Gute. Denn die Zeugenvernehmung kann ihm schädlich sein, wenn diese entweder seinen sekundärer Vortrag nicht bestätigt oder die Zeugen ihre Täterschaft[332] für den Tatrichter glaubwürdig abstreiten – und damit der Anschlussinhaber als einzig möglicher Täter verbleibt.

Ein Nebenaspekt der Entscheidung ist zudem, dass Erinnerungslücken des Anschlussinhabers diesem nicht zum Schaden gereichen, wenn zwischen Rechtsverletzung und Erhalt der Abmahnung ein gewisser Zeitraum (in der Streitsache: fast zwei Monate) verstrichen ist.[333] Jedoch bleibt unklar, ob es hinsichtlich Erinnerungslücken nicht eigentlich auf den Zeitpunkt der Zustellung der Klage ankommt.[334]

5. „Konferenz der Tiere“

Bereits in „Tauschbörse I“ hatte der BGH mit wenigen Worten entschieden, dass es für die Frage, ob eine Datei bzw. das darin verkörperte Leistungsschutzrecht öffentlich zugänglich gemacht wurde, jedenfalls im Rahmen der Leistungsschutzrechte irrelevant ist, wenn gegebenenfalls nur einzelne Dateifragemente übertragen wurden, da ein Leistungsschutzrecht *jeden* einzelnen Bestandteil einer Datei erfasse, die dieses Recht verkörpert.[335]

Dabei hatten zahlreiche Instanzgerichtsentscheidungen – vor allem des AG und LG Frankenthal – darauf hingewiesen, dass in Bezug auf Dateifragmente eine urheberrechtlich relevante Verwertungshandlung schon voraus setzt, dass diese überhaupt der Wahrnehmung zugänglich sind.[336] Probleme erwachsen hieraus vor allem im Zusammenhang mit dem BitTorrent-System,

[332] Zur Rechtmäßigkeit einer Frage nach der Täterschaft siehe Kapitel § 5 V. 4.

[333] BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16, Rz.18 – MMR 2018, 311 - „Ego-Shooter-Spiel“.

[334] Siehe Kapitel § 5 V. 3.

[335] Siehe Kapitel § 2 VI. 1.

[336] Mit dieser Stoßrichtung erstmals LG Frankenthal, Beschluss vom 6. März 2009, Az. 6 O 60/09, Rz. 26 – juris. Ausdrücklich LG Frankenthal, Urteil vom 30. September 2014, Az. 6 O 518/13, Rz. 26 – juris; LG Frankenthal, Urteil vom 11. August 2015, Az. 6 O 55/15, Rz. 14 – juris; LG Frankenthal, Beschluss vom 15. Juni 2016, Az. 6 O 134/16, Rz. 5 – juris; LG Frankenthal, Urteil vom 22. Juli 2016, Az. 6 O 22/15, Rz. 27 – juris; AG Frankenthal, Urteil vom 8. November 2017, Az. 3c C 169/17, Rz. 13 – juris.

da ein Endnutzer niemals die vollständige Datei an einen anderen Endnutzer überträgt, sondern immer nur Teile davon an verschiedene andere Nutzer.[337] In Bezug auf ISO-Container und Archivdateien überträgt der einzelne Nutzer für sich betrachtet nur Datenmüll, da deren Inhalt ausschließlich dann wahrnehmbar gemacht werden kann, wenn sie vollständig vorhanden sind.[338] Setzt man für eine urheberrechtlich relevante Verwertungshandlung die Wahrnehmbarkeit voraus, kann in Bezug auf solche Dateien ein einzelner BitTorrent-Nutzer isoliert betrachtet nie § 19a UrhG (zumindest in Bezug auf die vollständige Datei) verwirklichen.[339] Bei Musik-und Videodateien können zwar schon einzelne Fragmente ausreichen, um zumindest Teile des Inhalts abspielbar zu machen[340]; ob ein einzelner Nutzer aber hierfür ausreichende bzw. passende Fragmente übertragen hat, lässt sich von außen nicht feststellen.[341] Daher gilt auch in Bezug auf diese Dateien im Ergebnis dasselbe wie zu ISO-Containern und Archivdateien.

Andere Instanzgerichte entschieden jedoch, dass auch der einzelne Nutzer § 19a UrhG verwirkliche, beispielsweise mit der Begründung, dass schon das Zugänglichmachen nur eines Fragments jedenfalls kausal dazu beitrage, dass die empfangenden Nutzer eine vollständige und wahrnehmbare Datei erlangen[342] oder dass die Wahrnehmbarkeit keine Voraussetzung für § 19a UrhG sei, jedenfalls die Endnutzer aber als Mittäter anzusehen und damit die Übertragung der einzelnen Fragmente den jeweils anderen Nutzern zurechenbar seien, mithin in der Gesamtbetrachtung der einzelne Nutzer keinen Datenmüll übertrage.[343]

Als sich der BGH in dem Urteil „Konferenz der Tiere“[344] zu diesem Pro-

[337] Siehe Kapitel § 1 II. 5. b).

[338] Siehe Kapitel § 1 III.

[339] Siehe hierzu Kapitel § 4 II. 3.

[340] Erst im Anschluss an die Frage der Abspielbarkeit stellt sich die Frage, ob die abspielbaren Fragmente einem Schutzrecht unterfallen.

[341] Vgl. hierzu AG Braunschweig, Urteil vom Urteil 13. Oktober 2015, Az. 117 C 2852/15 – unveröffentlicht.

[342] OLG Köln, Beschluss vom 20. April 2016, I-6 W 37/16, 6 W 37/16, Rz. 20 – juris.

[343] OLG Celle, Urteil vom 26. Januar 2017, Az. 13 U 113/16 – aw3p.de.

[344] BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16 – GRUR 2018, 400 - „Konferenz der Tiere“; Berufung zu LG Frankenthal, Urteil vom 22. Juli 2016, Az. 6 O 22/15 – juris. In strafrechtlicher Perspektive hat das OLG Köln implizit eine Mittäterschaft zwischen den Betreibern einer Indexseite und deren Nutzern angenommen, siehe OLG Köln, Beschluss vom 28. März 2017, Az. III-1 RVs 281/16 – GRUR 2017, 1039.

blemkreis äußern musste, lies er eine Entscheidung über die Frage, ob er – im Anschluss an „Tauschbörse I“ auch weiterhin – kleinste Fragmente einer Datei, die ein Leistungsschutzrecht verkörpert, als selbst vom Leistungsschutzrecht umfasst ansieht, wegen dem zu dieser Frage anhängigen Vorlageverfahren[345] offen, tendierte aber dazu, diese zu bejahen; ein für diese Konstellation hieraus folgender stärkerer Schutz des Leistungsschutzrechts im Vergleich zum Werk sei durch die unterschiedlichen Schutzgegenstände gerechtfertigt.[346] Zur Frage des Erfordernisses der Wahrnehmbarkeit äußerte er sich nicht. Dieses konnte jedoch im Rahmen der von ihm gewählten Lösung auch offen bleiben: die Endnutzer seien, soweit sie technisch an der Zusammensetzung einer vollständigen Datei zusammenwirken, als Mittäter anzusehen.[347] Da in den Medien generell seit vielen Jahren die grundlegende Funktionsweise von *filesharing* kommuniziert werde, hätten Endnutzer jedenfalls den bedingten Vorsatz, mit anderen Endnutzern an der Zusammensetzung einer Datei[348] zusammen zu wirken; dass die Endnutzer keine Kenntnis über die Person der anderen Endnutzer haben, sei unschädlich.[349]

Damit ist im Rahmen der mittäterschaftlichen Lösung des Problems der segmentierten Dateiübertragung auch irrelevant, ob in den einzelnen Dateifragmenten ein Werk oder Leistungsschutzrecht verkörpert ist und ob dieses wahrnehmbar sein muss.

Diese Entscheidung ist wegen ihrer möglichen Konsequenzen für den Schadensersatz von allen neueren Entwicklungen im Bereich des *filesharing* am meisten geeignet, das Abmahnwesen[350] in seiner bisherigen Form unmöglich zu machen.[351]

345 EuGH, Rs. C-476/17 - „Metall auf Metall“.

346 BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 17ff. – GRUR 2018, 400 - „Konferenz der Tiere“.

347 Der BGH verweist bei seiner Begründung nicht auf das Urteil des OLG Celle, das zum selben Ergebnis kommt.

348 Also jedenfalls bei Systemen, die das *swarming* implementieren.

349 BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 24ff. – GRUR 2018, 400 - „Konferenz der Tiere“.

350 Siehe hierzu Kapitel § 3.

351 Siehe hierzu Kapitel § 4 II. 4. b) ff), § 4 IX. 3. und § 5 VII.

6. „Dead Island“

Mit der Entscheidung „Dead Island“[352] beantwortete der BGH zahlreiche Fragen zum TMG, und zwar sowohl für die Rechtslage vor Inkrafttreten des 2. TMGÄndG und nach Inkrafttreten des 3. TMGÄndG. Diese Konstellation kam dadurch zu Stande, dass die streitgegenständliche Verletzungshandlung 2013 stattgefunden hatte[353], der (im Verfahren geltend gemachte und in den Vorinstanzen zugesprochene) Unterlassungsanspruch grundsätzlich aber in die Zukunft wirkt, also auch in der Revisionsinstanz nach geltender Rechtslage zu beurteilen ist[354], der Anspruch auf Ersatz der Abmahngebühren aber nach der Rechtslage zum Zeitpunkt der Verletzungshandlung zu beurteilen ist[355], und dieser Anspruch wiederum auf dem Unterlassungsanspruch gründet.[356]

Hinsichtlich der alten Rechtslage bestätigte der BGH nachträglich die Literatur und die Instanzrechtsprechung[357], die eine Anwendung des § 8 Abs.1 Satz 1 TMG a.F. auf Anschlussinhaber (gleich ob private oder gewerblich handelnde) bejaht hatte[358], verneinte aber auch die zum Teil strittige Frage, ob diese Vorschrift Unterlassungsansprüchen entgegenstand[359]. Weiterhin bestünden Unterlassungsansprüche auf Grundlage der Störerhaftung gegen private Anschlussinhaber, wenn sie ihr WLAN nicht mit einem ausreichenden Passwort versehen.[360] Dies gelte auch für die gewerbliche Anschlussteilung, allerdings erst dann, wenn der Anschlussinhaber bereits einmal für eine (be-

[352] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17 – GRUR 2018, 1044 - „Dead Island“.

[353] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 1 – GRUR 2018, 1044 - „Dead Island“.

[354] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 36ff. – GRUR 2018, 1044 - „Dead Island“.

[355] Insofern bestätigt der BGH seine entsprechende frühere Rechtsprechung, siehe BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 9 – GRUR 2018, 1044 - „Dead Island“.

[356] Ausgespart blieb mithin eine Entscheidung über die Auslegung des § 8 TMG in der Fassung des 2. TMGÄndG, da es hierauf nicht mehr ankam.

[357] Siehe Kapitel § 2 VIII.

[358] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 17f. – GRUR 2018, 1044 - „Dead Island“.

[359] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 19ff. – GRUR 2018, 1044 - „Dead Island“.

[360] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 23 – GRUR 2018, 1044 - „Dead Island“.

liebige) Schutzrechtsverletzung abgemahnt worden war.[361]

Um (seiner Auffassung nach auftretende) Konflikte mit dem Unionsrecht zu vermeiden, erklärte der BGH, dass § 7 Abs.4 TMG analog auf die drahtgebundene Anschlussteilung anzuwenden sei.[362] Weiterhin entschied er, dass § 7 Abs.4 TMG nicht auf bestimmte Sperrmaßnahmen beschränkt, sondern eine Vielzahl von Sperrmaßnahmen – über die im Regierungsentwurf Genannten hinaus – denkbar sei, mithin (weiterhin) auch die Vorgabe, ein offenes WLAN mit einem Passwort zu versehen.[363] Soweit in laufenden Verfahren bereits der Unterlassungsanspruch geltend gemacht oder zugesprochen worden sei, müsste Klägern zudem Gelegenheit gegeben werden, diesen – wo einschlägig – gegen den Anspruch aus § 7 Abs.4 TMG auszutauschen.[364] Folglich entschied er auch nicht abschließend darüber, welche Sperrmaßnahmen im konkreten Verfahren zulässig gewesen wären, sondern verwies insofern an das OLG Düsseldorf zurück. Zuletzt sei der § 7 Abs.4 TMG unionsrechtskonform, mithin eine Vorlage an den EuGH nicht angezeigt.[365]

Da der beklagte Anschlussinhaber unstreitig die Urheberrechtsverletzung nicht begangen hatte[366], konnte der BGH allerdings nicht über das Verhältnis zwischen TMG und sekundärer Darlegungslast entscheiden.

7. „Riptide“

Weist der abgemahnte Anschlussinhaber auf einen Mitnutzer des Anschlusses als Täter hin, akzeptiert der Rechteinhaber diesen Hinweis und bestreitet auch der Mitnutzer seine Täterschaft nicht, so stellt sich die Frage, ob der Mitnutzer für die Rechtsanwaltskosten aufkommen muss, die für die Abmahnung des Anschlussinhabers entstanden sind, da in diesem Fall – in dem der Rechteinhaber die Nichtverantwortlichkeit des Anschlussinhabers für die

[361] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 27f. – GRUR 2018, 1044 - „Dead Island“, was vorliegend der Fall war.

[362] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 46ff. – GRUR 2018, 1044 - „Dead Island“.

[363] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 53ff. – GRUR 2018, 1044 - „Dead Island“.

[364] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 57 – GRUR 2018, 1044 - „Dead Island“.

[365] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 58 – GRUR 2018, 1044 - „Dead Island“.

[366] Vgl. LG Düsseldorf, Urteil vom 13. Januar 2016, Az. 12 O 101/15, Rz. 3ff. – juris.

Rechtsverletzung akzeptiert hat – von Letzterem keine Erstattung der Kosten verlangt werden kann. Einen solchen Anspruch auf Grundlage des Schadensersatzanspruches bejahte der BGH in der Entscheidung „Riptide“[367], mit Verweis auf die senatsübergreifende Rechtsprechung, derzufolge erforderliche und zweckmäßige Rechtsverfolgungskosten als Schaden anzusehen seien; die Abmahnung des Anschlussinhabers als einzigen „Ansprechpartner“ sei gegenüber einer formlosen Anfrage erforderlich und zweckmäßig, da regelmäßig nur die Abmahnung – unter anderem, weil sie das sofortige Anerkenntnis nach § 93 ZPO abschneide – den Anschlussinhaber dazu veranlasse, dem Rechteinhaber zu antworten.[368]

Die Begründung der Entscheidung bewegt sich im Rahmen der lange etablierten Rechtsprechung des BGH zu Rechtsverfolgungskosten als Schaden und dürfte in ihren praktischen Auswirkungen gering sein – denn dass Rechteinhaber den Verweis auf einen Mitnutzer als Täter akzeptieren und/oder dessen Täterschaft unstreitig bleibt, kommt nach Übersicht des Verfassers äußerst selten vor[369]. Die Entscheidung ist daher im Fortgang nicht Gegenstand der dogmatischen Analyse in dieser Arbeit.

8. „Saints Row“ und I ZB 38/20

Äußert sich ein Abgemahnter auf die Abmahnung hin nicht, kann aber in einem hierauf initiierten Prozess seine sekundäre Darlegungslast erfüllen und nachfolgend der Haftung als Täter entgehen, so unterliegt der klagende Rechteinhaber zumindest mit seinem Schadens- und Gebührenersatzbegehren.[370] Der Rechteinhaber wird dann argumentieren, dass der Abgemahnte ihn ins „offene Messer“ hat laufen lassen, da er – wenn Letzterer ihn bereits nach Erhalt der Abmahnung über die Anschlussnutzung aufgeklärt hätte – eine Klage gar nicht erst angestrengt oder diese zumindest gleich auf den Anspruch aus § 7 Abs.4 TMG beschränkt hätte. Daraus folgt die Über-

[367] BGH, Urteil vom 22. März 2018, Az. I ZR 265/16 – GRUR 2018, 914 - „Riptide“.

[368] BGH, Urteil vom 22. März 2018, Az. I ZR 265/16, Rz. 15ff. – GRUR 2018, 914 - „Riptide“.

[369] Siehe Kapitel § 3 V. und VII.

[370] Unter Geltung des 3. TMGÄndG wird zwar immer ein Anspruch nach § 7 Abs.4 TMG in Betracht kommen; da dessen Streitwert (siehe hierzu Kapitel § 4 VIII. 8.) aber die üblichen Schadens- und Gebührenersatzforderungen regelmäßig unterschreiten wird, werden Rechteinhaber im Falle des Unterliegens mit der Schadensersatzforderung den überwiegenden Teil der Gerichts-und Rechtsanwaltskosten tragen müssen.

legung, ob der Rechteinhaber in dieser Situation gegen den Abgemahnten einen materiell-rechtlichen Anspruch auf Ersatz des negativen Schadens hat, der ihm durch die Gerichts-und Anwaltskosten entstanden ist[371] oder einen prozessualen Kostenerstattungsanspruch nach § 269 Abs.3 Satz 3 1. Hs. ZPO.

Das OLG Köln hatte in einer *filesharing*-Entscheidung aus dem Jahr 2011 *obiter dictum* festgehalten, dass Anschlussinhaber verpflichtet wären, auf eine Abmahnung zu antworten.[372] Es berief sich dabei auf eine BGH-Entscheidung aus dem Jahr 1989[373], die eine solche Pflicht für wettbewerbsrechtliche Abmahnungen aufgestellt hatte.[374] Spätere *filesharing*-Entscheidungen anderer Gerichte lehnten jedoch die entsprechende Heranziehung dieses BGH-Urteils ab.[375] Wiederum andere Instanzgerichte bejahten jedoch eine Pflicht zur wahrheitsgemäßen Antwort auf eine Abmahnung und sprachen also für den Fall der Nichterfüllung derselben einen materiell-rechtlichen Anspruch auf Erstattung der Prozesskosten[376] oder einen dahingehenden prozessualen Anspruch[377] zu.

Der BGH lehnte jedoch in der Entscheidung „Saints Row“[378] einen materiellen Kostenerstattungsanspruch unter allen Gesichtspunkten ab.[379] Mit Beschluss vom selben Tage[380] lehnte er zudem einen prozessualen Kostenerstattungsanspruch ab.

---

371 Also der Schaden, der nicht eingetreten wäre, wenn der Abgemahnte die Umstände, die er ihm Rahmen seiner sekundären Darlegungslast vorgetragen hat, dem Rechteinhaber bereits nach Erhalt der Abmahnung mitgeteilt hätte.

372 OLG Köln, Urteil vom 22. Juli 2011, Az. 6 U 208/10 – NRWE.

373 BGH, Urteil vom 19. Oktober 1989, Az. I ZR 63/88 – GRUR 1990, 381.

374 OLG Köln, Urteil vom 22. Juli 2011, Az. 6 U 208/10, Rz. 11 – NRWE.

375 AG Charlottenburg, Urteil vom 22. September 2017, Az. 206 C 236/17, Rz. 22 – juris; LG Leipzig, Beschluss vom 11. April 2017, Az. 5 S 487/16 – unveröffentlicht; AG Hamburg, Beschluss vom 10. Oktober 2016, Az. 25b C 20/16 – aw3p.de; OLG Hamburg, Beschluss vom 27. August 2013, Az. 5 W 88/12, Rz. 6 – BeckRS 2014, 15800.

376 AG Hamburg, Urteil vom 14. Januar 2020, Az. 18b C 82/19 – GRUR-RS 2020, 1066; AG Köln, Urteil vom 25. Juli 2019, Az. 148 C 408/18 – ZUM-RD 2020, 41.

377 AG München, Beschluss vom 3. August 2016, Az. 264 C 2784/16 – BeckRS 2016, 135909.

378 BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19 – juris - „Saints Row“.

379 BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 20ff. – juris - „Saints Row“.

380 BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20 – juris.

XII. Zusammenfassung und Ausblick

1. Zusammenfassung

Die Rechtslage in Bezug auf die Haftung eines Internetanschlussinhabers für urheberrechtsverletzendes *filesharing* stellt sich damit gegenwärtig im Ergebnis *faktisch* wie folgt dar:

- Sobald über einen Internetanschluss in einem *filesharing*-System die Zugriffsmöglichkeit auf eine urheberrechtlich oder durch ein Leistungsschutzrecht geschützte Datei eröffnet wird, stellt dies eine öffentliche Zugänglichmachung nach § 19a UrhG dar. Ob tatsächlich ein Upload der Datei stattfindet ist ebenso irrelevant wie die Frage, ob die vollständige Datei oder nur Fragmente derselben an einen Dritten hochgeladen werden. Der Download stellt eine Vervielfältigung nach § 16 UrhG dar. Urheberrechtliche Schranken greifen sowohl bei § 16 als auch § 19a UrhG nicht. Soweit die Endnutzer bei der Verbreitung einer Datei technisch zusammen wirken, können sie diesbezüglich als Mittäter angesehen werden.

- Ein Auskunftsanspruch gegen ISPs auf Herausgabe von Name und Anschrift des Inhabers des Anschlusses, dem nach Ermittlungen eine *filesharing*-Aktivität zugeordnet wurde, erfordert kein gewerbliches Ausmaß selbiger. Entsprechende Gestattungsanordnungen ergehen in der Praxis allein auf Vorlage des Ermittlungsergebnisses (insbesondere IP-Adresse und bei BitTorrent des einschlägigen Hashwertes der Datei) und der Nennung des betroffenen Werkes. Nicht geklärt ist bisher, welche Probleme sich bei Anwendung des Tatbestandsmerkmals „*offensichtliche Rechtsverletzung*“ in § 101 Abs.2 UrhG und des Verhältnismäßigkeitsprinzips in § 101 Abs.4 UrhG ergeben können.

- Rechteinhaber haben einen Anspruch gegen ISPs, auf Zuruf die Zuordnung einer IP-Adresse zu einem Anschluss solange zu speichern, bis ein darauf bezogenes Auskunftsverfahren abgeschlossen ist. Nicht geklärt ist, ob ein entsprechender Anspruch im Falle des Vorhandenseins eines CG-NAT auch bezüglich der für die in diesem Fall für die Zuordnung erforderlichen Metadaten besteht.

- Der BGH erachtet es – soweit er hiermit befasst wurde – bisher nicht

als rechtsfehlerhaft, wenn der Instanzrichter die in der Praxis eingesetzten Ermittlungsmethoden im Rahmen der Beweiswürdigung als ausreichenden Nachweis der Verletzung bewertet. Offen ist, wie der BGH die erhöhten Anforderungen, die teils in der Instanzrechtsprechung an das Ermittlungsverfahren gestellt werden, bewerten würde oder wird.

- Den Anschlussinhaber trifft eine sekundäre Darlegungslast. Nach gegenwärtigem Stand ist die Rechtsprechung des BGH so zu verstehen, dass in nicht-familiären Kontexten der Anschlussnutzung der Anschlussinhaber darlegen muss, welche Personen zum Verletzungszeitpunkt Zugriff auf den Internetanschluss hatten und wie sich deren Internetnutzungsverhalten gestaltet (Nachforschungsplficht). Offen ist, ob der BGH so zu verstehen ist, dass bei offenem und/oder gewerblichem Betrieb des WLAN etwas anderes gilt. Soweit der Anschlussinhaber der sekundären Darlegungslast zunächst genügen kann, gilt er dennoch als Täter, wenn die benannten Mitnutzer nach Zeugenvernahme nach der Überzeugung des Tatrichters entweder als Täter ausscheiden oder der Vortrag zur Nutzungssituation als unplausibel erscheint. Sofern der Anschlussinhaber behauptet, den Täter zu kennen, der Rechteinhaber jedoch mit Nichtwissen die Täterschaft einer anderen Person als dem Anschlussinhaber bestreitet, und der Anschlussinhaber diese Person daraufhin nicht identifiziert, so hat er – sowohl im familiären als auch (vermutlich) im nicht-familiären Kontext der Anschlussnutzung – allein deswegen schon seine sekundäre Darlegungslast nicht erfüllt (Mitteilungspflicht). Sofern er die dritte Person identifiziert, der Rechteinhaber aber deren Täterschaft bestreitet, exkulpiert sich der Anschlussinhaber nur, wenn deren Täterschaft nach tatrichterlicher Würdigung der Zeugenvernehmung als plausibel erscheint. Im familiären Kontext der Anschlussnutzung muss nach BGH nicht zur Nutzungssituation im Verletzungszeitpunkt vorgetragen werden, sondern nur allgemein zur Nutzungssituation; die Nachforschungspflicht ist dort also begrenzt. Diese Rechtsprechung ist jedoch nach EuGH europarechtswidrig. Es ist daher davon auszugehen, dass der BGH in Zukunft in diesem Punkt familiäre und nicht-familiäre Anschlussnutzung gleichsetzt. Sofern die vom Anschlussinhaber benannten Mitnutzer ihr Zeugnis verweigern, geht dies – jedenfalls im familiären Kontext einer Anschlussnutzung – nicht zu Lasten des Anschlussinhabers, d.h. in die-

sem Fall muss sein Vortrag nicht durch tatrichterliche Würdigung von Zeugenvernehmungen als plausibel erscheinen.

- Hinsichtlich der Reformen des TMG ist bisher nur gesichert, dass eine Störerhaftung des Anschlussinhabers nicht mehr in Betracht kommt. Bezüglich der sonstigen Tatbestandsvoraussetzungen und der Rechtsfolgen (die Sperranordnung) sind auch nach den ersten gerichtlichen Entscheidungen hierzu viele Einzelheiten noch unklar. Ebenfalls unklar ist das Verhältnis der sekundären Darlegungslast zu den neuen Vorschriften im TMG.

- Die instanzgerichtlich übliche Berechnung des lizenzanalogen Schadens hat der BGH weitestgehend gebilligt, insbesondere wurde hinsichtlich der Berechnung des Schadens im Hinblick auf § 19a UrhG den Einwänden der Überkompensation sowie einem Erfordernis, auf die geschätzte Menge der tatsächlichen Zugriffe abzustellen, eine Absage erteilt. Der lizenzanaloge Schaden kann auch im Wege des Restschadensersatzanspruches verlangt werden, der zehn Jahre nach seiner Entstehung verjährt. Welche Konsequenzen die Entscheidung „Konferenz der Tiere“ für den Schadensersatzanspruch genau haben wird, ist noch ungewiss.

2. Ausblick

In der Einleitung dieses Kapitels wurde postuliert, dass sich die Rechtsentwicklung in zwei Phasen einordnen lasse, die sich vor allem aus den jeweiligen gerichtlichen Fallzahlen rechtfertige. In der ersten Phase – also bis 2008 – war es mangels des zivilrechtlichen Auskunftsanspruches schon schwer möglich, überhaupt einen Fall vor Gericht zu bringen und wenn doch, war die Haftung des Anschlussinhabers – wegen der schon damals verbreiteten Nutzung eines Anschlusses durch mehrere Personen – ungewiss. Nach Einführung des Auskunftsanspruches drehte sich das Verhältnis um, da Auskunft nun praktisch in jedem registrierten Verletzungsfall erlangt werden konnte und die Haftung von Anschlussinhabern durch den BGH gegenüber älterer Instanzrechtsprechung erheblich verschärft wurde. Parallel stieg die Nutzung von *filesharing* generell und die Nutzung von BitTorrent im Speziellen immer mehr an, bis Letzteres den „Markt“ dominierte.[381] Zugleich ist jeder Nutzer im BitTorrent-System ganz regelmäßig am Uploadvorgang beteiligt und

[381] Siehe dazu Kapitel § 1 II. 4. f).

damit potentielle Zielscheibe für einen Ermittler.[382] In der zweiten Phase bestanden also sowohl die tatsächlichen als auch rechtlichen Voraussetzungen dafür, dass sich auf dem Sachverhalt des *filesharing* ein Abmahnwesen etablieren konnte.[383] Ob die zweite Phase mit der Entscheidung „Konferenz der Tiere“ beendet ist, wird maßgeblich von deren Anwendung seitens der Gerichte abhängen.[384]

Im Übrigen ist in absehbarer Zukunft jedenfalls keine weitere, einschneidende höchstgerichtliche Rechtsprechung des BGH im Bereich des *filesharing* zu erwarten. Zwar ist es nicht unwahrscheinlich, dass es einige weitere BGH-Entscheidungen geben wird[385]; diese werden aber nur die bisherige Rechtsprechung in den Einzelheiten fortführen, mit einer großen Änderung oder Überraschung ist – nach gegenwärtiger Sachlage – nicht zu rechnen.

Weiterhin steht auch keine für das *filesharing* unmittelbar bedeutsame Gesetzgebung bevor:

Im Koalitionsvertrag von CDU, CSU und SPD für die 19. Legislaturperiode wird lediglich geäußert, dass die Störerhaftung bei WLANs nun abgeschafft sei und somit öffentliche WLANs flächendeckend eingerichtet werden können und sollen.[386] Eine Förderung kommunaler WLANs sieht auch die EU-Initiative „WiFi4EU“ vor.[387] Auf bundesgesetzlicher Ebene sollen Freifunk-Initiativen[388] als gemeinnützig anerkannt werden, was unmittelbar aber zunächst nur die steuerliche Begünstigung von Spenden zur Folge hat[389]; in der 18. Legislaturperiode war ein entsprechendes Vorhaben noch gescheitert[390]. Mit den für diese Arbeit interessanten Aspekten der Haftung des Anschlussinhabers oder dem Abmahnwesen haben diese Entwicklungen jedoch keine Berührungspunkte.

Zu dem am 15. Mai 2019 veröffentlichten Regierungsentwurfs eines Gesetzes

382 Siehe hierzu Kapitel § 1 II. 5. b) und § 1 IV.
383 Siehe hierzu sogleich Kapitel § 3.
384 Siehe hierzu Kapitel § 4 II. 4. b) ff), § 4 IX. 3. und § 5 VII.
385 Siehe Kapitel § 3 XI. 1. sowie *Reuther*, MMR 2018, 433, 436.
386 Koalitionsvertrag zwischen CDU, CSU und SPD vom 7. Februar 2018, S. 39, 12.
387 https://ec.europa.eu/digital-single-market/en/faq/wifi4eu-fragen-und-antworten - Zugriff am 31.03.2021.
388 Zu Freifunk siehe Kapitel § 1 I. 3. a) aa).
389 Koalitionsvertrag zwischen CDU, CSU und SPD vom 7. Februar 2018, S. 39.
390 *Rebiger*, Freifunk: Keine Anerkennung von Gemeinnützigkeit.

zur Stärkung des fairen Wettbewerbs[391] ließ die Bundesregierung in der zugehörigen Pressemitteilung verlauten, dass dieser insbesondere auch den Missbrauch urheberrechtlicher Abmahnungen einschränken werde.[392] Tatsächlich ist der Entwurf aber fast ausschließlich mit dem Wettbewerbsrecht und anderen Bereichen des geistigen Eigentums befasst. Betreffend Abmahnungen im Urheberrecht wird lediglich eine marginale Abwandlung des Wortlauts des § 97a Abs.2 Satz 1 Nr.4 UrhG vorgeschlagen.[393] Wegen des Rückgangs von Abmahnungen und illegalem *filesharing* seien im Urheberrecht im Übrigen keine weiteren Änderungen nötig.[394] Das Gesetz zur Stärkung des fairen Wettbewerbs[395] ist nunmehr am 2. Dezember 2020 in Kraft getreten, mit der besagten marginalen Änderung des § 97a Abs.2 Satz 1 Nr.4 UrhG.

Mit weiterer Aktivität des Bundesgesetzgebers betreffend *filesharing*-Abmahnungen ist daher in absehbarer Zeit nicht zu rechnen.

Auf EU-Ebene ist am 6. Juni 2019 die Richtlinie (EU) 2019/790[396] in Kraft getreten, die gemäß ihrem Art. 29 Abs.1 bis zum 7. Juni 2021 in nationales Recht umzusetzen ist. Umstritten war im Verlauf des Gesetzgebungsverfahrens insbesondere der Art. 13 der Entwurfsfassung (der in der Richtlinie nun in Art. 17 enthalten ist) und die hieraus möglicherweise entstehende Verpflichtung für Inhalteanbieter, Upload-Filter einzurichten.[397] Allgemein geltende Uploadfilterpflichten könnten für die Betreiber von BitTorrent-Indexseiten theoretisch relevant werden[398]; allerdings haften diese typischerweise schon unter Geltung des bisherigen Haftungsregimes[399]. Internetanschlussinhaber wären hiervon jedenfalls nicht betroffen. Andere Akteure des BitTorrent-Systems haben Art. 17 allerdings bereits als relevant für ihren

391 https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_fairen_Wettbewerbs.html - Zugriff am 31.03.2021.

392 https://bit.ly/2HL8W9x - Zugriff am 31.03.2021.

393 Seite 12 des Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs.

394 Seite 16 des Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs.

395 BGBl. I S. 2568.

396 Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG.

397 Vgl. *Spindler*, CR 2019, 277, 285ff.; *Senftleben*, ZUM 2019, 369, 371ff.

398 Siehe auch *Maxwell*, Will Piracy-Focused Torrent & Streaming Sites Be Affected by Article 13/17?

399 Siehe Kapitel § 5 II. 1.

Tätigkeitsbereich betrachtet.[400] Jedoch bleibt abzuwarten, wie Art. 17 bzw. die entsprechende Umsetzungsnorm in der Praxis angewendet wird. Überdies hat Polen insbesondere gegen Art. 17 der Richtlinie (EU) 2019/790 Klage vor dem EuGH erhoben, sodass abzuwarten bleibt, ob diese Regelung überhaupt Bestand haben wird.[401]

Auf EU-Ebene sind weiterhin die Pläne zum *Digital Services Act* zu beobachten. Jedoch sind diese noch zu wenig ausgereift, als dass sich hier eine Einschätzung abgeben lässt, wie sich diese genau auf die Plattformhaftung – insbesondere im Verhältnis zur soeben erwähnten Urheberrechtslinie – auswirken wird; Auswirkungen auf Endnutzer sind jedenfalls nicht zu erwarten.[402]

Anders sieht dies im Hinblick auf die Rechtsprechung des EuGH aus. Zwar gilt dies noch nicht für die Rs. C-682/18 und C-683[403], da diese die Haftung von Videodiensten wie YouTube sowie Sharehostern[404] zum Gegenstand hat, das Urteil des EuGH sich also möglicherweise auf die soeben angesprochene Haftung von Akteuren wie den Betreibern von BitTorrent-Indexseiten auswirken kann, aber nicht auf die Haftung von Anschlussinhabern; sehr wohl gilt dies aber aber für die Rs. C-597/19[405], die in Teilbereichen für die Haftung von BitTorrent-Endnutzern relevant sein wird.[406]

Zuletzt sind sodann auf internationaler Ebene wiederum keine relevanten Entwicklungen zu erwarten: Ob das *Transantlantic Trade and Investment Partnership*-Abkommen (TTIP) noch zu Stande kommt, und ob es für das *filesharing* relevante Regelungen enthalten würde, ist ungewiss. Die Verhandlungen zum *Comprehensive Economic and Trade Agreement* (CETA) werden wohl fortgeführt, allerdings wird es keine für das *filesharing* relevante Regelungen enthalten. Der in dem (gescheiterten) *Anti-Counterfeiting Trade Agreement* (ACTA) in Art. 27 Abs.4 vorgesehene Auskunftsanspruch von

400 *Maxwell*, Huge Torrent Tracker Calls it Quits After 12 Years, Citing Article 13.

401 becklink 2013223.

402 Vgl. https://ec.europa.eu/digital-single-market/en/digital-services-act-package - Zugriff am 31.03.2021.

403 Siehe hierzu die Schlussanträge vom 16. Juli 2020, Rs. C-682/18 und C-683 – ECLI:EU:C:2020:586 - „YouTube/Cyando“.

404 Dort dem Sharehoster *uploaded*.

405 Siehe hierzu die Schlussanträge vom 17. Dezember 2020, Rs. C-597/19 – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

406 Siehe hierzu die Kapitel § 3 I., § 4 II. 6.., § 4 IV. 1. f) und § 5 IV. 3. b) aa).

Behörden gegen ISPs betreffend IP-Adressen von Endnutzern ist in CETA jedenfalls ausdrücklich nicht vorgesehen.[407]

[407] *Lahmann*, Urheberrechte in CETA, S. 8.

§ 3 Das sogennante Abmahnwesen

I. Einleitung

Für das Verständnis des Begriffs „Abmahnwesen“ erscheint es für die Zwecke dieser Arbeit fruchtbarer, ihm sich durch eine Beschreibung seiner Extension zu nähern und eine Definition erst abschließend zu bilden als das umgekehrte Verfahren. Dies ist dem Vorverständnis des juristischen Lesers geschuldet. Für diesen ist das Instrument der Abmahnung zunächst nichts besonderes, sondern als Reaktion auf eine Rechtsverletzung Gegenstand regulärer rechtsanwaltlicher Tätigkeit. Von dieser Tätigkeit ein „Abmahnwesen“ eigener Art abzugrenzen, erscheint daher zunächst befremdlich oder zumindest künstlich. In diesem Kapitel wird jedoch aufgezeigt, dass eine solche Abgrenzung auf dem Gebiet der Urheberrechtsverletzungen durch *filesharing* nach Betrachtung der rechtstatsächlichen Entwicklungen berechtigt ist. Auf Basis dieser Betrachtung lässt sich sodann losgelöst vom konkreten Phänomen eine allgemeine Definition des Begriffs „Abmahnwesens“ bilden.

Vorausgeschickt werden kann, dass die wissenschaftliche Neutralität die Verwendung des Begriffs „Abmahnwesen“ – statt einer der im gesellschaftspolitischen Diskurs zahlreichen anderen benutzten Bezeichnungen – bedingt. Sprechen Nicht-Juristen im Zusammenhang mit *filesharing*-Abmahnungen beispielsweise dysphemistisch von einer „Abmahn-Industrie“[1], so schickt dies ein entsprechend negativ konnotiertes Vorverständnis voraus, das einen neutralen Diskurs von vornherein erschwert. Gleichwohl soll nicht ignoriert werden, dass eine solche Begriffsfindung Indikator dafür sein kann, dass die Eingangsprämisse der Andersartigkeit des Gebrauchs von Abmahnungen im Bereich des *filesharing* gegenüber anderen Rechtsbereichen nicht abwegig sein

[1] Zum Beispiel *Bleich*, c't, Bd. 1, 2010, S. 154.

muss.

Außerdem sei ergänzt, dass der Begriff „Troll“ in dieser Arbeit ebenfalls nicht verwendet wird. Als „Trolle“ bezeichnete man zunächst im journalistischen, später aber auch juristischen Sprachgebrauch, in den USA operierende Unternehmen, die selbst nichts produzieren, sondern Patente von – häufig – niedriger Erfindungshöhe ankaufen, um anschließend produzierende Unternehmen zu verklagen und – vor dem Hintergrund der Kosten eines US-Gerichtsverfahrens – zu einem ertragreichen Vergleich zu bewegen; diese Praxis hat mittlerweile auch in anderen Ländern Schule gemacht.[2] In der US-amerikanischen juristischen Literatur zum Urheberrecht werden Unternehmen, die für Urheberrechtsverstöße durch *filesharing* abmahnen lassen, ebenfalls als Trolle bezeichnet.[3] Auch in die europäische Judikatur hat dieser Begriff nunmehr Eingang gefunden.[4] Jedenfalls für Deutschland passt dieser Sprachgebrauch jedoch schon deswegen nicht, weil hier so gut wie keine Fälle bekannt sind, in denen ausschließliche Verwertungsrechte allein deswegen angekauft wurden, um gegen Verletzer vorzugehen. Und in denjenigen Fällen, in denen eine Klage auf ein ausschließliches Nutzungsrechts für das Angebot in *filesharing*-Systemen gestützt wurde, ist die Existenz eines solchen nach § 31 UrhG eigenständigen und abgrenzbaren Nutzungsrechts[5] und damit die Aktivlegitimation verneint worden.[6] Stattdessen sind Abmahnende und Kläger ganz regelmäßig diejenigen Filmstudios, Plattenproduzenten und Videospiele-Publisher, die in die Entstehung und Vermarktung der jeweils abgemahnten Werke auch investiert haben.

---

2 *Ohly*, GRUR Int. 2008, 787, 787.

3 Siehe hierzu Kapitel § 3 XII. 6.

4 Siehe Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 5 – ECLI:EU:C:2020:1063 - „M.I.C.M.“, mit Nachweis der Verwendung des Begriffs seit den 1870er Jahren.

5 Siehe hierzu auch *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 359ff.

6 Beispielsweise AG Charlottenburg, Urteil vom 26. Mai 2016, Az. 218 C 37/16, Rz. 20 – juris; auch in den USA ist die Existenz eines solchen Nutzungsrechts gelegentlich Streitgegenstand, *Van Der Sar*, Movie Company Has No Right to Sue, Accused Pirate Argues.

II. Empirie zum Umfang von *filesharing*

Ohne *filesharing* gibt es kein Abmahnwesen auf dem Gebiet des *filesharing*. Glaubt man mancher Presseberichterstattung, verliert *filesharing* jedoch rapide an Bedeutung.[7] Artikel wie der eben zitierte interpretieren jedoch die Datenlage falsch.

1. BitTorrent-Datenverkehr

Zunächst ist zu konstatieren, dass der mittels des BitTorrent-Protokolls abgewickelte Datenverkehr[8] *relativ* betrachtet – im Vergleich zu früher – nach und nach abgenommen hat. Beispielsweise hatte BitTorrent 2011 noch einen durchschnittlichen Anteil von über 28 Prozent am gesamten terrestrischen Datenverkehr in Europa – und damit auch den, relativ betrachtet, größten.[9] In 2016 sank dieser Anteil auf etwas über 8 Prozent und lag damit deutlich hinter HTTP- und YouTube-Datenverkehr.[10] Allerdings gehen die absoluten Zahlen hieraus nicht hervor[11], da sich die Größe des gesamten Internetdatenverkehrs in diesem Zeitraum mehr als verdreifacht hat.[12]

Nach den verfügbaren Daten ist der BitTorrent-Datenverkehr in *absoluten* Zahlen – jedenfalls im Vergleich zwischen 2009, 2013 und 2016 – nach Erhebungen des TK-Unternehmens *Cisco Systems* tatsächlich sogar jeweils gewachsen, nämlich von ca. 3500 Petabyte pro Monat im Jahr 2009[13] auf ca. 5100 im Jahr 2013[14] und sodann auf ca. 5400 im Jahr 2016[15]. Zwar wird nach der Untersuchung für das Jahr 2016 für die folgenden Jahre eine mittlere Schrumpfungsrate im mittleren einstelligen Bereich prophezeit; allerdings lag schon die Untersuchung für das Jahr 2013 mit derselben Vorhersage für die Jahre nach 2013 falsch.

Aus den für das Jahr 2020 verfügbaren Daten lässt sich ableiten, dass sich der Anteil von BitTorrent am globalen Datenverkehr nunmehr auf einem hohen

7 *Bershidsky*, Why Netflix Is Winning the Online Piracy Wars.
8 Zur gegenwärtig empirischen Irrelevanz anderer *filesharing*-Protkolle siehe Kapitel § 1 II. 4. f).
9 *Sandvine*, Global Internet Phenomena Report Spring 2011.
10 *Sandvine*, Global Internet Phenomena Asia-Pacific & Europe 2016.
11 *Van Der Sar*, BitTorrent Still Dominates Internet's Upstream Traffic.
12 https://en.wikipedia.org/wiki/Internet_traffic#Survey - Zugriff am 31.03.2021.
13 *Cisco*, Cisco Visual Networking Index: Forecast and Methodology, 2009–2014.
14 *Cisco*, Cisco Visual Networking Index: Forecast and Methodology, 2013–2018.
15 *Cisco*, Cisco Visual Networking Index: Forecast and Methodology, 2016–2021.

Niveau stabilisiert hat.[16] In der Zukunft sind Umstände wie die Lockdowns auf Grund der COVID19-Pandemie oder die Zersplitterung des Streaming-Marktes in eine Vielzahl von Anbietern geeignet, eine relevante Zunahme der BitTorrent-Nutzung zu bewirken.[17]

2. BitTorrent-Nutzer

Untersuchungen für die Zahl der Nutzer weisen zum Teil erhebliche Spannbreiten auf.[18] Es existieren jedoch drei Untersuchungen, die darin übereinstimmen, dass der Wert sehr hoch sein muss. So für das Jahr 2009 über 357 Millionen[19], für das Jahr 2013 über 210 Millionen[20] und für das Jahr 2014 über 300 Millionen *unique*-Nutzer.[21] Zu dieser Zahl passt die Angabe des BitTorrent-Entwicklers aus dem Jahr 2012, dass seine beiden Referenzclients ca. 150 Millionen Nutzer hätten[22], zusammen betrachtet mit einem Umfrageergebnis aus dem Jahr 2015, demzufolge der (nunmehr einzige) Referenzclient des Entwicklers einen Marktanteil von etwas über 42 Prozent habe.[23] Eine Dunkelziffer verbleibt jedenfalls unabhängig von der Untersuchungsmethode, da diejenigen Nutzer, die auf BitTorrent über einen VPN oder Socks5-Proxy zugreifen[24], in jedem Fall nicht erfasst werden können und die Zahl dieser Nutzer nicht zu vernachlässigen sein dürfte.[25]

Übertragen auf das Jahr 2018 wären – ausgehend von einer BitTorrent-

16 *Sandvine*, The Global InternetPhenomena Report COVID-19 Spotlight, S. 7, 9.

17 *Van Der Sar*, COVID-19 'Lockdowns' Directly Impacted Torrent Download Numbers in Several Countries; *Van Der Sar*, Fragmented Streaming Landscape Keeps Piracy Relevant, Research Suggests.

18 So ermittelte eine Untersuchung für das Jahr 2009 etwas über 5 Millionen *unique*-Nutzer, siehe *Zhang* et al., IEEE Transactions on Parallel and Distributed Systems, Nr. 7, Bd. 22, 2011, S. 1164, 1171; eine andere Untersuchung ermittelte von 2011 bis 2013 von 15 bis zu 27 Millionen *unique*-Nutzer pro Tag, mit steigender Tendenz – und das allein für die DHT, siehe *Wang/Kangasharju*, Measuring large-scale distributed systems: case of BitTorrent Mainline DHT, S. 1, 10; zur DHT siehe Kapitel § 1 II. 5. a) bb).

19 *Van Der Sar*, Thunder Blasts uTorrent's Market Share Away.

20 *Price*, Sizing the Piracy Universe, S. 11, 19.

21 https://www.rt.com/news/162744-p2p-file-sharing-increase/ - Zugriff am 31.03.2021 31.03.2021 ; die Methode dieser Untersuchung wird jedoch kritisch gesehen, siehe *Van Der Sar*, Media Companies Track Pirated Downloads For Marketing Purposes.

22 *Van Der Sar*, uTorrent & BitTorrent Surge to 150 Million Monthly Users.

23 *Henry*, Most Popular BitTorrent Client: uTorrent.

24 Siehe hierzu Kapitel § 1 IV. 6. b) aa).

25 *Bailey*, The Long, Slow Decline of BitTorrent.

Nutzerzahl von etwas über 300 Millionen, ca. 4,2 Milliarden Internetnutzern insgesamt[26] und der Annahme, dass die Nutzerbasis im wesentlichen konsistent bleibt (also Nutzer für längere Zeit Nutzer bleiben und neue Nutzer ungefähr im gleichen Maße hinzu kommen wie alte Nutzer wegfallen) – etwas über sieben Prozent aller Internetnutzer auch BitTorrent-Nutzer.

Kontraintuitiv befinden sich diese Nutzer nicht primär in Entwicklungsländern. Stattdessen besteht eine starke Korrelation zwischen *filesharing*-Nutzung, Bruttoinlandsprodukt und Bevölkerungsgröße.[27] Deutschland rangiert nach einer urheberrechtsindustrienahen Schätzung hinsichtlich des Online-Zugriffs auf urheberrechtsverletzende Dateien auf Platz 8.[28]

3. Urheberrechtsverletzende Nutzung von BitTorrent

Wie bereits in Kapitel § 1 III. dargestellt wurde, kann BitTorrent zum Tausch von Daten jeglicher Art verwendet werden, also sowohl urheberrechtskonformer- als auch verletzender. Nach den – hierzu vorhandenen – Untersuchungen, ist der weit überwiegende Anteil der getauschten Dateien (wenig überraschend) urheberrechtsverletzend. Genannt werden ein verletzender Anteil von 97 Prozent[29], 99 Prozent[30] und – pornographische Inhalte sogar ausgenommen – 99, 97 Prozent[31]. Jedoch wurde in diesen Untersuchungen jeweils eine Vorauswahl getroffen, d.h. sehr wenig getauschte Dateien wurden nicht berücksichtigt; der verletzende Anteil könnte daher insgesamt etwas niedriger sein.[32] Jedenfalls darf mangels anderweitiger Erkenntnisse davon ausgegangen werden, dass sich der urhe-

[26] http://www.internetworldstats.com/stats.htm - Zugriff am 31.03.2021.

[27] *Liu*, Quantifying the Heterogeneous Effects of Piracy on the Demand for Movies, S. 12f.; *Scanlon/Hannaway/Kechadi*, A week in the Life of the Most Popular BitTorrent Swarms, S. 4.

[28] *MUSO*, Global Piracy Report, S. 11; leider differenziert der Report in diesem Punkt nicht zwischen *filesharing* und Sharehosting. Da aber nicht ersichtlich ist, dass in Bezug auf den Zugriff auf diese Übertragungsmedien große Unterschiede zwischen den Ländern bestehen, ist diese Schätzung zumindest ein brauchbarer Näherungswert.

[29] *Watters/Layton/Dazeley*, Information Security Technical Report, Bd. 16, 2011, S. 79, 85.

[30] *Felten/Sahi*, Census of Files Available via BitTorrent.

[31] *Price*, Sizing the Piracy Universe, S. 29f.

[32] Zudem ist zu beachten, dass sich die Untersuchung von *Felten/Sahi* auf die DHT beschränkt und sich die Untersuchungen von *Watters et al.* und *Price* auf beliebte Tracker beschränken.

berrechtsverletzende Datenverkehr im Mittel gleichmäßig auf alle Nutzer verteilt. Mithin dürfte der weit überwiegende Teil der BitTorrent-Nutzer das BitTorrent-System (auch) für Urheberrechtsverletzungen nutzen.

4. Ergebnis

Als Fazit lässt sich damit die Aussage rechtfertigen, dass BitTorrent-*filesharing* nach wie vor ein Massenphänomen ist und bleiben wird. Soweit *filesharing* aus der öffentlichen und rechtswissenschaftlichen Wahrnehmung verschwunden ist, kann dies nicht an fehlender Relevanz liegen; Grund ist wohl vielmehr, dass die Urheberrechtsindustrie sich mit seiner Existenz arrangiert hat.[33]

5. Vergleich mit Streaming und Sharehosting

Vergleichsdaten zum Streaming und Sharehosting existieren kaum; jedenfalls nach der bereits zitierten industrienahen Untersuchung sind die Zugriffszahlen auf Sharehosting-Seiten und BitTorrent-Indexseiten ungefähr gleich hoch, die auf Streaming-Seiten ca. dreimal so hoch wie die Zugriffszahlen auf Sharehosting-Seiten und BitTorrent-Indexseiten jeweils für sich genommen.[34] Ob sich die Nutzerbasen jeweils überlappen, ist nicht ersichtlich. Jedenfalls erscheint es plausibel, dass Streaming-Dienste wegen der leichteren Auffindbarkeit und den geringeren technischen Hürden mehr genutzt werden als *filesharing* und Sharehosting. Jedoch sind, technisch bedingt, nicht alle Werke von Streaming betroffen, insbesondere nicht Videospiele und Software.

III. „Piraterie“ als Politikum

Die *Big Three* - Musiklabel[35], die *Big Six* - Filmstudios[36] und mehrere der großen Video-Spielepublisher[37] sind in den USA ansässig und vereinen jeweils das Gros der Umsätze ihrer Branche auf sich. Sie sind mithin ein wichtiger Teil der Exportwirtschaft der USA. Ausgehend von der in der Industrie vorherrschenden Überzeugung, dass das illegale Kopieren ihrer Werke in der

33 *Steele*, If You Think Piracy Is Decreasing, You Haven't Looked at the Data....
34 *MUSO*, Global Piracy Report, S. 9.
35 *McDonald*, The Big Three Record Labels.
36 https://en.wikipedia.org/wiki/Major_film_studio#Majors - Zugriff am 31.03.2021.
37 https://en.wikipedia.org/wiki/Video_game_publisher#Rankings - Zugriff am 31.03.2021.

ökonomischen Gesamtbetrachtung für sie schädlich ist[38], ist deren Interesse an einem möglichst weitreichenden und globalen Urheberrechtsschutz verständlich.

Die politikwissenschaftliche Forschung auf diesem Gebiet versteht die Art, wie diese Interessenverfolgung vonstatten geht, jedoch mehr als Hegemoniebestrebung, die im Mantel des Rechts erfolge und sich dadurch den Anschein des Interessenausgleichs gebe.[39] Plausibilieren lässt sich diese These am Beispiel der Entstehungsprozesse des TRIPS-Abkommens[40] und der EnforcementRL[41]. Weiterhin existieren zahlreiche Indizien dafür, dass die US-amerikanische Exekutive Druck auf verschiedene Länder ausübte und übt, mit dem Ziel, die Möglichkeiten der Urheberrechtsdurchsetzung in diesen Ländern zu verbessern. Ins öffentliche Bewusstsein drang diese Tatsache durch die Veröffentlichung zahlreicher diplomatischer Depeschen aus den 2000er-Jahren durch *WikiLeaks*.[42] Ein aktuelles Beispiel ist der Versuch, Costa Rica dazu zu bewegen, die .cr-Domain von *The Pirate Bay* zu dekonnektieren.[43] Stärkstes Druckmittel in Fällen wie diesen ist der sogenannte *Special 301 Report*, der auf Grundlage des 19 U.S.C ch.12 (Trade Act von 1974), § 2242, der unter der Ägide des US-Handelsbeauftragten erstellt wird.[44] Der Report listet Staaten auf, die nach Auffassung des Handelsbeauftragten ein starkes Defizit beim Schutz geistigen Eigentums aufweisen. Produkten aus Staaten, die sich auf der Liste wiederfinden, können – unter anderem – ohne Mitwirkung der Legislative Importzölle auferlegt werden.

38 Zur Bewertung der ökonomischen Folgen siehe Kapitel § 3 IX. 1.

39 *Ballano*, U.S. Global Hegemony in Intellectual Property and the Politics of Piracy and Resistance, S. 33, 38.

40 *Dobusch/Quack*, Internationale und nichtstaatliche Organisationen im Wettbewerb um Regulierung: Schauplatz Urheberrecht, S. 236, 245 und, mit weiteren Nachweisen, *Haunss/Kohlmorgen*, Lobbying or politics? Political claims making in IP conflicts, S. 107f.

41 *Haunss/Kohlmorgen*, Lobbying or politics? Political claims making in IP conflicts, S. 107, 116ff. und, mit weiteren Nachweisen, *Farrand*, Networks of power in digital copyright law and policy: political salience, expertise and the legislative process, S. 126ff.

42 *Moody*, International Journal of Communication, Bd. 11, 2017, 2912, 2915ff.

43 *Maxwell*, US Embassy Threatens to Close Domain Registry Over 'Pirate Bay' Domain.

44 *Bogedain*, GRUR Int. 2019, 543, 543ff., 550; *Burkart/Andersson Schwarz*, Gunboat Diplomacy and Pirate Sanctuaries: The Use of Trade Agreements to Promote Copyright Reform, S. 133, 135f.

Ein Beispiel für den Einsatz dieses Druckmittels trat 2017 nach einem *FOI-Request* zu Tage: Schweden war mit der Drohung, in die Liste aufgenommen zu werden, dazu bewegt worden, ein Strafverfahren gegen die (damaligen) Betreiber von *The Pirate Bay* aufzunehmen.[45] Ein anderes Beispiel: Südkorea wurde aus der Liste gestrichen, als es ein *graduated response system*[46] implementierte.[47]

Der Einfluss verschiedener Lobbyorganisationen – wie beispielsweise der *Recording Industrie Association of America* (RIAA) und der *Motion Picture Association of America* (MPAA) – auf den Inhalt des Special 301 Reports und die Ausübung von Sanktionen ist hinreichend dokumentiert.[48] Aktuelle Beispiele für diese Einflussnahme sind die Aufnahme der Schweiz in die Liste, mit der Begründung, dass das Schweizer Datenschutzrecht, das die Ermittlung von IP-Adressen in *filesharing*-Systemen verbietet, einen wirksamen Schutz des Urheberrechts verhindere[49], sowie der Versuch, Sanktionen gegen die Ukraine zu erreichen, da diese nicht genug gegen den Betrieb von BitTorrent-Indexseiten auf ukrainischen Servern tue.[50] Auch das soeben erwähnte Vorgehen gegen Schweden ereignete sich auf die Initiative von Lobbyorganisationen hin.[51] Die Einflussnahme beschränkt sich aber nicht auf den Special 301 Report. Beispielsweise besteht ein starker Verdacht, dass auf das Betreiben von Lobbyorganisationen hin in den USA ein Strafverfahren gegen den in Neuseeland ansässigen Betreiber des Sharehosters *megaupload* eingeleitet wurde (woraufhin dieser im Wege der Amtshilfe von der neuseeländischen Justiz verhaftet wurde).[52]

Im Übrigen sind für verschiedene Länder Bemühungen und zum Teil auch Erfolge dokumentiert, die dortige Gesetzeslage zu Gunsten der Urheberrecht-

---

45 *Van Der Sar*, How The US Pushed Sweden to Take Down The Pirate Bay.

46 Siehe hierzu Kapitel § 3 XII. 2. b).

47 *Elton*, MEIEA, Nr. 1, Bd. 14, 2014, S. 89, 103.

48 *Karaganis*, Media Piracy in Emerging Economies, S. 90f.

49 *Fahy/DeVore*, US puts Switzerland on copyright watch list; zur Rechtslage in der Schweiz siehe Kapitel § 3 XII. 2. a) aa).

50 *Van Der Sar*, Ukraine Faces Call for US Trade Sanctions over Online Piracy.

51 *Van Der Sar*, How The US Pushed Sweden to Take Down The Pirate Bay.

52 *Anderson*, The A-list conspiracy: Did Hollywood tell Obama to take down internet entrepreneur Kim Dotcom?

sindustrie zu beeinflussen, beispielsweise Kanada[53], Spanien[54], die Ukraine[55] und Neuseeland[56], insbesondere aber auch Deutschland[57].

Die Diskurshoheit der Urheberrechtsindustrie zeigt sich jedoch schon vor der Beeinflussung des Rechts in grundlegenden Dingen wie der Prägung des Sprachgebrauchs. Aus dieser Warte betrachtet ist nicht weiter verwunderlich, dass *filesharing*, UseNet-Anbieter, Sharehosting und Streaming (als ein Sonderfall des Sharehosting) zusammen erfolgreich mit dem Etikett „Piraterie“ versehen werden konnten, obwohl durch diese Dienste keine Geiseln genommen und niemanden Gewalt angetan wird.[58] Entsprechendes gilt für den, im deutschen Sprachraum durch Werbekampagnen forcierten, Begriff der „Raubkopie“.[59] Beide Begriffe werden unhinterfragt in juristischen Publikationen[60] oder Gesetzen[61] verwendet.

Wenn auch das in diesem kurzem Exkurs Gesagte nicht unmittelbar für die juristische Betrachtungsweise relevant ist, ist die Eruierung der außerjuristischen Vorverständnisse dennoch unabdingbar, da sie Erstere prägen. Die Kenntnis der politischen Hintergründe[62] zeigt das strukturelle Machtungleichgewicht auf: während die Urheberrechtsindustrie sprichwörtlich „Berge versetzen“ kann, um ihre – gegenüber urheberrechtsverletzenden Angeboten grundsätzlich berechtigten – Interessen durchzusetzen, geraten Internetanschlussinhaber demgegenüber ins Hintertreffen.

Nicht vergessen werden darf, dass das Gesamtbild freilich komplexer ist,

53 *Geist*, Wikileaks Cables Show Massive U.S. Effort to Establish Canadian DMCA.

54 *Masnick*, No Surprise: Wikileaks Leak Shows US Entertainment Industry Wrote Spain's New Copyright Law.

55 *McDonald*, International Journal of Cultural Policy, Nr. 5, Bd. 22, 2016, S. 686, 695f.

56 *Geist*, Wikileaks on New Zealand Copyright: US Funds IP Enforcement, Offers to Draft Legislation.

57 *Dobusch/Schüßler*, Technological Forecasting and Social Change, Bd. 83, 2014, S. 24, 30.

58 Vgl. *Kur*, APuZ 2012, 21, 21f.; *Mirghani*, Critical Studies in Media Communication, Nr. 2, Bd. 28, 2011, S. 113, 116.

59 *Krempl*, Filmwirtschaft startet Abschreckungskampagne gegen Raubkopierer.

60 Wie eine entsprechende Suchabfrage bei juristischen Datenbanken wie *beck-online* oder *juris* zeigt.

61 Beispielsweise Erwägungsgrund 1 Verordnung (EU) Nr. 608/2013 des Europäischen Parlaments und des Rates vom 12. Juni 2013 zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden und zur Aufhebung der Verordnung (EG) Nr. 1383/2003 des Rates.

62 Zu den ökonomischen siehe Kapitel § 3 IX. 1.

als hier dargestellt werden kann. In eine erschöpfende Betrachtung wären auch weitere Akteure wie ISPs und sonstige Service-Anbieter einzubeziehen, die wiederum eigene Interessen gegenüber Anschlussinhabern und Rechteinhabern haben oder haben können.[63] Auch ist es vereinfacht, von „den Rechteinhabern“ zu sprechen, da die Urheberrechtsindustrie sehr vielfältig ist (Musik, Filme und Serien, Videospiele, Software, Bücher und Hörbücher, Wissenschaftsverlage, Pornographie). Allerdings wiederum ist nicht bekannt, dass sich die Branchen beim Vorgehen gegen Urheberrechtsverletzungen oder Lobbying der Gesetzgeber gegenseitig behindern. Innerhalb der Branchen wird das jeweilige Brancheninteresse, wie bereits erwähnt, häufig konzentriert durch Interessenverbände wahrgenommen.[64]

Im Ergebnis ist zumindest festzuhalten: Das Recht berücksichtigt ständig Machtdisparitäten, wie beispielsweise im Verbraucherschutz und im Mietrecht. Sowie man regelmäßig darauf angewiesen ist, im Online-Versandhandel Waren zu bestellen und zur Miete zu wohnen, ist man regelmäßig genauso darauf angewiesen, einen Internetanschluss innezuhaben und/oder mit Dritten zu teilen. Folglich muss auch letzteres beim Ausgleich zwischen der Eigentumsfreiheit und der Sozialbindung des Eigentums beachtet werden.

IV. Das Vorgehen gegen Endnutzer im Konzert der Urheberrechtsdurchsetzung im Internet

1. Einleitung

Im Vorgehen gegen Online-„Piraterie“ hat die Urheberrechtsindustrie weltweit zahlreiche rechtliche Meilensteine[65] erreicht. Die bereits erwähnten

[63] Ein besonders eindrückliches Beispiel für die Interessendurchsetzung seitens dieser Gruppe sind die Proteste gegen die vormals geplanten Gesetzesvorhaben SOPA und PIPA in den USA, siehe https://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA - Zugriff am 31.03.2021. Als aktuelles Beispiel für die Beteiligung dieser Gruppe bei der Formulierung des *Special 301 Report* siehe *Van Der Sar*, Tech Giants Warn US Govt. Against Onerous Copyright Laws.

[64] Ein weiteres Beispiel für einen sehr umfassenden Interessenverband ist die im Jahr 2017 gegründete *Alliance for Creativity and Entertainment*, siehe *Maxwell*, Global Entertainment Giants Form Massive Anti-Piracy Coalition.

[65] Hiermit ist keine positive oder negative Wertung derselben durch den Verfassers verbunden.

Verfahren gegen Entwickler von *filesharing*-Systemen[66], gegen Sharehoster wie *megaupload*[67] und Betreiber von BitTorrent-Indexseiten wie *The Pirate Bay*[68] sind dabei nur die Spitze des Eisberges.

Erfolgreiches Vorgehen gegen Dienste dieser Art wird nicht nur aus der EU und den USA berichtet. Bezüglich Sharehostern beispielsweise aus Norwegen[69], vor allem aber auch aus Ländern, die auf der *Watch List* des Special 301-Reports stehen und daher typischerweise weniger mit ausreichendem Urheberrechtsschutz assoziiert werden, beispielsweise China[70] und Peru[71]. Bekannt sind zudem zahlreiche internationale Fälle, in denen große BitTorrent-Indexseiten und Tracker abgeschaltet werden konnten, beispielsweise durch länderübergreifende Operationen in den USA und Polen[72] sowie Frankreich und Schweden[73], im Übrigen aber auch in Ländern wie China[74] und Russland[75]. Das sind nur aktuelle Beispiele: Bereits Mitte der 2000er Jahre konnten länderübergreifend die Betreiber mehrerer großer Indexseiten erfolgreich verfolgt werden.[76]

Noch weitaus beliebter als das unmittelbare Vorgehen gegen die Betreiber solcher Dienste ist im internationalen Vergleich, ISPs die Pflicht zu DNS- und IP-Sperren bezüglich solcher Dienste aufzuerlegen. Netzsperren dieser Art werden praktisch – durch die Rechtsprechung des EuGH abgesichert[77] – EU-weit ausgesprochen[78], ebenso jedoch (mittlerweile) auch in praktisch den meisten anderen von Bevölkerungszahl und Wirtschaftskraft her relevanten

66 Siehe Kapitel § 1 II. 4.
67 Siehe Kapitel § 3 III.
68 Siehe Kapitel § 3 III.
69 Oberster Gerichtshof, Urteil vom 27. Januar 2005, Az. 2004/822 – GRUR Int. 2005, 522 - „napster.no“.
70 *Maxwell*, MPAA Wins Movie Piracy Case in China After Failed Anti-Piracy Deal.
71 *Maxwell*, Peru Authorities Shut Down First 'Pirate' Websites, Three Arrested.
72 *Van Der Sar*, The KickassTorrents Shutdown, One Year Later.
73 *Maxwell*, T411, France's Most-Visited Torrent Site, Has Been Shut Down.
74 *Odell*, Downloading Frenzy in China: Gov't Blocking All Torrent Sites Soon?
75 *Maxwell*, Russia Orders Public Tracker to Block Itself, Site Refuses.
76 *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 3: Suprnova und EliteTorrent; *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 4: Torrentspy und isoHunt.
77 EuGH, Urteil vom 27. März 2014, Rs. C-314/12 – ECLI:EU:C:2014:192 - „UPC Telekabel“.
78 Siehe mit einem Überblick *Riordan*, The Liability of Internet Intermediaries, S. 504ff.

Jurisdiktion, also zum Beispiel Australien[79], China[80], Russland[81] und Indien[82] (bisher nicht jedoch in den USA[83]). Nach der Zählweise der *MPA Canada* gibt es – Stand 2018 – weltweit in 42 Ländern die Möglichkeit, urheberrechtsverletzende Seiten mit Netzsperren zu belegen.[84] Für andere Länder wie Neuseeland, Japan und Südafrika sind entsprechende Gesetzesänderungen in Planung.[85]

Auch in Deutschland kann die Urheberrechtsindustrie auf eine lange Liste von Erfolgen blicken: für Sharehoster entwickelte der BGH in der Rechtsprechungsserie gegen den Dienst *Rapidshare*[86] eine strenge Störerhaftung.[87]

79 *Van Der Sar*, Court Orders Aussie ISPs to Block Dozens of Pirate Sites.

80 *Maxwell*, China Says It Will „Severely Strike" Websites Involved in Piracy.

81 *Maxwell*, Russia Blocks 500 'Pirate' Sites in Four Months, Without a Single Court Order.

82 *Van Der Sar*, Hollywood Studios Get ISP Blocking Order Against Rarbg in India.

83 *Kipshagen*, Haftung bei offenem WLAN, S. 231ff.

84 Siehe hierzu die Seiten 4ff. der Eingabe der MPA Canada in einem kanadischen Gesetzgebungsverfahren Netzsperren betreffend, abrufbar unter https://torrentfreak.com/images/mpa-can.pdf - Zugriff am 31.03.2021. Nach Stand 2019 waren in 31 dieser Länder knapp 4.000 Webseiten und über 8.000 Domainnamen geblockt, siehe *Van Der Sar*, Nearly 4,000 Pirate Sites Are Blocked by ISPs Around The World.

85 *Maxwell*, Hollywood Says Only Site-Blocking Left to Beat Piracy in New Zealand; *Maxwell*, Japan Government Presents Pirate Website Blocking Proposals; *Van Der Sar*, Copyright Holders Want ISPs to Police Pirate Sites and Issue Warnings.

86 Zuletzt BGH, Urteil vom 15. August 2013, Az. I ZR 80/12 – GRUR 2013, 1030 - „File-Hosting-Dienst"; zum Verlauf der Rechtsprechung siehe *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 8: Rapidshare.

87 Hierbei ist jedoch zu beachten, dass in gegenwärtig anhängigen Fällen gegen die Videoplattform *YouTube* und den Sharhoster *uploaded* der BGH dem EuGH (Rs. C-682/19 und C-683/19) mehrere Fragen zur Auslegung der InfoSocRL vorgelegt hat, sodass sich die Haftung von Sharehostern auch noch verschärfen könnte, vgl. *Soppe*, Wann und wie haften Sharehosting-Dienste? Hiervon unabhängig sind in der Instanzrechtsprechung mittlerweile Betreiber von Sharehosting-Plattformen wegen täterschaftlicher Haftung zu Schadensersatzleistungen verurteilt worden, siehe LG Hamburg, Urteil vom 14. Juli 2020, Az. 310 O 339/18 – juris. Die weiteren Entwicklungen diesbezüglich sind daher zu beobachten. Strafrechtliche Ermittlungen laufen derweil gegen die Betreiber der nunmehr abgeschalteten Plattform *share-online.biz*, siehe *Sobiraj*, Share-Online.biz: Staatsanwaltschaft will Top-Uploader verfolgen.

Gegen UseNet-Gruppen konnten sowohl zivilrechtliche Verurteilungen[88] als auch strafrechtliche Ermittlungen[89] erreicht werden. Strafrechtlich verurteilt wurden Hintermänner der großen Streaming-Seiten *kino.to*[90] und *kinox.to*[91]. Ansprüche gegen ISPs auf die Einrichtung von IP- und DNS-Sperren gegen urheberrechtsverletzende Seiten sind durch die hierzu ergangene Rechtsprechung des BGH seit 2015 anerkannt[92], die – zumindest in ersten instanzgerichtlichen Entscheidungen – auch unter Geltung des § 8 Abs.1 Satz 2 TMG n.F. fortgeführt[93], und deren Umsetzung ab 2021 durch eine privatwirtschaftliche Vereinbarung zwischen der Urheberrechtsindustrie und zahlreichen ISPs mittels einer Clearingstelle mit der Bezeichnung „Clearingstelle Urheberrecht im Internet“ (CUII) institutionalisiert wird[94].

Diese weltweiten rechtlichen Erfolge seit den 2000er Jahren scheinen jedoch in tatsächlicher Hinsicht wenig zu bewirken. Blickt man in den dem Special 301-Report beigefügten *2019 Review of Notorious Markets for Counterfeiting and Piracy*[95] oder das von der EU-Kommission herausgegebene Äquivalent hierzu, die *Counterfeit and Piracy Watch List* von 2020[96], die jeweils auf konkrete schutzrechtsverletzende Angebote eingehen, sind zwar die meisten Sharehoster und Indexseiten, die Gegenstand der beispielhaft erwähnten Verfahren waren, verschwunden; dafür sind jedoch zahlreiche neue solcher Diens-

88 OLG Düsseldorf, Urteil vom 15. Januar 2008, Az. I-20 U 95/07 – MMR 2008, 254; OLG Hamburg, Urteil vom 14. Januar 2009, Az. 5 U 113/07 – MMR 2009, 631; OLG Hamburg, Urteil vom 28. Januar 2009, Az. 5 U 255/07 – MMR 2009, 405; OLG Hamburg, Urteil vom 9. Januar 2014, Az. 5 U 52/10 – juris; LG Hamburg, Urteil vom 22. Juni 2018, Az. 308 O 314/16 – ZUM 2018, 814; weitere Übersicht bei *Tschmuck*, Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 7: Usenet.

89 *Maxwell*, Multi-National Police Operation Shuts Down Pirate Forums.

90 LG Leipzig, Urteil vom 14. Juni 2012, Az. 11 KLs 390 Js 191/11 – ZUM 2013, 338.

91 BGH, Beschluss vom 11. Januar 2017, Az. 5 StR 164/16 – GRUR 2017, 273.

92 BGH, Urteil vom 26. November 2015, Az. I ZR 174/14 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“; auch BGH, Urteil vom 26. November 2015, Az. I ZR 3/14 – MMR 2016, 188.

93 Siehe beispielsweise LG München I, Urteil vom 21. Dezember 2017, Az. 7 O 17752/17 – MMR 2018, 322; bestätigt durch OLG München, Urteil vom 14. Juni 2018, Az. 29 U 732/18 – GRUR 2018, 1050.

94 *Kleinz*, Urheberrechtsverletzungen auf Streaming-Sites: Neuer Anlauf für DNS-Sperren.

95 https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf - Zugriff am 31.03.2021.

96 https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf - Zugriff am 31.03.2021.

te entstanden, ohne dass sich am zu Grunde liegenden technischen Prinzip etwas Wesentliches geändert hätte.

Es kann an dieser Stelle offen bleiben[97], ob dies an einem Defizit der Rechtsdurchsetzungsmöglichkeiten (vor allem in Schwellenländern), dem fehlenden Willen oder fehlenden Anstrengungen seitens der Rechteinhaber oder aber an den faktischen und technischen Möglichkeiten der Anbieter solcher Dienste, der Rechtsverfolgung jedenfalls zeitweise auszuweichen, liegt. Wo jedoch die Anbieter schwer zu greifen sind und Maßnahmen gegen Intermediäre wenig helfen, rücken die „Abnehmer", also die Endnutzer, in den Fokus.

Diese sind wenig mobil, weniger technisch versiert als die Anbieter (insbesondere in Fragen der Anonymisierung und Identitätsverschleierung) und können grundsätzlich zudem leichter einer bestimmten Schadenshandlung zugerechnet werden, was die Berechnung des Schadensersatzes (der Theorie nach) erleichtert. Zudem werden sie regelmäßig – sofern sie, wie typisch, nur für eine oder wenige Verletzungshandlungen in Anspruch genommen werden (können) – auch in der Lage sein, die Schadenssumme zu bezahlen, während bei Anbietern häufig nicht zur Liquidierung des (behaupteten) Schadens ausreichendes Vermögen vorhanden sein dürfte.

2. Zum Vorgehen gegen Endnutzer von Streaming-Diensten

Bei Sharehostern und Streaming-Seiten (die ihre Inhalte regelmäßig auf Sharehostern speichern) ist die Rückverfolgung der Endnutzer in den meisten Fällen nicht möglich. Wie in Kapitel § 1 IV. gezeigt wurde, kann die IP-Adresse der Endnutzer von BitTorrent-*filesharing* regelmäßig ermittelt werden, weil diese dort wegen des systemseitig vorgesehenen Prinzips, dass der Endnutzer immer auch zum Anbieter von Dateifragmenten wird, zwangsweise zumindest denjenigen, die diese Fragmente abfragen, offenbart wird. Bei Sharehostern findet aber ein rein serverbasierter, zweiseitiger Datenübertragungsvorgang vom Hoster zum herunterladenden Endnutzer statt, der von außen nicht einsehbar ist.

Entsprechend verwunderlich war es folglich, als der (vermeintliche) Inhaber der Rechte von Filmen, die ohne seine Einwilligung auf der Porno-Streamingseite *RedTube* zu sehen waren, behauptete, die IP-Adressen von

[97] Siehe Kapitel § 3 IX. 2.

Nutzern der Seite, die diese Filme abgerufen hatten, geloggt zu haben. Ihm wurde daraufhin in mehreren Verfahren Auskunft über Name und Anschrift erteilt, die Nutzer anschließend abgemahnt. Es stellte sich jedoch im Nachhinein heraus, dass die IP-Adressen der abgemahnten Nutzer über einen *Honeypot* erlangt worden sein mussten.[98] Wahrscheinlich wurden sie von anderen Webseiten aus zunächst auf eine (nicht im Browser wiedergegebene) „Zwischenseite" eines Datenhändlers weitergeleitet, von der aus sie wiederum an die abgemahnten Videos weitergeleitet wurden. Durch das Aufrufen der zwischengeschalteten Webseite konnten die IP-Adressen der Zugreifenden erfasst und an den Abmahner übergeben werden.[99] Grundsätzlich ist denkbar, dass etwas vergleichbares sich in Zukunft wieder ereignet; sonderlich wahrscheinlich erscheint dies jedoch in Anbetracht der Tatsache, dass der RedTube-Fall der bisher einzig bekannte ist, in dem Streaming-Nutzer abgemahnt wurden, nicht. Gerade in Bezug auf die regulär genutzten illegalen Streaming-Seiten scheint das Aufsetzen eines Honeypots – schon völlig unabhängig von der beweisrechtlichen Verwertbarkeit einer auf diese Art „abgefischten" Adresse – kaum möglich zu sein.

Auch wenn also – zumindest für die EU – durch die Rechtsprechung des EuGH in der Entscheidung „Filmspeler" mittlerweile geklärt ist, dass das Streamen urheberrechtsverletzender Inhalte für den Empfänger des Streams nicht durch die Schranke des Art. 5 InfoSocRL gedeckt ist[100]: die Inanspruchnahme der Endnutzer von Streaming-Seiten scheitert ganz regelmäßig an den vorhandenen Ermittlungsmöglichkeiten. Dies dürfte – davon ausgehend, dass Streaming noch von deutlich mehr Personen genutzt wird als *filesharing*[101] – für die Urheberrechtsindustrie ein großes Ärgernis sein, da somit für einen ganzen Bereich die Endnutzer als „Zielscheiben" wegfallen.

3. Zum Vorgehen gegen Endnutzer von Sharehosting-Diensten

Selbiges wie für Streaming gilt betreffend Sharehosting-Diensten: auch hier ist der Dateiübertragungsvorgang zweiseitig, und zwar sowohl wenn der

98 *Bleich*, Briefkasten-Ermittlungen.

99 *Solmecke*, CR 2014, 137, 137.

100 EuGH, Urteil vom 26. April 2017, Rs. C-527/15, Rz. 72 – ECLI:EU:C:2017:300 - „Stichting Brein".

101 Siehe Kapitel § 3 II. 5.

Uploader Dateien auf die Server des Sharehosters hochlädt als auch dann, wenn ein Endnutzer eine Datei vom Sharehoster herunterlädt.[102] Uploader konnten in der Vergangenheit teilweise mit Erfolg ermittelt werden. Dies geschieht beispielsweise im Zusammenhang mit dem Vorgehen gegen den Sharehoster selbst, wobei direkt von diesem die im Benutzerkonto der Uploader hinterlegten Email-Adressen ermittelt wurden und dann – sofern die jeweiligen Betreiber der Email-Konten in Deutschland ansässig waren – von Letzteren die IP-Adresse, von der der letzte Zugriff auf das jeweilige Email-Konto getätigt worden war, erlangt wurde. Über die IP-Adresse konnten sodann vom jeweiligen ISP Name und Anschrift des entsprechenden Uploaders in Erfahrung gebracht werden. So gestaltete sich beispielsweise Vorgehen im Falle des Sharehosters *duckload.to*.[103]

Ein anderes Einfallstor für Ermittlungen ist der Umstand, dass Uploader zudem häufig Links auf die von ihnen hochgeladenen Inhalte auf hierfür vorgesehene Internetseiten einstellen, beispielsweise Messageboards. Beim Vorgehen gegen die Betreiber des Forums *boerse.bz* konnten so wiederum die dort in den Benutzerkonten hinterlegten Email-Adressen erlangt und im Ergebnis Uploader ermittelt werden.[104] Endnutzer bzw. Downloader müssen aber ganz regelmäßig keine Daten beim Sharehoster selbst hinterlegen, sofern sie dort kein Premiumkonto bekommen möchten; bei den genannten Foren kann aus dem Vorhandensein eines Benutzerkontos nicht geschlossen werden, welche Links letztlich angesteuert wurden. Einziges Identifikationsmerkmal ist also die IP-Adresse. Dass diese in der Vergangenheit, wie beim RedTube-Fall, durch Honeypots erlangt werden konnten, ist nicht bekannt. Es müsste also erstens der Sharehoster die IP-Adresse speichern, Letztere müssten zweitens einem Rechteinhaber mitgeteilt werden und zwar drittens, bevor die Zuordnung der IP-Adresse zu einem Endkundenanschluss zum Zeitpunkt des Downloads gelöscht wurde. Sharehoster werden natürlich im Eigeninteresse schon Schritt Nr.1 nicht durchführen. Von Premium-Nutzerkonten wird man zwar wie bei Uploadern die Email-Adresse erlangen können; dies sagt aber noch nichts darüber aus, welche Daten der Inhaber heruntergeladen hat.

---

[102] Vgl. BGH, Urteil vom 15. August 2013, Az. I ZR 80/12, Rz. 40 – GRUR 2013, 1030 - „File-Hosting-Dienst“.

[103] *Solmecke*, Duckload Premium Nutzer aufgepasst - Das LKA Dresden hat die Nutzerdaten ausgewertet.

[104] *Solmecke*, boerse.bz - Uploader wurden über die E-Mail Adressen ermittelt.

4. Ergebnis

Im Ergebnis sind die Anbieter von Sharehosting- und Streamingdiensten sowie von Indexseiten für die Urheberrechtsindustrie kaum greifbar. Die Endnutzer von Sharehosting- und Streamingdiensten sind – wie die bisherige Geschichte zeigt – noch weniger zu erreichen. Ganz anders die Endnutzer von BitTorrent-*filesharing*. Diese sind somit im Rahmen der Urheberrechtsdurchsetzung im Internet naturgemäß der einfachste und damit ein sehr beliebter Angriffspunkt.

V. Empirie zum Vorgehen gegen *filesharing*-Endnutzer

1. Einleitung

Die nachfolgenden Ausführungen beziehen sich auf Deutschland. Zum Vergleich mit anderen Ländern siehe Kapitel § 3 XII.

2. Zur Menge an Abmahnungen

Die genaue Zahl an ausgesprochenen Abmahnungen und abgemahnten Personen lässt sich nicht beziffern. Dennoch gibt es Schätzungen privater Initiativen sowie demoskopische Untersuchungen, die eine Schätzung erlauben. Auf diese Daten sowie eigens eingeholte Stellungnahmen von Rechtsanwaltskanzleien stützt sich auch der im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz erstellte Schlussbericht zur Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken.[105]

Die *Interessengemeinschaft gegen den Abmahnwahn* (IGGDAW) schätzt für die Jahre 2005 bis 2007 nach und nach steigende Zahlen von wenigen bis mehreren zehntausend, für das Jahr 2008 mit ca. 100.000 Abmahnungen.[106] 2009 sollen dann schon ca. 450.000[107], 2010 gar über 575.000 Abmahnun-

[105] *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, S. 193ff.

[106] *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, S. 201.

[107] https://www.iggdaw.de/filebase/index.php?file/17-die-gro\T1\sse-abmahnstatistik-2009/ - Zugriff am 31.03.2021.

gen ausgesprochen worden sein[108]; danach soll es jedoch einen deutlichen Rückgang gegeben haben: für 2011 werden ca. 220.000[109], für 2012[110] und 2013[111] ca. 110.000 und für 2014 „nur“ noch knapp 75.000[112] Abmahnungen geschätzt. Es wird jedoch nicht zwischen der Zahl der Abmahnungen und der Zahl der abgemahnten Personen differenziert, sodass nur spekuliert werden kann, wie viele Personen mehr als eine Abmahnung (und, in diesem Fall, wie viele Abmahnungen genau) erhalten haben. Von der IGGDAW sind ab 2015 keine Schätzungen mehr bekannt.

Laut einer im Auftrag der *Verbraucherzentrale Bundesverband* (vzvb) erstellten Umfrage des Meinungsforschungsinstituts *TNS Emnid* hätten im Zeitraum von August 2014 bis August 2016 sechs Prozent der bundesdeutschen Wohnbevölkerung ab 14 Jahre, also ca. 4,2 Millionen Personen[113], mithin im Schnitt ca. 2,1 Millionen pro Jahr, eine Abmahnung erhalten[114]; diese Zahl wird jedoch als deutlich zu hoch kritisiert, insbesondere sei die Zahl der Befragten nicht repräsentativ (nur etwas über 1000 Befragte).[115]

Nach Schätzung einer anderen privaten Initiative – der *Abmahnwahn drei-*

[108] https://www.iggdaw.de/filebase/index.php?file/18-abmahnstatistik-2010/ - Zugriff am 31.03.2021.

[109] https://www.iggdaw.de/filebase/index.php?file/19-abmahnstatistik-2011/ - Zugriff am 31.03.2021.

[110] https://www.iggdaw.de/filebase/index.php?file/20-abmahnstatistik-2012/ - Zugriff am 31.03.2021.

[111] https://www.iggdaw.de/filebase/index.php?file/21-abmahnstatistik-2013/ - Zugriff am 31.03.2021.

[112] https://www.iggdaw.de/filebase/index.php?file/22-abmahnstatistik-2014/ - Zugriff am 31.03.2021.

[113] Vgl. die Angaben zur Altersstruktur der Deutschen bei https://de.statista.com/statistik/daten/studie/1365/umfrage/bevoelkerung-deutschlands-nach-altersgruppen/ - Zugriff am 31.03.2021.

[114] *Emnid*, Bevölkerungsbefragung zum Thema Abmahnungen wegen Urheberrechtsverstößen, S. 2f.

[115] *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, S. 202; zudem differenziert die Umfrage nicht zwischen den verschiedenen Arten der Urheberrechtsverletzung, sondern fragt nur nach Urheberrechtsverletzungen allgemein. Wegen Streaming und Sharehosting-Nutzung werden Endnutzer faktisch jedoch nicht belangt, siehe Kapitel § 3 IV. Abmahnungen an Privatpersonen im nennenswerten Umfang wegen anderer Formen der Urheberrechtsverletzung, beispielsweise wegen unberechtigter Bildnutzung auf *ebay* oder *Facebook*, sind nicht bekannt. Es ist daher davon auszugehen, dass die Emnid-Umfrage primär *filesharing* erfasst.

page (AW3P) – wurden im Jahr 2017 etwas über 140.000 Abmahnungen versandt.[116] Da AW3P und IGGDAW zu Ergebnissen in ungefähr derselben Größenordnung kommen und ihre Schätzungen auf Grund von Auskünften von Anwaltskanzleien abgeben, erscheinen diese Zahlen nach hiesiger Einschätzung auch als realistischer als die Umfrage der *vzvb*. Dass nach der Schätzung von AW3P die Zahl der Abmahnungen im Jahr 2017 gegenüber der Schätzung der IGGDAW von 2014 entgegen dem vermuteten rückläufigen Trend[117] gestiegen ist, könnte sich etwa dadurch erklären, dass neben die Nutzung der regulären BitTorrent-Clients andere Dienste wie *Popcorn Time* getreten sind, die zwar wie typische Streaming-Dienste aussehen[118], auf Dateiübertragungsebene sich jedoch des BitTorrent-Protokolls bedienen.[119] Unerfahrene Nutzer, die eigentlich kein *filesharing* betreiben wollten, sehen sich daher einer Abmahnung ausgesetzt.[120]

Gegenüber den privaten Schätzungen und der Umfrage der *vzvb* ist aber zuletzt eine dritte Erkenntnisquelle zu berücksichtigen: laut einer im Jahr 2018 veröffentlichten empirischen Erhebung des *Max-Planck-Instituts für Innovation und Wettbewerb* hatten 2 Prozent der etwas über 5300 Befragten im Alter zwischen 12 und 64 Jahren in einem Zeitraum zwischen Juli 2015 und Juli 2017 eine Abmahnung erhalten.[121] Das entspricht auf ganz Deutschland hochgerechnet ca. eine Millionen Personen[122] insgesamt und damit im Schnitt 500.000 pro Jahr. Diese Erhebung liegt zahlenmäßig somit für den Vergleichszeitraum (2014 - 2017) ungefähr im Mittelfeld zwischen den Schät-

[116] AW3P-Statistik für 2017, https://www.abmahnwahn-dreipage.de/forum/viewtopic.php?f=17&t=15&start=11200 - Zugriff am 31.03.2021.

[117] *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, S. 201.

[118] Zu Streaming-Diensten siehe Kapitel § 1 I. 3. a) dd).

[119] Siehe Kapitel § 3 XI.

[120] Dieses Risiko besteht auch laut Auskünften von Anwälten, die sich in der Praxis mit Abmahnungen befassen. Siehe hierzu die Ausführungen in der AW3P-Statistik für 2015, https://www.abmahnwahn-dreipage.de/forum/viewtopic.php?f=19&t=216 - Zugriff am 31.03.2021.

[121] *Harhoff* et al., Nutzung urheberrechtlich geschützter Inhalte im Internet durch deutsche Verbraucher, S. 8; es ist – aus denselben Gründen wie bei der Umfrage des *vzvb* – davon auszugehen, dass diese Abmahnungen fast ausschließlich *filesharing* betroffen haben.

[122] Vgl. die Angaben zur Altersstruktur der Deutschen bei https://de.statista.com/statistik/daten/studie/1365/umfrage/bevoelkerung-deutschlands-nach-altersgruppen/ - Zugriff am 31.03.2021.

zungen der privaten Initiativen und der Erhebung des *vzvb*.

Welche Zahl letztlich glaubwürdiger ist, kann der Verfasser nicht abschließend beurteilen, näher liegt jedoch – wegen der im Vergleich zu den privaten Schätzungen besseren Methodik und dem im Vergleich zu der Erhebung des *vzvb* größeren Datensatzes – der Erhebung des MPI den Vorzug zu geben.

Damit kann der in dem Regierungsentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs[123] geäußerten Auffassung, dass ein spürbarer Rückgang der *filesharing*-Abmahnungen zu verzeichnen sei, allenfalls gefolgt werden, wenn man sich wie die Bundesregierung auf den Schlussbericht zur Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken stützt.[124] Die anderen, soeben genannten Untersuchen lassen einen solchen Schluss nicht zu, da sie nur für Zeiträume ab 2014 vorliegen und keinen Trend ermitteln. Jedenfalls aber kann der Auffassung der Bundesregierung, der Rückgang (sofern er denn überhaupt gegeben ist) sei nicht nur auf die rückläufige Nutzung illegalen *filesharings* zurückzuführen, sondern wesentlich auch auf das Gesetz gegen unseriöse Geschäftspraktiken[125], nicht zugestimmt werden. Ein solcher Kausalzusammenhang erscheint äußerst unwahrscheinlich, da sich die rechtliche Situation Abgemahnter durch dieses Gesetz nur in Teilbereichen leicht verbessert hat; tatsächlich ist das Gesetz kaum geeignet, *filesharing*-Abmahnungen für die Abmahnenden unattraktiv zu machen.[126] Zu einem etwaigen Rückgang von Abmahnungen dürfte das Gesetz gegen unseriöse Geschäftspraktiken also wenn dann nur einen marginalen Beitrag geleistet haben.

3. Zu den von Abmahnungen Betroffenen

Nach Einschätzung des Verfassers lässt sich aus den vorhandenen Gerichtsentscheidungen ableiten, dass der Großteil der Abmahnungen familiär genutzte Internetanschlüsse betrifft, ein kleinerer Teil den nicht-familiären privaten Bereich wie beispielsweise Wohngemeinschaften und ein geringer Teil

[123] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_fairen_Wettbewerbs.html - Zugriff am 31.03.2021.

[124] Vgl. Seite 14 des Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs.

[125] Vgl. Seite 14 des Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs.

[126] Siehe Kapitel § 3 V. 6. und § 4 X.

gewerblich genutzte Anschlüsse, beispielsweise von Hotels, Restaurants oder über Dienste wie *Airbnb* vermietete Wohnungen. Da durch die bloße Beteiligung an einem BitTorrent-Schwarm auch kein Geld verdient werden kann[127], sondern allenfalls durch Infrastruktureinrichtungen wie Indexseiten[128], ist auch davon auszugehen, dass nahezu alle abgemahnten *filesharing*-Endnutzer nicht aus kommerziellen Motiven handeln.

Betreffend Freifunk-WLAN, also kostenfrei, regelmäßig aus altruistischen Motiven angebotenes, offenes WLAN, sind dem Verfasser kaum Fälle bekannt, in denen eine Abmahnung ausgesprochen wurde. In Berlin werden seit 2012 über einen öffentlichen Träger zahlreiche kostenlose Hotspots angeboten; nach eigenem Bekunden ist es dabei noch nicht zu Urheberrechtsverletzungen gekommen.[129] Andere verlässliche Berichte zu Freifunk und Abmahnungen waren nicht auffindbar.

4. Zu den typischen Streitgegenständen der Abmahnungen

Gegenstand der Abmahnungen war bis zum Jahr 2009 noch weit überwiegend Musik, seitdem hat der Anteil an Filmen stetig zugenommen; im Jahr 2014 soll weit überwiegend wegen Filmen abgemahnt worden sein.[130] Andere Kategorien wie Videospiele, Musik und Pornographie haben demgegenüber nur noch einen Anteil von zusammen genommen etwas über einem Viertel; sonstige Werke wie Software, E-Books und Hörbücher haben nur einen sehr geringen Anteil.[131] Ab 2014 existieren keine Einschätzungen mehr zur

[127] Gegenwärtig arbeitet Rainberry unter dem Projektnamen *Project Atlas* daran, es BitTorrent-Nutzern zu ermöglichen, für das *seeden* mit Kryptowährung bezahlt zu werden, siehe hierzu die Webseite des Projekts https://www.bittorrent.com/btt/ - Zugriff am 31.03.2021 31.03.2021 sowie den Bericht hierzu bei *Van Der Sar*, BitTorrent and Tron Hope Other Clients Will Embrace 'Paid' Seeding. In Zukunft könnte es also auch möglich sein, dass Endnutzer aus kommerziellen Motiven handeln.

[128] Siehe hierzu das Schlusswort.

[129] *Mantz/Sassenberg*, CR 2015, 298, 301. Siehe dazu auch: Ausschuss für Wirtschaft und Energie, Protokoll-Nr. 18/118, S. 8.

[130] *Tschmuck*, Musik-Filesharing: Das Abmahnwesen in Deutschland – Teil 2; zu diesem Trend passen auch die Angaben bei *Lorenz*, JurPC WebDok. 132/2014, Abs. 2. Diese Angaben passen überdies zu einer informatischen Untersuchung, derzufolge der Anteil von TV-Serien und Filmen (einschließlich Pornographie) im Untersuchungszeitraum von 2009 bis 2012 über 80 Prozent betragen habe, siehe *Farahbakhsh* et al., CoRR, Bd. abs/1705.00548, 2017, S. 1, 7.

[131] *Tschmuck*, Musik-Filesharing: Das Abmahnwesen in Deutschland – Teil 2; *Lorenz*, JurPC WebDok. 132/2014, Abs. 2

Aufschlüsselung nach Werkskategorien; da aber die Möglichkeit, kostenlos und legal auf Musik über Plattformen wie *Spotify* und *YouTube* zuzugreifen, gegenüber den Jahren vor 2014 nur zugenommen hat, hingegen für andere Werksarten kaum Vergleichbares existiert, ist für gegenwärtige und zukünftige Abmahnungen wohl von einer ähnlichen Aufteilung, allerdings mit einem noch geringeren Musikanteil, auszugehen.

5. Zu den abmahnenden Kanzleien

Nach dem für den von der IGGDAW geschätzten Zeitraum sollen bis zum Jahr 2014 noch von über 70 verschiedenen Rechtsanwaltskanzleien Abmahnungen im Namen von insgesamt 465 Rechteinhabern ausgesprochen worden sein[132]; nach Angaben von AW3P werde mittlerweile jedoch der absolut überwiegende Teil der Abmahnungen von maximal ein bis zwei Kanzleien verschickt.[133] Ob sich an der Zahl der vertretenen Rechteinhaber etwas wesentliches geändert hat, ist nicht bekannt.

6. Zum typischen Inhalt von Abmahnungen

Inhaltlich werden die Abgabe einer Unterlassungsverpflichtungserklärung in Bezug auf das verletzte Werk sowie die Zahlung von Rechtsanwaltsgebühren für die Abmahnung sowie Schadensersatz verlangt. Da durch das Gesetz gegen unseriöse Geschäftspraktiken die Gebühren (für die Geltendmachung des Unterlassungsanspruches) auf EUR 124 gedeckelt wurden und Forderungen aus Abmahnungen vor seinem Inkrafttreten mittlerweile eingetrieben oder verjährt sind, sind Schätzungen zu den geltend gemachten Streitwerten, die dem Unterlassungsanspruch zu Grunde gelegt werden, mittlerweile uninteressant.[134] Nach einer Untersuchung der *vzvb* wird in der Mehrheit der Abmahnungen seit Inkrafttreten die Deckelung eingehalten und eine Berufung auf die Unbilligkeitsregel nach § 97a Abs.3 Satz 4 UrhG findet nicht statt.[135]

Dennoch beträgt die durchschnittlich geltend gemachte Summe der Rechts-

[132] *Tschmuck*, Musik-Filesharing: Das Abmahnwesen in Deutschland – Teil 2.

[133] AW3P-Statistik für 2017, https://www.abmahnwahn-dreipage.de/forum/viewtopic.php?f=17&t=15&start=11200 - Zugriff am 31.03.2021.

[134] Siehe hierzu auch Kapitel § 4 II. 2. c).

[135] *vzvb*, Untersuchung der urheberrechtlichen Regelungen des Gesetzes gegen unseriöse Geschäftspraktiken, S. 7.

anwaltsgebühren seit dem 9. Oktober 2013 EUR 364, da die Deckelung nur für die Gebühren in Bezug auf den Unterlassungsanspruch gilt. Zusätzlich hierzu werden Rechtsanwaltsgebühren für die Geltendmachung des Schadensersatzanspruches verlangt, der regelmäßig auf EUR 1000 veranschlagt wird; diese Summe bildet die Grundlage der Berechnung der Gebühren für den Schadensersatzanspruch. Im Ergebnis weicht die Gesamtsumme der Gebühren trotzdem erheblich nach unten von den vor dem 9. Oktober 2013 im Durchschnitt verlangten EUR 1051 ab.[136]

Am Gesamtergebnis hat sich allerdings für die Abgemahnten – jedenfalls im außergerichtlichen Verfahren – durch das Gesetz gegen unseriöse Geschäftspraktiken nicht viel geändert.[137] Zwar soll auch die im Durchschnitt geltend gemachte Schadenssumme von EUR 1076 auf EUR 867 gesunken sein[138]; dem wird jedoch von verschiedenen Quellen widersprochen. Diesen zu Folge soll der vor dem 9. Oktober 2013 durchschnittlich verlangte Schadensersatz von EUR 450 auf nunmehr EUR 700 gestiegen sein und sich damit am pauschalen Gesamt-Vergleichsangebot von jetzt EUR 915 statt vormals EUR 956 wenig geändert haben.[139] Letztere Schätzung erscheint plausibler, da nach der Untersuchung des *vzvb* die durchschnittliche außergerichtliche Vergleichssumme von EUR 757 auf EUR 872 gestiegen ist.[140] Dies wäre kaum vorstellbar, wenn vor der Gesetzesreform sowohl die verlangten Anwaltskosten als auch der geltend gemachte Schadensersatz deutlich höher gewesen wären als nach der Reform.

Zum gesamten Streitvolumen aller Abmahnungen zusammen genommen existieren für die Zeit nach 2014 keine Schätzungen, für den Zeitraum von 2009 bis 2014 beläuft es sich nach den Schätzungen der IGGDAW aber auf EUR 1,1 Milliarden.[141]

Dem Bericht eines Praktikers zu Folge sind die Abmahnungen bezüglich ih-

136 *vzvb*, Untersuchung der urheberrechtlichen Regelungen des Gesetzes gegen unseriöse Geschäftspraktiken, S. 11.

137 Siehe hierzu auch Kapitel § 4 X.

138 *vzvb*, Untersuchung der urheberrechtlichen Regelungen des Gesetzes gegen unseriöse Geschäftspraktiken, S. 12.

139 *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, S. 206.

140 *vzvb*, Untersuchung der urheberrechtlichen Regelungen des Gesetzes gegen unseriöse Geschäftspraktiken, S. 10.

141 *Tschmuck*, Musik-Filesharing: Das Abmahnwesen in Deutschland – Teil 2.

res übrigen Inhalts so verfasst, dass der Abgemahnte psychologisch einem möglichst starken Druck ausgesetzt wird. Typischerweise würde seitenlang aus Urteilen zitiert und somit eine bedrohliche Atmosphäre erzeugt; der Abgemahnte solle in den Glauben versetzt werden, sich in keinem Fall zur Wehr setzen zu können.[142] Dies kann der Verfasser aus eigener Erfahrung mit Abmahnungen nicht bestätigen. Möglicherweise waren ältere Abmahnungen aus der Anfangsphase der Abmahnwellen von damals aktiven Kanzleien so verfasst worden; die dem Verfasser ab 2011 zur Kenntnis gelangten Abmahnungen stammten jedenfalls von den heute noch bekannteren Kanzleien aus dem Markt und waren überwiegend sachlich und nicht aktiv irreführend verfasst. Dennoch verblieb auch in der sachlichen Fassung die Möglichkeit der Suggestion; zum Beispiel wurde, in einer dem Verfasser zur Kenntnis gelangten Abmahnung aus dem Jahr 2017, auf die Pflicht zur sekundären Darlegung über die Nutzungssituation des Anschlusses an Hand der Rechtsprechung bis „Tauschbörse III“ hingewiesen. Der Anschluss wurde jedoch familiär genutzt und daher wäre die für den Anschlussinhaber günstigere Entscheidung „Afterlife“ einschlägig gewesen. Es handelt sich hierbei nicht um eine Irreführung, da der Abmahnende nicht wissen kann, ob der betroffene Anschluss familiär genutzt wird; für den Abgemahnten kann diese Information jedoch den Unterschied machen, ob er sich Rechtsrat sucht und es auf eine Auseinandersetzung ankommen lässt oder ob er sofort bezahlt. Da die Abmahnungen mangels gegenteiliger Erkenntnisse nicht individualisiert werden, dürfte es sich bei diesem Beispiel nicht um einen Einzel-, sondern den Normalfall handeln.

Der Anreiz, ein Gerichtsverfahren zu vermeiden und gleich zu bezahlen, wird jedenfalls dadurch verstärkt, dass in den dem Verfasser bekannten Abmahnungen von vornherein Ratenzahlung angeboten, die Möglichkeit der Annahme des Vergleichsangebots auf wenige Wochen befristet und für den Fall eines gerichtlichen Verfahrens die Geltendmachung eines höheren Schadensersatzes angekündigt und umgekehrt bei einer sofortigen Zahlung eine Reduktion der Gesamtsumme angeboten wird. Dass ein solches Vorgehen den Abgemahnten psychologisch regelmäßig dazu bewegt, das Vergleichsangebot anzunehmen, ist empirisch bestätigt für den – dem *filesharing* einigermaßen vergleichbaren

[142] *Lorenz*, JurPC WebDok. 132/2014, Abs. 18ff.

Fall – der Abmahnungen wegen unberechtigter Nutzung von Bildern.[143]

7. Zur Menge an gerichtlichen Verfahren

Zur Zahl der gerichtlichen Verfahren existieren noch weniger Schätzungen als zur Zahl der Abmahnungen. Mangels staatlich geführter Dokumentationssysteme (wie PACER in den USA[144]), in denen sämtliche Verfahren erfasst werden, sagen die in Deutschland veröffentlichten Urteile zum *filesharing* nichts über die Gesamtzahl an Endurteilen aus. Zudem können gerichtliche Verfahren bereits im vorgelagerten Mahnverfahren oder zum Beispiel durch Prozessvergleich ohne ein Urteil beendet werden. Laut der IGGDAW-Statistik liegt die Quote der Abgemahnten, die zahlen, ohne es auf ein gerichtliches Verfahren ankommen zu lassen, bei ca. 40 Prozent.[145] Dies deckt sich ungefähr mit einer Praktikerbeobachtung, nach der knapp 50 Prozent der Abgemahnten einen vollen oder reduzierten Betrag bezahlen, ohne es auf ein gerichtliches Verfahren ankommen zu lassen.[146] Letzterer zu Folge soll die Klagequote im Falle der Nichtzahlung im Beobachtungszeitraum von 2009 bis 2013 nur bei knapp 3 Prozent gelegen haben, die Zahl der Mahnbescheide (auf die jedoch kein reguläres Gerichtsverfahren folgte) bei nur knapp 3,5 Prozent.[147]

Ob dies für den Zeitraum nach 2013 auch noch gilt, ist zweifelhaft. Die geringe Klagequote bis 2013 könnte dem Umstand geschuldet sein, dass in diesem Zeitraum noch eine sehr hohe Zahl an Kanzleien am Markt tätig war[148], die unter Umständen eher klageavers waren. In einem Interview mit AW3P äußerte ein Anwalt der gegenwärtig aktivsten Abmahn-Kanzlei, dass im Falle der Nichtzahlung auf eine Abmahnung ernsthaft mit einer Klage gerechnet werden müsse.[149] Dies entspricht auch der eigenen Erfahrung des Verfassers, nach der bei jeder Abmahnung, auf die nicht freiwillig gezahlt wurde, ein Mahnbescheid erging und nach Widerspruch das reguläre Gerichtsverfahren eingeleitet wurde. Jedoch wurden diese Fälle erstinstanzlich durch Vergleich beendet. Folglich kann zwar davon ausgegangen werden, dass gegenwärtig

143 Vgl. *Luo/Mortimer*, Journal of Economics & Management Strategy, Nr. 2, Bd. 26, 2017, 525f.
144 https://en.wikipedia.org/wiki/PACER_(law) - Zugriff am 31.03.2021.
145 BT-Drs. 17/13057, S. 10.
146 *Lorenz*, JurPC WebDok. 132/2014, Abs. 2.
147 *Lorenz*, JurPC WebDok. 132/2014, Abs. 2.
148 Siehe Kapitel § 3 V. 5.
149 https://aw3p.de/archive/3597 - Zugriff am 31.03.2021.

das Unterlassen der Zahlung auf eine Abmahnung in den meisten Fällen zu einem Mahn- oder Klageverfahren führt, nicht aber, dass dieses auch immer durch ein Endurteil beendet wird.

Über die Zahl der tatsächlich ergangenen Endurteile in *filesharing*-Fällen kann daher im Ergebnis nur spekuliert werden. Nach der Statistik von AW3P sind für das Jahr 2017 insgesamt 102 veröffentlichte Endurteile aus der Instanzrechtsprechung bekannt.[150] Laut dem bereits erwähnten Interview veröffentlicht die aktivste Abmahn-Kanzlei nur einen geringen Teil der von ihr erstrittenen Entscheidungen.[151] Soweit ersichtlich, veröffentlichen auch Gerichte und Verteidiger nur gelegentlich Entscheidungen aus ihrer Praxis. Es erscheint daher zumindest nicht unplausibel, für die Zeit ab dem Jahr 2006[152] insgesamt mehrere tausend ergangene Endurteile anzunehmen.

VI. Hintergründe zum Vorgehen gegen *filesharing*-Endnutzer

In den vorgehenden Kapiteln wurde festgestellt, dass *filesharing* in großem Umfang betrieben wurde und wird, die Urheberrechtsindustrie erheblichen Einfluss auf das Recht ausübt, um rechtliche Mittel dagegen zu schaffen oder auszubauen, die Endnutzer von *filesharing* im Vergleich zu anderen Akteuren im Bereich der Online-„Piraterie“ ein leicht greifbares Ziel sind und sich dementsprechend häufig Rechtsverfolgungsmaßnahmen ausgesetzt sehen.

Auch in Anbetracht der Machtdisparität zwischen Industrie und Endnutzern scheinen die Massenabmahnungen gegen Letztere daher auf den ersten Blick keine Besonderheit im Vergleich zu Abmahnungen in anderen Bereichen, sondern lediglich der Häufigkeit der Verletzungshandlungen geschuldet zu sein. Abmahnungen auf dem Gebiet des gewerblichen Rechtsschutzes dienen in der Konzeption des deutschen Rechts dazu, eine erkannte Rechtsverletzung außergerichtlich zu unterbinden und für die Zukunft zu verhindern; diese Funktion ist im Grundsatz dadurch abgesichert, dass Abmahnungen,

[150] https://www.abmahnwahn-dreipage.de/forum/viewtopic.php?f=17&t=15&start=11200 - Zugriff am 31.03.2021.

[151] https://aw3p.de/archive/3597 - Zugriff am 31.03.2021.

[152] Also ab dem Jahr, in dem erste zivilgerichtliche Urteile zum *filesharing* ergangen waren, siehe Kapitel § 2 II.

die unter sachfremden Erwägungen ausgesprochen werden, als rechtsmissbräuchlich angesehen werden können, was insbesondere zur Folge hat, dass für solche Abmahnungen kein Ersatz der Rechtsanwaltskosten verlangt werden kann.[153]

In der Gesetzesbegründung zum Gesetz gegen unseriöse Geschäftspraktiken wurde als Problem bei Massenabmahnungen angeführt, dass der gegenüber den Abgemahnten geltend gemachte Betrag betreffend die Gebühren nicht in derselben Höhe gegenüber dem Auftraggeber geltend gemacht werde[154]; mithin werde also gegenüber dem Auftraggeber pro Abmahnung eine Gebühr unterhalb der gesetzlichen Gebühren verlangt (was gebührenrechtlich gemäß § 4 Abs.1 RVG noch unproblematisch ist), gegenüber dem Abgemahnten aber die vollen gesetzlichen Gebühren, mithin also ein Betrag, der tatsächlich gar nicht angefallen ist. Das legt den Verdacht nahe, dass solche Abmahnungen nicht zum Zweck der Rechtsverfolgung, sondern zur Gewinnerzielung ausgesprochen wurden. Diese Problemanalyse geht jedoch fehl: nach der hierzu vorhandenen Literatur erfüllt eine solche Praxis den Tatbestand des (gewerbsmäßigen) Betrugs nach §§ 263 Abs.1, Abs.3 Nr.1 StGB.[155] Gegen eine ohnehin schon illegalen Praxis ist gesetzgeberische Aktivität, die nicht darauf abzielt, diese Praxis leichter aufzudecken, verfehlt.[156] Ob es sich hierbei überhaupt um eine weit verbreitete Praxis handelt, kann nicht mit Sicherheit

[153] BGH, Urteil vom 17. Januar 2002, Az. I ZR 241/99 – GRUR 2002, 357 - „Mißbräuchliche Mehrfachabmahnung".

[154] BT-Drs. 17/13057, S. 11.

[155] *Bülte*, NZWiSt 2014, 41, 46, 49. Mittlerweile hat der 1. Strafsenat des BGH in einer ähnlich gelagerten Konstellation im UWG entschieden. Leider geht aus der Entscheidung nicht eindeutig hervor, ob es der BGH – wie die Vorinstanz – ausreichen lassen möchte, dass der Auftraggeber mit dem abmahnenden Anwalt vereinbart, dass die vom Abgemahnten verlangte Summe von Seiten des Auftraggebers dem Anwalt (jedenfalls teilweise) tatsächlich nicht geschuldet ist, oder ob zusätzlich die Rechtsmissbräuchlichkeit der Abmahnung im Sinne von § 8 Abs.4 UWG erforderlich ist, vgl. BGH, Beschluss vom 8. Februar 2017, 1 StR 483/16, Rz. 13 – MMR 2019, 42 - „Gebührengenerierung". Wäre Letzteres der Fall, so dürfte in analogen *filesharing*-Konstellationen Strafbarkeit nicht gegeben sein, da dort Rechtsmissbräuchlichkeit nach § 242 BGB nicht angenommen werden kann, siehe Kapitel § 4 XI. Dogmatisch betrachtet liegt jedoch erstere Lesart näher, da für eine Täuschung im Sinne des § 263 StGB bereits genügt, dass die Existenz einer tatsächlich nicht bestehenden Forderung behauptet wird.

[156] Verfehlt ist also das Gesetz gegen unseriöse Geschäftspraktiken, siehe hierzu Kapitel § 4 X.

gesagt werden; es sind lediglich einzelne Fälle bekannt.[157]

Was hingegen mit Sicherheit gesagt werden kann, ist, dass mit jeder Abmahnung zugleich ein Schadensersatz von regelmäßig mehreren hundert Euro geltend gemacht wird und Gegenstand der Abmahnungen typischerweise Musikalben, Filme und Videospiele sind, deren Preis im Handel im niedrigen bis mittleren zweistelligen Bereich liegt.[158] Auch wenn nach Auffassung des BGH hier nach juristischen Betrachtung keine Überkompensation vorliegt: in wirtschaftlicher Betrachtung liegt – zumindest bei BitTorrent und allen Systemen mit einer vergleichbaren mehrseitigen Datenübertragung – in jedem Fall eine wirtschaftliche Überkompensation vor, da von einer einzelnen Person der mehrfache Betrag dessen erlangt werden kann, was sie für das legale Erlangen des betroffenen Werkes hätte bezahlen müssen.[159]

Da bei BitTorrent grundsätzlich *jeder* Benutzer erfolgreich auf Schadensersatz verklagt werden kann, ist der über den Schadensersatz erlangte Betrag also auch immer höher als der Betrag, den die betroffenen Personen hätten aufwenden müssen, um das betreffende Werk käuflich zu erwerben[160].

In einem an die Öffentlichkeit geleaktem Vortrag aus dem Jahr 2009, der von einer Firma, deren Geschäftszweck die Rechtsverfolgung von Rechtsverletzungen in *filesharing*-Netzwerken war, zu Werbezwecken erstellt worden war, wurde denn auch ausdrücklich beworben, dass sich mit einem Verletzer dasselbe verdienen lässt wie mit 150 legalen Verkäufen.[161] Der Wortlaut des Vortrags spricht spezifisch von „Ertrag“ und „Erwirtschaften“.

Berechtigterweise ließe sich jedoch hierauf einwenden, dass es sich hier um

[157] In einem Fall war eine entsprechende Pauschalvereinbarung im Internet geleaked worden, siehe http://nebelhorn-piratenradio.de/2013/12/12/gate/ - Zugriff am 31.03.2021. In einem anderen Fall wurde eine solche Pauschalvereinbarung durch ein Gerichtsverfahren bekannt, in dem ein Rechteinhaber rückständige Forderungen gegen eine Abmahnkanzlei aus dieser Vereinbarung geltend machte, siehe *Knies*, BaumgartenBrandt interne Gebührenabrede bei Abmahnungen. Ähnliche Konstellation auch bei LG Hamburg, Urteil vom 29. November 2017, Az. 308 O 236/15, Rz. 61f. – BeckRS 2017, 144177.

[158] Siehe Kapitel § 3 V. und VI.

[159] Siehe zu der juristischen Fragestellung Kapitel § 4 IX. 2. b).

[160] Ganz davon abgesehen, dass die Gewinnmarge nicht dem Kaufpreis entspricht.

[161] https://wikileaks.org/wiki/DigiRights_Solutions_Praesentation_zur_Gewinnverbesserung_durch_Abmahnungverfahren,_02_February_2009 - Zugriff am 31.03.2021. Siehe dort die Folien 26 und 27

ein „schwarzes Schaf“ handeln könnte und der Rest der Branche diese Überkompensation zwar hinnimmt, jedoch primär die Unterbindung der Rechtsverletzung anstrebt.

Das lässt sich nicht direkt widerlegen. Es lässt sich jedoch plausibel aufzeigen, dass die Unterbindung der Rechtsverletzung kaum eine taugliche Motivation für *filesharing*-Abmahnungen sein kann und somit nur die Motivation der Gewinnerzielung übrig bleibt:

- Die meisten Fälle der Urheberrechtsverletzung durch *filesharing* finden über Internetanschlüsse in privaten Haushalten statt[162], also in Familien und vereinzelt in Wohngemeinschaften. Die allermeisten privaten Haushalte bestehen in Deutschland nur aus wenigen Personen.[163] Der Pool aus Personen, die für eine Wiederholung der Rechtsverletzung (für die ja der Anschlussinhaber zumindest als Störer bzw. nunmehr mit dem Sperranspruch haftet) ist also regelmäßig relativ klein.[164] Da Musik, Filme und Videospiele nach ihrem Erscheinen mit der Zeit immer weniger nachgefragt werden, ist die Wahrscheinlichkeit dementsprechend gering, dass über ein und denselben Internetanschluss ein Werk mehr als einmal verletzt wird. Folglich sind auch nur vereinzelte Fälle bekannt, in denen gegen eine Unterlassungspflicht verstoßen wurde.[165] Bezeichnend ist in diesem Zusammenhang auch, dass Rechteinhaber extra das Recht erstritten hatten, den Ersatz der Abmahnkosten im Klagewege verlangen zu können, ohne den Unterlassungsanspruch gerichtlich geltend machen zu müssen[166] und zudem in empirischer Hinsicht praktisch nie eine einstweilige Verfügung beantragt oder im Hauptsacheverfahren der Unterlassungsanspruch geltend gemacht wird, wenn die Unterzeichnung der Unterlassungsverpflichtungserklä-

[162] Zwar gibt es hierzu keine Statistik, dem Verfasser sind aber im Rahmen der Recherchen für diese Arbeit im Vergleich nur wenige Fälle und Gerichtsentscheidungen bekannt geworden, in denen ein gewerblicher Anschluss benutzt wurde.

[163] *Bundesamt*, Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien, S. 9.

[164] Bei einem gewerblichen Anschluss wie bei einem Restaurant und Hotel wäre er naturgemäß viel größer.

[165] Siehe Kapitel § 2 VII. 1.

[166] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 61f. – GRUR 2016, 191 - „Tauschbörse III“.

rung nicht erfolgt ist.[167]

- Nicht nur die Nachfrage schrumpft mit Zeitablauf, sondern auch das Angebot. Es ist durch Untersuchungen gesichert, dass BitTorrent-Schwärme meist schon nach wenigen Tagen stark schrumpfen und innerhalb eines Jahres fast oder ganz verschwinden.[168]

- Nicht argumentiert werden kann, dass der Schadensersatz auch eine abschreckende Wirkung hat, mithin ein pönales Element aufweise, das zukünftigen Rechtsverletzungen ähnlich wie ein Unterlassungsanspruch vorbeugen soll. Zwar mögen die im *filesharing* üblichen Schadensersatzbeträge *de facto* eine abschreckende Wirkung haben, eine vom deutschen Recht gebilligte Funktion ist dies jedoch nicht.[169] Eine legitime Berufung auf diese Wirkung scheidet mithin aus.

Bei realistischer Betrachtung dienen Massenabmahnungen auf dem Gebiet des *filesharing* also nicht dem Ziel bzw. können praktisch nicht dem Ziel dienen, eine Rechtsverletzung (für die Zukunft) zu unterbinden. Mithin erfolgen sie mit der – *einzig möglich verbleibenden* – Intention, Profit zu erzielen.[170] Für Rechtsanwälte stellt der Versand von Massenabmahnungen dieser Art gegenüber sonstigen Abmahnungen auf dem Gebiet des gewerblichen Rechtsschutzes und des Urheber- und Medienrechts folglich ein Geschäftsmodell *sui generis* dar.[171]

Wie in Kapitel § 4 XI. gezeigt wird, ist dies jedoch nicht geeignet, die Abmah-

[167] Was bei immerhin knapp 15 Prozent der Klageverfahren und knapp 35 Prozent aller Abmahnungen laut Praktikerbeobachtung der Fall war, siehe *Lorenz*, JurPC Web-Dok. 132/2014, Abs. 2, 25

[168] *Zhang* et al., IEEE Transactions on Parallel and Distributed Systems, Nr. 7, Bd. 22, 2011, S. 1164, 1173; *Buford/ Yu/ Lua*, P2P networking and applications, S. 146.

[169] So irrtümlich BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 63 – GRUR 2016, 191 - „Tauschbörse III“; siehe zu Fragen des Schadensersatzes Kapitel § 4 IX. 2. a).

[170] Soweit Analysen zu dieser Frage wie *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 464ff. zu anderen Ergebnissen kommen, gehen sie also fehl, weil sie die Relevanz des Unterlassungsanspruches und die Relevanz des Schadens übersehen. Unzutreffend ist – aus den genannten Gründen – weiterhin auch die Behauptung einer bloßen Kompensationsfunktion bei *Nümann/ Mayer*, ZUM 2010, 321, 328.

[171] Ein Partner der bekanntesten Rechtsanwaltskanzlei, die auf diesem Gebiet tätig ist, bezeichnet seine Tätigkeit selbst als „Geschäftsmodell“, siehe *Bäuerlein*, Sie mahnen ab. Sie kassieren. Wer sind Waldorf Frommer?

nungen als rechtsmissbräuchlich einzustufen, weshalb auch im Ergebnis die Rechtsprechung des BGH in diesem Punkt[172] dogmatisch Bestand hat. Es handelt sich mithin um eine durch die bisherige, faktisch bestehende Rechtslage gebilligte und ermöglichte Praxis.

Ob Massenabmahnungen auch in Zukunft unter Anwendung der Entscheidung „Konferenz der Tiere“[173] diesen beabsichtigen Zweck erfüllen können, steht noch offen.[174]

VII. Rechtliche Säulen des Vorgehens gegen *filesharing*-Endnutzer

Die in Kapitel § 3 V. dargestellten Mengen an Abmahnungen würden nicht ausgesprochen werden, wenn das gerichtliche Vorgehen im Falle der Zahlungsverweigerung keine sehr hohe Erfolgsquote hätte. Dass eine solch hohe Erfolgsquote besteht, gewährleistet die seit dem Jahr 2010 ergangene Rechtsprechung[175]:

- ISPs müssen bei Vorlage einer ermittelten IP-Adresse praktisch immer Auskunft über Name und Anschrift des Inhabers des entsprechen Anschlusses erteilen, ohne das weitere Voraussetzungen an die Auskunft geknüpft sind, insbesondere also Massenabfragen ohne Hindernisse möglich sind. Die Auskünfte sind im Prozess beweisrechtlich in den allermeisten Fällen verwertbar.
- Die ISPs speichern die Zuordnung der IP-Adresse zum jeweiligen Anschluss freiwillig, müssen diese aber jedenfalls auf Zuruf bis zum Abschluss des Auskunftsverfahren speichern.
- Auf Grund der hohen Anforderungen an die sekundäre Darlegungslast können Anschlussinhaber ihre Täterschaft nur schwerlich ausräumen.
- Durch die von der Rechtsprechung gebilligte Berechnung des lizenzanalogen Schadens wurde ein starker finanzieller Anreiz geschaffen, auch massenhaft gegen Anschlussinhaber vorzugehen.

[172] Siehe Kapitel § 2 VI. 2.
[173] Siehe Kapitel § 2 XI. 5.
[174] Siehe hierzu Kapitel § 4 II. 4. b) ff), § 4 IX. 3. und § 5 VII.
[175] Vgl. jeweils Kapitel § 2 XII. 2.

Diese Aufzählung zeigt auch, dass die aufgezählten Punkte für ein lohnenswertes, massenhaftes Vorgehen gegen *filesharing*-Endnutzer ausreichend sind. Insbesondere ist die Störerhaftung und entsprechend auch ein Sperranspruch wie § 7 Abs.4 TMG irrelevant, da von einem Störer kein Schadensersatz verlangt werden kann; sie taugt allenfalls als zusätzliches Druckmittel, um einen Anschlussinhaber von einer gerichtlichen Klärung seiner Haftung abzubringen und stattdessen vorgerichtlich einen Vergleich zu schließen.[176] Entsprechend sind dem Verfasser bis zum Stand der Bearbeitung (März 2021) auch keine Entscheidungen bekannt geworden, in denen ein Anschlussinhaber auf Grundlage von § 7 Abs.4 TMG verurteilt worden war; auch Verurteilungen auf Grundlage der Störerhaftung (vor Einführung des § 7 Abs.4 TMG) hatte es so gut wie keine gegeben.

Mithin sind auch die Reformen des TMG wirkungslos, da sie an den genannten Säulen nicht rütteln. Sie zielten bzw. zielen nur auf die Abschaffung bzw. Modifizierung der Haftung bei bloßer Vermittlungstätigkeit ab[177], ändern jedoch – nach Auffassung des Verfassers – nichts an der zivilprozessual fingierten täterschaftlichen Haftung.[178]

VIII. Rechtspolitische Kritikpunkte am Vorgehen gegen *filesharing*-Endnutzer

Das Vorgehen gegen *filesharing*-Endnutzer erscheint daher auf Basis des Vorgesagten aus rechtspolitischer Perspektive kritikwürdig:

- Anstatt Rechtsverletzungen abzuhelfen und diese zu kompensieren, wird aus Rechtsverletzungen eine eigene Profitquelle geschaffen.
- Von Abmahnungen Betroffenen fehlt die kollektive Repräsentation. Während im UWG bestimmte qualifizierte Einrichtungen (§ 8 Abs.3 Nr.3 UWG) und im Datenschutzrecht der Datenschutzbeauftragte Verbraucherrechte wahrnehmen können, sind im Urheberrecht die Anschlussinhaber auf sich allein gestellt. Private Initiativen[179] können dies nicht kompensieren, insbesondere können diese nicht stellvertretend

[176] Siehe auch Kapitel § 4 II. 2. c).
[177] Siehe Kapitel § 5 VI.
[178] Siehe Kapitel § 4 VIII. 4. b).
[179] Siehe hierzu Kapitel § 3 V.

ein „Musterverfahren“ betreiben, in dem beispielsweise grundsätzliche Rechtsfragen *kompetent* erörtert werden und der Rechtsweg vollständig erschöpft wird. Den Rechteinhabern ist dies jedoch ohne weiteres möglich, wie die Vielzahl an Entscheidungen des BGH und EuGH zum *filesharing* aufzeigen.[180] Den Rechteinhabern ist es daher faktisch leichter möglich, die Rechtslage zu ihren Gunsten zu formen, als es den Abgemahnten möglich ist. Umgekehrt können sie eine Formung zu ihren Ungunsten durch Klagerücknahme abwehren.

- Das Machtungleichgewicht zwischen Rechte- und Anschlussinhabern äußert sich nicht nur in den ungleichen Möglichkeiten der Formung der Rechtslage, sondern im bestehenden gesetzlichen Kontext auch im Rechtsdurchsetzungswillen und den finanziellen Möglichkeiten der Rechtsdurchsetzung.[181] Abgemahnte werden somit faktisch davon abgehalten, Rechtsschutz vor Gericht zu suchen. Für die Urheberrechtsindustrie sind einzelne verlorene Verfahren irrelevant, für den einzelnen Abgemahnten ist ein verlorenes Verfahren wirtschaftlich desaströs. Im Jahr 2014 betrug der monatliche Bruttomedianlohn in Deutschland knapp EUR 3000[182], der Nettomedianlohn damit durchschnittlich etwas über EUR 2000. Dem gegenüber steht die Überlegung, entweder – von den Durchschnittswerten ausgehend[183] – sofort EUR 915 zu zahlen oder sich stattdessen auf Vergleichsverhandlungen einzulassen und diese Summe etwas zu reduzieren, oder sich auf ein Gerichtsverfahren einzulassen. Im Falle der Niederlage im Gerichtsverfahren kommen dann zu den EUR 915 (sofern der Rechteinhaber im Verfahren nicht sogar einen höheren Betrag geltend macht) Gerichts-und Rechtsanwaltsgebühren sowie anteilige Kosten des Auskunftsverfahrens hinzu, also geschätzt Kosten im Bereich von EUR 700. Zudem muss der Abgemahnte im Falle des Obsiegens mit einer Berufung und ggf. auch einer Revision rechnen, also nochmals jeweils ca. EUR 800

[180] Dass die großen Abmahnkanzleien bewusst „Musterverfahren“ führen, also strategische Prozessführung betreiben, räumen diese selbst ein, siehe *Bäuerlein*, Sie mahnen ab. Sie kassieren. Wer sind Waldorf Frommer? Zu den ungleichen Möglichkeiten der Rechtsdurchsetzung zwischen starken und schwachen Parteien siehe *Bender*, RabelsZ 1976, 718, 719f.

[181] So auch *Haedicke*, Patente und Piraten, S. 21f.

[182] https://bit.ly/2DMkwjH - Zugriff am 31.03.2021.

[183] Siehe Kapitel § 3 V. und 6.

bzw. EUR 1000. Da Rechteinhaber typischerweise im Falle ihres Unterliegens immer Rechtsmittel ergreifen, muss der Abgemahnte dieses Kostenrisiko einkalkulieren. Vor dem BGH ist typischerweise mit einer Niederlage zu rechnen; nur in Fragen der Störerhaftung („Silver Linings Playbook", „WLAN-Schlüssel") und der sekundären Darlegungslast („Afterlife" und „Ego-Shooter-Spiel") konnten Abgemahnte *gelegentlich* einen Sieg erringen. Prozesskostenhilfe kann der durchschnittliche Abgemahnte nicht in Anspruch nehmen, Rechtsschutzversicherungen decken *filesharing* meist nicht oder nur unter sehr eingeschränkten Bedingungen ab.[184] Dies alles weiß der Abgemahnte ohnehin erst, wenn er erstmalig eine Rechtsberatung in Anspruch genommen hat, für die wiederum Kosten anfallen. Bis dahin liegt ihm nur die Abmahnung vor, die zwar keine falsche Rechtsausführungen enthalten darf, aber auch bestimmte, für den Abgemahnten unter Umständen günstige Rechtsprechung nicht erwähnen muss. Der Abgemahnte gewinnt aus der Abmahnung also den Eindruck, dass er ohnehin verlieren wird.[185] Hinzu kommt, dass die gesetzte Frist von regelmäßig wenigen Wochen zusätzlichen Druck erzeugt; für eine Privatperson, die regelmäßig wenig Zeit für die Erledigung von außerplanmäßigen Rechtstreitigkeiten zur Verfügung hat, ist eine solche Frist faktisch deutlich schwieriger einzuhalten als für ein Unternehmen. Aus der empirischen Forschung zu dem (mit dem *filesharing* einigermaßen vergleichbaren) Gebiet der Abmahnungen wegen Verletzung von Bildrechten ist – wie bereits erwähnt – bekannt, dass das Angebot von (gegenüber der ursprünglich geforderten Summe) leicht gesenkten Vergleichssummen sowie die Setzung einer Frist, die Vergleichsbereitschaft des Abgemahnten gegenüber fehlenden Fristen und Festbeträgen erheblich erhöht.[186] Nimmt man also alle soeben genannten Faktoren zusammen, unterliegt der Abgemahnte einem erheblichen *psychologischen Druck* dahingehend, gar nicht erst Rechtsschutz nachzusuchen, sondern gleich zu bezahlen.

- Das Machtungleichgewicht zwischen Rechteinhabern und Abgemahnten zeigt sich auch in den Möglichkeiten der Tatsachenaufklärung tech-

[184] *Kern*, Welche Versicherung schützt vor Online-Abmahnung?
[185] *Ory*, FS Wandtke 2013, 475, 480.
[186] *Luo/Mortimer*, Journal of Economics & Management Strategy, Nr. 2, Bd. 26, 2017, S. 499, 525f.

nische Fragen betreffend. Für Abgemahnte ist es finanziell regelmäßig zu riskant, bisher ungeprüfte technische Fragen durch einen Sachverständigen beantworten zu lassen oder vermeintlich bereits geklärte technische Fragen (wie beispielsweise die Funktionsweise von BitTorrent) neu aufzuwerfen[187], da sie im Falle des Unterliegens für die Kosten des Sachverständigen aufkommen müssten.

- Das 3. TMGÄndG verstärkt diesen Effekt enorm, da dieses zahlreiche neue technische Fragen aufwirft.[188] Mithin kann es für einen Abgemahnten einen geringeren Aufwand bedeuten, einen Vergleich zu schließen, als etwaige, nach diesem Gesetz erlassene Sperranordnungen technisch umzusetzen. Abgemahnte werden – mit diesem Umstand konfrontiert – aller Voraussicht nach noch eher zu einem Vergleich bereit sein als nach der alten Rechtslage. Hinzu kommt, dass – anders als bei der Störerhaftung – den Anschlussinhaber der Sperranspruch in jedem Fall treffen kann, wenn er nicht als Täter haftet. Folglich verstärkt die Aussicht, in der einen oder anderen Form unausweichlich in Anspruch genommen zu werden, den Druck dahingehend, sofort einen Vergleich zu schließen.

- Über die genannten technischen Sachfragen wissen die damit befassten Gerichte naturgemäß nicht Bescheid. Entsprechend lässt sich deren Unkenntnis ausnutzen.[189] Soweit Abmahnkanzleien demgegenüber darauf verweisen, dass sich die Gerichte mittlerweile die erforderliche Expertise erarbeitet hätten[190], so handelt es sich dabei um eine einseitig geformte Sichtweise auf die technischen Fragen. Und nicht nur auf technischer Seite, sondern auch auf rechtlicher Seite ist es insbesondere für Amtsrichter auf Grund fehlender Spezialisierungsmöglichkeiten und häufiger Abteilungswechsel trotz der Konzentrationsermächtigung nach § 105 UrhG schwierig, Expertise auf dem Gebiet des *filesharing*

[187] Die Kosten für einen Sachverständigen in *filesharing*-Verfahren belaufen sich regelmäßig auf EUR 3000 bis 15.000, so jedenfalls nach Auskunft eines Anwalts der bekanntesten Abmahnkanzlei, siehe https://aw3p.de/archive/3597 - Zugriff am 31.03.2021.

[188] Siehe Kapitel § 4 VIII.

[189] So ausdrücklich AG Stuttgart Bad-Canstatt, Urteil vom 13. August 2015, Az. 8 C 1023/15, Rz. 48 – juris; so auch *Hunter*, 31 J. Marshall J. Info. Tech. & Privacy L. 105, 124 (2014).

[190] https://aw3p.de/archive/3281 – Zugriff am 31.03.2021.

aufzubauen.[191] Auch hier besteht also das Potential, dass diese fehlende Expertise ausgenutzt wird.

- Die technischen Schwierigkeiten des Sachverhalts und die schiere Menge an Fallzahlen nötigen Gerichte dazu, *filesharing*-Verfahren möglichst effizient abzuwickeln, um den ohnehin auch unabhängig hiervon existierenden Erledigungsdruck[192] zu mindern. Dies geht zu Lasten desjenigen, der den geringen Widerstand leistet bzw. leisten kann, also ganz regelmäßig der Abgemahnte.

- Massenabmahnungen muten wie eine Funktionsverschiebung des Zivilrechts an, da trotz des Umstandes, dass es sich der Zahl nach um *Massen*abmahnungen handelt, letztlich nur ein geringer Teil von *filesharing*-Nutzern belangt wird[193], diese aber – zumindest der öffentlichen Wahrnehmung nach – besonders heftig. Dem äußeren Eindruck (nicht aber der inneren Zielsetzung[194]) nach findet also eine generalpräventive „Erziehungsmaßnahme“ statt, die eigentlich dem Strafrecht vorbehalten ist, hier aber zivilrechtlich durchgeführt wird.

- Die im Rahmen der sekundären Darlegungslast zu leistende Sachaufklärung kann persönliche Verhältnisse, insbesondere – im Falle eines familiär geteilten Anschlusses – das Familienleben, schwer belasten.

- Auch wenn die Massenabmahnungen an sich völlig legal sind, verleiten sie in Einzelfällen dennoch zu berufsrechtswidrigem und strafbaren Verhalten.[195]

- Vereinzelt wird von der Literatur angemerkt, Massenabmahnungen schaden der Akzeptanz des Urheberrechts.[196] Dies kann – jedenfalls für Deutschland – empirisch jedoch nicht bestätigt werden. So zeigt eine groß angelegte Studie des *EUIPO* aus dem Jahr 2017 (mit dem Erhebungszeitraum 2016) im Vergleich zu einer sehr ähnlichen, im Jahr 2013 durchgeführten Studie, dass die Akzeptanz urheberrechtsverlet-

[191] Vgl. *Windau*, Justizminister wollen „Zivilprozess durch Reformen stärken“.
[192] Vgl. hierzu *Windau*, Der Glaube an die Justizstatistik als Quelle der Erkenntnis.
[193] Siehe Kapitel § 3 II. und V.
[194] Siehe Kapitel § 3 VI.
[195] Wie der Geltendmachung überhöhter Rechtsanwaltsgebühren, siehe Kapitel § 3 VI.
[196] *Ory*, FS Wandtke 2013, 475, 482; mit Verweis auf (mittlerweile) ältere empirische Studien die USA betreffend *Frey*, ZUM 2014, 554, 556f.

zenden Verhaltens in Deutschland tendenziell gesunken ist: Zwar hat sich die Zahl derjenigen Befragten, die angaben, urheberrechtsverletzendes Material heruntergeladen zu haben, von 4 Prozent im Jahr 2013 auf 7 Prozent im Jahr 2016 erhöht[197]; dies könnte jedoch dadurch erklärbar sein, dass sich die Zahl der Befragten, die eine Urheberrechtsverletzung akzeptabel finden, wenn es keine schnell verfügbare legale Quelle gibt, von 11 Prozent auf 22 Prozent verdoppelt hat. Jedenfalls ist die Zahl der Befragten, die eine Urheberrechtsverletzung mit der Begründung akzeptabel finden, dass sie dem persönlichen Gebrauch diene, von 37 Prozent auf 28 Prozent gesunken[198]; in der Folgeuntersuchung des *EUIPO* von 2020 war dieser Wert noch einmal erheblich gesunken, nämlich von 28 auf 17 Prozent, wobei die anderen beiden in Bezug genommenen Werte praktisch stabil geblieben waren.[199] Dass Massenabmahnungen der Akzeptanz des Urheberrechts im Kontext illegaler Downloads schaden, ist tatsächlich also *kein* valider rechtspolitischer Kritikpunkt.

IX. Rechtfertigung des Vorgehens gegen *filesharing*-Endnutzer?

Gibt es auch einen positiven rechtspolitischen Aspekt des Vorgehens gegen *filesharing*-Endnutzer bzw. Anschlussinhaber, der die rechtspolitischen Kritikpunkte (zumindest teilweise) aufwiegen kann? Das wäre möglicherweise der Fall, wenn *filesharing* für die Urheberrechtsindustrie ökonomisch schädlich ist und es durch das rechtliche Vorgehen dagegen zurückgeht.

---

197 Was zunächst eine Verringerung des Respekts vor dem Urheberrecht nahelegen könnte.

198 *EUIPO*, European Citizens and Intellectual Property: Perception, Awareness and Behaviour 2017, S. 136.

199 *EUIPO*, European Citizens and Intellectual Property: Perception, Awareness and Behaviour 2020, S. 39, 41; die genannte Lesart dieser Umfragen betrachtet natürlich den Bevölkerungsquerschnitt. Ob bei der Gruppe von Personen, die eine Abmahnung wegen *filesharing* erhalten haben, sich etwas an der Akzeptanz des Urheberrechts geändert hat, kann freilich nicht beurteilt werden, wobei ohnehin zu fragen wäre, warum man auf diese Gruppe abstellen sollte (auch wenn natürlich viele der Abgemahnten für die abgemahnte *filesharing*-Aktivität nicht verantwortlich waren).

1. Ökonomische Folgen des *filesharing*

A priori sind sowohl negative als auch positive Folgen denkbar.

Die offensichtliche negative Folge ist der Substitutionseffekt, d.h. ein über ein *filesharing*-System bezogenes Werk wäre legal erworben worden, wenn es nicht illegal hätte bezogen werden können.[200] Die Schwierigkeit besteht darin, auseinanderzuhalten, welche *filesharing*-Nutzer sogenannte *low reservation value consumer* und welche sogenannte *high reservation value consumer* sind: Erstere hätten zum Beispiel aus finanziellen Gründen ein Werk auch dann nicht legal erworben, wenn sie es hätten legal erwerben können; Letztere sind eher dazu geneigt, ein Werk legal statt illegal zu erwerben, wobei dies auch davon abhängt, ob das auf illegalem Wege beschaffte Werke einem legal beschafften Werk gleich kommt (Substitutionsgrad) und wie hoch die Kosten bzw. der Aufwand für den illegalen Erwerb sind.[201]

Denkbare positive Folgen sind Preiseffekte, Sampling-Effekte und Netzeffekte: der Preiseffekt meint, dass die durch *filesharing* substituierten Käufe an anderer Stelle (mehr als) ausgeglichen werden können, zum Beispiel wenn Musiknutzer weniger Geld für Musikkäufe, aber dafür mehr für Live-Konzerte ausgeben oder zwar zunächst weniger Musik kaufen, aber auf Grund der illegal erworbenen Werke „Fans“ der betroffenen Künstler werden und später mehr Musik legal erwerben; der Sampling-Effekt meint, dass eine Substitution nicht stattfinden muss, sondern im Gegenteil Nutzer ein Werk nur legal erwerben, weil sie es zuvor durch den illegalen Erwerb testen konnten; der Netzeffekt zuletzt schließt an den Sampling-Effekt an, d.h. ein Werk kann unter Umständen erst durch seine illegale Verbreitung eine Bekanntheit erlangen, die zu einer Steigerung der legalen Verkäufe führt.[202] Schwieriger einzuordnen ist das *Unbundling*, d.h. Werke, die früher nur in Kombination veräußert wurden, können nunmehr einzeln erworben werden, beispielsweise einzelne Songtitel statt Musikalben, weil Nutzer es gewohnt sind, einzelne Songs illegal erlangen zu können und daher auf den Kauf des ganzen Albums, das unter Umständen eine Vielzahl weiterer Titel enthält, die den Nutzer nicht interessieren, verzichtet wird. Denkbar ist, dass dies für den Rechtein-

[200] *Clement/Schreiber*, Internet-Ökonomie, S. 325.

[201] *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 103ff.

[202] *Clement/Schreiber*, Internet-Ökonomie, S. 327f.

haber im Ergebnis negativ oder positiv ist, je nachdem, ob auf Grund der Verfügbarkeit der Werke als Einzelstück die früher mit den Kombinationen erzielten Gewinne erreicht werden oder nicht.[203]

Ausgehend von diesen theoretisch denkbaren Effekten ist in der ökonomischen Forschung stark umstritten[204], welche Effekte *in praxi* jeweils wie stark auftreten und wie schädlich oder nützlich *filesharing* somit insgesamt für die Urheberrechtsindustrie ist.

Die meisten vorhandenen Studien beziehen sich auf die Musikindustrie, wenige auf die Filmindustrie, fast keine auf die Videospielindustrie oder andere Werksgattungen wie E-Books.[205] Um die *filesharing*-Aktivität zu messen, beziehen sich die meisten Studien entweder auf Proxy-Variablen wie die Verbreitung von Breitbandanschlüssen, auf Quasi-Experimente wie die Einführung neuer Technologien (Napster) bzw. die Ausschaltung alter Technologien (*megaupload*) oder auf Umfragen; nur die wenigsten beziehen sich auf direkte Beobachtungen von *filesharing*-Netzwerken.[206] Auf der Folgenseite wird dann die ermittelte *filesharing*-Aktivität mit Kennzahlen wie Branchenumsätzen oder Verkaufszahlen in Beziehung gesetzt.[207] Folglich lässt sich nur mehr oder weniger eine Korrelation messen, wobei es enorme Schwierigkeiten bereitet, das *filesharing* gegen andere denkbare Faktoren (Konjunktur,

[203] *Elberse*, Journal of Marketing, Nr. 3, Bd. 74, 2010, S. 107, 108.

[204] *Danaher et al.* behaupten hingegen, dass mittlerweile Konsens bestehe, dass Online-Piraterie signifikant schädlich sei, vgl. *Danaher/Smith/Telang*, Communications of the ACM, Nr. 2, Bd. 60, 2017, S. 68. Sie beziehen sich dabei jedoch auf lediglich 26 Studien, ohne diese Auswahl zu begründen, diese überhaupt zu benennen sowie einer Analyse zu unterziehen. Einen Konsens wird mithin von anderen Wissenschaftlern auch verneint, siehe *Poort/Weda*, Journal of Media Economics, Nr. 2, Bd. 28, 2015, S. 63, 65.

[205] *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy" and sales of cultural goods, S. 4f.; *Handke/Girard/Mattes*, Fördert das Urheberrecht Innovation? Eine empirische Untersuchung, S. 13; *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 128ff. Die spezifischen Wirkungen von *Sci-Hub* auf Wissenschaftsverlage werden im Rahmen dieser Arbeit ausgeblendet, da Sci-Hub kein *filesharing* in deren Sinne ist.

[206] *Liu*, Quantifying the Heterogeneous Effects of Piracy on the Demand for Movies, S. 6f.; *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 113ff.

[207] *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 113ff.

Trends, Konkurrenz innerhalb der Unterhaltungsindustrie, mangelnde Zugriffsmöglichkeiten auf legale Angebote) zu gewichten.[208]

Betrachtet man beispielsweise die aggregierten Umsatzerlöse der Musikbranche, ist direkt nach der Einführung von Napster ein starker Einbruch zu verzeichnen; einen starken Abwärtstrend hatte es jedoch schon die Jahre zuvor gegeben.[209] Umgekehrt hatte die Einführung von neuen Kopiermedien wie der Musikkassette oder der CD in der Vergangenheit keine Umsatzeinbrüche, sondern im Gegenteil Steigerungen zur Folge.[210] Eine kausale Verknüpfung des Umsatzeinbruches der Musikbranche mit der Einführung mit Napster erscheint daher zweifelhaft. Vergleicht man die Musikbranche mit der Filmbranche, können im Vergleich verschiedener europäischer Länder untereinander vom Jahr 2002 bis 2012 keine durchgehenden Umsatzeinbrüche, sondern zum Teil auch Seitwärtsbewegungen oder gar Zugewinne festgestellt werden[211], obwohl in diesem Zeitraum *filesharing* auch zum Tauschen von Filmen benutzt wurde und der denkbare Einwand einer geringeren Anfälligkeit der Filmbranche für *filesharing* im Vergleich zur Musikbranche plausible Gründe vermissen lässt. Insgesamt kann die Unterhaltungsindustrie trotz anhaltender Nutzung von *filesharing*, Sharehosting und Streaming steigende Umsatzprognosen vermelden[212] und in einem Beobachtungszeitraum zwischen den Jahren 2014 bis 2017 konnten auch alle Branchen der Unterhaltungsindustrie ein Wachstum verzeichnen.[213]

Nicht nur der Gegenstand an sich bereitet der ökonomischen Wissenschaft Schwierigkeiten. Naturgemäß ist die Frage der Schädlichkeit von Online-Piraterie ideologisch stark umkämpft, sodass auch die Integrität ihrer Ergeb-

[208] *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 126ff; so auch, mit ergänzender Auflistung weiterer Methoden *Danaher/Smith/Telang*, Piracy Landscape Study, S. 19ff.

[209] Vgl. die Darstellungen bei *Seekamp*, Die Trägheit der deutschen Musikunternehmen bei technologischem Wandel: Eine Analyse aus branchenkultureller Perspektive, S. 61.

[210] Vgl. die Darstellungen bei *Seekamp*, Die Trägheit der deutschen Musikunternehmen bei technologischem Wandel: Eine Analyse aus branchenkultureller Perspektive, S. 50, 53.

[211] *Handke/Girard/Mattes*, Fördert das Urheberrecht Innovation? Eine empirische Untersuchung, S. 95.

[212] *Eliashberg* et al., International Journal of Research in Marketing, Nr. 2, Bd. 33, 2016, S. 241.

[213] *Poort* et al., Global Online Piracy Study, S. 41.

nisse und Methoden in Zweifel geraten kann. So hatte zum Beispiel die EU die Veröffentlichung einer von ihr in Auftrag gegebenen Studie[214] (zunächst) zurückgehalten, womöglich, weil die Studie nur geringe Auswirkungen von *filesharing* auf die Unterhaltungsindustrie ermitteln konnte und dieses Ergebnis möglicherweise die Berechtigung der geplanten Verschärfung des EU-Urheberrechts in Frage gestellt hätte.[215] Welches Signal sendet ein solcher Vorgang Wissenschaftlern, die sich mit den ökonomischen Wirkungen des *filesharing* befassen? Andererseits lässt sich – als Gegenbeispiel – die mit Abstand meistzitierte Studie zum Thema ökonomische Wirkungen des *filesharing*[216], nämlich der Artikel *The Effect of File Sharing on Record Sales: An Empirical Analysis* von *Oberholzer-Gee* und *Strumpf* aus dem Jahr 2007, anführen, die eine sehr geringe Schädlichkeit des *filesharing* ermittelt hatte, deren Autoren aber aus – nicht restlos geklärten – Gründen die Offenlegung ihrer Primärdaten, nämlich die auf einem *filesharing*-Server angeblich gemessene Aktivität, verweigert hatten.[217] Darüber hinaus erschienen einige ihrer Sekundärannahmen nicht fundiert.[218] Allerdings konnten die Autoren in ihrer Verteidigungsschrift zu Recht darauf hinweisen, dass sich – unabhängig von der Validität ihrer Studie aus 2007 – die Umsätze der Musikbranche stabilisiert haben, obwohl *filesharing* nach wie vor ein Massenphänomen ist.[219] Auch wenn deren Ergebnisse also zweifelhaft sind, erscheint ein Schluss in die andere Richtung ebenfalls nicht als zwingend.

Worauf kann man also vertrauen? Wenn es auch keinen Konsens gibt, so scheint es aus fachfremder Perspektive dennoch vorzugswürdig, sich an der wissenschaftlich ermittelten Mehrheitsmeinung zu orientieren. Die Metastudie von *Hardy et al.*[220] analysierte alle aufgefundenen empirischen Studien

214 *van der Ende* et al., Estimating displacement rates of copyrighted content in the EU.

215 Vgl. *Maxwell*, EU Piracy Report Suppression Raises Questions Over Transparency; *Schulzki-Haddouti*, Auswirkungen von Raubkopien: EU-Kommission unterdrückt Piraterie-Studie.

216 *Liebowitz*, Econ Journal Watch, Nr. 3, Bd. 13, 2016, S. 373.

217 *Liebowitz*, Econ Journal Watch, Nr. 3, Bd. 13, 2016, S. 373, 374.

218 Vgl. die Zusammenfassung bei *Liebowitz*, Econ Journal Watch, Nr. 3, Bd. 13, 2016, S. 373, 394f. und *Liebowitz*, Econ Journal Watch, Nr. 2, Bd. 14, 2017, S. 174, 193f.

219 *Oberholzer-Gee/Strumpf*, Information Economics and Policy, Bd. 37, 2016, S. 61, 66.

220 Es handelt sich hierbei um die bisher einzige wissenschaftlich verlässliche Metastudie; vgl. *Poort* et al., Global Online Piracy Study, S. 24, die nur diese Studie anführen. Sie hat bisher jedoch weder in der Ökonomie noch in der Politik Beachtung gefunden, siehe *Perrin*, A critical analysis of the effect of copyright infringement on the UK film and cinema industries, S. 15.

aus den Jahren 2004 bis 2013.[221] Zwar zeigten sich erhebliche Unterschiede bei den Ergebnissen für die Musik- und die Filmbranche[222], jedoch scheint die Mehrheitsmeinung vom Überwiegen negativer Effekte auszugehen.[223] Allerdings sind die negativen Auswirkungen auf die Unterhaltungsindustrie auch nach der überwiegenden Mehrheitsmeinung sehr gering.[224]

Zudem ist weiterhin zu beachten, dass es bisher keine Metastudie gibt, die alle seit 2014 erschienenen Studien analysiert und zugleich davon ausgegangen werden kann, dass die negativen Auswirkungen von *filesharing* seit den frühen 2000er Jahren nach und nach abgenommen haben[225], sodass eine neuere Metastudie möglicherweise auch ergeben könnte, dass die negativen Effekte mittlerweile noch geringer sind oder gar nicht mehr bestehen.

Dem fachfremden Beobachter drängt sich im Ergebnis jedenfalls der Eindruck auf, dass Online-„Piraterie“ im Allgemeinen und *filesharing* im Speziellen zwar möglicherweise negative ökonomische Effekte auf die Unterhaltungsindustrie hat, diese jedoch sehr gering sind und die Studien auf diesem

---

221 *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, S. 5.

222 Für die Musikbranche wurde ein größerer negativer Effekt ermittelt, siehe *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, S. 6. Sie zu den beiden Branchen auch *Danaher/Smith/Telang*, Piracy Landscape Study, S. 23ff.

223 *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, S. 2, 11.

224 Vgl. die *funnel plots* und *forest plots* bei *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, S. 25ff. Zu beachten ist, dass *Danaher et al.* in ihrer Piraterie-Studie für das *USPTO* aus 2020 ein anderes Fazit zu ziehen scheinen und von starken negativen Effekten ausgehen, vgl. *Danaher/Smith/Telang*, Piracy Landscape Study, S. 32f. Allerdings nehmen diese keine Auswertung der Literatur im engeren Sinne vor, sondern bieten „lediglich“ eine Literaturübersicht; zudem fehlt auch eine Auseinandersetzung mit *Hardy et al.*, sodass für den Verfasser als ökonomischen Laien nicht klar erkennbar ist, dass der Beurteilung von *Danaher et al.* der Vorzug zu geben wäre. *Hardy et al.* halten jedenfalls in einer aktualisierten Fassung ihrer Meta-Studie aus 2020 daran fest, dass die negativen Auswirkungen statistisch nur eine schwache Signifikanz aufweisen und dass zudem ein *publication bias* hinsichtlich Resultaten bestehe, die negative Auswirkungen bestätigen, insbesondere in Zeitschriften mit hohem Ranking, siehe *Hardy/Krawczyk/Tyrowicz*, Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, S. 16.

225 *Suwelack*, Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, S. 130.

Feld ohnehin auf sehr unsicheren Annahmen und Datenmaterial beruhen.

2. Auswirkungen des Vorgehens gegen *filesharing*-Endnutzer

Geht durch das Vorgehen gegen *filesharing*-Endnutzer bzw. Anschlussinhaber die *filesharing*-Nutzung überhaupt zurück?

Es existiert gegenwärtig kein empirischer Nachweis dafür, dass dies in Deutschland der Fall ist. Die unter Kapitel § 3 IX. 2. aufgeführte Studie des *EUIPO* trifft hierzu leider keine Aussage. Zwar wurde festgestellt, dass in Deutschland ein Rückgang von Urheberrechtsverletzungen über das Internet zu verzeichnen ist, jedoch wurde bei der Fragegestaltung nicht zwischen den einzelnen Verletzungsmöglichkeiten (Streaming, Sharehosting, UseNet, *filesharing*) differenziert.[226] Soweit an anderer Stelle[227] auf Studien der Musikindustrie, die eine Korrelation zwischen Abmahnungen und Rückgang der *filesharing*-Nutzung erkennen wollen, verwiesen wird, so sind diese Studien vor der „Hochphase“ der Abmahnungen erschienen; sie sind also – unabhängig von ihrer Validität – veraltet, haben mithin keine Aussagekraft. Ein entsprechendes Studiendesign könnte beispielsweise Deutschland mit den Ländern der Kategorie 1[228] vergleichen, in denen gegen *filesharing*-Endnutzer überhaupt nicht vorgegangen werden kann und den jeweiligen Verlauf der BitTorrent-Datenmengen gegenüberstellen.

Jedoch ist nicht zu erwarten, dass eine solche Studie einen vergleichsweise höheren Rückgang oder niedrigeren Anstieg der BitTorrent-Datenmengen feststellen würde, da Studien mit vergleichbarer Zielsetzung besondere Effekte eines Vorgehen gegen *filesharing*-Endnutzer nicht einheitlich feststellen konnten. Nach einer kursorischen Literaturübersicht von *Poort et al.* kommen zwar vereinzelte Studien zu dem Ergebnis, dass im Rahmen des Vorgehens gegen Endnutzer die Verkaufszahlen anstiegen; dies könnte allerdings ebenso auf die Ankündigung entsprechender rechtlicher Maßnahmepakete zurückzuführen sein, da die Effekte nur kurzfristig anhielten.[229] Andere Studien beschäftigen sich lediglich mit dem Rückgang des *filesharing*-Datenverkehrs

[226] *EUIPO*, European Citizens and Intellectual Property: Perception, Awareness and Behaviour 2017, S. 136.
[227] *Nümann/Mayer*, ZUM 2010, 321, 323.
[228] Siehe hierzu Kapitel § 3 XII. 2.
[229] *Poort* et al., Global Online Piracy Study, S. 27f.

auf Grund des Vorgehens gegen Endnutzer[230], ohne einzubeziehen, dass erstens der Datenverkehr sich auch nur auf anonyme und anonymisierte Systeme verlagert haben könnte[231] und zweitens der Rückgang des Datenverkehrs zunächst einmal wenn dann überhaupt nur bedeutet, dass weniger heruntergeladen, nicht aber, dass mehr gekauft wird[232]. So kommt eine neuere Studie auch zu dem Ergebnis, dass sich die verschiedenen *graduated response*-Systeme[233] nicht positiv auf Verkaufszahlen auswirken.[234]

Das soeben Gesagte spiegelt auch den generellen Forschungsstand der Wirtschaftspsychologie wieder, demzufolge kein Konsens darüber besteht, von welchen Motivationen „Online-Piraterie" überhaupt getragen wird und mithin auch unklar ist, welche Gegenmaßnahmen also wirksam sind.[235]

3. Ergebnis

Zusammenfassend lässt sich feststellen, dass ökonomische Studien zum *filesharing* auf unsicherer Datengrundlage basieren und mehrheitlich allenfalls geringe negative ökonomische Effekte auf die Unterhaltungsindustrie feststellen können. Zudem fehlt es an einer Metastudie, die die Studienlage seit 2014 analysiert; es ist nicht unwahrscheinlich, dass neuere Studien mehrheitlich noch weniger negative oder gar keine negativen Effekte feststellen können. Weiterhin scheint nicht gesichert, dass das Vorgehen gegen Endnutzer irgendwelche positive ökonomische Effekte zeitigt.

Im Ergebnis können nach hiesiger Auffassung also die möglichen negativen Effekte des *filesharing* die rechtspolitischen Kritikpunkte am Vorgehen gegen Anschlussinhaber und Endnutzer nicht aufwiegen.

---

230 *Poort* et al., Global Online Piracy Study, S. 28.

231 *Alcock/Nelson*, Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users, S. 551, S.556; *Poort* et al., Telecommunications Policy, Nr. 4, Bd. 38, 2014, S. 383, 391.

232 *Jeong/Lee*, Applied Economics, Nr. 30, Bd. 42, 2010, S. 3885, 3891f.

233 Siehe Kapitel § 3 XII. 2. b).

234 *McKenzie*, Information Economics and Policy, Bd. 38, 2017, S. 1, 11.

235 Siehe die Metastudie von *Fleming* et al., Computers in Human Behavior, Bd. 72, 2017, S. 535, 544ff sowie *Danaher/Smith/Telang*, Piracy Landscape Study, S. 43f. Ein Grundproblem dürfte laut einer neurowissenschaftlichen Erklärung sein, dass – anders als beim Diebstahl körperlicher Gegenstände – der „Diebstahl" unkörperlicher Gegenstände mangels haptischer Erfahrung kaum Unrechtsbewusstsein aufkeimen lassen kann, siehe *Eres/Louis/Molenberghs*, Social Neuroscience, Nr. 4, Bd. 12, 2017, S. 366, 373ff.

X. Definition des Begriffs „Abmahnwesen“

In den vorstehenden Abschnitten wurde aufgezeigt, wie sich das Vorgehen gegen *filesharing*-Endnutzer von der regulären rechtsanwaltlichen Tätigkeit betreffend die Verfolgung von Rechtsverletzungen mittels Abmahnungen unterscheidet. Die in der Einleitung dieses Kapitels entsprechend aufgestellte Hypothese ist daher gerechtfertigt.

Im Ergebnis lässt sich damit, entlang dem Vorgesagten, definieren, wann – auch unabhängig vom Komplex *filesharing* – generell von einem rechtspolitisch kritikwürdigem Abmahnwesen gesprochen werden kann:

Als Abmahnwesen ist das massenhafte, durch die bestehende oder sich entwickelnde Rechtspraxis überwiegend gedeckte Vorgehen gegen nichtgewerblich[236] handelnde Rechteverletzer, gegebenenfalls aber auch gegen tatsächlich für die Rechtsverletzung nicht verantwortliche Dritte, mit Abmahnungen (oder ähnlicher vorgerichtlicher) Instrumente und sich anschließenden Gerichtsprozessen zu verstehen, bei dem nicht das Abstellen der Rechtsverletzungen im Vordergrund steht, sondern durch das Vorgehen eine eigene Profitquelle erschlossen wird und bei dem zwischen Abmahnenden und Abgemahnten ein strukturelles Machtungleichgewicht besteht, das sich vor allem in einem faktisch bestehenden Defizit der Möglichkeiten der Rechtswahrnehmung seitens der Abgemahnten und korrespondierend mit der Möglichkeit seitens der Abmahnenden, psychologischen Druck aufzubauen, ausdrückt.

[236] Dieses Merkmal ist nicht zwingend. Bereits in der Vergangenheit hatte beispielsweise im UWG die Tätigkeit von sogenannten „Gebührenvereinen“ Aufmerksamkeit erregt, deren Vorgehen dem in diesem Kapitel dargestellten Abmahnwesen nicht unähnlich war, vgl. hierzu *Kur*, GRUR 1981, 558, 559ff.. Auch gegenwärtig gerät die Abmahnpraxis im UWG wieder mehr in den Blick. Kleinunternehmer fühlen sich von den vielen Informationspflichten, die sie treffen überfordert, vgl. dazu die Petition 77180, https://epetitionen.bundestag.de/content/petitionen/_2018/_03/_08/Petition_77180.html - Zugriff am 31.03.2021. Laut einer Umfrage seien seit dem Jahr 2017 fast die Hälfte aller befragten Unternehmer in den vergangenen 12 Monaten abgemahnt worden; die Abmahnungen wurden zu einem bedeutenden Teil von Vereinen und Unternehmen ausgesprochen, die – wie schon in der Vergangenheit – im Verdacht stehen, es primär auf Gewinnerzielung und nicht auf Abstellen der Rechtverletzung abgesehen zu haben, siehe *TrustedShops*, Abmahnungen im Online-Handel 2017, S. 4, 13.

XI. Zukunftsprognosen

In diesem Abschnitt soll eine Prognose gewagt werden, wie sich der Komplex *filesharing*-Abmahnungen und Abmahnwesen in den nächsten Jahren weiter entwickeln wird.

1. Aufarbeitung von Altfällen

Nach Kenntnis und eigener Erfahrung des Verfassers arbeiten die größeren Abmahnkanzleien Abmahnungen mit einigen – durchschnittlich drei – Jahren Verzögerung ab; dies lässt sich auch aus den Tatbeständen der einschlägigen Urteile ableiten. Exemplarisch sei „Tauschbörse IV“ erwähnt: dort wurde die Abmahnung im Juli 2010 versandt, das Mahnverfahren im Oktober 2013 eingeleitet.[237] Mit einer erstinstanzlichen Entscheidung ist daher regelmäßig erst vier Jahre nach Erhalt einer Abmahnung zu rechnen, mit einer letztinstanzlichen Entscheidung gegebenenfalls erst sechs bis acht Jahre nach Erhalt der Abmahnung.

Grund für die zeitliche Verschiebung dürfte die großen Masse an Abmahnungen sein, die auch eine routinierte Kanzlei mit zahlreichen angestellten Anwälten nicht zeitnah bearbeiten kann. Grund dafür, warum nach drei Jahren spätestens gehandelt wird, ist, dass dann noch mit einem Mahnbescheid oder einer Klageerhebung die Verjährung des Anspruchs auf Ersatz der Rechtsanwaltsgebühren für die Abmahnung sowie der Schadensersatzanspruch, für die die regelmäßige Verjährungsfrist nach §§ 195, 199 BGB gilt, gemäß § 204 Abs.1 Nr.1, Nr.3 BGB gehemmt werden kann. Im Mahnverfahren kann das Verfahren zudem weiter hinaus gezögert werden, indem zum Beispiel für die Einreichung der Anspruchsbegründung nach Widerspruch der Sechs-Monats-Zeitraum des § 204 Abs.2 BGB ausgereizt wird. Ein (für den Abmahnenden sicher nicht unerwünschter) Nebeneffekt des Hinauszögerns ist, dass dem Anschlussinhaber im gerichtlichen Verfahren unter Umständen wegen Erinnerungslücken die Erfüllung der sekundären Darlegungslast erschwert wird.[238] Der – für den Abmahnenden besonders wichtige[239] – Schadensersatzanspruch kann darüber hinaus auch als Restschadensersatzanspruch geltend gemacht

[237] BGH, Urteil vom 12. Mai 2016, Az. I ZR 272/14, Rz. 2f. – ZUM 2016, 1037.
[238] Siehe auch Kapitel § 5 V. 3. c).
[239] Siehe Kapitel § 3 VI.

werden, der der zehnjährigen Verjährungsfrist unterliegt.[240] In einem Interview mit AW3P weist ein Anwalt der bekanntesten Abmahnkanzlei ausdrücklich auf diese Verjährungsfrist hin; es ist also davon auszugehen, dass diese bewusst ausgereizt wird.[241]

Es erscheint daher im Ergebnis nicht unwahrscheinlich, dass nach Veröffentlichung dieser Arbeit nicht nur zahlreiche Fälle aus den Jahren 2014 und Folgende erstmals erstinstanzlich anhängig gemacht und entschieden werden, sondern unter Umständen auch noch einige Altfälle aus früheren Jahren; aus den Jahren 2010 bis 2014, in denen enorm viele Abmahnungen versandt wurden[242], könnte manch Abmahnung noch nicht weiterverfolgt worden sein. In der Vergangenheit wurden zur Abarbeitung der Masse auch Inkassodienstleister eingesetzt[243], sodass auch die weitere Aufarbeitung von Altfällen praktisch bewältigbar erscheint.

2. Zur zukünftigen Entwicklung der Abmahnzahlen

Zunächst ist zu prognostizieren, dass Privatpersonen neben *filesharing*-Abmahnungen auch in Zukunft kaum Abmahnungen wegen Rechtsverletzungen über andere Plattformen wie Streaming- und Sharehosting-Dienste erhalten werden. Nicht nur können die Endnutzer dieser Dienste kaum ermittelt werden[244]; Massenabmahnungen wegen Urheberrechtsverletzungen durch Endnutzer dienen auf Grund der in Kapitel § 3 VI. genannten Gesichtspunkte vorrangig der Gewinnerzielung. Die Endnutzer dieser Dienste begehen „nur“ eine Vervielfältigung nach § 16 UrhG, bei der die Überlegungen des BGH zum lizenzanalogen Schaden bei öffentlicher Zugänglichmachung nach § 19a UrhG nicht greifen, mithin nur ein Schadensersatz verlangt werden könnte, der der Höhe nach dem Preis dem Erwerb einer Verkörperung des Werks oder einer digitalen Kopie entspricht.

Der zukünftige Nutzungsumfang „gewöhnlichen“ *filesharings*, also nichtanonymisiertes *filesharing* über einen Client zum Zwecke der Erlangung und dauerhaften Speicherung einer urheberrechtsverletzenden Datei, und der damit verbundenen Abmahnzahlen, lässt sich nur schwer prognostizieren. Ob

[240] Siehe Kapitel § 2 VII. 2.
[241] https://aw3p.de/archive/3597 - Zugriff am 31.03.2021.
[242] Siehe Kapitel § 3 V.
[243] *Bleich*, c't, Bd. 11, 2015, S. 153.
[244] Siehe Kapitel § 3 IV.

Massenabmahnungen auf gesamtgesellschaftlicher Ebene einen „Erziehungseffekt“ haben und damit einen Nutzungsrückgang bewirken können, ist zu bezweifeln.[245]

Unabhängig von dieser Frage könnten im Bereich des *filesharing* in Zukunft jedoch auch neue Formen und Inhalte für Abmahner (verstärkt) interessant werden.

a) P2P-Streaming

Beim P2P-Streaming wird – wie beim regulären Streaming auch – eine Video- oder Audiodatei bereits laufend während des Downloads wiedergegeben, wobei die Datei lediglich in den Arbeitsspeicher geladen wird ohne dass eine Kopie auf der Festplatte abgespeichert wird. Im Unterschied zum regulären Streaming basiert die Dateiübertragung auf dem Prinzip des *filesharing*, typischerweise dem BitTorrent-*filesharing*. Der einzige Unterschied zu „gewöhnlichem“ *filesharing* ist also, dass die Datei nicht dauerhaft gespeichert werden soll.[246]

Bereits im Jahr 2014 wurden erste Abmahnungen wegen P2P-Streaming versandt.[247] Am bekanntesten ist der Dienst *Popcorn Time*, für dessen Nutzung grundsätzlich ein Client heruntergeladen werden muss, in dessen Oberfläche ähnlich wie bei Diensten wie *Netflix* direkt Filme zum Abspielen ausgewählt werden können, der also in technischer Betrachtung die Funktionen klassischer BitTorrent-Clients und Indexseiten auf sich vereint.[248] Abmahnungen wegen der Nutzung von *Popcorn Time*[249] waren möglicherweise für den Anstieg der Abmahnzahlen nach 2014 verantwortlich.[250]

Mittlerweile ist der Abruf dieses Dienstes direkt aus dem Webbrowser, also ohne eigenen Client, möglich.[251] Andere Dienste, der direkt aus dem Browser abrufbar sind, sind beispielsweise *BitChute*[252] und *PeerTube*[253], die in ihrer

[245] Siehe hierzu Kapitel § 3 IX. 2.
[246] Vgl. auch Kapitel § 1 III.
[247] *Link*, Abmahnungen für P2P-Streaming machen die Runde: Vorsicht bei Cuevana, Popcorn Time und Co.
[248] en.wikipedia.org/wiki/Popcorn_Time - Zugriff am 31.03.2021.
[249] *Sawall*, Popcorn-Time-Nutzer zahlen in Vergleich 690 Euro.
[250] Siehe Kapitel § 3 V. 2.
[251] *Statt*, Popcorn Time for your browser makes illegal movie streaming even easier.
[252] *Maxwell*, BitChute is a BitTorrent-Powered YouTube Alternative.
[253] *Van Der Sar*, PeerTube: A 'Censorship' Resistent YouTube Alternative.

Aufmachung *YouTube* sehr ähneln. Technologien wie *WebTorrent* erlauben es Webseiten, die Möglichkeiten des *filesharing* auch für andere Zwecke als Streaming zu nutzen.[254] Allen diesen Diensten ist damit auch die Möglichkeit immanent, für urheberrechtsverletzende Inhalte verwendet zu werden.

Folglich gibt es also auch gegenüber dem clientgebundenen *filesharing* immer mehr attraktive Möglichkeiten der mobilen Nutzung von *filesharing*; der Trend weg vom Desktop[255] dürfte sich mithin verstärken.[256] Sollten folglich wegen der vermeintlichen Sicherheit, die das 3. TMGÄndG gewährt, mehr Privatpersonen und Gewerbetreibende als zuvor ihr WLAN für Dritte öffnen, und sollten mehr kommunale, freie WLANs entstehen[257], ergeben sich hiermit auch automatisch für die Anschlussinhaber neue Abmahnrisiken. Entweder, weil die Nutzer aus Unkenntnis über die Funktionsweise der genannten Technologien oder aus Unkenntnis über die Schutzlage betreffend einer aufgerufenen Datei nicht wissen, dass sie eine Urheberrechtsverletzung begehen, oder weil sie bewusst die mangelnde Rückverfolgbarkeit von Urheberrechtsverletzungen bei Nutzung fremder WLANs[258] für Urheberrechtsverletzungen nutzen.

Ein weiterer, potentieller Gegenstand zukünftiger Abmahnungen sind Set-Top-Boxen mit BitTorrent implementierender Kodi-Software. Set-Top-Boxen sind Geräte, die an einen Fernseher angeschlossen werden können.[259] Kodi ist eine individuell konfigurierbare Software für solche Geräte.[260] Durch diese Kombination lassen sich auf einem Fernseher Inhalte von Streaming-Anbietern (häufig illegaler Natur) abrufen. Während die Anbieter solcher Set-Top-Boxen selbst häufig Ziel rechtlicher Angriffe sind[261], sind auch deren Nutzer potentielle Ziele, wenn deren Kodi-Software so eingestellt ist, dass

254 *Van Der Sar*, WebTorrent Brings BitTorrent to the Web, Impresses Netflix.

255 *MUSO*, Global Piracy Report, S. 9.

256 Wenig verwunderlich gibt es daher mittlerweile erste Netzsperrverfügungen gegen Anbieter mobiler Internetzugänge, vgl. Oberster Gerichtshof in Österreich, Beschluss vom 24. Oktober 2017, Az. 4 Ob 121/17y – GRUR Int. 2018, 479.

257 Siehe Kapitel § 2 XII. 2.

258 Siehe Kapitel § 1 IV.

259 https://de.wikipedia.org/wiki/Set-Top-Box - Zugriff am 31.03.2021.

260 https://de.wikipedia.org/wiki/Kodi_(Software) - Zugriff am 31.03.2021.

261 Vgl. EuGH, Urteil vom 26. April 2017, Rs. C-527/15, Rz. 15ff. – ECLI:EU:C:2017:300 - „Filmspeler“.

BitTorrent-Streaming benutzt wird.[262]

b) P2P-Browsing

Noch weiter als P2P-Streaming geht P2P-Browsing: bei einem P2P-Browser werden nicht nur einzelne Inhalte einer Webseite durch *filesharing* verteilt, sondern stattdessen gleich die gesamte Webseite, die damit auch keinen zentralen Speicherort mehr aufweist.

Beispielsweise wurde bei BitTorrent Inc. ein solcher Browser unter dem Namen *Maelstrom* entwickelt, der sich die DHT[263] zu Nutze macht.[264] Webseiten in diesem System könnten folglich auch nicht durch IP-, DNS- oder URL-Sperren geblockt werden.[265] Das Projekt wird zwar gegenwärtig nicht fortgeführt, jedoch sind andere, ähnliche Projekte wie der Browser *Beaker*[266] in Arbeit und sicherlich werden weitere folgen.

Solche Browser eröffnen allerdings auch weitere Möglichkeiten für Urheberrechtsverletzungen, da dort bereits das Ansurfen einer Webseite mit urheberrechtsverletzenden Inhalten ein öffentliches Zugänglichmachen darstellt. Entsprechend ergeben sich auch hier Abmahnrisiken.

c) Zugriff auf Anonymisierungsdienste und private Börsen

Wie in Kapitel § 1 IV. 6. b) aufgezeigt, können die Nutzer von Anonymisierungsdiensten nicht direkt ermittelt werden, sondern nur der jeweils für das *filesharing* genutzte Anonymisierungsdienst. Rechteinhaber könnten in Zukunft versuchen, von solchen Diensten Auskunft über deren Nutzer zu erlangen, insbesondere da die Nutzung solcher Dienste – wohl auch für BitTorrent – konstant zunimmt.[267] Jedoch ermöglichen diese Dienste ihre Nutzung in der Regel anonym, es müsste also erstens eine Speicherpflicht bezüglich der Nutzerdaten (insbesondere der IP-Adressen der Nutzer) und ein Auskunftsanspruch gegen solche am jeweiligen Standort bestehen und durchsetzbar

[262] Vgl. für einen solchen Fall aus den USA *Van Der Sar*, BitTorrent Piracy Lawsuit Morphs into Attack on Dragon Box and Resellers.
[263] Siehe Kapitel § 1 II. 5. a) bb).
[264] *Farina/Kechadi/Scanlon*, JDFSL 2015, 115, 121f.
[265] *Van Der Sar*, Beating Internet Censors With BitTorrent's Maelstrom Browser.
[266] https://beakerbrowser.com - Zugriff am 31.03.2021.
[267] *Bailey*, The Long, Slow Decline of BitTorrent.

sein, was gegenwärtig nicht der Fall ist.[268]

Hinsichtlich der Endnutzer könnte es für Rechteinhaber in Zukunft statt dem Zugriff auf VPNs oder *seedboxen* interessanter sein, Ermittler in private Börsen[269] „einzuschleusen", anstatt wie bisher zu versuchen, diese insgesamt abzuschalten.[270]

d) Zugriff auf anonyme Systeme

Denkbar ist auch, dass versucht wird, die Endnutzer anonymer Systeme[271] zu ermitteln, sofern deren Nutzerzahlen in substantiellem Ausmaß zunehmen sollten. Gänzlich unmöglich ist dies nicht. Im Jahr 2012 wurde gegen einen Nutzer des Systems *RetroShare* vom LG Hamburg eine einstweilige Verfügung erlassen.[272] Bei diesem System werden zur Anonymisierung Daten über mehrere Nutzer weitergeleitet, bis sie am Ziel ankommen.[273] Der Nutzer, der hier nur Daten weiterleitet, ist also rechtlich ähnlich wie der Betreiber einer Tor-*exitnode*[274] einzustufen, kann mithin allenfalls als Störer bzw. nach § 7 Abs.4 TMG in Anspruch genommen werden.[275] Solange nur Nutzer ermittelt werden können, die lediglich eine Durchleitungsfunktion erbringen (wie es im Sachverhalt vor dem LG Hamburg der Fall war), sind anonyme Systeme für Abmahnwesen uninteressant.[276]

Es konnte jedoch bereits demonstriert werden, dass durch bestimmte Methoden auch die Empfänger in dem anonymen, hinsichtlich der Datenüber-

[268] Soweit bekannt, haben VPN-Dienste in der Vergangenheit nur vereinzelt Nutzerdaten gespeichert und herausgegeben, allerdings in strafrechtlichen Zusammenhängen, siehe *Leyden*, HideMyAss defends role in LulzSec hack arrest; *Van Der Sar*, PureVPN Explains How it Helped the FBI Catch a Cyberstalker. In Fällen das Urheberrecht betreffend ist eine Herausgabe bisher an fehlender Nutzerdatenspeicherung gespeichert, siehe zu einem Fall aus den USA *Maxwell*, OVPN Wins Court Battle After Pirate Bay Data Demands Rejected. Anbieter von *seedboxen* haben, soweit ersichtlich, bisher unterschiedliche Speicherpraxen, siehe *Van Der Sar*, How 'Anonymous' is a Seedbox Provider?

[269] Siehe hierzu Kapitel § 1 II. 5. c).

[270] Siehe Kapitel § 1 II. 5. c).

[271] Siehe hierzu Kapitel § 1 IV. 6. a).

[272] LG Hamburg, Beschluss vom 24. September 2012, Az. 308 O 319/12 – juris.

[273] https://bit.ly/2X3EJLe - Zugriff am 31.03.2021.

[274] Siehe hierzu Kapitel § 1 IV. 6. b) cc).

[275] Zur Haftung eines Tor-*exitnode*-Betreibers als Störer siehe LG Berlin, Urteil vom 13. Juni 2017, Az. 16 O 270/16 – juris sowie Kapitel § 2 XI. 6.

[276] Siehe Kapitel § 3 VI.

tragung aber ähnlich wie BitTorrent funktionierenden, System *OneSwarm* ermittelt werden können.[277] Es ist nicht ausgeschlossen, dass dies auch in anderen, ähnlichen Systemen möglich ist. Hinsichtlich der ermittelten Nutzer ergäbe sich rechtlich dann kein Unterschied gegenüber BitTorrent-Nutzern.

e) 3D-Druck

Bisher betrafen Massenabmahnungen wegen *filesharing* ausschließlich das Urheberrecht. Überhaupt sind die Möglichkeiten für nicht-gewerblich handelnde Privatpersonen, andere Schutzrechte als das Urheberrecht zu verletzen, bisher kaum vorhanden. Markenverletzungen sind wegen des Erfordernisses des Handelns im geschäftlichen Verkehr[278] für diese Personengruppe von vornherein ausgeschlossen. Im Patent-, Gebrauchsmuster- und Designrecht stellen die Schranken der §§ 11 Nr.1 PatG, § 12 Nr.1 GebrMG und 40 Nr.1 DesignG hohe Hürden dar.

Im Jahr 2003 wurden die Inhaber einiger .de-Domains im Auftrag eines Patentinhabers abgemahnt, dessen Patent angeblich die Kombination eines KfZ-Kennzeichens mit einer .de-Domain schütze. Gezahlt hatte auf die Abmahnungen jedoch augenscheinlich niemand, stattdessen wurde wegen versuchtem Betrug ermittelt.[279] Das Patent wurde jedenfalls vom BPatG für nichtig erklärt.[280] Abgesehen von diesem – eher bizarr anmutenden - Fall, sind keine Massenabmahnungen im Bereich des Patent- oder im Bereich des Gebrauchsmuster- und Designrechts bekannt.

Dies könnte sich in Zukunft jedoch durch die zunehmende Verbreitung von 3D-Druckern ändern. 3D-Drucker können durch ein additives Fertigungsverfahren beliebige dreidimensionale Objekte erzeugen, also beispielsweise mechanische Bauteile, Textilien und Lebensmittel.[281] Entsprechende Drucker existieren auch für den Heimgebrauch und finden – mit der Prognose weiterer Steigerungen – immer mehr Abnehmer.[282] Beschleunigt wird die

---

277 *Prusty/Levine/Liberatore*, Forensic Investigation of the OneSwarm Anonymous Filesharing System, S. 201, 204ff.

278 *Mielke* in: Kur/von Bomhard/Albrecht, BeckOK MarkenR, 24. Ed. 2021, § 14 MarkenG, Rz. 56ff.

279 *Klaß*, Betrugsversuch oder Patent-Wahnsinn?

280 BPatG, Urteil vom 3. März 2005, Az. 2 Ni 52/03 – MMR 2005, 593.

281 https://de.wikipedia.org/wiki/3D-Druck - Zugriff am 31.03.2021.

282 *Balasubramanian* et al., Technology Forecasting: Case of 3D Printing, S. 96f.

Entwicklung durch den Auslauf zahlreicher Grundlagenpatente[283], was Wettbewerbern den Marktzutritt erleichtert.

Gesteuert werden 3D-Drucker durch die in einer Datei im .cad-Format manifestierte, digitale Repräsentation eines körperlichen Erzeugnisses. Solche Dateien können entweder durch Nutzer erstellt werden, indem das zu replizierende Objekt gescannt wird, oder der Hersteller eines Erzeugnisses hat bereits selbst eine solche Datei erstellt.[284] Solche Dateien können wie andere Dateien auch ohne weiteres über *filesharing* im Internet verteilt werden, was gegenwärtig bereits in nicht zu vernachlässigendem Umfang praktiziert wird.[285] Zwar werden – zumindest gegen das Einscannen – bereits dem *Digital Rights Management* (DRM) ähnliche Sicherungsmechanismen wie physisches *watermarking* vorgeschlagen[286]; Sicherungsmechanismen haben aber schon gegen bisheriges *filesharing* nichts genutzt. Es ist daher kaum davon auszugehen, dass beim 3D-Druck wirkungsvolle, technische Schutzmaßnahmen implementiert werden können.

In der US-amerikanischen juristischen Literatur wird bereits seit geraumer Zeit darauf hingewiesen, dass auch das öffentliche Zugänglichmachen einer .cad-Datei eine Patentverletzung darstellen kann[287], mithin 3D-Druck (in Kombination mit *filesharing*) als disruptive Technologie das Patentrecht und die Sicht darauf genauso transformieren wird, wie es *filesharing* mit dem Urheberrecht getan hat.[288] Einer der Gründer von *The Pirate Bay* äußerte diesbetreffend in einem Interview, dass die rechtlichen Angriffe gegen BitTorrent-*filesharing* durch die Urheberrechtsindustrie seiner Meinung nach nichts im Vergleich zu dem seien, was kommen werde, wenn sich durch *filesharing* auch andere Industriezweige bedroht fühlen:

> *„With the MPAA and the RIAA and their likes, there haven't been any serious problems. There's actually been more downtime*

[283] *Schoffer*, How expiring patents are ushering in the next generation of 3D printing.

[284] *Van Overwalle/Leys*, IIC 2017, 504, 512ff.

[285] Ein Überblick über entsprechende Plattformen findet sich bei *Mendis/Secchi*, A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour, S. 24ff.; vertreten sind auch bekannte BitTorrent-Indexseiten wie *The Pirate Bay*.

[286] *Aron*, New Scientist, Nr. 2850, Bd. 213, 2012.

[287] *Doherty*, 26 Harv. L.J. & Tech. 1, 353, 358ff. (2012).

[288] *Desai/Magliocca*, 102 Geo. L. J. 1691, 1718ff. (2013); so auch *Kurz*, Auf Knopfdruck wird die Realität kopiert.

> *for the site due to drunk admins, than downtime due to raids. But when car manufacturers, oil companies and nations start feeling threatened, we're going to need something better.*"[289]

Die zukünftige, praktische Relevanz ist damit offensichtlich. Wie ist also die deutsche Rechtslage? Rechtsprechung existiert noch keine, das öffentliche Zugänglichmachen einer .cad-Datei soll nach den vorhandenen Literaturstimmen jedoch nicht nur § 19a UrhG erfüllen[290], sondern auch eine mittelbare Patent- und Gebrauchsmusterverletzung (§ 10 PatG, § 11 Abs.2 GebrMG) darstellen[291].

Hinsichtlich der gewerblichen Schutzrechte sollen sich nicht-kommerziell handelnde (also wie beim *filesharing* von Musik, Filmen und Spielen praktisch alle) Endnutzer nicht auf die Schrankenregelungen der § 11 Nr.1 PatG, § 12 Nr.1 GebrMG und § 40 Nr.1 DesignG berufen können. Denn diese Schrankenregelungen setzen ihrem Wortlaut nach neben dem nicht-gewerblichen Handeln kumulativ voraus, dass die Handlung zudem im *privaten* Bereich stattfindet. Laut der vorhandenen Literatur könne das öffentliche Zugänglichmachen in einem *filesharing*-System nicht als „*privater Bereich*" in diesem Sinne angesehen werden.[292]

Sollte sich diese Auffassung in Zukunft in der Rechtsprechung durchsetzen, stünden wegen des 3D-Drucks Massenabmahnungen gegen Private also auch im Patent-, Gebrauchsmuster- und Designrecht bevor. Abmahnungen auf diesen Rechtsgebieten wären für Privatpersonen aber noch verheerender als urheberrechtliche Abmahnungen:

Erstens wäre dort Rechtsschutz noch schwieriger zu erlangen, da in diesen Rechtsgebieten noch weniger spezialisierte Anwälte tätig sind[293], und deren Vergütungsmodelle zudem nicht auf Privatpersonen ausgerichtet sind und zweitens sind in den einschlägigen Gesetzen keine den §§ 97a, 104a UrhG entsprechenden Regeln enthalten. Drittens wird das Gros der patent- und

---

289 *Van Der Sar*, „Shut Down The Pirate Bay", Founder Says.

290 *Nordemann/Rüberg/Schaefer*, NJW 2015, 1265, 1266.

291 *Nordemann/Rüberg/Schaefer*, NJW 2015, 1265, 1269; *Haedicke/Zech*, GRUR-Beilage 2014, 52, 55f.; *Graf Ballestrem*, Mitt. 2016, 358, 363f.; *Blanke-Roeser*, GRUR 2017, 467, 470f.

292 *Haedicke/Zech*, GRUR-Beilage 2014, 52, 57; *Blanke-Roeser*, GRUR 2017, 467, 471.

293 Zudem müssten für einen Rechtsbestandsangriff auf Patente und Gebrauchsmuster Patentanwälte engagiert werden.

gebrauchsmusterrechtlichen Fälle vor wenigen, spezialisierten Landgerichten verhandelt; diese wären mit der Abwicklung von dem *filesharing* im Urheberrecht ähnlichen Fallmassen in ihren Kapazitäten überfordert, wären also genötigt, diese Fälle möglichst effizient abzuwickeln. Da die Abgemahnten hier strukturell weniger Widerstand leisten als die Abmahnenden Druck aufbauen können, dürfte – wie im Urheberrecht auch – diese Abwicklung rechtlich nicht zu Gunsten der Abgemahnten ausgehen.

f) Ergebnis

Auch wenn die Nutzung des „gewöhnlichen" *filesharing*, also nicht-anonymisiertes *filesharing* über einen Client zum Zwecke der Erlangung und dauerhaften Speicherung einer urheberrechtsverletzenden Datei, in Deutschland in Zukunft abnehmen sollte, existieren oder entstehen andere Nutzungsformen oder Nutzungsinhalte das *filesharing* betreffend, die bereits jetzt oder in Zukunft ein Abmahnrisiko bergen.

Folglich dürfte in Deutschland auch in Zukunft ein Abmahnwesen existieren und die damit verbundenen rechtlichen Fragen relevant bleiben.

XII. Abmahnwesen im internationalen Vergleich

1. Einleitung

Der Vergleich mit anderen Rechtsordnungen erlaubt es, zu überprüfen, ob diejenigen rechtlichen Institute, die in dieser Arbeit als notwendig und hinreichend erachtet wurden, um ein Abmahnwesen entstehen zu lassen und es tragen[294], zutreffend identifiziert wurden.

Entsprechend lassen sich Länder, für die Daten vorhanden waren, danach klassifizieren, ob

- In ihnen kein Abmahnwesen existiert und es an den genannten rechtlichen Voraussetzungen fehlt (Kategorie 1).
- In ihnen gegenwärtig kein Abmahnwesen existiert, jedoch die weiteren Entwicklungen abzuwarten sind (Kategorie 2).

[294] Siehe Kapitel § 3 VII.

- In ihnen kein Abmahnwesen existiert, obwohl dort die genannten rechtlichen Voraussetzungen bestünden (Kategorie 3).
- In ihnen ein Abmahnwesen existiert, obwohl dort die behaupteten rechtlichen Voraussetzungen fehlen (Kategorie 4).
- In ihnen ein Abmahnwesen existiert, und die dortige Rechtslage der deutschen sehr ähnelt (Kategorie 5).

In die Betrachtung wurden sämtliche Länder einbezogen, für die Gerichtsentscheidungen, juristische Literatur und/oder Presseberichterstattung betreffend Abmahnungen oder sonstigem Vorgehen gegen Endnutzer wegen *filesharing* auffindbar waren. Die Rechtsvergleichung wurde nach der funktionalen Methode[295] sowie, soweit möglich, unter einer *law-in-context* Betrachtung[296] vorgenommen.

2. Länder der Kategorie 1

a) Schweiz, Norwegen, Italien, Österreich, Singapur, Dänemark

In den aufgezählten Ländern muss die Etablierung eines Abmahnwesens schon an den fehlenden Auskunftsmöglichkeiten scheitern.

aa) Schweiz

Gemäß der Entscheidung *Logistep* des Schweizer Bundesgerichts vom 8. September 2010 ist es Ermittlungsfirmen in der Schweiz datenschutzrechtlich untersagt, die IP-Adressen von *filesharing*-Nutzern zu loggen.[297] Zwar kann dies nicht verhindern, dass Ermittlungsfirmen vom Ausland aus die IP-Adressen von *filesharing*-Nutzern in der Schweiz loggen; jedoch existiert kein zivilrechtlicher Auskunftsanspruch gegen ISPs. In einer Entscheidung aus dem Jahr 2014 musste daher die Staatsanwaltschaft Zürich verpflichtet werden, strafrechtliche Ermittlungen gegen die Inhaber von Anschlüssen, deren IP-Adressen ermittelt worden waren, aufzunehmen.[298] Daran zeigt sich auch, dass ein datenschutzrechtliches Ermittlungsverbot für das Bestehen oder

[295] Siehe hierzu *Van Hoecke*, Law and Method, Bd. 12, 2015, S. 9ff., 28.
[296] Siehe hierzu *Van Hoecke*, Law and Method, Bd. 12, 2015, S. 16ff., 29.
[297] BGE 136 II 508 – servat.unibe.ch.
[298] Obergericht des Kanton Zürich, Beschluss vom 3. Februar 2014, Geschäfts-Nr.: UE130087 – gerichte-zh.ch; der Rechtsbehelf entspricht dem deutschen Klageerzwingungsverfahren nach § 172 Abs.2 StPO.

Nichtbestehen eines Abmahnwesens irrelevant ist, sofern – wie in diesem Verfahren geschehen – die IP-Adressen vom Ausland aus ermittelt werden und trotz des Verstoßes gegen Datenschutzrecht nicht als unverwertbares Beweismittel betrachtet werden.

Es ist jedoch nicht ersichtlich, dass der Ermittlungsweg über das Strafverfahren weiter verfolgt wurde. Für Rechteinhaber steht der Umweg über das Strafverfahren Abmahnungen nicht grundsätzlich entgegen, macht ein echtes Abmahnwesen aber unpraktikabel, wie auch die Erfahrungen aus Deutschland zeigen.[299] Allerdings scheint sich entsprechendes in der Schweiz nicht abzuspielen. Zwar ist angesichts des Drucks aus den USA[300] derzeit eine Gesetzesnovelle in Planung, nach der die Ermittlung datenschutzrechtlich zulässig werden soll[301]; eine Änderung des Auskunftsrechts scheint aber nicht in Planung zu sein. Von daher ist davon auszugehen, dass auch in der Zukunft in der Schweiz kein Abmahnwesen entstehen kann.

Daran ändert auch die Urheberrechtsreform von 2019 nichts.[302] Gemäß dem am 1. April 2020 in Kraft getreten Art. 77i des Schweizer Urheberrechtsgesetzes dürfen Rechteinhaber zwar jetzt auch in der Schweiz selbst die IP-Adressen von *filesharing*-Nutzern loggen.[303] Jedoch ist nach dem Wortlaut der Norm die Durchsetzung der Auskunft über die Nutzerdaten im Zivilrechtswege nach wie vor versperrt und weiterhin die Einleitung eines Strafverfahrens notwendig. Folglich sind aus den genannten Gründen für die tatsächliche Praxis keine Änderungen zu erwarten.

bb) Norwegen

In Norwegen entschied der Oberste Gerichtshof am 26. April 2017, dass ISPs nur bei Nachweis schwerwiegender Urheberrechtsverletzungen Name und An-

299 Siehe Kapitel § 2 II.

300 Siehe Kapitel § 3 III.

301 *Van Der Sar*, Switzerland Hopes New Law Will Keep it Off U.S. 'Pirate Watchlist'.

302 Eines der Primärziele der Reform ist es, dass die Schweiz zukünftig nicht mehr im *Special 301 Report* des US-Handelsministeriums geführt wird, siehe *Van Der Sar*, Switzerland Urges U.S. to Remove it From its 'Pirate Watchlist'.

303 Diese Norm wurde in Reaktion auf die genannte Logistep-Entscheidung eingeführt, vgl. Seite 601 der Botschaft zur Änderung des Urheberrechtsgesetzes sowie zur Genehmigung zweier Abkommen der Weltorganisation für geistiges Eigentum und zu deren Umsetzung vom 22. November 2017, abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2018/591.pdf - Zugriff am 31.03.2021.

schrift von *filesharing*-Nutzern offenbaren müssen, praktisch also nie.[304] Ob ISPs eine entsprechende Auskunft freiwillig erteilen dürfen, ist unklar, jedoch scheint dies ohnehin keine verbreitete Praxis zu sein. Massenabmahnungen sind damit in Norwegen nicht möglich.

cc) Italien

Auch in Italien scheitert die Etablierung eines Abmahnwesens am fehlenden Auskunftsrecht. Nach einem Urteil des *Tribunale Civile di Roma* vom 14. Juli 2007 erstreckt sich der Auskunftsanspruch des italienischen Urheberrechtsgesetzes in Abwägung mit Datenschutz- und Verfassungsrecht nicht auf Name und Anschrift von *filesharing*-Endnutzern.[305]

dd) Österreich

In Österreich urteilte der OGH im Jahr 2008, dass der Inhaber eines Internetanschlusses nicht als Gehilfe für Urheberrechtsverletzungen seiner Mitnutzer angesehen werden kann; da in Österreich die Störerhaftung nicht existiert, konnte der Anschlussinhaber nicht in Anspruch genommen werden.[306] In diesem Verfahren stand die Täterschaft eines Mitnutzers fest. Ob wie in Deutschland die Täterschaft des Anschlussinhabers in Fällen, in denen die Täterschaft eines Mitnutzers nichts positiv feststeht, durch prozessrechtliche Instrumente konstituiert werden kann, konnte jedenfalls nicht mehr geklärt werden: ein Jahr später entschied der OGH, dass ISPs unter Berücksichtigung des Datenschutzrechts nicht zur Herausgabe von Name und Anschrift von Kunden verpflichtet sind, die in einem *filesharing*-System ermittelt wurden.[307] Nach den verfügbaren Informationen erteilen ISPs auch freiwillig keine Auskunft; nur aus Versehen soll dies gelegentlich vorgekommen sein, mit der Folge vereinzelter Gerichtsverfahren (mit unbekanntem Ausgang).[308] Ein echtes Abmahnwesen kann aber unter der geltenden Rechtslage nicht entstehen.

---

[304] Die Entscheidung ist bisher nicht auf Englisch oder Deutsch verfügbar; eine Besprechung findet sich bei *Maxwell*, ISP Lands Supreme Court Win Over Copyright Trolls.

[305] *Garofoli*, CRi 2007, 182.

[306] OGH Österreich, Beschluss vom 22. Januar 2008, Az. 4 Ob 194/07v – BeckRS 2008, 12291.

[307] OGH Österreich, Urteil vom 14. Juli 2009, Az. 4 Ob 41/09x – GRUR Int. 2010, 345.

[308] *Wimmer*, Auch in Österreich werden Filesharer verklagt.

ee) Singapur

In Singapur gab es bereits ab 2007 erfolgreiche Versuche, *filesharing* zu monetarisieren. Die Firma *Odex*, die als Vertriebshändler für Anime fungiert, versuchte die Kontaktinformationen zu über 3000 IP-Adressen zu erlangen, über die mittels BitTorrent von ihr lizenzierte Werke geteilt worden waren. In der ersten Instanz unterlag *Odex* noch, da das Gericht in Abwägung mit Datenschutzrecht keine Auskunft gewähren wollte. In der Berufungsinstanz erhielt sie jedoch Anfang 2008 recht. In Folge wurden die ermittelten Personen abgemahnt, ein unbekannter Anteil verglich sich auf Summen bis zu 6000 Singapur-Dollar.[309]

2015 wurden einige hundert Personen wegen eines geteilten Films abgemahnt. Als im Jahr 2017 erneut ein über Auskunftsbegehren vom Berufungsgericht zu entscheiden war, weil sich ein ISP der Auskunft verweigert hatte, entschied sich das Berufungsgericht nunmehr jedoch dafür, dass die Auskunft nicht zu gewähren sei, da die IP-Adresse kein hinreichendes Beweismittel für die Täterschaft des Anschlussinhabers sei.[310] Die Entscheidung ist mittlerweile rechtskräftig. Ein weiteres Vorgehen gegen Endnutzer in Singapur scheint damit ausgeschlossen.

ff) Dänemark

In Dänemark verpflichteten die Gerichte ISPs regelmäßig zur Auskunft[311], eine durchgehende Linie gab es jedoch nicht. ISPs weigerten in sich in neuerer Zeit häufig, Auskunft zu erteilen.[312] Zur Haftung gibt es nur wenige, ältere Entscheidungen, die meisten davon unveröffentlicht. In einer Entscheidung des Obersten Gerichtshofs aus dem Jahr 2011 wurde ein Anschlussinhaber zur Leistung von Schadensersatz verurteilt.[313] In dem Verfahren war die Täterschaft des Beklagten jedoch nicht streitig, sonder nur die Menge der Da-

309 https://en.wikipedia.org/wiki/Odex%27s_actions_against_file-sharing - Zugriff am 31.03.2021.

310 *Tham*, High Court throws out Hollywood movie piracy case.

311 Siehe beispielsweise Gericht in Frederiksberg, Entscheidung vom 11. Mai 2016, Az. BS B-2424/2015 – domstol.dk.

312 *Van Der Sar*, Danish ISPs Stand Up Against „Mafia-Like“ Copyright Trolls.

313 Oberster Gerichtshof, Urteil vom 24. März 2011, Az. 27/2009; eine Besprechung der Entscheidung findet sich bei *Jakobsen*, Kalkulation von Schadensersatz und Bewertung von Beweisen in Rechtsstreiten über illegales Filesharing.

teien, die er zum Upload zur Verfügung gestellt hatte.[314] Verurteilt wurde er wegen des öffentlichen Zugänglichmachen von 500 Musiktiteln zu einem Betrag von insgesamt (zum damaligen Kurs) umgerechnet ca. EUR 1300, also etwas über EUR 2 pro Musiktitel, was gegenüber den vom BGH in „Tauschbörse I“ gebilligten Beträgen von bis zu EUR 200 pro Titel verschwindend wenig ist.

Nach einer Entscheidung des Westlichen Obergerichts aus dem Jahr 2008 wurde die Klage gegen einen Anschlussinhaber abgewiesen, obwohl er keine Mitnutzer hatte; da er das WLAN jedoch offen Betrieb und er seiner Angabe nach zum Tatzeitpunkt nicht in seiner Wohnung anwesend war, sah das Gericht seine Täterschaft nicht als erwiesen an.[315] Allerdings vertritt eine dänische Anwaltskanzlei, die für Rechteinhaber tätig wird, dass der offene Betrieb eines WLAN mittlerweile nicht mehr üblich sei, mithin die Gerichte – sollte es zum Streitfall kommen – wohl anders entscheiden werden.[316]

Dänemark scheint also die Hypothese zu bestätigen, dass eine strenge, prozessrechtlich (oder wie auch immer) etablierte Täterschaftsvermutung bezüglich des Internetanschlussinhabers und überkompensatorische, gerichtlich gebilligte Schadenersatzforderungen notwendig sind, um ein Abmahnwesen zu etablieren, Rechteinhaber bei Fehlen dieser Instrumente und damit fehlender Profiterzielungsmöglichkeit also kein Interesse haben, Rechtsverletzungen über *filesharing*-Systeme massenhaft zu verfolgen.

Entsprechend war mit Spannung zu erwarten, ob die im Zuge der Gerichtsverfahren, die auf die Abmahnwellen seit 2015[317] hin initiiert worden waren, in Abkehr von der früheren Rechtsprechung auf Ebene der unteren Instanzen im Entstehen begriffene Annahme einer Vermutung der Täterschaft des Anschlussinhabers[318] höchstrichterlich Bestand haben würde. Dies dürfte jetzt aber irrelevant sein, da Dänemark als Testfall für diese Hypothese nunmehr

[314] Das verwendete System war *DirectConnect*, das Napster ähnlich ist. Andere Nutzer konnten auf alle Dateien, die in einem bestimmten Ordner gespeichert waren, zugreifen.

[315] Westliches Obergericht, Urteil vom 6. Oktober 2008, Az. U.2009.280V – unveröffentlicht.

[316] https://opus-law.dk/ofte-stillede-spoergsmaal/#13 - Zugriff am 31.03.2021.

[317] *Van Der Sar*, Danish ISPs Stand Up Against „Mafia-Like“ Copyright Trolls.

[318] https://bit.ly/3cbqLv2 - Zugriff am 31.03.2021.

ausscheidet. Denn mit Urteil vom 7. Mai 2018[319] hat das Östliche Obergericht einen Auskunftsanspruch in Abwägung des Urheberrechts mit dem Datenschutzrecht der Endnutzer versagt und damit die entgegenstehende Entscheidung der ersten Instanz aufgehoben. Das Oberste Gericht hat die Revision nicht zugelassen.[320] Die Entstehung eines Abmahnwesens scheidet für Dänemark daher – sollte dieses oder ein anderes Gericht von dieser Rechtsprechung nicht abweichen – in Zukunft schon mangels eines Auskunftsanspruchs aus.

b) Frankreich, Neuseeland, Südkorea, Taiwan, Irland

Diese Länder haben eine sogenannte *graduated response policy* gesetzlich oder – im Falle Irlands – gerichtlich verankert. In einem solchen System können Rechteinhaber von einem ISP grundsätzlich keine Auskunft über dessen Kunden, die *filesharing* betreiben, erlangen. Sie können ihm lediglich ermittelte IP-Adressen mitteilen. Der ISP muss nach Mitteilung den entsprechenden Nutzer verwarnen (*strike*) und nach einer gewissen Anzahl an Verwarnungen den Anschluss kündigen (und/oder der Nutzer muss eine Strafe zahlen), typischerweise nach *three strikes*, weshalb *three strikes* häufig auch als Synonym für ein solches System verwendet wird. In den USA und dem Vereinigten Königreich gibt bzw. gab es ein solches System jeweils auf Basis freiwilliger Vereinbarungen, was ein unmittelbares Vorgehen gegen Anschlussinhaber durch die Rechteinhaber jedoch nicht ausschließt bzw. ausschloss.[321]

aa) Frankreich

In Frankreich besteht ein *graduated response system* seit 2009, mit einer Besonderheit: zwischen Rechteinhaber und ISPs ist eine Behörde (mit dem Namen HADOPI, welcher auch der Name des zu Grunde liegenden Gesetzes ist) zwischengeschaltet, an die sich Erstere mit ermittelten IP-Adressen wenden müssen. Die Behörde betreibt dann das weitere Verfahren und schickt dem Anschlussinhaber einen Warnhinweis per Email. Erhält er einen drit-

[319] Östliches Obergericht, Urteil vom 7. Mai 2018, Az. 20. Div. Nr. B-2451-17; Besprechung bei *Maxwell*, ISPs Win Landmark Case to Protect Privacy of Alleged Pirates.

[320] *Maxwell*, Copyright Trolls Killed Off in Denmark After Supreme Court Hearing Denied.

[321] Siehe hierzu die Erörterungen die jeweiligen Länder betreffend.

ten Warnhinweis innerhalb eines Jahres nach einem zweiten Warnhinweis, kommt es zu einem gerichtlichem Verfahren, bei dem eine Geldbuße bis zu EUR 1500 ausgesprochen werden kann; in schwereren Fällen sind aber auch strafrechtliche Konsequenzen möglich. Die Möglichkeit, den ISP zudem zur Kündigung des Internetanschlusses zu verpflichten, wurde 2013 jedoch abgeschafft; diese Maßnahme wurde ohnehin nur ein einziges Mal ergriffen.[322] Aus dem HADOPI-Bericht von 2017 geht überdies hervor, dass insgesamt nur sehr wenige Strafen verhängt wurden: zwar gab es zwischen 2012 und 2017 ca. neun Millionen erste Warnungen/*first strikes*, seit Schaffung der Behörde im Jahr 2009 wurden aber insgesamt „nur" 394 Geldbußen verhängt und 189 strafrechtliche Verurteilungen ausgesprochen.[323]

Es gab Pläne, die Behörde HADOPI aufzulösen und ihre Aufgaben an die französische Rundfunkaufsichtsbehörde zu übertragen, diese wurden jedoch aufgegeben.[324] Das zu Grunde liegende Gesetz wurde von vielen Seiten als unbefriedigend empfunden und zunächst mehrfach überarbeitet, ohne jedoch größere Änderungen zu erfahren.[325] Die französische Nationalversammlung hat allerdings im Jahr 2016 beschlossen, dass das gesamte HADOPI-System bis 2022 aufgelöst werden soll.[326] Grund dürften die Kosten der Behörde sein, die immer wieder als zu hoch im Verhältnis zu den wenigen verhängten Sanktionen kritisiert wurden.[327] Was nach dem HADOPI-System kommt, ist bisher ungewiss.

bb) Neuseeland

In Neuseeland wurde im Jahr 2011 ein *graduated response system* etabliert. Diesem zu Folge muss ein ISP nach Versand einer dritten Verwarnung das sogenannte *Copyright Tribunal* anrufen, das sodann – unter Geheimhaltung der Identität des Anschlussinhabers – über dessen Sanktionierung entscheidet. Als Sanktion können „Geldbußen" verhängt werden. Internetsperren sieht das Gesetz als Möglichkeit grundsätzlich vor, jedoch nur, wenn eine entsprechende Verordnung von der zuständigen Behörde erlassen wird, was

322 *Meyer*, The Politics of Online Copyright Enforcement in the EU: Access and Control, S. 169f.
323 *Maxwell*, Seven Years of Hadopi: Nine Million Piracy Warnings, 189 Convictions.
324 *Champeau*, Le transfert Hadopi - CSA n'est „plus l'axe prioritaire".
325 *Schiff*, 16 Cardozo J. Conflict Resol. 909, 914f. (2014).
326 *Van Der Sar*, National Assembly 'Kills' French Three-Strikes Anti Piracy Law.
327 *Heidrich/Brinkert*, DSRITB 2013, 461, 467.

bisher nicht geschehen ist.[328] Die „Geldbußen“ beinhalten aber tatsächlich Entschädigungszahlungen an den betroffenen Rechteinhaber, wobei als schadensersatzähnliche Kompensation regelmäßig ca. 200 Neuseeland-Dollar und als strafschadensersatzähnliche Buße ca. 250 Neuseeland-Dollar sowie weitere Zahlungen für die Rechtsverfolgungskosten des Rechteinhabers zugesprochen werden.[329] Dies entspricht umgerechnet ca. EUR 300. Weiterhin haftet der Anschlussinhaber für diese Summe auch unabhängig davon, ob er selbst der Täter ist oder einer seiner Anschlussmitnutzer.[330]

Nur diese beiden Umstände betrachtet, bestünden in Neuseeland nach der Hypothese dieser Arbeit hervorragende Voraussetzungen für die Entstehung eines Abmahnwesens. Jedoch stehen dem die Regeln der Sec. 122D, 122E und 122F des *Copyright (Infringing File Sharing) Amendment Act 2011*[331] entgegen: Demnach darf die zweite Verwarnung nur versandt werden, wenn seit Versand der ersten Verwarnung mindestens 28 Tage, höchstens jedoch neun Monate vergangen sind, und in diesen Zeitraum über den betroffenen Anschluss ein Werk des Rechteinhabers verletzt wurde, der auch schon Betroffener derjenigen Verletzung war, die zur ersten Verwarnung geführt hat. Das gleiche Zeitfenster gilt wiederum für die dritte Verwarnung. Bis es also überhaupt zu einem Verfahren vor dem Copyright Tribunal kommen kann, muss dreimal derselbe Rechteinhaber betroffen gewesen sein und dies für die zweite und dritte Rechtsverletzung auch jeweils innerhalb eines bestimmten Zeitfensters. Zum Vergleich: in Deutschland kann eine Abmahnung bereits nach einer ersten registrierten Verletzung versandt werden und auch bereits dann der Schadensersatz eingeklagt werden.

Die Wahrscheinlichkeit, dass die genannten Voraussetzungen in einer nennenswerten Anzahl an Fällen erfüllt sind, ist offensichtlich sehr gering, und zwar auch dann, wenn der Anschlussinhaber Mitnutzer hat, deren *filesharing*-Konsum er nicht kontrollieren kann. Entsprechend sind – Stand 2017 – seit der Schaffung des Systems im Jahr 2011 auch nur 17 Entscheidungen

[328] *Austin*, Common Law Pragmatism: New Zealand's Approach to Secondary Liability of Internet Service Providers, S. 213, 221ff.

[329] Siehe exemplarisch [2013] NZCOP 16 - COP 006/13, Rz. 25ff.; abrufbar unter https://www.justice.govt.nz/tribunals/copyright/decisions/copyright-decisions/?Filter_Jurisdiction=25 - Zugriff am 31.03.2021.

[330] Siehe exemplarisch wiederum [2013] NZCOP 16 - COP 006/13, Rz. 12.

[331] Abrufbar unter http://www.legislation.govt.nz/act/public/2011/0011/latest/DLM2764327.html - Zugriff am 31.03.2021.

ergangen.[332]

Das neuseeländische Urheberrecht soll reformiert werden, das *graduated response system* wird hiervon aber nicht betroffen sein.[333] Im Ergebnis ist daher nach neuseeländischem Recht die Entstehung eines Abmahnwesens ausgeschlossen.

cc) Südkorea

In Südkorea wurden ab 2005 gegen mehr als 13.000 *filesharing*-Nutzer Strafverfahren eingeleitet; die Strafverfolgungsbörden entschieden jedoch, nur gegen gewerblich handelnde Nutzer vorzugehen, weshalb alle Verfahren eingestellt wurden.[334] Über einen zivilrechtlichen Auskunftsanspruch ist nichts bekannt.

Ohnehin: seit 2009 existiert ein *graduated response*-System. Das System wird unter der Aufsicht einer Behörde ausgeführt. Als Sanktion nach der dritten Verwarnung ist „lediglich“ die Sperrung des betroffenen Anschlusses vorgesehen.[335] Die Zahl der ausgesprochenen Verwarnungen ist im Verhältnis zur Zahl der letztlich verhängten Sanktionen – wie in Frankreich auch – enorm hoch. Nach dem letzten bekannten Stand aus dem Jahr 2012 wurden zwar seit 2009 insgesamt über 468.000 Verwarnungen ausgesprochen, aber „nur“ 408 Internetanschlüsse gesperrt.[336] In der öffentlichen Wahrnehmung Südkoreas wird die Sanktion der Internetsperre darüber hinaus als unverhältnismäßig empfunden, das System ist dort folglich starker Kritik ausgesetzt.[337] Änderungen wurden bisher allerdings nicht vorgenommen.

dd) Taiwan

Auch in Taiwan ist seit 2009 ein *graduated response system* gesetzlich vorgesehen, bei dem nach einer dritten Verwarnung der betroffene Anschluss gesperrt werden soll. Die praktische Implementierung steht jedoch noch aus.[338]

---

[332] *Austin*, Common Law Pragmatism: New Zealand's Approach to Secondary Liability of Internet Service Providers, S. 213, 226.
[333] *Maxwell*, New Zealand Prepares Consultation to Modernize Copyright Laws.
[334] *Leitner*, 22 Colum. J. Asian L. 1, 1, 24 (2008).
[335] *Moon/Kim*, 6 Wash. J.L. Tech. & Arts 171, 173ff. (2011).
[336] *Schiff*, 16 Cardozo J. Conflict Resol. 909, 912 (2014).
[337] *Heidrich/Brinkert*, DSRITB 2013, 461, 469.
[338] *Elton*, MEIEA, Nr. 1, Bd. 14, 2014, S. 89, 109f.

Entsprechend wurden auch noch keine Sanktionen verhängt.

ee) Irland

In Irland war die rechtliche Möglichkeit einer Auskunftsanordnung mittels einer *Norwich pharmacal order*[339] seit einer Entscheidung des Obersten Gerichtshofes im Jahr 1993 grundsätzlich anerkannt.[340] Zwischen 2005 und 2007 wurden daher auch ISPs in einigen erstinstanzlichen Entscheidungen zur Auskunft über die Kontaktdaten insgesamt einiger dutzend Kunden, über deren Anschluss *filesharing* betrieben worden war, verpflichtet. Gegen drei der Abgemahnten wurden Verfahren eingeleitet, wobei jedoch zwei vom Gericht als nicht haftbar angesehen wurden; mit dem Dritten wurde ein Vergleich geschlossen. Mit den übrigen Abgemahnten wurden außergerichtliche Vergleiche geschlossen. Die Einnahmen aus den Vergleichen blieben weit unter den Kosten für die Abmahnungen.[341] Ab 2008 gaben die Rechteinhaber das unmittelbare Vorgehen gegen Endnutzer – wohl deshalb – auf. Stattdessen wurde versucht, sich mit den ISPs darauf zu einigen, ein *graduated response system* freiwillig einzurichten.[342]

Warum nicht weiter versucht wurde, gegen Endnutzer unmittelbar vorzugehen, ist nicht ersichtlich, insbesondere nicht, ob auch für die Zukunft prognostiziert wurde, dass die aus Vergleichen und gerichtlichem Vorgehen erzielten Einnahmen unter den Kosten des Vorgehens bleiben würden. Mithin ist auch unklar, wie die irischen Gerichte die entscheidenden Fragen – Täterschaft und Schadenshöhe – beantwortet hätten. Folglich kann Irland auch nicht als Land der Kategorie 3 eingestuft werden. Vielleicht sahen die Rechteinhaber keine Aussicht darauf, mit dem Vorgehen gegen Endnutzer Profit erzielen zu können, vielleicht war ihnen aber auch die Idee dazu noch gar nicht gekommen. Schließlich zeichnete sich auch in Deutschland und (mit Einschränkungen) den USA[343] – also den beiden Ländern, in denen mit einem solchen Vorgehen Profit erzielt wird – erst ab dem Jahr 2010 ab, dass die Rechtsprechung ein solches Vorgehen billigen würde.

339 Siehe hierzu Kapitel § 3 XII. 4.

340 Supreme Court Ireland, Megaleasing v Barrett [1993] ILRM 497.

341 High Court of Ireland, EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd, [2010] IEHC 377, Rz. 62-64 – bailii.org.

342 *Kelly*, Journal of Intellectual Property Law & Practice, Nr. 3, Bd. 11, 2016, S. 183, 185

343 Siehe hierzu Kapitel § 3 XII. 6.

Jedenfalls zeigten sich die meisten ISPs für die Einrichtung eines *graduated response system* offen. Die irische Datenschutzbehörde hatte zwar versucht, das System zu verbieten, wurde jedoch vom Irischen Obersten Gerichtshof aufgehoben.[344] Da sich der ISP *UPC* allerdings der Teilnahme an dem System verweigerte, versuchten die Rechteinhaber die Implementierung eines solchen Systems durch UPC gerichtlich zu erzwingen. Dieses Vorhaben scheiterte zunächst: das Hohe Gericht lehnte einen dahingehenden Anspruch mangels einer einschlägigen Anspruchsgrundlage ab, erkannte aber zugleich an, dass die europarechtlichen Vorgaben zum Schutz des geistigen Eigentums in Irland nur unzureichend umgesetzt worden waren.[345] Eine Anpassung des irischen Urheberrechts an die europarechtlichen Vorgaben trat 2012 in Kraft.[346]

Der Wortlaut in Sec. 40 (5A) des Copyright and Related Rights Act 2000 sieht nunmehr vor, dass von Intermediären wegen Urheberrechtsverletzungen eine *injunction* verlangt werden kann. Rechtinhaber versuchten auf dieser Basis im Jahr 2014 erneut, UPC zur Implementierung des *graduated response system* zu zwingen. Das Hohe Gericht gab ihnen dieses mal recht. Insbesondere sah es – ganz in der Tradition des *common law* – kein Problem darin, allein auf den Wortlaut „*injunction*“ gestützt, die Implementierung eines ausdifferenzierten *graduated response system* vorzuschreiben.[347] Hervorzuheben ist, dass das Gericht es insbesondere als nicht sachgerecht ansah, die Rechteinhaber auf Auskunftsanordnungen betreffend der Anschlussinhaber und ein darauf folgendes Vorgehen mittels Abmahnungen zu verweisen, da ein solches Vorgehen einen unverhältnismäßigen Aufwand für die dann jeweils befassten Gerichte darstellen würde.[348] Die Entscheidung wurde 2016 vom (in dieser Sache als letzte Instanz fungierenden) Irischen Berufungsgericht bestätigt[349] und ist damit bindend.

---

344 *Van Der Sar*, Irish Supreme Court Okays Three-Strikes Anti-Piracy Scheme.

345 High Court of Ireland, EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd, [2010] IEHC 377, Rz. 138 – bailii.org.

346 *Kelly*, Journal of Intellectual Property Law & Practice, Nr. 3, Bd. 11, 2016, S. 183, 192.

347 High Court of Ireland, Sony Music Entertainment (Ireland) Limited & Ors -v- UPC Communications Ireland Limited (No. 1), [2015] IEHC 317, Rz. 244 – bailii.org.

348 High Court of Ireland, Sony Music Entertainment (Ireland) Limited & Ors -v- UPC Communications Ireland Limited (No. 1), [2015] IEHC 317, Rz. 167, 232ff. – bailii.org

349 Irish Court of Appeal, Sony Music Entertainment Ireland Ltd & Ors -v- UPC Communications Ireland Ltd, [2016] IECA 231 – bailii.org.

Auf Basis der Entscheidung dürfen Rechteinhaber nach einer dritten Verwarnung verlangen, dass der ISP ihnen Name und Anschrift des entsprechenden Anschlussinhabers mitteilt. Sodann dürfen sie verlangen, dass diesem der Internetanschluss gekündigt wird. Zudem dürfen sie aber auch unmittelbar selbst gegen den Anschlussinhaber vorgehen.[350] Theoretisch könnte damit auch innerhalb dieses *graduated response systems* – ähnlich wie in Neuseeland – ein Abmahnwesen etabliert werden. Jedoch erscheint es unwahrscheinlich, dass es ein Anschlussinhaber auf eine dritte Verwarnung ankommen lassen wird, zudem sind zivilrechtlich die Fragen der Täterschaft und Schadenshöhe nicht geklärt.

Die Etablierung eines Abmahnwesens scheidet nach hiesiger Wertung in Irland also auf Grund des Fehlens einer nach Auffassung des Verfassers hierfür notwendigen Rechtslage aus. Gegenwärtig verfolgen Rechteinhaber in Irland entsprechend stattdessen die gerichtlich verordnete Implementierung von *graduated response systems* weiter.[351] Seit dem Frühjahr 2019 hat ein Großteil der in Irland tätigen ISPs ein entsprechendes System implementiert.[352]

3. Länder der Kategorie 2

In den Ländern Niederlande, Schweden, Finnland, Spanien, Polen, Australien und Kanada ist ein Auskunftsanspruch gegen ISPs betreffend *filesharing*-Nutzern nicht kategorisch ausgeschlossen, jedoch existiert ein Abmahnwesen mangels Klärung der sonstigen rechtlichen Voraussetzungen bisher noch nicht. Die weiteren Entwicklungen sind abzuwarten.

a) Niederlande

Zwar haben die Niederlande den Art. 8 EnforcementRL durch einen zivilrechtlichen Auskunftsanspruch umgesetzt[353]; ob ISPs hinsichtlich Name und Anschrift der Endnutzer von *filesharing*-Systemen ausnahmslos zur Auskunft verpflichtet sind, ist bisher allerdings gerichtlich nicht abschließend geklärt. Es gibt vereinzelte Instanzrechtsprechung, die ISPs zur Auskunft verpflich-

350 *Kelly*, Journal of Intellectual Property Law & Practice, Nr. 3, Bd. 11, 2016, S. 183.
351 *Maxwell*, Sony, Universal and Warner Ask Sky to Disconnect Pirate Subscribers.
352 *Maxwell*, Vodafone Will Implement 'Three-Strikes' For Pirates.
353 *Cumming/Freudenthal/Janal*, Enforcement of Intellectual Property Rights in Dutch, English and German Civil Procedure, S. 114ff.

tet oder eine Auskunftsverpflichtung verneint[354], jedoch keine dahingehend zwingende Entscheidung des Obersten Gerichts.[355] Seit 2005 haben Rechteinhaber immer wieder angekündigt, gegen Endnutzer vorgehen zu wollen, woraufhin ISPs im Gegenzug ankündigten, keine Auskunft erteilen zu werden.[356]

Warum bisher keine gerichtliche Anspruchsdurchsetzung gegen Endnutzer, über die Auskunft erlangt werden konnte, versucht wurde, konnte vom Verfasser nicht aufgeklärt werden. An der Urheberrechtslage im Übrigen kann es nicht gelegen haben. Zwar galt in den Niederlanden bis 2014 die Privatkopieschranke ohne Ansehung der Rechtmäßigkeit der Quelle[357], die öffentliche Zugänglichmachung war hiervon jedoch nicht betroffen.

Ob auf die neuste Ankündigung, gegen Endnutzer vorgehen zu wollen[358], auch Taten folgen werden, bleibt abzuwarten.

b) Schweden

In Schweden gab es zunächst keine zu Deutschland parallele Entwicklung. Lediglich ein Urteil aus dem Jahr 2011 ist bekannt, in dem ein *filesharer* zu EUR 229 Schadensersatz für das öffentliche Zugänglichmachen von 44 Musiktiteln verurteilt wurde.[359] Als im Jahr 2016 eine Abmahnwelle angekündigt worden war, zog die verantwortliche Kanzlei nach einem großen Medienecho und öffentlichen Aufschrei ihr Mandat zurück.[360] Über eine andere Kanzlei wurde in den Jahren 2016 und 2017 jedoch Auskunft über Daten tausender Nutzer verlangt.[361] Ein ISP hat sich der Auskunft verweigert, ist aber erstinstanzlich zur Erteilung verpflichtet worden; er hat jedoch Berufung angekündigt und möchte eine Vorlage an den EuGH erreichen.[362] Erste

[354] *Van Der Sar*, Dutch ISP Does Not Have to Expose Alleged Pirates, Court Rules.

[355] *Stamatoudi*, ACTA, internet service providers and the acquis communautaire, S. 237, 257.

[356] *Liggenga*, Dutch anti-piracy unit targets ISPs; *Maxwell*, Dutch Film Distributor to Target BitTorrent Users For Cash 'Fines'.

[357] Diese Rechtslage befand der EuGH mit Urteil vom 10. April 2014, Rs. C-435/12 – ECLI:EU:C:2014:254 - „ACI Adam“ für europarechtswidrig.

[358] *Maxwell*, Dutch Film Distributor to Target BitTorrent Users For Cash 'Fines'.

[359] https://bit.ly/2KCDa0t - Zugriff am 31.03.2021.

[360] *Maxwell*, Copyright Trolls Abandon Sweden in a Blaze of Bad Publicity.

[361] *Maxwell*, ISP Bombarded With 82,000+ Demands to Reveal Alleged Pirates.

[362] *Van Der Sar*, ISP Wants EU Court Ruling on Identifying „Pirating“ Subscribers; siehe zu den Implikationen einer solchen Vorlage Kapitel § 2 III. 1. e).

Verurteilungen von Anschlussinhabern auf Grund dieser Abmahnungen stehen jedenfalls noch aus, die weitere Entwicklung bleibt daher abzuwarten. Die Zahl der von Auskunftsbegehren betroffenen IP-Adressen ist seit 2016 – Stand März 2021 – jedenfalls enorm angestiegen.[363]

c) Finnland

In Finnland sollen ISPs erstmals seit 2013 durch das zuständige Marktgericht zur Auskunft verpflichtet worden sein. Zwischen 2013 und 2017 sollen hiervon knapp 200.000 Anschlussinhaber betroffen gewesen sein, wobei das Gros der Auskunftsbegehren allerdings erst auf die Jahre ab 2015 fällt.[364] Da es sich hierbei um eine neue Entwicklung handelt, kann noch nicht bewertet werden, ob sich eine ähnliche Situation wie in Deutschland entwickeln wird. In einer Entscheidung im Sommer 2017 änderte das Marktgericht erstmals seine Rechtsprechung und versagte die Auskunft, da die vom Ermittlungsdienst dargestellte Teilnahme des fraglichen Nutzers in einem BitTorrent-Schwarm nicht die Schwere der Verletzung beweise, die für eine Auskunftsverpflichtung erforderlich wäre.[365] Ende 2018 kündigte ein großer Inkasso-Dienstleister an, in Zukunft keine Forderungsbeitreibung wegen *filesharing* mehr durchzuführen.[366] Die weiteren Entwicklungen bleiben daher offen.

d) Spanien

Die Gesetzeslage, wie sie noch dem EuGH-Urteil „Promusicae“ zu Grunde lag[367], war bereits kurze Zeit nach Verkündung des Urteils überholt. Art. 12 des Ley 34/2002 wurde durch das Änderungsgesetz Ley 56/2007[368] dahingehend modifiziert, dass eine Herausgabe von Name und Anschrift eines Anschlussinhabers kein Strafverfahren mehr voraussetzt, sondern auch bei einfachen Verletzungen geistigen Eigentums verlangt werden kann. Jedoch wurde erst im Jahr 2014 durch eine Änderung des Art. 256 der spanischen

363 *Van Der Sar*, BitTorrent 'Copyright Troll' Lawsuits Skyrocket In Sweden; *Maxwell*, Copyright Trolls Targeted 46,200+ Alleged BitTorrent Pirates in Sweden During 2020.

364 *Van Der Sar*, Copyright Trolls Obtained Details of 200,000 Finnish Internet Users.

365 *Van Der Sar*, ISP Doesn't Have to Expose Alleged BitTorrent Pirates, Finnish Court Rules.

366 *Van Der Sar*, Piracy Debt Collectors Back Off After Massive Backlash in Finland.

367 Siehe Kapitel § 2 III. 1. a).

368 https://www.boe.es/buscar/act.php?id=BOE-A-2007-22440 - Zugriff am 31.03.2021.

Zivilprozessordnung mittels der Ley 21/2014 gesetzlich bestimmt, dass ein Zivilgericht gegen ISPs entsprechende Auskunftsanordnungen erlassen kann.[369]

Vor der Gesetzesänderung hatten Rechteinhaber vor dem Berufungsgericht in Barcelona einen Anspruch gegen ISPs dahingehend erstritten, dass letztere – wenn sie auch nicht die Kontaktdaten von Anschlussinhabern herausgeben müssen – diesen zumindest kündigen müssen, wenn über deren Anschluss *filesharing* betrieben wird.[370] Die Entscheidung wurde in der Literatur jedoch heftig kritisiert[371] und es ist auch nichts dazu ersichtlich, dass in nennenswertem Umfang versucht wurde, diesen Anspruch durchzusetzen.

Stattdessen wurde im Jahr 2016 vor dem Handelsgericht Nr.1 in Bilbao erstmals von der Möglichkeit Gebrauch gemacht, eine Auskunftsanordnung zu erwirken und die Anschlussinhaber daraufhin abzumahnen.[372]

Im November 2017 wurde sodann erstmals eine darauf gestützte Klage gegen einen Anschlussinhaber wegen *filesharing* verhandelt, aber abgewiesen.[373] Das Gericht sah die Täterschaft des Anschlussinhabers wegen der Möglichkeit der Täterschaft eines Mitnutzers als nicht erwiesen an; eine zivilprozessuale Fiktion der Täterschaft wie in Deutschland kam folglich nicht zur Anwendung. Zudem lehnte das Gericht die Annahme des (nach spanischen Rechts erforderlichen) Vorsatzes ab, da bei BitTorrent-Clients automatisch geteilt werde, weshalb ein Wille zur Tat nicht zwingend angenommen werden könne.[374]

Da es sich hierbei um den ersten bekannten Fall dieser Art handelt und

[369] https://www.boe.es/buscar/doc.php?id=BOE-A-2014-11404 - Zugriff am 31.03.2021.

[370] Berufungsgericht in Barcelona, Promusicae et al v. R Cable y Telecomunicaciones Galicia, Urteil vom 18. Dezember 2013, Az. 470/2013, abrufbar unter http://estaticos.elmundo.es/documentos/2014/01/20/SentenciaAP.pdf - Zugriff am 31.03.2021. Zur Rechtslage betreffend solcher Ansprüche in den USA siehe Kapitel § 3 XII. 6.

[371] *Husovec/Peguera*, IIC 2015, 10, 27ff.

[372] Handelsgericht Nr.1 in Bilbao, Vorläufige Entscheidung vom 3. April 2016, Az. 890/2016-E; Bericht über die Entscheidung und Abmahnungen – in Spanisch – auf https://bit.ly/2VRCz1R - Zugriff am 31.03.2021.

[373] Handelsgericht Nr.1 in Donostien, Az. 239/17; Bericht hierüber – in Spanisch – auf https://www.genbeta.com/actualidad/la-primera-sentencia-en-espana-sobre-el-uso-de-p2p-absuelve-al-demandado - Zugriff am 31.03.2021.

[374] *Van Der Sar*, Dallas Buyers Club Loses Piracy Lawsuit, IP-Address is Not Enough.

er bisher nur erstinstanzlich entschieden ist, bleibt abzuwarten, ob sich die Rechtsprechung in Spanien ähnlich wie in Deutschland entwickeln wird oder nicht.

e) Polen

In Polen ist die Gesetzeslage gegenwärtig ähnlich wie die in Deutschland bis 2008, d.h. nur im Wege des Strafverfahrens können Name und Anschrift von Anschlussinhabern erlangt werden. Folglich sind auch nur vereinzelte Fälle bekannt, bei denen Letztere in Anspruch genommen wurden. Allerdings scheint es keine Bagatellgrenze zu geben und Staatsanwälte nehmen allein bei Hinweis auf eine IP-Adresse bereits Ermittlungen auf. Dieser Umstand war im Jahr 2016 auch Gegenstand von Diskussionen im Parlament, bisher scheint sich an dieser Praxis jedoch nichts geändert zu haben.[375] Ob die Rechtslage ausreicht, ein Abmahnwesen zu etablieren, bleibt also abzuwarten.

f) Australien

In Australien hatte die Urheberrechtsindustrie zunächst versucht, ISPs über den Zivilrechtsweg zu zwingen, ihren Kunden, die *filesharing* betreiben, den Providervertrag zu kündigen – wie auch in Irland, Spanien und gegenwärtig den USA. Der *High Court* lehnte dieses Ansinnen jedoch in einer Entscheidung aus 2012 ab.[376]

Im Nachgang versuchte die Urheberrechtsindustrie sodann, direkt gegen Endnutzer vorzugehen. Auf Ebene des *Federal Court* wurde ihr 2015 in mehreren Entscheidungen das Recht zugesprochen, von den ISPs die Kontaktdaten der Anschlussinhaber, denen die jeweiligen IP-Adressen zugeordnet waren, die in einem *filesharing*-Netzwerk ermittelt worden waren, heraus zu verlangen. Jedoch behielt sich das Gericht vor, die Zulässigkeit der geplanten Abmahnschreiben von seiner Genehmigung abhängig zu machen und verlangte zudem eine Sicherheit von 600.000 australischen Dollar. Es befürchtete insbesondere, dass das betroffene Unternehmen Schadensersatz geltend machen werde, der den Kauf einer einzelnen Kopie der betroffenen Werke

375 *Maxwell*, Police Seize Hundreds of Computers Over Pirate Movie Download in 2013.
376 High Court of Australia [2012] HCA 16 – eresources.hcourt.gov.au.

erheblich übersteigt.[377] Das Unternehmen sah in Folge davon ab, gegen die betroffenen Endnutzer vorzugehen.[378]

Jedoch hat die Urheberrechtsindustrie angekündigt, in Zukunft dennoch gegen Endnutzer vorgehen zu wollen.[379] Die weiteren Entwicklungen bleiben daher abzuwarten.

g) Kanada

In Kanada plante die Musikindustrie in den frühen 2000er-Jahren eine Kampagne nach dem Vorbild in den USA[380]: einige *filesharer* sollten vor Gericht zur Verantwortung gezogen werden, als abschreckendes Beispiel.[381]

Ein Auskunftsanspruch gegen ISPs ist im kanadischen Recht als *Norwich Pharmacal order*[382] grundsätzlich vorgesehen.[383] Jedoch lehnte ein mit dem Auskunftsbegehren der Musikindustrie befasstes Bundesgericht einen Auskunftsanspruch ab, insbesondere, da weder hinreichend aufgezeigt worden sei, dass die IP-Adresse einen ausreichenden Nachweis der Täterschaft des Anschlussinhabers biete noch, dass *filesharing* (nach der damaligen Rechtslage) überhaupt eine Urheberrechtsverletzung darstelle.[384] Mithin würde das Auskunftsbegehren nicht dem sogenannten *prima facie*-Test standhalten.[385] Nach Auffassung des Berufungsgerichts sei jedoch der *prima facie*-Test nicht anzuwenden; stattdessen sei nur ein *bona fide*-Anspruch darzulegen, mithin lediglich glaubhaft zu machen, dass ein Anspruch gegen die Endnutzer, über die Auskunft beansprucht wird, nicht ausgeschlossen erscheint und ernsthaft verfolgt werden soll.[386] Desweiteren sei bei *filesharing* eine Urheberrechtsverletzung nicht auszuschließen.[387] Jedoch sei im konkreten Fall das Auskunftsbegehren nicht begründet, da – wegen Zeitablaufs – bei den betroffenen ISPs

[377] *Webb/Key-Matuszak*, Implications of the Dallas Buyers Club v iiNet decisions.
[378] *Maxwell*, Dallas Buyers Club Gives Up Chasing Pirates in Australia.
[379] *Maxwell*, Healthy Aussie Pirates Set To Face Cash 'Fines', Poor & Sick Should Be OK.
[380] Siehe hierzu Kapitel § 3 XII. 6.
[381] *Giovanella*, Effects of Culture on Judicial Decisions: Personal Data Protection vs. Copyright Enforcement, S. 65, 77.
[382] Siehe zu diesem Institut Kapitel § 3 XII. 4.
[383] Federal Court, [2004] 3 FC 241, Rz. 10 – canlii.org.
[384] Federal Court, [2004] 3 FC 241, Rz. 20ff. – canlii.org.
[385] Federal Court, [2004] 3 FC 241, Rz. 13ff. – canlii.org.
[386] Federal Court of Appeal, [2005] 4 FCA 193, Rz. 34 – canlii.org.
[387] Federal Court of Appeal, [2005] 4 FCA 193, Rz. 46ff. – canlii.org

die Zuordnung der streitgegenständlichen IP-Adressen zu den Endnutzern im Verletzungszeitpunkt mittlerweile gelöscht worden war.[388]

Unabhängig von diesen Geschehnissen wurde ein sogenanntes *notice and notice system* gesetzlich verankert, das – ähnlich einem *graduated response system* – ISPs dazu verpflichtet, an Endnutzer, über deren Anschluss *filesharing* betrieben worden war, Warnbriefe zu versenden. Da Rechteinhaber über den Inhalt der Warnbriefe bestimmen konnten, wurde vereinzelt versucht, durch die Suggestion einer unvermeidlichen Haftung die Anschlussinhaber dazu zu bewegen, freiwillig an den jeweiligen Rechteinhaber heranzutreten und einen Vergleich zu schließen.[389] Es ist jedoch nicht bekannt, dass dieses Vorgehen erfolgreich war, insbesondere, da die Betroffenen wohl auf Grund der Medienberichterstattung vor diesem Vorgehen gewarnt waren. Seit Ende 2018 dürfen auf Grund einer Gesetzesreform in den Warnbriefen auch keine Geldforderungen mehr gestellt oder Vergleichsangebote mehr gemacht werden.[390] Im Übrigen ist das *notice and notice system* mit einem „echten" *graduated response system* wie in den genannten Ländern der Kategorie 1 allerdings ohnehin nicht vergleichbar, da es weder Sanktionen ermöglicht noch Auskunftsbegehren gegen ISPs über Kundendaten ausschließt.[391]

Auskunft über Kundendaten wurde in Folge der oben genannten Entscheidung des Berufungsgerichts daher auch vereinzelt begehrt und erteilt, beispielsweise in den Jahren 2011[392], 2012[393] und 2014[394]. Zivilrechtliche Klagen wurden auf Grund des Auskunftsbegehrens von 2011 jedoch nur vereinzelt eingereicht und zudem auch wieder zurückgenommen.[395] Über Klagen auf Grundlage der Auskunftsbegehren von 2012 und 2014 ist nichts bekannt. Vereinzelt wurden bis 2016 außergerichtliche Vergleiche geschlossen.[396] Eine Zunahme der Abmahnungen wurde erwartet, da Rechteinhaber im Jahr 2017 vor dem kanadischen Berufungsgericht erstritten hatten, dass sie den ISPs deutlich weniger Kosten als bisher für die Erfüllung des Auskunftsbegehrens

388 Vgl. Federal Court of Appeal, [2005] 4 FCA 193, Rz. 43 – canlii.org.
389 *Geist*, Rightscorp and BMG Exploiting Copyright Notice-and-Notice System: Citing False Legal Information in Payment Demands.
390 *Maxwell*, Canada Prohibits Piracy Settlement Demands in ISP Copyright Notices.
391 *Hoffmann*, 15 I.E.C.L.C. 1, 1, 4 (2015).
392 Federal Court, [2011] CF 1024 – canlii.org.
393 *Maxwell*, Canada Set For Mass BitTorrent Lawsuits, Anti-Piracy Company Warns.
394 Federal Court, [2014] FC 161 – canlii.org.
395 *Geist*, Canadian Hurt Locker Lawsuits Withdrawn.
396 *McKiernan*, Focus: Feds must take action on copyright trolls.

erstatten müssen.[397] Jedoch hat auf die Revision hin der *Supreme Court* die Kostentragungslast mittlerweile wieder mehr Richtung Rechteinhaber verschoben.[398]

Ob im Ergebnis in Zukunft auch mit Gerichtsverfahren zu rechnen ist, die tatsächlich ausgefochten werden, erscheint – wie die mehrfach ohne gerichtliche Konsequenzen gebliebenen „Testläufe" gezeigt haben – eher unwahrscheinlich. Die kanadische Literatur ist jedenfalls skeptisch, ob sich ein Abmahnwesen etablieren kann, da insbesondere zu erwarten ist, dass auf Grundlage des kanadischen Schadensersatzrechts nur geringe Beträge zugesprochen werden können.[399] Überdies hat der *Supreme Court* in der soeben zitierten Entscheidung *obiter dictum* in Zweifel gezogen hat, dass der bloße Nachweis der Urheberrechtsverletzung auch zu einer Verurteilung des Anschlussinhabers als Täter ausreichen kann.[400]

Der Ausgang der in 2019 und 2020 losgetretenen Klagewellen[401] bleibt daher abzuwarten.

h) Brasilien

Ende 2020 wurde bekannt, dass auch in Brasilien mehrere Tausend Anschlussinhaber abgemahnt worden waren, nachdem 2019 zwei Gerichte – eines in Rio de Janeiro, eines in Sao Paulo – ISPs zur Auskunftserteilung verurteilt hatten.[402] Zum Stand der Bearbeitung (März 2021) ist allerdings nicht bekannt geworden, dass dies bereits Gerichtsverfahren gegen Anschlussinhaber zur Folge gehabt hätte. Die weiteren Entwicklungen sind daher abzuwarten.

---

397 *Jackson*, Copyright ruling called 'bad news for consumers, bad news for Canada'.

398 Rogers Communications Inc. v. Voltage Pictures, LLC, 2018 SCC 38, [2018] 2 S.C.R. 643 – scc-csc.lexum.com.

399 *Geist*, Why Copyright Trolling in Canada Doesn't Pay: Assessing the Fallout From the Voltage – TekSavvy Case.

400 Rogers Communications Inc. v. Voltage Pictures, LLC, 2018 SCC 38, [2018] 2 S.C.R. 643, Rz. 41 – scc-csc.lexum.com.

401 *Van Der Sar*, Movie Studios Are Suing Canadian BitTorrent Users, But That's Nothing New; *Maxwell*, Movie Companies File Lawsuits in Canada Targeting 3,348 Alleged BitTorrent Pirates.

402 *Van Der Sar*, 'Copyright Trolls' Enter Brazil Demanding Money from Suspected Pirates.

i) Belgien

In Belgien ist ein Auskunftsverfahren vor dem *Ondernemingsrechtbank Antwerpen* auf Grund dessen Vorlage an den EuGH[403] gegenwärtig ausgesetzt. Da das Verfahren spezifisch einen Urheberrechtstroll[404] zum Gegenstand hat, ist unabhängig von der noch ausstehenden Entscheidung des EuGH abzuwarten, ob in Belgien in Zukunft Auskünfte erteilt werden und mithin der Grundstein für ein mögliches Abmahnwesen gelegt wird.

4. Land der Kategorie 3: Vereinigtes Königreich?

Länder der Kategorie 3 sollten nicht existieren, sofern die rechtlichen Voraussetzungen für ein Abmahnwesen zutreffend identifiziert wurden und davon ausgegangen werden kann, dass privatwirtschaftliche Akteure im Regelfall immer die vorhandenen rechtlichen Möglichkeiten ausschöpfen, sofern sie nicht aus sonstigen (zum Beispiel politischen oder kulturellen) Gründen von der Wahrnehmung gegebener Möglichkeiten absehen.

Im Vereinigten Königreich gab es von 2007 bis 2012 Abmahnungen in großem, danach nur noch in sehr geringem Ausmaß. Nach der in dieser Arbeit formulierten Hypothese sollte eine solche Konstellation eigentlich nicht existieren, da normalerweise davon auszugehen wäre, dass ein einmal etabliertes Abmahnwesen nur aufhört zu existieren, wenn sich entweder die rechtlichen Voraussetzungen ändern, keine *filesharing*-Nutzung mehr stattfindet oder spezifische sonstige, außerrechtliche Gründe dies bedingen. Zwar war im Vereinigten Königreich Letzteres der Fall – es gab einen erheblichen gesellschaftlichen *backlash*; tatsächlich jedoch hatte sich im Vereinigten Königreich auch nie eine Rechtslage entsprechend der deutschen herausgebildet.

Ein Auskunftsrecht gegen Dritte besteht im Vereinigten Königreiches als fallrechtlich gebildetes Institut (*Norwich Pharmacal*). Ein Auskunftsbegehren muss bei Gericht beantragt werden, die Entscheidung hierüber trifft ein *(Chief) Master* (vergleichbar mit einem Rechtspfleger).[405] Die spezifische Anwendung auf ISPs betreffend *filesharing*-Nutzer wurde vom *High Court*

[403] Siehe Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 28ff. – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

[404] Vgl. Kapitel § 3 I.

[405] Vgl. England and Wales Patents County Court, [2011] EWPCC 6, [2011] FSR 28, Rz. 11, 15 – bailii.org.

in einer Entscheidung aus dem Jahr 2012 bestätigt, Auskünfte wurden aber bereits seit 2007 erteilt.[406] Über die Zahl der Abmahnungen ist wenig bekannt; bis Ende 2010 sollen es etwas über 20.000 gewesen sein, für die überwiegend nur eine Rechtsanwaltskanzlei verantwortlich war.[407] Die einzig bekannte gerichtliche Entscheidung, die auf diese Abmahnungen folgte, ging zu Ungunsten des Rechteinhabers aus: das Gericht sah die Täterschaft der Anschlussinhaber (insgesamt waren 27 Personen beklagte Parteien des Verfahrens) nicht als erwiesen an, da theoretisch auch einer der Mitnutzer des jeweiligen Anschlusses die jeweilige Urheberrechtsverletzung durch *filesharing* begangen haben könnte.[408] Eine zivilprozessuale Fingierung der Täterschaft wie in Deutschland wurde also abgelehnt.[409]

Dem für die Abmahnungen verantwortlichen Rechtsanwalt wurde 2012 durch das *Solicitors Disciplinary Tribunal* (das Pendant zum deutschen Anwaltsgerichtshof) wegen der Massenabmahnungen vorübergehend die Anwaltszulassung entzogen.[410] Auch der öffentliche Aufschrei gegen diese Praxis war groß, mehrere Politiker äußerten Kritik.[411] Über Massenabmahnungen im Vereinigten Königreich ist seitdem nichts mehr bekannt geworden. Zur Aufgabe dieser Praxis dürfte auch beigetragen haben, dass die Abmahnungen bis 2010 fast ausschließlich Pornographie betroffen hatten, der Praxis also ein entsprechendes Stigma anhaftete. Die Musikindustrie distanzierte sich hiervon in Folge auch und kündigte an, diese Praxis nicht zu übernehmen.[412] Soweit in neuerer Zeit vereinzelte Abmahnungen bekannt geworden sind,

[406] England and Wales High Court (Chancery Division), [2012] EWHC 723 (Ch) – bailii.org; siehe hierzu *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 490f.

[407] *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 482.

[408] England and Wales Patent County Court, [2011] EWPCC 6, [2011] FSR 28, Rz. 28ff. – bailii.org; siehe hierzu auch *Moss*, Journal of Intellectual Property Law & Practice, Nr. 11, Bd. 6, 2011, S. 813, 815f.

[409] Siehe zu den genannten Fällen ausführlicher *Kipshagen*, Haftung bei offenem WLAN, S. 180ff.

[410] *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 485.

[411] *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 485.

[412] *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 485.

betrafen diese erneut ausschließlich Pornographie.[413]

Ob sich im Vereinigten Königreich eine Rechtslage wie in Deutschland hätte herausbilden können, wenn die abgemahnten Fälle durch alle Instanzen weiterverfolgt worden wären, kann hier dahinstehen; ebenfalls kann dahinstehen, ob englisches Anwaltsberufsrecht dem „Betrieb" eines Abmahnwesens generell entgegensteht. Denn im Ergebnis lässt sich jedenfalls festhalten, dass sich im Vereinigten Königreich eine Rechtslage entsprechend der deutschen jedenfalls nicht herausgebildet hat, der Rückgang der Abmahnungen also nicht die aufgestellte These über die erforderlichen rechtlichen Säulen eines Abmahnwesens widerlegt.

Zuletzt sei darauf hingewiesen, dass auch im Vereinigten Königreich durch den *Digital Economy Act 2010* die Einführung eines *graduated response system* gesetzlich vorgesehen ist. Jedoch schreibt das Gesetz nur einen groben Rahmen vor, die genaue Ausgestaltung ist Richtlinien vorbehalten, die durch das *Office for Communications* (Ofcom) ausgestaltet werden und durch das Parlament bestätigt werden müssen. Ein entsprechender Richtlinienentwurf ist seit 2012 nicht über das Entwurfsstadium hinausgekommen, insbesondere, da heftig über die Kostentragung hinsichtlich der Implementierung des Systems gestritten wurde.[414] Inhaltlich hätten Rechteinhaber Name und Anschrift eines Anschlussinhabers, der innerhalb bestimmter Fristen drei Verwarnungen erhalten hat, in Erfahrung bringen können, um dann selbstständig gegen diesen vorzugehen[415] (was aber nach bisheriger Rechtslage wie oben dargestellt bereits nach einem ersten Verstoß möglich ist). Mit der parlamentarischen Bestätigung dieses oder eines anderen Richtlinienentwurfs ist in absehbarer Zeit höchstwahrscheinlich nicht mehr zu rechnen. Stattdessen haben einige ISPs Anfang 2017 auf Grund einer Vereinbarung mit der Urheberrechtsindustrie unter Einbindung der Regierung ein freiwilliges *graduated response system* installiert.[416] Der Initiative werden aber keine großen Erfolgschancen eingeräumt, da ein vergleichbares System in den USA nach nur

413 *Maxwell*, UK Copyright Trolls Cite Hopeless Case to Make People Pay Up.

414 *Schmitz*, The Struggle in Online Copyright Enforcement: Problems and Prospects, S. 338, 348ff.

415 *Grisse*, ZGE 2014, 48, 54f.

416 *Van Der Sar*, UK „Piracy Warnings" Are Coming This Month; Here's How it Works.

vier Jahren Laufzeit wieder aufgegeben wurde.[417]

Als Ergebnis für dieses Kapitel bleibt festzuhalten: Länder der Kategorie 3, deren Existenz also die aufgestellte Hypothese widerlegen würden, existieren nicht.

5. Länder der Kategorie 4

Es konnte im Rahmen dieser Arbeit kein Land ermittelt werden, in dem ein Abmahnwesen existiert, ohne dass dort alle behaupteten rechtlichen Voraussetzungen existieren, was also die in Kapitel § 3 VII. aufgestellte Hypothese dieser Arbeit stützt.

6. Land der Kategorie 5: USA?

Die USA sind das erste Land, in dem Rechteinhaber gegen *filesharing*-Endnutzer vorgingen. 2003, also bereits ein Jahr bevor in Deutschland der erste *filesharer* verurteilt worden war[418], startete dort die Musikindustrie eine Kampagne, deren Ziel es war, durch die Verurteilung einiger weniger *filesharing*-Nutzer zu hohen Schadensersatzsummen eine abschreckende Wirkung zu erzielen, nicht jedoch, eine Gewinnquelle zu erschließen.[419] Zwischen 2003 und 2008 wurde ca. 35.000 Personen mit Schadensersatzklagen gedroht.[420] Die Kontaktdaten versuchte die Musikindustrie – wie ab 2008 in Deutschland – mittels eines direkt an die jeweiligen ISPs gerichteten Auskunftsbegehrens zu erlangen, die Gerichte lehnten dieses Vorgehen jedoch ab. Folglich reichte die Musikindustrie zunächst Klage gegen Unbekannt ein (sogenanntes *John Doe*-Verfahren[421]) und erlangte sodann *subpoenas* gegen die ISPs betreffend der Kontaktinformationen; diese identifizierten in Folge die jeweilige Person

[417] *Rigg*, Is the UK's new piracy email alert program dead on arrival?; siehe zu dem System in den USA Kapitel § 3 XII. 6. Gegenwärtig werden auf die Vereinbarung hin noch *piracy warnings* an Nutzer versandt, die *filesharing* betrieben haben, siehe *Van Der Sar*, UK ISPs Sent a Million Piracy Alert Emails.

[418] Siehe Kapitel § 2 II.

[419] *Sag*, 100 Iowa L. Rev. 1105, 1114 (2015).

[420] *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 1: Die RIAA vs. John Doe.

[421] Ein solches Vorgehen wäre in Deutschland wegen des Erfordernisses einer hinreichend bestimmten Parteibezeichnung nach § 253 Abs.2 Nr.1 ZPO grundsätzlich nicht möglich, siehe *Mantz*, NJW 2016, 2845, 2846.

des Beklagten namentlich.[422] Im Ergebnis können aber – wie in einem Auskunftsbegehren nach deutschem Recht[423] – mehrere Personen in einem *John Doe*-Verfahren zusammengefasst werden.[424]

Tatsächlich bis zum Ende ausgefochten wurden aber nur Verfahren gegen zwei Personen. Diese hatten jeweils die Täterschaft eingestanden, sodass die Frage der Darlegungs- und Beweislastverteilung nicht abschließend geklärt werden konnten. Die Verfahren erregten jedenfalls einen großen öffentlichen Aufschrei, da einer der Beklagten zu einem Schadensersatz von 222.000 US-Dollar[425] für das öffentliche Zugänglichmachen von 24 Musiktiteln und der andere zu einem Schadensersatz von 675.000 US-Dollar für 30 Musiktitel verurteilt worden war.[426] Der restlichen Verfahren wurden entweder außergerichtlich verglichen oder nicht weiter verfolgt.[427]

Die Kampagne der Musikindustrie endete 2008. Sie muss in Anbetracht ihrer Zielsetzung als gescheitert gelten, da ihr erklärtes Ziel, erzieherisch zu wirken und somit *filesharing*-Aktivitäten (in den USA) zu vermindern, nicht erreicht wurde.[428] Darüber hinaus war die Kampagne für die Musikindustrie ein PR-Desaster und überaus kostspielig.[429]

Zwischen 2008 und 2010 gab es nur vereinzelte Versuche, gegen *filesharing*-Endnutzer vorzugehen. Ab 2010 nahm die Zahl der Verfahren zu, jedoch scheiterten sie überwiegend, insbesondere, weil die Kläger häufig keine Aktivlegitimation nachweisen konnten; zudem wurde 2013 einigen Anwälten, die sich auf dieses Feld spezialisiert hatten, wegen Betruges die Zulassung entzogen.[430] Seit 2013 ist allerdings ein deutlicher Anstieg zu verzeichnen.

422 *Zilka*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667, 683ff. (2009).
423 Siehe Kapitel § 2 III. 1. g).
424 *Zilka*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667, 685 (2009).
425 Der aber später auf 56.000 US-Dollar reduziert wurde
426 *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 2: Der Fall Jammie ThomasRasset; *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 3: Der Fall Joel Tenenbaum.
427 *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 1: Die RIAA vs. John Doe.
428 Siehe mit einer Zusammenfassung der empirischen Ergebnisse *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 4: Cui bono?
429 *Zilka*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667, 685 (2009); *Tschmuck*, Die US-Musikindustrie vs. die FilesharerInnen - Teil 4: Cui bono?
430 *Greenberg*, 100 Iowa L. Rev. Bulletin 77, 81 (2015).

Empirisch lässt sich dies an Hand der Gerichtsdatenbank PACER[431] nachvollziehen: *Sag* und *Haskell* nehmen auf der Grundlage, dass praktisch alle eingetragenen *John Doe*-Verfahren *filesharing*[432] betreffen und pro *John Doe*-Verfahren regelmäßig etwas über vier bis acht Personen[433] betroffen sind an, dass seit 2010 über 100.000 *filesharing*-Verfahren angestrengt wurden.[434] Auch wenn es sich hierbei bereits um Gerichtsverfahren handelt, ist deren Gegenstück in Deutschland eher die Abmahnung statt ein Gerichtsverfahren, da in den USA die Einleitung eines *John Doe*-Gerichtsverfahrens nötig ist, um die Kontaktdaten der *filesharer* zu erlangen; tatsächlich wird dann aber praktisch keines der Verfahren zu Ende geführt, sondern entweder ein Vergleich (regelmäßig mit einer Vergleichssumme zwischen 1000 und 8000 US-Dollar) geschlossen oder die Klage zurückgenommen.[435] Tatsächlich ist die Zahl der „Abmahnungen" in den USA im Vergleich zu Deutschland eher niedrig: dort kann man berechtigterweise von über 1,5 Millionen Abmahnungen seit 2010 ausgehen. Ausgehend von einer viermal so großen Bevölkerung beträgt die Zahl an „Abmahnungen" in den USA im Zeitraum von 2010 bis 2016 relativ betrachtet also nur ca. 1,7 Prozent der Zahl der Abmahnungen in Deutschland im selben Zeitraum.[436]

Auch wenn in Ländern wie Finnland und Schweden bei erheblich kleinerer Bevölkerungsgröße in neuerer Zeit über 100.000 Abmahnungen innerhalb eines Jahres ausgesprochen wurden, ist es dennoch gerechtfertigt, diese Länder in Kategorie 2 zu führen und die USA im Rahmen der Kategorie 5 zu diskutieren, da in Letzterer „Abmahnungen" je nach Betrachtungsweise seit 2003, jedenfalls aber seit 2010 fester Bestandteil der dortigen Rechtsrealität sind.

Bestätigen die USA nun also die These[437] darüber, welche rechtlichen Säulen erforderlich sind, um Massenabmahnungen als festen Bestandteil einer

431 *Public Access to Court Electronic Records.*

432 Und hierbei wiederum BitTorrent-*filesharing.*

433 Zwar erlauben einige Gerichte die Zusammenfassung mehrerer Personen in einer Klage nicht, siehe *Civil*, 30 Syracuse Sci. & Tech. L. 2, 48f.; im Ergebnis macht dies jedoch keinen Unterschied, da das Verfahren dann eben jeweils gegen einzelne Personen geführt wird.

434 *Sag/Haskell*, 103 Iowa L. Rev. 571, 576ff. (2018).

435 *Sag/Haskell*, 103 Iowa L. Rev. 571, 580 (2018).

436 Der weitere Fortgang ist zu beobachten. Die Zahl der Verfahren steigt in den USA konstant an; siehe zu Daten aus der ersten Jahreshälfte 2018 *Van Der Sar*, US Online Piracy Lawsuits Break Record Numbers.

437 Siehe Kapitel § 3 VII.

Rechtsordnung zu etablieren? Diese Frage kann leider nicht eindeutig beantwortet werden. Denn zwar gibt es umfangreiche (und kritische) Literatur zu der Praxis der Massen„abmahnungen“[438]; jedoch wird nahezu kein *John Doe*-Verfahren bis zum Ende geführt, sondern – wie erwähnt – in den allermeisten Fällen nach Gewährung der *subpoena* gegen den jeweiligen ISP entweder durch Vergleich beendet oder die Klage zurückgenommen.[439] Soweit die Verfahren zu Ende geführt wurden, hatten die Beklagten ihre Täterschaft überwiegend nicht bestritten.[440] Sind die USA also in Wirklichkeit ein Land der Kategorie 4 und widerlegen die aufgestellte These? Dies jedenfalls kann verneint werden. Zunächst ist festzuhalten, dass – bis auf eine – alle behaupteten rechtlichen Voraussetzungen eines Abmahnwesens existieren: erstens ist die massenhafte Auskunft über Anschlussinhaber gewährleistet. Zweitens wären im Falle einer Verurteilung *statutory damages* von mindestens 750 bis zu 150.000 US-Dollar[441] zu leisten[442]; wie sich aus den Verurteilungen im Zuge der Kampagne der Musikindustrie gezeigt hat, können die zugesprochenen Schadensersatzsummen aber deutlich höher sein[443]. Drittens zeigt sich – in negativer Hinsicht – dass eine Störerhaftung in den USA nicht existiert, also offensichtlich keine notwendige Bedingung für ein Abmahnwesen ist.

Es fehlt also lediglich an einer gefestigten Rechtsprechung, die dazu führt, dass regelmäßig der Anschlussinhaber auch als Täter der Urheberrechtsverletzung in Anspruch genommen werden kann.[444] Da aber viele Gerichte bereits im Verfahrensstadium die Auskunft des ISP betreffend den Anschluss-

[438] Vgl. hierzu nur aus neuerer Zeit: *Grinvald*, 49 U.S.F.L. Rev. 409, 463 (2015); *Foreman*, 13 Wash. U. Global Stud. L. Rev. 127, 150ff. (2014); *Alberty*, 15 J. Marshall Rev. Intell. Prop. L. 799, 825f. (2016); *Bell*, 18 Chap. L. Rev. 799, 812ff. (2015); den kritischen Stimmen aus der Literatur wird nur in Bezug auf Details widersprochen, beispielsweise betreffend der Benutzung des Begriffs „Troll“ und ob tatsächlich in der Mehrzahl der Verfahren mehrere Beklagte in einer Klage zusammengefasst werden, siehe *Balganesh/Gelbach*, 101 Iowa L. Rev. Online 43, 60ff. (2016).

[439] Siehe die Erläuterung einiger Fälle im Detail bei *Kipshagen*, Haftung bei offenem WLAN, S. 246ff.

[440] *Sag/Haskell*, 103 Iowa L. Rev. 571, 635 (2018).

[441] Selbst wenn bei BitTorrent-Fällen streitgegenständlich in der Regel nur ein Werk ist.

[442] *Sag/Haskell*, 103 Iowa L. Rev. 571, 625 (2018).

[443] Siehe hierzu beispielsweise *Van Der Sar*, BitTorrent Pirate Ordered to Pay $1.5 Million Damages For Sharing 10 Movies.

[444] Die Täterschaft ablehnend beispielsweise District Court for the Western District of Washington at Seattle, CRi 2014, 22.

inhaber als Täter ansehen[445], erscheint es umgekehrt auch nicht unwahrscheinlich, dass die Rechtsprechung in den USA diesbetreffend einen ähnlichen Pfad wie die Rechtsprechung in Deutschland einschlagen wird.[446] Des Weiteren gibt es einige Spezifika des Abmahnwesens in den USA und im US-Rechtssystem, die die fehlende gefestigte Rechtsprechung zur Täterschaft kompensieren:

- Die drohenden Schadensersatzsummen, die selbst den deutschen Durchschnitt in *filesharing*-Fällen erheblich übersteigen, lassen eine gerichtliche Erklärung für den regulären Verbraucher als viel zu riskant erscheinen.
- Anders als in Deutschland, wo *filesharing*-Fälle viele Branchen der Unterhaltungsindustrie abdecken[447], ist in den USA überwiegend Pornographie streitgegenständlich.[448] Ähnlich wie bei den *RedTube*-Abmahnungen[449] dürfte vielen Betroffenen daran gelegen sein, die Verfahren möglichst diskret zum Abschluss zu bringen.
- In den USA müssen Beklagte die Gebühren ihres Rechtsanwalts – die zudem verglichen mit den Gebühren deutscher Rechtsanwälte deutlich höher sind – regelmäßig selbst tragen.[450] Folglich ist für Verbraucher ein Vergleich im Bereich der wie oben erörtert üblichen 1000 bis 8000 US-Dollar unter Umständen sogar kostengünstiger als ein Obsiegen im Prozess.[451]

Im Ergebnis kann der Vergleich mit den USA die These dieser Arbeit betreffend der für ein Abmahnwesen erforderlichen rechtlichen Rahmenbedingungen also zwar nicht abschließend bestätigten, aber zumindest aufzeigen, dass eine Störerhaftung des Internetanschlussinhabers (bzw. ein rechtlich vergleichbares Institut) nicht notwendig ist, um ein Abmahnwesen zu stüt-

[445] *Sag/Haskell*, 103 Iowa L. Rev. 571, 591f. (2018).
[446] Siehe mit einer Übersicht der (noch nicht eindeutig in eine bestimmte Richtung gehenden) Entwicklungen *Grahovec*, 30 DePaul J. Art, Tech. & Intell. Prop. L. 69, 81ff. (2020).
[447] Siehe Kapitel § 3 V. 4.
[448] *Sag/Haskell*, 103 Iowa L. Rev. 571, 578f. (2018).
[449] Siehe Kapitel § 3 IV. 2.
[450] *Sag/Haskell*, 103 Iowa L. Rev. 571, 621f. (2018).
[451] Gegenwärtig versuchen jedoch Abgemahnte immer häufiger, die Erstattung ihrer Rechtsanwaltsgebühren gerichtlich durchzusetzen, vgl. *Van Der Sar*, Wrongfully Accused 'Pirate' Wants 62,818 Compensation.

zen.

Zuletzt ist der Vollständigkeit halber zu erwähnen, dass in den USA auch zwei andere Modelle des Vorgehens gegen *filesharing*-Endnutzer versucht wurden bzw. werden.

Erstes Modell war eine freiwillige Vereinbarung zwischen ISPs und Rechteinhabern aus dem Jahr 2013, die ein sogenanntes *Copyright Alert System* errichtete, welches ähnlich wie ein *graduated response system* funktionierte. Vorgesehen war ein Verwarnungsmodell mit sechs Eskalationsstufen, weshalb es auch als *six strikes*-System bezeichnet wurde. Jedoch zog die sechste Verwarnung keine Kündigung des Internetanschlusses nach sich, stattdessen konnten nach der fünften Verwarnung Sanktionen wie eine Verlangsamung der Internetgeschwindigkeit verhängt werden.[452] Das Programm wurde Anfang 2017 allerdings aufgegeben, wohl weil es an dem Umfang der *filesharing*-Nutzung wenig geändert hat.[453]

Zweites Modell ist, ISPs unter Androhung ihrer Inanspruchnahme auf Schadensersatz zu zwingen, ihren Kunden, soweit sie wiederholt illegales *filesharing* betreiben, zu kündigen. Hintergrund ist ein Verfahren, das die Musikindustrie seit 2015 gegen einen ISP führt, da er zu wenig gegen diejenigen seiner Kunden tue, die Urheberrechte verletzen. Der *Fourth Circuit Court of Appeals* entschied Anfang 2018, dass ISPs tatsächlich auf Schadensersatz in Anspruch genommen werden können, wenn sie Kunden, die wiederholt Urheberrechte verletzen, nicht den Anschluss kündigen. ISPs haben infolgedessen Richtlinien erlassen, wann eine Kündigung ausgesprochen wird.[454]

Letzteres macht zunächst stutzig: sollte nicht davon ausgegangen werden, dass Rechteinhaber, sobald die Möglichkeit dazu besteht, immer versuchen werden, mit Abmahnungen Profit zu erzielen?[455] Grundsätzlich ja, doch ist in den USA die Besonderheit zu berücksichtigen, dass erstens die Musikindustrie wohl wegen der negativen Folgen ihrer Aufklärungskampagne aus den Jahren 2003 bis 2008 nicht mehr gegen Endnutzer direkt vorgehen möchte und zweitens die Beteiligung am Abmahnwesen in den USA mit der Porno-

[452] *Bridy*, 23 Fordham Intell. Prop. Media & Ent. L. J. 1, 32f. (2013).
[453] *Van Der Sar*, The US 'Six Strikes' Anti-Piracy Scheme is Dead.
[454] Siehe beispielsweise *Van Der Sar*, Comcast Explains How It Deals With Persistent Pirates.
[455] Siehe Kapitel § 3 XII. 4.

industrie verbunden wird; eine Assoziation, die andere Branchen regelmäßig vermeiden möchten. Letztlich lässt sich also mit spezifischen außerrechtlichen Gründen erklären, warum in den USA von diesen Branchen dieser Weg eingeschlagen wird.

7. Sonstige Länder

Über das Vorgehen gegen Privatpersonen wegen *filesharing* in anderen Ländern als den Genannten ist wenig bis nichts bekannt.

In Japan[456] und Hongkong[457] wurde 2004 bzw. 2005 jeweils ein Nutzer von *filesharing* strafrechtlich belangt. Weitere Fälle und insbesondere zivilrechtliches Vorgehen gab es dort nicht. In Indien scheint *filesharing* (bisher) nicht verfolgt zu werden.[458]

In Russland wurde erst mit dem 2013 in Kraft getretenen Anti-Piraterie-Gesetz ein Instrumentarium gegen Online-Urheberrechtsverletzungen implementiert. Ein Auskunftsanspruch gegen die Endnutzer von *filesharing* existiert jedoch nicht. Stattdessen liegt der Fokus auf Intermediären wie den Betreibern von Indexseiten und Trackern.[459]

In der Volksrepublik China wird seit den frühen 2000er Jahren verstärkt geistiges Eigentum durchgesetzt, sowohl durch administrative Maßnahmen als auch über den Zivilrechtsweg. Es gibt umfangreiche Rechtsprechung zur Verantwortlichkeit von ISPs und Hosting-Diensten, zur Haftung von Endnutzern von *filesharing* ist jedoch nichts bekannt.[460] BitTorrent-Nutzer gibt es zahlreich, jedoch geht die Regierung statt gegen diese vordringlich gegen Indexseiten vor.[461]

---

[456] *Leitner*, 22 Colum. J. Asian L. 1, 1, 21 (2008); *Cannon*, 16 Wash. U. Global Stud. L. Rev. 483, 492, 497 (2017).

[457] *Filby*, International Review of Law, Computers & Technology, Nr. 3, Bd. 21, 2007, S. 275, 278.

[458] Vgl. *Lal*, Illegal downloaders, you might not be criminals in India, but be careful abroad.

[459] Siehe *Schöttle*, GRUR Int. 2014, 119, 121 sowie die Nachweise bei OLG Köln, Urteil vom 18. Juli 2014, Az. I-6 U 192/11, 6 U 192/11, Rz. 966 – juris.

[460] Vgl. *Guo*, Modern China's Copyright Law and Practice, S. 194ff.

[461] *Odell*, Downloading Frenzy in China: Gov't Blocking All Torrent Sites Soon?

8. Zusammenfassung und Ergebnis

Massenhafte Abmahnungen gibt es auch in anderen Ländern als Deutschland; damit sie aber ein dauerhaftes Phänomen werden, sich mithin ein echtes Abmahnwesen im Sinne dieser Arbeit bilden kann, muss sich eine spezifische Rechtslage herausbilden, wie es bisher nur in Deutschland und (mit starken Einschränkungen) den USA geschehen ist. Das war im Vereinigten Königreich nie der Fall, folglich verschwanden dort Massenabmahnungen nach einiger Zeit auch wieder, während sie hingegen in Deutschland und (mit *starken* Einschränkungen) den USA seit über einem Jahrzehnt fester Bestandteil der jeweiligen Rechtspraxis sind.

Die Länder der Kategorie 2 werden die Hypothese dieser Arbeit in Zukunft auf die Probe stellen: ist sie zutreffend, werden Massenabmahnungen dort wieder verschwinden, wenn sich eine entsprechende Rechtslage wie in Deutschland nicht herausbildet; bildet sie sich aber heraus, sollten Massenabmahnungen fester Bestandteil der dortigen Rechtspraxis werden. Die Rechtslage im Vereinigten Königreich zeigt, dass Massenabmahnungen wieder verschwinden, wenn sich keine für Rechtsinhaber günstige Rechtslage herausbildet. Die Rechtslage in den USA kann die Hypothese dieser Arbeit weder vollständig verifizieren noch falsifizieren, da zwar eine der behaupteten rechtlichen Säulen fehlt, dies jedoch durch verschiedene andere Faktoren möglicherweise kompensiert wird. Jedenfalls bestätigt die Rechtslage in den USA, dass ein der Störerhaftung (oder dem Anspruch aus § 7 Abs.4 TMG) vergleichbares Rechtsinstitut nicht erforderlich ist, um ein Abmahnwesen entstehen zu lassen.

Der Vergleich mit anderen Ländern zeigt generell aber auch auf, dass die Situation in Deutschland einzigartig ist: Ein Abmahnwesen in solchem Umfang und mit solcher rechtlicher „Rückendeckung“ wie hier gibt es derzeit nirgendwo sonst auf der Welt.

§ 4 Dogmatische Bewertung der gegenwärtigen Rechtslage

I. Einleitung

In diesem Kapitel wird die gegenwärtige, faktische Rechtslage, wie sie von BGH und Gesetzgebung geschaffen und in Kapitel § 2 dieser Arbeit dargestellt wurde, nach rechtsdogmatischen Kriterien bewertet. Die Rechtsprechung des BGH und des EuGH wird auf ihre dogmatische Stimmigkeit hin überprüft und die neueren Gesetzesreformen (TMG und Gesetz gegen unseriöse Geschäftspraktiken), zu denen noch keine BGH-Rechtsprechung existiert, darauf hin, ob sich ihnen mit hergebrachter juristischer Methodik ausreichend bestimmte und handhabbare Auslegungsergebnisse entnehmen lassen sowie, ob ihnen klar formulierte Ziele zu Grunde liegen und wenn ja, ob diese erreicht werden.

Die dogmatische Bewertung von Rechtsprechung und Gesetzgebung kann je nach Ergebnis geeignet sein, die rechtspolitischen Kritikpunkte am Abmahnwesen[1] zu stützen.

Zu Rechtsfragen mit *filesharing*-Bezug, die der BGH bisher „übersehen“ oder noch nicht beantwortet hat, die sich aber (unter Umständen schon seit geraumer Zeit) stellen, wird in Kapitel § 5 bei den Überlegungen zur Rechtsentwicklung *de lege lata* Stellung genommen. Zu denjenigen Rechtsfragen, die der BGH bereits abschließend beantwortet hat, und zu den neueren Gesetzesreformen (TMG und Gesetz gegen unseriöse Geschäftspraktiken) werden im letzten Kapitel – soweit sie rechtsdogmatisch unbefriedigend gelöst wurden

[1] Siehe hierzu Kapitel § 3 VIII.

– Alternativen *de lege ferenda* vorgeschlagen.[2]

Die Reihenfolge der nachfolgenden dogmatischen Auseinandersetzung orientiert sich primär an einem Aufbau, wie er auch in der Praxis oder einer juristischen Prüfung nachzuvollziehen wäre, also: Vorliegen einer urheberrechtsverletzenden Handlung; Anforderungen an den Nachweis der Handlung; Ermittlung der Quelle der Handlung (Auskunftsanspruch, Sicherung des Auskunftsanspruch, jeweilige Kosten); prozessuale Fiktion der Täterschaft des Anschlussinhabers; subsidiäre Haftung des Anschlussinhabers nach TMG; Schadensersatz; Nebenaspekte des Gesetzes gegen unseriöse Geschäftspraktiken; Einrede des Rechtsmissbrauchs.

II. Zur Urheberrechtsverletzung an sich

1. Einleitung

Für diese Arbeit ist wegen ihres Fokus auf Endnutzer im Wesentlichen nur interessant, wie die Abwicklung von *filesharing*-Datenverkehr und insbesondere BitTorrent-Datenverkehr über einen Internetanschluss urheberrechtlich zu fassen ist, also welche Verwertungshandlungen betroffen sind und welche Beteiligungsform der Inhaber des Anschlusses erfüllen kann. Für die Bewertung der Rechtsprechung des BGH und des EuGH in diesem Punkt interessiert folglich nicht, ob sie die Handlungen anderer Akteure, insbesondere anderer Akteure im BitTorrent-System[3], zutreffend eingeordnet hat.

2. Einordnung des Download- und Uploadvorgangs

a) Vervielfältigung und öffentliche Zugänglichmachung

Wer eine urheberrechtlich geschützte Datei über ein *filesharing*-System empfängt, begeht grundsätzlich eine Vervielfältigungshandlung (§ 16 UrhG), wer eine solche Datei anderen über ein solches System zur Verfügung stellt, begeht grundsätzlich eine öffentliche Zugänglichmachung (§ 19a UrhG).[4] Ein-

[2] Siehe hierzu Kapitel § 5.

[3] Siehe hierzu Kapitel § 5 II. 1.

[4] *Heckmann/Paschke* in: Heckmann, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 3.2, Rz. 37. Soweit Computerprogramme betroffen sind, ist der entsprechend einschlägige § 69c Nr.4 UrhG wie § 19a UrhG anzuweden, siehe BGH, Urteil vom 28. März 2019, Az. I ZR 132/17, Rz. 25 – GRUR 2019, 950 - „Testversion“.

schränkungen können sich jedoch ergeben, wenn eine Datei segmentiert oder nicht vollständig übertragen wird; hier kommen die Besonderheiten verschiedener *filesharing*-Systeme ins Spiel.[5]

Darüber hinaus ist bei privaten Börsen im Rahmen des BitTorrent-Systems[6] fraglich, ob dort wegen des beschränkten Teilnehmerkreises die Nutzer überhaupt eine öffentliche Zugänglichmachung begehen können. Gegenwärtig sind Aktivitäten von Endnutzern auf privaten Börsen – soweit ersichtlich – noch nicht Gegenstand von Abmahnungen, auch wenn sich dies in Zukunft vielleicht ändern mag.[7] Mangels einer bestehenden oder sich entwickelnden Rechtsprechung zu dieser Frage wird eine Lösung in dieser Arbeit daher nicht entwickelt.

Wie andere Vorgänge – wie beispielsweise das Einstellen eines *magnet links* auf einer Indexseite[8] – urheberrechtlich zu bewerten sind, wird ebenfalls offengelassen. Es interessieren allein die Handlungen, die typischerweise von Endnutzern vorgenommen werden, also die (nicht-rechtlich gesprochen) bloße Teilnahme an einem *filesharing*-System.[9]

b) Haftung des Anschlussinhabers als Täter, Teilnehmer oder Störer

Zunächst erscheint es unproblematisch, den Anschlussinhaber lediglich dann als Täter einer urheberrechtlichen Verwertungshandlung anzusehen, wenn er diese eigenhändig begeht.[10] Etwas anderes gilt nur dann, wenn die Täterschaft nicht an die urheberrechtliche Verwertungshandlung, sondern einen anderen Tatbestand geknüpft ist, insbesondere die Aufsichtspflichtverletztung nach § 832 BGB. Gegen die Rechtsprechung des BGH zu Letzterer – namentlich also „Morpheus“ und „Tauschbörse II“[11] – bestehen keine dogmatischen Einwände. Der Begriff der „Aufsichtspflicht“ in § 832 Abs.1 Satz 1

[5] Siehe hierzu sogleich Kapitel § 4 II. 3. und 4.
[6] Siehe Kapitel § 1 II. 5. c).
[7] Siehe Kapitel § 3 XI. 2. c).
[8] Siehe hierzu in technischer Hinsicht Kapitel § 1 II. 5. a) aa) und cc).
[9] Siehe zu den Formen der Teilnahme in verschiedenen *filesharing*-Systemen Kapitel § 1 II. 4.
[10] Unterstellt, der Nachweis der Begehung durch den Anschlussinhaber selbst ist gelungen, was regelmäßig über die sekundäre Darlegungslast und tatsächliche Vermutung fingiert wird, siehe hierzu Kapitel § 4 VII.
[11] Siehe Kapitel § 2 IV. 2. und VI. 2.

1.Alt. BGB ist seiner generalklauselartigen Natur wegen der Rechtsprechung zur Ausfüllung überlassen.[12] Es scheint völlig vertretbar, Eltern die Pflicht aufzuerlegen, ihre minderjährigen Kinder über einen rechtmäßigen Umgang mit dem Internet aufzuklären und dazu anzuhalten. Zu ergänzen ist lediglich, dass eine solche Aufklärung nicht von vornherein zwecklos erscheint, sodass auch nicht davon ausgegangen kann, dass minderjährige Kinder trotz Aufklärung urheberrechtsverletzendes *filesharing* betreiben; mithin ist § 832 Abs.1 Satz 2 2.Alt BGB nicht einschlägig.

Abgesehen von § 832 BGB sind weitere spezielle Tatbestände nicht einschlägig. Die Unternehmerhaftung nach § 99 UrhG bei rein gewerblich genutzten Anschlüssen[13] dürfte praktisch ausscheiden, da diese voraussetzt, dass die Urheberrechtsverletzung von einem Arbeitnehmer oder Beauftragten nicht privat, sondern im Zusammenhang mit seiner beruflichen Tätigkeit ausgeübt wird.[14] Die denkbar einschlägigen Fallkonstellationen sind überschaubar; beispielsweise könnte man einen solchen Zusammenhang annehmen, wenn der Arbeitnehmer mittels *filesharing* eine Software besorgt, die sein Unternehmen benötigt. Dem Verfasser sind nur zwei Entscheidungen bekannt, bei denen Beklagter ein Arbeitgeber war und als potentieller Täter nur ein Arbeitnehmer in Betracht kam.[15]

Außerhalb des Anwendungsbereiches der § 832 BGB und § 99 UrhG kann ein Anschlussinhaber also für von anderen Personen über seinen Anschluss begangene Urheberrechtsverletzungen allenfalls als Störer haften, unter Geltung des § 7 Abs.4 TMG n.F. statt als Störer nur für den dort statuierten Sperranspruch[16] – sollte man meinen. Der BGH hatte in „Sommer unseres Lebens“ statuiert, dass die täterschaftliche Haftung im Urheberrecht im Allgemeinen und für Anschlussinhaber im Besonderen (abseits von Ansprüchen wie § 99 UrhG) nur bei eigenhändigem Tun in Betracht kommt, die Übertragung der Rechtsprechung zum UWG, die die täterschaftliche Haftung bei

[12] Vgl. zur Delegationslücke Kapitel § 4 XI.

[13] Bei Privaten kommt die Anwendung dieser Norm ohnehin nicht in Betracht, siehe *Ernst/Seichter*, ZUM 2007, 513, 514.

[14] *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 99 UrhG, Rz. 3.

[15] AG Charlottenburg, Urteil vom 8. Juni 2016, Az. 231 C 65/16 – juris; LG Köln, Urteil vom 28. Juni 2018, Az. 14 S 39/17 – waldorf-frommer.de. Die Anwendung des § 99 UrhG wurde dort auch gar nicht erwogen.

[16] Siehe hierzu Kapitel § 4 VIII.

Verletzung von Verkehrspflichten annimmt, jedoch ausscheidet.[17] Diese vermeintliche Gewissheit könnte jedoch durch die neuere EuGH-Rechtsprechung zur Haftung von Intermediären als Täter möglicherweise ins Wanken geraten.[18] Jene ist allerdings von der Rechtsprechung des BGH zur Haftung des Anschlussinhabers noch nicht aufgegriffen worden, sodass es hierzu im Rahmen der dogmatischen Kritik auch noch nichts zu sagen gibt.

Rein theoretisch denkbar ist neben der Haftung als Täter oder als Störer (bzw. der Haftung nach § 7 Abs.4 TMG) auch eine Haftung als Teilnehmer (wobei diese gemäß § 830 Abs.2 BGB dieselben Rechtsfolgen zeitigt wie die Haftung als Täter). Denkbar wäre zum Beispiel eine Beihilfehandlung in der Form, dass ein Anschlussinhaber seinen Anschluss anderen Personen bewusst zum Zwecke der Urheberrechtsverletzung mittels *filesharing* überlässt. Jedoch ist ein solcher Fall in der Praxis bisher nicht bekannt geworden und dürfte wenn dann auch regelmäßig an Beweisschwierigkeiten scheitern. Gleiches gilt für die Anstiftung.

c) Zur Irrelevanz der Störerhaftung

Abseits der Haftung des Anschlussinhabers als Täter kraft (vermuteter) eigenhändiger Durchführung von *filesharing* oder kraft Verletzung einer Pflicht wie der Aufsichtspflicht aus § 832 BGB kommt – wie vom BGH folgerichtig angenommen – eine Haftung als Störer aus § 1004 BGB analog iVm § 97 UrhG in Betracht.

In der öffentlichen Wahrnehmung scheint sich in Bezug auf das Abmahnwesen *alles* um die Störerhaftung zu drehen. Tatsächlich gäbe es aber ohne die täterschaftliche Haftung des Anschlussinhabers nach Meinung des Verfassers kein Abmahnwesen, da vom Störer kein Schadensersatz verlangt werden kann.[19] Zudem ist mit dem 3. TMGÄndG zwar die täterschaftliche Haftung des Anschlussinhabers nicht abgeschafft worden, die Störerhaftung aber schon.[20] Weiterhin blieben schon unter der Rechtslage vor der TMG-Reform kaum mehr Konstellationen übrig, in denen die Störerhaftung realistisch Anwendung finden konnte. Da der Unterlassunganspruch in die Zukunft gerich-

[17] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 13 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[18] Siehe hierzu genauer Kapitel § 5 II. 1.

[19] Siehe Kapitel § 3 VI. und VII.

[20] Siehe Kapitel § 2 X.

tet ist, fällt die Störerhaftung auch für Altfälle – soweit dort überhaupt ein Unterlassungsanspruch geltend gemacht wurde – weg.[21] Die Störerhaftung ist im Rahmen von *filesharing* also nur noch für die Frage relevant, ob Gebühren für Abmahnungen verlangt werden können, die vor Inkrafttreten des 3. TMGÄndG ausgesprochen worden waren.[22] Da der Gebührenersatzanspruch aber – anders als der (Rest-)Schadensersatzanspruch[23] – schon in der Regelfrist verjährt, ist die Zeit, in der entsprechende Altfälle noch gerichtlich „aufgerollt" werden können, entsprechend kurz bemessen.

Schon rein rechtstatsächlich wird die Störerhaftung für Anschlussinhaber also in Zukunft – selbst wenn sie gesetzlich wieder eingeführt werden sollte – so gut wie keine Rolle spielen. Sie ist aber auch aus rechtsdogmatischer Perspektive nicht mehr sonderlich interessant. Ob in einer bestimmten Konstellation die Störerhaftung Anwendung findet, ist allein eine richterrechtliche Entscheidung. Rechtswissenschaftlich bleibt damit[24] allein die Frage, ob sich aus dem bisherigen Richterrecht Ableitungen und Prognosen für zukünftig zu entscheidende Konstellationen treffen lassen. Mit „Tauschbörse IX / Silver Linings Playbook" ist jedoch offenkundig, dass der BGH auch außerhalb familiärer Kontexte geneigt ist, die Störerhaftung grundsätzlich auszuschließen (was zustimmungswürdig ist, da es im Rahmen der Störerhaftung nur darauf ankommt, inwiefern man auf einen verantwortungsvollen Umgang der Mitnutzer mit dem Anschluss vertrauen darf, mithin auf deren Eigenverantwortlichkeit; diese ist bei volljährigen Personen einheitlich zu bewerten).[25] Dogmatisch ist die Rechtsprechung des BGH zur Störerhaftung des Anschlussinhabers im Ergebnis nur noch interessant, soweit sich hieraus Rückschlüsse für die sekundäre Darlegungslast ziehen lassen.[26]

Im Ergebnis wird daher in dieser Arbeit von der Erörterung der Störer-

[21] Siehe Kapitel § 2 XI. 6.

[22] Da für die Frage, ob eine Abmahnung berechtigt ist und mithin einen Gebührenersatzanspruch auslöst, der Zeitpunkt des Ausspruchs maßgeblich ist, siehe Kapitel § 2 XI. 6. Der Unterlassungsanspruch an sich wird ohnehin fast nie geltend gemacht und endet, soweit er in der Vergangenheit erfolgreich geltend gemachte wurde, wegen seines Charakters als Dauerschuld jedenfalls automatisch ab Inkrafttreten des 3. TMGÄndG.

[23] Siehe hierzu Kapitel § 4 IX. 4.

[24] Soweit das Institut nicht an der Wurzel behandelt wird.

[25] Bei minderjährigen Kindern gilt in Fällen, die eigentlich Gegenstand der Störerhaftung wären, ohnehin § 832 BGB, siehe Kapitel § 2 IV. 2.

[26] Siehe hierzu Kapitel § 4 VII. 3. b).

haftung in *filesharing*-Konstellationen abgesehen. Sollte in Zukunft erstens § 7 Abs.4 TMG abgeschafft oder für nichtig/nicht anwendbar erklärt werden (beispielsweise wegen der europarechtlichen Bedenken[27]), zweitens die täterschaftliche Haftung des Anschlussinhabers auf Grund einer Änderung der Rechtsprechung oder einer Gesetzereform (häufiger als bisher) ausscheiden, drittens die Störerhaftung entgegen der Erwartungen in nicht-familiären Konstellationen für anwendbar erklärt werden und viertens entgegen der Prognosen des Verfassers ein Abmahnwesen auch dann bestehen bleiben, wenn in Folge nur Ersatz für die Abmahngebühren verlangt werden kann, dann – und nur dann – wäre die Störerhaftung des Anschlussinhabers (wieder) relevant. Sie wäre in diesem Fall von wissenschaftlicher Seite wieder aufzugreifen.

3. Die Wahrnehmbarkeit von Dateifragmenten als dogmatisches Problem bei der segmentierten Dateiübertragung

Unabhängig von der Schutzfähigkeit einzelner Segmente einer Datei ist es zunächst vom jeweiligen *filesharing*-System abhängig, ob nur *ein* Nutzer eine vollständige Datei überträgt oder mehrere. Bei Systemen mit zweiseitiger Dateiübertragung wie Gnutella[28] ist es lediglich eine Beweisfrage, ob jemand, der eine Datei anbietet, diese auch vollständig anbietet. Hierzu müsste ein Ermittler lediglich die entsprechende Datei von dem entsprechenden Nutzer herunterladen und könnte sodann überprüfen, ob sie vollständig ist. Anders verhält es sich bei Systemen mit mehrseitiger Dateiübertragung, insbesondere BitTorrent. Dort ist es ausgeschlossen, dass ein einzelner Nutzer anderen Nutzern eine vollständige Datei zugänglich macht, unabhängig davon, ob der jeweilige Nutzer die entsprechende Datei selbst vollständig auf seinem Rechner gespeichert hat oder nicht. Denn der Übertragungsvorgang läuft dort dergestalt ab, dass andere Nutzer von diesem jeweils nur einzelne Segmente der Zieldatei empfangen können, niemals aber dergestalt, dass ein Nutzer alle Segmente von *nur* einem anderen Nutzer empfängt.[29]

Folglich ist auch irrelevant, dass es für die öffentliche Zugänglichmachung nach § 19a UrhG nur auf die Zugriffsmöglichkeit ankommt und nicht darauf,

---

[27] Siehe Kapitel § 4 VIII. 10.

[28] Siehe Kapitel § 1 II. 4. b).

[29] Siehe hierzu genauer Kapitel § 1 II. 5. b). So auch *Solmecke/Bärenfänger*, MMR 2011, 567, 568.

ob diese Möglichkeit auch genutzt wurde[30]. Denn bei Systemen wie BitTorrent besteht nicht einmal die Möglichkeit, dass ein einzelner Nutzer eine Datei vollständig zugänglich macht. Dieses Problem kann nicht – wie beispielsweise vom OLG Köln[31] – durch eine Betrachtungsweise dahingehend umgangen werden, dass die Bereitstellung einzelner Dateifragmente (durch einen Nutzer A) letztlich ein adäquat-kausaler Beitrag zur Zusammensetzung der vollständigen Datei bei den Nutzern ist, die die einzelnen Dateifragmente von Nutzer A empfangen haben. Denn eine solche Gesamtbetrachtungsweise rechnet die Tatbeiträge der anderen Nutzer, die die übrigen Dateifragmente beisteuern, faktisch Nutzer A zu. Eine solche Zurechnung ist aber allenfalls im Rahmen der Mittäterschaft möglich[32], weshalb deren Voraussetzungen gegeben sein müssen.[33] Eine Zurechnung über die Abkürzung „Kausalität" würde diese Voraussetzungen unterlaufen.

Die Rechtsprechung steht also vor dem Problem, dass für das mittlerweile faktisch einzig relevante *filesharing*-System BitTorrent fraglich ist, ob ein einzelner Nutzer dort überhaupt eine öffentliche Zugänglichmachung nach § 19a UrhG begeht.[34] In der Entscheidung „Tauschbörse I" war noch das Gnutella-System streitgegenständlich[35], von daher konnte der BGH dieses Problem dort noch grundsätzlich ignorieren.[36]

In der Entscheidung „Konferenz der Tiere"[37], in der das BitTorrent-System

[30] Vgl. EuGH, Urteil vom 14. Juni 2017, Rs. C-610/15, Rz. 31 – ECLI:EU:C:2017:456 - „The Pirate Bay", mit weiteren Nachweisen der Rechtsprechung.

[31] OLG Köln, Beschluss vom 20. April 2016, Az. I-6 W 37/16, Rz. 20 – juris.

[32] *Solmecke/Bärenfänger*, MMR 2011, 567, 570f.

[33] Siehe hierzu sogleich Kapitel § 4 II. 4.

[34] Gleiches gilt prinzipiell auch für die Vervielfältigung nach § 16 UrhG. Diese ist aber schon nicht Gegenstand der Ermittlungen durch die Rechteinhaber, siehe Kapitel § 1 IV. 7. c) dd). Zudem wird in der Praxis ohnehin nur die öffentliche Zugänglichmachung geltend gemacht, da allein diese für den Schadensersatz interessant ist, siehe Kapitel § 3 VI. Das Problem der segmentierten Übertragung stellt sich aber bei der Vervielfältigung ähnlich wie bei der öffentlichen Zugänglichmachung, vgl. *Brinkel*, Filesharing, S. 100f.

[35] Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 3 – GRUR 2016, 176 - „Tauschbörse I".

[36] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 26ff. – GRUR 2016, 176 - „Tauschbörse I". Allerdings hätte der BGH dann das Ausmaß der zur Verfügung gestellten Dateifragmente bei der Berechnung des Schadensersatzes berücksichtigen müssen, siehe hierzu auch Kapitel § 5 VII.

[37] Siehe hierzu Kapitel § 2 XI. 5.

streitgegenständlich war, umgeht der BGH die Frage, ob ein urheberrechtlich relevantes Zurverfügungstellen von Dateifragmenten anzunehmen ist, indem er gleich auf die wechselseitige Zurechnung der Übertragung von Dateifragmenten über die Mittäterschaft abstellt. Diese Lösung ist jedoch bei genauer Betrachtung der Funktionsweise von BitTorrent nicht tragfähig.[38]

Besser wäre es daher gewesen, wenn der BGH das Zurverfügungstellen von Dateifragmenten urheberrechtlich bewertet hätte. Unproblematisch ist dabei zunächst, dass einzelnen Teilen eines Werkes ebenfalls Werkscharakter zukommen kann.[39] Streng genommen existiert der Begriff des „Werkteils" auch gar nicht, da für jeden betrachteten Gegenstand gesondert zu fragen ist, ob dieser eine geistige Schöpfung verkörpert oder nicht.[40] Auch Leistungsschutzrechte nach §§ 85 und 94 UrhG können schon bei der öffentlichen Zugänglichmachung einzelner Dateifragmente betroffen sein.[41] Die Unterscheidung zwischen Leistungsschutzrechten und Werk*teilen* dürfte beim *filesharing* jedoch unerheblich sein, da die relevanten Dateifragmente, soweit sie der Wahrnehmung zugänglich sind, Inhalte aufweisen, die Werkscharakter haben (einzelne Laufbilder einer Filmdatei, kurze Abschnitte eines Musikstückes etc.)[42], sodass diese letztlich dahinstehen kann.

Entscheidend ist vielmehr die vorgelagerte Frage, wie die bei einigen Dateiformaten fehlende Wahrnehmbarkeit von Fragmenten (von Dateien dieser Formate) urheberrechtlich zu bewerten ist. Wie bereits in Kapitel § 1 III. aufgezeigt, können sich hier bei verschiedenen Dateiformaten Unterschiede ergeben. Bei Videoformaten wie .avi oder Audioformaten wie .mp3 können wenige Dateifragemente dafür genügen, dass wenigstens ein oder mehrere

[38] Siehe hierzu sogleich Kapitel § 4 II. 4.

[39] EuGH, Urteil vom vom 4. Oktober 2011, Rs. C-403/08, C-429/08, Rz. 156f. – ECLI:EU:C:2011:631 - „Football Association Premier League"; EuGH, Urteil vom 16. Juli 2009, Rs. C-5/08, Rz. 39 – ECLI:EU:C:2009:465 - „Infopaq International". Folglich sind Rechtsauffassungen wie die des AG Braunschweig, Urteil vom 13. Oktober 2015, Az. 117 C 2852/15 – unveröffentlicht, die für § 19a UrhG einen vollständigen Upload der Datei fordern, unzutreffend, unabhängig davon, dass es einen solchen vollständigen Upload bei BitTorrent schon gar nicht geben kann.

[40] *Ahlberg* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 2 UrhG, Rz. 164.

[41] EuGH, Urteil vom 29. Juli 2019, Rs. C-476/17, Rz. 29ff.. – ECLI:EU:C:2019:624 - „Pelham". Ausnahmen sind demgemäß nur zum Zwecke des künstlerischen Schaffens denkbar. Siehe hierzu näher BGH, Urteil vom 30. April 2020, Az. I ZR 115/16, Rz. 22ff. – GRUR 2020, 843 - „Metall auf Metall IV".

[42] *Heckmann/Nordmeyer*, CR 2014, 41, 43.

Laufbilder des Videos bzw. nicht unerhebliche Teile eines Musikstückes abgespielt werden können.[43] Wahrnehmbarkeit kann dort also bereits bei Übertragung einiger Dateifragmente gegeben sein, die in ihrer wahrnehmbaren Form wiederum Werksschutz genießen und somit wiederum zumindest eine öffentliche Zugänglichmachung hinsichtlich dieser Fragmente vorliegt. Probleme ergeben sich dagegen zivilprozessual, da die theoretisch bestehende Möglichkeit, dass urheberrechtlich geschützte Werks„teile“ öffentlich zugänglich gemacht wurden, nicht den Nachweis einer solchen Behauptung erübrigt.[44] Gegenwärtig geben Ermittlungsdienste jedoch nur den Zeitraum bzw. einen Teil des Zeitraumes an, in dem sie Datenpakte von dem betroffenen Internetanschluss erhalten haben, sowie den Inhalt der vollständigen Datei, nicht jedoch den Inhalt der einzelnen Dateifragmente.[45] Dieser Nachweis kann nur dann entbehrlich sein, wenn es auf die Wahrnehmbarkeit nicht ankommt. Bei Archivdateien wie .rar oder .zip sowie .iso-Containern sind einzelne Fragmente derselben immer nur Datenmüll[46], sodass es bei diesen unabhängig von der praktischen Frage des Nachweises schon für die theoretische Möglichkeit der Urheberrechtsverletzung darauf ankommt, ob Letztere Wahrnehmbarkeit des potentiell verletzenden Fragments voraussetzt.

Die Lösung dieses Problems hängt davon ab, wie der Begriff „Schöpfung“ in § 2 Abs.2 UrhG auszulegen ist. Eine Schöpfung im Wortsinne kann zwar auch dann schon existieren, wenn sie die innere geistige Sphäre des Schöpfers noch nicht verlassen hat. Jedoch hat der BGH bereits in einer älteren Entscheidung überzeugend ausgeführt, dass es das Schutzanliegen des Urheberrechts ist, körperliche oder unkörperliche *Wiedergaben* eines geschützten Geistesgutes dem Urheber vorzubehalten.[47] Dies zeigt sich insbesondere an den Tatbeständen der Verwertungshandlungen der §§ 15ff. UrhG, die einen Akt eines Dritten in Bezug auf das jeweilige Werk voraussetzen. Das Schutzanliegen des Urhebers ist also nicht betroffen, wenn seine geistige Schöpfung einer Wahrnehmung eines Dritten nicht, auch nicht mit technischen Hilfsmitteln, zugänglich ist.[48] Für Leistungsschutzrechte kann dabei nichts anderes

43 *Heckmann/Nordmeyer*, CR 2014, 41, 42f.
44 *Solmecke/Bärenfänger*, MMR 2011, 567, 571f.
45 Siehe Kapitel § 1 IV. 7. c) dd).
46 Siehe Kapitel § 1 III.
47 BGH, Beschluss vom 27. Februar 1962, Az. I ZR 118/60, Rz. 21 – juris.
48 BGH, Beschluss vom 27. Februar 1962, Az. I ZR 118/60, Rz. 21 – juris.

gelten, da deren Zweck der Investitionsschutz ist[49] und dieser bei fehlender Wahrnehmbarkeit ebenfalls nicht vereitelt wird.

In die gleiche Richtung scheint die – bereits zitierte – Rechtsprechung des EuGH zu Werksteilen zu gehen. Demnach setzt der Schutz von Werks„teilen" voraus, dass diese eine eigene geistige Schöpfung ihres Urhebers „*zum Ausdruck*" bringen.[50] Das deutet ebenfalls auf das Erfordernis eines nach außen wahrnehmbaren Wiedergabeaktes hin. Die Wahrnehmbarkeit wird – darauf sei im Übrigen hingewiesen – auch von der Literatur für erforderlich gehalten.[51] Die einzig bekannte Gegenansicht hat das OLG Celle in Bezug auf Computerprogramme geäußert.[52] Bei solchen sei es für einzelne Datenteile nicht erforderlich, dass diese autonom abgespielt werden können. Das OLG Celle beruft sich hierfür auf eine Kommentarstelle von *Wandtke/Bullinger*[53], gibt diese jedoch falsch wieder. Dort wird nicht behauptet, dass einzelne Datenfragmente nicht autonom abspielbar sein müssten, sondern einzelne Unterfunktionen eines Programms.[54] Es handelt sich hierbei um einen völlig anderen Sachverhalt als die Frage der Wiedergabefähigkeit von Dateifragmenten von Computerprogrammen, da bei solchen ein Hauptprogramm, mit dem sie zusammen abgespielt werden könnten, nicht existiert (sonst wären es ja keine Fragmente). Folglich bleibt es dabei, dass auch bei Dateifragmenten von Computerprogrammen auf das Erfordernis der Wahrnehmbarkeit nicht verzichtet werden kann.

Im Ergebnis bleibt damit festzuhalten, dass eine *filesharing*-Aktivität mittels BitTorrent – isoliert von den Aktivitäten anderer BitTorrent-Nutzer – nur bei bestimmten Dateitypen (vor allen Video-und Audiodateien) als öffentliche Zugänglichmachung gewertet werden kann (und auch bei diesen nur unter bestimmten Umständen, die nachzuweisen sind), bei Archivda-

[49] Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 20ff. – GRUR 2018, 400 - „Konferenz der Tiere".

[50] EuGH, Urteil vom vom 4. Oktober 2011, Rs. C-403/08, C-429/08, Rz. 156 – ECLI:EU:C:2011:631 - „Football Association Premier League" ; EuGH, Urteil vom 16. Juli 2009, Rs. C-5/08, Rz. 39 – ECLI:EU:C:2009:465 - „Infopaq International".

[51] *Heckmann/Nordmeyer*, CR 2014, 41, 42, mit weiteren Nachweisen.

[52] OLG Celle, Urteil vom 26. Januar 2017, Az. 13 U 113/16 – aw3p.de.

[53] Nämlich *Grützmacher* in: Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, § 69a UrhG, Rz. 12.

[54] Eine Abspielbarkeit der Unterfunktionen zusammen mit dem Hauptprogramm ist jedoch auch nach dieser Literaturansicht erforderlich.

teien und .iso-Containern *niemals*. Und auch bei ersteren Dateitypen kann eine öffentliche Zugänglichmachung stets allenfalls nur in Bezug auf die Dateifragmente angenommen werden, die auch tatsächlich an andere Nutzer hochgeladen wurden, da bei allen anderen Dateifragmenten nicht einmal eine theoretische Zugriffsmöglichkeit auf ein Werk besteht.

Die BGH-Rechtsprechung, insbesondere die Entscheidung „Konferenz der Tiere“, ist insofern zu kritisieren, als dass sie diesen Aspekt überhaupt nicht behandelt hat. Zwar können bei der Annahme einer mittäterschaftlichen Haftung – wie sie der BGH aufstellt – die Auswirkungen einer isolierten Betrachtung der einzelnen Täter dahingestellt bleiben; jedoch ist selbst nach der Rechtsprechung des BGH bei BitTorrent nicht immer eine mittäterschaftliche Haftung der Nutzer anzunehmen, sondern nur regelmäßig[55], sodass es auch unter Geltung dieser Rechtsprechung unter Umständen auf eine isolierte Betrachtung jener ankommen kann.

Darüber hinaus ist ohnehin – wie sogleich aufgezeigt wird – die Lösung über die Mittäterschaft an sich problematisch.

4. Zur Mittäterschaft auf Seiten der Endnutzer

a) Problemverschiebung durch den BGH

Die in der Entscheidung „Konferenz der Tiere“[56] gefundene Lösung, die einzelnen Nutzer des BitTorrent-Systems in Bezug auf die untereinander getauschten Dateifragmente als Mittäter anzusehen, löst zwar zunächst das Problem der möglicherweise fehlenden Wahrnehmbarkeit und Schutzrechtsfähigkeit[57] der von den einzelnen Nutzern jeweils ausgesandten Dateifragmente, da auf Grund der Mittäterschaft die isolierte Betrachtung dieser Fragmente aufgehoben und stattdessen auf das „Gesamtergebnis“, also alle von den jeweils als Mittäter angesehenen Nutzer (für den Zeitraum, in denen sie Mittäter sind) ausgesandten Dateifragmente *zusammengenommen* abgestellt wird.

Diese Lösung verschiebt das Problem der möglicherweise fehlenden Wahrnehmbarkeit und Schutzrechtsfähigkeit jedoch nur auf das „Gesamtergebnis“,

[55] Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 27 – GRUR 2018, 400 - „Konferenz der Tiere“.

[56] Siehe zur Zusammenfassung Kapitel § 2 XI. 5.

[57] Siehe Kapitel § 4 II. 3.

da auch diesem die Wahrnehmbarkeit und Schutzrechtsfähigkeit fehlen kann. Denn dass von allen Mittätern zusammengenommen immer eine vollständig zugängliche und abspielbare Datei öffentlich zugänglich gemacht wird, ist nicht zwingend.[58] Dies übergeht der BGH in „Konferenz der Tiere".[59] Da sich aber bisher erst vereinzelt Instanzgerichte zu diesem Punkt äußern konnten, wird dieser an anderer Stelle *de lege lata* erörtert.[60]

b) Dogmatische Kritik der Lösung des BGH

Die Lösung des BGH stellt nicht nur eine Problemverschiebung dar, sondern ist auch rechtsdogmatisch überwiegend problematisch und nur teilweise unproblematisch.

aa) Strafrechtsakzessorietät und alternative Kausalität

Keine Bedenken bestehen zunächst gegen die weithin anerkannte Akzessorietät[61] der zivilrechtlichen Täterschafts- und Teilnahmedogmatik zu den Grundlagen der strafrechtlichen[62], welche letztlich allerdings nicht mehr bedeutet, als dass mit den grundsätzlichen dogmatischen Konzepten der Strafrechtslehre- und Rechtsprechung gearbeitet wird, ohne dass hieraus eine bedingungslose Anbindung an selbige erfolgt.[63]

Eine Differenzierung zwischen Beihilfe und Mittäterschaft ist wegen § 830 Abs.2 BGB normalerweise nicht erforderlich, beim BitTorrent-*filesharing* allerdings schon, da eine Tat überhaupt erst durch das kumulative und alternative Zusammenwirken[64] der Nutzer entsteht, es mithin ohne die Betrachtung der Nutzer als Mittäter keine Tat gäbe, zu der Beihilfe geleistet werden könnte.

---

58 *Rüthers*, K&R 2018, 308, 309.

59 Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 26 – GRUR 2018, 400 - „Konferenz der Tiere".

60 Siehe Kapitel § 5 III. 3.

61 BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 25 – GRUR 2018, 400 - „Konferenz der Tiere"; BGH, Urteil vom 10. Januar 2019, Az. I ZR 267/15, Rz. 107 – GRUR 2019, 813 - „Cordoba II".

62 Es erscheint unproblematisch, § 830 Abs.1 Satz 1 und Abs.2 BGB in systematischer Hinsicht zu § 25 StGB auszulegen, wobei hiermit kein Erkenntnisgewinn verbunden ist, da auch § 25 StGB die Mittäterschaft lediglich als gemeinsame Begehung einer Handlung definiert.

63 *Wagner* in: Säcker et al., MüKo-BGB, 8. Aufl. 2020, § 830 BGB, Rz. 9.

64 Hierzu sogleich Kapitel § 4 II. 4. b) bb).

Handelnde werden als Mittäter, also als gemeinsam Handelnde, angesehen, wenn sie jeweils objektive Tatbeiträge erbringen und dabei bewusst und gewollt zusammenwirken.[65]

Zutreffend ist die Aussage des BGH, dass in der Bereitstellung von Dateifragmenten an sich ein objektiver Tatbeitrag zu sehen ist[66], auch wenn er dabei das Problem der gemischt kumulativen und alternativen Kausalität der einzelnen Tatbeiträge übersieht. Wie bei Gremienentscheiden mit überschießender Mehrheit (die im Strafrecht den Standardfall der gemischt kumulativen und alternativen Kausalität bilden) auch könnte sich ein BitTorrent-Nutzer darauf berufen, dass die anderen Nutzer, die von ihm Dateifragmente empfangen haben, auf ihn hätten verzichten können, da sie diese Dateifragmente genauso gut von einem anderen Nutzer hätten empfangen können. Das ist faktisch zunächst zutreffend und würde nur in dem – praktisch wohl äußerst seltenen – Fall nicht gelten, in dem ein Dateifragment, das der betreffende Nutzer einbringt, bei keinem anderen Nutzer im Schwarm vorhanden war.[67]

Rechtlich lässt sich dieser Einwand so formulieren, dass der betrachtete Tatbeitrag zwar kumulativ mit anderen Tatbeiträgen zusammengenommen die Tat bedingt, jedoch lediglich alternativ kausal ist, da an seine Stelle auch andere Beiträge hätten treten können – mithin der einzelne Beitrag keine *conditio sine qua non* für den Taterfolg ist.

Würde dieser Einwand durchgreifen, stünde er jedem Nutzer zu, sodass letztlich kein Nutzer für die Bereitstellung einer *vollständigen* Zieldatei verantwortlich wäre, sondern allenfalls für die öffentliche Zugänglichmachung der von ihm jeweils selbst hochgelandenen Dateifragmente[68].

Der Einwand ist rechtlich allerdings unbeachtlich. Dies lässt sich im Zivilrecht mit einem Schluss *a fortiori* aus § 830 Abs.1 Satz 2 BGB begründen[69]: wenn

---

65 Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 25f. – GRUR 2018, 400 - „Konferenz der Tiere“, mit weiteren Nachweisen.

66 BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 25 – GRUR 2018, 400 - „Konferenz der Tiere“.

67 Zum sogenannten *missing piece syndrom* siehe Kapitel § 5 III. 3.

68 Siehe hierzu Kapitel § 4 II. 3.

69 Vgl. *Röckrath*, NStZ 2003, 641, 644f.

gemäß dieser Norm ein nicht gemeinschaftlich mit anderen Handelnder[70] für einen Schaden auch dann haften muss, wenn die Kausalität seines Handels für den Schaden nicht feststeht, so muss dies erst recht für gemeinschaftlich Handelnde gelten, bei denen immerhin die kumulative Kausalität feststeht.

Im Lichte des Ideals dogmatischer Stringenz und Vollständigkeit wäre es wünschenswert gewesen, wenn sich der BGH mit diesem Punkt auseinandergesetzt hätte, auch wenn dieser letztlich nichts am Ergebnis ändert.

bb) Objektiver Tatbeitrag ja, aber wofür?

Der BGH nimmt einen objektiven Tatbeitrag der einzelnen BitTorrent-Nutzer für eine öffentliche Zugänglichmachung nach § 19a UrhG an.[71] Für diese Annahme müsste also ein Kollektiv aus Mittätern auf Grund der Tatbeiträge, die die Mittäterschaft begründen, eine ein urheberrechtlich geschütztes Werk verkörpernde Datei einer Öffentlichkeit in einer Weise zugänglich machen, dass sie Mitgliedern dieser Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist. Nach ständiger Rechtsprechung des EuGH meint der Begriff der Öffentlichkeit eine unbestimmte Anzahl potentieller Leistungsempfänger, die zumindest „*recht viele Personen*“ betragen muss.[72] Der BGH hat dies zum Beispiel in der Entscheidung „Krankenhausradio“ präzisiert und das Vorliegen von „recht vielen Personen“ bei 49 Krankenhaus-Zimmern, die im Schnitt zu 80 Prozent belegt waren, bejaht.[73]

Das Vorliegen einer Öffentlichkeit bei BitTorrent-*filesharing* wäre beispielsweise unproblematisch der Fall, wenn in einem gedachten BitTorrent-System die Nutzer A, B, C und D einer Vielzahl von anderen Nutzern gemeinsam eine Datei übertragen, d.h. diese anderen Nutzern empfangen jeweils alle

[70] Der Norm der Wortlaut – „*mehrere Beteiligte*“ – ist missverständlich; gemeint ist, dass verschiedene Personen, die unabhängig voneinander gehandelt haben und eine der Handlungen einen Schaden verursacht haben muss, als Gesamtschuldner für den Schaden haften, auch wenn nicht feststeht, welche der Handlungen letztlich kausal für den Schaden war, siehe *Spindler* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 830 BGB, Rz. 16.

[71] BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 16 – GRUR 2018, 400 - „Konferenz der Tiere“.

[72] EuGH, Urteil vom 14. Juni 2017, Rs. C-610/15, Rz. 27 – ECLI:EU:C:2017:456 - „The Pirate Bay“, mit weiteren Nachweisen.

[73] BGH, Urteil vom 11. Januar 2018, Az. I ZR 85/17, Rz. 35f. – GRUR 2018, 608 - „Krankenhausradio“.

Dateifragmente, die sie benötigen, *exklusiv* von A, B, C und D, ohne dass diese anderen Nutzer selbst an der Zugänglichmachung der Datei mitwirken. So funktioniert BitTorrent jedoch nicht. Wie dargestellt[74], baut ein Nutzer niemals eine Verbindung zu allen anderen Nutzern des Schwarms, nicht einmal zu allen anderen Nutzern eines (im Falle der Tracker-Nutzung) *peer sets* auf und der Upload erfolgt regelmäßig immer nur an maximal vier Personen gleichzeitig, wobei davon auszugehen ist, dass die Personen, an die hochgeladen wird, nur nach und nach wechseln.

Beispielsweise empfängt also ein Nutzer A alle benötigten Dateifragmente von den Nutzern B, C, D und E. Nutzer B empfängt alle benötigten Dateifragmente von den Nutzern A, C, D, E und F. Nutzer C wiederum alle benötigten Dateifragmente von B sowie, im Übrigen, von völlig anderen Nutzern (G, H, usw.). Bezüglich A haben also B, C, D und E als Mittäter für eine Vervielfältigung (!) zusammengewirkt, weil sie alle Dateifragmente beigesteuert haben, die A für die Zusammensetzung der vollständigen Datei auf seiner Festplatte benötigt hat[75]. Eine öffentliche Zugänglichmachung der vollständigen Datei haben sie jedoch nicht begangen, da sie im Übrigen nicht als Gemeinschaft für die Zusammensetzung von Dateifragmenten zu einer vollständigen Datei bei anderen Nutzern verantwortlich sind, mithin kein Werk „recht vielen Personen“ öffentlich zugänglich gemacht haben. Gleiches lässt sich bezüglich Nutzer B für die Nutzer A, C, D, E und F sagen. Nutzer C hat zwar sowohl für Nutzer A und für Nutzer B dabei mitgewirkt, dass diese eine vollständige Datei haben, aber eben jeweils mit zum Teil unterschiedlichen Personen. Zudem kann sich auch sein objektiver Tatbeitrag jeweils unterscheiden, d.h. die Dateifragmente die er an A übertragen hat, müssen nicht die Dateifragmente sein, die er an C übertragen hat.

Ein Nutzer wirkt also während seiner Teilnahme an einem BitTorrent-Schwarm an der Zusammensetzung einer vollständigen Datei bei mehreren (aber wegen des *choke*-Algorithmus auch nicht bei sehr vielen) anderen Nutzern mit, jedoch jeweils zusammen mit zum Teil verschiedenen anderen Nutzern und verschiedenen Beiträgen (also verschiedenen Dateifragmenten). Die wechselseitige Zurechnung der jeweils in die verschiedenen „Nutzerkollekti-

[74] Siehe Kapitel § 1 II. 5. a) und b).

[75] A ist also auch Mittäter zusammen mit B, C, D und E für die Vervielfältigung der Datei auf seiner Festplatte, da sein Tatbeitrag die Bereitstellung seiner Festplatte zu diesem Zweck ist.

ven“ eingebrachten Beiträge wäre rechtlich also nur möglich, wenn es das Institut einer „Meta-Mittäterschaft“ gäbe, demzufolge die Handlungen verschiedener Handlungsgemeinschaften wechselseitig zugerechnet werden. § 830 BGB und § 25 StGB beziehen sich aber ihrem Wortlaut nach eindeutig auf das gemeinschaftliche Handeln einzelner Individuen, nicht das gemeinschaftliche Handeln unterschiedlich konstituierter Kollektive.

Folglich ist es auch irrelevant, wenn der BGH zur Begründung seiner Auffassung schreibt, dass der Teilnehmer an einem BitTorrent-Schwarm „*Dateifragmente von vielen verschiedenen Teilnehmern*“ empfängt[76], da es für die öffentliche Zugänglichmachung nicht darauf ankommt, von wem ein einzelner Teilnehmer seine Dateifragmente empfängt, sondern entscheidend ist, von wem die Öffentlichkeit (!), also recht viele Personen, Dateifragmente empfängt oder jedenfalls empfangen kann.

Ein einzelner Nutzer kann mithin, seine objektiven Tatbeiträge betrachtet, nur Mittäter für die Vervielfältigung der Zieldatei auf seiner eigenen Festplatte sein (der objektive Tatbeitrag ist hier das Zurverfügungstellen des Festplattenspeicherplatzes) sowie Mittäter für die Vervielfältigung der Zieldatei auf den Festplatten anderer Nutzer, an die er Dateifragmente hochgeladen hat (der objektive Tatbeitrag ist hier das Zusammenwirken mit anderen Nutzern zum Zwecke der Vervielfältigung der Datei auf der Festplatte des jeweiligen „Zielnutzers“) – und selbst diese Lösung ist, wie jede mittäterschaftliche Lösung im Rahmen des BitTorrent-Systems mit Folgeproblemen behaftet.[77]

Eine öffentliche Zugänglichmachung der vollständigen Datei kann im Ergebnis nur der *initial seeder*[78] begehen. Zwar gibt es auch in Bezug zu diesem wegen der Mechanik des BitTorrent-Systems keine Öffentlichkeit, die die vollständige Datei *exklusiv* von ihm bezieht; da aber zu Beginn niemand außer ihm alle Fragmente einer Datei hat, begeht er zumindest eine öffentliche Zugänglichmachung jedes einzelnen Fragments – und damit auch der gesamten Datei.

---

[76] BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 26 – GRUR 2018, 400 - „Konferenz der Tiere“.

[77] Siehe hierzu Kapitel § 5 II. 1.

[78] Siehe hierzu Kapitel § 1 II. 5. b).

cc) Fehlendes Publikum

Die mittäterschaftliche Lösung geht aus einem weiteren Grund fehl. Selbst unterstellt, BitTorrent würde der Vorstellung des BGH entsprechend funktionieren und *alle* Teilnehmer eines Schwarms würden an der Bereitstellung der jeweiligen Zeildatei technisch zusammenwirken, würde es dennoch an einer Zugänglichmachung für Mitglieder der Öffentlichkeit im Sinne von § 19a UrhG fehlen. Denn die Mitglieder der Öffentlichkeit und der Verwerter dürfen nicht identisch sein.[79] Dies legt schon der Wortlaut nahe, der zwischen der Zugänglichmachung einerseits und der Öffentlichkeit andererseits trennt; zudem lässt sich dies auch aus Erwägungsgrund 23 InfoSocRL ableiten, demzufolge der Tatbestand der öffentlichen Wiedergabe eine Wiedergabe an die Öffentlichkeit umfasst, die an dem Ort, an dem die Wiedergabe ihren Ursprung nimmt, nicht anwesend ist. Wenn aber alle Schwarmteilnehmer Mittäter der Zugänglichmachung sind, kann es außerhalb des Schwarms keine Öffentlichkeit geben, die die jeweilige Zieldatei vom Schwarm empfängt; wer die Datei empfangen möchte, wird notwendigerweise selbst Teil des Schwarms.

Damit stellt sich schon nicht mehr die Frage, ob es bei BitTorrent-*filesharing* ein *neues Publikum* geben kann.[80]

dd) Objektiver Tatbeitrag und anwendbares Recht

Vom BGH unbeachtet bleibt das Problem, dass diejenigen BitTorrent-Nutzer, die seiner Auffassung nach für eine mittäterschaftliche öffentliche Zugänglichmachung zusammenwirken, nicht alle notwendigerweise von dem Gebiet der Bundesrepublik Deutschland aus handeln müssen, da das

[79] *Götting* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 19a UrhG, Rz. 8.

[80] Das Kriterium des neuen Publikums hätte deswegen problematisch sein können, weil der EuGH mittlerweile auch den Betreibern von BitTorrent-Indexseiten eine öffentliche Zugänglichmachung zuschreibt, siehe Kapitel § 5 II. 1. Wenn bereits der Betreiber der Indexseite ein Werk öffentlich zugänglich macht, könnte fraglich sein, ob es dann noch die Nutzer des Schwarms tun, die sich ja zunächst Hashwert und Tracker-IPs von der Indexseite besorgen müssen. Jedoch hat der EuGH das Kriterium des „neuen Publikums“ mittlerweile so bestimmt, dass ein Upload immer dann an ein neues Publikum gerichtet ist, wenn mit einer konkludenten Einwilligung des Rechteinhabers nicht gerechnet werden kann, siehe Nachweise bei *Ohly*, GRUR 2018, 996, 998ff. Dies ist bei *filesharing* natürlich in den allermeisten Fällen nicht gegeben. Ein neues Publikum ablehnend entsprechend auch Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 63f. – ECLI:EU:C:2020:1063 - „M.I.C.M.“

BitTorrent-System keine Ländergrenzen kennt.

Zunächst wäre also zu fragen, ob eine mittäterschaftliche öffentliche Zugänglichmachung auch dann angenommen werden kann, wenn einige der objektiven Tatbeiträge nicht im Rahmen von § 19a UrhG erfasst werden können, sondern nur im Rahmen einer anderen, § 19a des deutschen UrhG vergleichbaren nationalstaatlichen Norm, die also – auf EU-Ebene – Art. 3 Abs.1 InfoSoc oder – auf internationaler Ebene – Art. 8 WCT umsetzt. Eine solche Kombination verschiedener Schutzrechtsordnungen mittels den Regeln der Mittäterschaft erscheint aber unter Geltung des Territorialitätsprinzips[81] ausgeschlossen.

Folglich stellt sich hieran anschließend die Frage, ob der Upload-Vorgang im BitTorrent-System auch dann eine öffentliche Zugänglichmachung nach *deutschem* Urheberrecht ist, wenn er von außerhalb der Bundesrepublik initiiert wird.[82] Dies ließe sich mit dem Argument bejahen, dass wegen des Erfordernisses der Zugriffsmöglichkeit der Öffentlichkeit auf das entsprechende Werk von Orten und zu Zeiten ihrer Wahl, die öffentliche Zugänglichmachung nicht nur durch den Zugänglichmachenden, sondern auch durch die Zugreifenden konstituiert wird, mithin für den Handlungsort auch auf Letztere abzustellen ist.[83] Der Uploadvorgang von außerhalb der Bundesrepublik ist dann also eine Handlung *in* der Bundesrepublik, sobald auf die hochgeladenen Dateifragmente auch in der Bundesrepublik zugegriffen werden kann. Dies ist immer der Fall, da im BitTorrent-System verschiedene Regionen nicht kategorial voneinander getrennt werden. In dogmatisch etablierten Begriffen ausgedrückt wäre die genannte Lösung mithin eine Anwendung des sogenannten „Schutzlandsprinzips“ auf das Urheberrecht im Allgemeinen und § 19a UrhG im Speziellen[84], das ausdrücklich in Art. 8 Abs.1 Rom-II-VO normiert ist und entsprechend vom BGH auch im Urheberrecht nach ständiger

[81] Siehe hierzu *Lauber-Rönsberg* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, Kollisionsrecht und internationale Zuständigkeit, Rz. 4.

[82] Siehe zur Problematik des anwendbaren Rechts bei ubiquitären Immaterialgüterrechtsverletzungen *Kur*, WRP 2011, 971, 976ff.

[83] *Gesmann-Nuissl* in: Ernsthaler/Weidert, Urheberrecht und Internet, S. 608ff.

[84] *Schäufele*, Zur Strafbarkeit des Raubkopierens im Internet, S. 72ff.

Rechtsprechung zur Anwendung gelangt.[85]

Weitergehend ist also zu fragen, ob das Schutzlandprinzip auch auf etwaige mittäterschaftliche Tatbeiträge und deren Zurechnung Anwendung finden kann. Der Wortlaut des Art. 8 Abs. 1 Rom-II-VO scheint in dieser Hinsicht nicht eindeutig, da dieser nur das jeweils zu betrachtende Schuldverhältnis betrifft („*Auf außervertragliche Schuldverhältnisse […]*“). Einerseits könnte dies so zu verstehen sein, dass die mittäterschaftlichen Tatbeiträge nach dem Recht des Landes, von dem diese ausgehen, zu bewerten sind, da auch diesbezüglich ein Schuldverhältnis zwischen Rechteinhaber und etwaigem Mittäter besteht – was unter Berücksichtigung des Territorialitätsprinzips eine Zurechnung zu der von Deutschland aus handelnden Person ausschließen würde. Andererseits könnte das Schutzlandprinzip auch für die Regeln der Zurechnung des Handels Dritter innerhalb des konkret zu betrachtenden Schuldverhältnisses gelten – mit der Folge, dass eine Zurechnung möglich wäre. Letztere Auslegung könnte insbesondere dann naheliegen, wenn andernfalls eine Schutzlücke entstünde, weil andernfalls letztlich keine der handelnden Personen in Haftung genommen werden könnte.[86] Jedenfalls wäre dieser Aspekt vom BGH zu erörtern und gegebenenfalls mittels einer Vorlage zum EuGH zu klären gewesen.

Dogmatisch zu verankern wäre dieses materielle Problem schließlich im Rahmen der Beweislast, denn gemäß den üblichen Regeln der Beweislastverteilung müsste eigentlich der klagende Rechteinhaber beweisen, dass der objektive Tatbeitrag des Beklagten mit anderen objektiven Tatbeiträgen, die nach deutschem Recht zu berücksichtigen sind, für eine öffentliche Zugäng-

[85] Siehe zuletzt BGH, Urteil vom 21. April 2016, Az. I ZR 43/14, Rz. 24 – GRUR 2016, 1048 - „An Evening with Marlene Dietrich“. Die dort in den Rz. 16ff. vertieft erörterte Frage, wann internationale Zuständigkeit besteht, stellt sich in *filesharing*-Konstellationen nicht, da dort bisher lediglich Personen in Anspruch genommen werden, die jedenfalls zum Tatzeitpunkt einen Wohnsitz in Deutschland hatten; ob Rechteinhaber in Zukunft auch versuchen werden, Personen, die im Ausland ihren Wohnsitz haben, dort handeln und nach den dortigen Regeln ermittelt werden, in Deutschland zu verklagen, ist offen.

[86] Hierfür müsste aber für jeden Fall, mithin für jede in Betracht kommende Rechtsordnung geklärt werden, ob eine solche Schutzlücke tatsächlich besteht. Siehe zum vergleichbaren Problem im Patentrecht, wenn ein Arbeitsverfahren teils in Deutschland, teils im Ausland durchgeführt wird LG Düsseldorf, Urteil vom 28. Juli 2020, Az. 4a O 53/19 – GRUR 2020, 1078 - „Online-Sehtest“.

lichmachung zusammengewirkt hat. Der Nachweis kann nur gelingen, wenn das Schutzlandprinzip dergestalt angewendet wird, dass alle Beiträge nach deutschem Recht zu bewerten sind, denn nur dann steht auch fest, dass alle anderen Tatbeiträge in jedem Fall zu berücksichtigen wären. Ohne eine solche Anwendung könnte der Nachweis *nie* gelingen, da es dem Rechteinhaber unmöglich ist zu ermitteln, ob alle BitTorrent-Nutzer, die den Schwarm um die streitgegenständliche Datei gebildet haben, auch vom Gebiet der Bundesrepublik aus gehandelt haben.[87]

Eine dogmatische Lösung, die am Ergebnis des BGH nichts geändert hätte, wäre im Problemkreis „objektiver Tatbeitrag und anwendbares Recht", wie dargestellt, jedenfalls zumindest über das Schutzlandprinzip gangbar gewesen. Dass dies übersehen oder ignoriert wurde, ist im Licht des Ideals dogmatischer Stringenz und Vollständigkeit dennoch kritikwürdig.

ee) Bewusstes und gewolltes Zusammenwirken

Bezüglich des Merkmals des bewussten und gewollten Zusammenwirkens der BitTorrent-Nutzer ist dem BGH[88] zunächst darin zuzustimmen, dass Mittäterschaft nicht erfordert, dass sich die Beteiligten untereinander kennen[89]. Der Verweis auf das entsprechende strafrechtliche Präjudiz[90] überzeugt als Begründung zwar noch nicht, da auch dort keine Argumente für diese Ansicht genannt werden. Als Argument lässt sich allerdings der Wortlaut des § 830 Abs.1 Satz 1 BGB anführen, der für die Mittäterschaft nur das gemeinschaftliche Handeln, nicht aber eine innere Verbundenheit der gemeinschaftlich Handelnden fordert. Zuzustimmen ist dem BGH weiterhin darin, dass es unbeachtlich ist, wenn ein Nutzer nur den Download anstrebt, den Upload aber lediglich billigend in Kauf nimmt; ein solcher Eventualvorsatz ist nach ganz allgemeiner Meinung auch „echter" Vorsatz im Rechtssinne.

Unproblematisch ist (wenn auch vom BGH übersehen) im Ergebnis des Wei-

87 Ein entsprechender Anscheinsbeweis lässt sich wohl auch nicht bei Werken in deutscher Sprache aufstellen, da an diesen ein Interesse auch aus Österreich und der Schweiz sowie deutschsprachigen Personen im sonstigen Ausland besteht.

88 Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 27 – GRUR 2018, 400 - „Konferenz der Tiere".

89 Bei BitTorrent wissen die Nutzer schon nicht, von welchem anderen Nutzer derjenige, an den sie gerade Dateifragmente hochladen, die übrigen Dateifragmente empfängt.

90 BGH, Urteil vom 12. November 2009, Az. 4 StR 275/09 – NStZ 2010, 342.

teren die Tatsache, dass sich Nutzer aus einem BitTorrent-Schwarm frei ein- und ausklinken können, mithin ein objektiver Tatbeitrag sich unter Umständen erst im Zusammenhang mit Tatbeiträgen verwirklicht, die zu einem Zeitpunkt gesetzt wurden, als die Nutzer, die die vorherigen Tatbeiträge gesetzt hatten, bereits aus dem Schwarm ausgeklinkt sind. Zu diesem Zeitpunkt können sie keinen Vorsatz mehr darüber haben, mittäterschaftlich an einer öffentlichen Zugänglichmachung mitzuwirken. Jedoch fallen das Ein- und Ausklinken auf Deliktsebene zwischen Versuch und Vollendung, denn die Tatbeiträge wirken solange fort, wie eine vollständige Datei im Schwarm vorhanden ist. Die Geltung des Vorsatzes für den gesamten Zeitraum zwischen Versuch und Vollendung ist aber ohne weiteres anzunehmen, weshalb sich das Problem der Geltung des Vorsatzes für den Zeitraum zwischen Vollendung und Beendigung einer Tat („sukzessive Mittäterschaft“)[91] nicht stellt. Wenn im Ergebnis auch unproblematisch, hätten der dogmatischen Vollständigkeit halber die oben gennanten Punkt dennoch angesprochen werden sollen.

Nicht unproblematisch ist allerdings die Annahme des BGH, dass der Upload grundsätzlich billigend in Kauf genommen wird. Hierzu müssten sich die entsprechenden Nutzer überhaupt im Klaren sein, dass sie bei der BitTorrent-Nutzung einen Upload durchführen. Der BGH scheint mit Verweis auf die mittlerweile seit zehn Jahren stattfindende mediale Berichterstattung über Tauschbörsen einen „generellen Vorsatz“ anzunehmen, d.h. jeder der BitTorrent benutzt weiß auch, wie es funktioniert.[92] Die dieser Frage am nächsten kommende aktuelle empirische Erhebung – eine Erhebung des *Max-Planck-Instituts für Innovation und Wettbewerb* aus dem Jahr 2018 – stellte jedoch fest, dass sich von den deutschen Internetnutzern im Alter von über 12 Jahren 24 Prozent nicht sehr sicher und 23 Prozent überhaupt nicht sicher sind, was in Bezug auf das Herunterladen, Streamen und öffentliche Weitergeben von Inhalten im Internet legal ist und was nicht.[93] Es erscheint also auch fraglich, ob diese Nutzer sich über die technischen Funktionsweisen der genannten Phänomene vollständig im Klaren sind. Die Annahme eines solch generellen Vorsatzes erscheint mithin allein deswegen schon fragwür-

[91] *Joecks/Scheinfeld* in: Joecks/Miebach, MuekoStGB, 4. Aufl. 2020, § 25 StGB, Rz. 205ff.

[92] Vgl. BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 27 – GRUR 2018, 400 - „Konferenz der Tiere“.

[93] *Harhoff* et al., Nutzung urheberrechtlich geschützter Inhalte im Internet durch deutsche Verbraucher, S. 8.

dig. Hinzu kommt, dass der BGH diese Annahme wohl für die Benutzung der üblichen BitTorrent-Clients aufstellt. Abgesehen davon, dass es auch BitTorrent-Clients wie BitThief gibt[94], bei denen ein Upload nicht durchgeführt wird, der BGH sich also fragen müsste, warum dann nicht mehr Nutzer solche Clients verwenden, wenn sie doch alle wissen, wie Tauschbörsen funktionieren, ist eine BitTorrent-Nutzung nicht auf die herkömmlichen Clients beschränkt. BitTorrent kann auch in Streaming-Angeboten im Webbrowser zur Anwendung kommen[95]; dies dürfte auch vielen versierten Internetnutzern unbekannt sein.[96] Konsequenterweise müsste der BGH also zumindest bei Filmwerken vom klagenden Rechteinhaber Vortrag darüber fordern, über welche Plattform der Beklagte ermittelt wurde, um diese Variante rechtlich bewerten zu können. Jedoch tut der BGH dies nicht.

Weiterhin kann ein Vorsatz nicht generell angenommen werden, sondern muss in jedem einzelnen Fall gesondert geprüft werden.[97] Eine generelle Annahme kann allenfalls als Anscheinsbeweis eingekleidet werden. Ein solcher Anscheinsbeweis bringt aber gleich zwei Folgeprobleme mit sich: Ersteres manifestiert sich in dem Umstand, dass die Täterschaft eines beklagten Anschlussinhabers nur Kraft einer tatsächlichen Vermutung festgestellt wird[98]. Wenn der Anschlussinhaber aber schon die Täterschaft bestreitet, kann er gar nicht mehr bestreiten, bei Benutzung einer Tauschbörse in Unkenntnis über deren Funktionsweise gewesen zu sein[99], zumal der BGH solchen Vortrag schon im Rahmen der sekundären Darlegungslast betreffend die Täterschaft als unbeachtlich einstuft[100]! Ein solcher Anscheinsbeweis würde deswegen also *de facto* nicht nur zu einer Umkehr der materiellen Beweislast, sondern darüber hinaus sogar zu einer unwiderleglichen Vermutung führen. Solche Vermutungen können aber, wie sich aus § 292 ZPO ergibt, nur durch Gesetz aufgestellt werden, nicht jedoch über die richterliche Beweiswürdigung nach § 286 ZPO.[101]

---

94 Siehe hierzu Kapitel § 1 II. 5. c).

95 Siehe hierzu Kapitel § 3 XI. 2. a).

96 *Rüthers*, K&R 2018, 308, 309.

97 So im Ergebnis auch *Galetzka/Stamer*, K&R 2020, 486, 492.

98 Ausgenommen sind die Fälle, in denen der Anschlussinhaber die Täterschaft einräumt. Solche Fälle kommen nach Kenntnis des Verfassers aber praktisch ohnehin nie zu Gericht.

99 *Rüthers*, K&R 2018, 308, 309.

100 Siehe Kapitel § 2 VI. 3.

101 Zur Dogmatik des Anscheinsbeweises siehe Kapitel § 4 VII. 1. b).

Auch das zweite Folgeproblem liegt in der Konsequenz für die Beweislast begründet: nach üblicher Beweislastverteilung wäre es Aufgabe des klagenden Rechteinhabers, zu beweisen, dass *alle* BitTorrent-Nutzer, die den Schwarm um die jeweils streitgegenständliche Datei gebildet haben, den erforderlichen Mittätervorsatz hatten. Denn nach Auffassung des BGH konstituieren – wie dargestellt – nur die objektiven Tatbeiträge aller Nutzer zusammengenommen die mittäterschaftlich begangene öffentliche Zugänglichmachung. Über den Anscheinsbeweis entstünde also abermals *de facto* eine unwiderlegliche Vermutung, denn dem Anschlussinhaber ist es mangels Kenntnissen über die anderen Nutzer unmöglich, zu entkräften, dass diese Vorsatz betreffend die Funktion von Tauschbörsen hatten.

Die Beweisproblematik spinnt sich noch weiter fort. In ständiger Rechtsprechung des BGH ist anerkannt, dass über die Mittäterschaft objektive Tatbeiträge eines Handelnden einem anderen Handelnden dann nicht zugerechnet werden, wenn sie nicht dessen Vorstellung vom Tatplan entsprechen, sondern über dessen Vorstellung vom Tatplan hinaus gehen („Mittäterexzess“).[102] Wie dargestellt[103], können sich die Beiträge der einzelnen Nutzer eines BitTorrent-Schwarms sehr voneinander unterscheiden: ein Nutzer A kann beispielsweise in dem von ihm verwendeten BitTorrent-Client seine Uploadrate sehr niedrig einstellen und lediglich *leechen*, d.h. nach Erlangen der vollständigen Datei den BitTorrent-Schwarm sofort verlassen. Ein anderer Nutzer B könnte dagegen die Upload-Rate sehr hoch einstellen und auch nach Erlangen der vollständigen Datei im Schwarm als *seeder* verbleiben. Wieder ein anderer Nutzer C mag eine *seedbox* benutzen[104] und daher Uploadraten zum Schwarm beisteuern, die die Uploadraten von herkömmlichen Internetanschlüssen bei weitem übersteigen. Für Nutzer A, der seinen Beitrag zum Schwarm bewusst gering hält, stellen sich die Beiträge von B und C offensichtlich als Exzess dar, soweit sie seine Vorstellung vom Tatplan übersteigen; allerdings ist eine Trennung zwischen exzessiven Anteilen und nicht-exzessiven Anteilen eines Tatbeitrag kaum möglich. Folglich müsste ein exzessiv Handelnder *insgesamt* außer Betracht bleiben, da andernfalls – mangels der Möglichkeit der Trennung zwischen exzessiven und nicht-exzessivem

[102] *Spindler* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 830 BGB, Rz. 6, mit Nachweisen der Rechtsprechung.

[103] Siehe Kapitel § 1 II. 5. b) und IV. 7. c) dd).

[104] Siehe hierzu Kapitel § 1 IV. 6. b) bb).

Anteilen – der Exzess entgegen dem Vorsatz der anderen Nutzer diesen zugerechnet werden würde.

Da das Vorhandensein wechselseitig zurechenbarer Tatbeiträge eine für den klagenden Rechteinhaber günstige Tatsache ist, muss er auch beweisen, dass die Beiträge nach der Vorstellung der Schwarm-Teilnehmer jeweils nicht exzessiv sind. Dieser Nachweis ist praktisch nicht möglich, daher müsste im Rahmen der Lösung des BGH der klagende Rechteinhaber eigentlich mangels des Nachweises einer mittäterschaftlich begangenen öffentlichen Zugänglichmachung gegen den beklagten Anschlussinhaber unterliegen. Wollte man Ersterem wiederum einen Anscheinsbeweis dahingehend zusprechen, dass ein Exzess nicht vorliegt, so könnte der Anschlussinhaber diesen Anschein abermals niemals entkräften, da er erstens nicht darlegen kann, welcher Beitrag genau über seinen Anschluss erbracht wurde und zweitens, welchen Beitrag genau die jeweils anderen Nutzer im Schwarm erbracht haben. Im Ergebnis würde ein solcher Anscheinsbeweis also wieder *de facto* eine unwiderlegliche Vermutung begründen, was – wie dargestellt – unzulässig wäre.

ff) Unklare Folgen für den Schadensersatz

In „Konferenz der Tiere“ spricht der BGH nicht an, was die mittäterschaftliche Lösung für den Schadensersatz bedeutet, obwohl dies dringend erforderlich gewesen wäre. Der BGH scheint den gesamten BitTorrent-Schwarm als Mittäter anzusehen, die Größe eines solchen Schwarms ist aber allenfalls grob schätzbar.[105] Geht man zum Beispiel von einem üblichen Schadensersatzverlangen von EUR 700 für einen Film[106] und von einer geschätzten Größe des Schwarms von 700 Teilnehmern aus, so könnten die Teilnehmer untereinander betrachtet (gleiche Tatbeiträge zur Aufrechterhaltung des Schwarms unterstellt) für jeweils einen Euro haften (§ 840 Abs.1 iVm § 426 Abs.1 Satz 1 BGB), wobei der Rechteinhaber gemäß § 421 BGB den vollständigen Betrag aber von nur einem der 700 Teilnehmer einfordern dürfte.

In „Tauschbörse I“ hatte der BGH jedoch das Dateifragment-Problem erkannt und dennoch – ohne eine mittäterschaftliche Lösung einzuschlagen – die in den Instanzgerichten übliche Schadensberechnung weitestgehend ge-

[105] Siehe Kapitel § 1 II. 5. b).
[106] Siehe Kapitel § 3 V. 4. und 6.

billigt.[107] Denkbar wäre also auch, dass er für lediglich ein oder mehrere Dateifragmente EUR 700 Schadensersatz bereits als vertretbar ansieht. Dann müsste der Schadensersatz für die öffentliche Zugänglichmachung der ganzen Datei nicht EUR 700 insgesamt, sondern EUR 700 pro Teilnehmer betragen. Nach obigem Beispiel gerechnet wären dies EUR 490.000 insgesamt, die aber von jedem beliebigem Teilnehmer (einmal) *insgesamt* verlangt werden könnten!

gg) *ad absurdum* geführte Rechtsfolgen

Das *argumentum ad absurdum*[108] zeigt die Inakzeptabilität eines Auslegungsergebnisses an Hand seiner Folgen auf.[109]

Die mittäterschaftliche Lösung des BGH erfüllt unter zwei bzw. – die obige Schadensersatzberechnung mit einer Summe von EUR 490.000 einbezogen – drei Gesichtspunkten alle Voraussetzungen des *argumentum ad absurdum*[110]:

- Die Inanspruchnahme als Gesamtschuldner ohne jede – mangels Kenntnis darüber, welche Personen sich hinter den anderen Schwarmteilnehmern verbergen – realistische Möglichkeit des Regresses an den anderen Gesamtschuldnern erscheint absurd. Diese absurde Konsequenz ergibt sich aber zwingend aus der Lösung des BGH. Umgekehrt tritt diese Konsequenz bei der in dieser Arbeit vertretenen Lösung[111] nicht im selben Maße ein. Zuletzt lässt sich diese Konsequenz der Lösung des BGH nicht verhindern, insbesondere scheidet eine einschränkende Auslegung des § 421 BGB aus.

- Die fehlende Regressmöglichkeit erscheint in besonderem Maße absurd, wenn der Schadensersatz wie in obigem Beispiel EUR 490.000 betragen würde. Ein solcher Anspruch hätte für die allermeisten Privathaushalte die sofortige Privatinsolvenz zur Folge und dies bei einer Bagatellhandlung, bei der jeder Staatsanwalt das Strafverfahren einstellen würde,

[107] Siehe Kapitel § 2 VI. 1.

[108] Gemeint im rechtsmethodischen Sinne. Zur anderen Bedeutung im Sinne der allgemeinen Argumentationslehre siehe https://de.wikipedia.org/wiki/Reductio_ad_absurdum - Zugriff am 31.03.2021.

[109] *Möllers*, Juristische Methodenlehre, S. 168. Warum das *argumentum ad absurdum* anders als andere Rechtsfolgenargumente zulässig ist siehe Kapitel § 4 IV. 1. b).

[110] Siehe zu den Voraussetzungen *Möllers*, Juristische Methodenlehre, S. 168.

[111] Siehe Kapitel § 5 II. 1.

würde sie zur Anzeige gebracht.[112]

- Der dritte Gesichtspunkt ist das erwähnte Problem des Mittäterexzesses. Wie dargestellt scheidet ein exzessiv handelnder Teilnehmer aus der wechselseitigen mittäterschaftlichen Zurechnung zwingend aus.[113] Mit dieser Folge im Blick, könnte sich ein beklagter Anschlussinhaber, der seine „Täterschaft" gesteht, darauf berufen, dass er exzessiv gehandelt habe (zum Beispiel weil er seine Uploadrate besonders hoch eingestellt hat und im Schwarm nach erfolgreichem Download als *seeder* verblieben ist) und folglich aus dem Kreis der Mittäter ausscheide – mit im Vergleich hierzu günstigeren Rechtsfolgen (kein § 19a UrhG in Bezug auf die gesamte Datei) trotz höherem Beitrag zur Aufrechterhaltung des Schwarms!

Erste instanzgerichtliche Entscheidungen haben zumindest das Problem der fehlenden Regressmöglichkeit bereits erkannt und versuchen dieses dadurch abzumildern, dass sie vom klagenden Rechteinhaber einen schlüssigen Vortrag darüber fordern, gegen welche Mittäter er bereits vorgegangen ist und mit welchem Erfolg; ohne eine Erklärung hierüber sei der Vortrag zum Schaden unsubstantiiert.[114] Das ist begrüßenswert, vermag aber allenfalls bertrügerisches Verhalten in Form der nicht offenbarten, mehrfachen Geltendmachung von Schadensersatz einzudämmen. An der Möglichkeit, nur einen Verletzer auf den vollen Schadensbetrag in Anspruch zu nehmen, woraufhin dieser auf diesem Betrag „sitzen bleibt", vermag dies nichts zu ändern.

c) Widerspruch des BGH zu seiner früheren Rechtsprechung

Weniger ein dogmatischer Kritikpunkt, aber immerhin ein Schönheitsfehler ist, dass der BGH vor „Konferenz der Tiere" eine Lösung über die Mittäter-

[112] Siehe Kapitel § 2 II.
[113] Siehe Kapitel § 4 II. 4. b) gg).
[114] AG Frankenthal, Urteil vom 25. April 2018, Az. 3c C 251/17, Rz. 18 – juris.

schaft ausdrücklich abgelehnt hatte[115], hierauf bei besagtem Urteil aber mit keinem Wort eingeht. Tatsächlich war dem BGH das Problem der fehlenden Regressmöglichkeiten (dort ging es um die Kosten des Auskunftsverfahrens[116]) als Argument gegen die Annahme einer Mittäterschaft bekannt.[117]

5. Zum Verschulden

Nie in Frage gestellt, also implizit[118] angenommen hat der BGH auch das Verschulden nach § 97 Abs.2 UrhG.[119] Prinzipiell gilt hinsichtlich des Vorsatzes dasselbe wie zum im Rahmen der Mittäterschaft erforderlichen Vorsatz (fehlende Exkulpationsmöglichkeit bei täterschaftlicher Haftung kraft Vermutung, keine verbreitete Kenntnis über die Funktionsweise von Tauschbörsen, BitTorrent-Funktionalitäten im Webbrowser), sodass auf die dortigen Ausführungen verwiesen wird.[120]

Ausreichend für § 97 Abs.2 UrhG ist auch Fahrlässigkeit. Wegen der mittäterschaftlichen Lösung für § 19a UrhG[121] kann Fahrlässigkeit aber allenfalls für § 16 UrhG relevant werden, der gegenwärtig jedoch in *filesharing*-Verfahren nie geltend gemacht wird. Welcher Sorgfaltsmaßstab daher anzulegen wäre, kann dahinstehen; es soll lediglich darauf hingewiesen werden, dass nach Auffassung des Verfassers bei P2P-Streamingplattformen[122], die

[115] BGH, Beschluss vom 15. Mai 2014, Az. I ZB 71/13, Rz. 16f. – ZUM 2014, 967 - „Deus Ex“. Jedoch muss hierzu erwähnt werden, dass aus der Entscheidung nicht ausdrücklich hervorgeht, ob dort streitgegenständlich das BitTorrent-System war. Wäre beispielsweise Gnutella streitgegenständlich gewesen, käme eine mittäterschaftliche Lösung von vornherein nicht in Betracht. Da jedoch offensichtlich die Klägerin bzw. Beschwerdeführerin eine mittäterschaftliche Haftung in den Raum gestellt hat und das Verfahren sich zu einem Zeitpunkt abspielt, in dem außer BitTorrent kaum andere Tauschbörsen verwendet wurden (siehe Kapitel § 1 II. 4. f)), ist davon auszugehen, dass es in diesem Verfahren auch um BitTorrent ging.

[116] Siehe zur Analyse der Entscheidung zu diesem Punkt Kapitel § 4 VI.

[117] BGH, Beschluss vom 15. Mai 2014, Az. I ZB 71/13, Rz. 17 – ZUM 2014, 967 - „Deus Ex“.

[118] Eine sehr knappe Bejahung des Verschuldens findet sich in „Tauschbörse I“, siehe BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 53 – GRUR 2016, 176 - „Tauschbörse I“.

[119] Selbiges gilt soweit ersichtlich auch für die Instanzrechtsprechung abgesehen von seltenen Ausnahmen, beispielsweise AG Ingolstadt, Endurteil vom 22. Dezember 2016, Az. 16 C 1661/16, Rz. 38 – juris.

[120] Siehe Kapitel § 4 II. 4. b) ee).

[121] Siehe Kapitel § 4 II. 4.

[122] Siehe Kapitel § 3 XI. 2. a).

auf ihre P2P-Funktionalität nicht hinweisen, selbst die Annahme von leichter Fahrlässigkeit unvertretbar erscheint.

6. Bewertung der BGH-Rechtsprechung

Nach allem Vorgesagten verdient die Rechtsprechung des BGH nur betreffend der generellen Anwendung der Handlungsformen (Abgrenzung von Täterschaft und Störerhaftung) Zustimmung, im Übrigen aber – insbesondere hinsichtlich der verwertungsrechtlichen Erörterung des Uploadvorgangs bei BitTorrent und die Erfassung desselben mit der Mittäterschaft – nicht.

Besonders eindrücklich treten der fehlende Wille, das fehlende Problembewusstsein oder die fehlenden Kapazitäten zu Tage, eine genaue technische Analyse des jeweils streitgegenständlichen *filesharing*-Systems vorzunehmen bzw. (nach einer Rückverweisung an die Tatsacheninstanz[123]) vornehmen zu lassen. So hätte in „Tauschbörse I“ eigentlich eine Klarstellung dahingehend erfolgen müssen, dass diese Rechtsprechung nur das dort streitgegenständliche System (Gnutella) oder diesem ähnliche Systeme (also solche mit zweiseitiger Dateiübertragung) gelten kann, nicht aber für das – zum Zeitpunkt der Entscheidungsverkündung im Jahr 2015 überwiegend relevante – BitTorrent-System. Dieser Fehler zog sich folgerichtig durch das Gros der Instanzrechtsprechung. Umgekehrt ist auch „Konferenz der Tiere“ – unabhängig von seinen ohnehin bestehenden dogmatischen Problemen – nicht verallgemeinerbar, also wiederum nicht auf alle *filesharing*-Systeme anwendbar, sondern nur auf solche, die hinsichtlich der Datenübertragung wie BitTorrent funktionieren.

Findet hier kein Umdenken statt, wird es bei den aufgezeigten absurden rechtlichen Konsequenzen bleiben; zukünftige Entscheidungen des BGH, die

[123] Denn dort finden sich lediglich Feststellungen zum Aspekt Dateifragemente als Datenmüll, siehe LG Frankenthal, Urteil vom 22. Juli 2016, Az. 6 S 22/15, Rz. 27f. – juris - „Konferenz der Tiere“. Der BGH hätte also gem. § 559 ZPO in seinem Urteil gar nicht von seinen dortigen tatsächlichen Annahmen ausgehen dürfen! Außerdem fehlen Feststellungen dazu, ob für jeden Mittäter ohne weiteres der erforderliche Vorsatz ohne entsprechende Hinweise hierauf angenommen werden darf. Auch hierzu wären Feststellungen erforderlich, da zumindest nach einer empirischen Untersuchung aus den USA Vorsatz bei Nutzern in P2P-Tauschbörsen in den seltensten Fällen vorliegt bzw. gerichtlich festgestellt werden kann, siehe *Depoorter*, 66 UCLA L.Rev. 400, 426, 428 (2019).

in diesem Paradigma verharren, werden also weiterhin unbefriedigende *ad hoc*-Lösungen sein.

Zuletzt ist anzumerken, dass die erörterten Probleme betreffend eine Vorlage an den EuGH nahegelegen hätte. Eine solche ist nunmehr – leider mit verkürzter Erfassung dieser Probleme – durch ein belgisches Gericht (Ondernemingsrechtbank Antwerpen) erfolgt. Mangels hinreichender tatsächlicher Aufbereitung geht der Generalanwalt in seinen Schlussanträgen von falschen Annahmen über die Funktionsweise von BitTorrent aus, denn anders als dort behauptet wird, macht der einzelne Nutzer dort Dateien gerade nicht der Öffentlichkeit zugänglich.[124] Dem hätte der BGH – ggf. nach Ermittlung der relevanten Tatsachen durch die Vorinstanz nach Zurückverweisung – durch eine besser aufbereitete Vorlage entgegenwirken können. Überdies steht auf Grund der soeben genannten Vorlage die mittäterschaftliche Lösung des BGH in Zweifel, sollte der EuGH dem Generalanwalt dahingehend folgen, dass jeder einzelne Nutzer eine öffentliche Zugänglichmachung begeht.[125] Die Probleme, die sich aus der Mittäterschafts-Lösung des BGH bezüglich dem Schadensersatzanspruch ergeben[126], würden sich allerdings auch nach dieser Lösung stellen.

III. Zum Beweis der Urheberrechtsverletzung

Mit *Beweis der Urheberrechtsverletzung* ist der Beweis darüber gemeint, dass die von einem Ermittler beobachtete *filesharing*-Aktivität auch tatsächlich von dem Anschluss ausgegangen ist, dem die in diesem Zusammenhang ermittelte IP-Adresse nach Auskunft des zuständigen ISP zum Verletzungszeitpunkt zugewiesen war. Dieses Verständnis zu Grunde gelegt, hat sich der BGH zu den Anforderungen an den Beweis einer Urheberrechtsverletzung durch *filesharing* von einem bestimmten Internetanschluss aus nur wenig geäußert; was auch kaum verwundert, ist er doch keine Tatsacheninstanz und kann die richterliche Beweiswürdigung nach § 286 ZPO nur eingeschränkt

[124] Vgl. Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 38 bis 49 – ECLI:EU:C:2020:1063 - „M.I.C.M." mit den Ausführungen in Kapitel § 4 II. 4. b) bb).

[125] Siehe Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 65f. – ECLI:EU:C:2020:1063 - „M.I.C.M.".

[126] Siehe Kapitel § 4 II. 4. b) ff) und gg).

nachprüfen[127].

Beim Beweis der Urheberrechtsverletzung ist zu trennen zwischen der Ermittlung und ihrem Beweiswert sowie der Auskunft des ISPs und deren Beweiswert.

Hinsichtlich Letzterer ist in der Praxis – soweit bekannt – kaum ein Fall aufgetreten, in dem ein ISP bei der Zuordnung einer IP-Adresse zu einer bestimmten Anschlusskennung zu einem bestimmten Zeitpunkt ein Fehler unterlaufen ist.[128] Folglich ist dem BGH – vorbehaltlich gegenteiliger Erkenntnisse – darin zuzustimmen, dass der Beweiswert der Auskunft regelmäßig nicht anzuzweifeln ist.[129]

Hinsichtlich der Ermittlung einer IP-Adresse in einem *filesharing*-System ist wiederum zu differenzieren zwischen der richtigen Ermittlung an sich und der sich im Anschluss ergebenden Frage, welche Datenmengen an wie viele Empfänger von einer IP-Adresse aus verteilt wurden.

Da der BGH Letzteres[130] als unerheblich erachtet, insbesondere für die Berechnung des lizenzanalogen Schadens[131], ist es auch (auf Revisionsebene) noch nicht zum Streit über die Anforderungen an einen Beweis dieser Tatsache gekommen.

Bei der Ermittlung der IP-Adresse an sich ist zu beachten, dass die IP-Adresse trotz zuverlässiger Ermittlung zum beobachteten Zeitpunkt nicht demjenigen Anschluss zugeordnet gewesen sein muss, über den später Auskunft erteilt wird. Denn dass eine Ermittlung zuverlässig war, besagt nur, dass der Ermittler eine IP-Adresse so aufgezeichnet hat, wie sie sich ihm präsentiert hat.[132] Auch wenn die Ermittlung zuverlässig war, kann erstens im Falle des Auseinanderliegens des vom ISP beauskunfteten Zeitpunkts und des Verletzungszeitpunkts eine Neuvergabe der ermittelten IP-Adresse an einen anderen Anschluss und zweitens die Ermittlung einer gespooften IP-

127 *Kessal-Wulf* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 546 ZPO, Rz. 19ff.

128 Siehe ein Beispiel bei *Leicht*, VuR 2009, 346, 347.

129 BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 38ff. – GRUR 2016, 176 - „Tauschbörse I“; grundsätzlich ist es rechtlich möglich, den Beweiswert der Auskunft anzuzweifeln, da die Gestattungsanordnung über die Auskunft für das Verletzungsgericht keine Bindungswirkung entfaltet, siehe Kapitel § 2 III. 1. b).

130 Siehe hierzu Kapitel § 1 IV. 7. c) dd).

131 Siehe Kapitel § 5 VII.

132 Siehe Kapitel § 1 IV. 7. a).

Adresse nicht völlig ausgeschlossen werden.[133] Drittens kann eine Ermittlung auch nur dann geeignet sein, eine Verletzungshandlung dem Grunde nach zu beweisen, wenn die Ermittlung aktiv war.[134] Diese drei Probleme können auch nicht durch eine Durchsuchung des PCs (oder eines anderen Endgeräts) des verdächtigten Endnutzers beseitigt werden, da das Vorhandensein oder Nichtvorhandensein der fraglichen Datei keinen Beweiswert dafür hat, ob dieser Endnutzer auch die streitgegenständliche *filesharing*-Aktivität durchgeführt hat.[135]

Ob dem BGH die Unterscheidung zwischen der Zuverlässigkeit der Ermittlung einerseits und den sich hieran anschließenden drei Problemen andererseits bewusst war, kann nicht abschließend beurteilt werden. Folglich darf die Aussage des BGH in „Tauschbörse I", dass die Annahme der Beweiskraft der ermittelten IP-Adresse (auf Grund der Annahme einer zuverlässigen Ermittlung) nicht rechtsfehlerhaft sei[136], nicht überbewertet werden. Soweit man die Aussage des BGH auf die Zuverlässigkeit der Ermittlung beschränkt, ist sie grundsätzlich richtig, jedoch ist nach hiesiger Auffassung dabei ein Entwicklungsgebot zu beachten, d.h. sobald eine neue Ermittlungssoftware oder eine neue Version einer bekannten Ermittlungssoftware verwendet wird, muss deren Zuverlässigkeit neu festgestellt werden.[137]

Konfrontiert mit der soeben getroffenen Differenzierung, ist jedenfalls auch eine Entscheidung denkbar, in der der BGH den Beweiswert der dort streitgegenständlichen Ermittlung anzweifelt.

IV. Zum Auskunftsanspruch gegen ISPs

1. Zur Nichterforderlichkeit eines gewerblichen Ausmaßes

a) Uneindeutigkeit des Wortlauts und seiner systematischen Beziehungen

Nach Erwägungsgrund 14 EnforcementRL ist es den Mitgliedstaaten überlassen, ob sie für das Auskunftsrecht ein gewerbliches Ausmaß der rechtsver-

[133] Siehe Kapitel § 1 IV. 7. c) bb) und cc).
[134] Siehe Kapitel § 1 IV. 7. a).
[135] Siehe Kapitel § 1 IV. 7. c) aa).
[136] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 33ff. – GRUR 2016, 176 - „Tauschbörse I".
[137] Siehe Kapitel § 1 IV. 7. a).

letzenden Tätigkeit als notwendig erachten oder nicht.

Aus dem Wortlaut des § 101 UrhG geht nur bei Abs.1 Satz 1 eindeutig hervor, dass der Rechtsverletzer in gewerblichem Ausmaß gehandelt haben muss. Der für das *filesharing* relevante § 101 Abs.2 Satz 1 Nr.3 UrhG lässt sich jedoch in zwei Richtungen auslegen: Einerseits könnte man daraus, dass das Handeln im gewerblichen Ausmaß ausdrücklich nur für den Auskunftsverpflichteten erwähnt wird, im Umkehrschluss folgern, dass die „*offensichtliche Rechtsverletzung*“ nach § 101 Abs.2 Satz 1 1. Alt UrhG gerade nicht ein gewerbliches Ausmaß erreichen muss bzw. der Verletzer nach § 101 Abs.2 Satz 1 2. Alt UrhG nicht in einem gewerblichen Ausmaß gehandelt haben muss. Andererseits könnten die Begriffe „Rechtsverletzung“ und „Verletzer“ in § 101 Abs.2 Satz 1 UrhG in systematischer Beziehung zu § 101 Abs.1 Satz 1 UrhG unter dessen Voraussetzungen, also einem Handeln in gewerblichem Ausmaß, zu lesen sein.

§ 101 Abs.1 UrhG fixiert keine eindeutige Bedeutung der „Rechtsverletzung“. Aus § 101 Abs.1 Satz 2 UrhG, demgemäß sich das gewerbliche Ausmaß aus der Anzahl oder Schwere von Rechtsverletzungen ergeben kann, lässt sich ableiten, dass der Begriff der „Rechtsverletzung“ nicht schon in sich das Kriterium des gewerblichen Ausmaßes enthalten muss.[138]

Methodisch wären also beide der genannten Schlüsse zulässig.[139] Weitere Argumente aus dem Wortlaut und der Systematik, die den einen oder den anderen stützen, existieren nicht. Aus dem Umstand, dass der Anspruch aus § 101 Abs.1 Satz 2 UrhG „*unbeschadet von Absatz 1*“ gewährt wird, kann lediglich gefolgert werden, dass die Auskunftspflichtigen nach Abs.2 auch im Falle ihrer Haftung als Störer nach Abs.1 in Anspruch genommen werden können.[140] Dass in den Auskunftsansprüchen andere Rechte des geistigen Eigentums betreffend (beispielsweise § 140b PatG) ein Erfordernis des Han-

[138] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 12 – GRUR 2012, 1026 - „Alles kann besser werden“.

[139] aA und für ein gewerbliches Ausmaß aus systematischen Erwägungen *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 220f.; *Stein*, Der Auskunftsanspruch gegen Access-Provider nach § 101 UrhG, S. 88ff.; *Sandor*, Datenspeicherung und urheberrechtliche Durchsetzungsansprüche, S. 54ff.; *Wick*, Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter, S. 46f.; *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 187f.

[140] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 13 – GRUR 2012, 1026 - „Alles kann besser werden“.

dels im gewerblichen Ausmaß nicht enthalten ist, lässt keine Rückschlüsse auf das Urheberrecht zu, da in den Gesetzen diese Schutzrechte betreffend ein Handeln mit nicht-kommerziellem Hintergrund ohnehin nur mit Einschränkungen eine Rechtsverletzung darstellt.[141]

Folglich kann eine Entscheidung in die eine oder andere Richtung nur auf Grundlage anderer Argumente als Wortlaut und Systematik getroffen werden.

b) Der ökonomischer Hintergrund als juristisches Argument?

Der BGH erkennt in seiner Entscheidung „Alles kann besser werden“[142] die „Pattsituation“ im Rahmen der Auslegung nach dem Wortlaut und der Systematik an. Seine Aussage, dass der Wortlaut des § 101 Abs.2 Satz 1 UrhG keinen hinreichenden Anhaltspunkt dafür biete, dass die Rechtsverletzung, über die Auskunft erteilt werden soll, ein gewerbliches Ausmaß erreichen muss[143], ist richtig; jedoch ist diese dahingehend zu ergänzen, dass – wie soeben dargestellt – auch der umgekehrte Fall keinen ausdrücklichen Niederschlag im Gesetzeswortlaut gefunden hat.

Um die Pattsituation aufzulösen, bedient sich der BGH zunächst eines Rechtsfolgenarguments, welches er jedoch unzutreffenderweise als teleologisches Argument deklariert: Bei § 101 Abs.2 Satz 1 Nr.3 UrhG sei (auch[144]) deswegen auf ein gewerbliches Ausmaß zu verzichten, weil *filesharing* die wirtschaftlichen Interessen der Rechteinhaber beeinträchtige[145], mithin also wirtschaftlich schädlich sei. Abgesehen davon, dass die wirtschaftliche Schädlichkeit des *filesharing* höchst umstritten ist[146], ist die Argumentationsfigur einer solchen Rechtsfolgenabwägung oder rechtsfolgenorientierten Auslegung

[141] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 15f. – GRUR 2012, 1026 - „Alles kann besser werden“; siehe dazu auch Kapitel § 3 XI. 2. e).

[142] Eine Übersicht über die Entscheidungskommentierungen findet sich bei *Heckmann/Paschke* in: Heckmann, jurisPK-Internetrecht, 6. Aufl. 2019, Kap. 3.2, Rz. 211.

[143] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 11, 27, 29 – GRUR 2012, 1026 - „Alles kann besser werden“; so auch *Jüngel/ Geißler*, MMR 2008, 787, 787 und *Musiol*, GRUR-RR 2009, 1, 3.

[144] Siehe zu den weiteren Argumenten sogleich Kapitel § 4 IV. 1. c).

[145] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 22f. – GRUR 2012, 1026 - „Alles kann besser werden“.

[146] Siehe hierzu Kapitel § 3 IX. 1.

aus mehreren Gründen *generell* abzulehnen:

- Sie missachtet den Vorbehalt des Gesetzes. Ein Richter ist dazu berufen, das Gesetz als begrifflich-systematisches System zu erfassen; wer eine bestimmte Rechtsfolge auf Basis ihrer nachfolgenden praktischen Konsequenzen rechtfertigt, fügt dem Tatbestand der Norm ein nicht vorhandenes Merkmal hinzu, betreibt also Rechtsschöpfung statt Auslegung.[147] Dieser Einwand wird gestützt durch den Umstand, dass es Normen gibt, die ökonomische Überlegungen miteinbeziehen, wie beispielsweise die *business judgement rule* in § 93 Abs.1 Satz 2 AktG. Normen, die ökonomische Erwägungen nicht explizit in ihrem Tatbestand enthalten, dürfen solche dann also *e contrario* nicht implizit über die Auslegung hinzugefügt werden.

- Weiterhin umgeht sie das Erfordernis des Sachverständigenbeweises. Über die ökonomische Rechtsfolgenargumentation werden durch den Richter Tatsachen als offenkundig oder gerichtsbekannt im Sinne des § 291 ZPO behandelt, obwohl sie nach den Regeln der §§ 402ff. ZPO ermittelt werden müssten.[148] Insbesondere in Spezialfragen wie den ökonomischen Folgen des *filesharing*, dürfte auch einem ökonomisch vorgebildeten Richter die hinreichende Sachkenntnis fehlen, die eine Annahme gerichtsbekannter Tatsachen erlauben würde.

- Ein weiteres Problem rechtsfolgenorientierter Argumentation ist das sogenannte Folgenparadox[149]: Angenommen dem Rechtsfolgenargument *filesharing ist gesamtökonomisch betrachtet schädlich und beim Vorgehen gegen die Nutzer geht es zurück, folglich muss Auskunft auch bei jeder einzelnen Urheberrechtsverletzung mittels filesharing in nichtgewerblichem Umfang erteilt werden* läge eine wahre Prämisse zu Grunde (*filesharing* ist gesamtökonomisch betrachtet schädlich und beim Vorgehen gegen die Nutzer geht es zurück), dann wäre das Argument nur solange gültig, wie *filesharing* in so ausreichendem Maße betrieben wird, dass es in ökonomischer Gesamtbetrachtung einen Schaden auslöst. Sobald dies nicht mehr der Fall ist, dürfte es als Argument

147 Vgl. *Möllers*, Juristische Methodenlehre, S. 166, 184f.

148 Vgl. zu diesem Problem allgemein *Cserne*, Consequence-Based Arguments in Legal Reasoning: A Jurisprudential Preface to *Law and Economics*, S. 31, 45f. sowie *Drakeman*, Jurisprudence, Nr. 2, Bd. 9, 2018, S. 300, 309ff.

149 Vgl. *Mathis*, Consequentialism in Law, S. 3, 21ff.

nicht mehr verwendet werden, die Auskunft mithin nicht mehr erteilt werden, sofern man es als für das Gesamtergebnis (Auskunft wird auch bei nicht gewerblichen Verletzungshandlungen erteilt) als notwendiges Argument ansieht. Da das Argument aber das Vorgehen gegen *filesharing*-Nutzer im breiten Umfang überhaupt erst ermöglicht hat, würde es zugleich zu seiner späteren Ungültigkeit führen (Rückgang des *filesharing* wegen Auskunft und daran anknüpfende rechtliche Schritte gegen Nutzer). Diese Konsequenz müsste aber bereits vor erstmaliger Verwendung des Rechtsfolgenarguments einbezogen werden, da es ansonsten willkürlich auf einen bestimmten Zeitraum begrenzt wäre (im Beispiel also willkürlich auf den Zeitraum, in dem *filesharing* noch ökonomisch schädlich ist). Ein Rechtsfolgenargument hat also die Tendenz, sich logisch selbst aufzuheben.[150]

- Zuletzt entscheidet ein Richter stets über einen Einzelfall, folglich müsste er, selbst wenn er die Konsequenzen der Entscheidung dem Grunde nach einbeziehen dürfte, beim *filesharing* zum Beispiel die ökonomische Schädlichkeit des von ihm zu entscheidenden Einzelfalls bewerten, nicht des *filesharing* insgesamt.[151] Einer ökonomischen Bewertung ist aber nur das Phänomen des *filesharing* insgesamt zugänglich.[152]

Die Anwendung ökonomischer Rechtsfolgenargumente spezifisch im Kontext des Auskunftsanspruches ist zudem aus einem weiteren Grund abzulehnen: Argumente dieser Art fußen auf der Prämisse, dass Rechtsunterworfene bei einer bestimmten Rechtsfolge ihr Verhalten anpassen.[153] Im Rahmen des Auskunftsanspruches ist also die Logik, dass bei (mehr) Auskunftserteilung mehr *filesharer* verurteilt werden, und dadurch andere *filesharing*-Nutzer davon abgeschreckt werden, Urheberrechtsverletzungen zu begehen und folglich der ökonomische Schaden, der durch *filesharing* entsteht, insgesamt verringert wird. Abgesehen davon, dass die abschreckende Wirkung des Vorgehens gegen Endnutzer empirisch nicht gesichert ist[154], trifft die Rechtsfolge hier

150 *Mathis*, Consequentialism in Law, S. 3, 21ff.

151 Vgl. *Albach*, Zur Verhältnismässigkeit der Strafbarkeit privater Urheberrechtsverletzungen im Internet, S. 247.

152 Siehe hierzu Kapitel § 3 IX. 1.

153 *Franck*, Vom Wert ökonomischer Argumente bei Gesetzgebung und Rechtsfindung für den Binnenmarkt, S. 70, 85ff.

154 Siehe Kapitel § 3 IX. 2.

schon nicht zwingend die jeweiligen Täter, sondern zunächst die Inhaber der Anschlüsse, über die eine Verletzung begangen wurde. Zwar wurden sehr viele Anschlussinhaber als Täter (erfolgreich) in Anspruch genommen, jedoch ist offen, wie viele davon auch tatsächlich Täter waren. Ob ein Mehr an Auskunftserteilung daher tatsächlich auch ein Weniger an Urheberrechtsverletzungen mittels *filesharing* zur Folge haben kann, lässt sich nicht aufklären, selbst wenn die Wirksamkeit des Vorgehens gegen Endnutzer empirisch feststünde. Ein entsprechendes Rechtsfolgenargument ist mithin ungültig.

Nichtsdestotrotz kommen ökonomische Argumente in *filesharing*-Kontexten nicht selten vor.[155] Erfreulich ist, dass explizite ökonomische Begründungen in neuerer Zeit in Urteilen nicht mehr zu finden sind, das Beispiel des BGH also (zumindest vorerst) keine Schule gemacht hat. Als namhafte Ausnahme sind die Schlussanträge in der Rs. 597/19 zu nennen[156] Der Generalanwalt behauptet dort pauschal Verluste, die in die Milliarden gehen würden. Als einzige Quelle hierfür führt er in Fußnote 2 eine im Auftrag der US-Handelskammer erstellte Studie von *Blackburn et al.*[157] an. Angesichts der unter Kapitel § 3 IX. 1. angeführten Metastudien, die Gegenteiliges postulieren, ist offenkundig, dass dieser Behauptung des Generalanwalts kein genügendes Quellenstudium vorausgegangen ist, unabhängig von der Frage, ob eine solche Aussage von vornherein nicht ohne einem nach Art. 70 der Verfahrensordnung des EuGH eingeholten Sachverständigengutachten zulässig wäre. Überdies verwundert, warum der Generalanwalt nicht zumindest die vergleichbare, im Auftrag der EU-Kommission angefertigte Studie anführt, die die Probleme der von *Blackburn et al.* verwendeten Methodik erörtert und

[155] In deutschen Gerichtsentscheidungen zum Beispiel in BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 28 – GRUR 2013, 511 - „Morpheus“; AG Köln, Urteil vom 10. März 2014, Az. 125 C 495/13, Rz. 21 – juris; LG Köln, Urteil vom 6. Juni 2007, Az. 28 O 384/06, Rz. 26 – juris; OLG Karlsruhe, Beschluss vom 1. September 2009, Az. 6 W 47/09, Rz. 23 – juris; das Rechtsfolgenargument mit guter Begründung ablehnend AG Offenburg, Beschluss vom 20. Juli 2007, Az. 4 Gs 442/07, Rz. 41, 43 – juris. Als Beispiel aus der ausländischen Rechtsprechung siehe High Court of Ireland, EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd, [2010] IEHC 377, Rz. 8, 19 – bailii.org.

[156] Siehe Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 1 – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

[157] *Blackburn/Eisenach/Harrsion*, Impacts of Digital Video Piracy on the U.S. Economy.

entsprechend zurückhaltend mir ihren Schlussfolgerungen ist.[158] Zwar baut der Generalanwalt auf diesem ökonomischen Vorverständnis kein konkretes Argument auf, rechtsrhetorisch ist ein solches *poisoning the well* dennoch problematisch.

Im Ergebnis jedenfalls sind (ökonomische) Rechtsfolgenargumente im Rahmen der juristischen Gesetzesauslegung schon im Allgemeinen abzulehnen, also auch im Besonderen deren Verwendung durch den BGH im Rahmen der Auslegung des § 101 Abs.2 UrhG.

Es lässt sich ohnehin nicht vermeiden, dass ökonomische Vorstellungen über das *filesharing* als Vorverständnisse[159] in die reguläre Gesetzesauslegung einfließen[160] So notierte auch ein mit zahlreichen *filesharing*-Fällen befasster Praktiker, dass sich bei vielen Urteilen (und dort insbesondere bei Bemessung des Schadensersatzes) der Eindruck aufdränge, die Gerichte hätten sich bei ihren Entscheidungen primär von ihren Vorstellungen über die vermeintlichen ökonomischen Auswirkungen des *filesharing* leiten lassen.[161] Wenn sich also schon eine (möglicherweise bestehende) implizite Beeinflussung der Entscheidungsfindung durch ökonomischer Vorstellungen nicht vermeiden lässt, sollten – aus den genannten Gründen – aber zumindest explizite ökonomische Rechtsfolgenargumente unzulässig sein.[162]

Zu beachten ist abschließend, dass das an anderer Stelle dieser Arbeit herangezogene *argumentum ad absurdum*[163] als spezifische Form eines Rechtsfolgenarguments anders als das soeben dargestellte Rechtsfolgenargument zulässig ist. Denn während beim Rechtsfolgenargument in seiner soeben dargestellten Form mittels empirischer Annahmen die Richtigkeit einer Auslegung begründet oder eine Auslegung gleich ganz ersetzt wird, wird mit dem *argumentum ad absurdum* die Inakzeptabilität eines Auslegungsergebnisses auf Grund der Rechtsfolgen, die es *logisch zwingend* zeitigt, aufgezeigt, ohne

158 Siehe *van der Ende* et al., Estimating displacement rates of copyrighted content in the EU, S. 148ff., 171ff..

159 *Esser*, Vorverständnis und Methodenwahl in der Rechtsfindung, S. 133ff.

160 Zum empirischen Nachweis des Einflusses außerrechtlicher Faktoren auf die Entscheidungsfindung siehe *Liu/Li*, Journal of Empirical Legal Studies, Nr. 3, Bd. 16, 2019, 630ff., mit weiteren Nachweisen.

161 *Solmecke*, MMR 2014, 483, 485.

162 Dieses Fazit gilt nicht für den Prozess der Gesetzgebung. Ökonomische Erwägungen gehören selbstverständlich zur Rechtspolitik, nicht aber zur Rechtsanwendung.

163 Siehe Kapitel § 4 II. 4. b) gg).

eben dass es hierzu empirischer Annahmen bedarf.[164]

c) Entscheidung nach dem „objektiven“ Willen des Gesetzes?

Der BGH entscheidet sich nicht nur auf Grund des Rechtsfolgenarguments dafür, bei der Verletzungshandlung im Rahmen des § 101 Abs.2 Satz 1 UrhG ein gewerbliches Ausmaß für nicht erforderlich zu halten. Begründet sei dies überdies durch den von ihm aufgefundenen *objektivierten* Willen des Gesetzgebers.[165] Folglich ist es für den BGH unproblematisch, dass in der Gesetzesbegründung[166] ein gewerbliches Ausmaß der Verletzung im Rahmen des § 101 Abs.2 Satz 1 UrhG gefordert wird. Die Gesetzesbegründung sei nicht zu berücksichtigen, da der (von ihm aufgefundene) objektive Sinn und Zweck des Gesetzes etwas anderes gebiete.[167]

Zwar ist die Begründungsfigur des „objektiven Willens“ an sich bereits höchst fragwürdig[168], allerdings ist auch die vom BGH vorgenommene Ermittlung des Sinn und Zwecks des Gesetzes an sich unzutreffend.

Zunächst ist seine Feststellung richtig, dass § 101 Abs.2 UrhG ein Hilfsanspruch ist, der dazu dient, Unterlassungs- oder Schadensersatzansprüche zu verfolgen.[169] Diese Aussage hat jedoch für die Auslegung keinen weiteren Erkenntniswert, da die zu entscheidende Frage ja gerade ist, welche Qualität die diesen Ansprüchen zu Grunde liegende Rechtsverletzung haben muss. Mithin gilt zu entscheiden, ob *jede* Rechtsverletzung verfolgbar sein muss oder nur manche, also nur Rechtsverletzungen gewerblichen Ausmaßes. Der BGH wiederholt folglich nur die zu klärende Frage, ohne hiermit – anders als intendiert – ein echtes Argument zu machen.

Das nächste Argument des BGH ist – insofern vom ihm unzutreffend eingeordnet – kein teleologisches, sondern ein logisches: Ein gewerbliches Ausmaß dürfe nicht verlangt werden, da die Rechteinhaber sonst faktisch schutzlos

---

164 Siehe auch Kapitel § 4 II. 4. b) gg).

165 BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 30 – GRUR 2012, 1026 - „Alles kann besser werden“.

166 Die insofern seiner Auffassung nach als „Wille des Gesetzgebers“ zu verstehen ist.

167 BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 22, 30 – GRUR 2012, 1026 - „Alles kann besser werden“.

168 Siehe hierzu sogleich Kapitel § 4 IV. 1. d).

169 BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 20 – GRUR 2012, 1026 - „Alles kann besser werden“.

gestellt wären.[170] Er meint also, § 101 Abs.2 Satz 1 Nr.3 UrhG würde Urheberrechtsverletzungen mittels *filesharing* faktisch nicht erfassen, würde man ein gewerbliches Ausmaß der Rechtsverletzung verlangen. Die Norm hätte dann also keinen Anwendungsbereich. Zunächst hat eine solche logische Argumentationsfigur (*Verbot der Normderogation*) generell einiges für sich[171], wenn man – nach Auffassung des Verfassers richtigerweise – davon ausgeht, dass unter Geltung des Demokratieprinzips und des Prinzips der Gewaltenteilung jedes Gesetz einen Anwendungsbereich haben muss, da die inhaltliche Entkernung einer Rechtsvorschrift einer gesetzgeberischen Tätigkeit gleichkommt, welche die Rechtsprechung nicht wahrnehmen darf. Jedoch verfängt diese Argumentationsfigur im konkreten Fall nicht, da § 101 Abs.2 Satz 1 Nr.3 UrhG seinem Wortlaut nach nicht nur auf *filesharing* zugeschnitten ist[172], sondern alle möglichen Urheberrechtsverletzungen über alle möglichen Dienstleister erfasst.

Sodann führt der BGH den Willen des Gesetzgebers an (BT-Drs. 16/5048, S. 39f.), demgemäß – was zutreffend ist – bei *filesharing* ein besonderes Interesse an der Auskunft bestehe.[173] Dies ist wiederum kein teleologisches Argument im eigentlichen Sinne, sondern ein historisches, da der BGH sich in diesem Punkt auf die Gesetzesmaterialien beruft. Inhaltlich widerspricht er sich zudem selbst, da er an anderer Stelle in der Entscheidung den Willen des Gesetzgebers, der ausdrücklich besagt, dass ein gewerbliches Ausmaß der Rechtsverletzung erforderlich ist, für unbeachtlich hält (hierzu sogleich). Die vom BGH zitierte Stelle aus der Gesetzesbegründung wäre also eigentlich im Zusammenhang mit dem übrigen Inhalt der Gesetzesbegründung zu lesen (hierzu wiederum sogleich).

Tatsächlich beruft sich der BGH mithin auf einen Zweck des Gesetzes, den er gar nicht herzuleiten vermag.

Fehlerhaft ist seine Auslegung also selbst dann, wenn man das Primat der objektiven Auslegung (fälschlicherweise) bejaht. Denn ein Sinn und Zweck,

[170] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 23 – GRUR 2012, 1026 - „Alles kann besser werden".

[171] Siehe *Möllers*, Juristische Methodenlehre, S. 164, 173.

[172] Wenn auch nach der Vorstellung des Gesetzesgebers (hierzu sogleich) die Norm gerade für diesen Fall geschaffen wurde.

[173] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 23 – GRUR 2012, 1026 - „Alles kann besser werden".

der eine Entscheidung in die eine oder andere Richtung vorgibt, lässt sich hier nicht ermitteln.

d) Entscheidung nach dem (fingierten) Willen des Gesetzgebers?

Unabhängig davon aber, dass der BGH einen Zweck des Gesetzes, demgemäß es auf ein gewerbliches Ausmaß der Rechtsverletzung nicht ankommen solle, nicht überzeugend herleitet, dürfte ein solcher, wie auch immer hergeleiteter Zweck, im vorliegenden Fall gar nicht für die Auslegung entscheidend sein.

Denn einer solchen rechtsmethodischen Entscheidung steht der vorrangige „subjektive Wille des Gesetzgebers“ entgegen.

aa) „Objektive“ oder „subjektive“ Auslegung?

In der Rechtstheorie tobt ein scheinbar immerwährender Streit darüber, ob Ziel der Gesetzesauslegung die Ermittlung des historischen Willens des Gesetzgebers ist (subjektive Theorie) oder eines vom historischen Gesetzgeber unabhängigen, verobjektivierten Sinne des Gesetzes (objektive Theorie).[174] Beide Theorien sind mit ontologischen und epistemologischen Problemen verknüpft. Existieren ein Wille des Gesetzgebers oder ein verobjektivierter Sinn überhaupt und wenn ja, sind sie dann einer Erkenntnis zugänglich?

Unabhängig davon, ob und wie diese Probleme aufgelöst werden können, wird der Streit hierüber häufig im luftleeren Raum geführt; zwar existiert in Deutschland – anders als beispielsweise im Völkerrecht oder anderen Ländern[175] – kein Methodengesetz. Dennoch ist die Entscheidung für oder gegen eine Methode der Auslegung im gewaltenteilenden Staat unmittelbar aus der Verfassung abzuleiten, da die Methode schließlich die Trennlinie zwischen gesetzgebender und rechtsprechender Gewalt markiert. Methodenfragen sind mithin Verfassungsfragen.[176] Folglich interessiert für die methodische Lösung eines konkreten Rechtsproblems zuvorderst, welche Lösungshinweise die Rechtsprechung des BVerfG hierzu gibt.

---

[174] Die Literatur hierzu ist praktisch unüberschaubar. Siehe mit einer kurzen Zusammenfassung aus jüngerer Zeit *Würdinger*, JuS 2016, 1, 2f.

[175] Art. 31ff. Wiener Vertragsrechtskonvention; zu nationalen Gesetzen siehe beispielsweise für die Schweiz Art. 1 Schweizerisches Zivilgesetzbuch oder für Neuseeland den *Interpretation Act 1999*.

[176] *Rüthers*, NJW 2011, 1856, 1857.

Den Grundstein seiner Methodenrechtsprechung legte das BVerfG 1952:

> *„Maßgebend für die Auslegung einer Gesetzesbestimmung ist der in dieser zum Ausdruck kommende objektivierte Wille des Gesetzgebers, so wie er sich aus dem Wortlaut der Gesetzesbestimmung und dem Sinnzusammenhang ergibt, in den diese hineingestellt ist. Nicht entscheidend ist dagegen die subjektive Vorstellung der am Gesetzgebungsverfahren beteiligten Organe oder einzelner ihrer Mitglieder über die Bedeutung der Bestimmung. Der Entstehungsgeschichte einer Vorschrift kommt für deren Auslegung nur insofern Bedeutung zu, als sie die Richtigkeit einer nach den angegebenen Grundsätzen erhaltenen Auslegung bestätigt oder Zweifel behebt, die auf dem angegebenen Weg allein nicht ausgeräumt werden können.“* [177]

Das BVerfG bekennt sich hier also zur objektiven Theorie. In der Verfassungsgerichtsrechtsprechung wird diese Entscheidung immer dann zitiert, sobald die Methodenfrage streitgegenständlich wird, oder es lassen sich jedenfalls alle Belegstellen einer Entscheidung in der Kette auf Erstere zurückführen. Sie wurde dadurch verselbstständigt und universalisiert, ist mithin eine echte Leitentscheidung geworden.[178]

Als wichtige Ergänzung zu dieser Entscheidung ist ein Urteil aus dem Jahr 1960 zu lesen, das die Methodik der Auslegung instruktiv erläutert: das Bekenntnis zur objektiven Theorie wird unter Berufung auf die „Rechtsphilosophie“ von *Radbruch* bekräftigt.[179] Sodann werden die vier nach *Savigny* überlieferten *canones* aufgezählt, die der Ermittlung dieses Willens dienen, also die Auslegung nach dem Wortlaut, die Auslegung nach dem systematischen Zusammenhang, die historischen Auslegung (Gesetzesmaterialien und Entstehungsgeschichte[180]) sowie die Auslegung nach dem Zweck (teleologische Auslegung).[181] Das mit der historischen Auslegung erzielte Ergebnis dürfe jedoch keinesfalls mit dem objektiven Inhalt des Gesetzes gleichge-

[177] BVerfG, Urteil vom 21. Mai 1952, Az. 2 BvH 2/52, Leitsatz Nr.2 – juris.

[178] Zu den Anforderungen an eine Leitentscheidung siehe *Yang*, Die Leitentscheidung, S. 69ff.

[179] BVerfG, Urteil vom 17. Mai 1960, Az. 2 BvL 11/59, 2 BvL 11/60, Rz. 16 – juris.

[180] Allerdings ist unklar, was die Entstehungsgeschichte genau umfasst und wie diese zu ermitteln ist.

[181] BVerfG, Urteil vom 17. Mai 1960, Az. 2 BvL 11/59, 2 BvL 11/60, Rz. 17 – juris.

setzt werden.[182] Durch weitere Entscheidungen ergänzte das BVerfG seine Methodenrechtsprechung dahingehend, dass eine Rangfolge der Methoden nicht existiere[183] sowie, dass die Grenze der Auslegung der Wortlaut darstelle[184]; über den Wortlaut hinaus sei die Rechtsprechung jedoch grundsätzlich zur Lückenfüllung und Rechtsfortbildung berechtigt.[185]

Der BGH hatte 1954 Gelegenheit, sich für die subjektive oder objektive Theorie zu entscheiden und folgte dem BVerfG.[186]

Dem Rechtsanwender mag das von den beiden Gerichten somit geschnürte Methodenkorsett[187] in rechtstheoretischer Hinsicht widerstreben, faktisch und rechtlich ist er jedoch daran gebunden.[188] Tatsächlich entfaltet die Rechtsprechung des BVerfG also die Wirkung eines aus der Verfassung abgeleiteten Methodengesetzes.

Im Ergebnis kann die Entscheidung „Alles kann besser“ unter Anwendung *dieses* Methodenparadigmas *verfassungsrechtlich* nicht beanstandet werden: der BGH erkennt, dass zwei der Auslegungsmethoden – Wortlaut und Systematik – kein eindeutiges Ergebnis ergeben, der Wortlaut aber den Einschluss oder Ausschluss des Erfordernisses eines gewerblichen Ausmaßes zulässt. Historische und teleologische Auslegung liefern zwei sich widersprechende Ergebnisse. Mangels einer Methodenrangfolge und unter Geltung der objek-

[182] BVerfG, Urteil vom 17. Mai 1960, Az. 2 BvL 11/59, 2 BvL 11/60, Rz. 18 – juris. Das BVerfG beruft sich für diese Aussage auf das Reichsgericht, RG, Urteil vom 25. März 1891, Az. I 11-91 – RGZ 27, 409, 411. Das RG selbst wiederum stellt diesen Grundsatz nur apodiktisch auf. Dass die Heranziehung von vorkonstitutionellen Präjudizien verfassungstheoretisch höchst problematisch erscheint, soll hier nur nebenbei bemerkt sein.

[183] Siehe aus neuerer Zeit und mit weiteren Nachweisen nur BVerfG, Urteil vom 17. Januar 2017, Az. 2 BvB 1/13, Rz. 555 – bverfg.de; BVerfG, Beschluss vom 26. August 2014, Az. 2 BvR 2172/13, Rz. 16 – bverfg.de.

[184] BVerfG, Beschluss vom 3. April 1990, Az. 1 BvR 1186/89, Rz. 22 – juris.

[185] BVerfG, Beschluss vom 3. April 1990, Az. 1 BvR 1186/89, Rz. 20ff. – juris; BVerfG, Urteil vom 18. Dezember 1953, Az. 1 BvL 106/53, Rz. 41 – juris; zu der (voraussetzungsvollen) Möglichkeit der Rechtsfortbildung *contra legem* BVerfG, Beschluss vom 14. Februar 1973, Az. 1 BvR 112/65, Rz. 45 – juris.

[186] BGH, Beschluss vom 20. Mai 1954, Az. GSZ 6/53, Rz. 26 – juris.

[187] Auf das sich der BGH in „Alles kann besser werden“ ausdrücklich beruft, siehe BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 30 – GRUR 2012, 1026 - „Alles kann besser werden“.

[188] Vgl. § 31 Abs.1 BVerfGG. Vgl. *Rüthers*, Die heimliche Revolution vom Rechtsstaat zum Richterstaat, S. 32.

tiven Theorie kann sich der BGH also für das Ergebnis der teleologischen Auslegung entscheiden (wenn auch seine Ermittlung des Telos methodisch fehlerhaft ist[189]).

bb) Paradigmenwechsel 2011?

Aber gilt das Bekenntnis des BVerfG zur objektiven Theorie überhaupt noch? Im Methodenstreit hatten Kritiker dieser Theorie immer wieder darauf hingewiesen, dass durch diese die Möglichkeit bestehe, im Wege der historischen Auslegung erzielte Ergebnisse hinter teleologischen Erwägungen zurücktreten zu lassen, richterliche Rechtsfortbildung also als Auslegung etikettiert werden könne.[190] Mit dem Schlagwort „Einlegung statt Auslegung“[191] wird darauf hingewiesen, dass der *in praxi* als teleologische Auslegung bezeichnete Vorgang in Wahrheit eine Abwägung darstellt: die Abwägung desjenigen Wertes, dem die Anwendung einer Norm auf einen bestimmten Fall dient, mit demjenigen Wert, dem die Nichtanwendung einer Norm auf diesen Fall dient.[192] Eine Abwägung ist aber stets ein subjektiv-gestaltender, kein objektiv-ermittelnder Akt. Als eigenständige Methode kann die teleologische Auslegung gar nicht existieren, da der Zweck einer Norm stets erst selbst durch Auslegung ermittelt werden muss. Wer die teleologische „Auslegung“ also als *Auslegungs*mittel ansieht, begeht einen Zirkelschluss.[193] Dieser Makel haftete der Methodenrechtsprechung des BVerfG mithin seit der Leitentscheidung aus 1952 an.

Im Minderheitsvotum in einer Entscheidung des BVerfG aus dem Jahr 2009 erblickte *Rüthers* jedoch erste Wetterzeichen einer Trendwende hin zur Begrenzung der methodischen Freiheit der rechtsprechenden Gewalt, die er auf die zum Senat neu hinzu gekommenen Richter zurückführte.[194] Das BVerfG hatte dort über die Verfassungsmäßigkeit der Auslegung des § 274 Satz 1 StPO durch den BGH zu befinden. Letzterer legte in dieser Norm das Wort „*Protokoll*“ derart aus, dass auch ein berichtigtes Protokoll (die StPO sieht eine Protokollberichtigung nicht ausdrücklich vor) zum Nachweis der Beachtung der für die Hauptverhandlung vorgeschriebenen Förmlichkeiten dienen

189 Siehe oben Kapitel § 4 IV. 1. c).
190 Siehe als aktuelles Beispiel nur *Rüthers*, ZfPW 2016, 383, 383.
191 Statt Vieler siehe beispielsweise nur *Rüthers*, Rechtstheorie 2009, 253, 262.
192 *Herzberg*, NJW 1990, 2525, 2527.
193 *Walz*, ZJS 2010, 482, 488.
194 *Rüthers*, NJW 2009, 1461, 1462; *Rüthers*, NJW 2011, 1856, 1858.

kann, mithin ein Revisionsführer Versäumnisse des Verfahrens nicht rügen kann, die zwar das unberichtigte Protokoll aufweist, das (auf Grundlage des Gedächtnisses des Urkundsbeamten und des Vorsitzenden) berichtigte Protokoll aber nicht mehr. Das BVerfG befand, dass diese Auslegung nicht die Grenzen der richterlichen Rechtsfortbildung überschreite; ein strenger Formalismus sei als anachronistisches Überbleibsel aus dem 19. Jahrhundert nicht angezeigt. Die Rechtsprechung müsse vielmehr angemessene Ergebnisse für den jeweiligen Einzelfall finden.[195] Die abweichenden Minderheitsvoten allerdings kritisierten, dass es die Senatsmehrheit dem BGH durchgehen lasse, dass er aus Praktikabilitätserwägungen seine eigene Regelungskonzeption an die Stelle der des Gesetzgebers setze.[196] Aus den Motiven[197] zur StPO sei eindeutig zu entnehmen, dass es der damalige Gesetzgeber ausdrücklich abgelehnt habe, eine Rekonstruktion der Hauptverhandlung des Strafprozesses mit zusätzlichen Beweismitteln neben dem ursprünglich angefertigten Protokoll zu erlauben[198]; die bloß kursorische Berücksichtigung der Materialien durch die Senatsmehrheit[199] sei also nicht angezeigt.[200]

Nach *Rüthers* deutete sich in dem abweichenden Votum mithin an, dass das BVerfG in Zukunft die historische Auslegung stärken werde.[201] Ergänzend zu *Rüthers* lässt sich auf eine bereits 2007 ergangene Entscheidung hinweisen. Das BVerfG hatte dort darüber zu entscheiden, ob mit der Einfügung der Worte „*und fortzuentwickeln*“ in Art. 33 Abs.5 GG eine Abschwächung der ebenfalls in dieser Norm statuierten Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums verbunden sei.[202] Die Senatsmehrheit

[195] BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 54 – bverfg.de.

[196] BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 98, 103 – bverfg.de.

[197] Damit beantworten die abweichenden Richter implizit die Frage mit, ob die Motive zu Reichsgesetzen im Rahmen der historischen Auslegung überhaupt herangezogen werden können, was nicht ganz unproblematisch ist: zwar besteht das Deutsche Reich staatsrechtlich in der Gestalt der Bundesrepublik Deutschland fort, vgl. BVerfG, Beschluss vom 21. Oktober 1987, Az. 2 BvR 373/83, Rz. 52ff. – juris; staatsorganisatorisch ist der Reichstag jedoch mit dem Bundestag nicht identisch. In der Rechtsprechung werden die Vorarbeiten zu vorkonstitutionellen Gesetzen jedenfalls regelmäßig herangezogen, ohne dass dies methodisch problematisiert würde, vgl. zum Beispiel BVerfG, Urteil vom 7. Juni 2005, Az. 1 BvR 1508/96, Rz. 2 – bverfg.de.

[198] BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 108ff. – bverfg.de.

[199] Vgl. BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 46ff. – bverfg.de.

[200] BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 107 – bverfg.de.

[201] *Rüthers*, Rechtstheorie 2009, 253, 282.

[202] BVerfG, Beschluss vom 19. September 2007, Az. 2 BvF 3/02 – bverfg.de.

lehnte dies ab, da in den Gesetzesmaterialien zu der Grundgesetzänderung, die zu jener Norm geführt hatte, eindeutig formuliert worden war, dass die hergebrachten Grundsätze des Berufsbeamtentums wie bisher auch zu berücksichtigen seien; dieselbe Aussage hatte Bundeskanzlerin *Merkel* zudem in der abschließenden Aussprache im Bundestag getätigt.[203] Einer der Richter widersprach in seinem Minderheitsvotum der Senatsmehrheit mit dem Verweis auf die bisherige Rechtsprechung des BVerfG, derzufolge Aussagen in Gesetzesmaterialien eigentlich nicht mit dem objektiven Willen des Gesetzes gleichgesetzt werden dürften.[204] Auch in dieser Entscheidung hatte sich also bereits eine Trendwende angedeutet.

Rüthers jedenfalls sah sich nach einer weiteren Entscheidung des BVerfG aus dem Jahr 2011[205] mit seiner Prognose endgültig bestätigt: das Gericht hatte dort darüber zu befinden, ob die unterhaltsrechtliche Rechtsprechung des BGH zu § 1578 BGB verfassungsgemäß ist.[206] Nach § 1578 Abs.1 Satz 1 BGB wird der nacheheliche Unterhalt auf Grundlage der „*ehelichen Lebensverhältnisse*“ berechnet. Der BGH verstand diesen Wortlaut als „wandelbare eheliche Lebensverhältnisse“ und berücksichtigte folglich in seiner Berechnung auch Umstände, die erst *nach* der Ehescheidung auftraten. Für das BVerfG setzt der BGH damit seine eigenen Regelungsvorstellungen an die des Gesetzgebers.[207] Es hatte zwar auch Einwände in grammatischer und systematischer Hinsicht[208]; der BGH setze sich aber zudem über den *Willen des Gesetzgebers* hinweg, da in den Gesetzesmaterialien zu einer älteren Fassung des Unterhaltungsrecht vorgesehen war, dass Stichtag für die ehelichen Lebensverhältnisse der Zeitpunkt der Scheidung sein soll[209]. Aus den Gesetzesmaterialien zur aktuellen Fassung des Gesetzes gehe weiterhin

[203] BVerfG, Beschluss vom 19. September 2007, Az. 2 BvF 3/02, Rz. 85ff. – bverfg.de. Kritisch zur Berücksichtigung von Aussagen einzelner Abgeordneter *Wischmeyer*, JZ 2015, 957, 965.

[204] BVerfG, Beschluss vom 19. September 2007, Az. 2 BvF 3/02, Rz. 131 – bverfg.de.

[205] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10 – bverfg.de.

[206] Eine „objektiv fehlerhafte“ Rechtsanwendung, mithin eine Rechtsanwendung, die sich nicht mehr innerhalb der Grenzen vertretbarer Auslegung bewegt und auch keine zulässige Form der Rechtsfortbildung darstellt, kann als Verstoß gegen die allgemeine Handlungsfreiheit iVm dem Rechtsstaatsprinzip (Art. 2 Abs.1 GG iVm Art. 20 Abs.3 GG) gerügt werden, siehe BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 50 – bverfg.de.

[207] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 65 – bverfg.de.

[208] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 69ff. – bverfg.de.

[209] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 57 – bverfg.de.

hervor, dass der Gesetzgeber die bisherige Regelungskonzeption beibehalten wollte.[210] Das BVerfG setzt hier also den Willen des Gesetzgebers mit den Gesetzesmaterialien gleich.[211]

Hat das BVerfG mit dieser Entscheidung nun einen Methodenparadigmenwechsel eingeläutet? Neben *Rüthers*[212] erhielt diese Lesart auch von anderen Literaturstimmen Zuspruch.[213] *Rieble* äußerte sich jedoch skeptisch: naheliegender sei, in der Entscheidung eine einzelfallbezogene, politische Intervention zu sehen. Als Argument führt er an, dass das BVerfG im Übrigen für sich selbst eine erhebliche Auslegungsfreiheit betreffend die Normen des Grundgesetzes in Anspruch nehme.[214] Auch gegenüber dem EuGH sei das BVerfG in Fragen der Gesetzesbindung sehr großzügig. In Folge stuft er das BVerfG mehr als politisches Gericht denn als streng nach juristischen Methoden entscheidendes Gericht ein. Auch wenn er selbst hofft, dass die Lesart von *Rüthers* zutreffend ist, räumt er dem nur geringe Chancen ein.[215]

Wer hat aus heutiger Perspektive nun recht?

Eine eindeutige Antwort kann leider nicht gegeben werden. Dies könnte daran liegen, dass beide soeben vorgestellten Lesarten unzutreffend sind und stattdessen eine dritte anzulegen ist: Zunächst bleibt zu festzuhalten, dass die Entscheidung aus 2011 die Geltung der objektiven Theorie selbst an keiner Stelle in Frage stellt. Eine Gleichsetzung des Willens des Gesetzgebers mit den Gesetzesmaterialien bedeutet nicht automatisch eine Affirmation der subjektiven Theorie, sondern lediglich, dass in Abwesenheit besserer Argumente eine in den Gesetzesmaterialien klar zum Ausdruck gekommene Regelungsvorstellung nicht übergangen werden darf. Diese Lesart wird durch zeitlich nachfolgende Rechtsprechung des BVerfG gestützt. Eine eindeutige Stellungnahme zum Verhältnis der Entscheidung aus 2011 zu seiner früheren Methodenrechtsprechung hat das Gericht zwar (unbewusst?) vermieden bzw. war hierzu nicht veranlasst; in Entscheidungen nach der aus 2011 hat das

[210] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 58 – bverfg.de.

[211] Vgl. BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 53, 74 – bverfg.de.

[212] *Rüthers*, NJW 2011, 1856, 1857f.

[213] *Kötter*, BVerfG: Das Ende der „objektiven" Auslegungsmethode?; so generell auch *Reimer*, Was ist die Frage, auf die die juristische Methodenlehre eine Antwort sein will?, S. 11, 30f.

[214] *Rieble*, NJW 2011, 819, 820f.

[215] *Rieble*, NJW 2011, 819, 822.

BVerfG den Willen des Gesetzgebers allerdings nicht mehr mit den Gesetzesmaterialien gleichgesetzt, sondern sich erneut auf die Geltung der objektiven Theorie berufen und zudem eine fehlende Rangfolge der Auslegungsmethoden bekräftigt.[216]

Direkt revidiert hat das BVerfG seine Aussage aus 2011 allerdings auch nicht. Eine *Abschwächung* derselben kann jedoch darin erblickt werden, dass das BVerfG den Gesetzesmaterialien nunmehr „lediglich" eine „*nicht unerhebliche Indizwirkung*" zuschreibt.[217] Gegenüber der vor 2011 geltenden Methodenbeliebigkeit stellt dies aber immer noch eine *Stärkung* der Gesetzesmaterialien im Rahmen der Auslegung dar.[218]

Zum Schwur kann es nur kommen, wenn sich das BVerfG zwischen einer Aussage in den Gesetzesmaterialien einerseits und einem systematischen und/oder teleologischen Argument andererseits entscheiden muss. Dazu ist es bisher jedoch noch nicht gekommen, auch nicht – wie man unter Umständen meinen könnte – in der Entscheidung mit dem Aktenzeichen 2 BvR 1137/14. Zu entscheiden hatte das BVerfG dort, ob „*private Unternehmen*" im Sinne des Art. 143b Abs. 3 Satz 1 GG nur die unmittelbaren privatrechtlichen Nachfolger der Deutschen Bundespost (Deutsche Post AG, Deutsche Postbank AG und Deutsche Telekom AG) oder auch deren später gegründeten Tochtergesellschaften sind. Die historische Auslegung schien eher erstere Auslegungsvariante zu stützen, dennoch gab das BVerfG einer teleologischen Auslegung, die letzteres Ergebnis nahelegte, den Vorzug.[219] Allerdings ergab die historische Auslegung dort eben kein *eindeutiges* Ergebnis, das der teleologischen Auslegung zuwider gelaufen wäre.[220]

Als Fazit kann somit festgehalten werden, dass durch die angeführte Ent-

[216] BVerfG, Urteil vom 17. Januar 2017, Az. 2 BvB 1/13, Rz. 555 – bverfg.de; BVerfG, Beschluss vom 31. März 2016, Az. 2 BvR 1576/13, Rz. 63 – bverfg.de; BVerfG, Beschluss vom 26. August 2014, Az. 2 BvR 2172/13, Rz. 16 – bverfg.de; BVerfG, Urteil vom 19. März 2013, Az. 2 BvR 2628/10, 2 BvR 2883/10, 2 BvR 2155/11, Rz. 66 – bverfg.de.

[217] BVerfG, Beschluss vom 6. Juni 2018, Az. 1 BvL 7/14, Rz. 74 – bverfg.de; BVerfG, Beschluss vom 26. August 2014, Az. 2 BvR 2172/13, Rz. 16 – bverfg.de; BVerfG, Urteil vom 19. März 2013, Az. 2 BvR 2628/10, 2 BvR 2883/10, 2 BvR 2155/11, Rz. 66 – bverfg.de.

[218] So auch *Höpfner*, RdA 2018, 321, 323.

[219] BVerfG, Beschluss vom 2. Mai 2016, Az. 2 BvR 1137/14, Rz. 30 – bverfg.de.

[220] Vgl. BVerfG, Beschluss vom 2. Mai 2016, Az. 2 BvR 1137/14, Rz. 30 – bverfg.de.

scheidung aus dem Jahr 2011 und einige nachfolgenden Entscheidungen die historische Auslegung gegenüber den anderen Methoden gestärkt worden, eine Hinwendung zur subjektiven Theorie aber nicht erfolgt ist. Jedenfalls unterliegt eine Abweichung von einem Ergebnis der historischen Auslegung von nun an einem erhöhten Begründungsaufwand, der insbesondere umso höher ist, je eindeutiger in den jeweils einschlägigen Gesetzesmaterialien eine bestimmte Regelungskonzeption vorgesehen ist.

Durch diese vermittelnde Lösung werden auch die inhärenten, rechtstheoretischen Schwächen der Gleichsetzung des „Willens des Gesetzgebers“ mit den Gesetzesmaterialien vermieden. Diese fangen schon bei der Definition des Gesetzgebers an: sind dies nur die Abgeordneten, die für einen Gesetzesentwurf stimmen oder auch diejenigen, die dagegen stimmen oder sich enthalten? Unabhängig von der Beantwortung dieser Frage sind an der Abfassung der Gesetzesmaterialien meistens keine Abgeordneten beteiligt; sie werden stattdessen regelmäßig von einem Referatsleiter des Bundesjustizministeriums[221] veranlasst und erfahren im Laufe des Gesetzgebungsverfahrens meist zahlreiche Änderungen.[222] Nach der Zuleitung der Gesetzesmaterialien ist auch nicht sichergestellt oder überhaupt erforderlich, dass jeder Abgeordnete diese liest oder eine Vorstellung hierzu bildet. Ohnehin wird über Gesetzesmaterialien nicht abgestimmt, sondern nur über Gesetze. Aus Art. 76 GG oder sonstigen Verfassungsnormen lässt sich eine Begründungspflicht für die „*Gesetzesvorlagen*“ nicht entnehmen.[223] Mithin kann aus dem GG nicht abgeleitet werden, dass der Beschluss über eine Gesetzesvorlage im Sinne der Art. 77ff. GG implizit einen Beschluss über die Gesetzesmaterialien enthält. Gleiches gilt für die Vorschriften der Geschäftsordnung des Bundestages (BTGO). Gemäß § 86 BTGO wird nach dem Schluss der dritten Lesung über „*Gesetzesentwürfe*“ abgestimmt. In § 76 Abs.2 BTGO werden „*Gesetzesentwürfe*“ und deren „*Begründung*“ begrifflich getrennt; einem Gesetzesentwurf ist nach dieser Norm eine Begründung anzufügen, also enthält der Gesetzesentwurf diese (im Rechtssinne) selbst nicht. Mithin wird auch nach der BTGO nicht über die Gesetzesmaterialien abgestimmt. Selbst aber wenn über diese abgestimmt werden würde, ließe sich aus einer formellen Zustimmung eines Abgeordneten zum Gesetz nicht ableiten, dass dieser dem Gesetz oder

[221] Bzw. eines der Landesjustizministerien.
[222] *Schneider*, Was der Gesetzgeber wollte!, S. 111, 117f.
[223] *Kersten* in: Herzog et al., Maunz/Dürig, 92. EL 2020, Art. 76 GG, Rz. 22.

der Begründung auch innerlich zustimmt, da die formelle Zustimmung auch aus anderen Gründen als innerlicher Zustimmung (Fraktionszwang, Kompromiss etc.) erfolgt sein könnte.[224] Ein „Wille des Gesetzgebers“ kann im Ergebnis also allenfalls fingiert werden.[225] Folglich kann auch die Gleichsetzung der Gesetzesmaterialien mit einem Willen des Gesetzgebers nur dann erfolgen, wenn Letzterer als Fiktion angesehen wird.

Die Verwendung des Begriffes „Wille des Gesetzgebers“ durch das BVerfG sollte also als Metapher für einen Teil des zur Verfügung stehenden Auslegungsmaterials verstanden werden, dem – soweit ihm ein bestimmtes Auslegungsergebnis entnommen werden kann – in Abwesenheit gewichtigerer Argumente der Vorzug zu geben ist.

Dieses Ergebnis ist handhabbar und kann auf die BGH-Entscheidung „Alles kann besser werden“ angewendet werden, auch wenn letzte ungeklärte Punkte verbleiben.[226]

cc) Anwendung der Rechtsprechung des BVerfG seit 2011 auf „Alles kann besser werden“

Die Entscheidung „Alles kann besser werden“ erweist sich unter Anwendung der Rechtsprechung des BVerfG seit 2011 nach hiesiger Wertung als verfassungswidrig in Form eines Verstoßes gegen Art. 2 Abs.1 GG iVm Art. 20

[224] *Lorz*, Die Gesetzesauslegung im Blick des Gesetzgebers?, S. 87, 97f.

[225] *Lorz*, Die Gesetzesauslegung im Blick des Gesetzgebers?, S. 87, 97f.; zu den mit dieser Fiktion wiederum verbundenen Schwierigkeiten siehe *von Landenberg-Roberg/Sehl*, Rechtswissenschaft 2015, 135, 142ff.

[226] Insbesondere ist in der Rechtsprechung des BVerfG offen, wie sich die Entstehungsgeschichte zu den Gesetzesmaterialien verhält. Das BVerfG hatte – wie dargestellt – *nur* die Gesetzesmaterialien mit dem Willen des Gesetzgebers gleichgesetzt, zum Teil aber auch die Entstehungsgeschichte – wie etwa Aussagen einzelner Abgeordneter – berücksichtigt. In einer Entscheidung aus dem Jahr 2018 hat das BVerfG jedenfalls klargestellt, dass nicht nur die Gesetzesbegründung zu berücksichtigen ist, sondern auch die Stellungnahmen des Bundesrats und der Bundesregierung hierauf sowie Stellungnahmen, Beschlussempfehlungen und Beschlüsse der Ausschüsse, siehe BVerfG, Beschluss vom 6. Juni 2018, Az. 1 BvL 7/14, Rz. 74 – bverfg.de; insbesondere zieht es aus nicht berücksichtigten Stellungnahmen bei Sachverständigenanhörungen sowie nicht berücksichtigten Änderungsanträgen den Umkehrschluss, dass der Gesetzgeber an seiner ursprünglich in der Gesetzesbegründung aufgestellten Regelungskonzeption festhalten möchte, siehe BVerfG, Beschluss vom 6. Juni 2018, Az. 1 BvL 7/14, Rz. 85 – bverfg.de.

Abs.3 GG. Das erzielte Auslegungsergebnis des BGH ist nicht nur objektiv fehlerhaft, sondern setzt sich darüber hinaus in krassen Widerspruch zu der zur Anwendung gebrachten Norm.

Wie aufgezeigt, lassen Wortlaut und Systematik des § 101 Abs.2 UrhG eine Auslegung sowohl dahingehend zu, dass der Anspruch ein gewerbliches Ausmaß der Verletzung verlangt, als auch dahingehend, dass ein solches Ausmaß nicht verlangt wird. Ein teleologisches Argument[227] lässt sich weder für die eine oder andere Richtung überzeugend herleiten. Andere vom BGH verwendete Argumente sind nicht zulässig oder verfangen nicht.[228]

In den Gesetzesmaterialien war ausdrücklich formuliert worden, dass die Verletzungshandlung im Sinne von § 101 Abs.2 UrhG „*im geschäftlichen Verkehr*“ erfolgen muss:

> *„Auch der in Absatz 2 geregelte Auskunftsanspruch gegenüber Dritten setzt voraus, dass die Rechtsverletzung im geschäftlichen Verkehr erfolgt ist. Damit wird auch hier dem Erwägungsgrund 14 der Richtlinie Rechnung getragen, wonach ein Auskunftsanspruch auf jeden Fall dann vorgesehen werden muss, wenn die Rechtsverletzung in gewerblichem Ausmaß vorgenommen worden ist. Auf eine Handlung im geschäftlichen Verkehr wird in der Regel dann zu schließen sein, wenn ihr Ausmaß über das hinausgeht, was einer Nutzung zum privaten Gebrauch entspricht.“* [229]

Mit „geschäftlicher Verkehr“ ist letztlich nichts anderes gemeint als mit dem „gewerblichen Ausmaß“; es handelt sich um eine inhaltlich nicht bedeutsame, rein terminologische Differenzierung, die für den Gesetzeswortlaut in der Beschlussempfehlung des Rechtsausschusses aufgehoben wurde.[230] Der Bundesrat hatte in seiner Stellungnahme zwar noch in inhaltlicher Hinsicht eingewandt, dass das Erfordernis eines gewerblichen Ausmaßes unter Umständen dazu führen könnte, dass in *filesharing*-Konstellationen gar keine Auskunft mehr erteilt werden könne.[231]; die Bundesregierung hielt in ihrer

[227] Unbeschadet allen diesem Konzept inhärenten Problemen, siehe Kapitel § 4 IV. 1. d) aa).
[228] Siehe Kapitel § 4 IV. 1. b) und c).
[229] BT-Drs. 16/5048, S. 49.
[230] BT-Drs. 16/8783, S. 28.
[231] BT-Drs. 16/5048, S. 59.

Gegenäußerung jedoch an dem Erfordernis fest.[232]

Folglich kommt in den Gesetzesmaterialien zum Ausdruck, dass die Verletzungshandlung im Sinne von § 101 Abs.2 UrhG in einem gewerblichen Ausmaß erfolgen muss. Dies wird vom BGH in der Entscheidung „Alles kann besser werden“ auch anerkannt, jedoch als unbeachtlich angesehen.[233] Folglich stellt er sich mit dieser Entscheidung in krassen Widerspruch zu der Regelungskonzeption des Gesetzgebers.

Einen Verstoß gegen Art. 2 Abs.1 GG iVm Art. 20 Abs.3 GG kann die Entscheidung mithin nur dann nicht (mehr) darstellen, wenn sie vom Gesetzgeber ausdrücklich oder stillschweigend gebilligt wurde. Das BVerfG erachtet die ausdrückliche oder stillschweigende Billigung einer Rechtsprechungspraxis grundsätzlich als möglich[234], die Annahme einer stillschweigenden Billigung komme aber regelmäßig nicht in Betracht.[235] Gleiches gilt für die Annahme einer Billigung auf Grund Untätigkeit des Gesetzgebers.[236] Eine genaue Konturierung der Voraussetzungen einer gesetzgeberischen Billigung fehlt jedoch bisher. Da eine stillschweigende Billigung oder Billigung durch Untätigkeit normalerweise nicht in Betracht kommt, wird für die Zwecke dieser Arbeit davon ausgegangen, dass – anknüpfend an die seit 2011 gesteigerte Bedeutung der Gesetzesmaterialien – eine Billigung zumindest voraussetzt, dass eine bestimmte Rechtsprechung in den Gesetzesmaterialien zur Kenntnis genommen und im weitesten Sinne gutgeheißen wird.

Dies vorausgesetzt, kann eine Billigung der Entscheidung „Alles kann besser werden“ durch den Gesetzgeber nicht angenommen werden. Eine Billigung wäre beispielsweise im Rahmen des Gesetzes gegen unlautere Geschäftspraktiken möglich gewesen. In den Gesetzesmaterialien hierzu wurde jedoch lediglich die – durch den BGH mitverantwortete – Praxis der Massenabmahnungen zur Kenntnis genommen[237], allerdings deren Ursachen – wie die Entscheidung „Alles kann besser werden“ – nicht namentlich benannt geschweige

[232] BT-Drs. 16/5048, S. 59.

[233] BGH, Beschluss vom 19. April 2012, Az. I ZB 80/11, Rz. 28 – GRUR 2012, 1026 - „Alles kann besser werden“.

[234] BVerfG, Beschluss vom 25. Januar 2011, Az. 1 BvR 918/10, Rz. 53 – bverfg.de; BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 137 – bverfg.de.

[235] BVerfG, Beschluss vom 9. Februar 1988, Az. 1 BvL 23/86, Rz. 17 – juris.

[236] BVerfG, Beschluss vom 15. Januar 2009, Az. 2 BvR 2044/07, Rz. 137 – bverfg.de.

[237] Vgl. BT-Drs. 17/13057, S. 11.

denn gutgeheißen.

e) Verfassungskonforme Auslegung im Übrigen

Im Übrigen bestehen gegen die Entscheidung „Alles kann besser werden“ jedoch keine verfassungsrechtlichen Bedenken. Die Überlegungen des BGH zur Grundrechtskonformität im Licht der Rechtsprechung zur Vorratsdatenspeicherung sind überflüssig, da es sich hierbei um einen gegenüber dem Auskunftsanspruch in Urheberrechtssachen spezielleren Fall handelt, aus dem für sonstige Formen des Umgangs mit IP-Adressen außerhalb seines Anwendungsbereichs keine Rückschlüsse gezogen werden können.[238] Das Erfordernis eines gewerblichen Ausmaßes einer Verletzungshandlung für den Auskunftsanspruch ist grundrechtlich im Übrigen (also abgesehen von dem Verstoß gegen Art. 2 Abs.1 GG iVm Art. 20 Abs.3 GG) nicht geboten.[239]

f) Bewertung der BGH-Rechtsprechung

Die Entscheidung des BVerfG, die die Gesetzesmaterialien erstmals gegenüber den übrigen Methoden aufwertete[240] erging am 25. Januar 2011. Der BGH bzw. der mit der Abfassung der Entscheidungsgründe betraute Berichterstatter hätte diese also ohne weiteres zur Kenntnis nehmen können. Jedoch fehlt in „Alles kann besser werden“ jegliche Auseinandersetzung mit dem BVerfG; gleiches gilt für die späteren drei Entscheidungen des BGH, in denen er mit knappen Worten „Alles kann besser werden“ bestätigt.[241]

Die Linie des BGH ist nicht nur wegen des Grundrechtsverstoßes an sich bedenklich, sondern in besonderem Maße auch wegen ihrer Folgen: schließlich beruht das Abmahnwesen im *filesharing* maßgeblich darauf, dass ohne weiteres Auskunft über Anschlussinhaber erlangt und im Verletzungsprozess verwertet werden kann.[242] Dabei verbleibt nicht einmal der Trost einer wenigstens konsequenten Linie. Beispielsweise schreibt der I. Senat in der Ent-

[238] Siehe Kapitel § 4 V. 2. b) und 3.
[239] Vgl. Kapitel § 4 V. 2. a).
[240] Siehe Kapitel § 4 IV. 1. d) bb).
[241] Vgl. BGH, Beschluss vom 25. Oktober 2012, Az. I ZB 13/12, Rz. 11 – ZUM 2013, 38; BGH, Beschluss vom 5. Dezember 2012, Az. I ZB 48/12, Rz. 30 – GRUR 2013, 536 - „Heiligtümer des Todes“; BGH, Beschluss vom 16. Mai 2013, Az. I ZB 44/12, Rz. 8 – BeckRS 2013, 13001.
[242] Siehe Kapitel § 3 VII.

scheidung „Kindersekt“ den dort einschlägigen Gesetzes- bzw. Verordnungsmaterialien für die Auslegung eine gegenüber den übrigen Auslegungsmitteln hervorgehobene Bedeutung zu.[243] Einen Widerspruch zur Entscheidung „Alles kann besser werden“ vermag der Senat hierin jedoch nicht zu erkennen; schließlich sei es dort lediglich um Motive und Vorstellungen von am Gesetzgebungsverfahren beteiligten Organen bzw. einzelner ihrer Mitglieder gegangen, die für die Auslegung aber irrelevant seien.[244] Abgesehen davon, dass dies auch nach verfassungsrechtlicher Rechtsprechung nicht unbedingt sein muss[245], ist diese Aussage jedenfalls unzutreffend, da auch in „Alles kann besser werden“ Gesetzesmaterialien und nicht nur etwa Aussagen einzelner Abgeordneter für die Auslegung heranzuziehen waren.

Die Rechtsprechung des ersten Senats bekommt damit den Anstrich methodischer Beliebigkeit. Anscheinend sollen – vom Ergebnis her gedacht – die Urheberrechtsdurchsetzungsmöglichkeiten maximiert werden; das Erfordernis eines gewerblichen Ausmaßes würde hierbei nur stören, sodass die Auslegung desselben vermieden werden soll, indem es einfach gleich für unbeachtlich erklärt wird. Daher verwundert nicht, dass der Senat auch andere Möglichkeiten der Korrektur hat verstreichen lassen: so wäre der Grundrechtsverstoß nach hiesiger Auffassung behoben worden, wenn der BGH das Merkmal in den Verletzungsprozess verschoben hätte, indem er zwar für den Auskunftsanspruch ein gewerbliches Ausmaß der Verletzung nicht fordert, im Verletzungsprozess im Rahmen der Beweiswürdigung nach § 286 Abs.1 ZPO jedoch schon. Beispielsweise könnte dann der Nachweis einer Verletzung nur als erbracht angesehen werden, wenn ein gewerbliches Ausmaß nachgewiesen wird, zum Beispiel indem mehrere Auskünfte über die Verletzung desselben Werkes über denselben Anschluss innerhalb eines kurzen Zeitraumes vorgelegt werden.[246] Solche Überlegungen hätten insbesondere in der Entscheidung „Tauschbörse I“ Platz finden können, in der sich der BGH ja mit der Beweiswürdigung teilweise auseinander gesetzt hat.[247]

[243] BGH, Beschluss vom 17. Juli 2013, Az. I ZR 211/12, Rz. 14f. – GRUR-RR 2014, 129 - „Kindersekt“.

[244] BGH, Beschluss vom 17. Juli 2013, Az. I ZR 211/12, Rz. 14f. – GRUR-RR 2014, 129 - „Kindersekt“.

[245] Siehe zur Berücksichtigung von Aussagen einzelner Bundestagsabgeordneter durch das BVerfG in Kapitel § 4 IV. 1. d) bb).

[246] Siehe zur näheren Ausgestaltung Kapitel § 5 IV. 4.

[247] Siehe Kapitel § 2 VI. 1.

Im Ergebnis jedenfalls verbleibt ein Grundrechtsverstoß, sodass nach hiesiger Wertung (letztinstanzliche) Gestattungsbeschlüsse, in denen Rechteinhabern gegenüber ISPs die Auskunft über Anschlussinhaber gestattet wird, obwohl ein gewerbliches Ausmaß der Rechtsverletzung nicht nachgewiesen wurde, letztlich erfolgreich mit einer Verfassungsbeschwerde angegriffen werden könnten.[248] In noch laufenden Verletzungsprozessen könnte ein Gericht die auf Grund eines solchen Gestattungsbeschlusses erteilte Auskunft mit einem Beweisverwertungsverbot belegen.[249]

g) Zusammenfassung

Bei der Auslegung des § 101 Abs.2 UrhG kommt es für die Frage, ob die Verletzung, über die Auskunft erteilt werden soll, in einem gewerblichen Ausmaß erfolgen muss, auf den Stellenwert der historischen Auslegung – verstanden als Betrachtung der Gesetzesmaterialien und der Entstehungsgeschichte – an (mangels Ergiebigkeit der übrigen Auslegungsmittel). Der BGH bewertet diesen angesichts der seit 2011 ergangenen Rechtsprechung des BVerfG zur historischen Auslegung falsch und lehnt daher das Erfordernis eines gewerblichen Ausmaßes unzutreffender Weise ab. Die Entscheidungen des BGH zum Auskunftsanspruch in *filesharing*-Konstellationen stellen somit nach hiesiger Wertung einen Grundrechtsverstoß dar. Gelegenheiten, diesen durch die Berücksichtigung des Erfordernisses eines gewerblichen Ausmaßes an anderer Stelle zu korrigieren, hat der BGH nicht genutzt.

2. Zum Auskunftsanspruch in Reseller-Konstellationen

Bei der Auskunft in Reseller-Konstellationen[250] gibt es zwei dogmatische Streitpunkte. Erstens, ob gegenüber dem Netzbetreiber eine Gestattungsanordnung ergehen darf, und zweitens, ob gegenüber dem Reseller eine Ge-

[248] Da es vorliegend, wie dargestellt, um einen Verstoß gegen das Willkürverbot geht, kann letztlich dahinstehen, ob in materieller Hinsicht nach der „Recht auf Vergessen"-Rechtsprechung des BVerfG europäische oder deutsche Grundrechte zu prüfen wären. Siehe hierzu BVerfG, Beschluss vom 6. November 2019, Az. 1 BvR 16/13, Rz. 42ff. – bverfg.de - „Recht auf Vergessen I" und BVerfG, Beschluss vom 6. November 2019, Az. 1 BvR 276/17, Rz. 42ff. – bverfg.de - „Recht auf Vergessen II".

[249] Eine Restitutionsklage nach § 580 ZPO gegen bereits rechtskräftig abgeschlossene Verletzungsverfahren kommt jedoch mangels einschlägiger Tatbestände der Norm nicht in Betracht.

[250] Siehe hierzu Kapitel § 1 IV. 5. c) und § 2 III. 1. d).

stattungsanordnung erforderlich ist. Der BGH hat sich in der Entscheidung „Benutzerkennung“ zu beiden Fragen geäußert.[251]

a) Zulässigkeit einer Gestattungsanordnung an den Netzbetreiber

Eine Gestattungsanordnung darf nur ergehen, wenn der Auskunftsanspruch materiell besteht.[252] In Reseller-Konstellationen kann der Netzbetreiber nur die Anschlusskennung, nicht jedoch den Namen und die Anschrift des Anschlussinhabers mitteilen. Gegenstand des Auskunftsbegehrens können dem Wortlaut des § 101 Abs.3 Nr.1 UrhG nach jedoch allenfalls Name und Anschrift, nicht die Anschlusskennung sein.

Der BGH löst das Problem allein durch eine rechtsfolgenorientierte Erwägung: der Wortlaut der Norm stünde der Gestattungsanordnung nicht entgegen, da andernfalls der Anschlussinhaber nicht ermittelt werden könne.[253] Diese Argumentation ist zirkulär, da es ja gerade fraglich ist, ob Ergebnis der Auslegung sein kann, dass der Anschlussinhaber auch in Reseller-Konstellationen ermittelt werden können soll. Methodisch vollzieht der BGH implizit einen Analogieschluss, da der Begriff „Anschlusskennung“ vom Wortlaut des § 101 Abs.3 Nr.1 UrhG eindeutig nicht gedeckt ist.

Nach Auffassung des Verfassers ist zwar – auf Grund der vom BVerfG betonten, strengen Gesetzesbindung[254] – mit Analogieschlüssen sehr zurückhaltend umzugehen[255], in diesem Fall würde sich ein Analogieschluss aber gerade zu aufdrängen. Weder vom europäischen Gesetzgeber noch vom Bundesgesetzgeber wurde die Möglichkeit einer Reseller-Konstellation berücksichtigt, jedoch war die Möglichkeit der Auskunft gegen Endkunden von ISPs ausdrücklich gewollt.[256] Hierzu wäre aber zuvor zu prüfen, ob eine richtlinienkonforme Auslegung der Rechtsfortbildung im Wege steht und sodann, ob eine planwidrige Regelungslücke vorliegt. Dies hat der BGH jedoch erst in

[251] BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16 – GRUR 2018, 189 - „Benutzerkennung“.

[252] Siehe Kapitel § 2 III. 1. b).

[253] BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16, Rz. 25 – GRUR 2018, 189 - „Benutzerkennung“.

[254] Siehe Kapitel § 4 IV. 1. d).

[255] Zur verfassungsrechtlichen Zulässigkeit der Analogie siehe grundlegend BVerfG, Beschluss vom 3. April 1990, Az. 1 BvR 1186/98 – juris.

[256] Vgl. BT-Drs. 16/5048, S. 32.

dem Entscheidungskomplex „YouTube-Drittauskunft“[257] nachgeholt. Streitig war dort, ob der Begriff der „Anschrift“ in § 101 Abs.3 Nr.1 UrhG auch Email-Adressen, Telefonnummern und IP-Adressen umfasst; im Hinblick auf eine wegen Art. 8 Abs.2 lit. a) EnforcementRL etwaig erforderliche richtlinienkonforme Auslegung rief der BGH den EuGH an.[258] Dieser entschied, dass der Begriff der „Adresse“ in Art. 8 Abs.2 lit. a) EnforcementRL nur die postalische Anschrift umfasst[259], diese Norm jedoch auch lediglich eine Mindestharmonisierung darstelle, die Mitgliedstaaten also weitergehende Auskunftsansprüche zulassen können.[260] Hieraus folgerte der BGH zutreffend, dass im Rahmen der richtlinienkonformen Auslegung andere Gegenstände als die die postalische Anschrift nicht vom Wortlaut des § 101 Abs.3 Nr.1 UrhG umfasst sind, die EnforcementRL einem Analogieschluss aber auch nicht grundsätzlich im Wege steht.[261]

Es verblieb somit die Frage, ob die für einen Analogieschluss erforderliche Regelungslücke vorliegt. In der obergerichtlichen Rechtsprechung war es bereits anerkannt, dass in dem Fall, in dem ein Bundesgesetz ausweislich seiner Gesetzesbegründung allein eine Richtlinie umsetzen soll, nach der Rechtsprechung des EuGH zu dieser Richtlinie aber der Wortlaut des Bundesgesetzes über den erlaubten Regelungsgehalt der Richtlinie hinausgeht, dieses im Wege der teleologischen Reduktion auf den vom EuGH fixierten Bedeutungsgehalt reduziert werden darf.[262] Entsprechend liegt nahe, dass für den umgekehrten Fall, in dem sich ein Bundesgesetz im relevanten Bereich ausweislich auf die Umsetzung einer Richtlinie beschränken soll, eine planwidrige Regelungslücke hinsichtlich eines außerhalb der Richtlinie liegenden Gegenstandes nicht angenommen werden kann. Folglich hat der BGH zutreffend

[257] BGH, Beschluss vom 21. Februar 2019, Az. I ZR 153/17 – GRUR 2019, 504 - „YouTube-Drittauskunft“; EuGH, Urteil vom 9. Juli 2020, Rs. C-264-19 – ECLI:EU:C:2020:542 - „Constantin Film Verleih“; BGH, Urteil vom 10. Dezember 2020, Az. I ZR 153/17 – NJW 2021, 779 - „YouTube-Drittauskunft II“.

[258] BGH, Beschluss vom 21. Februar 2019, Az. I ZR 153/17 – GRUR 2019, 504 - „YouTube-Drittauskunft“.

[259] EuGH, Urteil vom 9. Juli 2020, Rs. C-264-19, Rz. 28ff. – ECLI:EU:C:2020:542- „Constantin Film Verleih“.

[260] EuGH, Urteil vom 9. Juli 2020, Rs. C-264-19, Rz. 36, 39 – ECLI:EU:C:2020:542 - „Constantin Film Verleih“.

[261] BGH, Urteil vom 10. Dezember 2020, Az. I ZR 153/17, Rz. 18ff. – NJW 2021, 779 - „YouTube-Drittauskunft II“.

[262] Siehe Nachweise bei *Knops*, NJW 2020, 2297, 2298.

angenommen, dass sich der Gesetzgeber ausweislich der Begründung zum Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums mit § 101 Abs.3 Nr.1 UrhG auf die Umsetzung von Art. 8 Abs.2 lit. a) EnforcementRL beschränkt hat und daher eine planwidrige Regelungslücke betreffend andere Gegenstände als die postalische Anschrift nicht vorliegt.[263]

Nichts anderes kann daher für die Anschlusskennung gelten: weder kann diese im Rahmen der Auslegung in § 101 Abs.3 Nr.1 UrhG einbezogen werden noch darf die Norm im Wege der Analogie auf diese erstreckt werden. Dem BGH ist diesbezüglich daher betreffend die Entscheidung „Benutzerkennung" weder im Begründungsweg noch im Ergebnis zuzustimmen.

b) Erforderlichkeit einer Gestattungsanordnung an den Reseller

Eine Gestattungsanordnung gegenüber dem Reseller wäre gemäß § 101 Abs.9 UrhG iVm § 3 Nr.30 TKG nur erforderlich, wenn er dadurch, dass er eine Anschlusskennung mit einem konkreten Namen und einer Anschrift verknüpft und diese dem Auskunft begehrenden Rechteinhaber mitteilt, eine Auskunft unter Verwendung von Verkehrsdaten erteilt. Dann bräuchte der Rechteinhaber für eine Verwertbarkeit der Auskunft im Verletzungsprozess, sofern man das Fehlen der Gestattungsanordnung als Beweisverwertungsverbot einstuft, zwei Gestattungsanordnungen, nämlich die erste, den Netzbetreiber betreffend, der die IP-Adresse mit einer Anschlusskennung verknüpft, und die zweite, den Reseller betreffend, der Vertragspartner des Kunden ist, dem die entsprechende Anschlusskennung zugeordnet ist und der die Kennung mit Name und Anschrift verknüpft.

Dem Wortlaut des § 101 Abs.9 Satz 1 UrhG nach ist eine Gestattungsanordnung erforderlich, wenn die Auskunft „*nur unter Verwendung von Verkehrsdaten [...] erteilt werden kann*". Name und Anschrift selbst sind unstreitig Bestandsdaten im Sinne von § 3 Nr.3 TKG.[264] § 101 Abs.9 Satz 1 UrhG ist also nur einschlägig, wenn entweder die Anschlusskennung ein Verkehrsdatum (und kein Bestandsdatum) ist oder „*unter Verwendung*" auch dann als erfüllt anzusehen ist, wenn die Bestandsdaten nur mittelbar über Verkehrsdaten erlangt werden (nämlich über die Verkehrsdaten, die Gegenstand der

[263] BGH, Urteil vom 10. Dezember 2020, Az. I ZR 153/17, Rz. 19f., 29 – NJW 2021, 779 - „YouTube-Drittauskunft II".

[264] *Büttgen* in: Geppert/Schütz, BeckTKG, 4. Aufl. 2013, § 3 TKG, Rz. 9.

Auskunft des Netzbetreibers sind).

Zunächst ist anzumerken, dass die Benutzerkennung – sofern man sie als Bestandsdatum ansieht – nicht dadurch zum Verkehrsdatum wird, dass sie mittelbar mit Verkehrsdaten verknüpft wird.[265] Das TKG sieht in § 3 Nr.3 und Nr.30 TKG eine klare definitorische Trennung zwischen Bestands- und Verkehrsdaten vor, sodass die Möglichkeit der „Metamorphose" eines Datums, das bereits eindeutig als Bestandsdatum eingeordnet wurde, zu einem Verkehrsdatum nicht angezeigt erscheint.

Aber warum sollte die Anschlusskennung überhaupt ein Bestandsdatum sein? Der BGH nimmt dies ohne Begründung an.[266] Die als Beleg zitierte Instanzrechtsprechung liefert ebenfalls keine Begründung.[267] Für die Rechtsprechung, die das so sieht, scheint das entscheidende Kriterium zu sein, dass die Anschlusskennung statisch ist.[268] Diese Überzeugung speist sich wohl aus dem Umstand, dass *dynamische* IP-Adressen Verkehrsdaten sind. Jedoch spielt für das TKG die Unterscheidung zwischen dynamisch und statisch gar keine Rolle; ein Verkehrsdatum ist nach § 3 Nr.30 TKG jedes Datum, das bei der Erbringung eines Telekommunikationsdienstes genutzt wird. Die Kennung eines Anschlusses wird in technischer Hinsicht bei der Erbringung eines Telekommunikationsdienstes genutzt. Ohnehin führt bereits die Nr.1 des § 96 Abs.1 TKG, der damit befasst ist, welche Verkehrsdaten ein ISP erheben darf, die Anschlusskennung auf, ordnet Letztere also unzweifelhaft als Verkehrsdatum ein. Da die Anschlusskennung mithin bereits selbst ein Verkehrsdatum ist, kommt es auf die Frage, ob „*unter Verwendung*" in § 101 Abs.9 Satz 1 UrhG auch dann erfüllt ist, wenn ein Verkehrsdatum *mittelbar* verwendet wird, nicht mehr an.

Der Begründungsweg des BGH in der Entscheidung „Benutzerkennung" ist also, da die Benutzerkennung ein Verkehrsdatum ist, auch betreffend der Erforderlichkeit einer Gestattungsanordnung an einen Reseller dogmatisch unrichtig. Sie kann sich jedoch vom Ergebnis her als richtig erweisen, wenn

[265] AG Potsdam, Urteil vom 12. November 2015, Az. 37 C 156/15, Rz. 17ff. – juris. So aber *Zimmermann*, K&R 2015, 73, 74.

[266] Vgl. BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16, Rz. 21 – GRUR 2018, 189 - „Benutzerkennung".

[267] Vgl. OLG Köln, Beschluss vom 27. November 2012, Az. 6 W 181/12 – MMR 2013, 320; AG Potsdam, Urteil vom 12. November 2015, Az. 37 C 156/15, Rz. 17ff. – juris.

[268] AG Potsdam, Urteil vom 12. November 2015, Az. 37 C 156/15, Rz. 17ff. – juris.

§ 101 Abs.9 Satz 1 UrhG teleologisch reduziert werden dürfte.[269]

Dies dürfte vorliegend zulässig sein. Die zur analogen Anwendung von § 101 Abs.3 Nr.1 UrhG angestellten europarechtlichen Erwägungen und Bezüge[270] greifen vorliegend nicht, da § 101 Abs.9 UrhG keine europarechtlichen Vorgaben aus der EnforcementRL umsetzt.[271] Ein planwidriger Regelungsüberschuss besteht, da der Gesetzgeber die Reseller-Konstellation schlicht übersehen hat. Die Interessenlage ist vergleichbar, da weder der jeweils betroffene Reseller noch der jeweils betroffene Anschlussinhaber ein Schutzniveau benötigen, dem nicht schon durch die Gestattungsanordnung gegenüber dem Netzbetreiber Rechnung getragen wurde. Letztere wirkt zwar gemäß den Regeln des FamFG nur *inter partes*[272], vermittelt aber eine Legalisierungswirkung[273], da es für den Reseller keinen Gesichtspunkt zu prüfen gibt, der nicht schon durch den Netzbetreiber zu prüfen war. Folglich weist die Auskunft des Resellers gegenüber der des Netzbetreibers auch keine eigene Grundrechtssensibilität auf. Eine Gestattungsanordnung, die an Ersteren zu adressieren wäre, käme mithin einer bloßen Förmelei gleich.

Hierauf kann nicht erwidert werden, dass auch die Auskunft über die Bestandsdaten Name und Anschrift den besonderen datenschutzrechtlichen Vorschriften der §§ 111 Abs.1 Satz 1 Nr.2, 113 Abs.1, 3 TKG unterworfen sind.[274] Diese Vorschriften betreffen die Vorratsdatenspeicherung, die betreffend Auskunftsbegehren[275] für ihren eigenen Sachbereich *lex specialis* zu Auskunftsbegehren auf anderen Gebieten – also insbesondere dem Urheberrecht – ist.[276] Es können also aus den Vorschriften über die Vorratsdatenspeicherung keine Rückschlüsse für Auskunftsbegehren auf der Grundlage von Urheberrechtsverletzungen gezogen werden.

---

269 Zur verfassungsrechtlichen Zulässigkeit der teleologischen Reduktion siehe BVerfG, Beschluss vom 31. Oktober 2016, Az. 1 BvR 871/13, 1 BvR 1833/13, Rz. 22f. – bverfg.de.

270 Siehe vorstehend Kapitel § 4 IV. 2. a).

271 Siehe Kapitel § 2 III. 1. b).

272 *Zimmermann*, K&R 2015, 73, 74.

273 BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16, Rz. 21 – GRUR 2018, 189 - „Benutzerkennung“; *Sesing*, NJW 2018, 754, 755f; *Issa*, ZUM 2017, 390, 397.

274 So jedoch AG Augsburg, Urteil vom 22. Juni 2015, Az. 16 C 3030/14, Rz. 28f. – juris; AG Koblenz, Beschluss vom 2. Januar 2015, Az. 153 C 3184/14, Rz. 11ff. – juris.

275 Nicht jedoch – im Rahmen des Bundesrechts außerhalb einer Richtlinienumsetzung – betreffend *Sicherungs*begehren, siehe Kapitel § 4 V. 3.

276 Siehe hierzu Kapitel § 4 V. 2. b).

Im Ergebnis ist es daher vertretbar, für die Auskunft des Resellers eine eigene Gestattungsanordnung nicht für erforderlich zu halten.

Es soll hier dahinstehen, ob im Falle der Geltung der gegenteiligen Ansicht aus einer fehlenden Gestattungsanordnung im Zivilprozess für die Auskunft auch ein Beweisverwertungsverbot folgen würde.[277]

c) Bewertung der BGH-Rechtsprechung

Die Rechtsprechung des BGH zur Auskunft in Reseller-Konstellationen ist nur im Ergebnis teilweise vertretbar.

Hauptkritikpunkt ist, dass eine Vorlage an den EuGH betreffend den Auskunftsanspruch gegen Netzbetreiber auf Mitteilung der Anschlusskennung ausdrücklich unterlassen wurde[278], sodass der BGH eigentlich bereits für diesen Fall zu den Ergebnissen hätte gelangen können, die der Entscheidungskomplex „YouTube-Drittauskunft“ zu Tage gefördert hat – mit der Folge, dass er einen Anspruch gegen ISPs, die Benutzerkennung mitzuteilen, hätte verneinen müssen.

Der Bewertung der Zulässigkeit des Verzichts auf eine Gestattungsanordnung an den Reseller durch den BGH ist, wie dargestellt, jedoch zuzustimmen.

Zu den Konsequenzen aus dieser Bewertung siehe Kapitel § 5 IV. 5.

V. Zur Sicherung des Auskunftsanspruchs

Ein *ausdrücklich* normierter Anspruch auf Sicherung des Auskunftsanspruchs existiert nicht.

Die Rechtsprechung des BGH[279], derzufolge ein solcher Anspruch besteht[280], ist folglich in dogmatischer Hinsicht danach zu bewerten, ob erstens eine

277 Ablehnend *Issa*, ZUM 2017, 390, 395.

278 BGH, Urteil vom 13. Juli 2017, Az. I ZR 193/16, Rz. 28 – GRUR 2018, 189 - „Benutzerkennung“.

279 BGH, Urteil vom 21. September 2017, Az. I ZR 58/16 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“; siehe hierzu auch Kapitel § 2 III. 1. e).

280 Realisiert durch Zuruf von IP-Adressen an den zuständigen ISP, deren Zuordnung zu einem bestimmten Anschluss im Verletzungszeitpunkt Letzterer dann bis zum Abschluss des Auskunftsverfahrens speichern muss.

taugliche Anspruchsgrundlage besteht, zweitens ein solcher Anspruch europarechtlich und/oder grundgesetzlich geboten ist und drittens Argumente aus einfachem Bundesrecht einen solchen Anspruch (im Rahmen der Anspruchsgrundlage) begründen können.[281]

1. Taugliche Anspruchsgrundlage

Die Störerhaftung aus § 1004 BGB analog scheidet als Anspruchsgrundlage aus. Zunächst ist schon unklar, ob ISPs überhaupt für urheberrechtsverletzendes *filesharing* eines oder mehrerer ihrer Kunden als Störer in Anspruch genommen werden können. In der deutschen und europäischen Betrachtung hat sich die Diskussion mehr auf Netzsperren fokussiert.[282] Im internationalen Vergleich wäre die Verantwortlichkeit eines ISPs für die *filesharing*-Aktivitäten seiner Kunden kein *novum*.[283] Diese Frage kann jedoch im Rahmen des Umfangs dieser Arbeit nicht geklärt werden. Ohnehin könnte eine Störerhaftung als Rechtsfolge lediglich einen Unterlassungsanspruch dahingehend auslösen, dass der ISP zukünftige Verletzungen des jeweils streitgegenständlichen, urheberrechtlich geschützten Werkes durch seine Kunden verhindern muss. Mit dem Sicherungsanspruch wird jedoch ein Beitrag zur Aufklärung der Identität des jeweiligen Kunden begehrt, mithin keine Unterlassung der Rechtsverletzung.[284]

Einzig taugliche Anspruchsgrundlage ist § 101 Abs.2 UrhG iVm § 241 Abs.2 BGB, also eine Nebenpflicht des gesetzlichen Schuldverhältnisses, das aus § 101 Abs.2 UrhG entsteht. Die §§ 241ff. BGB enthalten keine Begrenzung auf bestimmte Schuldverhältnisse, weshalb sie grundsätzlich auch auf durch Gesetz entstandene Ansprüche anwendbar sind.[285] Der gesetzliche Auskunftsanspruch des § 101 Abs.2 UrhG regelt nichts gegenteiliges, folglich lässt auch

[281] Ein europarechtliches oder grundsätzliches Gebot kann eine zivilrechtliche Anspruchsgrundlage nicht ersetzen, sondern nur die Auslegung einer grundsätzlich tauglichen Anspruchsgrundlage determinieren. Bestünde zwar ein europarechtliches oder grundgesetzliches Gebot eines Sicherungsanspruches, jedoch keine taugliche Anspruchsgrundlage, so müsste der Gesetzgeber eine solche schaffen.

[282] Siehe hierzu Kapitel § 4 VIII. 10. a).

[283] Siehe Kapitel § 3 XII. 3. d) und 6.

[284] Daher unzutreffend OLG Hamburg, Urteil vom 17. Februar 2010, Az. 5 U 60/09, Rz. 34 – juris.

[285] *Sutschet* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 241 BGB, Rz. 5.

er ein gesetzliches Schuldverhältnis mit Nebenpflichten entstehen.[286]

Unbegründet ist hingegen der Einwand, ein solcher Anspruch aus dem gesetzlichen Schuldverhältnis sei dem Grunde nach ausgeschlossen, weil der mutmaßliche Rechtsverletzer, den betreffend die Sicherung stattfinden soll, zum Zeitpunkt der Sicherung noch nicht hinreichend konkretisiert ist.[287] Unklar ist schon, woraus sich dieser Einwand überhaupt ableiten soll. Ziel des Sicherungsanspruches ist es zudem ja gerade, einen Anspruch zu sichern, der die Konkretisierung, also die Identifizierung des mutmaßlichen Rechteverletzers erst ermöglicht. Unzutreffend ist weiterhin, dass die Gewährung eines Sicherungsanspruches das Erfordernis der Gestattungsanordnung des § 101 Abs.9 UrhG umgehen würde. Denn die Gestattungsanordnung soll nur verhindern, dass ISPs freiwillig, also ohne richterliche Entscheidung, einen ihrer Kunden identifizieren. Der Sicherungsanspruch identifiziert jedoch den betroffenen Kunden dem Anspruchssteller gegenüber nicht.

§ 101 Abs.2 UrhG iVm § 241 Abs.2 BGB ist daher dem Grunde nach eine taugliche Anspruchsgrundlage für den Sicherungsanspruch.[288] Ob jedoch die „*Rücksicht auf die Rechte, Rechtsgüter und Interessen*“ (§ 241 Abs.2 BGB) des Rechteinhabers es erfordert, dass als Nebenpflicht des Auskunftsanspruchs ein Anspruch auf Sicherung desselben besteht, lässt sich wegen des offenen, generalklauselartigen Wortlauts des § 241 Abs.2 BGB nur im Zusammenhang der Gesamtrechtsordnung beurteilen. Erforderlich ist also eine grundrechts- und richtlinienkonforme sowie eine systematische Auslegung des § 241 Abs.2 BGB an Hand einfachen Bundesrechts.

2. Europarechtliches und/oder grundgesetzliches Gebot

a) Europäische und deutsche Grundrechte

Zunächst erscheint es überzeugend, die Rechtfertigung eines Sicherungsanspruches an den Auskunftsanspruch zu koppeln. Ein zivilrechtlicher Sicherungsanspruch hätte ohne einen zivilrechtlichen Auskunftsanspruch keine

[286] LG Hamburg, Urteil vom 11. März 2009, Az. 308 O 75/09, Rz. 24 – juris.

[287] So aber OLG Hamm, Beschluss vom 2. Dezember 2010, Az. I-4 W 119/10 – MMR 2011, 193; OLG München, Beschluss vom 21. November 2011, Az. 29 W 1939/11 – MMR 2012, 764.

[288] aA *Sandor*, Datenspeicherung und urheberrechtliche Durchsetzungsansprüche, S. 236ff.; *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 222f.

sinnvolle Funktion.

Es ist also zu fragen, ob die Grundrechte einen zivilrechtlichen Auskunftsanspruch gebieten. Wäre dies der Fall, wäre es auch naheliegend, dass ein Sicherungsanspruch grundrechtlich geboten ist.

Bezüglich dieser Frage kann eine Abwägung kein zwingendes Ergebnis liefern: denkbar wären zwischen der Variante *kein Recht auf Auskunft* und der Variante *zivilrechtlicher Auskunftsanspruch ohne jegliche Verfahrensgarantien zu Gunsten desjenigen, der Auskunft erteilen muss und desjenigen, über den Auskunft erteilt wird* viele Zwischenstufen, die eine Balance zwischen den betroffenen Grundrechten – (geistigem) Eigentum[289] auf der einen, Schutz der Privatsphäre/des Fernmeldegeheimnisses[290] auf der anderen Seite – gewährleisten. Folglich überzeugt es methodisch am meisten, von den einschlägigen Präjudizien zu der Gebotenheit eines Auskunftsanspruchs auf die Gebotenheit eines Sicherungsanspruches zu schließen.

Dabei ergibt sich, dass sowohl der EuGH (in der Entscheidung „Promusicae“) als auch das BVerfG befunden haben[291], dass die Grundrechte einen zivilrechtlichen Auskunftsanspruch nicht gebieten. Mithin ist auch ein zivilrechtlicher Sicherungsanspruch grundrechtlich nicht geboten.

b) EnforcementRL, VorratsdatenspeicherungsRL und E-DatenschutzRL

Im nächsten Schritt ist zu fragen, ob die europäischen Richtlinien einen zivilrechtlichen Sicherungsanspruch gebieten. In „Promusicae“ hatte der EuGH entschieden, dass nicht nur nach Abwägung der Grundrechte kein zivilrechtlicher Auskunftsanspruch geboten ist, sondern – in Übertragung dieser Abwägung auf Art. 8 EnforcementRL – sich auch aus der EnforcementRL kein solches Gebot ergibt; stattdessen können die Mitgliedstaaten frei entscheiden, ob sie einen Auskunftsanspruch etablieren oder nicht.[292] Hieraus könnte man ableiten, dass es mithin auch dem Recht des jeweiligen Mitgliedstaates

[289] Art. 1 1.EMRK-ZProt, 7, Art. 17 Abs.2 GRC, Art. 14 GG.

[290] Art. 8 EMRK, Art. 7 GRC, Art. 10 GG.

[291] EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 65, 70 – ECLI:EU:C:2008:54 - „Promusicae“; BVerfG, Beschluss vom 17. Februar 2011, Az. 1 BvR 3050/10, Rz. 6ff. – bverfg.de.

[292] Siehe Kapitel § 2 III. 1. a).

überlassen ist, ob er einen zivilrechtlichen Sicherungsanspruch gewährt oder nicht.

Dieser Schluss ist jedoch nicht zwingend. Stattdessen liegt es nahe, dass europäisches Sekundärrecht einen zivilrechtlichen Sicherungsanspruch nach Maßgabe des BGH nicht nur nicht gebietet, sondern einen Sicherungsanspruch ohne mitgliedstaatlich ausdrücklich normierte Regelung sogar verbietet! Die EnforcementRL existiert nämlich nicht in einem Vakuum, sondern muss in ihren systematischen Beziehungen zur (mittlerweile für ungültig erklärten) VorratsdatenspeicherungsRL[293] und zur E-DatenschutzRL gelesen werden.

Die VorratsdatenspeicherungsRL und die E-DatenschutzRL betrafen bzw. betreffen die Rechte und Pflichten der Anbieter und Betreiber öffentlich zugänglicher Kommunikationsnetze, insbesondere also ISPs.[294]

In der Rechtssache „Bonnier“[295] musste sich der EuGH mit der Vorlagefrage befassen, ob die VorratsdatenspeicherungsRL den Art. 8 EnforcementRL modifiziert, ob eine Auskunft also gegebenenfalls nur unter den strengeren Voraussetzungen der VorratsdatenspeicherungsRL gewährt werden darf.[296] Der EuGH beantwortete die Frage richtigerweise mit Verweis auf die recht eindeutigen Verweisungen in den Richtlinien: Nach Art. 11 VorratsdatenspeicherungsRL gilt Art. 15 E-DatenschutzRL (der eine Klausel für die Mitgliedstaaten enthält, wie sie bestimmte Regeln der E-DatenschutzRL modifizeren dürfen) nicht für Daten im Anwendungsbereich der VorratsdatenspeicherungsRL; nach Erwägungsgrund 12 der VorratsdatenspeicherungsRL gilt Art. 15 E-DatenschutzRL stattdessen für alle sonstigen Daten, die nicht von der VorratsdatenspeicherungsRL betroffen sind.[297]

Zusätzlich besagt Erwägungsgrund 15 der EnforcementRL, dass Letztere die Richtlinie 95/46/EG (DatenschutzRL) unberührt lässt. Die E-DatenschutzRL ist gemäß ihres Art. 1 Abs.2 als Ergänzung zur DatenschutzRL zu verstehen. Mithin ist Erwägungsgrund 15 der EnforcementRL auch als mittelbarer Verweis auf die E-DatenschutzRL zu verstehen.

[293] Siehe hierzu Kapitel § 2 III. 1. e).
[294] Art. 1 Abs.1 VorratsdatenspeicherungsRL, Art. 3 Abs.1 E-DatenschutzRL.
[295] EuGH, Urteil vom 19. April 2012, Rs. C-461/10 – ECLI:EU:C:2012:219 - „Bonnier“.
[296] EuGH, Urteil vom 19. April 2012, Rs. C-461/10, Rz. 36 – ECLI:EU:C:2012:219 - „Bonnier“.
[297] EuGH, Urteil vom 19. April 2012, Rs. C-461/10, Rz. 41f. – ECLI:EU:C:2012:219 - „Bonnier“.

Zusammengefasst bedeutet das soeben Gesagte: Während die VorratsdatenspeicherungsRL *lex specialis* zur E-DatenschutzRL war, soweit es um die Datenspeicherung zu den in der VorratsdatenspeicherungsRL genannten Zwecken ging, ist die EnforcementRL kein (!) *lex specialis* zur E-DatenschutzRL, soweit es um die Datenspeicherung zu Zwecken der Rechtsverfolgung im Sinne der EnforcementRL geht. Aus der Ungültigerklärung der VorratsdatenspeicherungsRL durch den EuGH[298] lässt sich nichts gegenteiliges ableiten, da nicht erkennbar ist, dass diese etwas in den systematischen Beziehungen zwischen der E-DatenschutzRL und der EnforcementRL ändern sollte.

Die Zulässigkeit der Speicherung von Daten außerhalb des Anwendungsbereiches der VorratsdatenspeicherungsRL beurteilt sich mithin *allein* nach der E-DatenschutzRL. Umgekehrt muss mithin auch die Etablierung eines Sicherungs*anspruches* vereinbar mit der E-DatenschutzRL sein.

Folglich sind teleologische und systematische Überlegungen betreffend der Sicherung, die isoliert aus der EnforcementRL gewonnen werden, unzulässig. Für sich betrachtet mag es beispielsweise zweckmäßig sein, aus Art. 8 EnforcementRL *a fortiori* auch das Recht eines Mitgliedstaates abzuleiten, einen Sicherungsanspruch festzulegen, mit der Begründung, dass ein Auskunftsanspruch ohne Sicherung desselben wertlos ist. Auch könnte man – in systematischer Hinsicht – auf Art. 7 Abs.1 Satz 1 EnforcementRL verweisen, demgemäß die Mitgliedstaaten Maßnahmen zur Sicherung der rechtserheblichen Beweismittel hinsichtlich der behaupteten Verletzung zur Verfügung stellen können.[299] Jedoch ist diese isolierte Anschauung der EnforcementRL eben unzulässig.

Betrachtet man nun die E-DatenschutzRL, ergibt sich folgendes: Art. 6 E-DatenschutzRL betrifft die Speicherung von Verkehrsdaten, mithin IP-Adressen.[300] Art. 6 E-DatenschutzRL erlaubt die Speicherung (in datenschutzrechtlicher Terminologie: „*Verarbeitung*“[301]) von Verkehrsdaten in bestimmten Fällen für einen gewissen Zeitraum. Die Speicherung zum Zwe-

[298] Siehe hierzu Kapitel § 2 III. 1. e).

[299] Zwar scheint Art. 7 Abs.1 Satz 2 EnforcementRL darauf hinzuweisen, dass es um Maßnahmen der Beweissicherung spezifisch gegen den Verletzer geht, jedoch regelt Satz 2 nur Beispielsfälle, während hingegen Satz 1 allgemein gehalten ist und eine solche Beschränkung nicht aufweist.

[300] Siehe Kapitel § 2 III. 1. a).

[301] Siehe Kapitel § 2 III. 1. e).

cke der Verfolgung von Urheberrechtsverletzungen ist dort nicht aufgeführt. Nach Art. 15 Abs.1 Satz 2 E-DatenschutzRL dürfen die Mitgliedstaaten jedoch durch Rechtsvorschriften vorsehen, dass Verkehrsdaten zu den in Satz 1 genannten Zwecken für eine begrenzte Zeit aufbewahrt werden müssen. Satz 1 enthält die Verfolgung von Urheberrechtsverletzungen nicht ausdrücklich. Insbesondere passen offensichtlich die Ausnahmen der öffentlichen Sicherheit, der Landesverteidigung usw. nicht auf das *filesharing*.[302] Im Ergebnis kann dem EuGH jedoch darin beigepflichtet werden, dass Art. 15 Datenschutz-RL über Art. 13 Abs.1 lit. g) DatenschutzRL den Schutz des Urheberrechts inkorporiert. Unzutreffend ist allerdings, dass Art. 15 Abs.1 Satz 1 DatenschutzRL eine voraussetzungslose Verweisung auf Art. 13 DatenschutzRL enthalte.[303] Stattdessen ist die Verweisung auf Art. 13 DatenschutzRL dem Wortlaut nach eine mit den anderen Tatbeständen kumulative Voraussetzung („*[...] sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für [...] in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.*“). Dogmatisch lässt sich jedoch dasselbe Ergebnis erzeugen, wenn man das Tatbestandsmerkmal „*unzulässiger Gebrauch von elektronischen Kommunikationssystemen*“ als Generalklausel liest, über die Tatbestände des Art. 13 Abs.1 DatenschutzRL umgekehrt in Art. 15 Abs.1 E-DatenschutzRL hineingelesen werden können, was insbesondere deswegen Sinn macht, da Art. 13 E-DatenschutzRL und Art. 15 Abs.1 E-DatenschutzRL zahlreiche identische Ausnahmetatbestände enthalten, die gesetzgeberische Verweisung von letzterer auf erstere Vorschrift also eine Synchronisation zwischen den beiden Richtlinien herstellen soll.

Im Ergebnis jedenfalls erlaubt – sowohl nach der Lösung des EuGH als auch nach der hier alternativ vorgeschlagenen Lösung – die E-Datenschutzrichtlinie über Art. 15 Abs.1 einen Speicheranspruch wegen Urheberrechtsverletzungen. Weiterhin lässt sich in systematischer Betrachtung zu Art. 7 Abs.1 EnforcementRL auch vertreten, dass ein solcher

[302] EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 51ff. – ECLI:EU:C:2008:54 - „Promusicae“.

[303] So jedoch EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 53 – ECLI:EU:C:2008:54 - „Promusicae“.

Anspruch sogar europarechtlich vorgeschrieben ist.[304] Allerdings legt Art. 15 Abs.1 E-DatenschutzRL weitere Voraussetzungen fest, denn eine nach dieser Norm erlaubte Speicherung darf erstens nur mittels „*Rechtsvorschrift*“ (Art. 15 Abs.1 Satz 1 E-DatenschutzRL) und zweitens nur für „*eine begrenzte Zeit*“ (Art. 15 Abs.1 Satz 2 E-DatenschutzRL) ermöglicht werden. Hinsichtlich ersterer Voraussetzung zeigt schon der Sprachvergleich mit der englischen Fassung der Richtlinie („*legislative measures*“), dass eine Rechtsvorschrift durch ein normsetzendes Organ erlassen werden muss, mithin eine richtlinienorientierte Auslegung einer Generalklausel (§ 241 Abs.2 BGB) – wie vorliegend – nicht genügt[305]. Hinsichtlich letzterer Voraussetzung existieren keine Anhaltspunkte in der Richtlinie, welcher Zeitraum genau zulässig sein kann; jedenfalls muss der Zeitraum definiert sein („*begrenzt*“) und darf daher zeitlich nicht unbestimmt, also zum Beispiel für die Dauer des Auskunftsgestattungsverfahrens (so jedoch der BGH[306]), definiert werden.[307]

Im Ergebnis stehen Art. 6, 15 E-DatenschutzRL also einer Auslegung entgegen, die § 241 Abs.2 iVm § 101 Abs.2 UrhG einen Sicherungsanspruch entnimmt.[308] Ein solcher Anspruch müsste stattdessen durch den Bundesgesetzgeber ausdrücklich normiert werden.

[304] Dies widerspricht nicht dem oben dargestellten Verhältnis der beiden Richtlinien zueinander, da die E-DatenschutzRL – wie erarbeitet – insofern keine der EnforcementRL entgegenstehende Regelung trifft, mithin die EnforcementRL etwas zwingend vorschreiben kann, was nach der E-DatenschutzRL lediglich erlaubt ist.

[305] OGH Österreich, Urteil vom 14. Juli 2009, Az. 4 Ob 41/09x – GRUR Int. 2010, 345.

[306] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 59 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[307] Vgl. OGH Österreich, Urteil vom 14. Juli 2009, Az. 4 Ob 41/09x – GRUR Int. 2010, 345.

[308] Im Übrigen ist noch darauf hinzuweisen, dass wegen Art. 95 DS-GVO, der statuiert, dass die DS-GVO den Telekommunikationsdienstleistern keine weitergehenden Pflichten als die E-DatenschutzRL auferlegt, sich unter der Geltung der DS-GVO nichts an der soeben dargestellten Rechtslage ändert.

3. Argumente aus einfach-gesetzlichem Bundesrecht und der Rechtsprechung des BVerfG

a) Argumente aus einfach-gesetzlichem Bundesrecht

Selbst jedoch wenn man die Richtlinien hinwegdenkt und nur das einfach-gesetzliche Bundesrecht betrachtet, erscheint die Etablierung eines Sicherungsanspruches im Rahmen von § 241 Abs.2 BGB nach gegenwärtiger Rechtslage unvertretbar.

Zunächst wäre es zirkelschlüssig, die Existenz des Auskunftsanspruches als Letztbegründung für die Existenz des Sicherungsanspruches heranzuziehen. Denn die Existenz des Auskunftsanspruches ist bereits notwendige Bedingung für einen Sicherungsanspruch, da Letzterer wenn dann nur als Nebenpflicht in das gesetzliche Schuldverhältnis, das dem Auksunftsanspruch entspringt[309], hineingelesen werden kann. Folglich ist es, nur die ausdrücklich normierte Existenz des Auskunftsanspruches und die fehlende ausdrücklich normierte Existenz eines Sicherungsanspruches betrachtet, in gleichem Maße plausibel, einen Sicherungsanspruch *a fortiori* anzunehmen wie einen Sicherungsanspruch *e contrario* abzulehnen.

Mithin muss auf Grund weiterer Argumente eine der beiden Entscheidungsalternativen plausibler erscheinen. In der systematischen Betrachtung ist zunächst festzuhalten, dass ein *lex specialis*-Verhältnis zwischen Vorratsdatenspeicherung im eigentlichen Sinne[310] und Speicherung aus sonstigen Gründen im deutschen – anders als im europäischen – Recht nicht existiert: die gegenwärtigen Regelungen der Vorratsdatenspeicherung im deutschen Recht auf Grund des „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ setzen, anders die Vorgängerregelungen des „Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ keine EU-Richtlinie um.[311]

Mithin lässt sich aus den §§ 113bff. TKG ableiten, dass der Gesetzgeber dort nur diejenigen Auskunftsbegehren als zulässig erachtet, die auf Verkehrsdaten gerichtet sind, die auf Grund einer gesetzlichen *Pflicht* gespeichert

[309] Siehe oben Kapitel § 4 V. 1.
[310] Siehe hierzu Kapitel § 2 III. 1. e).
[311] Zur Geschichte der Vorratsdatenspeicherung siehe Kapitel § 2 III. 1. e).

wurden; mithin also nur die in § 113c TKG normierten Auskunftsbegehren, zu denen das Auskunftsbegehren nach § 101 Abs.2, 9 UrhG nicht gehört.[312] Folglich kann Letzteres nur auf Verkehrsdaten gerichtet werden, die ein ISP freiwillig gespeichert hat.[313] Damit scheidet ein Sicherungsanspruch der Rechteinhaber aus.

Diese systematische Betrachtung wird gestützt durch den Umstand, dass im Gesetzgebungsverfahren zum „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ der Rechtsausschuss des Bundesrates vorgeschlagen hatte, die Anwendung der Vorratsdatenspeicherung auch auf das geistige Eigentum zu erstrecken, da die dies betreffenden Gesetze keinen Sicherungsanspruch vorsähen.[314] Der Bundesrat sah jedoch keinen Änderungsbedarf und rief den Vermittlungsausschuss nicht an.[315] Bei der Neuregelung der Vorratsdatenspeicherung im Jahr 2015 musste dem Gesetzgeber der Regelungsbedarf bewusst gewesen sein. Jedoch wurde das Verhältnis der Vorratsdatenspeicherung zum geistigen Eigentum nicht erörtert.[316] Daraus lässt sich folgern, dass die Vorratsdatenspeicherung das geistige Eigentum nicht betreffen sollte, mithin für Letzteres keine Sicherungspflichten oder – aus zivilrechtlicher Perspektive – Sicherungsansprüche bestehen.

Zuletzt ist zudem anzumerken, dass im deutschen Recht ausdrückliche Regelungen existieren, wie und in welchem Umfang außerhalb eines gerichtlichen Verfahrens, das die Rechtsfolgen einer Verletzung eines Rechts des geistigen Eigentums selbst zum Gegenstand hat, Beweise gesichert werden können, namentlich insbesondere das selbstständige Beweisverfahren nach den §§ 485ff. ZPO sowie die Besichtigungsansprüche nach §§ 809f. BGB, § 101a UrhG

[312] So auch OLG Frankfurt a.M., Beschluss vom 12. Novmeber 2009, Az. 11 W 41/09 – MMR 2010, 62; jedoch war zum Zeitpunkt dieser Entscheidung jene Ableitung noch unzulässig, da das damalige Gesetz die VorratsdatenspeicherungsRL umsetzte, aus der – wegen ihrer Natur als *lex specialis*-Regelung – keine Umkehrschlüsse für andere Bereiche getroffen werden konnten. Auch in der Literatur wird dieser Punkt übersehen, vgl. beispielsweise *Sandor*, Datenspeicherung und urheberrechtliche Durchsetzungsansprüche, S. 239f.

[313] Zu den Rechten der ISPs auf freiwillige Speicherung siehe Kapitel § 2 III. 1. e).

[314] BR-Drs. 798/1/07.

[315] BR-Drs. 798/07.

[316] Vgl. BT-Drs. 18/5088.

etc.[317] Es erscheint daher systematisch betrachtet naheliegender, dass es dem Gesetzgeber überlassen ist, zusätzliche Beweissicherungsregeln zu schaffen, anstatt diese aus teleologischen Erwägungen in Generalklauseln hineinzulesen.

Folglich ist – auch die einschlägigen Richtlinien hinweggedacht und nur das einfach-gesetzliche Bundesrecht betrachtet – die Etablierung eines nicht ausdrücklich normierten Sicherungsanspruches gegenwärtig unvertretbar.

b) Argumente aus der Rechtsprechung des BVerfG

Zuletzt könnte auch die neuere Rechtsprechung des BVerfG nahelegen, dass ein Sicherungsanspruch im Lichte des grundrechtlichen Gesetzesvorbehalts ausdrücklich normiert sein muss, mithin eine Ableitung eines solchen Anspruchs aus § 241 Abs.2 BGB nicht zulässig ist. Dieser Rechtsprechung zu Folge war es nicht verfassungswidrig, einem Email-Provider ein Ordnungsgeld aufzuerlegen, weil dieser sich gegen eine Anordnung auf Herausgabe der IP-Adresse des Nutzers eines seiner Email-Accounts mit der Begründung stellte, dass er IP-Adressen seiner Nutzer gar nicht erhebe.[318] Dem Provider zu Folge läge eine Verletzung von Art. 12 GG vor, da die entsprechende Anordnung ohne einfachgesetzliche Grundlage ergangen sei.[319] Letztlich wurde im Kern darum gestritten, ob angesichts der technischen Ausgestaltung des Dienstes, nach der (zumindest laut den Feststellungen der Instanzgerichte) theoretisch ein Zugriff auf die IP-Adressen der Nutzer möglich ist, der Provider diese jedoch vor seinen internen Systemen verbirgt, der Provider die IP-Adressen im Sinne der Telekommunikations-Überwachungsverordnung „vorhält“ oder nicht.[320]

Damit lässt sich aus der Entscheidung des BVerfG ableiten, dass dem grund-

[317] Die auch außerhalb eines streitigen Verfahrens im Wege der einstweiligen Verfügung – also wie die Gestattungsverfügung nach § 101 Abs.9 UrhG außerhalb eines Hauptsacheverfahrens – durchgesetzt werden können, siehe *Gehrlein* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 809 BGB, Rz. 7. Der Gesetzgeber hat also das Bedürfnis der einem Hauptsacheverfahren vorgelagerten Beweissicherung berücksichtigt.

[318] BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018, Az. 2 BvR 2377/16 – bverfg.de.

[319] BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018, Az. 2 BvR 2377/16, Rz. 16 – bverfg.de.

[320] BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018, Az. 2 BvR 2377/16, Rz. 48ff. – bverfg.de.

rechtlichen Gesetzesvorbehalt bei der Speicherung von IP-Adressen im strafrechtlichen Kontext auf Grund des engmaschigen Netzes an Vorschriften aus StPO, TKG und Telekommunikations-Überwachungsverordnung genügt wird.[321] Umgekehrt könnte daraus gefolgert werden, dass ein zivilrechtlicher Anspruch allein auf Grundlage einer Generalklausel wie § 241 Abs.2 BGB dem Gebot des Vorbehalts des Gesetzes nicht genügt.[322] Jedoch räumt das BVerfG den Zivilgerichten große Freiheiten bei der Ableitung von Ansprüchen aus Generalklauseln ein[323], weshalb eine solche Schlussfolgerung keinesfalls zwingend erscheint. Aus verfassungsrechtlicher Perspektive bleibt also offen, ob aus § 241 Abs.2 BGB ein Sicherungsanspruch abgeleitet werden darf oder nicht.

4. Bewertung der BGH-Rechtsprechung

Das Vorgesagte zu Grunde gelegt, erscheint die Rechtsprechung des BGH zum Sicherungsanspruch[324] mangelhaft.[325] Als Anspruchsgrundlage sieht der BGH richtigerweise § 101 Abs.2 UrhG iVm § 241 Abs.2 BGB an.[326] Die Begründung für das Bestehen des Anspruches geht jedoch fehl:

Sein Verweis auf die Rechtsprechung des EuGH, dergemäß die E-DatenschutzRL einem zivilrechtlichen Auskunftsanspruch als Umsetzung des Art. 8 EnforcementRL nicht entgegensteht[327] ist insoweit nicht einschlägig, da es nicht um die Auskunft, sondern die Sicherung geht. Gleiches gilt für die Erörterung der Entscheidung des EuGH die Vorratsdatenspeicherungs-RL betreffend[328], da diese Richtlinie – als *lex specialis* für einen anderen Sachbereich – keine Rolle für die Sicherung zum Zwecke der Durchsetzung

[321] Vgl. BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018, Az. 2 BvR 2377/16, Rz. 45ff. – bverfg.de.

[322] Vgl. *Habel/Briske*, „Speichern auf Zuruf“ verfassungsrechtlich abgesegnet.

[323] Vgl. BVerfG, Beschluss vom 24. Februar 2015, Az. 1 BvR 472/14, Rz. 39ff. – bverfg.de

[324] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[325] aA ohne Begründung *Maaßen*, GRUR-Prax 2017, 565, 565.

[326] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 33 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[327] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 64 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[328] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 65 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

geistigen Eigentums spielt.[329]

Kernargument des BGH ist im Ergebnis eine an der EnforcementRL orientierte teleologische Überlegung (*Auskunft macht ohne Sicherung keinen Sinn*)[330], die jedoch – wie aufgezeigt – in Wirklichkeit fehlplatziert ist und stattdessen einer systematischen Betrachtung weichen müsste.

Wünschenswert wäre es gewesen, wenn der BGH zumindest dem EuGH vorgelegt hätte. Gegenstand der Vorlage hätte die Frage sein müssen, ob die Art. 6 und 15 E-DatenschutzRL und Art. 8 EnforcementRL dahingehend auszulegen sind, dass sie eine mitgliedstaatliche, nicht ausdrücklich normierte Regelung erlauben, derzufolge Rechteinhabern ein Anspruch auf Sicherung von Verkehrsdaten zugesprochen wird, die später Gegenstand eines Auskunftsverfahrens eine Urheberrechtsverletzung betreffend sind. Dies wäre auch im Sinne der Rechtssicherheit für alle Beteiligten angebracht gewesen. Es erscheint fragwürdig, eine Rechtsprechung zu etablieren, die Jahre später möglicherweise auf Grund einer Vorlage aus einem anderen Mitgliedstaates gekippt wird.

Dies zeigt sich im Vergleich hierzu aktuell auf dem Gebiet der Verantwortlichkeit von Sharehostern: dort hat der BGH strenge Prüfpflichten im Rahmen der Störerhaftung statuiert, dennoch aber auf eine Vorlage an den EuGH verzichtet[331]; die Vereinbarkeit dieser Rechtsprechung mit der ECommerceRL hätte er jedoch klären müssen, insbesondere, ob seine Anforderungen „*allgemeine Überwachungspflichten*“ darstellen, die nach Art. 15 ECommerceRL verboten wären. Dies wurde Gegenstand einer Vorlage aus Österreich[332], die das Potential dazu hatte, die Sharehoster-Rechtsprechung des BGH unions-

[329] Siehe Kapitel § 4 V. 2. b).

[330] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 59 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“.

[331] Siehe zu den gegenwärtigen Vorlagen betreffend die Haftung von *YouTube* und *uploaded* bei *Soppe*, Wann und wie haften Sharehosting-Dienste?

[332] OGH Österreich, Beschluss vom 25. Oktober 2017, Az. 6 Ob 116/17b – MMR 2018, 145.

rechtswidrig zu machen.[333] Vielleicht auch deshalb hat der BGH mittlerweile Fragen zur Haftung Sharehostern und anderen Speicherdiensten, konkret dem Sharehoster *uploaded* sowie der Videoplattform *YouTube*, dem EuGH vorgelegt.[334]

VI. Zu den Kosten der Sicherung des Auskunftsanspruches und des Auskunftsverfahrens

Betreffend die Kosten der Sicherung des Auskunftsanspruches und des Auskunftsverfahrens gibt es zweierlei zu betrachten, zum einen die Regelungen betreffend die Frage, wer *anfänglich* die Kosten trägt, zum anderen betreffend die Frage, wer *letztlich* die Kosten trägt.

1. Anfängliche Kostentragung

Wie aufgezeigt[335], trägt der Rechteinhaber anfänglich alle Kosten, wobei dies nur bezüglich dem Auskunftsverfahren gesetzlich geregelt ist (§ 101 Abs.2 Satz 3 UrhG). Für die Sicherung des Auskunftsverfahrens fehlt eine entsprechende Regel, wobei die Rechtsprechung einen Anspruch der ISPs auf Kostentragung durch die Rechteinhaber mittelbar dadurch anerkennt[336], dass sie die dies betreffend (wohl freiwillig) geleisteten Zahlungen der Rechteinhaber an die ISPs als notwendige Kosten der Rechtsverfolgung im Sinne des § 91 Abs.1 Satz 1 ZPO ansieht, was nur dann möglich ist, wenn die Rechteinhaber diese Kosten den ISPs nicht freiwillig erstatten. Dogmatisch ließe sich ein entsprechender Anspruch der ISPs – wie auch der Anspruch auf Sicherung selbst – aus dem gesetzlichen Schuldverhältnis, das aus § 101 Abs.2 UrhG entsteht, herleiten: wenn der Rechteinhaber schon die durch Auskunftserteilung veranlassten Kosten erstatten muss (§ 101 Abs.2 Satz 3 UrhG), muss er *a fortiori* auch die Kosten tragen, die durch die Sicherung der Auskunftser-

[333] *Holznagel*, ZUM 2018, 350, 352f. Diese Bedenken dürften sich nach der Entscheidung des EuGH nunmehr wohl zerstreut haben, da ein Vergleich der vom EuGH gebilligten Handlungspflichten mit den vom BGH aufgestellten Kongruenz vermuten lässt, vgl. EuGH, Urteil vom 3. Oktober 2019, Rs. C-18/18, Rz. 41 und 45 – ECLI:EU:C:2019:821 - „Glawischnig-Piesczek“ mit BGH, Urteil vom 12. Juli 2012, Az. I ZR 18/11, Rz. 34f. – MMR 2013, 185 - „Alone in the Dark“.

[334] Siehe hierzu *Soppe*, Wann und wie haften Sharehosting-Dienste?

[335] Siehe Kapitel § 2 III. 1. g).

[336] Ohne dies bewusst auszudrücken.

teilung veranlasst sind.[337] Da der Sicherungsanspruch sich dogmatisch nicht überzeugend herleiten lässt, kann allerdings auch ein Anspruch auf Ersatz der Sicherungskosten nicht (dogmatisch überzeugend) hergeleitet werden.

Die gesetzliche Regelungen die Kostentragung betreffend (§ 101 Abs.2 Satz 3 und Abs.9 Satz 5 UrhG) überzeugen: anfänglich sollte immer derjenige die Kosten tragen, die durch sein Verhalten veranlasst werden. Da die Rechteinhaber also das Auskunftsverfahren und – soweit ISPs nicht ohnehin schon freiwillig die Zuordnung von IP-Adressen zu einem bestimmten Anschluss für eine bestimmte Zeit speichern – seine Sicherung veranlassen, ist es richtig, wenn sie für die hierdurch veranlassten Kosten aufkommen.

2. Letztliche Kostentragung

Nach § 91 Abs. Satz 1 ZPO hat die unterliegende Partei die Kosten des Rechtsstreits zu tragen, insbesondere die dem Gegner erwachsenen Kosten zu erstatten, soweit sie zur zweckentsprechenden Rechtsverfolgung oder Rechtsverteidigung notwendig waren. Das Erfordernis der „Notwendigkeit“ drückt aus, dass die Kosten einen *konkreten* Bezug zum jeweiligen Prozess aufweisen müssen; insbesondere soll dadurch verhindert werden, dass die obsiegende Prozesspartei versucht, ihre allgemeinen Kosten der unterliegenden Prozesspartei aufzubürden.[338] Da in § 91 ZPO nur bezüglich einzelner, denkbarer Posten geregelt ist, ob und in welchem Umfang diese notwendig sind, hat es der Gesetzgeber im Umkehrschluss der Rechtsprechung überlassen, Fallgruppen der Notwendigkeit auszubilden.[339]

Die Urteile des BGH über die Kosten des Auskunftsverfahrens als notwendige Kosten des Rechtsstreits müssen also grundsätzlich danach bewertet werden, wie sie sich in die vorhandenen Präjudizien einfügen. Dies tun sie nahtlos: es ist in ständiger Rechtsprechung anerkannt, dass vorbereitende Handlungen, ohne die eine Klage riskiert, unzulässig oder unbegründet zu sein, notwen-

[337] Soweit aber ISPs ohnehin schon freiwillig sichern (siehe Kapitel § 2 III. 1. e).), hat der Rechteinhaber die hierfür entstandenen Kosten nicht veranlasst, sollte diese also auch nicht tragen müssen.

[338] *Jaspersen* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 91 ZPO, Rz. 93.

[339] § 91 ZPO kann also als – unbewusste oder bewusste – Delegationslücke bezeichnet werden. Zur Methodik der Delegationslücke siehe *Dück*, ZfPW 2018, 76, 85ff.

dige Kosten der Rechtsverfolgung sind.[340] Deswegen sind beispielsweise die Kosten für Testkäufe, mittels derer die etwaig schutzrechtsverletzende Beschaffenheit eines Angebots überprüft wird, notwendige Kosten der Rechtsverletzung, nicht aber die Kosten einer Abmahnung, da eine Klage auch ohne vorhergehende Abmahnung zulässig und begründet ist; die Kosten letzterer können folglich nur mittels eines materiell-rechtlichen Anspruches geltend gemacht werden.[341]

Mithin sind richtigerweise auch die Kosten der Sicherung des Auskunftsanspruches und des Auskunftsverfahrens, die vom Rechteinhaber anfänglich zu tragen waren, notwendige Kosten der Rechtsverfolgung, da ohne die Auskunft schon – mangels einem Äquivalent zu dem US-amerikanischen *John Doe*-Verfahren[342] in der ZPO – keine zulässige Klage eingereicht werden kann.[343] Auch sind richtigerweise die Gebühren eines Rechtsanwalts für die Durchsetzung des Auskunftsanspruchs notwendige Kosten der Rechtsverfolgung, selbst wenn im Unternehmen des Rechteinhabers eine Rechtsabteilung vorhanden ist[344], da ein Rechteinhaber nicht riskieren muss, dass wegen des Betreibens des Auskunftsverfahrens (für das rechtlich nicht zwingend ein Rechtsanwalt notwendig ist) durch einen hierauf nicht spezialisierten Vertreter die spätere Vereitelung einer Klage riskiert wird.

§ 91 Abs.1 Satz 1 ZPO könnte also nur dann keine Anwendung finden, wenn der Gesetzgeber die Anwendbarkeit ausgeschlossen haben sollte. In diesem Punkt widersprechen sich der BGH in seinem Beschluss aus 2014 und die Vorinstanz. Die Gesetzesbegründung zur Umsetzung der EnforcementRL verweist auf Seite 49 betreffend § 101 UrhG auf die Ausführungen zu § 140b PatG. Dort wiederum ist bestimmt, dass vom Verletzer die Kosten der Gestattungsanordnung als Schadensersatz verlangt werden können.[345] Wie in Kapitel § 4 IV. d) dargestellt, ist der „Wille“ des Gesetzgebers unbedingt zu

[340] BGH, Urteil vom 20. Oktober 2005, Az. I ZB 21/05, Rz. 11 – GRUR 2006, 439 - „Geltendmachung der Abmahnkosten“ mit Nachweisen der Rechtsprechung.

[341] BGH, Urteil vom 20. Oktober 2005, Az. I ZB 21/05, Rz. 12 – GRUR 2006, 439 - „Geltendmachung der Abmahnkosten“.

[342] Siehe Kapitel § 3 XII. 6.

[343] Vgl. BGH, Beschluss vom 15. Mai 2014, Az. I ZB 71/13, Rz. 10 – ZUM 2014, 967 - „Deus Ex“.

[344] BGH, Beschluss vom 26. April 2017, Az. I ZB 41/16, Rz. 13 – GRUR 2017, 854 - „Anwaltskosten im Gestattungsverfahren“.

[345] BT-Drs. 16/5048, S. 40.

berücksichtigen. Die Ausführungen in der Gesetzesbegründung sind jedoch derart knapp, dass ein eindeutiger „Wille“ für oder gegen die Anwendbarkeit des § 91 Abs.1 Satz 1 ZPO nicht erkennbar ist. Entsprechend mag der BGH einen Ausschluss der Anwendbarkeit nicht erkennen[346], mithin können die Kosten entweder als materieller Anspruch oder über § 91 Abs.1 Satz 1 ZPO geltend gemacht werden. Die Vorinstanz hingegen liest die Ausführungen des Gesetzgebers als Beschränkung auf den materiellen Anspruch.[347] Aus folgendem Grund ist dem BGH zuzustimmen: wäre der Rechteinhaber auf den materiellen Schadensersatzanspruch verwiesen, könnte er die Kosten des Auskunftsverfahrens nur im Rahmen der Differenzhypothese geltend machen, was ihm aber die gleichzeitige Berechnung des Schadens nach Lizenzanalogie verwehren würde; auf Letztere ist er jedoch in *filesharing*-Konstellationen angewiesen.[348] Praktisch müsste der Rechteinhaber dann auf seine Aufwendungen für das Auskunftsverfahren verzichten (was der Gesetzgeber wohl übersehen hat), obwohl es dem Gesetzgeber – wie es die Formulierungen in der Gesetzesbegründung nahelegen – nur darauf ankam, dass der Verletzer diese Kosten „*im Ergebnis*“[349] trägt. Der dogmatische Weg zu diesem Ergebnis war ihm also offensichtlich egal. Folglich müssen diese Kosten anstatt über einen materiell-rechtlichen Anspruch auch über § 91 Abs.1 Satz 1 ZPO geltend gemacht werden können.

VII. Zur sekundären Darlegungslast

1. Sekundäre Darlegungslast, Anscheinsbeweis oder tatsächliche Vermutung?

a) Einleitung

Trifft den Anschlussinhaber eine sekundäre Darlegungslast oder wird seine Täterschaft vermutet? Oder gilt für Letztere ein Anscheinsbeweis? Über diese Begriffe, ihre Verwendung und Prüfungsreihenfolge besteht Verwirrung. Hierfür ist maßgeblich der BGH verantwortlich. So hatte er 2010 in „Sommer unseres Lebens“ noch geurteilt, aus der Behauptung, über einen Anschluss sei

346 BGH, Beschluss vom 15. Mai 2014, Az. I ZB 71/13, Rz. 10 – ZUM 2014, 967 - „Deus Ex“.

347 OLG Hamburg, Beschluss vom 4. September 2013, Az. 8 W 17/13, Rz. 16 – juris.

348 Siehe Kapitel § 4 IX. 1.

349 BT-Drs. 16/5048, S. 39, 40.

eine Urheberrechtsverletzung mittels *filesharing* erfolgt, folge eine tatsächliche Vermutung der Täterschaft des Anschlussinhabers, aus der sich wiederum für diesen eine sekundäre Darlegungslast ergebe.[350] 2014 urteile er dann in „BearShare“, dass keine tatsächliche Vermutung gelte, wenn zum Zeitpunkt der Rechtsverletzung auch andere Personen den Anschluss nutzen konnten, den Anschlusshaber allerdings eine sekundäre Darlegungslast treffe.[351] Im Jahr 2016 urteilte er schließlich in „Afterlife“, dass die Behauptung, über einen Anschluss sei eine Urheberrechtsverletzung mittels *filesharing* erfolgt, keinen Anscheinsbeweis dahingehend zur Folge habe, dass der Anschlussinhaber auch Täter der Urheberrechtsverletzung sei, Letzteren allerdings eine sekundäre Darlegungslast treffe, deren Nichterfüllung zur „*Annahme*“ (gemeint ist wohl „Vermutung“) seiner Täterschaft führe.[352]

Diese Rechtsprechung veranlasst zu der Frage: Was denn nun? Dabei wäre das Verhältnis der Institute der tatsächlichen Vermutung, des Anscheinsbeweises und der sekundären Darlegungslast unter- und zueinander nicht sonderlich kompliziert. Eine nachvollziehbare dogmatische Festlegung wäre also bereits in „Sommer unseres Lebens“ ohne weiteres möglich gewesen.

Die tatsächliche Vermutung und der Anscheinsbeweis sind im Rahmen der Beweiswürdigung nach § 286 Abs.1 Satz 1 ZPO richterrechtlich entwickelte Institute. Die sekundäre Darlegungslast fußt in der zivilprozessualen Pflicht, sich auf gegnerischen Parteivortrag wahrheitsgemäß zu erklären (§ 138 Abs.1 und Abs.2 ZPO) und ist in ihren jeweiligen Anwendungsbereichen und Anforderungen ebenfalls richterrechtlich präzisiert.

b) Tatsächliche Vermutung und Anscheinsbeweis

Der offene Wortlaut von § 286 Abs.1 Satz 1 ZPO gibt dem Richter eine große Freiheit dahingehend, wann er eine Tatsache als erwiesen ansieht und wann nicht. Der BGH hatte diese Freiheit schon früh auf die überzeugende Formel herunter gebrochen, dass sich ein Richter in der Beweisfrage in Zweifelsfällen mit einem für das praktische Leben brauchbaren Grad an Gewissheit

[350] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[351] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 15f. – GRUR 2014, 657 - „BearShare“.

[352] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 18 – GRUR 2017, 386 - „Afterlife“.

begnügen dürfe, „*der den Zweifel Schweigen gebietet, ohne sie völlig auszuschließen*“.[353] Es ist offensichtlich, dass eine solche Fassung des Rechts der Beweiswürdigung die Bildung typisierter Erfahrungssätze erlaubt.[354] Die tatsächliche Vermutung bedeutet also, dass sich aus dem Feststehen einer Tatsache typisiert Ableitungen für das Feststehen einer anderen Tatsache treffen lassen, wenn ein entsprechender Erfahrungssatz dies gebietet. Welche Reichweite diese Ableitungen haben, wird vom BGH sehr unterschiedlich beurteilt: manchmal leitet er aus dem Feststehen einer bestimmten Tatsache nur ein Indiz für eine andere Tatsache ab; manchmal leitet er aus dem Feststehen einer bestimmten Tatsache nicht nur ein Indiz, sondern eine, dem Anscheinsbeweis gleich wirkende, Regel für das Feststehen einer anderen Tatsache ab; zuletzt leitet er manchmal aus dem Festehen einer bestimmten Tatsache auch ab, dass in Folge zudem eine andere Tatsache positiv feststeht.[355]

Daraus folgt wiederum, dass der Anscheinsbeweis dieser Lesart zu Folge letztlich nur ein Unterfall der tatsächlichen Vermutung ist.[356] Die Voraussetzungen sind dieselben, die Rechtsfolgen wie dargestellt unterschiedlich, und zwar abhängig davon, welche Rechtsfolge (Indiz, Anscheinsbeweis, Umkehr der materiellen Beweislast) der BGH betreffend die zu entscheidende, typisiert vorkommende Sachverhaltskonstellation bevorzugt.

Wenn die Voraussetzungen identisch sind, ist es irrelevant, ob der BGH mit „Sommer unseres Lebens“ aus dem Feststehen einer Urheberrechtsverletzung über einen Internetanschluss eine tatsächliche Vermutung für die Täterschaft des Anschlussinhabers ableiten wollte oder nicht. Denn in „Afterlife“ hat er der Anwendung des Anscheinsbeweises auf diese Fallkonstellation eine Absage erteilt[357] und damit also allen Formen der tatsächlichen Vermutung.

Hierin ist dem BGH zuzustimmen, da ein Anscheinsbeweis und die tatsächli-

353 BGH, Urteil vom 17. Februar 1970, Az. III ZR 139/67, Rz. 72 – juris.

354 *Musielak*, JA 2010, 561, 565; vgl. BGH, Urteil vom 24. Januar 1951, Az. II ZR 23/50, Rz. 24 – juris.

355 Siehe mit umfangreichen Nachweisen der Rechtsprechung des BGH *Laumen*, MDR 2015, 1, 2. Die Ableitung dahingehend, dass aus dem Festehen einer bestimmten Tatsache eine andere Tatsache positiv feststeht, ist *contra legem*, da eine solche Ableitung wie eine Umkehr der materiellen Beweislast wirkt; eine solche Umkehr würde eine gesetzliche Regelung erfordern, vgl. *Laumen*, MDR 2015, 1, 4.

356 *Doukoff*, SVR 2015, 245, 251.

357 BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 18f. – GRUR 2017, 386 - „Afterlife“.

che Vermutung voraussetzen, dass der Kausalverlauf, für den der Anscheinsbeweis bzw. die tatsächliche Vermutung gelten soll, so häufig vorkommen muss, dass die Wahrscheinlichkeit, einen solchen Kausalverlauf in jedem entsprechenden Einzelfall vor sich zu haben, sehr hoch ist.[358] Eine hohe Wahrscheinlichkeit dahingehend, dass der Inhaber eines Internetanschlusses auch Täter einer Urheberrechtsverletzung ist, die über diesen Anschluss begangen wurde, könnte es mithin nur dann geben, wenn Internetanschlüsse in Deutschland statistisch gesehen überwiegend von nur einer Person benutzt würden. Leider begnügt sich der BGH mit dem Argument, dass es eine „*naheliegende Möglichkeit*“ gäbe, dass ein Internetanschluss auch von einer anderen Person als dem Anschlussinhaber benutzt wird.[359] Er hätte sich an dieser Stelle dazu auslassen können, welche Erkenntnismittel für die Annahme eines Anscheinsbeweises bzw. einer tatsächlichen Vermutung heranzuziehen sind. Zunächst wäre anzunehmen, dass über die Annahme oder Nichtannahme nicht im Rahmen der Beweislast entschieden werden kann, denn die aufzustellende Vermutungsregel soll ja über einen jeweils konkret zu entscheidenden Einzelfall hinaus anwendbar sein. Damit wäre unvereinbar, wenn diejenige Partei, der die Vermutungsregel zu Gute kommen soll, deren Geltung (also die hohe Wahrscheinlichkeit für einen bestimmten Kausalverlauf) in dem Einzelfall, der sie betrifft, beweisen müsste. Der Grad an Wahrscheinlichkeit könnte also als offenkundige Tatsache im Sinne von § 291 ZPO zu sehen sein. Der BGH lehnt jedoch die Annahme der Geltung eines Erfahrungssatzes als offenkundige Tatsache ab, da dies eine Umgehung des Erfordernisses eines Sachverständigenbeweises darstellen würde.[360] Konsequent zu Ende gedacht stünde dies freilich im Widerspruch zum Gros der Rechtsprechung des BGH betreffend tatsächlicher Vermutungen, da er solche ohne Not auch ohne Sachverständigenbeweis aufstellt. Diese Überlegung außer Acht gelassen, würde ein Anscheinsbeweis bzw. eine tatsächliche Vermutung betreffend Anschlussinhaber jedenfalls erfordern, dass in einem Verletzungsverfahren in der ersten oder notfalls zweiten Instanz durch einen Sachverständigen begutachtet wird, wie viele Internetanschlüsse (Mobilfunk-

[358] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 19f. – GRUR 2017, 386 - „Afterlife“.

[359] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 20 – GRUR 2017, 386 - „Afterlife“.

[360] BGH, Urteil vom 2. Oktober 2003, Az. I ZR 150/01 – NJW 2004, 1163 - „Marktführerschaft“, betreffend Verkehrsauffassungen.

verbindungen ausgenommen) in Deutschland statistisch betrachtet von nur einer Person verwendet werden. Hätte ein solches Gutachten ergeben, dass dies sehr häufig der Fall ist (beispielsweise über 98 Prozent Alleinnutzer), hätte das jeweilige Instanzgericht dann einen Anscheinsbeweis aufstellen können. Der BGH wiederum hätte diesen anschließend in der Revision billigen können.[361] Die Erkenntnisse des Sachverständigengutachtens aus diesem Verfahren könnten dann über § 291 ZPO als offenkundige Tatsache in anderen Verfahren verwendet werden.

Da ein wie eben geschildertes Vorgehen bisher nicht geschehen ist, hätte der BGH spätestens in „Afterlife“ eigentlich zum Zwecke der weiteren Beweisaufnahme mittels Sachverständigengutachten zurückverweisen müssen, da er ohne ein solches die in Randziffer 20 getätigte Aussage nicht hätte treffen dürfen. Ob ein solches Sachverständigengutachten eine statistisch betrachtet enorm hohe Zahl an Alleinnutzern festgestellt hätte, ist jedoch höchst fraglich.

Jedenfalls im Ergebnis ist damit dem BGH in der Ablehnung eines Anscheinsbeweises bzw. einer tatsächlichen Vermutung für die Täterschaft eines Anschlussinhabers für eine Urheberrechtsverletzung allein auf Grund der Tatsache, dass diese über seinen Anschluss erfolgt ist, zuzustimmen. Zwar existiert kein eindeutig belastbares Zahlenmaterial dahingehend, wie viele Internetanschlüsse in Deutschland von nur einer Person benutzt werden; auf Grund des soeben dargestellten Vorgehens, das dogmatisch erforderlich ist bzw. sein müsste, um einen Anscheinsbeweis aufzustellen, muss dies aber zu Lasten der klagenden Rechteinhaber gehen. Abgesehen davon wird auch von Seiten der Rechteinhaber vorgebracht, dass 70 Prozent der Internetanschlüsse in Deutschland Familienanschlüsse sind und auch bei den restlichen 30 Prozent nicht klar ist, wie viele von diesen Internetanschlüsse ausmachen,

[361] Die Beweiswürdigung ist zwar grundsätzlich Aufgabe des Tatrichters, jedoch ist der Prozess der Würdigung (beispielsweise deren Vollständigkeit und Widerspruchsfreiheit) einer rechtlichen Überprüfung zugänglich, siehe BGH, Urteil vom 14. Januar 1993, Az. IX ZR 238/91, Rz. 16 – juris. Das ist überzeugend, da § 286 ZPO seinem Wortlaut nach keine dahingehende Einschränkung enthält und somit dessen Anwendung – wie die Anwendung anderer Rechtsnormen auch – im Wege der Revision überprüfbar sein muss.

die von nur einer Person genutzt werden.[362]

In der Folge kann sich aus der Feststellung, dass über einen Internetanschluss eine Urheberrechtsverletzung begangen wurde, nur eine sekundäre Darlegungslast des Anschlussinhabers ergeben.[363] Für einen Anscheinsbeweis ist dann nur noch Raum, wenn die sekundäre Darlegungslast nicht erfüllt werden kann.[364]

c) Sekundäre Darlegungslast

§ 138 Abs.1 und Abs.2 ZPO statuieren die Pflicht, sich über die Tatsachen, die eine Partei vorträgt, wahrheitsgemäß zu erklären. Nach § 138 Abs.3 ZPO gelten nicht bestrittene Tatsachen als zugestanden. Was „*zu erklären*“ in § 138 Abs.2 ZPO genau bedeutet, lässt sich dem Wortlaut nicht entnehmen. Aus zivilprozessualen Grundsätzen wie dem Beibringungsgrundsatz[365] sowie dem (grundsätzlichen) Verbot des Ausforschungsbeweises bzw. des Beweismittelantrages[366] ließe sich ableiten, dass als „Erklärung“ ein einfaches Bestreiten genügt, da eine Partei einer anderen Partei – anders als in anderen Rechtsordnungen, die beispielsweise ein *discovery*-Verfahren kennen – nicht bei der Auffindung der für sie günstigen Tatsachen und Beweise behilflich sein muss. Jedoch lässt sich diesen Grundsätzen das verfassungsrechtliche Gebot der Waffengleichheit[367] entgegenhalten. Ein Rechtsstreit darf daher nicht allein deswegen aussichtslos sein, nur weil bestimmte Tatsachen einer Partei verborgen sind.[368] Parteien müssen also Tatsachen, die sich nur in ihrem Wahrnehmungsbereich befinden, im Prozess grundsätzlich vortragen, wenn diese Tatsachen für die andere Partei streitentscheidend sind.[369]

---

362 Schlussanträge vom 6. Juni 2018, Rs. C-149/17, Rz. 42 – ECLI:EU:C:2018:400 - „Bastei Lübbe“. Siehe mit einer ähnlichen Schätzung *Zimmermann*, MMR 2014, 368, 369f.

363 Ergänzend kann erwähnt werden, dass sich aus zahlreichen Normen ein gesetzliches Leitbild der Mehrfachnutzung eines Anschlusses ableiten lässt, siehe *Zimmermann*, MMR 2014, 368, 369. Auch mit diesem Argument ließe sich ein Anscheinsbeweis ablehnen, ohne dass es jedoch hierauf noch ankäme.

364 Siehe hierzu sogleich Kapitel § 4 VII. 5.

365 *Bacher* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 284 ZPO, Rz. 34.

366 *Prütting* in: Rauscher/Krüger, MüKo-ZPO, 6. Aufl. 2020, § 284 ZPO, Rz. 79f.

367 *Safferling*, NStZ 2004, 181, 183f.

368 *Solmecke/Rüther/Herkens*, MMR 2013, 217, 218.

369 BGH, Urteil vom 23. Oktober 2007, Az. XI ZR 423/06, Rz. 19 – NJW-RR 2008, 1269, mit weiteren Nachweisen der Rechtsprechung des BGH.

Folglich ist es dogmatisch überzeugend, wenn der BGH bezüglich Urheberrechtsverletzungen über einen Internetanschluss statt einem Anscheinsbeweis für die Täterschaft des Anschlussinhabers zumindest eine sekundäre Darlegungslast[370] desselben annimmt, da es außerhalb des Wahrnehmungsbereiches des klagenden Rechteinhabers liegt, welche Personen Zugriff zu einem Internetanschluss haben.

Der Anschlussinhaber muss also bestimmte Tatsachen vortragen. Die Möglichkeit, dass eine andere Person als der Anschlussinhaber die Urheberrechtsverletzung begangen hat, setzt denknotwendig voraus, dass eine andere Person außer dem Anschlussinhaber zum Verletzungszeitpunkt Zugriff auf den Internetanschluss hatte. Die sekundäre Darlegungslast ist mithin nur erfüllt, wenn sich aus dem Vortrag des beklagten Anschlussinhabers ergibt, dass zum Verletzungszeitpunkt auch tatsächlich andere Personen Zugriff auf den Internetanschluss hatten.

Wird sie nicht erfüllt, gilt es als zugestanden, dass der Anschlussinhaber den Anschluss anderen Personen nicht in beabsichtigter Weise zur Verfügung stellt.[371] Die Behauptung des klagenden Rechteinhabers, der Anschlussinhaber sei Täter, ist also aufzuteilen in zwei Behauptungen, nämlich erstens, dass der Anschlussinhaber den Anschluss alleine benutzt, bzw. genauer: *beabsichtigt* diesen alleine zu nutzen, und zweitens auch eine unbeabsichtigte Nutzung des Anschlusses zum Tatzeitpunkt durch einen Dritten, zum Beispiel dadurch, dass dieser eine technische Sicherheitslücke ausnutzt, nicht stattfand. Zugestanden ist bei Nichterfüllung der sekundären Darlegungslast nur die erste Tatsache; die Rechtsprechung des BGH lässt sich jedoch so verstehen, dass für die zweite dann ein Anscheinsbeweis gilt[372].

Kernfrage des Streits in *filesharing*-Konstellationen ist mithin, welcher Vortrag ausreicht, um die Schlussfolgerung dahingehend, dass der Anschlussinhaber den Anschluss tatsächlich allein benutzt hat, ziehen zu können.

---

[370] Zutreffenderweise fordert der BGH eine sekundäre Darlegungslast statt einem substantiierten Bestreiten. Letzteres obliegt einer Prozesspartei graduell zunehmend in dem Maße, wie die andere Prozesspartei ihren Vortrag graduell zunehmend substantiiert. Die sekundäre Darlegungslast greift hingegen, wenn der anderen Partei überhaupt kein substantiierter Vortrag möglich ist, siehe *von Selle* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 138 ZPO, Rz. 19.1.

[371] *Völzmann-Stickelbrock*, in: FS Schilken, 539, 547.

[372] Siehe hierzu Kapitel § 4 VII. 5.

d) Richtiges Verhältnis der Institute zueinander

Nach dieser dogmatischen Einordnung lassen sich die genannten rechtlichen Institute ins richtige Verhältnis zueinander setzen. Würde aus der über einen Internetanschluss begangenen Urheberrechtsverletzung ein Anscheinsbeweis für die Täterschaft dessen Inhabers gelten, müsste der Anschlussinhaber zur Erschütterung desselben *beweisen*, dass andere Personen den Anschluss zum Tatzeitpunkt nutzen konnten, denn nur der Nachweis eines vom typischen Geschehensverlauf abweichenden Geschehensverlaufs vermag einen Anscheinsbeweis zu erschüttern.[373] Unter Geltung der sekundären Darlegungslast muss der Anschlussinhaber nur ausreichend *vortragen*, dass andere Personen den Anschluss zum Tatzeitpunkt nutzen konnten. Die sekundäre Darlegungslast erweist sich prozessual im Verhältnis zum Anscheinsbeweis damit als ein Minus zu Letzterem, da jener gegenüber Ersterer zwar höhere Geltungsvoraussetzungen hat, allerdings auch nur schwerer erschüttert als Ersterer genügt werden kann.[374]

2. Die Bestimmung des Rahmens der sekundären Darlegungslast

Da die sekundäre Darlegungslast in dem kaum begrenzten Wortlaut „*zu erklären*“ in § 138 Abs.2 ZPO verankert wird, handelt es sich bei ihr offenkundig um eine Generalklausel. Grundsätzlich ist daher dem BGH eine weitreichende dogmatische Freiheit bei ihrer inhaltlichen Bestimmung zuzubilligen. Jedoch ist rechtsdogmatisch nicht nur zu fordern, dass die inhaltliche Bestimmung konsequent oder jedenfalls in sich widerspruchsfrei ist[375], sondern auch zu keiner inhaltlichen Überlappung mit den Instituten des Anscheinsbeweises oder gar der Umkehr der materiellen Beweislast führt. Wenn der BGH die sekundäre Darlegungslast also nur gegen die Umkehr der materiellen Beweis-

[373] *Doukoff*, SVR 2015, 245, 252.

[374] Eine Umkehr der materiellen Beweislast wäre gegenüber den beiden genannten Instituten ein prozessuales Plus. Der Gegenstandsbezug wäre wiederum derselbe (aus dem Feststehen der Urheberrechtsverletzung wird eine Ableitung für die Täterschaft getroffen), die Anforderungen an den Anschlussinhaber wären aber höher als im Falle des Anscheinsbeweises, da es nicht ausreichen würde, wenn er nachweist, dass andere Personen zum Tatzeitpunkt den Anschluss nutzen konnten; stattdessen müsste er beweisen, dass er *nicht* der Täter der Urheberrechtsverletzung ist.

[375] Siehe hierzu sogleich Kapitel § 4 VII. 3.

last abgrenzt[376], ist dies unzureichend.

Da die Konstituierung einer Umkehr der materiellen Beweislast[377] dem Gesetzgeber vorbehalten ist[378], verbietet sich eine Bestimmung der sekundären Darlegungslast des Anschlussinhabers in einer Weise, die einer solchen Umkehr gleichkommt, also nicht nur aus Gründen der rechtsdogmatischen Konsistenz sondern auch auf Grund des Rechtsstaatsgebots und des Grundsatzes der Gewaltenteilung. Eine richterrechtlich etablierte Umkehr der materiellen Beweislast bzw. sekundäre Darlegungslast, die einer solchen Umkehr gleichkommt, wäre selbst dann unzulässig, wenn eine in § 138 Abs.2 ZPO verankerte Grundrechtsabwägung (die wegen der mittelbaren Drittwirkung der deutschen[379] und europäischen[380] Grundrechte angezeigt ist) oder eine richtlinienkonforme Auslegung zu dem Ergebnis kommen würde, dass eine Umkehr der materiellen Beweislast geboten ist, da weder eine grundrechts- noch eine richtlinienkonforme Auslegung *contra legem* zulässig ist.[381]

Die Konstituierung eines Anscheinsbeweises ist nicht dem Gesetzgeber vorbehalten, sodass eine richterrechtliche Etablierung desselben oder eine inhaltliche Fassung der sekundären Darlegungslast des Anschlussinhabers, die einem Anscheinsbeweis gleichkommt, zwar – wegen der unterschiedlichen Voraussetzungen von Anscheinsbeweis und sekundärer Darlegungslast – rechtsdogmatisch unrichtig, jedoch rechtlich möglich wäre, wenn eine grund- oder europarechtskonforme Auslegung die Konstituierung gebieten würden. Jedoch

376 Vgl. BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 15 – GRUR 2017, 386 - „Afterlife“.

377 Die materielle Beweislast oder Feststellungslast betrifft die Frage, zu wessen Lasten die Nichterweislichkeit einer Tatsache geht. Sie greift also erst am Ende der Beweisführung, wenn diese zu keinem eindeutigen Ergebnis führt, siehe *Kur*, Beweislast und Beweisführung im Wettbewerbsprozeß, S. 17ff.

378 Mit Nachweisen hierzu siehe *Laumen*, MDR 2015, 1, 4. Zur Beweislastverteilung nach dem Günstigkeitsprinzip siehe *Laumen*, NJW 2002, 3739, 3741 und *Brand*, NJW 2017, 3558, 3560, jeweils mit Nachweisen der Rechtsprechung.

379 *Armbrüster* in: Säcker et al., MüKo-BGB, 8. Aufl. 2018, § 134 BGB, Rz. 34.

380 Schlussanträge vom 6. Juni 2018, Rs. C-149/17, Rz. 34ff. – ECLI:EU:C:2018:400 - „Bastei Lübbe“.

381 Zum Verbot der grundrechtskonformen Auslegung *contra legem* siehe BVerfG, Beschluss vom 11. Juni 1958, Az. 1 BvL 149/52, Rz. 22 – juris. Zum Verbot der europarechtskonformen Auslegung *contra legem* siehe EuGH, Urteil vom 16. Juli 2009, Rs. C-12/08, Rz. 61 – ECLI:EU:C:2009:466 - „Mono Car Styling“.

lässt sich ein solch konkretes Ergebnis dieser Auslegung nicht entnehmen.[382] Eine ausreichende Berücksichtigung der Grundrechte und des Europarechts kann mithin auch innerhalb der regulären Grenzen der sekundären Darlegungslast erfolgen.

Abgesehen hiervon ist die Rechtsprechung bei der Anwendung der sekundären Darlegungslast – bedingt durch den offenen Wortlaut des § 138 Abs.2 ZPO – relativ frei. Sie muss lediglich berücksichtigen, dass die sekundäre Darlegungslast nur ein Kompromiss zwischen Beibringungsgrundsatz und prozessualer Waffengleichheit ist, sie also nicht so weit gehen darf, dass der zur sekundären Darlegung Verpflichtete alles tun muss, um dem Kläger zum Prozesserfolg zu verhelfen; die Pflicht zur Wahrheit führt nicht zu einer Pflicht zur optimalen Wahrheitsfindung.[383]

Nachdem der Rahmen nun gesteckt ist, kann die inhaltliche Ausprägung der sekundären Darlegungslast durch die Rechtsprechung des BGH in *filesharing*-Sachverhalten bewertet werden.

3. Die Bestimmung des Inhalts der sekundären Darlegungslast

a) Kritik aus der heutigen Perspektive

Wie dargestellt, war es nach der anfänglichen Rechtsprechung des BGH zunächst unklar, welche zivilprozessualen Institute hinsichtlich der Haftung des Anschlussinhabers genau zum Einsatz kommen sollen und in welchem Verhältnis sie zueinander stehen. Seit „Afterlife“ ist dies nun überwiegend geklärt. Weniger als dogmatische Kritik denn als Kritik an der mangelnden Erfüllung der obergerichtlichen Aufgabe, Rechtssicherheit zu stiften, verbleibt somit, dass diese Klärung sechs Jahre gedauert und mehrere *filesharing*-Entscheidungen benötigt hat. Inhaltlich musste die dogmatisch unklare

[382] Vgl. hierzu die entsprechende Aussage des BGH zur Störerhaftung, BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 24f. – GRUR 2016, 1289 - „Silver Linings Playbook“. Siehe auch Schlussanträge vom 6. Juni 2018, Rs. C-149/17, Rz. 37 – ECLI:EU:C:2018:400 - „Bastei Lübbe“.

[383] Vgl. *Brand*, NJW 2017, 3558, 3560. In eine ähnliche Richtung geht das im Rahmen der sekundären Darlegungslast von der Rechtsprechung geschaffene Erfordernis der Zumutbarkeit, siehe BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 18 – GRUR 2014, 657 - „BearShare“. Mit weiteren Nachweisen aus anderen Rechtsbereichen siehe auch *Forch*, GRUR-Prax 2015, 49, 50.

Lage dabei nicht einmal einen Unterschied machen: da in „Sommer unseres Lebens“ der BGH immerhin geäußert hatte, dass aus der tatsächlichen Vermutung eine sekundäre Darlegungslast folgt[384], bestand in der nachfolgenden Instanzrechtsprechung zumindest weitestgehende Übereinstimmung darin, dass es nicht auf die tatsächliche Vermutung ankomme, sondern darauf, wie die sekundäre Darlegungslast inhaltlich zu bestimmen sei. Weil der BGH hierfür inhaltlich jedoch keinerlei Hinweise gegeben hatte, ergaben sich je nach Gerichtsbezirk erhebliche Unterschiede.[385] In der Entscheidung „BearShare“ hatte der BGH lediglich ergänzt, dass den Anschlussinhaber eine Nachforschungspflicht treffe[386], ohne diese jedoch – *obiter dictum* – auszubuchstabieren, weshalb die Instanzrechtsprechung in Folge auch in diesem Punkt sehr uneinheitlich blieb.[387]

Da der BGH mit den Urteilen „Tauschbörse III“, „Every time we touch“, „Afterlife“ und „Loud“ die sekundäre Darlegungslast inhaltlich nunmehr stärker konturiert hat, ist der Makel der fehlenden Rechtssicherheit (zumindest bei geschlossenem Betrieb eines WLAN) deutlich abgeschwächt.[388]

Erledigt haben sich auch Rechtsfragen betreffend die Darlegungs- und Beweislast, die sich noch im Zusammenhang mit strafrechtlichen Ermittlungen ergeben konnten. Wie dargestellt, mussten Rechteinhaber vor Implemen-

[384] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

[385] Siehe mit zahlreichen Nachweisen *Solmecke/Rüther/Herkens*, MMR 2013, 217, 219 und *Zimmermann*, MMR 2014, 368, 368.

[386] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 18 – GRUR 2014, 657 - „BearShare“.

[387] Mit zahlreichen Nachweisen der Rechtsprechung *Solmecke/Rüther/Büring*, MMR 2016, 153, 154f. Mit umfangreichen Nachweisen auch LG Braunschweig, Urteil vom 1. Juli 2015, Az. 9 S 433/14, 9 S 433/14 (59), Rz. 41 – juris. Die Uneinheitlichkeit der Rechtsprechung wird auch vom BVerfG in zwei Verfassungsbeschwerden anerkannt, die eine Verletzung des rechtlichen Gehörs wegen Nichtzulassung der Revision trotz ungeklärter Reichweite der sekundären Darlegungslast gerügt hatten. Die Verfassungsbeschwerden wurden nur deshalb nicht angenommen, weil in der Zwischenzeit die Entscheidung „Tauschbörse III“ ergangen war und das BVerfG daher keine Erfolgsaussichten einer Revision sah, siehe BVerfG, Nichtannahmebeschluss vom 23. September 2016, Az. 2 BvR 1797/15 – juris und Nichtannahmebeschluss vom 23. September 2016, Az. 2 BvR 2193/15 – juris.

[388] Siehe hierzu genauer Kapitel § 4 VII. 3. b) aa). Behoben sind auch andere Makel wie insbesondere die fragwürdige Heranziehung von Grundsätzen des Transportrechts in „BearShare“, die in „Afterlife“ aufgegeben wurde, siehe Kapitel § 2 IV. 3 und XI. 1.

tierung des zivilrechtlichen Auskunftsanspruchs noch den Umweg über das Strafverfahren gehen[389], was regelmäßig mit Hausdurchsuchungen bzw. Durchsuchungen von PCs sowie polizeilichen Vernehmungen verbunden war.[390] Folglich flossen auch die Ergebnisse der strafrechtlichen Ermittlungen regelmäßig in die Prüfung der sekundären Darlegungslast ein. Diese fallen wegen der nunmehr rein zivilrechtlich geführten Verfahren weg.[391]

b) Dogmatische Analyse der Rechtsprechung des BGH

Zuzustimmen ist der Aufteilung der Pflichten des Anschlussinhabers in eine Nachforschungspflicht[392] und eine Mitteilungspflicht[393] (also eine Pflicht zur Mitteilung über die im Rahmen der Nachforschungen erlangten Erkenntnisse), da sie eine passende Einordnung verschiedener Sachverhaltskonstellationen erlauben. Die Behandlung dieser Pflichten durch den BGH ist in ihren Einzelheiten teilweise kritikwürdig, teilweise zustimmungsfähig. Hierzu im Einzelnen:

aa) Unterschiedliche Behandlung unterschiedlicher Nutzungsformen eines Internetanschlusses im Rahmen der Nachforschungspflicht

Wie dargestellt, kann ein Netzwerk auf unterschiedliche Weisen benutzt werden[394], wobei in ihrer technischen Wirkung die kabelgestützte Verbindung zu einem Router, der geschlossene Betrieb eines WLAN und der Hotspot-Betrieb eines WLAN praktisch gleich sind, da der Anschlussinhaber kontrolliert, wer sich zu seinem Netzwerk verbindet, weil er nach eigenem Be-

389 Siehe Kapitel § 2 II.

390 Vgl. beispielsweise BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 4 – GRUR 2013, 511 - „Morpheus“; BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 2 – GRUR 2014, 657 - „BearShare“; BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 2 – GRUR 2016, 184 - „Tauschbörse II“. Zum Beweiswert der Durchsuchung eines PC siehe Kapitel § 1 IV. 7. c) aa).

391 Zu der Frage, ob auch zivilrechtlich eine Herausgabe und nachfolgende Duldung einer Durchsuchung von Geräten wie PCs etc. verlangt werden kann siehe Kapitel § 5 V. 3. e).

392 Erstmals BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 18 – GRUR 2014, 657 - „BearShare“.

393 Erstmals BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 42 – GRUR 2016, 191 - „Tauschbörse III“.

394 Siehe Kapitel § 1 IV. 3.

lieben Verbindungskabel trennen sowie das Passwort oder einen Hotspot-Account nur denjenigen Personen geben kann, deren Verbindung zu seinem Netzwerk er akzeptieren möchte; unberechtigter Weitergabe von Passwörtern oder Hotspot-Accounts kann er durch Passwortänderung oder Account-Sperrungen entgegenwirken. Solange ein WLAN hingegen offen betrieben wird, hat der Anschlussinhaber keine Kontrolle darüber, welche Personen sich mit diesem verbinden. Ein geschlossenes Netzwerk kann wiederum erstens familiär, zweitens nicht-familiär und nicht-gewerblich, drittens nicht-familiär und gewerblich und viertens in Mischformen familiär/nicht-familiär benutzt werden. Bei einem offenem Betrieb scheidet eine Differenzierung auf Grund der Möglichkeit des Zugriffs durch beliebige Personen aus.

Der BGH behandelt diese Konstellationen im Hinblick auf die Nachforschungspflicht[395] zum Teil ausdrücklich, zum Teil implizit unterschiedlich, zum Teil war er mit diesen auch noch nicht befasst. Die rein familiäre Nutzung war bis zur „Bastei Lübbe"-Entscheidung des EuGH[396] gegenüber der rein nicht-familiären privilegiert, da die Anforderungen an die Nachforschungspflicht bei Ersterer laut BGH geringer sind als bei Letzterer, wobei der BGH offen ließ, ob er diese Differenzierung in Zukunft aufrecht erhalten wird.[397] Unklar ist, wie der BGH bezüglich dem offenem Betrieb zu verstehen ist, sofern dieser bestritten wird oder sofern dieser zwar zugestanden, aber die Täterschaft des Anschlussinhabers dennoch behauptet wird. Dem BGH zu Folge greife die tatsächliche Vermutung / ein Anscheinsbeweis zwar nicht, wenn ein Internetanschluss „*nicht hinreichend gesichert*" ist; die sekundäre Darlegungslast gelte aber dennoch.[398] Dies ist wohl so zu verstehen, dass bei zugestandenem offenem Betrieb der Kläger voll beweisbelastet für die Täterschaft des Anschlussinhabers bleibt (da die Täterschaft eines anderen dann nicht ausgeschlossen ist); bei bestrittenem offenen Betrieb ist unklar, welche Tatsachen ein Anschlussinhaber vortragen muss, um seiner sekundären Darlegungslast zu genügen (mithin also, um einen offenen Betrieb zu

[395] Bezüglich der Mitteilungspflicht differenziert er nicht zwischen verschiedenen Formen der Anschlussteilung.

[396] Siehe Kapitel § 2 XI. 1.

[397] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 26 – GRUR 2017, 386 - „Afterlife".

[398] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 15 – GRUR 2017, 386 - „Afterlife"; BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 15 – GRUR 2014, 657 - „BearShare".

plausibilisieren).[399]

Vom BGH noch überhaupt nicht angesprochen wurde die Frage, wie eine gewerbliche Nutzung[400] oder verschiedene Mischformen der Nutzung[401] zu behandeln sind.

Die dogmatische Betrachtung ist folglich auf die unterschiedliche Behandlung von familiärer und nicht-familiärer Nutzung zu begrenzen, wie sie in der Entscheidung „Afterlife“ vorgenommen wurde. Grundsätzlich ist die Rechtsprechung berechtigt, vergleichbare Sachverhalte unterschiedlich zu behandeln. Eine mittelbare Drittwirkung des Art. 3 Abs.1 GG kommt nur in (hier nicht einschlägigen) Ausnahmefällen in Betracht.[402] Jedoch folgt aus Art. 3 Abs.1 GG auch für die Gerichte ein Willkürverbot.[403] Eine Ungleichbehandlung von zwei Sachverhalten ist mithin nur gerechtfertigt, wenn sich ein sinnvolles Differenzierungskriterium in tatsächlicher oder rechtlicher Hinsicht finden lässt.

Implizit scheint der BGH als Differenzierungskriterium zwischen familiärer und nicht-familiärer Nutzung anzusehen, dass sich Anschlussinhaber in familiären Kontexten gegenüber Anschlussinhabern in nicht-familiären Kontexten auf ein *zusätzliches* Grundrecht berufen können, nämlich nicht nur das Recht auf Informationsfreiheit (Art. 11 GRC und Art. 5 Abs.1 Satz 1 GG) und das Recht auf Freiheit und Achtung des Privatlebens (Art. 6, 7 GRC und Art. 2 Abs.1 GG)[404], sondern zudem auf das Grundrecht auf das ungestörte eheliche und familiäre Zusammenleben (Art. 7 GRC und Art. 6

399 Siehe hierzu Kapitel § 5 V. 3. a).

400 In „Sommer unseres Lebens“ hatte der BGH lediglich argumentiert, eine strenge Störerhaftung privater Anschlussinhaber sei gerechtfertigt, da diese kein schützenswertes Geschäftsmodell verfolgen, siehe BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 24 – GRUR 2010, 633 - „Sommer unseres Lebens“. Ob er – an dieses Argument anschließend – die Anforderungen an die sekundäre Darlegungslast bei gewerblichen Nutzungen entsprechend niedrig stellen wird, ist daher offen. Relevant könnte dies vor allem bei der gewerblichen Bereitstellung eines Hotspots werden. Siehe hierzu auch Kapitel § 5 V. 3. b).

401 Siehe hierzu ebenfalls Kapitel § 5 V. 3. b).

402 BVerfG, Beschluss vom 11. April 2018, Az. 1 BvR 3080/09, Rz. 40ff. – bverfg.de.

403 Siehe nur BVerfG, Beschluss vom 28. Juli 2015, Az. 2 BvR 2558/14, 2 BvR 2571/14, 2 BvR 2573/14, Rz. 74 – bverfg.de, mit weiteren Nachweisen.

404 Dass sich der Anschlussinhaber auf diese berufen kann, hat der BGH ausdrücklich im Rahmen der Störerhaftung festgehalten, siehe BGH, Urteil vom 12. Mai 2016, Az. I ZR 86/15, Rz. 26 – GRUR 2016, 1289 - „Silver Linings Playbook“.

GG)[405]. Solch eine „Grundrechtsarithmetik“ ist jedoch kein durchschlagendes Argument, da in einer Grundrechtsabwägung drei Grundrechten nicht automatisch mehr Gewicht zukommt als zwei. D.h., dass auch die Grundrechte auf Informationsfreiheit und auf Freiheit und Achtung des Privatlebens ausreichen könnten, um ein Abwägungsergebnis wie in „Afterlife“ zu erzielen.[406] Der BGH müsste also festlegen, inwiefern das Grundrecht auf das ungestörte eheliche und familiäre Zusammenleben familiäre Mitnutzer vor *Nachforschungen* mehr als nicht-familiäre Mitnutzer schützen soll. Ihm zu Folge bedeutet das ungestörte eheliche und familiäre Zusammenleben in diesem Kontext aber den Schutz der Familienmitglieder vor dem Risiko einer zivil- oder strafrechtlichen Inanspruchnahme.[407] Dieser Schutz wird allerdings erst auf Ebene der *Mitteilungspflicht* relevant, da durch Nachforschungen allein dieses Risiko nicht erhöht wird.

Art. 7 GRC und Art. 6 GG müssten das Familienleben also darüber hinaus auch spezifisch vor Nachforschungen und nicht nur vor Mitteilungspflichten schützen. Dies ist allerdings nicht der Fall. Sicherlich ist es für das Familienleben aufwühlend, wenn eine Abmahnung „ins Haus flattert“ und diese thematisiert werden muss. Es ist aber nichts dahingehend ersichtlich, dass diese Grundrechte vor jeder Unannehmlichkeit schützen. Im Rahmen von Nachforschungen können sie also nur relevant sein, sofern sie gegenüber den Grundrechten auf Freiheit und Achtung des Privatlebens (Art. 6, 7 GRC und Art. 2 Abs.1 GG) einen gesteigerten Privatspährenschutz innerhalb der Familie konstituieren. Auch hierfür ist jedoch nichts ersichtlich. Im Gegenteil haben Familienmitglieder untereinander einen geringeren Schutz der Privat-

[405] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 23 – GRUR 2017, 386 - „Afterlife“

[406] Zwar kann eine inhaltliche Stärkung des Grundrechtsschutzes eintreten, wenn sich ein Grundrechtsträger in der Abwägung auf mehr als ein Grundrecht berufen kann. Dem liegt jedoch kein Automatismus zu Grunde, vgl. BGH, Urteil vom 7. Juli 2020, Az. VI ZR 246/19, Rz. 45 – GRUR 2021, 100 mit weiteren Nachweisen.

[407] BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 23 – GRUR 2017, 386 - „Afterlife“; BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 21 – GRUR 2017, 1233 - „Loud“.

sphäre als nicht-familiär verbundene Personen untereinander.[408]

Im Ergebnis rechtfertigt also die mittelbare Drittwirkung der Grundrechte keine Differenzierung zwischen einer familiären und einer nicht-familiären Anschlussnutzung im Rahmen der Nachforschungspflicht. Die Rechtsprechung des BGH ist in diesem Punkt mithin dogmatisch unrichtig.

Der Vollständigkeit halber zu ergänzen ist jedoch, dass dem BGH mit „Afterlife“ kein Widerspruch zu seinen Entscheidungen „Loud“ und „Siliver Linings Playbook“ vorzuwerfen ist. Zwar wurden in diesen Entscheidungen familiäre und nicht-familiäre Anschlussnutzungen in Folge einer Grundrechtsabwägung gleich behandelt, jedoch betrafen die Abwägungen dort jeweils andere Fragen: in „Afterlife“ war fraglich, ob innerhalb einer Familie ein größerer Schutz der Privatsphäre gilt als zwischen nicht familiär verbundenen Personen; in „Loud“ war fraglich[409], ob Familienmitgliedern untereinander ein größerer Schutz vor der Verpflichtung zu Auskünften, die das Risiko der zivilrechtlichen Verfolgung mit sich bringen, gebührt als nicht familiär verbundenen Personen untereinander; in „Silver Linings Playbook“ wurde entschieden[410], dass es im Rahmen der Störerhaftung auf die Eigenverantwortlichkeit der Mitnutzer ankommt, mithin volljährige Kinder anderen Volljährigen, die nicht familiär verbunden sind, gleichzustellen sind. *Prima facie* kann in letzteren beiden Konstellationen bei der Grundrechtsabwägung dasselbe Ergebnis herauskommen (Gleichstellung von familiär verbundenen und familiär nicht verbundenen Personen), muss aber nicht.

Folglich kann dem BGH bezüglich „Silver Linings Playbook“ zugestimmt, bezüglich „Afterlife“ jedoch widersprochen werden: Bei ersterer Entscheidung ist allein die erwartbare Eigenverantwortlichkeit der Nutzer entscheidend, die – wie vom BGH richtig erkannt – bei volljährigen Familienangehörigen nicht anders zu bewerten ist als bei nicht familiär verbundenen Personen; bei letzterer Entscheidung ist allein das erwartbare Maß an Privatsphäre

[408] So jedenfalls im Verhältnis minderjähriger Kinder zu ihren Eltern der Wissenschaftliche Dienst des Deutschen Bundestages, WD 3 - 3000 - 046/16; WD 7 - 3000 - 027/16, S. 5f. Auch *Köhler* geht von einem Erfordernis der Gleichbehandlung der familiären und nicht-familiären Anschlussnutzung in diesem Zusammenhang aus, siehe *Köhler*, Die Haftung privater Internetanschlussinhaber, S. 163ff., 277. aA und gegen die Pflicht zur Befragung von Familienangehörigen *Gotthardt*, ZUM 2021, 7, 14f.

[409] Siehe Kapitel § 2 XI. 3.

[410] Siehe Kapitel § 2 VII. 3.

entscheidend, das – wie vom BGH verkannt – zwischen Familienangehörigen untereinander nicht größer ist als zwischen volljährigen Personen, die familiär nicht miteinander verbunden sind.

Hierin ist jedoch nach hier vertretener Auffassung lediglich eine unzutreffende Grundrechtsabwägung zu sehen, kein Verstoß gegen das Willkürverbot.

bb) Gleiche Behandlung unterschiedlicher Nutzungsformen eines Internetanschlusses im Rahmen der Mitteilungspflicht

Die in „Tauschbörse III“ postulierte Mitteilungspflicht gilt gemäß dem Urteil „Loud“ auch für Familien, wobei in „Loud“ spezifisch über die Frage gestritten wurde, ob Eltern ihre (volljährigen) Kinder verraten müssen, wenn sich diese den Eltern gegenüber als Täter der Urheberrechtsverletzung gestellt haben.[411] Dies ist ein besonderer, „überschießender“ Teil der Mitteilungspflicht, da sie in diesem Punkt nicht mit der Nachforschungspflicht korrespondiert. Denn die Nachforschungspflicht gebietet nicht die Ermittlung des wahren Täters. Eine Entscheidung zu Gunsten der Eltern hätte mithin die Nachforschungs- und Mitteilungspflicht im Übrigen unberührt gelassen, die Möglichkeit der Rechtsverfolgung für den betroffenen Rechteinhaber also nicht vollständig vereitelt.

Möglicherweise war dies dem BGH in der Entscheidung „Loud“ nicht bewusst, da er dort der Auffassung ist, eine Entscheidung zu Gunsten der Eltern würde eine Rechtsverfolgung praktisch unmöglich machen.[412] Hätte der BGH mit diesem Punkt recht, wäre sein Ergebnis vertretbar. Denn er hätte dann eine binäre Entscheidung zwischen zwei Grundrechten treffen müssen: Entweder er entscheidet zu Gunsten des klagenden Rechteinhabers, dann kann der Schutz der Familie überhaupt nicht berücksichtigt werden, da Familien in diesem Punkt in Folge den nicht familiär verbundenen Personen gleichgestellt sind und eine Gleichstellung nicht gerechtfertigt wäre, da Private kein Grundrecht haben, das sie davor schützt, Auskunftsverpflichtungen auferlegt zu bekommen, die andere Personen dem Risiko zivilrechtlicher Inanspruchnahme aussetzen. Oder er entscheidet zu Gunsten der beklagten

[411] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 5 – GRUR 2017, 1233 - „Loud“. Ob im Verhältnis von Eltern zu ihren minderjährigen Kindern etwas anders gilt, ist offen.

[412] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 28 – GRUR 2017, 1233 - „Loud“.

Eltern, dann könnte umgekehrt der Eigentumsschutz keinerlei Berücksichtigung finden.

Nun war die Entscheidung aber keine binäre: eine Entscheidung zu Gunsten der beklagten Eltern hätte den Schutz der Familie zur Geltung gebracht, ohne den Eigentumsschutz völlig auszublenden, da die Nachforschungs- und Mitteilungspflicht *im Übrigen* noch Bestand gehabt hätte. Die vom BGH tatsächlich getroffene Entscheidung zu Gunsten der Rechteinhaber verwehrt dem Familienschutz *jegliche* Geltung, da Familien in dieser Sachverhaltskonstellation den nicht familiär verbundenen Personen völlig gleichgestellt werden, obwohl Ersteren durch das Recht auf Schutz des Familienlebens ein höhere Schutz vor Auskunftspflichten eingeräumt ist als Letzteren. Da also nur eine Entscheidung zu Gunsten der Eltern die Grundrechte *beider* Parteien zur Geltung gebracht hätte, hätte er auch diese Entscheidung treffen müssen. Der Vorrang eines Abwägungsergebnisses, das beide abgewogenen Grundrechte zur Geltung bringt, vor einem Abwägungsergebnis, das nur eines der abgewogenen Grundrechte zur Geltung bringt, ist ein allgemeines Prinzip.

Die Entscheidung des BGH wäre mithin nur dann vertretbar, wenn das nach hiesiger Ansicht vertretene Ergebnis eine Auslegung *contra legem* wäre[413] und folglich als einzig mögliche Auslegungsvariante nur die des BGH verbleiben würde. Dass der BGH dies möglicherweise so sieht, lässt sich seinem Hinweis auf § 383 Abs.1 Nr.1 bis Nr.3 ZPO entnehmen, demgemäß nur Zeugen das Recht zusteht, Angaben zu Familienangehörigen zu verweigern, mithin Prozessparteien dieses Recht nicht zustehe.[414] Verstehen ließe sich dieser Hinweis als impliziter Schluss *e contrario*; eine Auslegung, die einen solchen Schluss nicht zieht, ist allerdings nicht *contra legem* – nur eine Auslegung gegen den Wortlaut einer Norm kann *contra legem* sein. Ohnehin ist aber schon fraglich, ob der vom BGH implizit vollzogene Umkehrschluss berechtigt ist, da § 383 Abs.1 ZPO nur die *vollständige* Verweigerung einer Aussage ermöglicht[415], während hingegen bezüglich der sekundären Darlegungslast nur fraglich ist, ob *einzelne* Angaben nicht verlangt werden dürfen. Da ohnehin

[413] Die auch im Falle ihrer Grundrechtskonformität unzulässig ist, siehe Kapitel § 4 VII. 2.

[414] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 28 – GRUR 2017, 1233 - „Loud".

[415] § 383 Abs.3 ZPO, der die Zeugenvernahme in Bezug auf nur einzelne Tatsachen verbietet, findet nur auf § 383 Abs.1 Nr.4 bis 6 ZPO Anwendung.

aber eine grundrechtskonforme Auslegung einer Auslegung, die mittels eines Umkehrschlusses erzielt wurde, vorzuziehen ist[416], kann die Berechtigung des vom BGH hier implizit vollzogenen Umkehrschlusses dahinstehen.

Im Übrigen stützt der BGH seine Entscheidung lediglich auf das Argument, dass die Beeinträchtigung der Grundrechte der Eltern kein entscheidendes Gewicht zukomme, da die Geständnisfiktion des § 138 Abs.3 ZPO auf Grund einer nicht ausreichend erfüllten sekundären Darlegungslast unterschiedslos jede prozessual ungenügend vortragende Partei treffe.[417] Dies ist jedoch zirkelschlüssig, da es ja gerade fraglich ist, ob Familien in dem zu entscheidenden Sachverhalt unterschiedslos wie jede andere Prozesspartei behandelt werden dürfen.

Eine letzte Möglichkeit, die Entscheidung des BGH zu rechtfertigen, bestünde allenfalls, wenn der Schutz der Familie an *anderer* Stelle als im Verletzungsverfahren gegen den Anschlussinhaber ausreichend zur Geltung gebracht werden könnte. Dies klingt bei *Schaub* an, wenn sie darauf verweist, dass nur die Mitteilung des Namens des Familienmitglieds, das sich als Täter gestellt hat, noch nicht automatisch zu dessen Haftung führt, sondern der Rechteinhaber einen Folgeprozess gegen das benannte Familienmitglied führen müsste, in dem der Anschlussinhaber wiederum als Zeuge geladen werden müsste und dort schließlich wegen § 383 Abs.1 Nr.1 bis Nr.3 ZPO jede Angabe verweigern könnte.[418] Es verbleibt jedoch das Problem, dass die Bekanntgabe des Täters im Tatbestand (§§ 313 Abs.1 Nr.5, Abs.2, 314 ZPO) des Urteils im Verfahren gegen den Anschlussinhaber enthalten ist und zusätzlich auch, auf Antrag des klagenden Rechteinhabers, nach § 160 Abs.4 ZPO in das Protokoll der mündlichen Verhandlung aufgenommen werden kann. Nach *Schaub* solle dem Schutz der Familie dann aber im Rahmen der Beweiswürdigung Rechnung getragen werden können.[419] Gemeint ist wohl, dass die Möglichkeit bestünde, Urteilstatbestand und Protokoll als nicht ausreichende Beweismittel zu werten. Das ist jedoch unzutreffend, da Urteilstatbestand[420] und Protokoll[421] als öffentliche Urkunden gemäß § 418 Abs.1

[416] Vgl. BVerfG, Beschluss vom 19. September 2007, Az. 2 BvF 3/02, Rz. 92f. – bverfg.de.
[417] BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 26 – GRUR 2017, 1233 - „Loud".
[418] *Schaub*, NJW 2018, 17, 18.
[419] *Schaub*, NJW 2018, 17, 18.
[420] *Schreiber* in: Rauscher/Krüger, MüKo-ZPO, 6. Aufl. 2020, § 418 ZPO, Rz. 6.
[421] Vgl. BGH, Beschluss vom 2. November 2010, Az. VIII ZA 14/10 – BeckRS 2010, 27525.

ZPO den vollen Beweis über die in ihnen enthaltenen Tatsachen erbringen und deren Verwertung im Prozess gegen den benannten Täter nicht gegen den Unmittelbarkeitsgrundsatz aus § 355 ZPO verstößt.[422] Eine teleologische Reduktion des § 418 Abs.1 ZPO aus Gründen der Grundrechtskonformität kommt nicht in Betracht.[423] Im Folgeprozess gegen den benannten Mittäter kann der Schutz des Familienlebens folglich nicht in gleichem Maße berücksichtigt werden wie im Prozess gegen den Anschlussinhaber.

Es bleibt daher bei dem Ergebnis, dass die Entscheidung des BGH in „Loud“ bezüglich der Mitteilungspflicht betreffend den wahren Täter der Urheberrechtsverletzung im familiären Kontext der Anschlussnutzung dogmatisch unrichtig ist.[424] Gleiches gilt entsprechend für den auf die Verfassungsbeschwerde gegen „Loud“ ergangenen Nichtannahmeentschluss des BVerfG, in dem das soeben erörterte unterschiedliche Gewicht der hier einschlägigen Grundrechtspositionen verkannt wird.[425]

Hierin ist jedoch nach hier vertretener Auffassung lediglich eine unzutreffende Grundrechtsabwägung zu sehen, kein Verstoß gegen das Willkürverbot.

cc) Namentliche Benennung der Mitnutzer im Rahmen der Mitteilungspflicht

Zuzustimmen ist dem BGH darin, dass die Erfüllung der Mitteilungspflicht die namentliche Benennung der Mitnutzer umfasst. Dogmatisch zwingend ist dies nicht, da eine sekundäre Darlegungslast nicht generell überflüssig wäre, wenn sie die Namensnennung nicht beinhalten würde. Hiergegen mag man einwenden, dass Anschlussinhaber dann immer das Vorhandensein von Mitnutzern behaupten würde, auch wenn es nie welche gab. Ein solches Argu-

[422] Vgl. BGH, Urteil vom 12. Juli 2013, Az. V ZR 85/12, Rz. 7 – NJOZ 2014, 572.

[423] Siehe zu den Voraussetzungen der teleologischen Reduktion BVerfG, Beschluss vom 31. Oktober 2016, Az. 1 BvR 871/13, 1 BvR 1833/13, Rz. 22f. – bverfg.de.

[424] Würde man die Mitteilungspflicht *insgesamt*, mit Verweis auf den Schutz des Familienlebens, ablehnen wollen, so würde dies umgekehrt den Schutz des Eigentums vollständig vereiteln, da dann die Inanspruchnahme irgendeiner Person als Täter (und damit auf Schadensersatz) von vornherein komplett ausscheiden würde, was ebenfalls nicht zulässig wäre. Nur die begrenzte Aufhebung der Mitteilungspflicht für Familien, wie sie soeben herausgearbeitet wurde, berücksichtigt beide Grundrechtspositionen.

[425] Vgl. BVerfG, Nichtannahmebeschluss vom 18. Februar 2019, Az. 1 BvR 2556/17, Rz. 11ff. – bverfg.de. Dort wird gar nicht erst erörtert, dass die vom BGH gesehene, mögliche Beeinträchtigung des Art. 14 GG tatsächlich nicht vorliegt.

ment wäre jedoch auf die pauschale Annahme des (versuchten) Prozessbetruges gestützt, was unter Geltung der Unschuldsvermutung nicht zulässig sein kann.[426] Eine sekundäre Darlegungslast ohne die Pflicht zur namentlichen Nennung von Mitnutzern könnte allerdings nur in Ein-Personen-Haushalten zur Täterschaft des Anschlussinhabers führen und würde somit einen quasi umgekehrten Anscheinsbeweis der Nichttäterschaft des Anschlussinhabers in Mehr-Personen-Haushalten begründen, da dieser mit der wahrheitsgemäßen Behauptung[427] der Existenz von Mitnutzern seiner sekundären Darlegungslast genügen würde. Für solch einen „umgekehrten" Anscheinsbeweis[428] fehlt aber wiederum die empirische Basis[429], da bei einer Mehrfachnutzung die Täterschaft eines jeden Nutzers betreffend einer Urheberrechtsverletzung über den Anschluss gleich wahrscheinlich ist, also der Anschlussinhaber *prima facie* nicht mehr, aber auch nicht weniger (!) als Täter der Urheberrechtsverletzung in Betracht kommt.

Nachdenken ließe sich allenfalls, ob eine unterlassene Nennung der Mitnutzer nicht als Fall der Nichterfüllung der sekundären Darlegungslast, sondern als Fall der Beweisvereitelung anzusehen wäre. So hatte es der dritte Senat des BGH (auf einem anderen Sachgebiet) entschieden.[430] Er begründet dies mit § 373 ZPO, demgemäß die Zeugenbenennung nicht Teil des Tatsachenvortrages, sondern der Beweisführung sei. Jedoch spricht § 373 ZPO auch davon, dass der Zeugenbeweis dadurch angetreten wird, dass die Tatsachen, über die der Zeuge befragt werden sollen, bezeichnet werden müssen. Das Argument des dritten Senats zu Ende gedacht, würde salopp gesagt also auch entsprechender Tatsachenvortrag nicht zum prozessualen Tatsachenvortrag gehören. Dem § 373 ZPO kann also keine kategoriale Zuordnung der Zeugenbenennung zur Beweisführung entnommen werden; die Lesart des dritten Senats ist daher abzulehnen.

---

426 Vgl. hierzu auch *Khazaeli*, ZUM-RD 2019, 659, 659f.

427 Und wahrheitsgemäß wäre diese auch dann, wenn sich der Anschlussinhaber betreffend der Nutzungssituation im Verletzungszeitpunkt nicht sicher ist. Erinnerungslücken dürften wegen der oft erst Jahre später erfolgenden prozessualen Aufarbeitung einer Urheberrechtsverletzung mittels *filesharing* der Regelfall sein, siehe hierzu Kapitel § 5 V. 3. c).

428 Also dahingehend, dass der Anschlussinhaber in einem Mehr-Personen-Haushalts typischerweise nicht der Täter einer über seinen Anschluss begangenen Urheberrechtsverletzung ist.

429 Siehe zu den Voraussetzungen eines Anscheinsbeweises Kapitel § 4 VII. 1. b).

430 BGH, Urteil vom 17. Januar 2008, Az. III ZR 239/06, Rz. 18 – NJW 2008, 982.

Im Ergebnis ist also die fehlende Benennung der Namen (und ladungsfähigen Anschriften) der behaupteten Mitnutzer grundsätzlich als Nichterfüllung der sekundären Darlegungslast (oder genauer: der Mitteilungspflicht innerhalb der sekundären Darlegungslast) anzusehen.

dd) Sonstige Kritikpunkte

- In „Tauschbörse I“ hatte es der BGH für die sekundäre Darlegungslast als unbeachtlich angesehen, wenn der Anschlussinhaber vorträgt, dass er auf Grund Eigenheiten seiner Person (beispielsweise, dass – sofern Musik streitgegenständlich ist – diese seinen Musikgeschmack nicht treffe) nicht als Täter in Betracht komme.[431] Dies ist zutreffend, da sich solche Eigenheiten zu Erfahrungssätzen verdichten lassen müssten, um beachtlich zu sein (beispielsweise: wer eine bestimmte Musik nicht hört, wird diese ganz regelmäßig auch nicht mittels *filesharing* herunterladen), was in den allermeisten Fällen nicht in Betracht kommt. Gleiches gilt für andere Eigenheiten wie beispielsweise IT-Fähigkeiten, da die *filesharing*-Nutzung regelmäßig keine besonderen Fähigkeiten voraussetzt. Dasselbe wie für den Anschlussinhaber müsste dann aber auch für die Mitnutzer gelten. Dem BGH zu Folge können Mitnutzer allerdings als potentielle Täter ausscheiden, wenn dies durch deren Nutzungsverhalten, Kenntnisse oder Fähigkeiten nahegelegt wird.[432] Das ist inkonsequent. Wenn Eigenheiten des Anschlussinhabers nicht zu seinen Gunsten wirken können, dürfen Eigenheiten der Mitnutzer nicht zu dessen Lasten gehen. Denn das Argument fehlender Erfahrungssätze gilt auch für Letztere gleichermaßen.

- In „Tauschbörse III“ und „Every time we touch“ hatte es der BGH gebilligt, dass es das jeweilige Berufungsgericht zu Lasten des Anschlussinhabers gewertet hatte, dass dieser seinen PC (der von den anderen Haushaltsangehörigen jeweils mitbenutzt worden war) nicht daraufhin

[431] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 49ff. – GRUR 2016, 176 - „Tauschbörse I“.

[432] Vgl. zuletzt BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 15 – GRUR 2017, 1233 - „Loud“.

untersucht hatte, ob *filesharing*-Software auf diesem installiert ist.[433] Aus „Afterlife“ lässt sich zudem unter Umständen ableiten, dass der Anschlussinhaber die Geräte seiner behaupteten Mitnutzer auf solche Software hin untersuchen muss.[434] Ob die Untersuchung fremder Geräte überhaupt datenschutz- und persönlichkeitsrechtlich verlangt werden darf, kann dabei dahinstehen. Es wäre schon dogmatisch verfehlt, vom Anschlussinhaber zu verlangen, seine eigenen Geräte, die von Haushaltsangehörigen mitgenutzt werden konnten, oder die Geräte seiner Haushaltsangehörigen auf *filesharing*-Software hin zu untersuchen. Denn die Untersuchung kann frühestens dann stattfinden, wenn der Anschlussinhaber mit einer Abmahnung von der Verletzung in Kenntnis gesetzt wurde. Das Auffinden oder Nichtauffinden von *filesharing*-Software hat dann keinen Erkenntniswert, da im ersteren Fall die Software erst nach dem Verletzungszeitpunkt installiert worden sein könnte, im letzteren Fall vor der Untersuchung gelöscht worden sein könnte. Sinnvoll kann also allenfalls sein, dem Anschlussinhaber im Rahmen seiner Nachforschungspflicht aufzutragen, seine Mitnutzer dahingehend zu befragen, ob diese zum Tatzeitpunkt *filesharing*-Software installiert hatten und dies mitzuteilen (und ebenso mitzuteilen, ob er selbst zum Verletzungszeitpunkt *filesharing*-Software installiert hatte). Dies kann allerdings nur gelten, wenn der Rechteinhaber vorträgt, über welches *filesharing*-System die Verletzung begangen wurde, da es eine Vielzahl von Protokollen gibt und nicht jeder Client jedes Protokoll implementiert.[435] Aus dem Vorhandesein oder Nichtvorhandesein von *filesharing*-Software im Verletzungszeitpunkt können daher nicht zwingend Ableitungen getroffen werden. Trägt der Rechteinhaber (was regelmäßig der Fall sein wird) eine Verletzung über das BitTorrent-System vor, ist zu beachten, dass insbesondere Videodateien auch im Webbrowser über das BitTorrent-System übertragen werden können[436] und daher eine *filesharing*-Nutzung mittels BitTorrent auch ohne einen

[433] BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 41 – GRUR 2016, 191 - „Tauschbörse III“ und BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 49 – GRUR 2016, 1280 - „Every time we touch“.

[434] Vgl. BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 26 – GRUR 2017, 386 - „Afterlife“.

[435] Siehe Kapitel § 1 II. 4. und 5.

[436] Siehe Kapitel § 3 XI. 2. a).

eigens hierfür ausgerichteten Client möglich ist.

- In „Loud“ hatte der BGH die sekundäre Darlegungslast ohne Bedenken auch auf eine Mehrheit von Anschlussinhabern angewendet (im Fall waren beide beklagten Elternteile Vertragsparteien des Providervertrages mit dem einschlägigen ISP). Dies begegnet zunächst keinen Bedenken, da auch bei einer Mehrheit von Anschlussinhabern es allein in deren Macht und Sphäre liegt, über potentielle Mitnutzer vorzutragen. Im Fall „Loud“ selbst konnte der BGH die sekundäre Darlegungslast als nicht erfüllt ansehen, weil die Eltern ihrer Mitteilungspflicht nicht nachgekommen waren. Es begegnet wiederum keinen Bedenken, in solchen Fällen eine Mittäterschaft anzunehmen, da es für die Geständnisfiktion irrelevant ist, ob der fingierte Sachverhalt auch tatsächlich – wäre er nicht fingiert – vorstellbar wäre.[437] Der BGH lässt damit aber im Unklaren, was in dem – sicher nicht allzu selten auftretenden – Fall gilt, wenn zwei Anschlussinhaber (zum Beispiel zwei Eheleute) vortragen, dass außer ihnen niemand den Anschluss benutzt. In der Konstellation, wo es nur einen Anschlussinhaber gibt, wäre dann die (beabsichtigte) Alleinnutzung des Anschlusses zugestanden und es gälte eine tatsächliche Vermutung (mit einer Wirkung wie ein Anscheinsbeweis) seiner Täterschaft. Würde dies auch bei zwei Anschlussinhabern gelten, wäre die Nutzungssituation „ein Anschlussinhaber - ein Mitnutzer“ gegenüber der Nutzungssituation „zwei Anschlussinhaber“ privilegiert (da in Ersterer der Anschlussinhaber der sekundären Darlegungslast mit dem Vortrag, einen Mitnutzer zu haben, genügen könnte, während hingegen die beiden Anschlussinhaber keine Mitnutzer vortragen könnten). Dies kann nicht richtig sein (Willkürverbot)[438]. Folglich muss dann auch bei einer Mehrheit von Inhabern eines Anschlusses allein auf Grund der Tatsache, dass sie eine Mehrheit von Anschlussinhabern sind und keine Mitnutzer haben, die sekundäre Darlegungslast als erfüllt angesehen werden. Die Zeugenvernehmung, die bei Mitnutzern stattfinden

[437] Dass zwei Anschlussinhaber gemeinschaftlich eine Urheberrechtsverletzung mittels *filesharing* begehen, wäre als echter Lebenssachverhalt in der Tat schwer vorstellbar. Da die Mittäterschaft aber nur fingiert wird, ist dies wie gesagt irrelevant; mithin greifen auch entsprechende Bedenken wie die von *Forch*, GRUR-Prax 2017, 522, 524, nicht.

[438] Siehe Kapitel § 4 VII. 3. b) aa).

würde, ist dann (da beide Anschlussinhaber als Beklagte Parteien des Prozesses sind) durch eine Parteivernehmung (§ 445 ZPO) zu ersetzen.

ee) Ergebnis

Die Bestimmung des Inhalts der sekundären Darlegungslast durch den BGH ist in rechtsdogmatischer Hinsicht überwiegend kritikwürdig, auch wenn sie sich grundsätzlich im verfassungsrechtlich erlaubten Rahmen (wie in Kapitel § 4 VII. 2. dargestellt) bewegt. Zustimmungsfähig ist die Gleichbehandlung der familiären und nicht-familiären Anschlussnutzung im Rahmen der Mitteilungspflicht nur insoweit, als Erkenntnisse mitgeteilt werden müssen, die im Rahmen der Nachforschungspflicht gewonnen wurden, nicht jedoch insoweit, als im Rahmen der familiären Nutzung der Täter mitgeteilt werden muss, falls sich dieser dem Anschlussinhaber gestellt hat. Die Gleichbehandlung von familiärer und nicht-familiärer Nutzung muss stattdessen – entgegen dem BGH – im Rahmen der Nachforschungspflicht gelten.[439] Die Nachforschungspflicht selbst dürfte eigentlich nur dazu verpflichten, nachzuforschen, welche Personen zum Verletzungszeitpunkt entweder per Kabel zum Router verbunden waren (LAN-Verbindung) oder das WLAN-Passwort kannten (geschlossener Betrieb)[440], sofern sie eigene internetfähige Geräte besitzen, die zur *filesharing*-Benutzung geeignet sind.[441] Sofern sie Zugriff auf das Internet nur oder auch über *filesharing*-fähige Geräte des Anschlussinhabers haben, muss auch dies ermittelt und mitgeteilt werden.

Die Mitteilungspflicht beinhaltet – hier ist dem BGH zuzustimmen – die Pflicht zur Mitteilung der im Rahmen der Nachforschung gewonnenen Ergebnisse, also die namentliche Bezeichnung der Personen, die zum Verletzungszeitpunkt entweder eine LAN-Verbindung zum Router hatten oder das WLAN-Passwort kannten (und/oder Geräte des Anschlussinhabers benutzen konnten) sowie deren ladungsfähige Anschrift.[442] Zudem erstreckt sich die Mitteilungspflicht richtigerweise auf solche Personen, die gegenüber dem An-

[439] Im Ergebnis ist dies auf Grund der Entscheidung „Bastei Lübbe“ des EuGH nunmehr der Fall. Jedoch ist auch die dogmatische Begründung des EuGH nicht zustimmungsfähig, siehe Kapitel § 4 VII. 3. c).

[440] Zum offenen Betrieb siehe Kapitel § 5 V. 3. a).

[441] Dies betreffend ist die Rechtsprechung des BGH nicht eindeutig, siehe Kapitel § 5 V. 1.

[442] Zum Problem der Unkenntnis der ladungsfähigen Anschrift seitens des Anschlussinhabers siehe Kapitel § 5 V. 3. c).

schlussinhaber die Urheberrechtsverletzung eingeräumt haben, jedoch nicht – anders BGH – soweit diese Personen Familienangehörige des Anschlussinhabers sind.

c) Dogmatische Analyse der Rechtsprechung des EuGH

Mit der Entscheidung „Bastei Lübbe“[443] erklärt der EuGH die „Afterlife“-Rechtsprechung des BGH mit Art. 8 Abs.1 und 2 InfoSocRL sowie Art. 3 Abs.1 und 2 EnforcementRL für unvereinbar.[444] Im Ergebnis ist ihm zuzustimmen[445]; gilt das auch für die Begründung?

Unproblematisch ist zunächst die generelle Anwendbarkeit der InfoSocRL und EnforcementRL auf nicht-gewerbliche Handlungen, denn diese Richtlinien sind in ihrem Anwendungsbereich nicht auf gewerbliche Handlungen beschränkt.[446] Schwieriger ist allerdings die Frage, ob InfoSocRL und EnforcementRL überhaupt Vorgaben zu Fragen der Darlegungs- und Beweislast im Rahmen eines nationalen Zivilprozesses machen können. Der Generalanwalt hatte auf ein mehr ergebnisorientiertes Verständnis der Richtlinien abgestellt und argumentiert, dass die aus Art. 8 Abs.2 InfoSocRL erwachsende Pflicht, wirksame Rechtsbehelfe zur Durchsetzung des geistigen Eigentums bereitzustellen, eine volle Überprüfung einer nationalen Rechtsprechung erlaube, wenn diese jene Pflicht mittels darlegungs- oder beweisrechtlicher Institute umsetzt.[447] Der EuGH hatte jedoch in einer produkthaftungsrechtlichen Sache entschieden, dass nationale, letztinstanzliche Gerichte aus europarechtlicher Perspektive im Wesentlichen frei darin sind, inwieweit sie die Beweiswürdigung von Tatsacheninstanzen überprüfen.[448] Sowohl eine volle als auch eine sehr eingeschränkte europarechtliche Nachprüfbarkeit der BGH-Rechtsprechung zur sekundären Darlegungslast schien mithin vertretbar. Insofern ist aus der Warte des Bedürfnisses nach dogmatischer Vollständigkeit

[443] EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

[444] Zu den Auswirkungen auf die zukünftige Bestimmung der sekundären Darlegungslast siehe Kapitel § 5 V. 1.

[445] Siehe Kapitel § 4 VII. 3. b) bb).

[446] Vgl. Erwägungsgrund 14 EnforcementRL.

[447] Schlussanträge vom 6. Juni 2018, Rs. C-149/17, Rz. 31 – ECLI:EU:C:2018:400 - „Bastei Lübbe“.

[448] EuGH, Urteil vom 21. Juni 2017, Rs. C-621/15, Rz. 51 – ECLI:EU:C:2017:484 - „W u.a.“.

bedauerlich, dass der EuGH in seinem Urteil in „Bastei Lübbe“ eine vollständige Nachprüfbarkeit für sich in Anspruch nahm, ohne auf dieses Problem ausdrücklich einzugehen; insbesondere hat er damit eine Konturierung des nationalen Spielraums in Fragen der Darlegungs- und Beweislast verpasst.

Die eigentliche Begründung des EuGH leidet zudem an demselben Problem wie des BGH, denn auch der EuGH sieht in seiner Grundrechtsabwägung das Grundrecht auf Achtung des Privat- und Familienlebens (Art. 7 GRC) insofern als betroffen an, als in den einschlägigen Sachverhaltskonstellationen Familienmitglieder verpflichtet werden, sich gegenseitig zu belasten.[449] Das ist jedoch unzutreffend, da sich auf Ebene der Nachforschungspflicht allein die Frage stellt, ob Familienmitglieder untereinander einen Schutz an Privatsphäre genießen, der den Schutz des geistigen Eigentums (Art. 17 Abs.2 GRC) in der Abwägung übertrifft.[450]

Weiterhin „verschleiert“ der EuGH (wohl unbewusst) einen entscheidenden Punkt: Seiner Begründung nach müsse der Schutz des geistigen Eigentums überwiegen, da andernfalls eine Identifizierung des Täters der Urheberrechtsverletzung unmöglich gemacht würde[451]; bei der hier binären Entscheidung zwischen Schutz der Familie und Schutz des geistigen Eigentums müsse also der Schutz der Familie zurückstecken. Jedoch dient das Ergebnis seiner Entscheidung ja gerade nicht dazu, eine Identifizierung des *wahren* Täters der Urheberrechtsverletzung zu ermitteln, sondern die Haftung des Anschlussinhabers qua seiner *vermuteten* Täterschaft zu ermöglichen. Ob die Art. 8 Abs.1 und 2 InfoSocRL sowie Art. 3 Abs.1 und 2 EnforcementRL im Lichte der europäischen Grundrechte mögliche „Kollateralschäden“ (Haftung auf Grund einer Vermutung) in Kauf nehmen, erscheint begründungsbedürftiger als die Schadensersatzhaftung eines erwiesenen Täters zu ermöglichen.

[449] EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 49 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

[450] Siehe Kapitel § 4 VII. 3. b) aa).

[451] EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 51 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

Diesen Begründungsaufwand vermeidet der EuGH.[452]

Im Ergebnis ist die Entscheidung des EuGH daher hinsichtlich ihrer Begründung unbefriedigend.

4. Zum Beweis der Täterschaft des Anschlussinhabers

a) Kategorialer Zuordnungsfehler?

Wie dargestellt, beinhaltet die sekundäre Darlegungslast eine Nachforschungs- und eine Mitteilungspflicht. Die sekundäre Darlegungslast müsste also erfüllt sein, sobald beiden Pflichten nachgekommen wurde. Nach Nennung der Mitnutzer werden diese regelmäßig im Prozess als Zeugen vernommen. Nicht ganz eindeutig war es in der Rechtsprechung des BGH zunächst, ob er es als richtig ansieht, eine Erfüllung der sekundären Darlegungslast zu verneinen, wenn sich nach Vernehmung herausstellt, dass keiner der benannten Mitnutzer als Täter in Betracht kommt, mithin nur noch der Anschlussinhaber als möglicher Täter verbleibt; mithin also, ob der BGH das Ergebnis der Zeugenvernehmung nicht an der Beweislast des Klägers (die darauf gerichtet ist, die Täterschaft des Anschlussinhabers zu beweisen), sondern an der sekundären Darlegungslast des Anschlussinhabers (die darauf gerichtet ist, andere mögliche Mitnutzer des Anschlusses im Verletzungszeitpunkt zu benennen) aufhängt.[453]

Dass Letzteres nicht richtig sein kann, folgt schon daraus, dass – wie nun mehrfach festgehalten – den Anschlussinhaber nur eine sekundäre Darlegungslast trifft, keine (sekundäre) materielle Beweislast betreffend die sekundär vorgetragenen Tatsachen. Ein Beweis der sekundär vorgetragenen Tatsachen ist also nicht nötig; als Beweisthema verbleiben die Tatsachen, die der Kläger im Rahmen *seiner* Darlegungslast vorgetragen hat, mithin die Täterschaft des Anschlussinhabers.

[452] Der Generalanwalt hatte dagegen „das Kind beim Namen genannt“ und ausdrücklich in den Raum gestellt, dass ein Anschlussinhaber möglicherweise rechtsmissbräuchlich handelt, wenn er Familienmitglieder „vorschiebt“ und *deswegen* seine Haftung gerechtfertigt sein könnte, siehe Schlussanträge vom 6. Juni 2018, Rs. C-149/17, Rz. 45f. – ECLI:EU:C:2018:400 - „Bastei Lübbe“. Es pauschal als rechtsmissbräuchlich anzusehen, wenn jemand nicht für eine Tat haften möchte, die er nicht begangen hat, scheint freilich fernliegend.

[453] Ein guter Problemaufriss findet sich bei LG Düsseldorf, Urteil vom 24. Februar 2016, Az. 12 S 2/15, Rz. 16f. – juris.

Weiterhin wäre ein solches Ergebnis auch durch eine Kontrollüberlegung widerlegt: Dass die Beweislast beim Kläger verbleibt, ist unzweifelhaft. Also muss der Beweislast irgendein Anwendungsbereich verbleiben. Dies ist allerdings nicht möglich, wenn alle prozessrelevanten Tatsachen die Täterschaft des Anschlussinhabers betreffend bereits im Rahmen der sekundären Darlegungslast abgehandelt werden.

Die Zuordnung der Würdigung der Zeugenaussagen zur sekundären Darlegungslast oder zur Beweislast ist nicht nur akademischer Natur, sondern macht auch im Ergebnis einen Unterschied, nämlich dann, wenn die Zeugen die Aussage verweigern. Keinen Unterschied macht die Zuordnung dann, wenn sie – wie auch immer – aussagen, da dann allein entscheidend ist, welche Ableitungen aus der Aussage getroffen werden und nicht, wo die Ableitungen verortet werden. Bei einer Zeugnisverweigerung muss jedoch gefragt werden, zu wessen Lasten diese geht. Wird die Erfüllung der sekundären Darlegungslast vom Ergebnis der Zeugenvernehmung abhängig gemacht, so müsste die Verweigerung zu Lasten des Anschlussinhabers gehen. Ist jedoch die sekundäre Darlegungslast bereits mit Benennung der späteren Zeugen erfüllt, so muss es zu Lasten des Klägers gehen, wenn diese ihr Zeugnis verweigern, da er den Beweis der Täterschaft des Anschlussinhabers dann schuldig bleibt.

Entsprechend erfreulich ist daher, dass aus der Entscheidung „Ego-Shooter-Spiel“ nunmehr klarer als früher hervorgeht, dass das Ergebnis der Zeugenvernehmung im Rahmen der Beweislast des Klägers zu behandeln ist.[454] Früheren Entscheidungen war diese Aussage noch nicht so eindeutig zu entnehmen.[455]

b) Zur Würdigung von Zeugenaussagen

Die Beweiswürdigung ist zwar – wie bereits erwähnt – grundsätzlich Aufgabe des Tatrichters, jedoch ist der Prozess der Würdigung (beispielsweise von deren Vollständigkeit und Widerspruchsfreiheit) einer rechtlichen Überprüfung

[454] BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16, Rz. 22ff. – MMR 2018, 311 - „Ego-Shooter-Spiel“. Zu der dogmatischen Bewertung dieser Entscheidung siehe sogleich Kapitel § 4 VII. 4. b).

[455] Siehe nur BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 35ff. und 48ff. – GRUR 2016, 1280 - „Every time we touch“. Der BGH prüft dort das Ergebnis der Zeugenvernehmung, bevor er auf die Prüfung der sekundären Darlegungslast eingeht. Unsicherheit betreffend die Lesart daher auch bei *Forch*, GRUR-Prax 2017, 522, 522.

in der Revisionsinstanz zugänglich.[456]

Nach hiesiger Lesart erachtet es der BGH generell für unproblematisch, wenn die Instanzgerichte nach Vernehmung der behaupteten Mitnutzer als Zeugen den Anschlussinhaber als Täter ansehen, sofern die Mitnutzer nicht als (Allein-)Täter in Betracht kommen.[457]

Hiergegen gibt es zunächst keine Einwände, wenn die Zeugen aus spezifischen Gründen glaubwürdiger erscheinen als der Anschlussinhaber, beispielsweise weil deren Aussagen konkreter, konziser und widerspruchsfreier als die des Anschlussinhabers waren. Problematisch könnte dies jedoch sein, wenn die Täterschaft jedes Nutzers des Internetanschlusses – einschließlich des Anschlussinhabers – als gleich wahrscheinlich erscheint, was dann der Fall sein könnte, wenn der Anschlussinhaber seine Täterschaft verneint und die Mitnutzer eine Zugriffsmöglichkeit auf den Internetanschluss zum Verletzungszeitpunkt verneinen. Dann käme eine Beweiswürdigung, die die Täterschaft des Anschlussinhabers quasi im „Ausschlussverfahren“ annehmen würde, womöglich einer Missachtung der Beweislastverteilung gleich, da dann nicht der Rechteinhaber die Täterschaft des Anschlussinhabers beweisen müsste, sondern die Nichterweislichkeit der sekundär vorgetragenen Tatsachen zu Lasten des Anschlussinhabers gehen würde; diesen träfe also nicht nur die sekundäre Darlegungs-, sondern auch eine sekundäre Beweislast.

Jedoch ist die Prämisse dieses Arguments, nämlich dass die Täterschaft jedes Nutzers des Internetanschlusses – einschließlich des Anschlussinhabers – als gleich wahrscheinlich erscheint, wenn der Anschlussinhaber seine Täterschaft verneint und die Mitnutzer eine Zugriffsmöglichkeit auf den Internetanschluss zum Verletzungszeitpunkt verneinen, unzutreffend. Denn der Anschlussinhaber hat *qua* seiner rechtlichen Hoheit über den Internetanschluss *immer* die Möglichkeit des Zugriffs auf diesen[458]; folglich ist seine Täterschaft *a priori* auch dann wahrscheinlicher als die eines seiner Mitnutzer, wenn das Ergebnis deren Zeugenvernehmung ist, dass das Abstreiten der Urheberrechtsverlet-

[456] BGH, Urteil vom 14. Januar 1993, Az. IX ZR 238/91, Rz. 16 – juris.

[457] Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 38ff. – GRUR 2016, 191 - „Tauschbörse III“ und BGH, Urteil vom 12. Mai 2015, Az. I ZR 48/15, Rz. 35ff. – GRUR 2016, 1280 - „Every time we touch“.

[458] Etwas anderes könnte ausnahmsweise nur gelten, wenn der Anschlussinhaber vortragen kann, dass er die Verwaltung des Anschlusses delegiert hat und der Delegat ihn vom Zugriff auf den Anschluss ausgeschlossen hat.

zung durch den Anschlussinhaber genauso glaubwürdig ist wie Verneinung einer Zugriffsmöglichkeit auf den Anschluss zum Tatzeitpunkt durch die Mitnutzer.[459]

Die Würdigung der Zeugenaussagen mittels des eben dargestellten „Ausschlussverfahrens“ ist mithin dogmatisch zulässig.

5. Zur Entkräftung der tatsächlichen Vermutung

Genügt entweder der Anschlussinhaber seiner sekundären Darlegungslast nicht oder genügt er ihr zwar, jedoch folgt aus der Zeugenvernehmung, dass die Mitnutzer nicht als Täter in Betracht kommen, so kann in beiden Fällen dennoch nicht automatisch geschlussfolgert werden, dass der Anschlussinhaber auch Täter ist. Wie dargestellt, soll die sekundäre Darlegungslast und die anschließende Zeugenvernehmung nur zu Tage fördern, welche Mitnutzer als Täter in Betracht kommen, deren Mitnutzung *beabsichtigt* ist.[460]

Denkbar wäre es jedoch auch dann, wenn es zum Tatzeitpunkt keine Mitnutzer gab, deren Mitnutzung beabsichtigt war, dass ein Dritter die Urheberrechtsverletzung begangen hat. In Betracht kommt beispielsweise das unberechtigte Eindringen in ein geschlossenes WLAN.[461] Dies erscheint jedoch sehr unwahrscheinlich. Schließlich müsste nicht nur das unberechtigte Eindringen in WLANs sehr häufig vorkommen, sondern hinzukommen, dass ein Eindringling das entsprechende WLAN auch für Urheberrechtsverletzungen benutzt. Hierzu ist in empirischer Hinsicht nichts bekannt.

Es erscheint folglich vertretbar, an dieser Stelle einen Anscheinsbeweis für die Täterschaft des Anschlussinhabers anzunehmen, auch wenn das Nichtvorliegen der soeben geschilderten Möglichkeit nicht empirisch gesichert ist. Der BGH spricht von einer tatsächlichen Vermutung der Täterschaft[462], was wegen der identischen Voraussetzungen von tatsächlicher Vermutung und

[459] Zu der Frage, inwiefern die Täterschaft (und nicht nur die Zugriffsmöglichkeit) der Mitnutzer zum Gegenstand der Zeugenvernehmung gemacht werden darf, siehe Kapitel § 5 V. 4.

[460] Siehe Kapitel § 4 VII. 1. d) und 4.

[461] Siehe als Beispiel für ein unberechtigtes Eindringen in mittels WPA2 geschützte WLANs *Schirrmacher*, Details zur KRACK-Attacke: WPA2 ist angeschlagen, aber nicht gänzlich geknackt.

[462] Vgl. nur zuletzt BGH, Urteil vom 30. März 2017, Az. I ZR 19/16, Rz. 29 – GRUR 2017, 1233 - „Loud“.

Anscheinsbeweis[463] ebenfalls vertretbar ist. Unter welchen Voraussetzungen diese als entkräftet angesehen werden kann, ist jedoch offen.[464]

6. Zusammenfassung und Ergebnis

Dogmatisch überzeugend in der Rechtsprechung des BGH vorgenommen wurde die Einordnung und die Abgrenzung der verschiedenen, in diesem Abschnitt der Arbeit vorgestellten prozessualen Institute voneinander, wenn auch erst die Rechtsprechung neueren Datums die erforderliche Klarheit gebracht hat. Ebenfalls überzeugend ist die Aufteilung der sekundären Darlegungslast in eine Nachforschungs- und eine Mitteilungspflicht, wobei Letztere die Mitteilung über die nachgeforschten Umstände enthält sowie die Mitteilung darüber, wenn sich ein Mitnutzer freiwillig als Täter bekannt hat (und gegebenenfalls welcher).

Nicht zuzustimmen ist der ungleichen Behandlung von familiärer und nicht-familiärer Anschlussnutzung im Rahmen der Nachforschungspflicht sowie die Gleichbehandlung von familiärer und nicht-familiärer Anschlussnutzung im Rahmen der Pflicht der namentlichen Mitteilung sich freiwillig als Täter bekennender Mitnutzer.

Zugestimmt werden kann dagegen der vom BGH gebilligten Würdigung der Zeugenaussagen und der Würdigung der Verweigerung von Zeugenaussagen durch die Instanzgerichte sowie der Annahme einer tatsächlichen Vermutung / eines Anscheinsbeweises im Falle der Nichterfüllung der sekundären Darlegungslast.

VIII. Zum 2. und 3. TMGÄndG

1. Einleitung

Im Folgenden wird erörtert, ob die durch das 2. und 3. TMGÄndG geänderten und neu eingebrachten Vorschriften betreffend Anschlussinhabern (insbesondere § 8 Abs.3 und § 7 Abs.4 TMG) dazu geeignet sind, in einer konsistenten und vorhersehbaren Art ausgelegt zu werden, mithin dem Ziel jeder

[463] Siehe Kapitel § 4 VII. 1. b).

[464] Da nach Kenntnis des Verfassers in Verletzungsverfahren nur noch selten eine Hackerattacke auf das WLAN des Beklagten behauptet wird, kann diese Frage für die Zwecke dieser Arbeit auch dahingestellt bleiben.

guten Gesetzgebung, Rechtssicherheit zu stiften, gerecht werden.

Das 2. TMGÄndG erweiterte ausdrücklich nur den Anwendungsbereich des TMG auf WLAN-Anbieter. Nicht ausdrücklich in den Wortlaut aufgenommen wurde, ob als Rechtsfolge ein Unterlassungsanspruch gegen Anschlussinhaber, die der Privilegierung unterfallen, ausscheidet. Vor der Änderung des TMG war der Wortlaut „*nicht verantwortlich*“ in § 8 Abs.1 Satz 1 TMG a.F. so verstanden worden, dass er sich nur auf Schadensersatzansprüche bezieht.[465] Unklar ist, ob der Wortlaut „*nicht verantwortlich*“ nach der Änderung auch Unterlassungsansprüche erfasst. Diese Frage hat sich für die Zukunft durch das 3. TMGÄndG erledigt, da nunmehr nach § 8 Abs.1 Satz 2 TMG n.F. Unterlassunganspruche ausdrücklich ausgeschlossen sind, dafür gemäß § 7 Abs.4 TMG n.F. (unter dessen weiteren Voraussetzungen) ein Anspruch auf „*Sperrung der Nutzung von Informationen*“ besteht.

Die Bedeutung von „*nicht verantwortlich*“ in § 8 Abs.1 Satz 1 TMG a.F. in der Fassung des 2. TMGÄndG kann daher nur für Fälle relevant werden, in denen über Abmahngebühren für die außergerichtliche Geltendmachung eines Unterlassungsanspruches während der Geltung des § 8 Abs.1 Satz 1 TMG a.F. in der Fassung des 2. TMGÄndG gestritten wird. Die Zahl dieser Fälle dürfte wegen des kurzen Geltungszeitraums eher gering sein, zudem sind Anschlussinhaber von der Störerhaftung in den meisten relevanten Konstellationen überhaupt nicht mehr betroffen.[466] Von Interesse ist daher vorrangig die jetzt geltende Rechtslage.

Es soll mithin nur kurz erörtert werden, dass ein Verständnis von „*nicht verantwortlich*“, das Unterlassungsansprüche nicht umfasst, ausgeschlossen ist. Da Wortlaut und Systematik nicht eindeutig sind, wird das Ergebnis im Widerstreit der historischen mit der europarechtskonformen Auslegung bestimmt. Die historische Auslegung spräche für eine Einbeziehung des Unterlassungsanspruches in den Wortlaut: zwar war in der Entwurfsfassung des 2. TMGÄndG ein Absatz 4 zu § 8 TMG vorgesehen, der eine ausdrückliche Beseitigung des Unterlassungsanspruches vorsah, der dann jedoch wieder gestrichen wurde; die Streichung war allerdings aus Gründen veranlasst, die mit dem Unterlassungsanspruch nichts zu tun hatten.[467] Stattdessen sollte aus-

[465] Siehe Kapitel § 2 VIII.
[466] Siehe Kapitel § 4 II. 2. c).
[467] Siehe Kapitel § 2 VIII. Insofern übersehen bei *Lütke/Gramlich*, NJ 2016, 413, 416.

weislich der Gesetzesmaterialien ein Unterlassungsanspruch gegen Anschlussinhaber ausdrücklich ausscheiden, was angesichts der Abwesenheit besserer Argumente bei der Auslegung des Wortlauts maßgeblich zu berücksichtigen wäre.[468] Jedoch ist eine richtlinienkonforme Auslegung gegenüber anderen Auslegungsmethoden vorrangig, also auch bei der Auslegung von „*nicht verantwortlich*“. Da der EuGH in „McFadden“ geurteilt hat, dass Art. 12 ECommerceRL Unterlassungsansprüchen nicht entgegensteht[469], umgekehrt aber klar ist, dass Art. 8 Abs.3 InfoSocRL und Art. 11 Satz EnforcementRL die Möglichkeit von Maßnahmen gegen Vermittler – im deutschen Recht also, mangels anderer Ansprüche, einen Unterlassungsanspruch – gebieten, muss auch nach § 8 Abs.1 Satz 1 TMG a.F. ein Unterlassungsanspruch gegen Diensteanbieter möglich sein.[470]

2. § 8 Abs.3 TMG

Gemäß dem mit dem 2. TMGÄndG eingeführten § 8 Abs.3 TMG gelten die Absätze 1 und 2 des § 8 TMG auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

a) Privilegierung auch für geschlossenes WLAN und LAN?

§ 8 Abs.3 TMG erweitert den Begriff des Diensteanbieters im Sinne des TMG um diejenigen Personen, die anderen Nutzern einen Internetzugang über ein „*drahtloses lokales Netzwerk*“ zur Verfügung stellen. Letzteres ist in § 2 Satz 1 Nr. 2a TMG genauer definiert, wobei die Definition auf eine technische

[468] Siehe Kapitel § 4 IV. 1. d). aA *Lütke/Gramlich*, NJ 2016, 413, 416.

[469] EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 79 – ECLI:EU:C:2016:689 - „McFadden“.

[470] So im Ergebnis *Sesing*, MMR 2016, 507, 510; *Nordemann*, GRUR 2016, 1097, 1100; *Lütke/Gramlich*, NJ 2016, 413, 416f; *Grigorjew*, CR 2016, 701, 704; KG, Beschluss vom 8. Februar 2017, Az. 24 U 117/15 – MMR 2017, 486. Als einem voraussetzungslosen Unterlassungsanspruch nicht gleichwertig dürfte es anzusehen sein, dass auch nach § 8 Abs.1 Satz 2 TMG a.F. in der Fassung des 2. TMGÄndG ein Unterlassungsanspruch dann nicht ausgeschlossen gewesen wäre, wenn der Diensteanbieter mit einem Nutzer absichtlich zusammenarbeitet, um eine Rechtsverletzung zu begehen. Abgesehen davon, dass InfoSocRL und EnforcementRL eine solche Einschränkung nicht enthalten, dürfte bei diesem Tatbestand kaum mehr eine bloße Vermittlungshandlung des Diensteanbieters angenommen werden können, da er nach deutscher Konzeption dann wohl bereits als Mittäter anzusehen wäre.

Abgrenzung von WLAN zu anderen Funknetzwerken, namentlich solche mit nicht bloß lokal begrenzter Reichweite, abzielt.[471]

Der Wortlaut mutet daher abschließend an, sodass eine Differenzierung nach der Art des Betriebs des WLAN innerhalb des Wortlauts ausgeschlossen erscheint. Erst recht ist eine direkte Anwendung des § 8 Abs.3 TMG auf eine kabelgestützte Anschlussteilung (LAN) mittels des Ethernet-Standards[472] ausgeschlossen, da § 2 Satz 1 Nr.2a TMG sich unzweifelhaft nur auf einen bestimmten technischen Standard, nämlich den WLAN-Standard[473], bezieht. Dem Wortlaut nach sind also sowohl der offene als auch der geschlossene Betrieb umfasst, eine Zugangsvermittlung mittels LAN hingegen nicht.

Der Anwendung des § 8 Abs.3 TMG auf den geschlossenen Betrieb eines WLAN könnte mithin nur mittels einer teleologischen Reduktion ausgeschlossen, die Anwendung auf die Zugangsvermittlung über LAN nur mittels einer Analogie eingeschlossen werden. Eine von beiden Lösungen muss jedoch zur Anwendung kommen, da geschlossenes WLAN und LAN in ihren rechtlichen Implikationen keinen Unterschied aufweisen (in beiden Fällen bestimmt der Anschlussinhaber bewusst, wem er Zugang zum Internet vermittelt), eine unterschiedliche Behandlung also willkürlich wäre.

aa) Regelungsziel des Gesetzgebers

Es stellt sich mithin die Frage, was das Regelungsziel des Gesetzgebers war. Hier rächt sich, dass eine klare Formulierung eines Regelungsziels im Gesetzesentwurf zum 2. TMGÄndG versäumt wurde. Ausdrücklich angesprochen wurde zwar ein Mangel an *öffentlichen* WLAN-Zugängen[474], jedoch kann nicht davon ausgegangen werden, dass hier zwischen den möglichen Arten des Betriebs eines WLAN differenziert werden sollte, da auch das Fehlen von WLAN-Zugängen in Hotels und Cafés angesprochen wird[475], dort aber regelmäßig ein Zugang nur per Passwort vermittelt wird. Zudem wurde als Problem das Haftungsrisiko identifiziert[476]; dieses traf allerdings alle Betriebsformen eines WLAN gleichermaßen. Folglich ist davon auszugehen, dass

[471] BT-Drs. 18/6745, S. 17.
[472] Siehe hierzu Kapitel § 1 I. 3. a) aa).
[473] Siehe hierzu Kapitel § 1 II. 3. a) aa).
[474] BT-Drs. 18/6745, S. 1.
[475] BT-Drs. 18/6745, S. 1.
[476] BT-Drs. 18/6745, S. 1.

der Gesetzgeber mit der Privilegierung bezwecken wollte, dass mehr Personen ihren Internetanschluss generell der Öffentlichkeit zur Verfügung stellen oder zumindest ihr Passwort großzügiger aushändigen und somit für einen größeren Kreis an unbestimmten Personen als bisher im öffentlichen Raum ein Internetzugang über WLAN zur Verfügung steht.

Das 2. TMGÄndG sollte also wohl entsprechende Anreize setzen. Diese verfangen jedoch bei privaten Anschlussinhabern nur, wenn sie im Vergleich zu Anschlussinhabern, die ihren Anschluss öffnen, nicht schlechter behandelt werden, da es für einen privaten Anschlussinhaber keine sonstigen Anreize[477] (beispielsweise geschäftlicher Natur) gibt, seinen Anschluss anderen Personen als Familienmitgliedern oder häuslichen Gästen zur Verfügung zu stellen. Dies könnte nahelegen, dass private Anschlussinhaber, die ein geschlossenes WLAN betreiben und ihr Passwort grundsätzlich geheim halten, nicht von der Privilegierung erfasst sein sollten, mithin also der Heimbereich von der Privilegierung ausgeklammert werden sollte. Andererseits steht im Gesetzesentwurf auch, dass die Privilegierung unabhängig davon gilt, zu welchen Zwecken (kommerziellen oder anderen) der Zugang zum Internet vermittelt wird[478]; dies könnte eine Gleichbehandlung aller Betriebsarten implizieren, allerdings auch einen offenen Betrieb voraussetzen.

Stichhaltigstes Argument dafür, dass das Gesetz nicht zwischen den Betriebsarten differenzieren möchte ist, dass in der Gesetzesbegründung erwähnt wird, dass bisher in der Rechtsprechung nicht geklärt gewesen sei, ob die Störerhaftung auch einen Anschlussinhaber treffe, der das Passwort zu einem *geschlossenen* WLAN an andere Nutzer weitergibt[479], dieser Umstand zu einer allgemeinen Rechtsunsicherheit beitrage und diese Rechtsunsicherheit durch das 2. TMGÄndG beseitigt werden solle.[480]

Im Ergebnis erscheint es daher überzeugender, dass § 8 Abs.3 TMG auch auf den geschlossenen Betrieb Anwendung finden soll, eine teleologische Reduktion mithin nicht in Betracht kommt. Eine solche Anwendung durch den BGH ist aber wegen der mangelnden Klarheit des Gesetzesentwurfs nicht

[477] Altruistische Motive hinweg gedacht.
[478] BT-Drs. 18/6745, S. 17.
[479] BT-Drs. 18/6745, S. 7f.
[480] BT-Drs. 18/6745, S. 8.

gesichert.[481]

bb) Gleichbehandlung von WLAN und LAN

Gleiches gilt hinsichtlich einer analogen Anwendung des § 8 Abs.3 TMG auf LAN. Zunächst ist darauf hinzuweisen, dass diese Überlegung nicht dadurch überflüssig wird, dass ein Anschlussinhaber, der mittels LAN den Zugang zum Internet vermittelt, auch als „*Diensteanbieter*“ im Sinne von § 8 Abs.1 Satz 1 TMG angesehen werden könnte, weil die Definition in § 8 Abs.3 TMG nicht abschließend sei („*Die Absätze 1 und 2 gelten auch für Diensteanbieter[...]*“). Dies würde das Problem nur verlagern, da LAN dann immer noch nicht mit WLAN gleichbehandelt werden würde, da § 7 Abs.4 TMG ausdrücklich nur auf Diensteanbieter gemäß § 8 Abs.3 TMG Anwendung findet.[482] Für LAN würde dann eigentlich § 8 Abs.1 Satz 2 TMG gelten (der jegliche Haftung ausschließt), was jedoch wiederum dadurch verkompliziert wird, dass (in dem ersten instanzgerlichten Urteil zur Norm) das LG München I den Begriff des „*Diensteanbieters*“ in § 8 Abs.1 Satz 2 TMG mittels einer verfassungs-und richtlinienkonformen Auslegung so versteht, dass dieser nur Diensteanbieter im Sinne von § 8 Abs.3 TMG meint.[483] Die Komplikationen werden dann noch einmal um eine Stufe gesteigert, da Anschlussinhaber, die den Zugang mittels LAN vermitteln, zuletzt immer noch als Diensteanbieter im Sinne von § 8 Abs.1 Satz 1 TMG angesehen werden könnten, was wiederum die Frage aufwerfen würde, wie „*nicht verantwortlich*“ in der Norm dann auszulegen wäre.[484]

In jedem Fall verbliebe aber eine Ungleichbehandlung zwischen geschlossenem WLAN und LAN im Heimbereich, obwohl diese inhaltlich keine beachtenswerten Unterschiede aufweisen.[485] Wenn möglich, sollte diese Ungleich-

[481] Ganz abgesehen davon, dass der BGH sich ohnehin große methodische Freiheiten herausnimmt, siehe Kapitel § 4 IV. 1. f).

[482] Überlegungen zu einer analogen Anwendung des § 7 Abs.4 TMG auf Anschlussinhaber, die den Zugang mittels LAN vermitteln bei *Köhler*, Die Haftung privater Internetanschlussinhaber, S. 213f.

[483] LG München I, Endurteil vom 1. Februar 2018, Az. 7 O 17752/17 – MMR 2018, 322. Bestätigt durch OLG München, Urteil vom 14. Juni 2018, Az. 29 U 732/18 – GRUR 2018, 1050.

[484] Siehe hierzu Kapitel § 4 VIII. 1.

[485] Die schnellere Übertragungsgeschwindigkeit von LAN und damit auch die schnellere Übertragungsgeschwindigkeit bei *filesharing* ist nur ein gradueller Unterschied, der nicht als echtes Differenzierungskriterium taugt.

behandlung also vermieden werden. Eine Vermeidung im Wege der verfassungskonformen Auslegung scheidet jedoch aus. Zu beachten ist nämlich, dass die Gerichte bei der Rechtsanwendung zwar einem Willkürverbot unterliegen[486], jedoch eine verfassungskonforme Auslegung nicht die Wortlautgrenze überschreiten darf[487]. Die regulären Anforderungen an eine Analogie dürfen also nicht durch eine verfassungskonforme Auslegung unterlaufen werden.

Hinsichtlich der Voraussetzungen einer Analogie lässt sich hier Folgendes festhalten: Eine vergleichbare Interessenlage lässt sich leicht bejahen, da wie gesagt zwischen geschlossenem WLAN und LAN keine inhaltlichen Unterschiede bestehen. Schwierigkeiten bereitet aber die Feststellung einer planwidrigen Regelungslücke. Gegen eine solche spricht, dass die Materialien den WLAN-Standard gegenüber anderen Formen drahtloser Netzwerke abgrenzen[488], die Materialien also augenscheinlich in Kenntnis der technischen Umstände abgefasst wurden, mithin der Begriff „*drahtlos*“ ganz bewusst alle Formen der drahtgebundenen Verbindung ausschließen sollte. Hiergegen ließe sich jedoch einwenden, dass der Gesetzgeber wohl generell die Rechtsunsicherheiten der Anschlussteilung im Heimbereich abmildern wollte.[489] Erhebliche Rechtsunsicherheiten würden sich jedoch bei Mischbetrieben ergeben, wenn nämlich – was nicht unüblich ist – manche Geräte zum Router per Kabel (vor allem Smart-TVs und PCs), andere Geräte hingegen per WLAN (Smartphones, Tablets) zum Router verbunden sind. Ein Anschlussinhaber in dieser Konstellation könnte dann überhaupt nicht vorhersehen, welche Rechtslage nun ihn betreffend gilt. Es wäre also zu schlussfolgern, dass die Materialien zum 2. TMGÄndG[490] zwar generell technisch informiert abgefasst wurden, der Sonderfall der kabelgestützten Verbindung im Heimbereich jedoch übersehen wurde. Dafür spricht auch, dass die Materialien WLAN gegenüber anderen drahtlosen Netzwerken deshalb abgrenzen, weil es Letzteren anders als Ersterem am lokalen Bezug fehle.[491] Wenn es dem Gesetzgeber

[486] BVerfG, Beschluss vom 28. Juli 2015, Az. 2 BvR 2558/14, 2 BvR 2571/14, 2 BvR 2573/14, Rz. 74 – bverfg.de, mit weiteren Nachweisen.

[487] BVerfG, Beschluss vom 28. Juli 2015, Az. 2 BvR 2558/14, 2 BvR 2571/14, 2 BvR 2573/14, Rz. 46 – bverfg.de.

[488] BT-Drs. 18/6745, S. 17.

[489] Siehe oben Kapitel § 4 VIII. 2. a) aa).

[490] Anders als die Materialien zum 3. TMGÄndG, siehe hierzu Kapitel § 4 VIII. 3. d).

[491] BT-Drs. 18/6745, S. 17.

jedoch auf den lokalen Bezug ankommt, liegt nahe, dass er übersehen hat, dass auch LAN einen solchen aufweist.

Im Ergebnis lässt sich also vertretbar argumentieren, dass die Voraussetzungen einer Analogie vorliegen, jedoch erscheint dies nicht zwingend.

cc) Lösungsweg des BGH

Der BGH hat in der Entscheidung „Dead Island“[492] mittlerweile die analoge Anwendung des § 7 Abs.4 TMG auf die drahtgebundene Anschlussteilung bejaht.[493] Die Begründung, dass die Analogie aus Gründen der Richtlinienkonformität zwingend angezeigt sei[494], ist jedoch unzutreffend, da es auch richtlinienkonform wäre, auf die drahtgebundene Anschlussteilung die Störerhaftung anzuwenden – methodisch auf demselben Weg, wie es auch bei ISPs getan wird.[495] Die eigentliche Begründung der Analogie aus der Vergleichbarkeit der drahtgebundenen und drahtlosen Anschlussteilung heraus ist etwas knapp geraten[496]; ihr kann jedoch – sofern die drahtgebundene Anschlussteilung per LAN geschieht – zugestimmt werden.

b) Privilegierung auch für andere Formen der Anschlussteilung?

Problematisch ist, dass der BGH § 7 Abs.4 TMG auch im Hinblick auf die Anschlussteilung mittels einer Tor-Exitnode anwendet.[497] Wie soeben dargestellt[498] ist die vom Verfasser vertretene Vergleichbarkeit von drahtgebundener und drahtloser Anschlussteilung nur gerechtfertigt, sofern bei beiden der lokale Bezug gegeben ist. Bei der Anschlussteilung mittels LAN ist dies der Fall, da der Nutzer, der sich mittels LAN zu einem Anschluss verbindet, nur eine geringe räumliche Entfernung zum Router aufweisen kann. Wer hingegen als Tor-Exitnode fungiert, vermittelt theoretisch den Datenverkehr von

[492] Siehe hierzu Kapitel § 2 XI. 6.
[493] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 44ff. – GRUR 2018, 1044 - „Dead Island“.
[494] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 44ff. – GRUR 2018, 1044 - „Dead Island“.
[495] Siehe § 4 VIII. 10.
[496] Vgl. BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 49 – GRUR 2018, 1044 - „Dead Island“.
[497] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 44 – GRUR 2018, 1044 - „Dead Island“.
[498] Siehe Kapitel § 4 VIII. 2. a).

Tor-Nutzern von jedem beliebigen Punkt auf der Erde ins offene Internet, sodass es am lokalen Bezug fehlt.

Dem BGH kann also nicht beigepflichtet werden, sofern sich der Analogieschluss auf Tor-Exitnodes bezieht. Methodisch richtig wäre es gewesen, gegen diese (wie gegen ISPs auch) grundsätzlich die Störerhaftung zu ermöglichen.[499]

c) Privilegierung für private und gewerbliche Diensteanbieter

Weniger Probleme als die Frage der Anwendbarkeit des § 8 Abs.3 TMG auf geschlossenes WLAN und LAN bereitet dagegen die Frage, ob § 8 Abs.3 TMG nur für Anschlussinhaber gilt, die ihren Anschluss anderen Personen aus gewerblichen bzw. kommerziellen Gründen zur Verfügung stellen oder auch für solche, die dies aus privaten Gründen tun. Im TMG ist dies nicht ausdrücklich zur Sprache gebracht worden, dafür aber in der Gesetzesbegründung[500], sodass eine historische Auslegung dieses Ergebnis nahelegt, und umgekehrt andere Auslegungsmethoden nichts anderes ergeben.[501]

Dies gilt insbesondere auch für die richtlinienkonforme Auslegung. Zwar entschied der EuGH in „McFadden“, dass WLAN-Anbieter und generell andere Zugangsvermittler nur dann als Diensteanbieter im Sinne von Art. 2 lit.a) ECommerceRL angesehen werden können, wenn die Zugangsvermittlung einen gewerblichen Hintergrund hat.[502] Jedoch ist zu berücksichtigen, dass nationale Gesetze, die eine Richtlinie umsetzen, mehr als eine bloße Umsetzung derselben sein und also einen Bedeutungsgehalt über die Umsetzung hinaus enthalten können. Dies gilt bis hinunter zu einzelnen Begriffen eines gesetzlichen Tatbestandes. So wird beispielsweise für den Begriff des Mangels in § 434 Abs.1 BGB diskutiert, ob dieser in Anwendungsfällen außerhalb der VerbrauchsgüterkaufsRL anders auszulegen ist als innerhalb.[503] Folglich kann es grundsätzlich auch zulässig sein, den Begriff des „*Diensteanbieters*“ auf zwei verschiedene Arten zu verstehen, nämlich betreffend ge-

499 Siehe Kapitel § 4 VIII. 10.

500 BT-Drs. 18/6745, S. 8.

501 Vielmehr legt auch eine verfassungskonforme Auslegung dieses Ergebnis nahe, siehe *Grigorjew*, CR 2016, 701, 704.

502 EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 42f. – ECLI:EU:C:2016:689 - „McFadden“. Siehe auch Kapitel § 2 IX.

503 *Möllers*, Juristische Methodenlehre, S. 292.

werblichen Diensteanbietern als Umsetzung der ECommerceRL, betreffend privaten Diensteanbietern als national verordnete Gleichstellung derselben mit den gewerblichen statt als strikte Bindung der Auslegung des „*Diensteanbieters*“ im TMG an die Auslegung des „*Diensteanbieters*“ in der ECommerceRL. Der EuGH hat solch eine „*gespaltene Auslegung*“[504] ausdrücklich gebilligt.[505]

Eine gespaltene Auslegung setzt allerdings voraus, dass die ECommerceRL keine Vollharmonisierung dahingehend anstrebt, dass alle Diensteanbieter, die keine Diensteanbieter im Sinne der Richtlinie sind, durch nationale Vorschriften keine Privilegierung erfahren dürfen, die den Privilegierungen der ECommerceRL gleichkommt. Zwar ist es allgemeine Meinung, dass die Art. 12ff. ECommerceRL vollharmonisierend sind[506]; kein überwiegendes Meinungsbild gibt es jedoch betreffend die Frage, ob auch die Begriffe „*Dienste*“ und „*Diensteanbieter*“ in Art. 2 lit. a) und b) ECommerceRL vollharmonisiert sind. Stimmen aus der Literatur lehnen dies allerdings ab.[507] Dem ist im Ergebnis zuzustimmen. Die ECommerceRL ist nicht aus der Perspektive der Inhaber von Rechten des geistigen Eigentums, sondern aus der Perspektive der Erbringer von Diensten der Informationsgesellschaft geschrieben.[508] Ihr Gegenstand ist also nicht, welche Dienste maximal erlaubt sein dürfen, sondern, was gewerblichen Diensteanbietern minimal (EU-weit einheitlich) erlaubt ist. Folglich sind private Diensteanbieter aus Art. 12 ECommerceRL nicht ausgeschlossen, sondern nur ausgeklammert. Sie dürfen daher durch nationale Vorschriften den Diensteanbietern der ECommerceRL gleichgestellt werden, solange die Limitierungen der InfoSocRL und der EnforcementRL beachtet werden.

Im Ergebnis kann § 8 Abs.3 TMG daher zuverlässig so ausgelegt werden, dass ihm Anschlussinhaber unabhängig davon unterfallen, ob sie den Zugang zum

---

504 *Möllers*, Juristische Methodenlehre, S. 291f.

505 EuGH, Urteil vom 17. Juli 1997, Rs. C-28/95, Rz. 33 – ECLI:EU:C:1997:369 - „A. Leur-Bloem“.

506 *Spindler*, ZUM 2017, 473, 478, mit zahlreichen Nachweisen. In der Rechtsprechung der Höchstgerichte ist anerkannt, dass für jeden einzelnen Regelungsbestandteil einer Richtlinie nach deren Harmonisierungsgrad zu fragen ist, siehe BVerfG, Beschluss vom 6. November 2019, Az. 1 BvR 276/17, Rz. 78ff. – bverfg.de - „Recht auf Vergessen II“, mit Nachweisen der Rechtsprechung des EuGH.

507 *Köhler*, Die Haftung privater Internetanschlussinhaber, S. 208f.

508 Vgl. nur Erwägungsgründe 4ff. ECommerceRL.

Internet aus gewerblichen oder privaten Gründen vermitteln.

d) Darlegungs- und Beweislast

Da die Frage, ob und wenn ja, inwiefern der Anschlussinhaber die Darlegungs- und Beweislast für die tatsächlichen Voraussetzungen des § 8 Abs.3 TMG (analog) trägt, nicht von der Frage des Verhältnisses des TMG zur sekundären Darlegungslast des Anschlussinhabers im Sinne von Kapitel § 4 VII. 1. c) und 3. getrennt werden kann, werden beide Fragen zusammen in Kapitel § 4 VIII. 4. b) behandelt.

3. § 7 Abs.4 TMG

Gemäß dem mit dem 3. TMGÄndG eingeführten § 7 Abs.4 Satz 1 TMG kann bei Vorliegen bestimmter Tatbestandsvoraussetzungen als Rechtsfolge von einem Diensteanbieter im Sinne des § 8 Abs.3 TMG die „*Sperrung der Nutzung von Informationen*“ verlangt werden.

a) „Verletzung des geistigen Eigentums“

Erste Anspruchsvoraussetzung des § 7 Abs.4 Satz 1 TMG ist die Verletzung geistigen Eigentums.

Der Begriff „geistiges Eigentum“ ist offensichtlich der EnforcementRL entnommen (Art. 1 EnforcementRL). Unzweifelhaft sind das für *filesharing* relevante Urheberrecht (sowie das in Zukunft möglicherweise relevante Patent- und Designrecht[509]) geistiges Eigentum.

b) „Telemediendienst“

Zweite Anspruchsvoraussetzung des § 7 Abs.4 Satz 1 TMG ist, dass ein Telemediendienst von einem Nutzer in Anspruch genommen wurde, um das Recht am geistigen Eigentum eines anderen zu verletzen.

Der Begriff „*Telemediendienst*“ existierte bisher im TMG nicht; es ist davon auszugehen, dass der Gesetzgeber „*Telemedien*“ im Sinne von § 1 Abs.1 TMG gemeint hat[510], also alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht ausschließlich die Übertragung von Signalen

[509] Siehe Kapitel § 3 XI. 2. e).
[510] *Nicolai*, ZUM 2018, 33, 36.

über Telekommunikationsnetze betreffen. Da gegenwärtig der praktisch einzig relevante Anwendungsfall von § 7 Abs.4 TMG Urheberrechtsverletzungen sind, die darin bestehen, dass über einen Internetanschluss Dateien bzw. Dateifragmente in einem *filesharing*-System übertragen werden[511], müssten also die hierzu benutzten *filesharing*-Clients oder – soweit ein Webbrowser für P2P-Streaming[512] benutzt wird – der Webbrowser, bzw. der hierin aufgerufene Dienst, als Telemedium anzusehen sein. Dies ist der Fall, da „*Telemedien*" ein weit zu fassender Oberbegriff für Medien aller Art ist, soweit diese elektronisch zur Verfügung stehen[513] und die Gesetzesbegründung zum 3. TMGÄndG vorsieht, dass der Anspruch gegen „*Peer-to-Peer Netzwerke*" gerichtet ist[514], was sinnlos wäre, wenn diese nicht unter den Tatbestand fallen würden.[515]

Das ist insofern wichtig, da § 7 Abs.4 TMG praktisch irrelevant wäre, wenn er das *filesharing* nicht erfassen würde. Schließlich lassen sich andere Formen der Urheberrechtsverletzung oder Verletzung anderer Rechte des geistigen Eigentums über einen Internetanschluss regelmäßig nicht ermitteln.[516]

c) Kausalität

Anders als bei Netzsperren gegen ISPs ist die Kausalität zwischen Inanspruchnahme eines Telemediendienstes und der Verletzung geistigen Eigentums bei § 7 Abs.4 TMG unproblematisch. Bei Netzsperren gegen ISPs macht dieses Merkmal deshalb Schwierigkeiten, weil das verletzende Online-Angebot, das gesperrt werden soll, auch ohne die Vermittlung des ISPs existiert und für dessen Kunden (durch Hilfsmittel wie alternative DNS-Resolver) aufrufbar ist, folglich die Vermittlung keine *conditio sine qua non* für die Verletzung darstellt.[517] In § 7 Abs.4 TMG lässt sich jedoch die Nutzung des Internetanschlusses nicht hinwegdenken, ohne dass die konkret über

511 Siehe Kapitel § 3 IV.
512 Siehe Kapitel § 3 XI. 2. a).
513 *Martini* in: Gersdorf/Paal, BeckOK InfoMedienR, 31. Ed. 2021, § 1 TMG, Rz. 8.
514 BT-Drs. 18/12202, S. 12.
515 So im Ergebnis auch *Nicolai*, ZUM 2018, 33, 36 und *Spindler*, NJW 2017, 2305, 2306.
516 Siehe Kapitel § 3 IV.
517 *Sesing/Baumann*, K&R 2018, 461, 464. Nach der Rechtsprechung des BGH stellt das Entfallen des Beitrags von Intermediären jedoch lediglich einen hypothetischen Kausalverlauf dar, der die Ursächlichkeit des Beitrags für die Verletzung nicht entfallen lässt, siehe BGH, Urteil vom 15. Oktober 2020, Az. I ZR 13/19, Rz. 19 – MMR 2021, 138 - „Störerhaftung des Registrars".

diesen begangene Verletzungshandlung entfiele.

d) „Keine andere Möglichkeit der Abhilfe“

Dritte Anspruchsvoraussetzung des § 7 Abs.4 Satz 1 TMG ist, dass dem Inhaber des verletzten Rechts keine andere Möglichkeit zur Verfügung steht, der Verletzung seines Rechts abzuhelfen, als den Diensteanbieter nach § 8 Abs.3 TMG in Anspruch zu nehmen.

aa) Übersicht

Die Inanspruchnahme eines Internetanschlussinhabers ist also subsidiär. Die Gesetzesbegründung bezeichnet sie ausdrücklich als „*letztes Mittel*“.[518] Genauer schreibt die Gesetzesbegründung vor, dass der Rechteinhaber gegen diejenigen Beteiligten vorgehen müsse, die die Rechtsverletzung selbst begangen oder zu ihr durch die Erbringung von Dienstleistungen beigetragen haben. Für erstere Variante wird als Beispiel der „*Betreiber der Internetseite*“, für letztere Variante der „*Host-Provider*“ genannt. Um diese Beteiligten zu ermitteln, müsse der Rechteinhaber zumutbare Nachforschungen anstellen. Anschließend müsse er zumutbare Anstrengungen unternehmen, um Erstere in Anspruch zu nehmen; nur wenn dies scheitert oder dem jede Erfolgsaussicht fehlt, dürfe zuletzt der Anschlussinhaber in Anspruch genommen werden.[519]

Hierzu im Einzelnen:

bb) Einschlägige Beteiligte

Aus dem Kreis der im Rahmen von § 7 Abs.4 Satz 1 TMG einschlägigen Beteiligten lässt sich zunächst ohne weiteres derjenige Nutzer ausscheiden, der den Anschluss für die einschlägige Rechtsverletzung benutzt hat. Denn wenn der Anschlussinhaber gerichtlich nach § 7 Abs.4 TMG in Anspruch genommen wird, dann nur, weil dieser Nutzer nicht ermittelbar war oder er

[518] BT-Drs. 18/12202, S. 12.
[519] BT-Drs. 18/12202, S. 12.

bereits in Anspruch genommen wurde oder wird.[520]

Im Übrigen lassen sich jedoch kaum sinnvolle Eingrenzungen machen. Ob dem Gesetzgeber bewusst war, womit er in technischer Hinsicht eigentlich genau zu tun hat, ist angesichts der gegebenen Beispiele potentiell Beteiligter (Webseitenbetreiber, Host-Provider) höchst fraglich. Da § 7 Abs.4 TMG praktisch ausschließlich für *filesharing* relevant werden kann[521] und *filesharing* gegenwärtig fast ausschließlich mittels BitTorrent stattfindet[522], können zu einer Rechtsverletzung im Sinne des § 7 Abs.4 Satz 1 TMG eine kaum überschaubare Zahl an Akteuren beigetragen haben.

Hierzu ein fiktives, aber *in praxi* denkbares Beispiel: ein Nutzer, der ein urheberrechtliches geschütztes Werk mittels *filesharing* erlangen will, sucht zunächst über eine Suchmaschine wie *Google*[523] nach einer Metasuchmaschine für BitTorrent[524], findet schließlich eine und sucht in dieser nach dem gewünschten Werk. Die Suchmaschine schlägt ihm mehrere Indexseiten[525] vor, die entsprechende .torrent-Container[526] oder *magnet links*[527] enthalten. Der Nutzer möchte eine der Indexseiten ansteuern, jedoch löst der DNS-Resolver seines ISP[528] die Domain wegen einer Netzsperre nicht auf. Daher greift der Nutzer auf einen alternativen DNS-Resolver[529] zurück. Die Indexseite selbst wird auf einem Drittanbieter gehostet[530], hat von einem Registrar[531] eine Domain erhalten, verwendet einen verteilten Nameserver[532] und hat für die Verwendung von HTTPS von einer autorisierten Zertifizierungsstelle ein TLS-Zertifikat[533] erhalten. Sie finanziert sich mittels Werbung sowie Spen-

[520] Dass ein Rechteinhaber die Geltendmachung einer Schadensersatzforderung gegen diesen unterlässt, erscheint unwahrscheinlich. Ist der Nutzer dem Rechteinhaber allerdings bekannt und weigert sich dieser gegen jenen vorzugehen, so wäre ihm der Anspruch aus § 7 Abs.4 TMG gegen den Anschlussinhaber auf Grund Subsidiarität richtigerweise zu versagen.

[521] Siehe Kapitel § 3 IV.

[522] Siehe Kapitel § 1 II. 4. f).

[523] Siehe Kapitel § 1 V. 4. e).

[524] Siehe Kapitel § 1 V. 4. e).

[525] Siehe Kapitel § 1 II. 5. a) aa).

[526] Siehe Kapitel § 1 II. 5. a) aa).

[527] Siehe Kapitel § 1 II. 5. a) cc).

[528] Siehe Kapitel § 1 V. 1. b) cc).

[529] Siehe Kapitel § 1 V. 4. b).

[530] Siehe Kapitel § 1 V. 4. f).

[531] Siehe Kapitel § 1 V. 4. c).

[532] Siehe Kapitel § 1 V. 4. c).

[533] Siehe Kapitel § 1 V. 4. h).

den auf ein PayPal-Konto[534]. Der Nutzer erhält auf der Indexseite schließlich einen *magnet link* mit einem Hashwert[535], der die gewünschte Datei repräsentiert, und die IPs mehrerer Tracker.[536] Der Nutzer hat zudem in seinem BitTorrent-Client eine Verbindung zur Mainline DHT[537] aktiviert, sodass für den Hashwert auch über die DHT – und somit über die Nutzer in der DHT – nach Partnern für den Dateiaustausch gesucht wird.

Theoretisch lässt sich der Subsidiaritäts-Tatbestand also so auslegen, dass der Rechteinhaber gegen alle diese Beteiligten vorgehen müsste. Wer hiergegen einwenden möchte, dass dies viel zu weitgehend wäre, müsste umgekehrt darlegen können, welche Begrenzung gerechtfertigt ist und wieso. Irgendeinen Inhalt muss der Tatbestand wegen des Verbots der Normderogation[538] haben. Der Verweis auf die in der Gesetzesbegründung genannten Beispiele hilft nicht weiter, da es sich hierbei erstens nur um Beispiele handelt und zweitens nicht einzusehen ist, warum beispielsweise der Anbieter des Hostservers als Beteiligter in Frage kommen sollte, beispielsweise der Anbieter des Trackers aber nicht, obwohl Letzterer „näher“ an dem *filesharing*-Vorgang ist als Ersterer. Ebenfalls erscheint es nicht plausibel, nur bestimmte Beteiligungsformen im rechtlichen Sinne als einschlägig zu erachten (beispielsweise nur Täterschaft und Beihilfe, nicht aber die Störerhaftung). Zwar wird man zumindest irgendeine rechtlich relevante Beteiligungsform, also mindestens Störerhaftung (die anwendbare Rechtsordnung zunächst ausgeklammert) fordern müssen, da die Inanspruchnahme des entsprechenden Beteiligten zumindest eine gewisse Erfolgsaussicht haben muss (hierzu sogleich); eine Begrenzung auf Täterschaft und Teilnahme lässt sich aber weder dem Gesetz noch der Gesetzesbegründung entnehmen (Letztere spricht nur von einem „*Beitrag*“) noch verbliebe dem Tatbestand dann noch ein ausreichender Anwendungsbereich, da außer für die Betreiber von Indexseiten[539] bisher für die übrigen hier diskutierten Akteure keine Haftung als Täter- oder Teilnehmer letztinstanzlich anerkannt worden ist. Ein weiterer Widerspruch ergäbe sich zur Gesetzesbegründung dahingehend, dass diese als Beispiel Hostserver nennt und für deren Betreiber gerichtlich bisher lediglich die Störerhaftung

534 Siehe Kapitel § 1 V. 4. l).
535 Siehe Kapitel § 1 II. 4. d).
536 Siehe Kapitel § 1 II. 5. a) aa).
537 Siehe Kapitel § 1 II. 5. a) bb).
538 Siehe *Möllers*, Juristische Methodenlehre, S. 164, 173.
539 Siehe hierzu Kapitel § 5 II. 1.

etabliert ist.[540]

Erschwerend kommt hinzu, dass auch eine Beschränkung auf deutsche Gerichtsstände und deutsches Recht nicht gesichert ist. Das Subsidiaritätskriterium wurde schon vor dem 3. TMGÄndG durch den BGH im Rahmen seiner Netzsperren-Rechtsprechung für ISPs geschaffen.[541] In der Literatur wird vorgeschlagen, die dort aufgestellten Kriterien auch im Rahmen von § 7 Abs.4 Satz 1 TMG anzuwenden.[542] Dies überzeugt insoweit, als diese nicht in der Gesetzesbegründung zum 3. TMGÄndG genannt oder strenger als diese sind, da es unter der Geltung des Willkürverbots nicht einzusehen wäre, ISPs mildere Vorschriften aufzuerlegen als Internetanschlussinhabern. Zudem zeigt ein Blick auf das Netzsperren-Urteil „Störerhaftung des Access-Providers", dass die Gesetzesbegründung teilweise von der dortigen Rz. 82 abgeschrieben hat.[543] Die Mindestkriterien dieses Urteils sind also auf § 7 Abs.4 TMG zu übertragen. Dabei ergibt sich, dass der BGH auch eine Rechtsverfolgung im Ausland als notwendig erachtet.[544] Eine Beschränkung auf deutsche Gerichtsstände und deutsches Recht scheint daher nicht angezeigt und wäre auf Grund der Ubiquität des Internets auch willkürlich.

Soweit man dieser Rechtsprechung eine Begrenzung der vorrangig in Anspruch zu nehmenden Akteure entnehmen wollte, würde sich eine solche Lesart zur Gesetzesbegründung (die – wie dargestellt – bestimmte Akteure nur beispielhaft aufzählt) in Widerspruch setzen; und der Gesetzesbegründung ist bei der Gesetzesauslegung in Abwesenheit von besseren Argumenten (von

[540] Siehe Kapitel § 1 V. 4. f).

[541] BGH, Urteil vom 26. November 2015, Az. I ZR 174/14 – GRUR 2016, 268 - „Störerhaftung des Access-Providers"; BGH, Urteil vom 26. November 2015, Az. I ZR 3/14 – MMR 2016, 188. Bisher hatte der BGH keine Gelegenheit, dieses Kriterium weiterzuentwickeln, vgl. BGH, Urteil vom 15. Oktober 2020, Az. I ZR 13/19, Rz. 40ff. – MMR 2021, 138 - „Störerhaftung des Registrars".

[542] *Spindler*, NJW 2017, 2305, 2306; *Mantz*, GRUR 2017, 969, 972.

[543] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 82 – GRUR 2016, 268 - „Störerhaftung des Access-Providers" und BT-Drs. 18/12202, S. 12.

[544] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 86f. – GRUR 2016, 268 - „Störerhaftung des Access-Providers".

denen hier keine ersichtlich sind) der Vorrang zu geben.[545] Ohnehin nennt aber auch der BGH den Webseitenbetreiber und den Hostserver nur als Beispiel[546]: Die Äußerung in Rz. 82, dass nur gegen den Webseitenbetreiber und den Hostserver, nicht jedoch gegen eine Vielzahl von Anbietern vorgegangen werden müsse, bezieht sich erstens nur auf den konkret entschiedenen Fall; zweitens bezieht sich der Verweis auf die „*Vielzahl von Anbietern*“ auf diejenigen Nutzer, die die rechtswidrigen Angebote auf der Webseite, für die der Zugriff gesperrt werden soll, eingestellt haben. Das wären auf BitTorrent übertragen diejenigen Nutzer, die .torrent-Container oder *magnet links* auf Indexseiten einstellen. Die Notwendigkeit eines Vorgehens gegen diese ergibt sich auch nach hiesiger Auslegung nicht aus der Gesetzesbegründung. Die oben genannten Dienste (wie beispielsweise alternative DNS-Resolver oder Registrare) leisten dagegen genauso wie Hostserver einen wichtigen Beitrag dafür, dass die Indexseite als Plattform für Rechtsverletzungen im Internet zur Verfügung steht. Ihr Beitrag kann häufig auch wichtiger sein als der des Hostserver-Anbieters, da sich Letzterer wegen der geringen Speicheranforderungen von Indexseiten[547] gegebenenfalls leichter ersetzen lässt als beispielsweise eine Domain.

Im Ergebnis lässt sich dem Tatbestand der Subsidiarität also auch unter Heranziehung der Gesetzesbegründung und der Netzsperren-Rechtsprechung des BGH keine sinnvolle Eingrenzung dahingehend entnehmen, welche Beteiligten in Anspruch zu nehmen sind. Folglich ist nach hiesiger Auffassung vorrangig gegen alle Akteure vorzugehen, die einen strukturellen Beitrag dazu leisten, dass *filesharing*, insbesondere BitTorrent-*filesharing*, betrieben werden kann, gleich an welchem Gerichtsstandort und gleich nach welchem anwendbaren Recht.

[545] Siehe Kapitel § 4 IV. 1. d). Folglich kann auch der in der Instanzrechtsprechung teilweise vertretenen Auffassung (vgl. beispielsweise OLG München, Urteil vom 14. Juni 2018, Az. 29 U 732/18, Rz. 54 – GRUR 2018, 1050), das Subsdiaritätskriterium sei weniger streng zu verstehen, jedenfalls im Rahmen der direkten Anwendung des § 7 Abs.4 TMG nicht beigepflichtet werden. Ob dies auch für die dort behandelte Frage der analogen Anwendung des § 7 Abs.4 TMG auf ISP gilt, kann vorliegend dahinstehen, scheint aber vor dem Hintergrund, dass eine analoge Anwendung gerade in eine Gesetzeslücke stoßen soll und daher nicht den von den Gesetzesbegründung angedachten Fall betrifft, vertretbar.

[546] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 82 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

[547] Siehe Kapitel § 1 II. 5. a) cc).

cc) Ermittlung der einschlägigen Beteiligten

Laut der Gesetzesbegründung muss der Rechteinhaber zumutbare Nachforschungen anstellen, um zu ermitteln, welche Beteiligten in Frage kommen und wer diese sind.[548] Überträgt man richtigerweise die Netzsperren-Rechtsprechung auch in diesem Punkt[549], gehören zu den zumutbaren Nachforschungen Strafanzeigen, private Ermittler sowie Auskunftsklagen gegen Intermediäre – gegebenenfalls auch im Ausland.[550] Weiterhin genügt es nicht, es bei dem gescheiterten Versuch der Zustellung einer erlangten einstweiligen Verfügung zu belassen.[551]

Problematisch ist in allen Fällen, dass dem Rechteinhaber in BitTorrent-Fällen nur der Hashwert der Zieldatei und gegebenenfalls (einer) der Tracker, der benutzt wurde, bekannt ist.[552] Auskunft darüber, von welcher Indexseite der entsprechende .torrent-Container oder *magnet link* erlangt wurde, könnte allenfalls derjenige geben, der den *filesharing*-Vorgang durchgeführt hat; wenn aber bereits der Anschlussinhaber über § 7 Abs.4 TMG in Anspruch genommen wird, dann nur, weil sich diese Person nicht ermitteln lies. Ebenfalls nicht aufklären lässt sich, welcher *filesharing*-Client benutzt wurde, sodass ein Vorgehen gegen die Hersteller und/oder Anbieter desselben allein schon aus diesem Grund ausscheidet.

Ohne weiteres ermitteln ließe sich aber, welche Indexseiten .torrent-Container oder *magnet links* anbieten, die den jeweils streitgegenständlichen Hashwert enthalten und zu welchen Trackern diese verbinden. Letztlich kommt dann jede Indexseite und jeder Tracker, für die/den dies zutrifft, als Beteiligte(r) der Verletzung in Betracht, was im gegenwärtigen BitTorrent-„Ökosystem“ durchaus eine (niedrige) zweistellige Zahl an einschlägigen Indexseiten und ähnliche Zahl an einschlägigen Trackern bedeuten kann. Zudem kann auch ohne weiteres in der DHT nach diesem Hashwert gesucht werden; wird er dort aufgefunden, kommen zwar nicht die einzelnen Nut-

548 BT-Drs. 18/12202, S. 12.

549 Einwände gegen die Reichweite der Subsidiarität in der Netzsperren-Rechtsprechung bei *Grisse*, Internetangebotssperren, S. 351.

550 Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 87 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

551 Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 3/14, Rz. 73 – MMR 2016, 188.

552 Siehe Kapitel § 1 IV. 4.

zer in der DHT[553] als Beteiligte in Betracht, wohl aber der Anbieter des *bootstrapping*-Mechanismus der DHT.[554]

Wollte man hiergegen einwenden, dass der Gesetzgeber eine solch weitreichende Subsidiarität nicht gewollt habe, so müsste, dieses Argument zu Ende gedacht, der Rechteinhaber gegen gar keine Indexseite vorgehen, denn die tatsächlich benutzte Indexseite lässt sich nicht ermitteln und eine Beschränkung auf einige wenige Indexseiten lässt sich mangels Auffindbarkeit plausibler Auswahlkriterien nicht herleiten. Übrig bliebe als ermittelbarer Beteiligter dann nämlich nur der vom Ermittler benutzte Tracker. Dieser Einwand kann also nicht richtig sein, da erstens die Gesetzesbegründung als Beteiligten zumindest den Webseitenbetreiber nennt (eine Beschränkung auf einen Tracker also nicht zulässig ist), zweitens – wie aufgezeigt – der Rechteinhaber Nachforschungen anstellen muss, bei einer Beschränkung auf den vom Ermittler benutzten Tracker jedoch keine weiteren Nachforschungen erforderlich wären, und drittens, weil ausweislich der Gesetzesbegründung die Haftung nach § 7 Abs.4 TMG nur *ultima ratio* sein soll, die Beschränkung der Subsidiarität auf nur einen Beteiligten jedoch nicht alle verfügbaren Mittel ausschöpft.

Mithin sind die ermittelbaren Beteiligten im Sinne der Norm alle diejenigen Indexseiten, die .torrent-Container oder *magnet links* anbieten, die den jeweils streitgegenständlichen Hashwert enthalten, sowie alle diejenigen Tracker, die Nutzer bezüglich diesem Hashwert untereinander verbinden. Der Anbieter für *bootstrapping* in die DHT kommt ebenfalls in Betracht, wenn sich der Hashwert dort auffinden lässt. Hinsichtlich der Indexseiten lassen sich des Weiteren all diejenigen Akteure ermitteln, die für die Erreichbarkeit der jeweiligen Indexseiten einen Beitrag leisten, also insbesondere Registrare, (verteilte) Nameserver, TLS-Zertifizierungsstellen, Hostserver, Suchmaschinen, alternative DNS-Resolver und Tor-Proxies. Darüber hinaus kommt auch derjenige ISP in Betracht, dessen Kunde der in Anspruch genommene Anschlussinhaber ist, da dieser ISP durch Routing von IP-Adressen und seinen

[553] Aus denselben Gründen, aus denen auch die Nutzer, die auf eine Indexseite .torrent-Container oder *magnet links* hochladen, nicht in Anspruch genommen werden müssen.

[554] Siehe Kapitel § 1 II. 5. a) bb) und 6.

DNS-Resolver Beteiligter der Verletzung war.[555] Zuletzt kann zwar nicht ermittelt werden, welcher BitTorrent-Client benutzt wurde, allerdings bedingt die Nutzung von BitTorrent zwingend, dass ein Client benutzt worden sein muss, der das BitTorrent-Protokoll implementiert. Beteiligt sind somit auch (zunächst unabhängig von der Frage, ob sie haften) die Entwickler des BitTorrent-Protokolls.[556]

In der Gesamtschau sind gegebenenfalls mehrere dutzend Akteure potentiell ermittelbare Beteiligte im Sinne von § 7 Abs.4 Satz 1 TMG.[557]

Die einzig sinnvolle Einschränkung, die sich ziehen lässt, ist eine zeitliche. Die Auffindbarkeit des Hashwerts auf anderen Seiten kann allenfalls bis zum Zeitpunkt der letzten mündlichen Verhandlung für die Subsidiarität eine Rolle spielen; andernfalls ließe sich nie eine Entscheidung fällen, da .torrent-Container oder *magnet links* immer wieder neu auf verschiedenen Seiten

[555] Denn gemäß den ersten instanzgerichtlichen Entscheidungen zu § 8 Abs.1 Satz 2 TMG n.F. gilt diese Norm nach richtlinienkonformer, verfassungskonformer sowie historischer Auslegung nur für Diensteanbieter nach § 8 Abs.3 TMG, siehe LG München I, Urteil vom 21. Dezember 2017, Az. 7 O 17752/17 – MMR 2018, 322; bestätigt durch OLG München, Urteil vom 14. Juni 2018, Az. 29 U 732/18 – GRUR 2018, 1050. Mithin sind Netzsperren gegen ISPs auch nach dem 3. TMGÄndG möglich.

[556] In der Anfangszeit des *filesharing* war es üblich, die Hersteller von Clients in Anspruch zu nehmen, bei BitTorrent steht dies gegenwärtig noch aus, siehe Kapitel § 1 II. 4. a), b), c) und V. 4. j). Ob international überhaupt eine erfolgreiche Chance auf die Inanspruchnahme der Entwickler des BitTorrent-Protokolls oder der Hersteller von Clients besteht (unabhängig davon, dass dies eine komplette Technologie sperren würde und damit rechtspolitisch nicht wünschenswert wäre), scheint hingegen fraglich. Beispielsweise erscheint dies in den USA unter Geltung des Standards aus der Grokster-Rechtsprechung ausgeschlossen, da zumindest bis 2018 weder die Entwickler des BitTorrent-Protokolls noch die Hersteller von BitTorrent-Clients mit der Nutzung von BitTorrent für Rechtsverletzungen warben oder hierzu verleiteten, siehe *Giblin*, IEEE Internet Computing, Nr. 3, Bd. 16, 2012, S. 92, 94; siehe hierzu aber nunmehr Kapitel § 1 V. 4. j). Siehe zum Grokster-Standard *Post/Sandefur*, 2004-2005 Cato Sup. Ct. Rev. 235, 253ff. (2005). In Deutschland ist die Rechtslage ähnlich, da der BGH in der „Cybersky"-Entscheidung geurteilt hat, dass eine Störerhaftung für den Betrieb eines *filesharing*-Systems nur dann in Betracht kommt, wenn die Möglichkeit dessen Nutzung für Rechtsverletzungen aktiv beworben wird, siehe BGH, Urteil vom 15. Januar 2009, Az. I ZR 57/07, Rz. 33 – GRUR 2009, 841 - „Cybersky". Zur Haftung der Entwickler von (anonymen) *filesharing*-Systemen siehe aus neuerer Zeit *Scheder-Bieschin*, Modernes Filesharing: Störerhaftung und Auskunftspflicht von Anonymisierungsdiensten, S. 236ff.

[557] Insofern unzutreffend *Sesing/Baumann*, MMR 2017, 583, 587.

auftauchen können.[558]

dd) Scheitern oder mangelnde Erfolgsaussicht der Inanspruchnahme der ermittelten Beteiligten

Der Rechteinhaber muss zuletzt zumutbare Anstrengungen anstellen, um die ermittelten Beteiligten in Anspruch zu nehmen; nur wenn dies scheitert oder dem jede Erfolgsaussicht fehlt, darf zuletzt der Anschlussinhaber in Anspruch genommen werden.[559] Aus der Netzsperren-Rechtsprechung des BGH lassen sich keine Erkenntnisse dafür ziehen, welche Anstrengungen genau noch zumutbar sind, da der dort klagende Rechteinhaber gar keine Anstrengungen unternommen hatte, gegen Beteiligte vorzugehen.[560] Keine Rolle kann in diesem Zusammenhang spielen, dass Indexseitenbetreiber ohne weiteres die Infrastruktur wechseln können[561] (neue Domain, neuer Nameserver, neuer Hostserver etc.); dies trifft zwar zu, betrifft aber nur die faktische Wirksamkeit des Vorgehens gegen Beteiligte, nicht dessen rechtliche Erfolgsaussichten.

Mangels klarer Vorgaben sind also viele Varianten denkbar, wann eine Inanspruchnahme gescheitert ist oder mangelnde Erfolgsaussichten hat.

Ein *Scheitern* könnte in einem verlorenen Gerichtsverfahren oder in der Untätigkeit von Behörden trotz Antrag auf Handeln und/oder in mangelnden Vollstreckungsaussichten nach einem gewonnenen Gerichtsverfahren oder nach ergangenen Behördenanordnungen zu sehen sein. *Mangelnde Erfolgsaussichten* könnten erstens dann anzunehmen sein, wenn keine höchstgerichtliche Rechtsprechung bezüglich einer bestimmten Beteiligungsform vorliegt (beispielsweise der Haftung alternativer DNS-Resolver), zweitens dann, wenn zumindest keine einschlägigen erstinstanzlichen Präzedenzfälle bezüglich einer bestimmten Beteiligungsform vorliegen oder drittens nur dann, wenn es gar keine denkbar einschlägigen Gesetze gibt.

Nach Auffassung des Verfassers wird ein *Scheitern* in den beiden genannten Fällen anzunehmen sein, da der untechnische Begriff des „Scheiterns“ einen Ergebnisbezug nahelegt, mithin das Vorgehen gegen einen Beteiligten nicht

[558] Vgl. auch *Grisse*, Internetangebotssperren, S. 349f.

[559] BT-Drs. 18/12202, S. 12.

[560] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 87 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

[561] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 85 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

nur dann scheitert, wenn kein Titel erlangt werden kann, sondern auch dann, wenn der Versuch der Vollstreckung eines erlangten Titels scheitert; gleiches gilt in Bezug auf Behördenanordnungen und deren Vollzug.

Bezüglich der *mangelnden Erfolgsaussichten* kann es nicht darauf ankommen, dass eine Rechtsprechungspraxis bezüglich bestimmter Formen der Beteiligung bereits besteht, da die Urheberrechtsindustrie sich ansonsten durch Untätigkeit (dahingehend, erst gar keine Rechtsprechungspraxis zu erzeugen) Vorteile verschaffen könnte. Zudem bedeutet Erfolgsaussichten nicht Erfolgsgarantie; der Wortlaut „*Aussichten*“ legt nahe, dass ein Erfolg lediglich nicht völlig unwahrscheinlich erscheinen darf. Besteht also bereits eine höchst- oder instanzgerichtliche Rechtsprechungspraxis bezüglich einer bestimmten Beteiligtengruppe, erhöht dies die Erfolgsaussichten, das Fehlen einer solchen Praxis beseitigt aber umgekehrt nicht jede Erfolgsaussicht.

Den Vortrag des klagenden Rechteinhabers[562] zu den Erfolgsaussichten kann das befasste Gericht in eigener Sachkunde beurteilen, soweit es darum geht, ob deutsche Gerichtsstände eröffnet sind und sofern deutsches Recht anwendbar ist. Geht es um die Frage, ob im Ausland ein Gerichtsstand besteht oder wie nach ausländischem Recht die Erfolgsaussichten zu beurteilen sind, wird das Gericht dies wegen der strengen Anforderungen des BGH zu § 293 ZPO[563] regelmäßig nicht ohne ein gerichtliches Sachverständigengutachten beurteilen können. Ein pauschaler Verweis auf den angeblich mangelnden

[562] Zur Darlegungs- und Beweislast siehe Kapitel § 4 VIII. 4. c).
[563] *Bacher* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 293 ZPO, Rz. 27.

Urheberrechtsschutz in einem Land[564] kann nicht ausreichen, da – wie an Hand zahlreicher Beispiele in dieser Arbeit aufgezeigt[565] – auch in vielen Ländern, die typischerweise nicht mit einem starken Urheberrechtsschutz assoziiert werden, in den letzten Jahren erfolgreich gegen Urheberrechtsverletzer vorgegangen werden konnte. Mithin erscheinen auch vage Gradmesser wie beispielsweise der Special 301 Report[566] oder der *WJP Rule of Law Index*[567] nicht dazu geeignet, eine Beurteilung im Einzelfall zu ersetzen. Insbesondere ist dabei darauf hinzuweisen, dass einige Beteiligte (verteilte Nameserver, TLS-Zertifizierungsstellen etc.) ihren Sitz häufig in den USA haben und gerade in den USA wegen der Erstreckung von Unterlassungstiteln auch auf Dritte mittels Regel 65 (d)(2)(C) der Federal Rules of Civil Procedure deren Inanspruchnahme stark erleichtert wird.[568]

Jedenfalls wird der Vortrag des klagenden Rechteinhabers bzw. das Sachverständigengutachten zum ausländischen Recht auch die Erfolgsaussichten etwaiger Rechtsmittel mit abdecken müssen, da wegen des *ultima ratio*-Gedankens des § 7 Abs.4 TMG vom Rechteinhaber die Rechtswegerschöpfung zu verlangen sein wird. Wird der Anschlussinhaber in Anspruch genom-

[564] Die Vorinstanz hatte in der „Störerhaftung des Access-Providers"-Rechtsprechung richtigerweise darauf hingewiesen, dass die pauschale Behauptung der Klägerin, in Russland (dort saß der Host-Provider der streitgegenständlichen Webseite) sei Rechtsschutz aussichtslos, zweifelhaft erscheine. Da die Parteien über diese Frage jedoch anscheinend nicht stritten, unterstellte das Gericht, dass der Klägerin beizupflichten sei, siehe OLG Köln, Urteil vom 18. Juli 2014, Az. 6 U 192/11, Rz. 973 – NRWE. Der BGH legte seinem Urteil diese Unterstellung zu Grunde, siehe BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 86 – GRUR 2016, 268 - „Störerhaftung des Access-Providers". Ob das OLG Köln und der BGH hier richtig gehandelt haben, darf bezweifelt werden, denn ausländisches Recht ist von Amts wegen zu ermitteln, siehe BGH, Beschluss vom 7. Februar 2017, Az. V ZB 166/15, Rz. 7 – BeckRS 2017, 104200. Die unterlassene Ermittlung ist in der Revision als Rechtsfehler anzusehen, *Bacher* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 293 ZPO, Rz. 27. Jedoch halten sich Gerichte bisher nicht an diese Regel: Auch das LG Köln hat im Verfahren gegen einen Registrar betreffend einer Domaindekonnektierung ein Verfahren gegen den in Vietnam ansässigen Hostprovider pauschal als nicht erfolgversprechend eingestuft, ohne dies an Hand des vietnamesischen Rechts zu begründen, siehe LG Köln, Urteil vom 5. Dezember 2017, Az. 14 O 125/16, Rz. 106 – juris.

[565] Siehe Kapitel § 3 III.

[566] Siehe hierzu Kapitel § 3 III.

[567] https://worldjusticeproject.org/sites/default/files/documents/RoLI_Final-Digital_0.pdf - Zugriff am 31.03.2021.

[568] *Kesari/Hoofnagle/McCoy*, 32 Berkeley Tech. L. J. 1093, 1106ff. (2017).

men, bevor ein laufender Rechtsstreit gegen einen der vorrangig haftenden Beteiligten abgeschlossen ist, so wird das Verfahren gegen den Anschlussinhaber nach § 148 ZPO bis zum Abschluss dieser Verfahren auszusetzen sein.[569]

Im Ergebnis muss der klagende Rechteinhaber also ausführlich dazu vortragen, warum ein Vorgehen gegen die ermittelten bzw. ermittelbaren Beteiligten sowohl in Deutschland als auch im Ausland mangelnde Erfolgsaussichten hat oder bereits gescheitert ist. Das Gericht kann diesen Vortrag in eigener Sachkunde würdigen, zu Fragen des ausländischen Rechts wird es regelmäßig ein Sachverständigengutachten einholen müssen.

Leider hat der Gesetzgeber dabei übersehen, dass der Anschlussinhaber – wenn er den Vortrag des klagenden Rechteinhabers bezüglich dessen Möglichkeiten zum Vorgehen im Ausland bestreitet – die Kosten des dann einzuholenden Sachverständigengutachtens gemäß § 91 Abs.1 ZPO tragen muss, sofern dieses den Vortrag des Rechteinhabers bestätigt und der Anspruch nach § 7 Abs.4 Satz 1 TMG in Folge besteht. Allein wegen des Kostenrisikos von unter Umständen mehreren tausend Euro werden Anschlussinhaber also den Vortrag klagender Rechteinhaber dahingehend, dass ihnen ein erfolgreiches Vorgehen im Ausland nicht möglich sei, regelmäßig unstreitig stellen, sodass der Tatbestand der Subsidiarität *in praxi* im Vergleich zu seiner theoretischen Reichweite deutlich eingeschränkt bleiben wird.

ee) Inanspruchnahme durch Rechteinhaber selbst?

§ 7 Abs.4 Satz 1 TMG lässt den Subsidiaritätstatbestand ausdrücklich für den Anspruchsgläubiger selbst gelten, setzt also ein Vorgehen gegen Beteiligte auch durch den klagenden Rechteinhaber *selbst* voraus. Diese Wortlautfassung lässt es also nicht ausreichen, wenn statt dem Rechteinhaber ein mit ihm konzernverbundenes Unternehmen oder ein Interessenverband, in dem er Mitglied ist, gegen Beteiligte vorgeht, was jedoch durchaus üblich ist.[570] Da es ausweislich der Gesetzesbegründung jedoch Ziel des Subsidiaritätstatbestandes ist, dass Anschlussinhaber nicht das erstbeste Ziel sind[571], nicht

[569] § 148 ZPO findet auch Anwendung, wenn das Verfahren, wegen dem ausgesetzt werden soll, ein ausländisches Gerichts- oder Verwaltungsverfahren ist, siehe *Wendtland* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 148 ZPO, Rz. 10f.

[570] Siehe zu Interessenverbänden Kapitel § 3 III.

[571] BT-Drs. 18/12202, S. 12.

jedoch, dass auch genau der jeweils betroffene Rechteinhaber gegen andere Beteiligte vorgeht, liegt ein planwidriger Regelungsüberschuss vor. § 7 Abs.4 Satz 1 TMG ist also teleologisch dahingehend zu reduzieren, dass es auch ausreichend ist, wenn statt dem Rechteinhaber ein mit ihm konzernverbundenes Unternehmen oder ein Interessenverband, in dem er Mitglied ist, gegen Beteiligte der Rechtsverletzung vorgeht.

e) „Sperrung der Nutzung von Informationen“

Als Rechtsfolge ordnet § 7 Abs.4 Satz 1 TMG an, dass der Inhaber des verletzten Rechts von dem Diensteanbieter nach § 8 Abs.3 TMG, über dessen Anschluss die Verletzung begangen wurde, die „*Sperrung der Nutzung von Informationen*“ verlangen kann. Jedoch ist die Sperrung selbst wiederum an drei Vorbehalte geknüpft: sie muss erstens zumutbar und zweitens verhältnismäßig sein und drittens der Verhinderung der Wiederholung der Rechtsverletzung dienen.

aa) Anspruchs- oder Anordnungsgrundlage?

Da § 7 Abs.4 TMG nicht mit einem Richtervorbehalt versehen ist, handelt es sich hierbei unstreitig[572] um eine Anspruchsgrundlage, was sich zudem auch eindeutig aus dem Wortlaut der Norm („*kann [...] verlangen*“) ergibt.[573]

bb) „Zumutbar und verhältnismäßig“

Gemäß § 7 Abs.4 Satz 2 TMG muss die verlangte Sperrung zumutbar und verhältnismäßig sein.

- Die Zumutbarkeit wird in der Gesetzesbegründung lediglich als „*wirtschaftliche Zumutbarkeit*“ definiert, die eine Interessenabwägung im Einzelfall erfordert.[574] Wie dargestellt[575], können können in handelsüblichen Routern regelmäßig, aber nicht immer, IP-, DNS- und Portsperren sowie Datenmengenbegrenzungen, die nicht nach bestimmten Inhalten oder Nutzern differenzieren, eingerichtet werden, wobei es hin-

[572] *Mantz*, GRUR 2017, 969, 975; *Obergfell*, K&R 2017, 361, 363.

[573] Folglich findet für die Durchsetzung auch die ZPO Anwendung. Siehe hierzu und warum die Anwendung des FamFG möglicherweise besser gewesen wäre *Grisse*, GRUR 2017, 1073, 1081.

[574] BT-Drs. 18/12202, S. 12.

[575] Siehe Kapitel § 1 V. 2. b).

sichtlich IP- und DNS-Sperren gelegentlich ein mengenmäßiges Limit gibt. Maßnahmen, die eine Filterung des Datenverkehrs erfordern, also URL-Sperren (mittels SPI) und Datenmengenbegrenzungen hinsichtlich *filesharing*-Datenpaketen (mittels DPI), lassen sich mit handelsüblichen Routern und gewöhnlichen IT-Kenntnissen nicht implementieren. Verlangt ein Rechteinhaber also IP-, DNS- und Portsperren und ermöglicht der Router des in Anspruch genommenen Anschlussinhabers diese Sperren, so dürfte deren Implementierung grundsätzlich immer wirtschaftlich zumutbar sein; Ausnahmefälle wären denkbar, wenn der Rechteinhaber beispielsweise die Eingabe mehrerer tausend IP-Adressen und Domains verlangt, da dies den einer Privatperson oder einem Kleingewerbetreibenden zumutbaren Zeitaufwand übersteigen dürfte. Schwieriger ist die Frage der wirtschaftlichen Zumutbarkeit dann, wenn der Router des Anschlussinhabers die geforderten Maßnahmen technisch gar nicht implementieren kann. Dürfen diese Maßnahmen dann trotzdem (unbeschadet anderer rechtlicher Einwände) verlangt werden, der Anschlussinhaber also, wenn er ein Zwangsgeld nach § 888 Abs.1 ZPO vermeiden möchte, mittelbar gezwungen ist, sich einen neuen Router anzuschaffen? Dies dürfte mit der gesetzgeberischen Wertung aus § 11 Abs.3 Satz 2 FTEG[576] nicht vereinbar sein. Diese Norm gewährt Kunden eines ISP die freie Wahl darüber, welchen Router sie verwenden möchten. Zwar bindet diese Norm direkt nur ISPs[577], allerdings kommt in dieser Norm generell die Bestrebung der Liberalisierung des Telekommunikationssektors zum Ausdruck[578], die konterkariert werden würden, wenn über § 7 Abs.4 Satz 1 TMG und § 888 ZPO nun Anschlussinhaber mittelbar gezwungen wären, sich einen Router mit bestimmten Fähigkeiten zuzulegen. Jedenfalls erscheint es – auch diese systematische Betrachtung hinweg gedacht – zumindest nicht wirtschaftlich zumutbar, von einem Anschlussinhaber mittelbar die Anschaffung eines Routers zu verlangen, der für SPI und DPI geeignet ist, da ein solcher erhebliche Kosten mit sich bringt und dem Verwender überdurchschnittliche IT-Kenntnisse abverlangt.

[576] Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen. Siehe hierzu *Koch/Lißek*, K&R 2016, 572, 575ff.

[577] Diese dürfen ihren Kunden also nicht vorschreiben, welchen Router jene benutzen dürfen.

[578] *Koch/Lißek*, K&R 2016, 572, 572.

- Auch die Verhältnismäßigkeit wird in der Gesetzesbegründung nicht genau definiert. Stattdessen verweist diese wiederum auf eine Abwägung im Einzelfall sowie darauf, dass eine Sperrmaßnahme nicht zu „*overblocking*“ führen, also nicht über ihr Ziel hinausschießen dürfe.[579] Dem BGH zu Folge ist unter *overblocking* die Mitbetroffenheit legaler Inhalte bei Sperrmaßnahmen zu verstehen.[580] Da sich bei den einzelnen Präventionsmaßnahmen für die Verhältnismäßigkeit jeweils Unterschiede ergeben können, wird sie dort (siehe sogleich) jeweils gesondert behandelt. Als Faustregel lassen sich – wie schon beim Subsidiaritätstatbestand[581] – die in der Netzsperren-Rechtsprechung des BGH aufgestellten Kriterien heranziehen. Demnach kommt es für die Verhältnismäßigkeit bzw. *overblocking* auf das Verhältnis von illegalen zu legalen Inhalten an. Ein *overblocking* ist also nicht schon immer dann anzunehmen, sobald legale Inhalte von einer Sperrmaßnahme mitbetroffen sind, da sich andernfalls Anbieter von illegalen Inhalten hinter legalen Inhalten „verstecken“ könnten. Folglich ist eine Sperrmaßnahme verhältnismäßig, wenn von ihr weit überwiegend illegale Inhalte betroffen sind (in der Entscheidung „Störerhaftung des Access-Providers“ war das von den dortigen streitgegenständlichen Sperrmaßnahmen betroffene Verhältnis von illegalen zu legalen Inhalten ca. 96:4).[582] In der Literatur zu Netzsperren wird zudem vorgeschlagen, qualitative Überlegungen einfließen zu lassen, zum Beispiel, ob das betroffene Angebot überhaupt eine gewisse Größe und Sichtbarkeit aufweist und ob es gegen Rechtsverletzungen (durch Inhalte, die seine Nutzer einstellen)

[579] BT-Drs. 18/12202, S. 12.

[580] Vgl. BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 54 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

[581] Siehe Kapitel § 4 VIII. 3. d).

[582] BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 53ff. – GRUR 2016, 268 - „Störerhaftung des Access-Providers“. Nicht relevant dürfte in diesem Kontext die Entscheidung des EGMR betreffend die Zulässigkeit von Webseitensperren sein, da die Mitbetroffenheit legaler Inhalte durch eine Webseitensperre dort dadurch bedingt war, dass der Hosting-Anbieter zwei Webseiten über eine IP-Adresse zur Verfügung stellte, und nur eine der Webseiten illegale Inhalte aufwies, die des betroffenen Antragstellers jedoch nicht, siehe EGMR, Urteil vom 23. Juni 2020, No. 10795/14, Rz. 6, 39f. – hudoc.echr.coe.int - „Vladimir Kharitonov/Russland“. Dies kann nicht gleichgesetzt werden mit dem Fall, in dem eine Webseite überwiegend illegale und nur teilweise legale Inhalte aufweist. Dennoch zeigt der Fall, dass in Zukunft auch der EGMR diesbezüglich angerufen werden könnte.

vorgeht oder diese stattdessen durch sein Geschäftsmodell eher noch anlockt.[583]

cc) Verhinderung der Wiederholung der Rechtsverletzung

Nach § 7 Abs.4 Satz 1 TMG soll die Sperrung von Informationen dazu dienen, die Wiederholung der jeweils streitgegenständlichen Rechtsverletzung zu „*verhindern*“. Wie in Kapitel § 1 V. 1. b) dargestellt, gibt es keine technischen Möglichkeiten, eine Rechtsverletzung mittels *filesharing* vollständig zu verhindern. Alle denkbaren Maßnahmen können diese lediglich erschweren. Es wäre jedoch nach der Rechtsprechung des EuGH unionsrechtswidrig, wenn von Diensteanbietern nur solche Maßnahmen verlangt werden könnten, die eine Rechtsverletzung vollständig verhindern können; es müssen stattdessen auch solche Maßnahmen verlangt werden können, die eine Rechtsverletzung nur erschweren.[584] Mithin ist fraglich, ob der Wortlaut des § 7 Abs.4 Satz 1 TMG betreffend dem Begriff „*Verhindern*“ durch eine teleologische Reduktion korrigiert werden kann. Dies kann bejaht werden, da die Gesetzesbegründung gerade diejenigen technischen Maßnahmen anführt (zu diesen im Einzelnen sogleich), von denen bekannt ist, dass sie eine vollständige Verhinderung einer Rechtsverletzung nicht erlauben[585]; es liegt mithin ein planwidriger Regelungsüberschuss vor.

dd) IP- und DNS-Sperren

Die Gesetzesbegründung schlägt als Sperrmaßnahme ausdrücklich die Sperrung des Zugangs zu Webseiten vor[586]; diese lässt sich mit IP- und DNS-Sperren realisieren.[587] Folglich kommen IP- und DNS-Sperren grundsätzlich als Anspruchsinhalt von § 7 Abs.4 Satz 1 TMG in Betracht. Betreffend die Zumutbarkeit wurde bereits erörtert, dass diese Sperrmaßnahmen grundsätzlich immer zumutbar sind, sofern sie der beim Anschlussinhaber vorhandene Router technisch ermöglicht, und sich Ausnahmen allenfalls in Fällen ergeben können, in denen der Rechteinhaber die Sperrung einer unvertretbar

583 *Grisse*, Internetangebotssperren, S. 448ff.

584 BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 45ff. – GRUR 2016, 268 - „Störerhaftung des Access-Providers“ und EuGH, Urteil vom 27. März 2014, Rs. C-314/12, Rz. 62 – ECLI:EU:C:2014:192 - „UPC Telekabel“.

585 BT-Drs. 18/12202, S. 12.

586 BT-Drs. 18/12202, S. 12.

587 Siehe Kapitel § 1 V. 1. b) aa) und cc).

hohen Anzahl von IP-Adressen und Domains verlangt.[588]

Die Verhältnismäßigkeit ist für jede IP-Adresse und Domain, die gesperrt werden soll, im Einzelfall zu beantworten. Grundsätzlich kommen als Sperrgegenstände BitTorrent-Indexseiten und Tracker-IPs in Betracht, wobei der klagende Rechteinhaber für jeden einzelnen Sperrgegenstand darlegen und beweisen müssen wird[589], dass dessen Sperrung überwiegend illegale Inhalte betreffen wird. Zwar haben empirische Untersuchungen ergeben, dass das BitTorrent-System insgesamt überwiegend zum Tausch illegaler Inhalte verwendet wird[590], jedoch lässt sich dies nicht für jeden einzelnen Bestandteil des BitTorrent-„Ökosystems“ verallgemeinern; entsprechenden Vortrag des klagenden Rechteinhabers können diese Untersuchungen daher nicht ersetzen.

Im Übrigen lässt sich als Faustregel festhalten, dass Suchmaschinen wie *Google* oder Tor-Proxies nicht als Sperrgegenstand in Betracht kommen, da diese zwar das Auffinden von bzw. den Zugriff auf Indexseiten erleichtern, deren Sperrung jedoch auch eine Vielzahl (überwiegend) legaler Angebote betreffen würde.

Zuletzt ist in die Verhältnismäßigkeitsprüfung immer einzubeziehen, dass über eine zeitliche Befristung der Sperrmaßnahmen nachzudenken ist. Dies ist in der Gesetzesbegründung ausdrücklich erwähnt.[591] Konkretere Vorschläge lassen sich dieser jedoch nicht entnehmen. Letztlich wird sich hier in der gerichtlichen Praxis ein bestimmter Richtwert etablieren müssen.

ee) URL-Sperren

Da die Gesetzesbegründung als Sperrmaßnahme ausdrücklich die Sperrung des Zugangs zu Webseiten vorschlägt[592]und als Webseite auch einzelne Bestandteile einer Webseite (also einzelne Unterseiten bzw. Ressourcen auf einer Webseite) angesehen werden können, wären als Sperrmaßnahme auch URL-Sperren[593] denkbar. URL-Sperren wären von allen Maßnahmen die verhältnismäßigste, da sich mit ihnen gezielt illegale Inhalte sperren lassen, ohne

588 Siehe Kapitel § 4 VIII. 3. e) dd).
589 Zur Darlegungs- und Beweislast siehe Kapitel § 4 VIII. 4.
590 Siehe Kapitel § 3 II. 3.
591 BT-Drs. 18/12202, S. 12.
592 BT-Drs. 18/12202, S. 12.
593 Siehe hierzu Kapitel § 1 V. 1. b) dd).

legale Inhalte in Mitleidenschaft zu ziehen. Mithin könnte ein Anschlussinhaber mit URL-Sperren gezielt einzelne Unterseiten auf BitTorrent-Indexseiten sperren.

Jedoch sind sie nicht zumutbar, sofern ein Anschlussinhaber keinen hierfür geeigneten Router aufweist – was regelmäßig der Fall sein wird. Folglich kann im Rahmen dieser Arbeit dahinstehen, ob die Anwendung von SPI oder gegebenenfalls weiterer, für HTTPS erforderlicher Entschlüsselungsmaßnahmen[594] datenschutzrechtlich zulässig wäre (und also bei Unzulässigkeit nicht von einem Anschlussinhaber verlangt werden könnten)[595].

ff) Portsperren

Die Gesetzesbegründung erwähnt ausdrücklich Portsperren als mögliche Sperrmaßnahme im Sinne von § 7 Abs.4 Satz 1 TMG.[596] Bezüglich der Zumutbarkeit gilt für Portsperren im Wesentlichen das zu IP- und DNS-Sperren Gesagte, d.h. wenn der streitgegenständliche Router technisch in der Lage ist Portsperren einzurichten, ist deren Einrichtung auch zumutbar.[597] Im Gegensatz zu IP- und DNS-Sperren ist jedoch bei Portsperren eine Unzumutbarkeit auf Grund zu hohen Arbeitsaufwandes nicht denkbar, da Gegenstand nur einige TCP-Portnummern (für Tracker) und UDP-Portnummern (für die DHT) sind.[598]

Schwieriger gestaltet sich dagegen die Frage der Geeignetheit (für die Erschwerung der Wiederholung von Rechtsverletzungen) und die der Verhältnismäßigkeit.

- Wie oben dargestellt[599], kann gemäß dem Wortlaut des § 7 Abs.4 Satz 1 TMG eine Sperrung nur zu dem Zweck verlangt werden, eine Wiederholung der Rechtsverletzung zu verhindern bzw. – in einem teleologisch

[594] Siehe Kapitel § 1 V. 1. b) cc).

[595] Bejaht von BGH, Urteil vom 26. November 2015, Az. I ZR 174/14, Rz. 64ff. – GRUR 2016, 268 - „Störerhaftung des Access-Providers“, verneint von der Vorinstanz mit Verweis darauf, dass für URL-Sperren Einsicht in den Dateninhalt genommen wird, siehe OLG Köln, Urteil vom 18. Juli 2014, Az. I-6 U 192/11, 6 U 192/11, Rz. 934, 939 – juris. Differenzierter bei *Grisse*, Internetangebotssperren, S. 298, wobei die dortigen Ausführungen nicht auf private Anschlussinhaber übertragbar sind.

[596] BT-Drs. 18/12202, S. 12.

[597] Vgl. Kapitel § 4 VIII. e) bb).

[598] Siehe Kapitel § 1 V. 1. b) bb).

[599] Siehe Kapitel § 4 VIII. 3. e) cc).

reduzierten Sinne richtig verstanden – zu erschweren. Eine Sperrmaßnahme muss also *zumindest* eine Erschwerung der Wiederholung einer Rechtsverletzung leisten; tut sie nicht einmal dies, fällt sie (nicht einmal unter den teleologisch reduzierten) Wortlaut des § 7 Abs.4 Satz 1 TMG und kann mithin nicht Anspruchsgegenstand sein. Der Idee nach verhindern Portsperren, dass ein bestimmter Prozess adressiert werden kann; werden also an einem Router alle von BitTorrent verwendeten Ports gesperrt, kann über diesen Router gar kein BitTorrent-Datenverkehr mehr abgewickelt werden, was folglich eine Wiederholung einer Rechtsverletzung (mittels BitTorrent) erschweren würde. Nach bisherigen Untersuchungen können umfangreiche Portsperren den BitTorrent-Datenverkehr zumindest teilweise eingrenzen.[600] Da eine Erschwerung genügt, sind Portsperren also zumindest geeignete Sperrmaßnahmen.

- Sie sind jedoch *generell* unverhältnismäßig, sodass deren Anordnung immer ein Verstoß gegen § 7 Abs.4 Satz 2 TMG wäre. Dies erscheint zunächst kontraintuitiv: wie festgestellt wurde, ist der über BitTorrent insgesamt abgewickelte Datenverkehr weit überwiegend urheberrechtsverletzend.[601] Dann müsste es eigentlich – unter der Anwendung der Regel des BGH, dass eine Sperrung dann verhältnismäßig ist, solange sie weit überwiegend illegale Inhalte betrifft[602] – auch verhältnismäßig sein, BitTorrent-Datenverkehr insgesamt einzudämmen. Jedoch betrifft die Regel des BGH die Sperrung eines einzelnen Webangebots, nicht die Sperrung einer ganzen Technologie. Der Regel des BGH dürfte also die implizite Überlegung zu Grunde liegen, dass die Sperrung einer Indexseite verhältnismäßig ist, weil die dort legal vorhandenen Angebote auch von anderswo bezogen werden können. Wird jedoch eine ganze Technologie wie BitTorrent gesperrt, ist ein Ausweichen auf andere legale Angebote im Rahmen dieser Technologie nicht mehr möglich.[603] Das Aussperren einer Technologie insgesamt erscheint daher *per se* als

[600] Siehe Kapitel § 1 V. 1. b) bb).
[601] Siehe Kapitel § 3 II. 3.
[602] Siehe Kapitel § 4 VIII. 3. e) bb).
[603] Mit Portsperren lässt sich nicht nach (überwiegend) legalen und (überwiegend) illegalen Angeboten differenzieren, siehe Kapitel § 1 V. 1. b) bb).

overblocking.[604] Portsperren sind daher immer als unverhältnismäßig abzulehnen.

- Dies stellt keinen Widerspruch zu der an anderer Stelle in dieser Arbeit vertretenen Auffassung bezüglich der gehobenen Bedeutung der Gesetzesbegründung für die Auslegung[605] dar: zwar werden in der Gesetzesbegründung Portsperren ausdrücklich als mögliche Sperrmaßnahme bezeichnet, jedoch ist auch nach der in dieser Arbeit vertretenen Auffassung eine historische Auslegung *gegen* den Gesetzeswortlaut nicht möglich – und das Erfordernis der Verhältnismäßigkeit ist, anders als Portsperren, im Gesetzeswortlaut aufgeführt. Zudem hat die Bundesregierung in ihrer Gegenäußerung auf die Stellungnahme des Bundesrates zu der Gesetzesbegründung mitgeteilt, dass sie die genannten Sperrmaßnahmen nicht als zwingend ansieht.[606] Dies schwächt entsprechende Aussagen in der Gesetzesbegründung ab. Überdies ist dem Verfasser der Gesetzesbegründung zu unterstellen, dass er über die technischen Hintergründe von Portsperren nicht informiert war. So wird auf Seite 14 der Gesetzesbegründung behauptet, mit Portsperren könnte der Zugriff auf bestimmte Webseiten verhindert werden.[607] Das ist, wie dargestellt, unzutreffend, da mit Portsperren nur generell die Adressierung von Prozessen über die gesperrten Portnummern verhindert werden kann.

Die Anordnung von Portsperren wäre also im Ergebnis ein Verstoß gegen den Wortlaut von § 7 Abs.4 Satz 1 und Satz 2 TMG und kann daher generell nicht von einem Anschlussinhaber verlangt werden.

Aus der BGH-Entscheidung „Dead Island“ ergibt sich nichts gegenteiliges; der BGH stützte die dortige Behauptung, dass durch Portsperren der Datenverkehr für *filesharing* gesperrt werden kann, auf die unstreitigen Feststellungen in der Vorinstanz[608], die jedoch in technischer Hinsicht unzutreffend sind.[609]

---

[604] So im Ergebnis auch der Sachverständige *Tripp* in der Ausschussanhörung zum 3. TMGÄndG, siehe Ausschuss für Wirtschaft und Energie, Protokoll-Nr. 18/118, S. 9.

[605] Siehe Kapitel § 4 IV. 1. d).

[606] BT-Drs. 18/12496, S. 4.

[607] Vgl. BT-Drs. 18/12202, S. 14.

[608] Vgl. BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 31 – GRUR 2018, 1044 - „Dead Island“.

[609] Siehe Kapitel § 1 V. 1. b) bb).

Dieser Sachverhalt kann in einem neuen Verfahren ohne weiteres streitig gestellt werden.[610]

gg) Datenmengenbegrenzung

Datenmengenbegrenzungen existieren in Form von Geschwindigkeits- und/oder Volumenbegrenzungen, wobei entweder alle Daten einheitlich betroffen sind oder mittels DPI zwischen verschiedenen Datentypen differenziert werden kann.[611] Die Gesetzesbegründung sieht ausdrücklich Datenmengenbegrenzungen vor, ohne jedoch zwischen den verschiedenen Möglichkeiten zu unterscheiden.[612] Grundsätzlich ist also davon auszugehen, dass alle Möglichkeiten in Betracht kommen sollen. Allerdings ergeben sich bei Prüfung der drei Vorbehalte (Zumutbarkeit, Verhältnismäßigkeit und Geeignetheit für die Erschwerung der Wiederholung der Rechtsverletzung) bei allen Möglichkeiten (zum Teil erhebliche) Schwierigkeiten:

- Allen Möglichkeiten der Datenmengenbegrenzung gemein ist, dass sie jedenfalls im weitesten Sinne geeignet sind, die Wiederholung einer Rechtsverletzung zu erschweren. Ein Herausfiltern aller BitTorrent-Daten beispielsweise würde eine Wiederholung der Rechtsverletzung (zumindest über BitTorrent) sogar vollständig verhindern. Das Absenken der Übertragungsgeschwindigkeit für alle Datentypen oder nur für *filesharing*-Daten würde *filesharing* zumindest verlangsamen, was noch als Erschwerung angesehen werden kann. Volumengrenzen verhindern *filesharing*, wenn das Volumen aufgebraucht ist; dies kommt dann (wenn alle Datentypen von der Grenze betroffen sind) einer vollständigen Anschlusssperrung gleich. Schwieriger ist es, Datenmengenbegrenzungen, die nicht nach bestimmten Dateitypen differenzieren, als „*Sperrung*“ im Sinne von § 7 Abs.4 Satz 1 TMG anzusehen, da *filesharing* durch solche Begrenzungen zwar erschwert, aber eigentlich kein Zugriff auf irgendwelche Inhalte „gesperrt“ wird. Immerhin dieses Problem hat die Gesetzesbegründung im Ansatz berücksichtigt: „*Möglich sind daher auch Maßnahmen, die vom Eingriffscharakter unterhalb einer Sperrung liegen, wie zum Beispiel Datenmengenbegrenzungen, wenn sie im Ein-*

[610] *Spoenle*, jurisPR-ITR 25/2017, Anm. 4.
[611] Siehe Kapitel § 1 V. 1. b) ee).
[612] Vgl. BT-Drs. 18/12202, S. 12.

zelfall angemessen sind.“.[613] Mit dem Wortlaut des Gesetzes ist dies (gerade) noch vereinbar, nämlich dann wenn „*Sperrung der Nutzung von Informationen*“ so ausgelegt wird, dass die gesperrten Informationen nicht unmittelbar solche sein müssen, die eine Verletzung ermöglichen. Eine „*Sperrung der Nutzung von Informationen*“ kann also auch dann angenommen werden, wenn gewünschte Daten nicht mit der eigentlich möglichen Geschwindigkeit erlangt werden können.[614]

- Wie in Kapitel § 4 VIII. 3. e) bb) dargestellt, sind handelsübliche Router regelmäßig in der Lage, allgemein wirkende Geschwindigkeits- und Volumenbegrenzungen vorzusehen, nicht jedoch Begrenzungen, die nur für einen bestimmten Dateityp oder nur für bestimmte Nutzer wirken. In den allermeisten Fällen wird ein Anspruch auf solche Begrenzungen also bereits an der Zumutbarkeit scheitern.

- Die größtem Probleme bereitet die Verhältnismäßigkeit. Eine Datenmengenbegrenzung, die *alle* BitTorrent-Daten ausschließt, würde die gesamte BitTorrent-Technologie aussperren, was aus den bereits unter Kapitel § 4 VIII. 3. e) ff) angestellten Überlegungen nicht zulässig ist. Allgemein wirkende Geschwindigkeits- und Datenmengenbegrenzungen würden überwiegend legale Daten betreffen[615], und sind daher auf Grund der unter Kapitel § 4 VIII. 3. e) bb) dargestellten Erwägungen *per se* unverhältnismäßig. Es verbleiben als verhältnismäßige (aber in den meisten Fällen nicht zumutbare) Datenmengenbegrenzungen daher nur Geschwindigkeits- und Mengenbegrenzungen, die spezifisch für *filesharing*-Dateien (insbesondere BitTorrent-Dateien) wirken, sofern sie diese nicht vollständig blockieren. Jedoch würde ein dahingehender Anspruch letztlich die Pflicht bedeuten, den Datenverkehr der Mitnutzer eines Anschlusses zu überwachen. Der EuGH hat in „McFadden“ richtigerweise entschieden, dass eine solche Überwachung gegen das

613 BT-Drs. 18/12202, S. 12.

614 Diese Informationen sind also für den bestmöglichen Zugriff „gesperrt“.

615 Nimmt man das statistische Mittel, so ist zwar der Großteil der über BitTorrent getauschten Daten urheberrechtsverletzend; am gesamten Internetdatenverkehr hat BitTorrent aber mittlerweile, relativ betrachtet, nur noch einen geringen Anteil. Und für den übrigen Datenverkehr gibt es keine Hinweise darauf, dass dieser überwiegend urheberrechtsverletzend ist. Siehe im Einzelnen Kapitel § 3 II.

Überwachungsverbot in Art. 15 ECommerceRL verstößt.[616] Private Anschlussinhaber fallen zwar nicht unter den Anwendungsbereich der ECommerceRL, jedoch gilt das TMG unterschiedslos auch für sie[617], mithin auch § 7 Abs.2 TMG, mit dem Art. 15 ECommerceRL umgesetzt wird. Mithin verbietet sich ein Anspruch auf Begrenzung von *filesharing*-Daten mittels DPI für alle Diensteanbieter nach § 7 Abs.2 TMG. Hinzu kommt noch die datenschutzrechtliche Unzulässigkeit[618], im Falle gewerbliche handelnder Diensteanbieter die telekommunikationsrechtliche Unzulässigkeit[619], und im Falle offener WLANs steht ein Verstoß gegen Art. 3 Abs.2 NetzneutralitätsVO[620] im Raum[621]. Im Ergebnis sind also Datenmengenbegrenzungen – wie schon Portsperren – generell keine zulässigen Sperrmaßnahmen, auch wenn diese in der Gesetzesbegründung vorgeschlagen werden.[622]

hh) Passwortschutz, Einstellung des Dienstes, Registrierung der Nutzer und Überwachung des Datenverkehrs der Nutzer

Als weitere Maßnahmen denkbar wären die in der Überschrift genannten. Die Gesetzesbegründung verhält sich zu diesen nicht.[623] Die Überwachung des Datenverkehrs lässt sich wie die Implementierung von DPI von vornherein mit Verweis auf § 7 Abs.2 TMG ablehnen.[624] Hinsichtlich der übrigen Maßnahmen besagt § 8 Abs.4 TMG, dass diese nicht durch eine Behörde angeordnet werden dürfen. Dies schließt im Umkehrschluss aber nicht aus, dass ein Gericht diese anordnen kann.[625] Das legt auch die Gegenäußerung

616 EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 87 – ECLI:EU:C:2016:689 - „McFadden“.

617 Siehe Kapitel § 4 VIII. 2. c).

618 *Krügel*, MMR 2017, 795, 798; *Grisse*, Internetangebotssperren, S. 362.

619 *Mantz*, MMR 2015, 8, 10.

620 Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union.

621 *Mantz*, GRUR 2017, 969, 974.

622 Zu der Zulässigkeit der Nichtbeachtung der Gesetzesbegründung siehe Kapitel § 4 VIII. 3. e) ff).

623 Vgl. BT-Drs. 18/12202, S. 12.

624 Siehe Kapitel § 4 VIII. 3. e) gg).

625 *Grisse*, GRUR 2017, 1073, 1076; *Hennemann*, ZUM 2018, 754, 760f.

der Bundesregierung zur Stellungnahme des Bundesrates auf den Gesetzesentwurf nahe, in der ausdrücklich mitgeteilt wird, dass die in § 8 Abs.4 TMG bezeichneten Maßnahmen nach wie vor „*gerichtlich*“ angeordnet werden können.[626] Zunächst ließe sich überlegen, ob damit nur verwaltungs- oder strafgerichtliche Anordnungen gemeint sind. Allerdings wurde der Ausschluss der Verantwortlichkeit nach § 8 Abs.1 Satz 1 TMG schon vor dem 2. und 3. TMGÄndG als Ausschluss der verwaltungs- und strafrechtlichen Verantwortlichkeit verstanden, sodass sich die Gegenäußerung der Bundesregierung scheinbar auf den zivilrechtlichen Anspruch in § 7 Abs.4 Satz 1 TMG bezieht.[627] Allerdings wird wiederum in der Gesetzesbegründung betreffend § 8 Abs.4 TMG darauf hingewiesen, dass die dort genannten Maßnahmen ursprünglich (was zutreffend ist) Gegenstand der Entscheidung „McFadden“ waren und der EuGH dort davon ausging bzw. zu Grunde zu legen hatte, dass sie die einzigen Maßnahmen sind, die ein Anschlussinhaber implementieren kann.[628] Das sei jetzt überholt, da in der Gesetzesbegründung nunmehr andere Sperrmaßnahmen vorgeschlagen werden.[629] Zusammengefasst deutet also die Gesetzesbegründung daraufhin, dass die in der Überschrift genannten Maßnahmen nicht Gegenstand eines Anspruches nach § 7 Abs.4 Satz 1 TMG sein können, die Gegenäußerung der Bundesregierung scheint dies hingegen zu bejahen. Aus den Gesetzesmaterialien insgesamt lässt sich mithin kein eindeutiges historisches Argument ableiten.[630]

Folglich ist danach zu entscheiden, ob diese Maßnahmen mit den im Wortlaut des § 7 Abs.4 Satz 1 TMG ausdrücklich formulierten Vorbehalten vereinbar sind. Dabei ergibt sich, dass eine Registrierung[631] schon keine „*Sperrung der Nutzung von Informationen*“ darstellt, selbst unter Berücksichtigung der weiten Auslegung dieses Begriffs.[632] Denn eine Registrierung ändert überhaupt nichts an der Verfügbarkeit von Informationen. Darüber hinaus wird

626 BT-Drs. 18/12496, S. 5.

627 *Mantz*, GRUR 2017, 969, 971.

628 Vgl. BT-Drs. 18/12202, S. 13f.; EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 85 – ECLI:EU:C:2016:689 - „McFadden“.

629 Vgl. BT-Drs. 18/12202, S. 13f.

630 aA BGH, der aus der Gesetzeshistorie die Zulässigkeit von Passwortsperren ableitet, siehe Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 55 – GRUR 2018, 1044 - „Dead Island“.

631 Mit Registrierung ist wohl eine Verifzierung im Rahmen eines Hotspot-Betriebes gemeint. Siehe zum Hotspot-Betrieb Kapitel § 1 IV. 3.

632 Siehe Kapitel § 4 VIII. 3. e) gg).

auch die Wiederholung einer Rechtsverletzung nicht durch eine Registrierung erschwert. Ein Passwortschutz[633] und eine vollständige Einstellung der Anschlussteilung stellen zwar eine „*Sperrung der Nutzung von Informationen*“ dar (der Passwortschutz, weil der Kreis von möglichen Informationsempfängern erheblich verringert wird, die Einstellung, weil es dann gar keine Informationsempfänger mehr gibt). Die Einschränkung des Nutzerkreises ist auch grundsätzlich dazu geeignet, eine Wiederholung einer Rechtsverletzung unwahrscheinlicher zu machen, mithin zu erschweren. Jedoch wird in beiden Fällen – da nicht davon ausgegangen werden kann, dass jeder potentielle Nutzer einen Anschluss überwiegend für illegale Aktivitäten nutzen möchte – die Verhältnismäßigkeit nicht gewahrt; schließlich werden somit überwiegend legale Aktivitäten ausgesperrt[634]. Betreffend der Einstellung des Dienstes kommt hinzu, dass der EuGH in „McFadden“ ausdrücklich bestimmt hat, dass diese nicht verlangt werden kann.[635] Das ist im Anwendungsbereich der ECommerceRL bei der Auslegung des § 7 Abs.4 Satz 1 TMG mithin zusätzlich zu beachten.

Umgekehrt könnte sich auswirken, dass es der EuGH in „McFadden“ für mit dem Unionsrecht vereinbar und sogar für erforderlich gehalten hat, wenn gerichtlich die Passwortsicherung eines WLAN angeordnet wird.[636] Jedoch enthält das Urteil hierzu einen Vorbehalt, denn der Randziffer 99 wurde zu Grunde gelegt, dass gegen WLAN-Anbieter überhaupt nur drei Maßnahmen in Betracht kommen.[637] Diese Ausnahme entspricht jedoch, wie soeben dargestellt, regelmäßig nicht den Tatsachen, da bei den meisten Routern zumindest auch IP-, DNS- und Portsperren sowie generell wirkende Datenmengenbegrenzungen möglich sind. Nur wenn einem Anschlussinhaber all dies technisch nicht möglich ist[638], kann sich die Notwendigkeit ergeben, § 7 Abs.4 Satz 1 TMG europarechtskonform dahingehend auszulegen, dass von

633 aA *Nicolai*, ZUM 2018, 33, 37.

634 Dies übersieht der BGH, der Passwortsperren weiterhin für grundsätzlich zulässig hält, siehe Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 54ff – GRUR 2018, 1044 - „Dead Island“.

635 EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 88 – ECLI:EU:C:2016:689 - „McFadden“.

636 EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 99 – ECLI:EU:C:2016:689 - „McFadden“.

637 EuGH, Urteil vom 15. September 2016, Rs. C-484/14, Rz. 85, 98f. – ECLI:EU:C:2016:689 - „McFadden“.

638 Oder nicht zugemutet werden kann.

einem Anschlussinhaber eine Passwortsicherung verlangt werden kann.[639] Das Verhältnismäßigkeitskriterium in § 7 Abs.4 Satz 2 TMG müsste dann in diesem Fall ebenfalls in europarechtskonformer Auslegung als erfüllt angesehen werden.

ii) Antragsfassung

Gemäß § 253 Abs.2 Nr.2 ZPO ist Zulässigkeitsvoraussetzung einer Klage ein hinreichend bestimmter Antrag. Grundsätzlich ist ein Antrag nur dann hinreichend bestimmt, „*wenn er den erhobenen Antrag konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308) absteckt, Inhalt und Umfang der begehrten Entscheidung (§ 322) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abwälzt und schließlich eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt.*“[640] Diese Anforderungen an einen Antrag gelten auch dann, wenn – wie bei § 7 Abs.4 Satz 1 TMG der Fall – Anspruchsziel ein aktives Tun ist.[641]

Ausreichen kann daher nicht ein Antrag, der nur den Gesetzeswortlaut wiederholt („*Sperrung der Nutzung von Informationen*“). Da der Rechteinhaber – keine anderen Abhilfemöglichkeiten vorausgesetzt – nach hiesiger Auffassung über § 7 Abs.4 Satz 1 TMG zumindest IP- und DNS-Sperren betreffend BitTorrent-Indexseiten sowie Trackern verlangen kann (wiederum vorausgesetzt, dass diese überwiegend zu urheberrechtsverletzendem Material vermitteln) und weiterhin auch ermitteln kann, welche Indexseiten .torrent-Container oder *magnet links* mit dem streitgegenständlichen Hashwert enthalten sowie welche Tracker Nutzer betreffend diesem Hashwert untereinander verbinden, muss er im Klageantrag die IP-Adressen und Domains dieser Indexseiten und Tracker benennen und vom Beklagten verlangen, dass er den Zugang zu diesen sperrt.

---

639 Vgl. auch *Sesing/Baumann*, MMR 2017, 583, 588.

640 *Becker-Eberhard* in: Rauscher/Krüger, MüKo-ZPO, 6. Aufl. 2020, § 253 ZPO, Rz. 88, mit zahlreichen Nachweisen der Rechtsprechung des BGH.

641 *Becker-Eberhard* in: Rauscher/Krüger, MüKo-ZPO, 6. Aufl. 2020, § 253 ZPO, Rz. 140.

Der BGH hat den nötigen Antragsumfang bisher noch offen gelassen.[642]

jj) Ergebnis

Von den möglichen Sperrmaßnahmen können grundsätzlich nur IP- und DNS-Sperren verlangt werden. URL-Sperren, Portsperren, Datenmengenbegrenzungen, Passwortsicherungen, Diensteinstellung, Registrierung der Nutzer oder Überwachung der Nutzer scheiden als Anspruchsinhalt von vornherein aus, wobei Passwortsicherungen in Ausnahmefällen in Betracht kommen können.

f) Abmahngebühren

Siehe zu § 7 Abs.4 Satz 3 TMG das Kapitel § 4 X. 3.

4. Darlegungs- und Beweislast

a) Sekundäre Darlegungslast betreffend den verwendeten Router

Da der klagende Rechteinhaber nicht weiß, welchen Router der Anschlussinhaber verwendet, vom Routertyp jedoch abhängt, welche Sperrmaßnahmen der Anschlussinhaber überhaupt implementieren kann, dürfte Letzteren unzweifelhaft eine sekundäre Darlegungslast dergestalt treffen, dass er dem Rechteinhaber den (zum Verletzungszeitpunkt) verwendeten Routertyp nennen muss.[643] Probleme ergeben sich dann, wenn der Vortrag von Rechteinhaber und Anschlussinhaber darüber, welche Sperrmaßnahmen der verwendete Router überhaupt implementieren kann, auseinandergeht. Unabhängig von der Beweislastverteilung[644] müsste das Gericht dann, wenn es sich eine Bewertung aus eigener Sachkunde nicht zutraut, ein Sachverständigengutachten einholen. Für Rechteinhaber besteht somit eine potentielle Möglichkeit, das Kostenrisiko für den Anschlussinhaber[645] zu erhöhen, was Letzteren stärker noch als die frühere Rechtslage zu einem Vergleich drängt.

---

642 Vgl. BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 57 – GRUR 2018, 1044 - „Dead Island“.

643 Zu einer sekundären Darlegungslast die tatsächlichen Umstände der Zumutbarkeit betreffend auch *Spindler*, NJW 2017, 2305, 2308.

644 Siehe hierzu sogleich Kapitel § 4 VIII. 4. b).

645 Da dieser im Falle des Unterliegens dann die Kosten des Sachverständigen erstatten muss.

b) Darlegungs- und Beweislast betreffend die Anschlussnutzung

Kompliziert erscheint zunächst die Verteilung der Darlegungs- und Beweislast betreffend die Begebenheiten der Anschlussnutzung und die Tatbestandsvoraussetzungen der §§ 8 Abs.3, 7 Abs.4 TMG. Wie dargestellt[646], traf nach der bisherigen Rechtsprechung des BGH den Anschlussinhaber – unabhängig von der Anwendung des TMG – eine sekundäre Darlegungslast über diejenigen Mitnutzer, die statt seiner als Täter der Rechtsverletzung in Betracht kommen. Dem 2. TMGÄndG nach war der Anschlussinhaber über § 8 Abs.3 iVm Abs.1 Satz 1 TMG a.F. privilegiert, sodass er für die Voraussetzungen des § 8 Abs.3 TMG den allgemeinen Regeln nach eigentlich die Beweislast tragen müsste, da jede Partei die für sie günstigen Umstände beweisen muss.[647] Unter Geltung des 3. TMGÄndG ist der Anschlussinhaber immer noch über § 8 Abs.3 iVm Abs.1 Satz 2 TMG n.F. privilegiert, jedoch ist § 8 Abs.3 TMG zugleich eine Tatbestandsvoraussetzung des § 7 Abs.4 TMG und da es sich bei Letzterem um einen Anspruch des Rechteinhabers gegen den Anschlussinhaber handelt, mithin eine für Ersteren günstige Norm, trägt dieser auch die Beweislast für alle Anspruchsvoraussetzungen.[648]

Die Lösung des Problems der nun gültigen Darlegungs-und Beweislastverteilung lässt sich aus dem Haftungskonzept, das das 3. TMGÄndG vorsieht, ableiten. Hierbei ist zunächst zu überlegen, was passiert, wenn ein Anschlussinhaber unter Geltung des 3. TMGÄndG[649] in Anspruch genommen wird. Da es den Rechteinhabern primär auf den Schadensersatz ankommt[650] und dieser nach wie vor nur vom Täter der Rechtsverletzung verlangt werden kann, werden Rechteinhaber auch in Zukunft versuchen, Anschlussinhaber zunächst als Täter der Rechtsverletzung in Anspruch zu nehmen. Denkbar wären als Haftungskonzept des 3. TMGÄndG nun folgende Varianten:

- Variante 1: Anschlussinhaber können gar nicht mehr als Täter haften, sondern nur noch nach § 7 Abs.4 TMG.
- Variante 2: Anschlussinhaber können nach wie vor als Täter haften. Darüber hinaus tragen sie zudem die volle Beweislast dafür, dass sie

646 Siehe Kapitel § 4 VII. 3.
647 *Sesing*, MMR 2015, 423, 427.
648 So im Ergebnis auch *Spindler*, NJW 2017, 2305, 2308.
649 Zum Geltungszeitpunkt siehe Kapitel § 4 VIII. 7.
650 Siehe Kapitel § 3 VI.

zum Zeitpunkt der Rechtsverletzung Diensteanbieter nach § 8 Abs.3 TMG waren.

- Variante 3: Es ändert sich nichts an der bisherigen Haftung, mit der Ausnahme, dass § 7 Abs.4 TMG an die Stelle der Störerhaftung tritt[651]. Anschlussinhaber trifft wie bisher eine sekundäre Darlegungslast über die Umstände der Anschlussnutzung.

- Variante 4: Die sekundäre Darlegungslast soll zumindest in Teilbereichen der Nachforschungs- und/oder Mitteilungspflicht modifiziert werden

Eine Variante 5, die zwar ein Täterhaftung des Anschlussinhabers vorsieht, diesem jedoch keinerlei sekundäre Darlegungslast auferlegt, wäre identisch mit Variante 1, da im Falle einer fehlenden sekundären Darlegungslast der Beweis der Täterschaft nie erbracht werden kann. Variante 1 (und damit auch Variante 5) wiederum lässt sich mit Blick auf Wortlaut und Systematik der §§ 7, 8 TMG eindeutig ablehnen. Gemäß § 7 Abs.1 TMG sind Diensteanbieter für „*eigene Informationen*“ nach wie vor gemäß den „*allgemeinen Gesetzen*“ verantwortlich, mithin auch nach § 97 UrhG.[652] Die Privilegierung des § 8 Abs.3 iVm Abs.1 Satz 2 TMG gilt gemäß § 8 Abs.1 Satz 1 TMG nur für die Durchleitung „*fremder Informationen*“. Ein Anschlussinhaber kann mithin auch unter Geltung des 3. TMGÄndG als Täter haften. Variante 1 und 5 scheiden im Ergebnis also aus.

Variante 2 hingegen würde gegenüber der früheren Rechtslage die Haftung des Anschlussinhabers verschärfen. Schließlich müsste er dann beweisen, dass er Diensteanbieter im Sinne von § 8 Abs.3 TMG ist, die Rechtsverletzung also durch die Durchleitung fremder Informationen verursacht worden ist und nicht durch die Durchleitung eigener Informationen. Dies käme betreffend seiner eigenen Täterschaft einer Umkehr der materiellen Beweislast gleich, da der Beweis, fremde und nicht eigene Informationen durchgeleitet zu haben, zwar nicht den Beweis der Täterschaft eines konkreten anderen Mitnutzers des Anschlusses, allerdings zumindest die Widerlegung der eigenen

[651] Und zwar unterschiedslos, d.h. die Differenzierungen, die früher im Rahmen der Störerhaftung vorgenommen wurden – Störerhaftung bei fehlendem Passwortschutz, keine Störerhaftung bei Anschlussteilung mit Volljährigen – fallen nun weg.

[652] *Leistner* in: Loewenheim/Leistner/Ohly, Schricker/Loewenheim, 6. Aufl. 2020, § 97 UrhG, Rz. 111.

Täterschaft fordert.[653] Gegen Variante 2 spricht, dass § 8 Abs.3 TMG eine Tatbestandsvoraussetzung des § 7 Abs.4 Satz 1 TMG ist, letztere Norm einen Anspruch des Rechteinhabers darstellt und mithin für diesen günstig ist. Jede Partei trägt für die ihr günstigen Umstände die Beweislast, mithin für die Voraussetzungen des § 8 Abs.3 TMG der Rechteinhaber[654] statt dem Anschlussinhaber. Würde man dies anders sehen, hätte § 7 Abs.4 TMG zudem keinen Anwendungsbereich, da mangels Rekonstruierbarkeit eines *filesharing*-Vorgangs[655] der Anschlussinhaber nie beweisen könnte, dass die Rechtsverletzung nicht auf eigenen Informationen beruht, er also immer als Täter haften würde statt nach § 7 Abs.4 TMG. Letzterer könnte dann also nie zur Anwendung kommen. Variante 2 ist mithin abzulehnen.

Für Variante 4 müsste die Gesetzesbegründung Anhaltspunkte geben, da der Gesetzeswortlaut und die Systematik für eine solche differenzierende Auslegung schon im Ansatz nichts hergeben. Das ist allerdings nicht der Fall. Die Gesetzesbegründung verhält sich zur sekundären Darlegungslast überhaupt nicht. Nach Stimmen aus der Literatur sei jedoch (zumindest) die in „Loud“ erstmals ausführlich behandelte Mitteilungspflicht betreffend Personen, die sich dem Anschlussinhaber gegenüber als Täter offenbart haben, nicht mit § 8 Abs.3 TMG vereinbar, da hier die Anwendung der sekundären Darlegungslast zu einer täterschaftlichen Haftung führe, obwohl der Anschlussinhaber doch eine Vermittlertätigkeit darlege, die nur den Anspruch des § 7 Abs.4 TMG zur Folge haben dürfe.[656] Dies sei zudem ein logischer Widerspruch, da eine Vermittlertätigkeit und eine Haftung als Täter sich gegenseitig ausschließen müssten.[657] Würde man dieser Meinung folgen, wäre die hier vorgeschlagene Variante 4 also dahingehend zu fassen, dass der in „Loud“ vorgeschriebene Inhalt der Mitteilungspflicht in Zukunft nicht mehr angewendet werden dürfte. Diese Ansicht übersieht jedoch, dass für die rechtliche Subsumtion nicht der zivilprozessual behauptete, unbewiesene

653 Nach der bisherigen Rechtsprechung des BGH war es dagegen für den Aussschluss der täterschaftlichen Haftung ausreichend, wenn nach Erfüllung der sekundären Darlegungslast und anschließender Beweisaufnahme feststand, dass die Täterschaft eines Mitnutzers zumindest genauso wahrscheinlich ist wie die Täterschaft des Anschlussinhabers; dann war dem Rechteinhaber also der Nachweis der Täterschaft des Anschlussinhabers nicht gelungen.

654 *Spindler*, NJW 2017, 2305, 2308.

655 Siehe Kapitel § 1 IV. 7. c) aa).

656 *Köhler*, ZUM 2018, 27, 29f.

657 *Köhler*, ZUM 2018, 27, 29.

Vortrag maßgeblich ist, sondern nur der *unbestrittene*, oder *bestrittene, aber bewiesene* Vortrag. Würde der klagende Rechteinhaber die Behauptung des Anschlussinhabers, er kenne den Täter, verrate ihn aber nicht, zugestehen, dürfte der Anschlussinhaber – auch das TMG hinweggedacht – schon nach bisheriger BGH-Rechtsprechung nicht als Täter in Anspruch genommen werden. So trägt es sich aber in den meisten *filesharing*-Fällen nicht zu, da die klagenden Rechteinhaber kein Interesse an der restlosen Sachverhaltsaufklärung haben, sondern möglichst schnell einen Schadensersatz – von wem auch immer – erlangen wollen, und also praktisch nie die behauptete Täterschaft eines Mitnutzers unstreitig stellen. Der logische Widerspruch, den die Literaturstimme sieht, besteht also nicht, wenn richtigerweise erst der Sachverhalt betrachtet wird, der der rechtlichen Subsumtion zu Grunde zu legen ist, und nicht schon die bloßen Behauptungen der Parteien. Die auch vom hiesigen Verfasser geteilte Kritik, dass die Rechtsprechung des BGH in „Loud“[658] (sowie nach Meinung des Verfassers darüber hinaus in *filesharing*-Verfahren generell) wohl von der rechtstatsächlichen Motivation getragen scheint, Rechteinhabern zumindest irgendeinen Adressaten für die Schadensersatzhaftung zu sichern, kann aus den genannten Gründen rechtsdogmatisch zumindest nicht verfangen, soweit aus § 8 Abs.3 TMG Folgerungen für die sekundäre Darlegungslast gezogen werden, die dieser nicht hergibt. Variante 4 scheidet mithin aus.[659]

Es verbleibt somit nur Variante 3. In der Praxis bedeutet dies, dass ein Anschlussinhaber für eine Rechtsverletzung, die über seinen Anschluss stattgefunden hat, entweder als Täter oder nach § 7 Abs.4 TMG haftet, und zwar logisch zwingend nach einer der beiden Varianten, da die Verletzung entweder der Anschlussinhaber (dann haftet dieser als Täter) oder ein Mitnutzer begangen haben muss (dann haftet der Anschlussinhaber nach § 7 Abs.4 TMG). Nimmt ein Rechteinhaber den Anschlussinhaber also als Täter und hilfsweise nach § 7 Abs.4 TMG in Anspruch, gilt wie bisher die sekundäre Darlegungslast des Anschlussinhabers. Erfüllt er diese und erscheint in der

[658] *Köhler*, ZUM 2018, 27, 31.

[659] Denkbar ist allein, die Gesetzesbegründung zum 2. TMGÄndG – zu der die Begründung zum 3. TMGÄndG insoweit nichts Gegenteiliges enthält – als Argument für ein spezifisches Pflichtenprogramm beim offenen Betrieb eines WLAN heranzuziehen, ohne jedoch dass sich ein bestimmtes Pflichtenprogramm aus dieser ergibt. Siehe hierzu Kapitel § 5 V. 3. b).

Beweisaufnahme die Täterschaft eines Mitnutzers als gleich wahrscheinlich wie die des Anschlussinhabers, ist der Nachweis der Täterschaft nicht erbracht. Da der Anschlussinhaber die Behauptung seiner Täterschaft bzw. der Alleinnutzung des Anschlusses zivilprozessual durch die Behauptung der Täterschaft eines Mitnutzers bestreitet, ist sodann, wenn der Nachweis seiner Täterschaft nicht gelingt, die Täterschaft eines Mitnutzers zugestanden. Diese Tatbestandsvoraussetzung des § 7 Abs.4 TMG („*[...] von einem Nutzer in Anspruch genommen, um [...]*“) ist in Folge automatisch unbestritten.[660] Macht ein Rechteinhaber hingegen direkt § 7 Abs.4 TMG geltend, so ist die einzig mögliche Verteidigung (abgesehen von den übrigen Tatbestandsvoraussetzungen), dass der Anschlussinhaber vorträgt, er selbst habe die Urheberrechtsverletzung begangen, was dann automatisch zu dessen Haftung als Täter führt, sofern der Rechteinhaber entsprechende Sachanträge im Prozess stellt.[661]

Es lässt sich also festhalten, dass es fortan zwei unterschiedliche sekundäre Darlegungslasten gibt, einmal die in Bezug auf § 97 UrhG (wenn also der Anschlussinhaber als Täter in Anspruch genommen wird) und einmal die in Bezug auf § 7 Abs.4 TMG iVm § 8 Abs.3 TMG, wobei der Erfüllung einer der beiden Darlegungslasten automatisch zur Haftung nach der jeweils anderen Norm führt.

c) Darlegungs- und Beweislast betreffend § 7 Abs.4 TMG im Übrigen

Da § 7 Abs.4 TMG als Anspruchsgrundlage eine für den Rechteinhaber günstige Vorschrift ist, trägt jener die Darlegungs-und Beweislast für alle übrigen Tatbestandsmerkmale.[662] Die Verletzung des geistigen Eigentums durch die

[660] Möglich ist also nicht eine Verteidigung dergestalt, dass der Anschlussinhaber vorträgt, er könne sich nicht mehr erinnern, ob er der Täter ist oder ein Dritter die Rechtsverletzung begangen habe und sodann, falls nach der Beweisaufnahme also die Täterschaft eines Dritten genauso wahrscheinlich erscheint wie die des Anschlussinhabers, sowohl seine täterschaftliche Haftung als auch die Haftung nach § 7 Abs.4 TMG ausscheide, eben weil auch die Täterschaft eines Mitnutzers nicht wahrscheinlicher sei als die Täterschaft des Anschlussinhabers.

[661] Was er tun wird, um den Schadensersatz zu erlangen. Ohnehin werden Rechteinhaber, da es ihnen primär um den Schadensersatz geht, zunächst versuchen, den Anschlussinhaber als Täter in Anspruch zu nehmen.

[662] *Spindler*, NJW 2017, 2305, 2308.

Nutzung eines Telemdiendienstes wird bereits ihm Rahmen der Ermittlung nachgewiesen.[663] Die fehlende Möglichkeit einer anderweitigen Abhilfe dürfte sich auf Grund der denkbaren Reichweite dieses Tatbestandsmerkmals[664], insbesondere wegen dessen internationaler Komponente, nur schwer darlegen und beweisen lassen; da für den Nachweis aber in der Regel ein gerichtlich eingeholtes Sachverständigengutachten zum ausländischen Recht erforderlich sein wird, werden Anschlussinhaber dieses Merkmal auf Grund des Kostenrisikos voraussichtlich regelmäßig unstreitig stellen.

Zuletzt müssen die Rechteinhaber noch darlegen und beweisen, welche Maßnahmen zumutbar und verhältnismäßig sind. Die Zumutbarkeit leitet sich aus dem beim Anschlussinhaber vorhandenen Routertyp ab, zu dem dieser vortragen muss.[665] Rechteinhabern ist es hierauf ohne weiteres möglich, auf Grund öffentlich zugänglicher Informationen seitens der Routerhersteller dazu vorzutragen, welche Sperrmaßnahmen der verwendete Router implementieren kann. Im Falle des Bestreitens müsste ein Sachverständigengutachten eingeholt werden, weshalb Anschlussinhaber auch hier regelmäßig den Vortrag des Rechteinhabers zur Vermeidung des Kostenrisikos unstreitig stellen werden. Schwieriger erweist sich die Bestimmung der Darlegungs- und Beweislast betreffend die Verhältnismäßigkeit, da die zulässigen Sperrmaßnahmen (grundsätzlich nur IP- und DNS-Sperren) einen ganzen Internetauftritt erfassen und somit auch legale Inhalte betreffen können. Da im Rahmen dieser Arbeit vorgeschlagen wurde, die Verhältnismäßigkeit primär an quantitativen Merkmalen festzumachen[666], stellt sich die Frage, inwieweit der klagende Rechteinhaber das Verhältnis von legalen und illegalen Inhalten darlegen und beweisen muss. Eine Darstellung des vollständigen Inhalts eines Angebots wird man regelmäßig nicht verlangen können, wenn das Angebot einigermaßen umfangreich ist und sich dessen Inhalte mit der Zeit nach und nach ändern; richtigerweise muss daher die Darstellung eines repräsentativen Ausschnitts genügen.[667] Eine Beweisaufnahme dürfte – wenn der Anschlussinhaber die Verhältnismäßigkeit bestreitet – aber regelmäßig ohne Sachverständigen durchführbar sein, da die Sachfrage (Inhalt des streitigen Angebots) auch ohne technischen Sachverstand beantwortbar sein

663 Zu den Problemen der Ermittlung siehe Kapitel § 1 IV. 7. und § 5 III.
664 Siehe Kapitel § 4 VIII. 3. d).
665 Siehe Kapitel § 4 VIII. 4. a).
666 Siehe Kapitel § 4 VIII. 3. e) bb).
667 *Grisse*, Internetangebotssperren, S. 448.

sollte.

5. Das Verhältnis des TMG zur tatsächlichen Vermutung

Erfüllt der Anschlussinhaberschaft die sekundäre Darlegungslast nicht, gilt nicht seine Täterschaft zugestanden, sondern nur seine beabsichtigte Alleinnutzung des Anschlusses zum Tatzeitpunkt. Da aber grundsätzlich nicht damit gerechnet werden kann, dass die Verletzung durch einen Dritten begangen wurde, der den Anschluss zum Tatzeitpunkt unberechtigt nutzt, gilt richtigerweise ein Anscheinsbeweis / eine dem Anscheinsbeweis gleichkommende tatsächliche Vermutung der Täterschaft des Anschlussinhabers, den / die dieser in der Praxis praktisch nie entkräften kann.[668] Da das TMG schon nichts an der sekundären Darlegungslast ändert, ändert es auch nichts an der Geltung der tatsächlichen Vermutung.[669] Es lassen sich aus denselben Erwägungen, wie oben unter Kapitel § 4 V VIII. 4. b) dargelegt, weder aus dem Wortlaut, noch der Systematik noch der Gesetzesbegründung der Änderungsgesetze zum TMG Gründe gegen deren Geltung ableiten.

Letztere sollen zwar offene WLANs fördern; wie jedoch sekundäre Darlegungslast und tatsächliche Vermutung bei offenen WLANs zu beurteilen sind, gestaltet sich unabhängig von der Geltung des TMG.[670]

6. Das Verhältnis des TMG zu § 832 BGB

Der Anspruch nach § 7 Abs.4 TMG schließt die Anwendbarkeit des § 832 BGB nicht aus, da beide Normen verschiedene Fälle betreffen, Erstere nämlich die Haftung für die Informationsübermittlung, Letztere die Haftung für eine ungenügende Aufsicht über minderjährige Kinder.[671] § 832 BGB ist damit als *lex specialis* zu § 7 Abs.4 TMG anzusehen.

---

668 Siehe Kapitel § 4 VII. 5.

669 aA *Spindler*, GRUR 2018, 16, 20, der darauf verweist, dass die früher korrespondierende Säule zur widerlegten Vermutung, die Störerhaftung, nun weggebrochen sei. Jedoch ist nicht ersichtlich, warum nunmehr etwas anderes gelten sollte, denn unter Geltung des 3. TMGÄndG haftet der Anschlussinhaber bei Entkräftung der Vermutung nach § 7 Abs.4 TMG, da dann automatisch die Täterschaft eines (unbekannten und unberechtigten) Mitnutzers feststeht.

670 Siehe hierzu Kapitel § 5 V. 3. a).

671 *Köhler*, Die Haftung privater Internetanschlussinhaber, S. 211.

7. Zeitpunkt der Anwendung

Dem Rechtsgedanken des Art. 170 EGBGB und dem Prinzip der Rechtssicherheit (Art. 20 Abs.3 GG) zu Folge entfalten Normen ihre Wirkung ab Inkrafttreten.[672] Wird ein Anschlussinhaber jedoch als Täter in Anspruch genommen, spielt der Zeitpunkt der Rechtsverletzung keine Rolle, da das 3. TMGÄndG an der täterschaftlichen Haftung und der darauf bezogenen sekundären Darlegungslast nichts ändert.[673] Insbesondere ändert dies auch nichts am Anspruch auf Ersatz der Gebühren für die Abmahnung hinsichtlich des Unterlassungsanspruches, da der Ausschluss des Gebührenersatzes nach § 7 Abs.4 Satz 3 TMG nur für den Anspruch aus § 7 Abs.4 Satz 1 TMG, nicht jedoch für den Anspruch aus § 97 UrhG gilt.

Ein Unterschied besteht mithin nur insoweit, als gemäß der früheren Rechtslage eine Störerhaftung des Anschlussinhabers bestand, wobei die Gesetzeslage zum Zeitpunkt der Abmahnung und die jeweils aktuelle Rechtsprechungslage[674] maßgeblich ist. Bestand demnach auf Grund der früheren Rechtslage ein Unterlassungsanspruch aus Störerhaftung, so können – da § 7 Abs.4 TMG seine Wirkung erst ab Inkrafttreten entfaltet – die Gebühren für eine Abmahnung noch verlangt werden.[675] Da der Unterlassungsanspruch selbst jedoch in die Zukunft gerichtet ist, kann er seit Inkrafttreten des 3. TMGÄndG nicht mehr geltend gemacht werden.[676]

Ob der Unterlassungsanspruch aus Störerhaftung automatisch durch den Anspruch aus § 7 Abs.4 Satz 1 TMG (bei Vorliegen von dessen Voraussetzungen) ersetzt wird[677] und wie dies dogmatisch in den verschiedenen denkbaren Konstellationen (laufende Gerichtsverfahren, rechtskräftig abgeschlossene Gerichtsverfahren, Unterlassungserklärungen[678]) zu bewerkstelligen ist, kann im Rahmen dieser Arbeit allerdings dahinstehen, da – wie dargestellt[679]

672 *Sesing/Baumann*, MMR 2017, 583, 586.
673 Siehe Kapitel § 4 VIII. 4. b).
674 Für die Rechtsprechung gilt insoweit kein Rückwirkungsverbot.
675 *Sesing/Baumann*, MMR 2017, 583, 585.
676 *Sesing/Baumann*, MMR 2017, 583, 585.
677 Was auf Grund der unionsrechtlich vorgeschriebenen Vermittlerhaftung angezeigt erscheint.
678 Unterlassungserklärungen sind grundsätzlich eine eigene vertragliche Grundlage des Unterlassungsanspruches, sollten daher durch das 3. TMGÄndG eigentlich nicht tangiert sein.
679 Siehe Kapitel § 3 VI.

– der Unterlassungsanspruch auf Grundlage der Störerhaftung in der Praxis von nur sehr untergeordneter Bedeutung ist.

8. Streitwert

Bisher gab es mehrere Aspekte des Streitwertes, sowohl was die Gebühren der Abmahnung als auch den Gebührenstreitwert eines Gerichtsverfahrens betraf.

Wird ein Anschlussinhaber also als Täter der Urheberrechtsverletzung auf Schadensersatz, Unterlassung sowie Ersatz der Abmahngebühren in Anspruch genommen, so ist für die Berechnung der Gebühren für die Geltendmachung des Schadensersatzanspruches als Streitwert der in der Abmahnung geltend gemachte Schaden zu Grunde zu legen; die Abmahngebühren für die Geltendmachung des Unterlassungsanspruches sind gemäß § 97a Abs.3 UrhG begrenzt[680]. Der gerichtliche Gebührenstreitwert bildet sich aus der Höhe der geltend gemachten Abmahngebühren, des geltend gemachten Schadensersatzes sowie des Wertes des Unterlassungsanspruches, der frei geschätzt werden darf[681]; Letzterer beträgt in der Praxis der meisten Instanzgerichte und des BGH regelmäßig mehrere tausend Euro.[682] Der Gebührenstreitwert, auf dessen Grundlage die Gerichtsgebühren und die Rechtsanwaltsgebühren berechnet werden, beträgt also typischerweise mehrere tausend Euro für den Unterlassungsanspruch, mehrere hundert Euro für den Schadensersatzanspruch und mehrere hundert Euro für die Abmahngebühren. Dabei ist jedoch zu berücksichtigen, dass der Unterlassungsanspruch ganz regelmäßig nie eingeklagt wird bzw. wurde[683], weshalb dieser für die Streitwertberechnung regelmäßig wegfällt bzw. wegfiel.

An dieser Streitwertberechnung ändert § 7 Abs.4 TMG nichts, sofern ein Anschlussinhaber als Täter in Anspruch genommen werden kann. Rechteinhaber werden in Zukunft voraussichtlich den Anspruch aus § 7 Abs.4 TMG hilfsweise geltend machen, eine Addition der Streitwerte von Haupt- und Hilfsanspruch findet jedoch nur statt, sofern über den Hilfsanspruch entschieden wird (§ 45 Abs.1 Satz 2 GKG).

680 Siehe dazu Kapitel § 2 V.

681 Insbesondere gilt für das Urheberrecht nicht die Bemessungsgrenze des § 51 Abs.3 GKG.

682 Siehe mit einer Übersicht *Bohlen*, NJW 2017, 777, 779.

683 Siehe Kapitel § 3 VI.

Der Streitwert des Anspruches aus § 7 Abs.4 TMG spielt in Zukunft also nur eine Rolle, sofern über diesen entschieden wird. In der Literatur wird vorgeschlagen, einen deutlich niedrigeren Wert als für Unterlassungsansprüche festzusetzen, da im Vergleichs zu Letzteren der sachliche Umfang geringer und die Zielrichtung spezifischer sei.[684] Da das Gesetz aber keine Anleitung gibt, ist nicht abzusehen, was die Gerichte letztlich in dieser Hinsicht tun werden.

Am Gebührenrisiko ändert § 7 Abs.4 TMG ohnehin nichts, da ein Anschlussinhaber zunächst mit dem Gebührenrisiko konfrontiert ist, das auf Grund seiner Inanspruchnahme als Täter besteht und sich somit nicht von der Rechtslage vor dem Inkrafttreten des 3. TMGÄndG unterscheidet.

9. § 7 Abs.4 TMG und Vergleichsabschlüsse

Wie dargestellt, ist es gegenwärtige Praxis des Abmahnwesens, in *filesharing*-Abmahnungen zunächst die Täterschaft des Anschlussinhabers (implizit) zu behaupten und eine Schadensersatzforderung zu stellen, jedoch zugleich einen Vergleich gegen Zahlung einer Summe, die etwas geringer als die Summe der behaupteten Forderung ist, anzubieten.[685] Zunächst hindert § 7 Abs.4 TMG nicht daran, auch in Zukunft so vorzugehen, da auch unter dessen Geltung die Haftung eines Anschlussinhabers als Täter möglich ist.[686]

Darüber hinaus steht § 7 Abs.4 TMG Vergleichsschlüssen[687] selbst dann nicht im Weg, wenn die Täterschaft des Anschlussinhabers gar nicht (mehr) im Raum steht, sondern nur dessen Haftung nach § 7 Abs.4 TMG. Insbesondere sind Vergleiche mit dem Inhalt, dass der Anschlussinhaber Geld bezahlt statt nach § 7 Abs.4 TMG in Anspruch genommen zu werden, zulässig. Als (eine) materielle Voraussetzung erfordert ein Vergleichsvertrag ein „*gegenseitiges Nachgeben*“; da dieses in § 779 BGB nicht weiter definiert ist, lässt es die Rechtsprechung richtigerweise ausreichen, wenn die streitenden Parteien Zugeständnisse beliebiger Art machen, auch wenn diese nicht gleichwertig

[684] *Mantz*, GRUR 2017, 969, 975.
[685] Siehe Kapitel § 3 V. 6.
[686] Siehe Kapitel § 4 VIII. 4. b).
[687] Sowohl vorgerichtlichen als auch solchen, die im Laufe eines Prozesses geschlossen werden.

sind.[688] Es erscheint daher nicht unzulässig, eine Handlungspflicht (Sperrung von Informationen) gegen eine Zahlungspflicht auszutauschen, auch wenn Letztere für den klagenden Rechteinhaber letztlich wirtschaftlich erstrebenswerter ist.

Für den Anschlussinhaber wird die Zahlung unter Abwägung des Kostenrisikos eines Gerichtsverfahrens[689], das von § 7 Abs.4 TMG nicht abgemildert[690], sondern wegen der potentiell erforderlichen Sachverständigengutachten[691] eher noch gesteigert. An der gegenwärtigen Sachlage, nämlich dass das Gros der *filesharing*-Abmahnungen nicht zu einem Endurteil führt, sondern die behauptete Rechtsverletzung durch eine im Vergleichswege gezahlte Geldsumme abgegolten wird[692], wird § 7 Abs.4 TMG also voraussichtlich nichts ändern.[693]

10. Unionsrechtswidrigkeit des § 7 Abs.4 TMG?

Zu der Bewertung einer Norm hinsichtlich ihrer Tauglichkeit, Rechtssicherheit zu stiften, gehört nicht nur die Frage, ob sie geeignet ist, in einer konsistenten und vorhersehbaren Art ausgelegt zu werden, sondern auch die Frage, ob sie gegenüber höherrangigem Recht Bestand hat bzw. im Falle des Verstoßes gegen Unionsrechts nicht angewendet werden darf. Entscheidend ist in diesem Zusammenhang also, wie der EuGH in einem Vorlageverfahren über die Unionsrechtswidrigkeit des § 7 Abs.4 TMG entscheiden würde. Das lässt sich wiederum schwer prognostizieren. In der Literatur wurde überwiegend nur die Unionsrechtswidrigkeit von § 8 Abs.1 Satz 2 TMG erörtert, soweit dieser Access-Provider, die keine WLAN-Anbieter sind, von jeglicher Haftung befreit.[694] § 7 Abs.4 TMG scheint dagegen als weniger problematisch wahrgenommen zu werden, da die in der Entscheidung „McFadden“ des

[688] *Habersack* in: Säcker et al., MüKo-BGB, 8. Aufl. 2020, § 779 BGB, Rz. 27, mit Nachweisen der Rechtsprechung des BGH.

[689] Siehe hierzu Kapitel § 3 VIII.

[690] Siehe hierzu Kapitel § 4 VIII. 8.

[691] Für technische Fragen der Möglichkeiten, die ein Routertyp zur Implementierung von Sperrmaßnahmen hat, siehe Kapitel § 4 VIII. 4. a). Für Fragen der Möglichkeit der Inanspruchnahme anderer Beteiligter nach ausländischem Recht siehe Kapitel § 4 VIII. 3. d) dd).

[692] Siehe Kapitel § 3 V. 7.

[693] So im Ergebnis auch *Grigorjew/Bile*, ZD-aktuell 2017, 05621 sowie *Haun*, WRP 2018, 780, 784.

[694] Siehe nur *Nicolai*, ZUM 2018, 33, 41f.

EuGH angeordnete Möglichkeit einer Passwortsperre nur unter der Annahme zu Stande gekommen ist, dass keine anderen Sperrmöglichkeiten bestehen – was unter Geltung des § 7 Abs.4 TMG nicht der Fall ist und in bestimmten, notwendigen Fällen immer noch im Rahmen einer europarechtskonformen Auslegung möglich ist.[695]

a) Verstoß gegen die InfoSocRL und die EnforcementRL

Schwierigkeiten könnten unter Umständen der Subsidiaritätstatbestand[696] und – wegen Art. 14 EnforcementRL – der Ausschluss der Erstattungsfähigkeit von Abmahngebühren nach § 7 Abs.4 Satz 3 TMG bereiten[697].

- Gegen das Subsidiaritätskriterium wird eingewandt, dass Art. 8 Abs.3 InfoSocRL und Art. 11 Satz 3 EnforcementRL ein solches nicht vorsähen; Erwägungsgrund 59 InfoSocRL erlaube den Mitgliedstaaten zwar Freiheiten bei den „*Modalitäten*“ des Anspruches gegen Vermittler, Modalitäten beträfen ihrem Wortlaut nach jedoch nur die Rechtsfolgen, nicht aber den Tatbestand einer Norm – zu dem das Subsidiaritätskriterium gehört.[698] Allerdings regelt Erwägungsgrund 59 InfoSocRL, dass auch die „*Bedingungen*“ des Anspruchs im Ermessen der Mitgliedstaaten stehen. Gleiches gilt in Bezug auf Art. 11 EnforcementRL nach Erwägungsgrund 23 EnforcementRL, der regelt, dass die „*Voraussetzungen*“ (und das Verfahren für Anordnungen im Sinne der Norm) Gegenstand der Rechtsvorschriften der Mitgliedstaaten bleiben sollen. Eine EuGH-Vorlage kann klären, wie weit das Ermessen der Mitgliedstaaten geht. Angesichts des Wortlauts der Erwägungsgründe dürfte jedoch von einem großen Umsetzungsspielraum auszugehen sein.

- Eine Unionsrechtswidrigkeit von § 7 Abs.4 Satz 3 TMG würde § 7 Abs.4 TMG im Übrigen unberührt lassen. Der BGH hat in der Entscheidung „Dead Island“ jedenfalls eine Vorlage an den EuGH abgelehnt, mit dem knappen Hinweis darauf, dass – wie bereits erwähnt – die Modalitäten des gegen Zugangsvermittler zu gewährenden Rechtsbehelfs den Mit-

695 Siehe dazu Kapitel § 4 VIII. 3. e) hh) sowie *Sesing/Baumann*, MMR 2017, 583, 588.
696 So *Nordemann*, GRUR 2018, 1016, 1018f.
697 *Sesing/Baumann*, MMR 2017, 583, 588. Siehe dazu auch Kapitel § 5 XI.
698 *Nordemann*, GRUR 2018, 1016, 1018f. Siehe hierzu auch *Nordemann*, GRUR 2021, 18, 21.

gliedstaaten überlassen sind[699]; die Tragfähigkeit dieser Begründung für die Nichtvorlage lässt sich bezweifeln, da der EuGH demgegenüber in „McFadden“ einzelne Modalitäten europarechtlich gewürdigt hat.

Im Ergebnis lässt sich zumindest festhalten, dass es unwahrscheinlich erscheint, dass § 7 Abs.4 TMG aus den soeben genannten Gründen vom EuGH *insgesamt* für unionsrechtswidrig befunden wird.

b) Ungleichbehandlung von Anschlussinhabern und ISPs

Weiterhin dürfte sich auch das Problem der Ungleichbehandlung zwischen Diensteanbietern wie ISPs einerseits und WLAN-Anbietern andererseits dergestalt, dass Erstere überhaupt nicht mehr in Anspruch genommen werden können, erledigt haben.[700] Schließlich hat das LG München I geurteilt, dass § 8 Abs.1 Satz 2 TMG nach historischer, verfassungskonformer und europarechtskonformer Auslegung dahingehend zu verstehen ist, dass „*Diensteanbieter*“ im Sinne dieser Vorschrift nur Diensteanbieter nach § 8 Abs.3 TMG sind[701], weshalb ISPs – die Anwendung dieser Rechtsprechung vorausgesetzt – auch in Zukunft gemäß der „Störerhaftung des Access-Providers“-Rechtsprechung des BGH auf Grundlage der Störerhaftung auf Netzsperren in Anspruch genommen werden können. Der BGH scheint dagegen dahin zu tendieren, stattdessen den Anspruch aus § 7 Abs.4 TMG analog auf alle Access-Provider anwenden zu wollen.[702] So oder so stellen sich im Nachgang im Wesentlichen dieselben Rechtsfragen wie bei einer Lösung über die Stö-

[699] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 58 – GRUR 2018, 1044 - „Dead Island“.

[700] Soweit noch kleinere Differenzierungen verbleiben, erscheinen diese gerechtfertigt, weil WLAN-Anbieter, anders als ISPs, der Auskunftsanspruch nach § 101 Abs.2 Nr.3 UrhG nicht trifft; folglich darf dies an anderer Stelle kompensiert werden. So auch der Sachverständige *Frey* in der Ausschussanhörung zum 3. TMGÄndG, siehe Ausschuss für Wirtschaft und Energie, Protokoll-Nr. 18/118, S. 13.

[701] LG München I, Urteil vom 21. Dezember 2017, Az. 7 O 17752/17 – MMR 2018, 322; bestätigt durch OLG München, Urteil vom 14. Juni 2018, Az. 29 U 732/18 – GRUR 2018, 1050. Es kann – da diese Rechtsfrage für den Schwerpunkt dieser Arbeit nicht sonderlich relevant ist – dahinstehen, ob diese Auslegung sich noch in den Grenzen des Wortlauts von § 8 Abs.1 Satz 2 TMG hält.

[702] BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 41ff. – GRUR 2018, 1044 - „Dead Island“. Siehe hierzu auch OLG Düsseldorf, Urteil vom 9. Oktober 2020, Az. 6 U 32/20, Rz. 103 – MMR 2020, 854 sowie *Nordemann*, GRUR 2021, 18, 19.

rerhaftung.[703] Im Ergebnis ist in beiden Varianten die Vereinbarkeit des § 7 Abs.4 TMG mit dem Europarecht jedenfalls gesichert, da – wie dargestellt – nach beiden Varianten ISPs und Anschlussinhaber nicht ungleich behandelt werden.

11. Konventionswidrigkeit des § 7 Abs.4 TMG?

Der EGMR hat sich in der Entscheidung „Vladimir Kharitonov/Russland“ ausführlich mit Aspekten der Zulässigkeit von Netzsperren befasst.[704]

Gemäß der Entscheidung verletzte Russland die in Art. 10 EMRK geschützte Meinungsfreiheit des Antragsstellers durch eine staatlich verhängte Webseitensperre. Die gesetzliche Vorschrift, auf die die Sperrung gestützt war, würde nicht den Anforderungen an eine ausreichende Entscheidungsvorhersehbarkeit sowie die ausreichende Verhinderung von *overblocking* genügen, die der Gesetzesvorbehalt in Art. 10 Abs.2 EMRK erfordere.[705] Dies wirft in Folge die Frage auf, inwiefern § 7 Abs.4 TMG dem Gesetzesvorbehalt in Art. 10 Abs.2 EMRK genügt, da dieser seinem Regelungsgehalt nach noch rudimentärer als die russische Vorschrift ist.[706]

Hierzu wären folgende Überlegungen anzustellen:

- Art. 10 EMRK müsste zunächst eine Drittwirkung im Verhältnis Rechteinhaber – Anschlussinhaber ausüben bzw. auch in diesem Verhältnis eine staatliche Schutzpflicht bestehen[707]; denn die Entscheidung „Vladimir Kharitonov/Russland“ betrifft einen unmittelbar staatlichen

[703] Vgl. *Nordemann*, GRUR 2018, 1016, 1018ff. Problematisch ist dabei, dass hinsichtlich ISPs dann theoretisch auch Portsperren und Datenmengenbegrenzungen in Betracht kommen könnten, siehe *Spindler*, GRUR 2018, 1012, 1015. Solche Maßnahmen gegenüber ISPs dürften jedoch mit der NetzneutralitätsVO unvereinbar sein, siehe Kapitel § 4 VIII. 3. e) gg).

[704] EGMR, Urteil vom 23. Juni 2020, No. 10795/14 – hudoc.echr.coe.int - „Vladimir Kharitonov/Russland“. Siehe im Übrigen auch die Parallelentscheidung hierzu, EGMR, Urteil vom 23. Juni 2020, No. 61919/16 – hudoc.echr.coe.int - „Engels/Russland“.

[705] EGMR, Urteil vom 23. Juni 2020, No. 10795/14, Rz. 37ff. – hudoc.echr.coe.int - „Vladimir Kharitonov/Russland“.

[706] Vgl. die Erörterung der russischen Rechtslage insbesondere in EGMR, Urteil vom 23. Juni 2020, No. 10795/14, Joint Concurring Opinion Rz. 4ff. – hudoc.echr.coe.int - „Vladimir Kharitonov/Russland“.

[707] Zur unklaren dogmatischen Einordnung der entsprechenden Rechtsprechung des EGMR siehe *Payandeh*, JuS 2016, 690, 692.

Eingriff. Der EGMR hat eine solche Drittwirkung bzw. Schutzpflicht bisher im Verhältnis zwischen Arbeitnehmer und Arbeitgeber angenommen; staatliche Gerichte müssen Art. 10 EMRK in diesem Verhältnis also zur Entfaltung bringen.[708] Da die dogmatischen Voraussetzungen der Drittwirkung bzw. Schutzpflichtbegrüdung von Art. 10 EMRK bisher unklar sind[709], ist offen, ob der EGMR Art. 10 EMRK auch auf das Verhältnis zwischen Rechteinhaber und Anschlussinhaber anwenden würde.

- Der Gesetzesvorbehalt des Art. 10 Abs. 2 EMRK müsste sodann uneingeschränkt auch im Verhältnis zwischen Rechteinhaber und Anschlussinhaber gelten. Da der EGMR in der Entscheidung „Heinisch/Deutschland" den Gesetzesvorbehalt uneingeschränkt auf das Verhältnis zwischen Arbeitnehmer und Arbeitgeber angewendet hat[710], dürfte dies zu bejahen sein.

- Schließlich müsste – da der bloße Wortlaut von § 7 Abs.4 TMG nicht den strengen Anforderungen des EGMR genügen dürfte – die Gesetzesbegründung aus konventionsrechtlicher Perspektive zu berücksichtigen sein, da diese zwar ebenfalls inhaltliche Probleme aufweist, jedoch die zulässigen Sperrmaßnahmen spezifiziert und auf das Problem des *overblocking* näher eingeht[711], sodass bei deren Berücksichtigung den Anforderungen des EGMR Genüge getan sein dürfte. Nach der Rechtsprechung des EGMR sind für den Gesetzesvorbehalt alle außenrechtsverbindlichen Rechtssätze zu berücksichtigen; ob ein Rechtssatz verbindlich ist, bestimmt sich wiederum nach dem Recht der Staaten. Geklärt ist in der Rechtsprechung des EGMR bisher, dass beispielsweise Richterrecht aus *common law*-Staaten ebenfalls dem Gesetzesvorbehalt wie ein Parlamentsgesetz genügen kann, wenn ihm die gleiche Verbindlichkeit zukommt.[712] Dies dürfte für Gesetzesbegründungen nach deutschem Recht zu verneinen sein, da diese nach der Rechtsprechung

[708] EGMR, Urteil vom 21. Juli 2011, No. 28274/08, Rz. 44f. – hudoc.echr.coe.int - „Heinisch/Deutschland".

[709] Vgl. *Payandeh*, JuS 2016, 690, 692.

[710] Vgl. EGMR, Urteil vom 21. Juli 2011, No. 28274/08 – hudoc.echr.coe.int, Rz. 47ff. - „Heinisch/Deutschland".

[711] Siehe Kapitel § 4 VIII. 3.

[712] *Cornils* in: Gersdorf/Paal, BeckOK InfoMedienR, 31. Ed. 2021, Art. 10 EMRK, Rz. 45.

des BVerfG bei der Auslegung zwar als gewichtiges Indiz heranzuziehen sind, aber bei der Auslegung nicht zwingend zu berücksichtigen sind, wenn andere, gewichtigere Argumente entgegenstehen[713] – eine echte Verbindlichkeit der Gesetzebegründungen für die Gesetzesauslegung ist damit nicht garantiert. Entsprechend erscheint die Vereinbarkeit von § 7 Abs.4 TMG mit den Anforderungen des EGMR zweifelhaft.

Nach dem vorstehend Skizzierten erscheint die Vereinbarkeit von § 7 Abs.4 TMG mit der Auslegung von Art. 10 EMRK durch den EGMR insgesamt nicht unproblematisch. Auf Grund der nur punktuell geklärten Rechtsfragen ist hierzu jedoch noch weitere Forschungsarbeit vonnöten.

12. Ergebnis

Im Ergebnis sind die durch das 2. TMGÄndG und das 3. TMGÄndG gebrachten Änderungen, zumindest soweit sie Anschlussinhaber betreffen, überwiegend als negativ zu bewerten. § 8 Abs.3 und § 7 Abs.4 TMG lassen in ihren einzelnen Merkmalen zum Teil (viele) verschiedene Auslegungsvarianten zu und machen damit deren Anwendung durch die Gerichte wenig vorhersehbar. Es schlägt sich durchweg das Grundproblem durch, dass bei der Formulierung der Gesetzesbegründung übersehen wurde, inwieweit die Reformen für die Anschlussteilung im privaten Bereich eine Rolle spielen und sich zum Komplex *filesharing*-Abmahnungen verhalten sollen, obwohl dies für den Gesetzgeber ein ohne weiteres ersichtlicher Sachverhaltskomplex gewesen wäre; ein weiteres Problem ist die mangelnde technische Informiertheit der Gesetzesbegründung, die sich vor allem im Subsidiaritätsmerkmal und den möglichen Sperrmaßnahmen auswirkt.

Für Abgemahnte dürften die Reformen in der Praxis eher eine Verschlechterung als eine Verbesserung darstellen, da erstens das Kostenrisiko steigt und zweitens im Zweifel unklare, komplizierte Regeln für die strukturell unterlegenen Anschlussinhaber[714] schlechter sind als für die strukturell überlegenen Rechteinhaber.

Wie der BGH zu den verschiedenen Rechtsfragen Stellung beziehen wird, bleibt abzuwarten. Die erste Entscheidung hierzu hat bisher nur vereinzelte

[713] Siehe hierzu die Darstellung in Kapitel § 4 IV. 1. d).
[714] Siehe hierzu Kapitel § 3 VIII.

Fragen beantwortet.[715]

Siehe zu Verbesserungsvorschlägen *de lege ferenda* Kapitel § 5 VI.

IX. Zum Schadensersatz nach Lizenzanalogie

1. Die Wahl der richtigen Berechnungsmethode

Ohne Weiteres zuzustimmen ist – dem Grunde nach – der Berechnung des Schadensersatzes in *filesharing*-Fällen auf Basis der Schätzung des Wertes einer fiktiven Lizenz (§ 97 Abs.2 Satz 3 UrhG), der Schätzung des Betrages also, der einem Rechteinhaber zu zahlen gewesen wäre, hätte dieser der öffentlichen Zugänglichmachung seines Werkes[716] in einem *filesharing*-System zugestimmt.[717] Eine Berechnung auf Basis des Verletzergewinns (§ 97 Abs.2 Satz 2 UrhG) kommt nicht in Betracht, weil *filesharing*-Endnutzer aus ihrer Tätigkeit keinen Gewinn erzielen. Auch eine Berechnung nach der Differenzhypothese, insbesondere eine Berechnung des entgangenen Gewinns (§ 252 BGB), scheidet aus, da der klagende Rechteinhaber nachweisen müsste, dass und wie viele Vervielfältigungsstücke er kausal durch die öffentliche Zugänglichmachung nicht verkaufen konnte. Ein solcher Nachweis ist nicht möglich, und zwar selbst dann nicht, wenn sich ermitteln ließe, wie viele Zugriffe es konkret auf das Werk gegeben hat.[718] Denn es lässt sich nicht automatisch annehmen, dass der jeweils zugreifende Nutzer ein Vervielfältigungsstück erworben hätte, wenn er es nicht auf Grund der öffentlichen Zugänglichmachung hätte erlangen können.[719]

Gegen die Berechnung auf Basis einer fiktiven Lizenz lassen sich nur zwei Einwände formulieren, die beide aber erkennbar nicht durchgreifen. Der erste Einwand zielt auf die Zulässigkeit einer *fiktiven* Lizenz selbst ab und postuliert, dass ein Rechteinhaber keinen lizenzanalogen Schaden verlangen dürfe, wenn er eine Lizenz solcher Art, wie sie für die Zulässigkeit der jeweils streitgegenständlichen Handlung nachgefragt werden müsste, generell nicht

[715] Siehe Kapitel § 2 XI. 6.
[716] Probleme der segmentierten Dateiübertragung hinten angestellt.
[717] Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 49ff. – GRUR 2016, 191 - „Tauschbörse III“.
[718] Siehe hierzu Kapitel § 1 IV. 7. c) dd).
[719] *Specht* in: Dreier/Schulze/Specht, UrhG, 6. Aufl. 2018, § 97 UrhG, Rz. 81.

anbietet.[720] Dem ist jedoch schon der Wortlaut des § 97 Abs.2 Satz 3 UrhG entgegenzuhalten, der nur auf die Vergütung abstellt, die der Verletzer hätte entrichten müssen, wenn er die Erlaubnis zur Nutzung des verletzten Rechts eingeholt hätte, nicht also darauf, ob er die Erlaubnis auch erteilt bekommen hätte. Der zweite Einwand besagt spiegelbildlich, dass ein lizenzanaloger Schaden ausscheide, wenn der Verletzer gar keine Lizenz nachsuchen wollte. Dies ist jedoch als *venire contra factum proprium* unzulässig, da ein Rechtsverletzer nicht einerseits ein Recht in Anspruch nehmen und sich dann andererseits darauf berufen kann, es gar nicht in Anspruch nehmen zu wollen.[721]

2. Strafschaden und Überkompensation

a) Verstoß gegen ein Verbot des Strafschadensersatzes?

Zunächst erscheint es nicht abwegig, die in *filesharing*-Fällen zugesprochenen Schadenssummen in die Nähe eines Strafschadens zu rücken, da ihnen allgemein eine generalpräventive Wirkung zukommen kann; eine spezialpräventive Wirkung ist hingegen fraglich, da Anschlussinhaber meist nur auf Grund einer prozessualen Fiktion ihrer Täterschaft zu Schadensersatz verurteilt werden und eine spezialpräventive Wirkung sich nur entfalten kann, wenn die Schuld des Täters feststeht. Ohnehin reicht es nicht aus, dass ein Schadensersatz lediglich eine poenale Nebenwirkung entfaltet, da dies praktisch immer der Fall ist.[722] Um einen zugesprochenen Schadensersatz als Strafschaden ansehen zu können, muss sich dieser einer beständigen, von der Rechtsprechung gebildeten Fallgruppe zuordnen lassen, in der der Schadensersatz nicht primär auf Basis des Ausgleichsprinzips (hierzu sogleich) berechnet wird, sondern stattdessen primär auf Basis poenaler Kriterien wie dem Maß des Verschuldens oder sonstiger Strafzumessungskriterien wie der Präventionswirkung.[723] Demnach lässt sich beispielsweise die sogenannte GEMA-Rechtsprechung als Beispiel für die Zuerkennung eines Strafschadens einordnen.[724] Für die *filesharing*-Rechtsprechung des BGH trifft dies jedoch

[720] *Specht* in: Dreier/Schulze/Specht, UrhG, 6. Aufl. 2018, § 97 UrhG, Rz. 82.
[721] *Specht* in: Dreier/Schulze/Specht, UrhG, 6. Aufl. 2018, § 97 UrhG, Rz. 82.
[722] *Schäfer*, AcP 2002, 397, 399f.
[723] *Schäfer*, AcP 2002, 397, 415.
[724] *Schäfer*, AcP 2002, 397, 418f.

nicht zu.[725] Der BGH hat dort seine Überlegungen zum Schadensersatz strikt am Ausgleichsprinzip orientiert.[726] Folglich kann offen bleiben, ob ein Strafschadensersatz im deutschen Recht überhaupt zulässig wäre.[727]

b) Verstoß gegen ein Verbot der Überkompensation?

Wenn die in *filesharing*-Fällen zugesprochenen Schadensbeträge keinen Strafschaden darstellen, stellen sie dann jedenfalls eine Überkompensation dar? Wird der den Rechteinhabern entstandene Schaden also nicht nur ausgeglichen, sondern werden diese gar bereichert? In Kapitel § 3 VI. wurde postuliert, dass bei mehrseitigen Dateiübertragungssystemen, also insbesondere BitTorrent, zumindest in wirtschaftlicher Betrachtung eine Überkompensation vorliegt, da sich praktisch jeder Nutzer ermitteln lässt und von jedem Nutzer ein Vielfaches von dem verlangt werden kann, was er für den Erwerb eines legalen Vervielfältigungsstückes des getauschten Werkes hätte bezahlen müssen. Für diese wirtschaftliche Betrachtung würde es selbst dann keine Rolle spielen, wenn jedem Nutzer eine öffentliche Zugänglichmachung des *vollständigen* Werkes vorgeworfen werden könnte, da dies an der Bereicherung in wirtschaftlicher Hinsicht nichts ändern würde. Durch die Entscheidung „Konferenz der Tiere“[728] ist nunmehr jedoch geklärt, dass nicht jedem Nutzer, sondern nur der Gesamtheit der Nutzer[729] eine öffentliche Zugänglichmachung des vollständigen Werkes vorgeworfen werden kann;

[725] Das AG Köln rückte jedoch in einem Urteil die in *filesharing*-Fällen üblichen Schadensbeträge in die Nähe eines Strafschadens, siehe AG Köln, Urteil vom 10. März 2014, Az. 125 C 495/13, Rz. 21 – juris.

[726] Vgl. nur BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 56ff. – GRUR 2016, 176 - „Tauschbörse I“ sowie BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14 Rz. 50ff. – GRUR 2016, 191 - „Tauschbörse III“.

[727] Die europarechtliche Zulässigkeit offen gelassen in EuGH, Urteil vom 25. Januar 2017, Rs. C-367/15, Rz. 29 – ECLI:EU:C:2017:36 - „Stowarzyszenie“. Die verfassungsrechtliche Zulässigkeit wohl grundsätzlich bejaht in BVerfG, Beschluss vom 9. Januar 2013, Az. 2 BvR 2805/12, Rz. 14 – bverfg.de. Die zivilrechtliche Zulässigkeit hat der BGH mehrfach abgelehnt, jedoch ist keine eindeutige Linie erkennbar, siehe *Behr*, ZJS 2010, 292, 295f. Vgl. auch die Darstellungen bei BT-Drs. 16/5048, S. 37 sowie aus neuerer Zeit BGH, Urteil vom 28. Juni 2011, Az. KZR 75/10, Rz. 62 – NJW 2012, 928 - „ORWI“ und BGH, Urteil vom 25. Mai 2020, Az. VI ZR 252/1, Rz. 67 – NJW 2020, 1962.

[728] Siehe Kapitel § 2 XI. 5.

[729] Zu den technischen Hintergründen der hiermit verbundenen rechtlichen Probleme siehe Kapitel § 4 II. 4.

jedoch ist offen, welche Auswirkungen genau dies auf das Abmahnwesen haben wird. Das wird insbesondere auch davon abhängen, ob dem in der Instanzrechtsprechung vorhandenen Ansatz[730], Rechteinhabern eine sekundäre Darlegungslast dahingehend aufzuerlegen, gegen welche Mittäter sie bereits vorgegangen sind, gefolgt wird und welche Nutzer vor dem Hintergrund der technischen Funktionsweise des BitTorrent-Systems[731] als Mittäter angesehen werden. Kurz gesagt ist denkbar, dass letztlich einzelne Anschlussinhaber nur noch auf Bruchteile der bisher üblichen Beträge in Anspruch genommen werden können und somit eine wirtschaftliche Überkompensation wegfällt, sodass auch automatisch die Fragestellung entfällt, ob eine in juristischer Hinsicht verbotene Überkompensation vorliegt. Die Fragestellung ist damit in die Zukunft verschoben und wird mithin im Rahmen dieser Arbeit offen gelassen.[732]

Keine Aussagekraft hat jedenfalls mehr die Ansicht des BGH, dass eine Überkompensation auch zu verneinen sei, wenn sowohl der Anbieter als auch der Empfänger einer Datei Schadensersatz leisten, da beide urheberrechtlich betrachtet unterschiedliche Verwertungshandlungen vornehmen würden.[733] Streitgegenständlich war in dieser Entscheidung[734] das System Gnutella[735] – ein System mit zweiseitiger Dateiübertragung. Der dortige Beklagte hatte also eine Vielzahl von Musikdateien gleichzeitig über seinen Rechner zum Herunterladen angeboten, ohne jedoch, dass an dem Übertragungsvorgang andere Nutzer mitwirken können. Bei Systemen mit zweiseitiger Dateiübertragung stellt sich die Frage der Überkompensation tatsächlich nicht, da die herunterladenden Nutzer gar nicht ermittelt[736] und folglich auch nicht in Anspruch genommen werden können. Und selbst wenn Letzteres möglich wäre, so könnte von diesen „lediglich“ ein Lizenzschaden für eine Vervielfältigung verlangt werden, der sich in jedem Fall in der Höhe des Preises für eine ein-

730 AG Frankenthal, Urteil vom 25. April 2018, Az. 3c C 251/17 – juris.

731 Siehe Kapitel § 1 II. 5. und § 4 II. 4.

732 Soweit zu dieser Frage vor der Entscheidung „Konferenz der Tiere“ von Seiten der Literatur Stellung genommen worden war, wurde eine rechtlich verbotene Überkompensation bejaht, siehe *Heinemeyer* et al., MMR 2012, 705, 282.

733 BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 63f. – GRUR 2016, 176 - „Tauschbörse I“.

734 Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 3 – GRUR 2016, 176 - „Tauschbörse I“.

735 Siehe hierzu Kapitel § 1 II. 4. b).

736 Vgl. Kapitel § 3 IV.

fache Lizenz an einer Werkskopie[737] bewegen müsste. Wirtschaftlich wäre an eine Überkompensation dann zu denken, wenn alle Downloader sowie der Uploader in Anspruch genommen werden könnten, da dann ein Betrag erzielt würde, der höher ist als der Betrag der erzielt worden wäre, wenn alle das Werk auf legalem Wege erworben hätte. Ob dies juristisch ebenfalls eine Überkompensation wäre kann allerdings dahinstehen, da zweiseitige Systeme ohnehin faktisch nicht mehr relevant sind[738] und Downloader nicht ermittelt werden können, weshalb auch nicht entschieden werden muss, ob die von diesen erlangten Schadensersatzbeträge in irgendeiner Form auf den Schadensersatz des Uploaders anzurechnen wären.

Da in *filesharing*-Sachverhalten gegenwärtig also rechtliche Überlegungen zur Überkompensation nicht mehr oder noch nicht relevant sind, aber es mit einiger Wahrscheinlichkeit nicht mehr werden, kann die dogmatisch vorgelagerte Frage, ob das deutsche Schadensrecht überhaupt ein Überkompensationsverbot kennt[739] und insbesondere die Frage, ob die Entscheidung „Tripp-Trapp-Stuhl“[740], in der der BGH die mehrfache Abschöpfung von Verletzergewinnen in der Vertriebskette als zulässig erachtete, auch auf die Berechnung des Schadens im Wege der Lizenzanalogie übertragbar ist[741], dahinstehen.

3. Berechnung der fiktiven Lizenz

Der BGH war mit Einzelfragen der Berechnung der fiktiven Lizenz bisher nicht befasst. Soweit er hierzu in „Tauschbörse I“[742] Stellung genommen hat, sind die entsprechenden Ausführungen durch die Entscheidung „Konferenz der Tiere“[743] *de facto* überholt.

Wie mit der Lizenzberechnung in Zukunft umzugehen ist bzw. umgegangen

[737] Wobei hier zu überlegen wäre, ob der Lizenzschaden nicht sogar darunter liegen müsste, weil dem Rechteinhaber Gestehungskosten, die ihm für die Bereitstellung von Werkskopien durch eigene Vertriebswege entstanden sind, beim Download in einem *filesharing*-System nicht angefallen sind.

[738] Siehe Kapitel § 1 II. 4. f).

[739] Bejahend beispielsweise *Gregor*, Das Bereicherungsverbot, S. 254f. Ablehnend beispielsweise *Wagner*, AcP 2006, 352, 470f. Mit einer differenzierenden Darstellung siehe *Maute*, Dreifache Schadens(ersatz)berechnung, S. 99f., 101, 116 sowie *Raue*, Die dreifache Schadensberechnung, S. 236.

[740] BGH, Urteil vom 14. Mai 2009, Az. I ZR 98/06 – GRUR 2009, 856.

[741] Dagegen *Hoffmann*, ZGE 2017, 72, 81ff. und *Holzapfel*, GRUR 2012, 242, 247f.

[742] Siehe Kapitel § 2 VI. 1.

[743] Siehe Kapitel § 2 XI. 5.

werden sollte, wird daher in Kapitel § 5 VII. behandelt.

4. Zur Anwendung der zehnjährigen Verjährungsfrist

Nur mit Vorbehalt kann der Anwendung der zehnjährigen Verjährungsfrist des § 852 Satz 2 BGB (über § 102 Satz 2 UrhG), also die Geltendmachung des Schadensersatzes als sogenannter Restschaden, auf § 97 UrhG iVm § 19a UrhG[744] zugestimmt werden.[745] Wenn der Restschadensersatzanspruch auch nicht an die Voraussetzungen der §§ 812ff. BGB gebunden ist, es sich also um eine Rechtsfolgenverweisung auf § 818 BGB handelt[746], setzt die Verweisung in § 102 Satz 2 UrhG zumindest voraus, dass durch die Verletzung „*etwas*“ auf Kosten des Berechtigten erlangt wird.

Hinsichtlich des Erlangten ist der Wortlaut mit der Verwendung des Begriffs „*etwas*“ – in Orientierung an § 812 Abs.1 Satz 1 BGB – denkbar weit zu verstehen, sodass dem BGH darin zuzustimmen ist, dass dieser auch im Rahmen von § 102 Satz 2 UrhG bloße Gebrauchsvorteile umfassen kann.[747] Der BGH scheint als Gebrauchsvorteil des *filesharing*-Vorgangs allerdings den Gebrauch des verletzten Rechts ohne rechtlichen Grund zu sehen.[748] Damit setzt er die Verletzung und das erlangte Etwas gleich, das Erlangte ist also die öffentliche Zugänglichmachung. Das ist mit dem Wortlaut des § 102 Satz 2 UrhG nicht vereinbar, da demgemäß das Etwas „*durch*“ die Verletzung erlangt werden muss, Verletzung und erlangtes Etwas also zwei verschiedene Dinge sein müssen. Allenfalls ließe sich daran denken, als erlangten Gebrauchsvorteil die Möglichkeit anzusehen, von den anderen Nutzern Dateifragmente zu erhalten, da dies im BitTorrent-System in technischer Hinsicht typischerweise voraussetzt, dass umgekehrt anderen Nutzern Fragmente

[744] Unbeschadet dessen, dass eine öffentliche Zugänglichmachung, auch in Mittäterschaft, abzulehnen ist, siehe Kapitel § 4 II. 4.

[745] So aber festgehalten in BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 92ff. – GRUR 2016, 1280 - „Every time we touch“. Später noch einmal bestätigt durch BGH, Beschluss vom 23. Januar 2017, Az. I ZR 265/15 – ZUM 2017, 596.

[746] LG Köln, Urteil vom 17. Mai 2018, Az. 14 S 32/17, Rz. 40 – juris.

[747] BGH, Urteil vom 15. Januar 2015, Az. I ZR 148/13, Rz. 34 – GRUR 2015, 780 - „Motorradteile“. In dieser Entscheidung hatte der Beklagte unberechtigt Fotos zu Werbezwecken auf seiner Webseite verwendet.

[748] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 95f. – GRUR 2016, 1280 - „Every time we touch“. Diese Lesart auch bei *Reber* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 102 UrhG, Rz. 5.

zur Verfügung gestellt wurden.[749] Das erlangte Etwas ist also die Vervielfältigung der Zieldatei auf dem Rechner des jeweiligen Nutzers, die durch die öffentliche Zugänglichmachung einzelner Fragmente ermöglicht wird. Diese geschieht auch „*auf Kosten*“ des betroffenen Rechteinhabers: In Anlehnung an die Nichtleistungskondition ist auch in § 102 Satz 2 UrhG „*auf Kosten*“ so zu verstehen, dass das erlangte Etwas aus dem Vermögen des Rechteinhabers stammen muss.[750] Zur Vervielfältigung ist nur der Rechteinhaber berechtigt, die widerrechtliche Vervielfältigung „stammt“ also aus dessen Vermögen.[751]

In der Praxis stellt sich freilich das Problem, dass in *filesharing*-Verfahren ein Download – auch wenn er höchstwahrscheinlich stattgefunden hat – nie nachgewiesen wird[752], sondern nur der Upload. Abgesehen davon ist rechtlich zwar die Anwendung der zehnjährigem Verjährungsfrist im Ergebnis dogmatisch vertretbar, jedoch kann der vom BGH gezogenen Rechtsfolge nicht zugestimmt werden: Er spricht gemäß § 818 Abs.1 BGB Wertersatz zu; da er allerdings als erlangtes Etwas die Verletzungshandlung selbst ansieht, gewährt er als Wertersatz eine Lizenzgebühr für eine öffentliche Zugänglichmachung.[753] Erlangtes Etwas ist jedoch nur die Vervielfältigung, sodass nach Ablauf der dreijährigen Regelverjährungsfrist (für den Schadensersatzanspruch) bis zum Ablauf der zehnjährigen Verjährungsfrist richtigerweise nur Wertersatz für eine Vervielfältigung verlangt werden dürfte, nicht aber ein Betrag, der dem Schadensersatz für eine öffentliche Zugänglichmachung entspricht.

749 Siehe Kapitel § 1 II. 5. b).

750 *Wendehorst* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 812 BGB, Rz. 110.

751 In privaten Börsen wird neben der Vervielfältigung zudem eine verbesserte *seedratio* erlangt, siehe Kapitel § 1 II. 5. c). Diese ermöglicht jedoch nur den Zutritt zu Schwärmen bezüglich aller möglicher anderer Dateien. Dieser Zutritt weist also keinen Bezug zu dem Vermögen des jeweils betroffenen Rechteinhabers auf.

752 Siehe Kapitel § 1 IV. 7. c) dd).

753 BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 96 – GRUR 2016, 1280 - „Every time we touch“.

X. Zum Gesetz gegen unseriöse Geschäftspraktiken

Wie aufgezeigt[754], sollte das Gesetz gegen unseriöse Geschäftspraktiken den „Missbrauch“[755] von Abmahnungen im Urheberrecht eindämmen, ohne dass klar formuliert wurde, worin der Missbrauch eigentlich liegt.

1. Wirkungsvolle Regelungen

Dies soll nicht bedeuten, dass das Gesetz völlig untauglich ist. Im Gegenteil: die Abschaffung des fliegenden Gerichtsstandes für nicht-gewerblich Handelnde in § 104a UrhG hat für Abgemahnte eine große Hürde für die Inanspruchnahme von Rechtsschutz beseitigt, da nun erstens das Reisekosten-Risiko und der Reiseaufwand deutlich vermindert sind[756], zweitens eine Konzentration der Verfahren bei Gerichten, deren Rechtsauffassungen die Rechteinhaber als besonders günstig für sich erachteten, nicht mehr möglich ist. Umgekehrt können auch Gerichte, die bestimmte Rechtsfragen anders beantworten als andere Gerichte oder neue Rechtsfragen aufwerfen, nicht mehr gemieden werden. Im Ergebnis sichert dies eine verbesserte Pluralität der Rechtsprechung[757].

Positiv zu bewerten ist grundsätzlich auch § 97a Abs.2 UrhG[758], der Rechteinhabern die Pflicht auferlegt, ihre Abmahnung inhaltlich zu präzisieren. Die Anforderungen dieser Norm stellen aber das absolute Minimum dar; sie ähneln den Voraussetzungen des § 11a RDG, der ebenfalls durch das Gesetz gegen unseriöse Geschäftspraktiken eingeführt wurde. Es sollte selbstverständlich sein, dass ein Forderungsschuldner über den genauen Inhalt der behaupteten Forderung nicht im Unklaren gelassen werden darf. Fälle mit

---

754 Siehe Kapitel § 2 V.

755 Das Wort wird hier umgangssprachlich verwendet, ein Rechtsmissbrauch im Sinne von § 242 BGB ist nicht gemeint.

756 Früher bestand für den Abgemahnten theoretisch das Risiko, für eine mündliche Verhandlung beispielsweise von Kiel nach München kommen sowie die Reisekosten des fremden und gegebenenfalls eigenen Anwalts tragen zu müssen.

757 Die – soweit noch keine eindeutige höchstgerichtliche Rechtsprechung zu einer bestimmten Frage existiert – nach Auffassung des Verfassers auch wünschenswert ist, da so in den Berufungs- und Revisionsentscheidungen eine höhere Wahrscheinlichkeit besteht, dass alle relevanten Argumente berücksichtigt werden.

758 Dessen Satz 1 Nr. 4 durch den Austausch des Wortes „ob“ mit „inwieweit“ durch das Gesetz zur Stärkung des fairen Wettbewerbs, BGBl. I S. 2568, noch zusätzlich leicht zu Gunsten der Abgemahnten verbessert wurde.

filesharing-Bezug sind jedoch ungleich komplexer als die gewöhnliche Forderungseintreibung gegenüber Privatpersonen, auf die § 11a RDG abzielt, entsprechend höher sollten auch die inhaltlichen Anforderungen an eine hierauf bezogene Abmahnung sein.[759]

2. Im Wesentlichen wirkungslose Regelungen

Gut gemeint war die Deckelung der Höhe der Summe in § 97a Abs.3 UrhG, die als Aufwendungsersatz verlangt werden kann. Laut der Gesetzesbegründung beträfen die Beschwerden der Abgemahnten häufig nicht die Behauptung der Rechtsverletzung selbst, sondern die Forderungshöhe.[760] An der Forderungshöhe hat sich durch das Gesetz gegen unseriöse Geschäftspraktiken jedoch nichts geändert, da nach Inkrafttreten des Gesetzes statt höherer Abmahngebühren einfach höhere Schadensersatzbeträge verlangt wurden, was letztlich durch die Rechtsprechung abgesegnet ist, da diese eine relativ freie Schätzung des lizenzanalogen Schadens erlaubt und auch selbst vornimmt.[761] Eine Deckelung oder Pauschalierung, die nicht zugleich auch am Schadensersatz ansetzt, ist folglich wirkungslos. Weiterhin betrifft die Deckelung dem Wortlaut des § 97a Abs.3 Satz 2 UrhG nach nur Beseitigungs- und Unterlassungsansprüche, sodass zusätzlich noch Abmahngebühren für die Geltendmachung des Schadensersatzanspruches verlangt werden können, die damit – wie letzterer selbst – variabel sind. § 97a Abs.3 UrhG ist also – anders als intendiert – nicht geeignet, die Forderungshöhe insgesamt zu begrenzen.

Darüber hinaus ermöglicht § 97a Abs.3 Satz 4 UrhG, dass die Deckelung keine Anwendung finden muss, nämlich dann, wenn diese nach den besonderen Umständen des einschlägigen Einzelfalls unbillig wäre. In der Vorgängervorschrift des § 97a Abs.2 UrhG hatte der BGH die dortige Deckelung bei *filesharing* nicht angewandt, da Letzteres nie ein „*einfach gelagerter Fall*“ im Sinne der Norm sei.[762] Eine solche „Bereichsausnahme“ scheint in § 97a Abs.3 Satz 4 UrhG zwar versperrt, da dessen Wortlaut nach der jeweils einschlägige *Einzel*fall einen besonderen Umstand enthalten muss, folglich nicht ein ganzer Sachbereich pauschal einen besonderen Umstand darstellen kann;

[759] Siehe Kapitel § 5 IX.
[760] BT-Drs. 17/13057, S. 11.
[761] Siehe hierzu die Kapitel § 3 V. 6. und § 4 IX. 3.
[762] Siehe Kapitel § 2 III. 2.

zudem betreffen an Privatpersonen adressierte Abmahnungen wegen Urheberrechtsverletzungen schon rein empirisch betrachtet nahezu ausschließlich das *filesharing* [763] – käme § 97a Abs.3 Satz 4 UrhG hingegen bei *filesharing* immer zu Anwendung, wäre das mit der Norm erkennbar intendierte Regel-Ausnahme-Verhältnis umgekehrt. Jedoch ist nicht gesichert, dass dies im Zweifel von der Rechtsprechung auch so gesehen wird.[764] § 97a Abs.3 Satz 4 UrhG konterkariert mithin unnötigerweise das gesetzgeberische Ziel einer rechtssicher prognostizierbaren Gebührenrechtsprechung.

Hinsichtlich der Höhe der erstattungsfähigen Kosten hat der Gesetzgeber berücksichtigt, dass Rechteinhaber vereinzelt höhere Kosten geltend gemacht haben, als tatsächlich angefallen sind[765] – und dementsprechend auch gemäß § 97a Abs.3 Satz 1 UrhG nur die *erforderlichen* Aufwendungen, nicht eine der Obergrenze entsprechende Summe *per se* als erstattungsfähig erachtet. Jedoch haben Abgemahnte keine Möglichkeit herauszufinden, welche Kosten dem Rechteinhaber tatsächlich angefallen sind. Der Rechtsprechung des BGH zu Folge ist es unbeachtlich, wenn der Anschlussinhaber bestreitet, dass dem Rechteinhaber Gebühren oberhalb oder genau auf Höhe der Deckelungsgrenze angefallen sind („Bestreiten ins Blaue hinein“).[766] Zwar ist diese Rechtsprechung des BGH durchaus kritikwürdig, weil der Abgemahnte keinen Einblick in die Vergütungsstrukturen des Rechteinhabers hat, jedoch Fälle aus der *filesharing*-Abmahnpraxis bekannt sind, in denen tatsächlich niedrigere Gebühren geltend gemacht wurden als an die für die Abmahnung tätig werdende Kanzlei zu leisten waren[767]; dies müsste eigentlich genügen, um ein Bestreiten der behaupteten Gebührenhöhe generell als substantiiert anzusehen (das entspräche auch dem Willen des Gesetzgebers, der – wie aufgezeigt – davon ausging dass zu hoch veranschlagte Gebühren ein tatsächlich vorhandenes Problem sind und folglich sichergestellt sein muss, dass Abgemahnte nur auf die tatsächlich angefallenen Gebühren in Anspruch

[763] Siehe Kapitel § 3 IV.

[764] Allerdings geht der Verfasser wegen der genannten Argumente nicht davon aus, dass der BGH dies tun wird. Sollte er dies doch tun, dann wäre auch die Berechnung des Unterlassungsstreitwerts, mithin auch die Entscheidungen Tauschbörse IV-VII wieder relevant.

[765] BT-Drs. 17/13057, S. 11; zu den bekannten Fallen siehe Kapitel § 3 VI.

[766] BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 69 – GRUR 2016, 184 - „Tauschbörse II“.

[767] Siehe Kapitel § 3 VI.

genommen werden). Allerdings ist nicht davon auszugehen, dass der BGH seine Rechtsprechung in diesem Punkt ändern wird. Im Ergebnis müssen Abgemahnte also *de facto* immer Gebühren in Höhe der Deckelungsgrenze leisten, auch wenn tatsächlich niedrigere Gebühren angefallen sein sollten. Die Beschränkung des Gebührenersatzanspruchs auf erforderliche Gebühren ist mithin wirkungslos.

Letztlich wirkungslos ist auch § 97a Abs.4 UrhG. Dieser spricht dem Abgemahnten einen Anspruch auf Erstattung der außergerichtlich angefallenen Rechtsverteidigungskosten zu, wenn die Abmahnung unberechtigt oder unwirksam war, also entweder die geltend gemachten Ansprüche nicht bestehen oder die Anforderungen des § 97a Abs.2 UrhG nicht eingehalten wurden. Eine unberechtigte Abmahnung löst den Ersatzanspruch jedoch nur aus, wenn es für den Abmahnenden im Zeitpunkt der Abmahnung erkennbar war, dass die Abmahnung unberechtigt ist. Letzteres dürfte praktisch nie der Fall sein, da ein Abmahnender in *filesharing*-Fällen im Zeitpunkt der Abmahnung nicht erkennen kann, ob der abgemahnte Anschlussinhaber über die sekundäre Darlegungslast als Täter haften wird oder nicht. Zudem gehen Teile der Rechtsprechung wohl davon aus, dass eine Abmahnung nur dann unberechtigt ist, wenn dem Abmahnenden *insgesamt* kein Anspruch gegen den Abgemahnten zusteht.[768] Da unter Geltung des 3. TMGÄndG praktisch immer ein Sperranspruch gegen den Anschlussinhaber im Raum steht, ist auch nach dieser Betrachtung ein Ersatzanspruch nach § 97a Abs.4 UrhG in *filesharing*-Konstellationen grundsätzlich ausgeschlossen. § 97a Abs.4 UrhG hat damit in allen Auslegungsvarianten keinen praktischen Anwendungsfall, ist also überflüssig.

Zu den Verbesserungsvorschlägen des Verfassers alle soeben genannten Kritikpunkte betreffend siehe Kapitel § 5 XI., XII. und XIII.

3. Zum Verhältnis von § 7 Abs.4 Satz 3 TMG zu § 97a UrhG

Zuletzt ist darauf hinzuweisen, dass § 7 Abs.4 Satz 3 TMG, demgemäß die Geltendmachung und Durchsetzung einer Sperranordnung keinen Anspruch auf Ersatz der hierfür angefallenen vor- und außergerichtlichen Aufwendungen auslöst, Rechteinhaber nicht daran hindert, in einer Abmahnung zunächst die in § 97a Abs.3 UrhG genannten Kosten geltend zu machen.

[768] LG München I, Urteil vom 20. April 2017, Az. 7 O 14719/12, Rz. 48 – juris.

Schließlich können sie bei Versand der Abmahnung noch nicht wissen, ob der Anschlussinhaber als Täter oder „lediglich“ nach § 7 Abs.4 TMG haften wird. Folglich ist eine solche Abmahnung auch dann nicht als rechtswidrig anzusehen, wenn der betroffene Anschlussinhaber im Falle eines gerichtlichen Verfahrens nicht als Täter haftet.[769] Hätte der Gesetzgeber mit dem 3. TMGÄndG etwas anderes gewollt, so hätte er in dessen Zuge auch den § 97a UrhG entsprechend ändern müssen. Dafür, dass auch der BGH dies so sehen wird, spricht seine bisherige Rechtsprechung, derzufolge die Abmahnung in *filesharing*-Konstellationen (auch) der Sachverhaltsaufklärung dient und der Rechteinhaber sich nicht mit einer unförmlichen Nachfrage beim Anschlussinhaber mit der Bitte um Sachverhaltsaufklärung begnügen muss.[770]

XI. Zum Rechtsmissbrauch durch Abmahnungen (§ 242 BGB)

Der BGH hatte in „Tauschbörse II“ mit recht knappen Worten der Anwendung des § 242 BGB auf *filesharing*-Abmahnungen eine Absage erteilt[771] und knüpft damit an frühere Rechtsprechung zum Urheberrecht an[772].

Demgegenüber ist in der Literatur erörtert worden, ob sich vereinzelte Aspekte des *filesharing*-Abmahnwesens mit § 242 BGB erfassen lassen. Die Frage müsste jedoch in präzisierter Form lauten, welche Aspekte welchen von der Rechtsprechung im Rahmen des § 242 BGB entwickelten Kategorien des Rechtsmissbrauchs[773] zugeordnet werden können.

Die Erschließung einer eigenständigen Profitquelle mittels des lizenzanalogen Schadens könnte sich beispielsweise als institutioneller Rechtsmissbrauch

[769] Vgl. LG München I, Urteil vom 20. April 2017, Az. 7 O 14719/12, Rz. 48 – juris.

[770] BGH, Urteil vom 22. März 2018, Az. I ZR 265/16, Rz. 19ff. – GRUR 2018, 914 - „Riptide“.

[771] Siehe Kapitel § 2 VI. 2.

[772] Vgl. BGH, Urteil vom 31. Mai 2012, Az. I ZR 106/10, Rz. 16ff. – GRUR 2013, 176 - „Ferienluxuswohnung“.

[773] § 242 BGB lässt sich als – bewusste oder unbewusste – Delegationslücke einstufen, eine Norm also, bei der es der Rechtsprechung überlassen ist, sie mit Inhalt zu füllen, siehe BVerfG, Beschluss vom 24. Februar 2015, Az. 1 BvR 472/14, Rz. 39 – bverfg.de. Daher sollte versucht werden, neue Phänomene in bereits existierende, vom BGH entwickelte Fallgruppen einzuordnen. Zur Methodik der Delegationslücke siehe *Dück*, ZfPW 2018, 76, 85ff.

darstellen. Mit dieser Kategorie lässt sich der strukturelle Missbrauch eines Rechtsinstituts fassen.[774] Während also bei der Kategorie des Rechtsmissbrauchs im eigentlichen Sinne[775] nur jeweils ein singuläres Schuldverhältnis betrachtet werden kann, können beim institutionellen Rechtsmissbrauch eine Menge von Schuldverhältnissen in ihrer Gesamtheit bewertet werden. Wenn mithin – jedes einzelne Schuldverhältnis betrachtet – der beim *filesharing* zugesprochene, lizenzanaloge Schaden eine wirtschaftliche Überkompensation darstellt[776], summiert sich dies in der Gesamtbetrachtung zu einer zweckwidrigen Profiterzielung auf. In beiden Betrachtungsweisen – institutioneller Rechtsmissbrauch und Rechtsmissbrauch im Einzelfall – stellt sich als „Fehlerursache" aber bereits die Mittäterschaftslösung sowie die Schadensberechnung dar; die Möglichkeit der zweckwidrigen Profiterzielung ist nur eine unmittelbare Folge hiervon, die sich aus der großen Menge gleich gelagerter Fälle ergibt. Eine Korrektur muss also bereits dort ansetzen; es wäre widersinnig, einerseits die Mittäterschaftslösung und die Schadensberechnung zu billigen, andererseits die unmittelbaren Folgen der Schadensberechnung über § 242 BGB zu missbilligen.[777]

Abgesehen hiervon ist § 242 BGB in *filesharing*-Konstellationen für den Fall ins Spiel gebracht worden, dass der Abmahnende zwar ein ausschließliches Nutzungsrecht am abgemahnten Werk hat, dieses jedoch schuldrechtlich auf das Vorgehen gegen Endnutzer in *filesharing*-Konstellationen begrenzt ist.[778] Das Vorgehen aus einem solcherart begrenzten Recht sei rechtsmissbräuchlich, da es dem Abmahnenden dann an einem schützenswerten Eigeninteresse fehlen würde, weil er mit dieser Konstruktion kein tatsächlich nutzbares Verwertungsrecht innehabe.[779] Da solche Konstellationen praktisch aber nahezu

[774] *Sutschet* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 242 BGB, Rz. 51.

[775] *Sutschet* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 242 BGB, Rz. 57ff.

[776] Bereits auf Ebene eines einzelnen Schuldverhältnisses die sachfremde Motivation der Profiterzielung festzustellen, wird letztlich immer auch an der Beweisbarkeit scheitern, vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 7/14, Rz. 70 – GRUR 2016, 184 - „Tauschbörse II".

[777] Daher kann auch dahinstehen, ob die Kategorie des institutionellen Rechtsmissbrauchs unter Geltung des grundgesetzlichen Bestimmtheitsgrundsatzes überhaupt noch haltbar ist, vgl. *Schubert* in: Säcker et al., MüKo-BGB, 8. Aufl. 2019, § 242 BGB, Rz. 206.

[778] Ein von vornherein auf diesen Bereich dinglich beschränktes Nutzungsrecht existiert nicht, siehe Kapitel § 3 I.

[779] *Adolphsen/Mayer/Möller*, NJOZ 2010, 2394, 2398.

überhaupt nicht vorkommen[780], wird diese Frage hier nicht entschieden.

Zuletzt ist vorgeschlagen worden, Abmahnungen, die Gerichtsentscheidungen, die für den Abmahnenden unter Umständen ungünstig sind, verschweigen, als rechtsmissbräuchlich anzusehen.[781] Zwar ist eine solche Anforderungen an *filesharing*-Abmahnungen nach Auffassung des Verfassers wünschenswert[782]; jedoch kann diese Auffassung nicht durch Auslegung dem Gesetz entnommen werden. In der Begründung zum Gesetz gegen unseriöse Geschäftspraktiken hat sich der Gesetzgeber mit der Problematik der *filesharing*-Abmahnungen auseinandergesetzt und die Anforderungen des § 97a Abs.2 UrhG offensichtlich als ausreichenden Inhalt einer Abmahnung genügen lassen. Diese Wertung ist dem Grundsatz der Gewaltenteilung folgend zu respektieren und darf nicht über § 242 BGB „korrigiert" werden.

Generell ist allen Versuchen, Aspekte der *filesharing*-Abmahnungen, die als ungerecht empfunden werden, über § 242 BGB fassen zu wollen, die Existenz des § 8 Abs.4 UWG entgegenzuhalten: der Gesetzgeber hat sich bezüglich dem UWG dazu entschlossen, eine Missbrauchsnorm zu erlassen. In der Begründung zum Gesetz gegen unseriöse Geschäftspraktiken wurde die Norm ausdrücklich angeführt[783], war dem Gesetzgeber in diesem Zuge also „bewusst". Da er sich für das Urheberrecht nicht entschieden hat, eine entsprechende Norm einzuführen, sondern stattdessen konkrete Probleme der Abmahnpraxis spezifisch in den §§ 97a und 104a UrhG zu behandeln, darf eine solche Norm nicht durch eine entsprechende Auslegung des § 242 BGB quasi über die „Hintertür" eingeführt werden.[784]

Lediglich der Vollständigkeit halber ist daher anzumerken, dass der BGH an die Anwendbarkeit des § 8 Abs.4 UWG hohe Anforderungen stellt; beispielsweise erachtet er es als erforderlich, dass die Abmahnung allein dem Zweck dient, den Abmahnkostenerstattungsanspruch entstehen zu lassen oder dass der Abmahnende neben der Abmahntätigkeit nur in geringem Umfang ei-

[780] Siehe Kapitel § 3 I.

[781] *Tyra*, ZUM 2009, 934, 942; *Haedicke*, Patente und Piraten, S. 19f.

[782] Siehe Kapitel § 5 IX.

[783] BT-Drs. 17/13057, S. 10.

[784] Es ist jedoch darauf hinzuweisen, dass der BGH aus § 8 Abs.4 UWG keinen Umkehrschluss für das Urheberrecht gezogen hat; allerdings erging die entsprechende Entscheidung vor Inkrafttreten des Gesetz gegen unseriöse Geschäftspraktiken, vgl. BGH, Urteil vom 31. Mai 2012, Az. I ZR 106/10, Rz. 16f. – GRUR 2013, 176 - „Ferienluxuswohnung".

ner eigentlichen gewerblichen Tätigkeit nachgeht.[785] Dies ist in *filesharing*-Konstellationen praktisch nie der Fall, da die Abmahnenden dort primär die Erlangung von Schadensersatz begehren und das Aussprechen von Abmahnungen neben ihrer eigentlichen gewerblichen Tätigkeit nur von untergeordneter Bedeutung ist.[786] Eine Übertragung dieser Rechtsprechung des I. Senats auf *filesharing*-Fälle hätte also gegenüber „Tauschbörse II“ keine Änderung zur Folge.

Der Rechtsprechung des BGH zur Anwendung des Rechtsmissbrauchseinwands gegen *filesharing*-Abmahnungen kann im Ergebnis mithin zugestimmt werden.

XII. Zur Pflicht zur Antwort auf Abmahnungen

Der BGH hat eine solche Pflicht verneint[787]; unterliegt der klagende Rechteinhaber also im Prozess, weil der beklagte Anschlussinhaber dort erst seine sekundäre Darlegungslast erfüllt (und nicht schon nach Erhalt der Abmahnung Auskunft über die Anschlussnutzung gibt), kann er die Kosten des Rechtsstreits nicht vom Beklagten herausverlangen, und zwar weder über einen materiell-rechtlichen noch über einen prozessualen Anspruch.

1. Materiell-rechtlicher Anspruch

Das Anspruchsziel – Erstattung der Prozesskosten – ist auf das negative Interesse gerichtet; inhaltlich geht es also um einen Schadensersatz. Als Anspruchsgrundlage kommen daher Vertrag iVm § 280 Abs.1 ZPO, § 280 BGB iVm § 241 Abs.2 BGB wegen Verletzung einer Nebenpflicht aus einer gesetzlichen Sonderverbindung, *culpa in contrahendo* (§ 311 Abs.2 BGB), Geschäftsführung ohne Auftrag (§§ 677ff. BGB) oder Delikt (§ 826 BGB, § 823 Abs.1 BGB) in Betracht.

---

785 BGH, Urteil vom 26. April 2018, Az. I ZR 248/16, Rz. 20f. – juris - „Abmahnaktion II“. Gleiches galt nach der, zumindest in *filesharing*-Fällen wohl (nicht mehr) anwendbaren „Ferienluxuswohnung“-Rechtsprechung, siehe BGH, Urteil vom 31. Mai 2012, Az. I ZR 106/10, Rz. 21 – GRUR 2013, 176 - „Ferienluxuswohnung“.

786 Siehe Kapitel § 3 VI.

787 Siehe Kapitel § 2 XI. 8.

a) Vertrag iVm § 280 BGB

Ein Vertrag liegt in *filesharing*-Konstellationen dann vor, wenn der Abmgemahnte eine strafbewehrte Unterlassungserklärung abgegeben oder diese modifiziert hat und der Rechteinhaber die Modifizierung annimmt. Eine Pflicht, den wahren Täter zu ermitteln und/oder mitzuteilen, kann sodann als Nebenpflicht im Sinne von § 241 Abs.2 BGB bestehen. Dem BGH ist zuzustimmen, dass es für die Annahme einer solchen Nebenpflicht im Einzelfall darauf ankommt, was die Parteien vereinbart haben.[788] Bei einer – in der Praxis häufig vorkommenden – modifizierten Unterlassungserklärung, die ohne Anerkennung einer Rechtspflicht abgegeben wird, liegt es daher nahe zu folgern, dass – im Falle der Annahme durch den Rechteinhaber – den Anschlussinhaber auch keinerlei Pflicht zur Ermittlung und/oder Mitteilung des wahren Täters trifft.[789]

Da die Fälle, in denen der Rechteinhaber eine modifizierte Unterlassungserklärung annimmt oder der Anschlussinhaber unmittelbar die ihm angebotene Unterlassungserklärung (die regelmäßig mit einer Verpflichtung zur Leistung der Abmahngebühren und Schadensersatz verbunden ist) in der Praxis jedoch eher selten anzutreffen sind[790], dürften die praktischen Auswirkungen dieses Aspekts der Entscheidung „Saints Row“ des BGH begrenzt bleiben.

b) Verletzung einer Nebenpflicht aus einer gesetzlichen Sonderverbindung

In dem der Entscheidung „Saints Row“ zu Grunde liegenden Sachverhalt haftete der beklagte Anschlussinhaber weder als Täter noch als Störer und ein Anspruch aus § 7 Abs.4 TMG war nicht streitgegenständlich. Der BGH konnte also offenlassen, ob bei Bestehen einer derartigen gesetzlichen Sonderverbindung aus § 241 Abs.2 BGB eine Antwortpflicht folgt.[791]

Diese Frage ist daher in Kapitel § 5 X. *de lege lata* zu beantworten.

---

[788] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 21 bis 32 – juris - „Saints Row“.

[789] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 27 – juris - „Saints Row“.

[790] Siehe Kapitel § 3 V. 6.

[791] Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 43ff. – juris - „Saints Row“.

c) *culpa in contrahendo* (§ 311 Abs.2 BGB)

Das Entstehen eines vorvertraglichen Schuldverhältnisses durch eine Abmahnung lehnt der BGH für *filesharing* -Konstellationen augenscheinlich generell ab, wobei er in seiner Begründung nicht genau zwischen § 311 Abs.2 Nr.2 BGB und § 311 Abs.2 Nr.3 BGB differenziert.[792] Diese betrifft jedoch den Aspekt der Vertragsanbahnung und damit § 311 Abs.2 Nr.2 BGB. Der BGH hält insofern zutreffend fest, dass es dem Abmahnenden nicht um eine offene Vertragsverhandlung, sondern um die Unterbreitung eines vorgefassten Angebots geht und § 311 Abs.2 Nr.2 BGB daher keine Anwendung finden kann.

Zu ergänzen ist entsprechend, dass auch eine Sonderverbindung auf Grundlage von § 311 Abs.2 Nr.3 BGB ausscheiden muss. Einem Urteil des AG München und einer Literaturstimme zu Folge[793], stelle eine *filesharing*-Abmahnung jedoch einen „*geschäftlichen Kontakt*“ im Sinne von § 311 Abs.2 Nr.3 BGB dar. Der BGH hatte allerdings in einem anderen Zusammenhang bereits ausdrücklich entschieden, dass die bloße Geltendmachung eines Anspruches grundsätzlich keine Sonderverbindung zwischen Anspruchsteller und Anspruchsgegner entstehen lasse.[794] Zudem lässt sich auch der Gesetzesbegründung zur Schuldrechtsreform entnehmen, dass „geschäftliche Kontakte“ nur solche Kontakte sind, bei denen zwar noch kein Vertrag angebahnt wird, aber vorbereitet werden soll.[795] Eine *filesharing*-Abmahnung dient nicht der Vorbereitung eines Vertrages, sondern der Geltendmachung einer Forderung auf Grund eines behaupteten Delikts. Folglich scheidet auch eine Sonderverbindung nach § 311 Abs.2 Nr.3 BGB aus.

Wollte man dennoch eine *culpa in contrahendo* dem Grunde nach annehmen annehmen, so wäre im nächsten Schritt fraglich, ob eine Verletzung der Antwortpflicht kausal für den Schaden, mithin also kausal für die Klageerhebung war. Der Rechteinhaber könnte hier in Beweisschwierigkeiten geraten, da beispielsweise Rechtsanwälten, die auf die Verteidigung von Anschlussinhabern spezialisiert sind, durchaus zahlreiche Fälle bekannt sein dürften, in

[792] Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 36f. – juris - „Saints Row“.

[793] AG München, Endurteil vom 4. November 2016, Az. 224 C 11869/16, Rz. 26 – juris; *Lach*, jurisPR-ITR 17/2017, Anm. 3.

[794] BGH, Urteil vom 12. Dezember 2006, Az. VI ZR 224/05, Rz. 13f. – NJW 2007, 1458.

[795] BT-Drs. 14/6040, S. 163.

denen gegen Letztere geklagt wurde, obwohl sie bereits vorprozessual Auskünfte gemacht hatten, die im Prozess dann zur Erfüllung der sekundären Darlegungslast geführt haben, die Erfüllung oder Nichterfüllung der Antwortpflicht für Rechteinhaber dort also irrelevant war.[796]

Der Vollständigkeit halber ist zu ergänzen, dass auch die „Bastei Lübbe"-Entscheidung des EuGH kein anderes Ergebnis – beispielsweise dergestalt, dass § 311 Abs.2 Nr.3 BGB europarechtskonform dahingehend auszulegen wäre, dass der Erhalt einer Abmahnung in *filesharing*-Konstellationen zu einem vorvertraglichen Schuldverhältnis führt, das Nebenpflichten analog zur sekundären Darlegungslast enthält – nahelegt.[797] Die „Bastei Lübbe"-Entscheidung ist allein damit befasst, wie die im Rahmen eines Prozessrechtsverhältnisses bestehende sekundäre Darlegungslast im Lichte des Unionsrechts anzuwenden ist.[798]

In diesem Sinne hat der BGH in „Saints Row" auch zutreffend festgehalten, dass die EnforcementRL im Übrigen keine Hinweise darauf gibt, dass in europarechtskonformer Auslegung ein vorgerichtliches Schuldverhältnis anzunehmen wäre, insbesondere weil der Auskunftsanspruch nach Art. 8 EnforcementRL die Auskunftsrechte abschließend aufzählt und eine Pflicht des Anschlussinhabers zur Ermittlung und/oder Mitteilung des wahren Täters dort nicht aufgeführt ist.[799]

d) Geschäftsführung ohne Auftrag (§§ 677ff. BGB)

Der BGH hat offen gelassen, ob Fremdgeschäftsführungswille vorliegt, da es in der von ihm zu entscheidenden Konstellation mangels einer gesetzlichen Sonderverbindung an einem Handeln im objektiven Interesse des beklagten Anschlussinhabers fehlte.[800]

Folglich wird in Kapitel § 5 X. *de lege lata* erörtert, wie die Rechtslage zu

[796] So auch *Forch*, GRUR-Prax 2014, 367, 369.

[797] So jedoch implizit AG München, Urteil vom 5. November 2018, Az. 132 C 14777/18, Rz. 36, 54 – MMR 2019, 409.

[798] Vgl. EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 35f. – ECLI:EU:C:2018:841 - „Bastei Lübbe". Daher unzutreffend AG München, Urteil vom 5. November 2018, Az. 132 C 14777/18, Rz. 38 – MMR 2019, 409.

[799] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 74f. – juris - „Saints Row".

[800] Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 58ff. – juris - „Saints Row".

bewerten wäre, wenn Fremdgeschäftsführungswille anzunehmen wäre und bei Vorliegen einer gesetzlichen Sonderverbindung ein Handeln im objektiven Interesse des beklagten Anschlussinhabers vorliegen würde.

e) Delikt

Einen Anspruch aus § 826 BGB lehnt der BGH richtigerweise mit dem Hinweis darauf ab, dass der deliktische Anknüpfungspunkt ein Unterlassen ist und eine Handlungspflicht eine besondere Verwerflichkeit des Nichthandels erfordern würde, die die Instanzgerichte nicht festgestellt hatten.[801] Es ist kaum vorstellbar, dass in regulären *filesharing*-Konstellationen eine besondere Verwerflichkeit der unterlassenen Antwort festgestellt werden könnte. Gleiches gilt für den Schädigungsvorsatz, der entsprechend vom BGH ebenfalls verneint wurde.[802] Richtig ist allerdings auch das *obiter dictum* des BGH, dass die aktive und wissentliche Mitteilung falscher Tatsachen durch den Anschlussinhaber einen Anspruch aus § 826 BGB auslösen kann[803], was keiner weiteren Erörterung bedarf.

Zu ergänzen ist lediglich, dass auch ein deliktischer Anspruch aus § 823 Abs.1 BGB ausscheidet, da diese Norm allein in der Variante *Verletzung eines sonstigen Rechts durch Missachtung einer Verkehrssicherungspflicht* Anwendung finden könnte, jedoch der Erhalt einer Abmahnung keine Schaffung einer Gefahrenlage ist[804] und als „*sonstiges Recht*“ allein das Vermögen des klagenden Rechteinhabers (das durch den Verlust des Prozesses geschädigt wird) in Betracht kommen könnte, jedoch das Vermögen nach allgemeiner Meinung kein „*sonstiges Recht*“ im Sinne der Norm ist[805].[806]

2. Prozessualer Anspruch

Ein prozessualer Anspruch käme nur in der Konstellation in Betracht, in der der klagende Rechteinhaber, nachdem der beklagte Anschlussinhaber seine

[801] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 68ff. – juris - „Saints Row“.

[802] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 70 – juris - „Saints Row“.

[803] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 71 – juris - „Saints Row“.

[804] Die jedoch für eine Verkehrssicherungspflicht erforderlich wäre, siehe *Förster* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 823 BGB, Rz. 302.

[805] *Wagner* in: Säcker et al., MüKo-BGB, 8. Aufl. 2020, § 823 BGB, Rz. 423.

[806] Unzutreffend daher AG München, Urteil vom 5. November 2018, Az. 132 C 14777/18, Rz. 36 – MMR 2019, 409.

sekundäre Darlegungslast erfüllt und also dem Kläger eine Prozessniederlage droht, die Klage zurücknimmt (was nach § 269 Abs.1 ZPO auch ohne Einwilligung des Beklagten bis zu Beginn der mündlichen Verhandlung zulässig ist). Mögliche Anspruchsgrundlage wäre dann § 269 Abs.3 Satz 3 1. Hs. ZPO. Die Erfüllung der sekundären Darlegungslast müsste demnach einen Wegfall des Anlasses zur Klageeinreichung vor Rechtshängigkeit darstellen.

Die Norm dient der Regelung des Falls, in dem der Anlass zur Klage zwischen Anhängigkeit und Rechtshängigkeit, also nach Einreichung aber vor Zustellung, wegfällt. Fraglich ist also zunächst, zu welchem prozessualen Zeitpunkt der „Wegfall“ in *filesharing*-Konstellationen eintritt. Dies ist regelmäßig die Erfüllung der sekundären Darlegungslast im Prozess[807]; der Wegfall tritt also ganz eindeutig nach Rechtshängigkeit ein. Für diesen Fall kann § 269 Abs.3 Satz 3 1. Hs. ZPO seinem Wortlaut nach von vornherein keine Anwendung finden. Auch eine analoge Anwendung kommt nicht in Betracht, da es dem allgemeinen Prozessrisiko eines Klägers entspricht, ob er die seinem geltend gemachten Anspruch zu Grunde liegenden Tatsachen (vorliegend also die Täterschaft des Anschlussinhabers) beweisen kann oder nicht und zudem für den Wegfall des Klageanlasses nach Rechtshängigkeit andere Instrumente wie die einseitige Erledigungserklärung für den Kläger zur Verfügung stehen; es fehlt mithin an einer planwidrigen Regelungslücke.[808]

Im Übrigen kommt der BGH nach einer eingehenden Erörterung zu dem Schluss, dass ein Anlass zur Klageeinreichung im Sinne des § 269 Abs.3 Satz 3 1. Hs. ZPO nur dann vorliegt, wenn die Klage zum Zeitpunkt der Einreichung zulässig und begründet war oder zu irgendeinem Zeitpunkt zulässig und begründet gewesen wäre.[809] Im Streitfall sei dies nicht der Fall, da die Beklagte für die Urheberrechtsverletzung nicht verantwortlich sei.[810] Dem kann für den vom BGH entschiedenen Fall sowie in *filesharing*-Konstellationen generell nicht beigepflichtet werden, und zwar auch dann nicht, wenn die Kla-

[807] So auch in der maßgeblichen Entscheidung des BGH, in der die sekundäre Darlegungslast in der Klageerwiderung erfüllt wurde, siehe BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20, Rz. 2 – juris.

[808] So im Ergebnis auch BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20, Rz. 31ff. – juris. Entsprechend kann es der BGH auch offen lassen, ob § 269 Abs.3 Satz 3 1. Hs. ZPO auf den Wegfall vor Anhängigkeit angewendet werden kann, siehe BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20, Rz. 23f. – juris.

[809] BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20, Rz. 18ff. – juris.

[810] BGH, Beschluss vom 17. Dezember 2020, Az. I ZB 38/20, Rz. 30 – juris.

ge allein auf eine Inanspruchnahme des Anschlussinhabers als Täter (und nicht auch, als Haupt-oder Hilfsantrag, nach § 7 Abs.4 TMG) gerichtet ist. Denn zum Zeitpunkt der Klageerhebung liegt nur der Vortrag des klagenden Rechteinhabers vor. Zu diesem Zeitpunkt ist noch nicht absehbar, ob der beklagte Anschlussinhaber seiner sekundären Darlegungslast nachkommen kann (was – wie in dieser Arbeit dargestellt – mit hohen rechtlichen Hürden verbunden ist sowie ergänzend tatsächlichen Hürden verbunden sein kann, insbesondere wenn für den Anschlussinhaber auf Grund einer zeitlich weit nach der Urheberrechtsverletzung erhobenen Klage eine Sachaufklärung erschwert ist), sodass davon auszugehen ist, dass er kraft tatsächlicher Vermutung als Täter in Haftung genommen werden kann. Klagen werden in *filesharing*-Konstellationen also wenn dann erst auf Grund des regelmäßig in der Klageerwiderung enthaltenen Vortrags des beklagten Anschlussinhabers unbegründet, sind zum Zeitpunkt der Erhebung folglich aber als zulässig und begründet anzusehen.

Am Ergebnis ändert dies jedoch nichts: es bleibt dabei, dass der Anlass zur Klageeinreichung in diesen Konstellationen erst nach Rechtshängigkeit wegfällt, sodass die Ablehnung der Anwendbarkeit von § 269 Abs.3 Satz 3 1. Hs. ZPO hierauf zu bejahen ist.

3. Ergebnis

Den Entscheidungen des BGH zur Pflicht zur Beantwortung von Abmahnungen kann im Ergebnis und überwiegend auch in der Begründung zugestimmt werden.

Folglich besteht also keine Pflicht, auf eine *filesharing*-Abmahnung zu antworten – insbesondere nicht in einer Form zu antworten, die dem Vortrag innerhalb der sekundären Darlegungslast entspricht. Reagiert ein Anschlussinhaber auf eine Abmahnung nicht und haftet dann in einem Folgeprozess auch nicht als Täter, löst dies also keine Schadensersatzansprüche oder prozessuale Kostenerstattungsansprüche aus.[811]

Die dogmatische Antwort auf die Frage der Antwortpflicht deckt sich zudem auch mit der in dieser Arbeit aufgestellten rechtspolitischen Überlegung, dass

[811] Umgekehrt ist ein Rechteinhaber aber auch nicht gehalten, auf eine Antwort des Abgemahnten zu reagieren, also zum Beispiel mitzuteilen, ob er dessen Vortrag für ausreichend hält.

Rechteinhaber dazu gehalten werden sollen, eine gerichtliche Klärung möglichst schnell und nicht erst Jahre nach einer Abmahnung herbeizuführen[812], zu der also die Ablehnung einer Antwortpflicht beiträgt.

XIII. Zusammenfassung der Ergebnisse

Die in diesem Teil der Arbeit analysierte Rechtsprechung des BGH zum *filesharing* vermag dogmatisch überwiegend nicht zu überzeugen.

- Der Annahme einer mittäterschaftlichen öffentlichen Zugänglichmachung eines Werkes durch die Nutzer in Tauschbörsen mit mehrseitiger Dateiübertragung steht deren technische Funktionsweise entgegen.
- Hinsichtlich der Beweistauglichkeit von Ermittlungssystemen ist der bisherigen Rechtsprechung des BGH zwar zuzustimmen, sie lädt jedoch zu Missverständnissen hinsichtlich ihrer Reichweite ein.
- Beim Auskunftsanspruch verkennt der BGH die Methodenrechtsprechung des BVerfG und erachtet deshalb fälschlicherweise ein gewerbliches Ausmaß der zu beauskunftenden Rechtsverletzung als nicht erforderlich. Auch bezüglich der Auskunft in Resellerkonstellationen kann ihm insbesondere vor dem Hintergrund seiner neueren Rechtsprechung und der des EuGH im Ergebnis nicht zugestimmt werden.
- Der Herleitung des Sicherungsanspruches stehen gegenwärtig sowohl das Europarecht als auch das Bundesrecht entgegen.
- Der Rechtsprechung zur Kostentragung kann im gegenwärtigen Rechtsrahmen allerdings zugestimmt werden.
- Die Struktur der sekundäre Darlegungslast und der tatsächliche Vermutung sowie das Verhältnis der beiden Institute zueinander hat der BGH nunmehr überzeugend hergeleitet, auch wenn zu bemängeln ist, dass dies bereits zu Beginn seiner *filesharing*-Rechtsprechung möglich gewesen wäre. Die Bestimmung des Inhalts der sekundären Darlegungslast überzeugt allerdings zum Teil nicht.
- Bei der Lizenzanalogie besteht das Problem, dass die Aussagen des BGH hierzu betreffend Tauschbörsen mit zweiseitiger Dateiübertra-

[812] Siehe Kapitel § 3 VIII., § 5 V. 3. c) und § 5 VIII.

gung getroffen wurden und gegenwärtig dogmatisch offen ist, ob und falls ja, wie, sich diese auf Systeme mit mehrseitiger Dateiübertragung übertragen lässt.

- Der Rechtsprechung zum (fehlenden) Rechtsmissbrauch durch Abmahnungen sowie zur (fehlenden) Pflicht zur Beantwortung derselben ist beizupflichten.

Auch der Gesetzgeber ist zu kritisieren:

- Das 2. und 3. TMGÄndG haben gegenüber der früheren Rechtslage nur mehr Auslegungsschwierigkeiten und Haftungsrisiken gebracht.
- Das Gesetz gegen unseriöse Geschäftspraktiken hat zum Teil echte, sinnvolle Verbesserungen gebracht; andere Aspekte des Gesetzes waren zwar gut gemeint, jedoch wirkungslos.

§ 5 Möglichkeiten *de lege lata* und Alternativen *de lege ferenda*

I. Einleitung

Im dritten Kapitel dieser Arbeit wurde aufgezeigt, dass die existierende Rechtslage zu einem Abmahnwesen geführt hat, das rechtspolitisch zu kritisieren ist. Im vierten Kapitel dieser Arbeit wurde aufgezeigt, dass die höchstgerichtliche Rechtsprechung sowie die Gesetzgebung, die zu dieser Rechtslage geführt hat, in rechtsdogmatischer Hinsicht in weiten Teilen nicht haltbar ist. Im fünften und letzten Kapitel dieser Arbeit werden daher Alternativen *de lege ferenda* entwickelt[1], die die Situation der Anschlussinhaber verbessern, ohne dabei die berechtigten Interessen der Urheberrechtsindustrie außer Acht zu lassen. Soweit in den für das *filesharing* relevanten Bereichen noch keine gefestigte, ausdrücklich explizierte höchstgerichtliche Rechtsprechung existiert, wird *de lege lata* die jeweils vorzugswürdige Auslegungsvariante aufgezeigt.

Die Reform- und Auslegungsvorschläge setzten dabei primär an den Säulen des Abmahnwesens an (Auskunft, sekundärer Darlegungslast, lizenzanaloger Schaden), widmen sich aber auch § 19a UrhG, dem TMG in seiner Fassung des 3. TMGÄndG sowie einigen wichtigen Nebenaspekten wie Verjährung, dem erforderlichen Inhalt von Abmahnungen, der Antwortpflicht auf Abmahnungen, der Gebührenbeschränkung und der Darlegung der Gebührenhöhe, Erstattungsansprüchen des Anschlussinhabers und der Begrenzung der Streitwerthöhe.

---

[1] Davon ausgehend, dass BGH und EuGH ihre einmal gefestigte Rechtsprechung nicht mehr ändern werden, mithin der Gesetzgeber aktiv werden muss.

Der Aufbau spiegelt dabei den Aufbau des vierten Kapitels dieser Arbeit, orientiert sich mithin am Prüfungsaufbau, wie er auch in der Praxis oder einer juristischen Prüfung nachzuvollziehen wäre.[2]

II. Modifizierung des Haftungsregimes und der urheberrechtlichen Nutzungshandlungen

1. Neubewertung der Dogmatik der täterschaftlichen Haftung?

Dogmatisch gibt es keine strenge Trennung zwischen der täterschaftlichen Haftung und der Haftung als Störer. Weder § 823 BGB noch die spezielleren deliktischen Tatbestände wie § 97 UrhG setzen eine Rechtsgutsverletzung mittels einer *eigenhändigen* Handlung voraus. § 823 Abs.1 BGB fordert seinem Wortlaut nach nur eine „*Verletzung*“, § 97 Abs.2 UrhG darüber hinaus eine „*Handlung*“, ohne jedoch zu spezifizieren, dass zwischen Verletzung und Handlung ein unmittelbarer Zusammenhang bestehen muss. Auf Grund der Strafrechtsakzessorietät des Zivilrechts im Bereich der Täterschafts- und Teilnahmedogmatik ist im Bereich fahrlässiger Handlungen zudem nicht einmal Tatherrschaft erforderlich, sodass der für Patentrecht zuständige X. Senat des BGH seit der Entscheidung „MP3-Player Import“ Sachverhalte, die der I. Senat im Urheber-und Markenrecht unter die Störerhaftung fassen würde, mit der Täterhaftung greift. Dies lässt er zudem für alle Verschuldens-und Teilnahmeformen gelten, da das Zivilrecht dort hinsichtlich der Rechtsfolgen nicht differenziert (vgl. § 139 Abs.2 Satz 1 PatG, § 830 Abs.2 BGB).[3] Unabhängig davon war für § 823 BGB ohnehin seit jeher anerkannt, dass eine Haftung auch bei der Verletzung von Verkehrssicherungspflichten, deren Verletzung erst mittelbar zur Rechtsgutsverletzung führt, besteht.[4] Wegen des dargestellten, offenen Wortlauts der Norm bestehen hiergegen auch keine grundsätzlichen Einwände. Gleiches gilt für § 97 UrhG. Letztlich lässt sich die Aufweichung der Differenzierung zwischen Täter- und Störerhaftung im Immaterialgüterrecht als Übertragung der Dogmatik der Verkehrssiche-

---

2 Vgl. Kapitel § 4 I.

3 BGH, Urteil vom 17. September 2009, Az. Xa ZR 2/08, Rz. 30ff. – GRUR 2009, 1142 - „MP3-Player-Import“.

4 *Wagner* in: Säcker et al., MüKo-BGB, 8. Aufl. 2021, § 823 BGB, Rz. 441ff.

rungspflichten einkleiden.[5] Eine Trennlinie zwischen den Prüfpflichten im Rahmen der Störerhaftung einerseits und den Verkehrssicherungspflichten andererseits lässt sich nicht ziehen.[6]

Im Ergebnis würde der Wortlaut des § 97 UrhG also eine Ausdehnung der täterschaftlichen Haftung auf Fälle erlauben[7], die vormals unter die Störerhaftung zu fassen waren, mithin auch den Inhaber eines Internetanschlusses betreffend, sofern eine europarechtskonforme, insbesondere richtlinienkonforme, Auslegung dies gebieten würde.[8]

Tatsächlich hat der EuGH mit den Entscheidungen „GS Media“[9], „Filmspeler“[10] und „The Pirate Bay“[11] begonnen, ein eigenes System der Primärhaftung aufzubauen, in dem zahlreiche Vorfeldhandlungen, die vor einer eigentlichen öffentlichen Wiedergabe im Sinne von Art. 3 InfoSocRL stattfinden, bereits selbst eine öffentliche Wiedergabe darstellen können.[12] Für das deutsche Recht folgt daraus, dass solche Vorfeldhandlungen bereits als täterschaftlich zu qualifizieren sind.[13] Was folgt hieraus nun für Anschlussinhaber? Nach den ersten Vorschlägen zur Systematisierung der Rechtsprechung des EuGH ist jedenfalls erkennbar, dass eine öffentliche Wiedergabe durch Vorfeldhandlungen eines Intermediäres dessen Kenntnis von der nachgelagerten Verletzungshandlung sowie eine aktive Rolle, beispielsweise dergestalt, dass die nachgelagerten Verletzungshandlungen durch Strukturierung

5 *Achilles*, Die Verantwortlichkeit von Onlinediensteanbietern für das rechtsverletzende Verhalten Dritter unter Anwendung der Verkehrspflichtendogmatik, S. 44ff.

6 *Wielsch*, ZGE 2018, 1, 21; *Wagner*, GRUR 2020, 329, 334.

7 So im Ergebnis auch *Nordemann*, GRUR Int. 2018, 526, 533, mit weiteren Nachweisen.

8 Diese Grundlegung ist wichtig, da auch der EuGH nämlich keine grenzenlose richtlinienkonforme Auslegung, insbesondere keine richtlinienkonforme Auslegung *contra legem*, erlaubt, siehe *Pötters*, JZ 2011, 387, 392.

9 EuGH, Urteil vom 8. September 2016, Rs. C-160/15 – ECLI:EU:C:2016:644 - „GS Media“.

10 EuGH, Urteil vom 26. April 2017, Rs. C-527/15 – ECLI:EU:C:2017:300 - „Filmspeler“.

11 EuGH, Urteil vom 14. Juni 2017, Rs. C-610/15 – ECLI:EU:C:2017:456 - „The Pirate Bay“.

12 *Leistner*, GRUR 2017, 755, 759.

13 *Ohly*, ZUM 2017, 793, 801.

und Präsentation des Angebots[14] erleichtert werden, erfordert.[15] Eine solche Rolle ist bei Anschlussinhabern ausgeschlossen, da sie nicht mehr tun (können) als einen Internetanschluss, mithin ein neutrales Medium, zur Verfügung zu stellen. Zudem: der EuGH scheint die ECommerceRL nur auf Dienste anzuwenden, die im Sinne des Erwägungsgrundes 42 ECommerceRL rein technischer, automatischer und passiver Art sind. Eine Anwendung der Richtlinie auf Intermediäre, denen er bereits eine öffentliche Wiedergabe nach Art. 3 InfoSocRL durch Vorfeldhandlungen zuschreibt, scheint er hingegen abzulehnen.[16] Da das Zurverfügungstellen eines Internetanschlusses nach der Entscheidung „McFadden" laut EuGH bereits unter den Anwendungsbereich der ECommerceRL fällt[17], scheidet die Annahme einer täterschaftlichen Haftung eines Anschlussinhabers für Rechtsverletzungen durch Dritte, die diese über seinen Anschluss begehen, in europarechtlicher Perspektive im Anwendungsbereich der ECommerceRL also aus.

Rein bundesrechtlich betrachtet kommt eine solche Annahme ohnehin schon unter Geltung des § 7 Abs.4 TMG n.F. nicht in Betracht; dieser muss als *lex specialis* zu einer etwaigen Täterschaft auf Basis einer Verkehrs(sicherungs)pflichtverletzung gesehen werden.

Im Ergebnis muss also die täterschaftliche Haftung des Anschlussinhabers nicht neu bewertet werden[18], was bizarr anmuten mag, da Vorfeldhandlungen wie das Betreiben einer BitTorrent-Indexseite nunmehr eine öffentliche Zugänglichmachung darstellen, die eigentliche Verbreitung eines Werkes in einem BitTorrent-Schwarm nach hiesiger Wertung jedoch nicht[19].

---

[14] Bei „Filmspeler" die Vorkonfiguration der Medienabspielgeräte, bei „The Pirate Bay" die Verwaltung der Indexseite zum Beispiel durch das Entfernen „toter Links" oder die Einteilung des Angebots in Kategorien.

[15] *Ohly*, GRUR Int. 2018, 517, 522; *Nordemann*, GRUR Int. 2018, 526, 528f. Dieses Verständnis stützen auch die gegenwärtig einschlägigen Vorlagen des BGH, siehe BGH, Beschluss vom 13. September 2018, Az. I ZR 140/15 – GRUR 2018, 1132 - „YouTube" sowie BGH, Beschluss vom 20. September 2018, Az. I ZR 53/17 – GRUR 2018, 1239 - „uploaded".

[16] *Leistner*, GRUR 2017, 755, 759f.; *Ohly*, GRUR Int. 2018, 517, 523.

[17] Siehe Kapitel § 2 IX.

[18] Die Überlegungen zur sekundären Darlegungslast sind – da es sich um ein prozessuales Institut handelt – hiervon unabhängig zu betrachten, siehe Kapitel § 4 VII. 1. aA wohl *Paschold*, GRUR Int. 2018, 621, 635f.

[19] Was aber eben den technischen Gegebenheiten einerseits und der Ausdehnung des Rechts der öffentlichen Wiedergabe durch den EuGH andererseits geschuldet ist.

2. Novellierung der Nutzungshandlungen

In Kapitel § 4 II. 4. wurde aufgezeigt, dass die Ansicht des BGH, BitTorrent-Nutzer würden eine öffentliche Zugänglichmachung in Mittäterschaft begehen, nicht nur dogmatisch verfehlt ist, sondern auch in der Praxis bezüglich der Behandlung des Schadensersatzanspruches erhebliche Probleme aufwerfen dürfte.

Zugestanden werden muss jedoch, dass auch die Lösung des Verfassers – Annahme einer Vervielfältigungshandlung in Mittäterschaft bezüglich des gesamten Werkes, Annahme einer öffentliche Zugänglichmachung einzelner Fragmente der Datei, in der ein Werk verkörpert ist, soweit die Fragmente der Wahrnehmung zugänglich sind sowie Annahme einer öffentlichen Zugänglichmachung des gesamten Werkes durch den *initial seeder* – zwar nach hiesiger Auffassung dogmatisch schlüssiger erscheinen mag[20], jedoch hinsichtlich der Behandlung des Schadensersatzanspruches *in praxi* nicht viel weniger Probleme auftreten dürften: Die Mittäter der Vervielfältigung kann der Ermittler nicht feststellen, genausowenig wie die Anzahl der über einen Anschluss öffentlich zugänglich gemachter Dateifragmente; weiterhin kann nur für einen kurzen Zeitraum nach Ingangsetzung eines Schwarms festgestellt werden, wer der *initial seeder* ist.[21] Hinsichtlich der Menge an Dateifragmenten wird man auf Basis einiger Annahmen eine Schätzung abgeben können[22], jedoch verbleibt hier ein Spielraum, der in Anbetracht des begrenzten Vermögens von privaten Anschlussinhabern nicht hinnehmbar ist. Hinsichtlich der mittäterschaftlichen Vervielfältigung bestehen dieselben Regress- und Anrechnungsprobleme wie bei der Lösung des BGH.

Es ist mithin zu konstatieren, dass *de lege lata* hier kein befriedigendes Ergebnis erzielt werden kann. Folglich wäre zu überlegen, eine eigene Nutzungshandlung nur für die Teilnahme an einem *filesharing*-System mit mehrseitiger Dateiübertragung zu schaffen, die den eigentlichen technischen Beitrag

[20] Wobei noch das – in dieser Arbeit offen gelassene – Problem verbleibt, ob die öffentliche Zugänglichmachung eines Dateifragments noch als eigenständige Nutzungshandlung zu betrachten ist, wenn dieses Dateifragment nachfolgend mit anderen Dateifragmenten zu einer mittäterschaftlichen Vervielfältigung führt.

[21] Der *initial seeder* eines Schwarms kann ermittelt werden, solange im Schwarm im Übrigen nur *leecher* vorhanden sind, siehe *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 313, 317.

[22] Siehe hierzu Kapitel § 5 VII.

jedes Nutzers, nämlich die Hilfe bei der Aufrechterhaltung der Verfügbarkeit der Datei, erfasst. Problematisch dürfte dabei sein, dass nach der Rechtsprechung des EuGH das Recht der öffentlichen Wiedergabe nach Art. 3 InfoSocRL vollharmonisierend und dies für das Vervielfältigungsrecht zumindest sehr umstritten ist.[23] Da die Teilnahme an einem *filesharing*-System mit mehrseitiger Dateiübertragung bisher durch diese beiden Nutzungshandlungen zu fassen ist, wäre mithin eine Lösung auf europäischer Ebene notwendig, was im Rahmen dieser Arbeit aber nicht vertieft ausgeführt werden kann. Eine solche Reform sollte jedenfalls dann auch den Bereich, in dem sich der Schadensersatz für die unerlaubte Begehung einer solchen Nutzungshandlung bewegen kann, sinnvoll eingrenzen.[24] Dass eine solche Reform zum gegenwärtigen Zeitpunkt unrealistisch erscheint, steht auf einem anderen Blatt.

3. Sorgfältigere Berücksichtigung des Verschuldenserfordernisses

Die Frage des Verschuldens gemäß § 97 Abs.2 Satz 1 UrhG, das bisher praktisch keine Beachtung findet, sollte in Zukunft genauer geprüft werden. Insbesondere wäre in dogmatischer Hinsicht festzuhalten, dass über die sekundäre Darlegungslast nicht nur eine täterschaftliche Handlung des Anschlussinhabers fingiert wird, sondern zugleich dessen Verschulden; insbesondere kann ein Anschlussinhaber, der die Begehung der Urheberrechtsverletzung abstreitet, nicht zu seinem (angeblichen) Verschulden Stellung nehmen. Hiergegen ließe sich zwar einwenden, dass es sich hierbei um eine zwangsläufige Folge der sekundären Darlegungslast handle. Jedoch ist nicht erkennbar, warum die prozessuale Fiktion einer täterschaftlichen Handlung automatisch die Prüfung weiterer Tatbestandsmerkmale des § 97 UrhG, mithin des Verschuldens, ersetzen sollte.

In klassischen *filesharing*-Fällen dürfte diese Prüfung noch unproblematisch sein, da solche Fälle mittlerweile eine solche Bekanntheit erlangt haben dürften, dass einem (fingierten) Täter zwar kein (bedingter) Vorsatz unterstellt werden dürfte[25], wenn er unerlaubtes *filesharing* betreibt, jedoch grundsätz-

[23] Siehe *Roder*, Die Methodik des EuGH im Urheberrecht: Die autonome Auslegung des Gerichtshofs der Europäischen Union im Spannungsverhältnis zum nationalen Recht, S. 295ff., jeweils mit zahlreichen Nachweisen.

[24] Siehe hierzu Kapitel § 5 VII.

[25] Siehe Kapitel § 4 II. 4.

lich Fahrlässigkeit. Schwieriger wird es, wenn streitgegenständlich eine Kombination aus *filesharing* und Streaming wie Popcorn Time ist[26], da einem durchschnittlichen Internetnutzer wohl nicht unterstellt werden kann, dass er dessen Funktionsweise realisiert hat oder realisieren konnte. Würde man hier die Haftung des Anschlussinhabers, dessen Täterschaft über die sekundäre Darlegungslast fingiert worden ist, ohne eine Prüfung des Verschuldens vorzunehmen, bejahen, so würde man dem Anschlussinhaber implizit möglicherweise eine Gefährdungshaftung auferlegen; jedoch steht die Etablierung einer Gefährdungshaftung grundsätzlich unter Gesetzesvorbehalt.[27] In solchen Fällen dürfte ein Richter das Verschulden also nicht auf die Annahme der allgemeinen Bekanntheit der Funktionsweise von *filesharing* stützen, sondern müsste das Verschulden individuell prüfen. Dies sollte dadurch geschehen, dass er sich von den Internetkenntnissen des Anschlussinhabers ein Bild macht. Nur wenn es dann zur Überzeugung des Richters steht, dass der Anschlussinhaber dahingehend fortgeschrittene Kenntnisse aufweist, dass damit zu rechnen ist, dass ihm die Funktionsweise von *filesharing*-basiertem Streaming bekannt sein könnte, dürfte ihm Fahrlässigkeit unterstellt werden.

III. Anforderungen an den Beweis einer Verletzungshandlung

Nach hiesigem Verständnis hat der BGH in „Tauschbörse I“ zahlreiche Fragen zur Beweiswürdigung der *filesharing*-Ermittlung offen gelassen, weshalb für die zukünftige Rechtsentwicklung in diesem Bereich noch Spielraum besteht.[28] Dieser lässt sich in drei Problemkreise einteilen:

- Erstens, wie beweisrechtlich mit dem Problem umzugehen ist, dass ein gewisser Prozentsatz aller Ermittlungen auch bei Beachtung größtmöglicher Sorgfalt aus ungeklärten Gründen fehlerhaft ist[29], d.h. die entsprechenden Abmahnungen unberechtigt sind, ohne dass ein mit (auf diesen aufbauenden) Verletzungsfällen befasster Richter wissen kann, welche genau.

[26] Siehe hierzu Kapitel § 3 XI. 2. a).
[27] Siehe zuletzt BGH, Urteil vom 19. September 2006, Az. XI ZR 204/04, Rz. 42 – BeckRS 2006, 13865.
[28] Siehe Kapitel § 4 III.
[29] Siehe Kapitel § 1 IV. 7. c) ee).

- Zweitens, wie beweisrechtlich mit der Möglichkeit des Wechsels bzw. der Neuvergabe einer IP-Adresse[30] umzugehen ist.
- Drittens, welcher Vortrag über den Umfang der Verletzungshandlung zu verlangen ist.

1. Umgang mit Fehlerquoten

Nach einer vom BGH mittlerweile in ständiger Rechtsprechung verwendeten Formel, darf ein Tatrichter eine Tatsache als bewiesen ansehen, wenn er in einem für das „ *[...] praktische Leben brauchbaren Grad Gewissheit von dieser Tatsache hat, der den Zweifeln Schweigen gebietet, ohne sie völlig auszuschließen [...]*“.[31] Sofern man diese Aussage quantifizieren wollte, wird mithin eine Wahrscheinlichkeit von über 50 Prozent zu fordern sein. Geht man von einer Fehlerquote von einem Prozent aus[32], so würde ein hypothetischer Richter, der über *filesharing*-Fälle zu entscheiden hätte, beim ersten zu entscheidenden Fall – vorausgesetzt die Ermittlung hat allen Sorgfaltsanforderungen entsprochen – eine Wahrscheinlichkeit für die Richtigkeit der Ermittlung in Höhe von 99 Prozent annehmen können. Beim zweiten Fall würde die Wahrscheinlichkeit nach den Regeln der Stochastik jedoch auf 98 Prozent sinken. Ab dem fünfzigsten Fall würde die Wahrscheinlichkeit dann nur noch 50 Prozent betragen, sodass hier die Richtigkeit der Ermittlung nicht mehr als erwiesen angesehen werden dürfte.

Jedoch lassen sich die Regeln der Stochastik hier nicht auf den Zivilprozess übertragen. Zunächst ist ein Richter berufen, einen Einzelfall zu entscheiden, muss also das Beweismaß auch am Einzelfall orientieren. Ein Richter könnte zwar seine Entscheidungen aus anderen Fällen und das dort ermittelte Maß an Wahrscheinlichkeit über § 291 ZPO als offenkundige bzw. gerichtskundige Tatsache in seine Entscheidungen inkorporieren; jedoch müsste er dann jeden 50. Fall abweisen, weil bei jedem 50. Fall nach den Regeln der Stochastik (die Fehlerquote von einem Prozent vorausgesetzt) keine überwiegende Wahrscheinlichkeit mehr für die Richtigkeit der Ermittlung bestünde. Sowohl für den jeweils betroffenen Rechteinhaber als auch für den jeweils betroffenen

[30] Siehe Kapitel § 1 IV. 7. c) bb).

[31] Siehe nur BGH, Urteil vom 6. Mai 2015, Az. VIII ZR 161/14, Rz. 11 – NJW 2015, 2111, mit weiteren Nachweisen der Rechtsprechung des BGH.

[32] Siehe Kapitel § 1 IV. 7. c) ee).

Anschlussinhaber wäre eine solche Vorgehensweise höchst willkürlich. Folglich verbleibt nur, die Fehlerquote und damit eine möglicherweise fehlerhafte Verurteilung einzelner Anschlussinhaber zu akzeptieren.

Umso mehr muss daher rechtlich gesichert sein, dass nur solche Ermittlungen als Beweismittel akzeptiert werden, die höchsten Sorgfaltsansprüchen genügen.[33]

2. Umgang mit dem möglichen Wechsel bzw. der möglichen Neuvergabe einer IP-Adresse

Auf Grund der soeben erörterten Fehlerquoten-Problematik sollte jedenfalls an anderen Stellen die absolute „Wasserfestigkeit" der Ermittlung gefordert werden. Relevant ist insbesondere das Problem des möglichen Wechsels bzw. der möglichen Neuvergabe einer IP-Adresse.[34] Aus der Instanzrechtsprechung sind einige Fälle bekannt, in denen die Gerichte einen Nachweis der Verletzungshandlungen, bzw. genauer: einen Nachweis darüber, dass eine Verletzungshandlung über den Anschluss des beklagten Anschlussinhabers stattgefunden hat, mit der Begründung verneinten, dass der Rechteinhaber keine *Mehrfachermittlung* vorweisen kann.[35]

Eine Mehrfachermittlung ist dann gegeben, wenn der Anschluss eines Beklagten zu unterschiedlichen Zeitpunkten mit unterschiedlichen dynamischen IP-Adressen im Hinblick auf dasselbe Werk ermittelt und beauskunftet wurde.[36] Soweit ersichtlich, halten alle Gerichte, die sich mit dem Thema Mehrfachermittlung (überhaupt) auseinandersetzen, diese jedenfalls auch für erforderlich. Strittig ist insofern lediglich, ob zwischen den unterschiedlichen Zeitpunkten mehr als 24 Stunden liegen müssen.[37] Der Zeitraum von 24 Stunden liegt darin begründet, dass bei den meisten ISPs spätestens nach 24 Stunden eine Zwangstrennung des Anschlusses und eine Neueinwahl stattfindet, so-

[33] Insbesondere sollte vorausgesetzt werden, dass eine eingesetzte Ermittlungssoftware regelmäßige Updates erfährt und jeder neuen Version einer solchen Software die einwandfreie Funktionstauglichkeit gutachterlich bestätigt wurde.

[34] Siehe Kapitel § 1 IV. 7. c) bb).

[35] Mit zahlreichen Nachweisen der Rechtsprechung siehe LG Frankfurt a.M., Urteil vom 10. Juli 2018, Az. 2-03 S 13/16 – aw3p.de.

[36] LG Frankfurt a.M., Urteil vom 10. Juli 2018, Az. 2-03 S 13/16 – aw3p.de.

[37] Bejahend – und mit weiteren Nachweisen – LG Frankfurt a.M., Urteil vom 10. Juli 2018, Az. 2-03 S 13/16 – aw3p.de; verneinend LG Köln, Urteil vom 14. Dezember 2017, Az. 14 S 1/17, Rz. 29 – juris.

dass dem Anschlussinhaber innerhalb eines solchen Zeitraums zwangsweise zwei verschiedene dynamische IP-Adressen zugewiesen werden.[38]

Grundsätzlich ist der Tatrichter in seiner Beweiswürdigung gemäß § 286 ZPO weitestgehend frei, sodass es kein rechtlich zwingendes Argument gibt, eine Mehrfachermittlung im Allgemeinen und einen Zeitraum von mindestens 24 Stunden im Besonderen für zwingend erforderlich zu erachten. Um jedoch die Fehlerquelle „Wechsel oder Neuvergabe der IP-Adresse“[39] auszuschließen, sowie die Fehlerquelle der „unrichtigen Ermittlung aus ungeklärten Gründen“[40] wenigstens einzudämmen[41] sollte der BGH – was revisionsrechtlich möglich ist[42] – im Rahmen von § 286 ZPO eine Mehrfachermittlung mit einem Mindestzeitraum von 24 Stunden zwischen den Ermittlungen fordern.[43] In „Tauschbörse I“ konnte der BGH den Einwand der möglichen Neuvergabe der IP-Adresse noch als unbeachtlich zurückweisen, da es sich hierbei um einen Tatsacheneinwand handelt und ein solcher im Revisionsverfahren nicht mehr zulässig ist.[44]

3. Zum Beweis des Umfangs einer Verletzungshandlung

Naheliegend ist die Überlegung, dass es im Rahmen der Schätzung des Schadensersatzanspruches nach § 287 ZPO eine Rolle spielen muss, welche Datenmengen der Nutzer eines *filesharing*-Systems, insbesondere BitTorrent, hochgeladen hat. Jedoch ist rechtlich hierfür im Rahmen der gegenwärtigen mittäterschaftlichen Lösung des BGH kein Raum[45], da es wegen der wechselseitigen Zurechnung der Tatbeiträge der einzelnen Nutzer untereinander auf den Umfang der Verletzungshandlungen eines isoliert in Anspruch genommenen Mittäters nicht ankommt.

---

38 LG Frankfurt a.M., Urteil vom 10. Juli 2018, Az. 2-03 S 13/16 – aw3p.de.

39 Siehe Kapitel § 1 IV. 7. c) bb).

40 Siehe Kapitel § 1 IV. 7. c) ee) und § 5 III. 1.

41 Diese Fehlerquelle kann nicht vollständig beseitigt werden. Die Mehrfachermittlung kann aber zumindest dazu beitragen, die Fehlerquote zu senken.

42 Siehe Kapitel § 4 VII. 4. b).

43 Im Rahmen des Auskunftsverfahrens muss jedoch die einmalige Ermittlung genügen. Ansonsten könnte ein Rechteinhaber nie zwei Auskünfte über denselben Anschlussinhaber erlangen, also auch nie eine Mehrfachermittlung nachweisen.

44 BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14 , Rz. 36 – GRUR 2016, 176 - „Tauschbörse I“. Der Beklagte hatte entsprechendes Vorbringen in den Tatsacheninstanzen versäumt.

45 Siehe hierzu Kapitel § 4 II. 4.

Die mittäterschaftliche Lösung hinweggedacht, stünden einer Einbeziehung des Umfangs der Verletzungshandlung im Rahmen von § 287 ZPO zwar keine rechtlichen Gründe entgegen, jedoch ist dessen Ermittlung im BitTorrent-System praktisch nicht möglich.[46] Ermittlungsdienste können auf Grund der Funktionsweise des BitTorrent-Systems in der Regel nur eine Verbindung von wenigen Sekunden bis Minuten zu einzelnen Nutzern aufzubauen. Auch die Mehrfachermittlung bietet demgegenüber einen kaum gesteigerten Erkenntniswert, denn sie beweist lediglich, dass der entsprechende Nutzer zu zwei Zeitpunkten für wenige Sekunden oder Minuten BitTorrent benutzt hat, nicht aber, dass er auch über den gesamten Zeitraum zwischen den zwei Zeitpunkten hinweg BitTorrent benutzt hat.

Auch im Rahmen der mittäterschaftlichen Lösung ist jedoch eine gesonderte Anforderung an das Beweismaß möglich, nämlich die Erforderlichkeit des Nachweises, dass die Datei, auf die sich ein BitTorrent-Schwarm bezieht, innerhalb des Schwarms vollständig vorhanden ist. Wie in Kapitel § 4 II. 3. und § 1 III. dargestellt, sind Dateien bestimmter Dateitypen lediglich Datenmüll, wenn sie nicht zu 100 Prozent vollständig sind; nach hier vertretener Auffassung kann bezüglich solcher Dateien keine Urheberrechtsverletzung vorliegen.[47] Der BGH hat sich zu dieser Auffassung noch nicht geäußert, eine Rechtsentwicklung *de lege lata* ist hier also noch möglich.[48] Das Fehlen einer vollständigen Datei innerhalb eines Schwarms ist nicht unüblich und wird als *missing piece syndrome* bezeichnet. Insbesondere in schnell und stark anwachsenden Schwärmen kann es vorkommen, dass diejenigen Nutzer, die alle Segmente der Zieldatei haben, den Schwarm verlassen, während hingegen zwischen den übrigen Nutzern untereinander nicht alle Segmente der Zieldatei vorhanden sind und sie mithin keine vollständige Datei mehr erlangen können.[49] Der Schwarm kann dann beliebig weiterwachsen, ohne dass es den Teilnehmern möglich sein wird, noch eine vollständige Datei zu erhalten. Der BGH hatte in „Konferenz der Tiere“ mangels gegenteiliger Feststellungen der Tatsacheninstanz zu Gunsten des Rechteinhabers unterstellt, dass sich in dem dort streitgegenständlichen Schwarm im zeitlichen Zusammenhang mit der Verletzungshandlung des dortigen Beklagten alle Segmente der

[46] Siehe Kapitel § 1 IV. 7. c) dd).
[47] Siehe Kapitel § 4 II. 3.
[48] Siehe Kapitel § 4 II. 4. a).
[49] *Zhu* et al., Distributed Computing, Nr. 6, Bd. 28, 2015, S. 391, 394f.

Zieldatei vorhanden waren.[50] Da es sich hierbei um eine für den klagenden Rechteinhaber günstige Tatsache handelt und er deswegen die Beweislast für die Vollständigkeit der Datei trägt, muss der BGH implizit einen Anscheinsbeweis annehmen, um diese Unterstellung machen zu können. Angesichts des soeben geschilderten *missing piece syndrome*, scheint die Annahme eines solchen Anscheinsbeweises jedoch nicht haltbar.[51] Weil dem BGH allerdings keine eindeutige Aussage in diese Richtung entnommen werden kann, ist abzuwarten, wie er sich hierzu in Zukunft positionieren wird. Die ersten Instanzgerichtsentscheidungen zu dieser Frage nehmen richtigerweise an, dass der klagende Rechteinhaber die volle Darlegungs- und Beweislast trägt.[52] Der entsprechende Vortrag sollte für klagende Rechteinhaber dadurch möglich sein, dass sie entweder ein vollständiges *bitfield*[53] darlegen oder darlegen können, dass sie in einem zeitlich engen Zusammenhang mit der ermittelten Verletzungshandlung über den Schwarm eine vollständige Datei beziehen konnten.

IV. Änderung des Auskunfts- und Sicherungsverfahrens?

1. Normierung eines Sicherungsanspruches?

Wie in Kapitel § 4 V. dargelegt, ist die Herleitung des Sicherungsanspruchs gegen ISPs dogmatisch *de lege lata* fragwürdig und nach hiesiger Auffassung auch europarechtswidrig. Erforderlich wäre stattdessen eine ausdrückliche, gesetzliche Regelung.

Ungeklärt ist die Frage, wie der BGH mit CG-NAT[54] umgehen wird[55]. Die Sicherung der Zuordnung einer IP-Adresse ist sinnlos, wenn diese mehreren Anschlüssen zugeordnet ist und die für eine eindeutige Zuordnung eines

[50] BGH, Urteil vom 6. Dezember 2017, Az. I ZR 186/16, Rz. 26 – GRUR 2018, 400 - „Konferenz der Tiere“.

[51] aA, jedoch ohne Berücksichtigung des *missing piece syndrome*, bei *Heine/Schopp*, GRUR-Prax 2018, 129, 129.

[52] AG Frankenthal, Urteil vom 18. April 2018, Az. 3c C 27/18, Rz. 17 – juris; AG Frankenthal, Urteil vom 25. April 2018, Az. 3c C 251/17, Rz. 20 – juris; AG Frankenthal, Urteil vom 7. November 2018, Az. 3c C 196/18, Rz. 17 – juris.

[53] Siehe hierzu Kapitel § 1 IV. 7. c) dd).

[54] Siehe dazu Kapitel § 1 IV. 5. d).

[55] Siehe dazu auch Kapitel § 2 III. 1. f).

Anschlusses erforderlichen Metadaten nicht gleichfalls gespeichert werden. Gegenwärtig besteht eine Speicherpflicht dieser Metadaten nicht einmal im Rahmen der Vorratsdatenspeicherung.[56] Da der Wortlaut von § 96 Abs.1 TKG ebenso wenig wie der Wortlaut von § 113b Abs.3 TKG die im Rahmen des CG-NAT anfallenden Metadaten erfasst, ist auch eine Übertragung der Rechtsprechung des BGH zum Sicherungsanspruch – abgesehen von ihren dogmatischen Mängeln in sonstiger Hinsicht – dogmatisch nicht möglich und stattdessen eine gesetzliche Regelung erforderlich.

Zum Vergleich: Die (ehemalige) Regierung in Österreich hat demgegenüber erwogen, ISPs die Verwendung von CG-NAT zu untersagen.[57] Praktisch wären ISPs durch ein solches Verbot also gezwungen, sofort vollständig auf den IPv6-Standard umzusteigen. In Deutschland dürfte ein solches Verbot verfassungsrechtlich nicht ohne finanzielle Kompensation für den Mehraufwand der sofortigen Implementierung von IPv6 möglich sein, wenn überhaupt.

2. Beteiligung des Anschlussinhabers am Auskunftsverfahren?

Bisher sind Anschlussinhaber in das Gestattungsverfahren nach § 101 Abs.9 UrhG nicht involviert. Es findet lediglich zwischen Rechteinhaber und ISP statt. Der Anschlussinhaber erfährt von dem Gestattungsverfahren erst in der Abmahnung. Folglich stellt sich die Frage, ob Anschlussinhaber an dem Verfahren zu beteiligen sind. Hierfür müssten sie gemäß § 101 Abs.9 Satz 4 UrhG iVm § 7 FamFG als Beteiligte im Sinne von § 7 FamFG anzusehen sein. Dies scheidet aber schon deswegen aus, weil zum Zeitpunkt des Gestattungsverfahrens der Anschlussinhaber noch gar nicht bekannt ist; um den Anschlussinhaber zu beteiligen, müsste die Auskunftserteilung dem Gestattungsverfahren vorgezogen werden, was in § 101 Abs.9 UrhG gerade eben nicht vorgesehen ist. Die Beteiligung des Anschlussinhabers am Gestattungsverfahren kommt daher nicht in Betracht.[58]

---

[56] VG Köln, Beschluss vom 25. Januar 2017, Az. 9 L 1009/16, Rz. 132 – juris.

[57] *Krempl*, Österreich: Neue schwarz-blaue Regierung will Überwachung ausbauen.

[58] *Stein*, Der Auskunftsanspruch gegen Access-Provider nach § 101 UrhG, S. 226f.

3. Beschwerde gegen den Gestattungsbeschluss durch den Anschlussinhaber

Der BGH hatte in dem Beschluss „Heiligtümer des Todes“[59] entschieden, dass Anschlussinhaber immer ein Beschwerderecht gegen den Gestattungsbeschluss gemäß den §§ 58ff. FamFG haben[60], wobei die Beschwerdefristen des § 63 Abs.3 FamFG für Anschlussinhaber nicht gelten[61], weshalb diese zeitlich unbegrenzt zulässig erhoben werden kann. Fraglich ist jedoch, was das Beschwerderecht dem Anschlussinhaber überhaupt nützt. Der Rechtsprechung des BGH zu Folge kann nicht gerügt werden, dass eine Verletzung kein gewerbliches Ausmaß erreicht hat.[62]

Zu denken wäre *de lege lata* aber an andere Rechtsfragen, die bisher in Beschwerden kaum oder gar keine Rolle gespielt haben. Da im Rahmen des Gestattungsverfahren geprüft werden muss, ob der Auskunftsanspruch materiell besteht[63], können alle Tatbestandsmerkmale des § 101 UrhG einer Prüfung unterzogen werden.

a) „offensichtliche Rechtsverletzung“ und Täterschaft des Anschlussinhabers

Nicht in Betracht kommt die Rüge, dass keine „*offensichtliche Rechtsverletzung*“ im Sinne von § 101 Abs.2 Satz 1 UrhG vorgelegen habe, weil das Gericht nicht geprüft habe, ob der Anschlussinhaber auch der Täter ist. Dies könnte nur dann gerügt werden, wenn das Merkmal nicht lediglich das Feststehen einer objektiven Rechtsverletzung ausreichen lassen würde – unabhängig davon, ob der Anschlussinhaber auch der Täter ist. Der Gesetzgeber hatte das Merkmal nicht näher definiert.[64] Soweit die Rechtsprechung hierzu

[59] BGH, Beschluss vom 5. Dezember 2012, Az. I ZB 48/12 – GRUR 2013, 536 - „Heiligtümer des Todes“.

[60] BGH, Beschluss vom 5. Dezember 2012, Az. I ZB 48/12, Rz. 13ff. – GRUR 2013, 536 - „Heiligtümer des Todes“.

[61] BGH, Beschluss vom 5. Dezember 2012, Az. I ZB 48/12, Rz. 17ff. – GRUR 2013, 536 - „Heiligtümer des Todes“.

[62] Auch wenn dies dogmatisch nach Auffassung des Verfassers unzulässig ist, siehe Kapitel § 4 IV. 1. g). Zum einem dies betreffenden Vorschlag *de lege ferenda* siehe sogleich Kapitel § 5 IV. 4.

[63] BGH, Urteil vom 21. September 2017, Az. I ZR 58/16, Rz. 24 – GRUR 2017, 1236 - „Sicherung der Drittauskunft“, mit weiteren Nachweisen.

[64] *Klein*, JurPC Web-Dok. 131/2011, Abs. 23.

Stellung genommen hat, hat sie das Feststehen einer objektiven Rechtsverletzung ausreichen lassen.[65] Dem ist beizupflichten, da andernfalls das Merkmal der offensichtlichen Rechtsverletzung leerlaufen würde, da, bevor ein Prozess gegen den Anschlussinhaber nicht abgeschlossen ist, nie ausgeschlossen werden kann, dass nicht auch eine andere Person als der Anschlussinhaber Täter sein könnte.[66] Zudem sind Ansprüche gegen den Anschlussinhaber denkbar, auch wenn dieser nicht Täter ist (früher die Störerhaftung, nunmehr § 7 Abs.4 TMG).

b) Datenschutzrechtliche Probleme

aa) Zulässigkeit der Ermittlung

Das OLG Köln hat unter Berufung auf die Gesetzesbegründung zur Umsetzung der EnforcementRL richtigerweise entschieden, dass das Tatbestandsmerkmal „*offensichtlich*“ in § 101 Abs.2 Satz 1 UrhG gewährleisten soll, dass ein Auskunftsanspruch nur dann zuerkannt wird, wenn eine ungerechtfertigte Belastung des Auskunftsschuldners ausgeschlossen erscheint. Folglich ist im Rahmen dieses Merkmals auch die Zuordnung der Rechtsverletzung zu den verfahrensgegenständlichen Verkehrsdaten zu prüfen.[67] Damit erweist sich dieses Tatbestandsmerkmal als Einfallstor für die Prüfung des Ermittlungsvorganges und insbesondere von dessen datenschutzrechtlichen, bisher von der Rechtsprechung übersehenen, Implikationen.

Bereits seit längerem wurde in der Literatur immer wieder in Frage gestellt, ob die Ermittlung und Speicherung von IP-Adressen, wie sie auch Ermittlungsdienste in *filesharing*-Systemen vornehmen[68], datenschutzrechtlich überhaupt zulässig ist.[69]

---

65 Siehe mit einer Übersicht *Scheder-Bieschin*, Modernes Filesharing: Störerhaftung und Auskunftspflicht von Anonymisierungsdiensten, S. 310.

66 *Klein*, JurPC Web-Dok. 131/2011, Abs. 26.

67 OLG Köln, Beschluss vom 21. Oktober 2008, Az. 6 Wx 2/08, Rz. 40 – NRWE.

68 Siehe hierzu Kapitel § 1 IV. 4.

69 *Kitz*, ZUM 2006, 444, 448; *Maaßen*, MMR 2009, 511, 512f.; *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 293ff.; *Nietsch*, Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, S. 156ff.; *Lutz*, DuD 2012, 584, 588. Im internationalen Vergleich wäre die Unzulässigkeit der Ermittlung auch kein Unikum, siehe Kapitel § 3 XII. 2. a) aa).

Diese Rechtsfrage war früher nach dem BDSG zu beurteilen gewesen[70]; die E-DatenschutzRL und das TKG[71] spielten von vornherein keine Rolle, da die E-DatenschutzRL gemäß Art. 3 Abs.1 nur für die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste relevant ist, was die Ermittlungstätigkeit in einem *filesharing*-System nicht ist.

Nach gegenwärtiger Rechtslage ist die Ermittlung an Hand der DS-GVO zu bewerten.[72] Um in deren Anwendungsbereich zu fallen, müssten die dynamischen IP-Adressen, die der Ermittlungsdienst in *filesharing*-Systemen erfasst, personenbezogene Daten im Sinne des Art. 2 Abs.1, 4 Nr.1 DS-GVO sein. Der EuGH hatte bereits 2011 in der Entscheidung „Scarlet/SABAM“ *obiter dictum* apodiktisch festgehalten, dass dies – bezüglich der DatenschutzRL der Fall sei – der Fall sei.[73] 2016 bestätigte er dies – nunmehr entscheidungsrelevant – in der Entscheidung „Breyer“. Die Entscheidung enthält zwar die Einschränkung dahingehend, dass der Ermittler rechtliche Mittel haben müsse, um die hinter der IP-Adresse stehende Person, also den Anschlussinhaber, ermitteln zu können[74]; dies ist jedoch auf Grund des urheberrechtlichen Auskunftsanspruch gegen den ISP ohne weiteres der Fall. Da die DS-GVO bezüglich der Definition der personenbezogenen Daten nur unwesentlich von der in Art. 2 lit.a) DatenschutzRL abweicht, ist davon auszugehen, dass der EuGH diese Rechtsprechung auch auf die DS-GVO anwenden würde.

Weil andere Tatbestände nicht einschlägig sind, ist die Zulässigkeit der Ermittlung und Speicherung der IP-Adresse nach der Generalklausel des Art. 6

---

70 Die alte Rechtslage dürfte allerdings auch noch für Altfälle, d.h. Fälle, in denen vor Inkrafttreten der DS-GVO ermittelt abgemahnt worden war, relevant sein

71 Diese sind für die Sicherung der Zuordnung einer IP-Adresse zu einem Anschluss relevant, siehe Kapitel § 4 V. 2. b).

72 Zum Verhältnis des mittlerweile analog zu § 101 UrhG geschaffenen Auskunftsrechts bei Persönlichkeitsrechtsverletzungen in § 14 Abs.3 bis 5 TMG zum BDSG und der DS-GVO siehe BGH, Beschluss vom 24. September 2019, Az. VI ZB 39/18, Rz. 34ff. – juris. Die dortigen Ausführungen dürften sich auf § 101 UrhG übertragen lassen, sodass die DS-GVO bzw. das BDSG der Anwendung des § 101 UrhG nicht vorgeht. § 101 UrhG betrifft aber nur die Beauskunftung von Bestandsdaten durch den ISP an den Rechteinhaber. Auf die Bewertung der Ermittlungstätigkeit des Rechteinhabers hat die BGH-Entscheidung also keinen Einfluss.

73 EuGH, Urteil vom 24. Oktober 2011, Rs. C-70/10, Rz. 51 – ECLI:EU:C:2011:771 - „Scarlet/SABAM“.

74 EuGH, Urteil vom 19. Oktober 2016, Rs. C-582/14, Rz. 49 – ECLI:EU:C:2016:779 - „Breyer“.

Abs.1 Satz 1 lit. f) DS-GVO zu bewerten, also danach, ob in Abwägung der Grundrechte des Ermittlers (bzw. dessen Auftraggebers) mit denen der von der Ermittlung betroffenen Person die Ermittlung von einem berechtigten Interesse getragen ist. Aus den Aussagen des EuGH in der Entscheidung „Breyer“ zur entsprechenden Generalklausel in der DatenschutzRL lassen sich für die Beurteilung keine Ableitungen treffen, da dort streitgegenständlich die Frage war, inwiefern Webseitenbetreiber die IP-Adressen ihrer Besucher loggen dürfen, und Webseitenbetreiber im Wesentlichen nur Interessen technischer Art (Funktionsfähigkeit der Webseite etc.) geltend machen können.[75] In der Sache „Promusicae“ konnte der EuGH es noch den Mitgliedstaaten überlassen, bei der Beantwortung der Frage, inwiefern Rechteinhaber von ISPs Auskunft über deren *filesharing* betreibenden Kunden verlangen können, einen gerechten Ausgleich zwischen dem Recht auf geistiges Eigentum und dem Recht auf Datenschutz zu finden[76]; der bundesdeutsche Gesetzgeber glaubte einen solchen Ausgleich darin gefunden zu haben, dass die Auskunftserteilung mit einem Richtervorbehalt versehen ist.[77] Hinsichtlich der der Auskunft vorgeschalteten Ermittlung wird der EuGH wegen der unmittelbaren Anwendbarkeit der DS-GVO in Zukunft selbst eine Lösung finden müssen. Dies wird dadurch erheblich erschwert, dass es dort einen Ausgleich – beispielsweise durch Verfahrensgarantien – aus praktisch-technischen Gründen nicht geben kann: entweder der Ermittler darf IP-Adressen ermitteln und speichern, dann ist zwar das Recht auf geistiges Eigentum gewahrt, aber das Recht auf Datenschutz muss vollständig zurückstehen – oder der Ermittler darf dies nicht, dann verhält es sich umgekehrt; zwischen beiden Rechten muss also eine binäre Entscheidung getroffen werden, wobei die Ermittlung dem Wortlaut des Art. 6 Abs.1 Satz 1 lit. f) DS-GVO zu Folge nur dann zulässig wäre, wenn die Interessen des Rechteinhabers die des betroffenen Anschlussinhabers überwiegen.

Für die Entscheidung dieser Frage sind drei Gesichtspunkte maßgeblich:

- Zum alten Datenschutzrecht war umstritten, ob eine heimliche Ermitt-

[75] EuGH, Urteil vom 19. Oktober 2016, Rs. C-582/14, Rz. 64 – ECLI:EU:C:2016:779 - „Breyer“.

[76] EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 68 – ECLI:EU:C:2008:54 - „Promusicae“.

[77] BT-Drs. 16/8783, S. 48.

lung zulässig ist.[78] Die DS-GVO greift diesen Gedanken nun ausdrücklich auf und sieht es in Erwägungsgrund 47 Satz 3 und 4 für die Interessenabwägung als relevant an, ob die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten rechnen muss.[79] Rein faktisch wird der Nutzer eines *filesharing*-Systems sicher mit einer Ermittlung rechnen müssen, da die Überwachung dieser Systeme mittlerweile in sehr weitem Umfang stattfindet.[80] Dass hier die Faktizität scheinbar eine normative Geltung schaffen kann, erscheint problematisch, da dann der bloße Umstand, dass ermittelt wird, die Ermittlung rechtfertigen kann. Zudem weiß die von der Ermittlung letztlich betroffene Person – der Anschlussinhaber – von der Ermittlung nichts, wenn er nicht auch das *filesharing* betreibt, kann also mit dieser auch nicht rechnen. Stellt sich also in einem Verletzungsverfahren heraus, dass die Täterschaft des Anschlussinhabers nicht nachgewiesen werden kann, wäre – diese Überlegung zu Grunde gelegt – die Ermittlung datenschutzwidrig und damit nicht verwertbar, sodass auch die Haftung nach § 7 Abs.4 TMG ausscheiden würde.

- Daran anknüpfend ist zudem die Überlegung, dass die Verletzung des geistigen Eigentums nur dann relevant ist, wenn gegen die in Anspruch genommene Person überhaupt ein Anspruch besteht und dies schon bei Ermittlung vorhersehbar ist.[81] Das ist jedoch nicht der Fall, da insbesondere bei Ermittlung noch nicht absehbar ist, ob zumindest der Subsidiaritätsvorbehalt des § 7 Abs.4 TMG greifen wird und der entsprechende Anschlussinhaber also gar nicht (schon nicht als Täter und auch nicht nach § 7 Abs.4 TMG) in Anspruch genommen werden kann.[82]

- Zuletzt muss die Interessenabwägung für jeden Einzelfall erfolgen.[83] Da die Ermittlung regelmäßig aber automatisiert erfolgt, ist eine Ein-

78 BT-Drs. 16/5048, S. 57.

79 Die beiden Sätze lassen sich als allgemeines Kriterium der „Absehbarkeit der Verarbeitung“ fassen, vgl. *Albers/Veit* in: Brink/Wolff, BeckOK DatenschutzR, 35. Ed. 2021, Art. 6 DS-GVO, Rz. 53.

80 Siehe Kapitel § 1 IV. 4.

81 Vgl. zur alten Rechtslage *Lutz*, DuD 2012, 584, 588.

82 Siehe hierzu Kapitel § 4 VIII. 3. d).

83 EuGH, Urteil vom 19. Oktober 2016, Rs. C-582/14, Rz. 62 – ECLI:EU:C:2016:779 - „Breyer“.

zelfallabwägung gar nicht möglich.[84]

Im Ergebnis bestehen also erhebliche Zweifel, ob die Ermittlung von Teilnehmern in einem *filesharing*-System unter Geltung der DS-GVO[85] überhaupt zulässig ist. Folglich bestehen auch hier *de lege lata* Ansatzpunkte für Abgemahnte.

Mittlerweile ist diesbezüglich auch eine Vorlage eines belgischen Gerichts (Ondernemingsrechtbank Antwerpen) beim EuGH anhängig.[86] Leider spricht der Generalanwalt dort jedoch die soeben benannten Probleme – heimliche Ermittlung, Bestehen eines Anspruchs gegen den ermittelten Anspruchsinhaber, Interessenabwägung im Einzelfall – nicht an und geht lediglich davon aus, dass die Ermittlung durch bzw. im Auftrag von Urheberrechtstrollen datenschutzrechtlich unzulässig sein kann.[87] Es steht daher zu erwarten, dass auch der EuGH die Ermittlung im Übrigen – trotz der benannten Probleme – datenschutzrechtlich für zulässig erachten wird.

bb) Mitteilung der Ermittlung

Die Ermittlung und Speicherung der IP-Adresse fällt überdies in den Anwendungsbereich des Art. 14 DS-GVO, da sie ohne Beteiligung des betroffenen Anschlussinhabers bzw. *filesharing*-Nutzers stattfindet.[88] Art. 14 Abs.1 DS-GVO verpflichtet den Ermittler, dem Ermittelten verschiedene Informationen über die Ermittlung und seine diese betreffenden Rechte mitzuteilen. Da Art. 14 Abs.3 DS-GVO für die Mitteilung einen zeitlich recht flexiblen Rahmen gewährt, ist davon auszugehen, dass die Mitteilung erst in einer Ab-

---

84 So zur alten Rechtslage *Lutz*, DuD 2012, 584, 588.

85 Die DS-GVO dürfte auch auf die Nutzung von IP-Adressen als Beweismittel im Zivilprozess anwendbar sein, wenn diese vor Inkrafttreten der DS-GVO ermittelt wurden. Denn die Nutzung im Prozess dürfte eine datenschutzrechtlich erhebliche Verarbeitung in Form des Abfragens von Daten darstellen, vgl. *Schild* in: Brink/Wolff, BeckOK DatenschutzR, 35. Ed. 2021, Art. 4 DS-GVO, Rz. 47.

86 Rs. C-597/19. Siehe hierzu die Schlussanträge vom 17. Dezember 2020, Rs. C-597/19 – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

87 Vgl. Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 127 bis 133 – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

88 *Schmidt-Wudy* in: Brink/Wolff, BeckOK DatenschutzR, 35. Ed. 2021, Art. 14 DS-GVO, Rz. 31.

mahnung ausreichend ist.[89] Ein Verstoß gegen die Pflicht aus Art. 14 Abs.1 DS-GVO kann nach gegenwärtiger Rechtslage ohnehin nur zu behördlichen Sanktionen führen, nicht aber zur Rechtswidrigkeit der Ermittlung an sich.[90] Die Mitteilung der Ermittlung ist mithin *de lege lata* nicht weiter von Interesse.

c) Verhältnismäßigkeit

Die hohe Zahl an Abmahnungen[91] korrespondiert notwendigerweise mit einer hohen Zahl an Auskunftsbegehren. Die entsprechenden Gestattungsbegehren werden vor einigen wenigen Landgerichten verhandelt, da zuständig für Erstere das Landgericht am Sitz des jeweiligen ISPs ist, § 101 Abs.9 Satz 2 UrhG. Nach Einführung des Auskunftsanspruches[92] wurden diese Landgerichte mit entsprechenden Anträgen überhäuft. Nach Mitteilung eines vorsitzenden Richters des LG Köln beispielsweise seien dort von Januar bis September 2009 über 2824 Anträge auf Gestattung der Auskunft eingegangen, die jeweils ca. 15 bis 3000 IP-Adressen umfasst haben sollen; im Oktober 2009 soll ein Antrag sogar mehr als 11.000 IP-Adressen umfasst haben. Nahezu allen Anträgen wurde stattgegeben.[93] Es ist offensichtlich, dass bei dieser Masse eine, auch nur kursorische, Einzelfallprüfung daraufhin, ob die Anspruchsvoraussetzungen erfüllt sind[94], unwahrscheinlich erscheint.[95] Die *Digitale Gesellschaft e.V.* sah sich daraufhin veranlasst, diesen Sachverhalt bei der EU-Kommission mit einem Schreiben vom 4. April 2013 zu rügen.[96]

---

89 So auch die BFDI Bund, siehe https://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/InternetArtikel/AuskunftsrechtsBeiUrheberrechtsverstoss.html - Zugriff am 31.03.2021.

90 *Schmidt-Wudy* in: Brink/Wolff, BeckOK DatenschutzR, 35. Ed. 2021, Art. 14 DS-GVO, Rz. 18f.

91 Siehe Kapitel § 3 V. 2.

92 Siehe Kapitel § 2 III. 1.

93 *Bleich*, c't, Bd. 1, 2010, S. 155.

94 Zumindest müssten Angaben über Hashwerte, IP-Adressen und dem Verletzungszeitraum mit den angefügten Beweismitteln des Ermittlungsdienstes abgeglichen werden. Zudem müsste die Rechteinhaberschaft geprüft werden.

95 Siehe Seite 2 des Anschreibens der Digitalen Gesellschaft e.V. an die EU-Kommission, abrufbar unter https://digitalegesellschaft.de/wp-content/uploads/2013/04/anschreiben_eu_kommission.pdf - Zugriff am 31.03.2021.

96 Siehe Anschreiben der Digitalen Gesellschaft e.V. an die EU-Kommission, abrufbar unter https://digitalegesellschaft.de/wp-content/uploads/2013/04/anschreiben_eu_kommission.pdf - Zugriff am 31.03.2021.

Die EU-Kommission forderte schließlich mit Schreiben vom 11. Dezember 2014 die Bundesregierung zur Stellungnahme auf.[97] Kern der Beschwerde der Digitalen Gesellschaft e.V. war, dass die Zusammenfassung so vieler IP-Adressen in einem Antrag Art. 8 EnforcementRL verletze, demgemäß Auskunftsanträge die Verhältnismäßigkeit wahren müssen, sowie Art. 3 Abs.2 EnforcementRL, der das Verhältnismäßigkeitsprinzip allgemein für Maßnahmen auf Grundlage der EnforcementRL statuiert. Die Bundesregierung teilte in ihrer Antwort vom 21. April 2015 an die EU-Kommission mit, dass sie eine Verletzung des Verhältnismäßigkeitsprinzips nicht sehe: „*Dass sich ein Antrag auf eine größere Zahl von IP-Adressen bezieht, ist für sich genommen kein Beleg für eine Unverhältnismäßigkeit.*“.[98] Im Übrigen verwies sie darauf, dass jedenfalls im anschließenden Verletzungsverfahren die regulären Beweisanforderungen gelten würden[99], was wohl so zu verstehen ist, dass dies eine Abschwächung der Prüfungsdichte im Gestattungsverfahren rechtfertigen soll. Die EU-Kommission gab sich jedenfalls mit der Antwort zufrieden und beendete das Verfahren am 11. Dezember 2015.

Ob das dem Verfahren zu Grunde liegende tatsächliche Problem der „aufgeblähten“ Anträge auch zum gegenwärtigen Zeitpunkt noch besteht, kann nicht mit Sicherheit festgestellt werden; jedoch ist auf Grund der nach wie vor hohen Abmahnzahlen[100] davon auszugehen, auch wenn das Problem nicht mehr im gleichen Maße wie früher bestehen dürfte.

Sollte ein Anschlussinhaber also feststellen, dass der Gestattungsbeschluss, auf Grund dessen über ihn Auskunft erteilt wurde, eine derart hohe Anzahl an IP-Adressen umfasst, dass nicht davon auszugehen ist, dass in Anbetracht der Dauer zwischen Antrag und Erlass des Beschlusses eine Einzelfallprüfung

97 Siehe Bericht hierüber bei *Beckedahl*, Abmahnindustrie: EU-Kommission bereitet Klage wegen Verletzung des EU-Rechts vor. Dieses Kommissionsverfahren hat das Az. 7210/14/MARK. Die Unterlagen des Verfahrens sind nicht öffentlich. Der Verfasser hat sie auf Grund einer IFG-Anfrage vom BMJV erhalten. Siehe zum Beschwerderecht und dem anschließenden Pilotverfahren als Vorstufe zum Vertragsverletzungsverfahren *Cremer* in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Art. 258 AEUV, Rz. 4.

98 Seite 10 der Antwort der Bundesregierung.

99 Seite 10 der Antwort der Bundesregierung.

100 Siehe Kapitel § 3 V. 2.

stattgefunden hat[101], könnte er eine Beschwerde gegen den Beschluss versuchen.

Das Verhältnismäßigkeitserfordernis des Art. 8 EnforcementRL ist in § 101 Abs.4 UrhG umgesetzt[102] und damit auch nach deutschem Recht ein ausdrücklich normiertes Tatbestandsmerkmal des Anspruchs aus § 101 Abs.2 UrhG. Zwar erscheint es zunächst unzutreffend, eine unterlassene Einzelfallprüfung als Verhältnismäßigkeitsproblem einzuordnen. Jedoch lässt sich das Erfordernis der Verhältnismäßigkeit mangels inhaltlicher Eingrenzung als Einfallstor für eine Grundrechtsprüfung verstehen, sodass sich eine unterlassene Einzelfallprüfung als Verstoß gegen das Gebot rechtlichen Gehörs nach Art. 103 Abs.1 GG fassen lässt. Dem Anspruch aus § 101 Abs.2 UrhG steht dann § 101 Abs.4 UrhG iVm Art. 103 Abs.1 GG entgegen. Da nicht ausgeschlossen werden kann, dass ein Gestattungsbeschluss nicht ergangen wäre, wenn eine Einzelfallprüfung vorgenommen worden wäre[103], ist das Gestattungsverfahren dann im Hinblick auf den beschwerdeführenden Anschlussinhaber zu wiederholen[104], auch wenn die Tatbestandsvoraussetzungen des Auskunftsanspruches im Übrigen tatsächlich bestehen und eine Wiederholung des Gestattungsverfahrens mangels (noch bestehender) Speicherung der Zuordnung der einschlägigen IP-Adresse zum Anschlussinhaber beim ISP *de facto* nicht mehr möglich ist.

Demgegenüber kann der Auffassung der Bundesregierung, dass eine geringe Prüfungsdichte im Gestattungsverfahren durch die Beweisanforderungen im anschließenden Verletzungsverfahren kompensiert wird, nicht gefolgt werden. Das Gebot rechtlichen Gehörs ist in jedem Verfahren zu beachten; die Heilung eines Verstoßes durch Gewährung rechtlichen Gehörs in einem anderen Verfahren ist ausgeschlossen.[105] Schließlich ist es nicht gewährleistet, dass

[101] Eine feste Zahl lässt sich nicht bestimmen; allerdings sollte nach Auffassung des Verfassers davon auszugehen sein, dass ca. 500 IP-Adressen bei einem Entscheidungszeitraum von weniger als einer Woche das Limit sind.

[102] *Dreier* in: Dreier/Schulze/Specht, UrhG, 6. Aufl. 2018, § 101 UrhG, Rz. 22.

[103] Zu den geringen Anforderungen an das Erfordernis des Beruhens einer Entscheidung auf der Verweigerung rechtlichen Gehörs siehe *Radtke* in: Epping/Hillgruber, BeckOK GG, 46. Ed. 2021, Art. 103 GG, Rz. 17, mit Nachweisen der Rechtsprechung des BVerfG.

[104] Die Wiederholung ist auch im Rahmen des Beschwerdeverfahrens selbst möglich.

[105] Eine Heilung kommt nur innerhalb eines Verfahrens oder in einer Rechtsmittel- bzw. Rechtsbehelfsinstanz in Betracht, vgl. BVerfG, Beschluss vom 14. September 2016, Az. 1 BvR 1304/13, Rz. 28 – bverfg.de.

es überhaupt zu einem Verletzungsverfahren kommt; der Verstoß kann also nicht zwingend noch behoben werden.

Ob der (massenhafte) Verstoß gegen § 101 Abs.4 UrhG iVm Art. 103 Abs.1 GG ein Vertragsverletzungsverfahren (Art. 258 AEUV) gegen die Bundesrepublik gerechtfertigt hätte, kann dahinstehen, da wegen der Verfahrenseinstellung durch die Kommission mit einem solchen nicht mehr zu rechnen ist. Die Frage der Vereinbarkeit der Praxis der Gestattungsbeschlüsse mit EU-Recht, insbesondere Art. 8 EnforcementRL, könnte aber immer noch durch ein Vorlageverfahren allgemeinverbindlich geprüft werden.[106]

d) Aussetzung des Verfahrens und/oder Beweisverwertungsverbot

Die Auskunft eines ISP ist ohne einen rechtmäßigen Gestattungsbeschluss nicht verwertbar.[107] Das Gericht, das über die nach Auskunftserteilung erhobene Klage gegen einen Anschlussinhaber zu entscheiden hat, müsste daher, wenn der Anschlussinhaber Beschwerde gegen den Gestattungsbeschluss erhebt, das Verfahren gegen diesen nach § 148 ZPO aussetzen, bis über die Beschwerde rechtskräftig entschieden ist.

Die auf Basis eines erteilen Gestattungsbeschlusses gewährte Auskunft ist aber umgekehrt von dem Gericht, das über die nachfolgende Klage gegen den Anschlussinhaber zu entscheiden hat, nicht zwingend zu berücksichtigen, da die Rechtskraft des Beschlusses mangels Beteiligung des Anschlussinhabers nicht gegen diesen wirkt.[108] Erhebt ein Anschlussinhaber also nicht Beschwerde gegen den Gestattungsbeschluss, könnte das Gericht die Auskunft immer noch im Rahmen der Beweiswürdigung als unverwertbar einstufen, wenn es die, soeben dargestellten, Probleme des Datenschutzes und der Verhältnismäßigkeit sieht.

---

[106] In der Rs. C-597/19 hat der Generalanwalt nun ausdrücklich festgehalten, dass Massenauskunftsbegehren, die keine Differenzierung nach dem Einzelfall enthalten, unverhältnismäßig sein können, siehe Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 120f. – ECLI:EU:C:2020:1063 - „M.I.C.M.“. Es bleibt abzuwarten, wie der EuGH diesbezüglich entscheiden wird.

[107] Siehe Kapitel § 2 III. 1. b).

[108] Siehe Kapitel § 2 III. 1. b).

4. Ausdrückliche Normierung des Erfordernisses eines gewerblichen Ausmaßes

Nach der hier vertretenen Auffassung ist die Rechtsprechung des BGH, derzufolge der Auskunftsanspruch gemäß § 101 Abs.2 Satz 1 Nr.3 UrhG kein gewerbliches Ausmaß der Rechtsverletzung fordert, verfassungswidrig; somit ist in der Rechtspraxis hier noch nicht das letzte Wort gesprochen und ein Gang zum BVerfG möglich.[109]

Alternativ könnte das Erfordernis eines gewerblichen Ausmaßes der Rechtsverletzung auch *de lege ferenda* in § 101 Abs.2 UrhG aufgenommen werden. Dies hätte den Vorteil, dass in der Gesetzesbegründung eine Auslegung des Begriffes vorgeschlagen werden könnte, mit der sich die gegenwärtige Realität des *filesharing* fassen lässt. In seiner Stellungnahme zum Entwurf des Umsetzungsgesetzes der EnforcementRL hatte der Bundesrat zu Recht angemerkt, dass eine Definition des gewerblichen Ausmaßes, die auf den Umfang der Rechtsverletzung abstellt, vor dem Hintergrund der damals genutzten *filesharing*-Systeme Probleme bereiten könnte.[110] Das Gutachten, auf das sich der Bundesrat gestützt hatte, wies richtigerweise darauf hin, dass bei älteren Systemen alle Dateien, die ein Nutzer zur Verfügung stellt, eingesehen werden können, bei neuen Systemen jedoch nicht.[111] Als Beispiel: während man zum Beispiel beim Napster-System alle Lieder, die ein Nutzer zur Verfügung stellt, nachsehen konnte, war dies bei dem von den Gutachtern untersuchten eDonkey-System nicht der Fall. Für Ersteres war also eine Definition des gewerblichen Ausmaßes, die auf den Umfang der Verletzungshandlung abstellt, tauglich, da eine Differenzierung möglich gewesen wäre (zum Beispiel hätte das gleichzeitige Angebot von mehr als einem Lied als gewerbliches Ausmaß angesehen werden können). Für Letzteres wäre eine solche Definition mangels Differenzierungsmöglichkeit nicht tauglich gewesen, da der Umfang der Verletzungshandlung dort nicht ausreichend ermittelt werden kann. Der Bundesrat befürchtete also, dass dann keinem Nutzer ein gewerbliches Ausmaß vorgeworfen werden kann und eine Auskunft in *filesharing*-Fällen mithin nie erteilt werden könnte.

---

[109] Siehe zum Ganzen Kapitel § 4 IV. 1. g).

[110] BT-Drs. 16/5048, S. 59.

[111] *Steinebach/Zmudzinski*, Auswirkung einer Bagatellklausel auf die Verfolgbarkeit von Urheberrechtsverletzungen in Internet-Tauschbörsen, S. 2ff.

Bei dem mittlerweile fast ausschließlich benutzten BitTorrent-System ist eine Differenzierung allerdings wieder möglich, da im Rahmen der Ermittlung grundsätzlich zwischen *leechern* und *seedern* unterschieden werden kann.[112] Hierauf könnte also, wollte man das Erfordernis des gewerblichen Ausmaßes *de lege ferenda* ausdrücklich in den Wortlaut aufnehmen, in der entsprechenden Gesetzesbegründung hingewiesen werden. In der Praxis ergäbe sich dabei – zumindest für öffentliche Tracker – voraussichtlich auch ein gemischtes Verhältnis zwischen gewerblichen und nicht-gewerblichen Nutzern, da – zumindest nach älteren Untersuchungen – öffentliche Tracker im Schnitt zwischen zwei bis sieben *seeder* pro *leecher* per Zieldatei aufweisen.[113]

Dem Wunsch einer technologieneutralen Regelung wird man nicht entsprechen können, da einziger Anknüpfungspunkt für eine Definition des gewerblichen Ausmaßes der Umfang der Verletzungshandlung(en) ist, der sich eben bei manchen Systemen ermitteln lässt, bei anderen nicht. Eine wahrhaft technologieneutrale Regelung müsste also den *status quo* bewahren und das Erfordernis eines gewerblichen Ausmaßes ausschließen.

5. Normsetzung betreffend die Resellerproblematik

Die ausdrückliche Normierung eines Auskunftsanspruches und die Nicht-Erforderlichkeit eines Gestattungsbeschlusses gegen Reseller kann zunächst unterbleiben, da der BGH beides bereits durch seine Rechtsprechung etabliert hat.[114]

Wie dargestellt[115] ist ein Anspruch gegen ISPs auf Mitteilung der Benutzerkennung vor dem Hintergrund des Entscheidungskomplexes „YouTube-Drittauskunft“ zu verneinen. Beklagte Anschlussinhaber können daher in Resellerkonstellationen geltend machen, dass der Netzbetreiber deren Anschlusskennung nicht an den klagenden Rechteinhaber hätte herausgeben bzw. eine entsprechende Gestattungsanordnung nicht hätte ergehen dürfen und also auch die Mitteilung von dessen Namen und Anschrift durch den Reseller nicht von einer Legalisierungswirkung der Gestattungsanordnung erfasst ist; parallel kann auch die Gestattungsanordnung an den ISP direkt

[112] Siehe Kapitel § 1 IV. 7. c) dd).
[113] *Meulpolder* et al., Public and Private BitTorrent Communities: A Measurement Study, S. 4.
[114] Siehe Kapitel § 4 IV. 2.
[115] Siehe Kapitel § 4 IV. 2. a).

mittels Beschwerde angegriffen werden[116]. Konsequenz ist in jedem Fall, dass die Mitteilung von Name und Anschrift des Anschlussinhabers durch den Reseller datenschutzrechtlich unzulässig war und deshalb einem Beweisverwertungsverbot unterliegt – mit der Konsequenz, dass eine Verurteilung des Anschlussinhabers aus Beweisgründen ausscheiden muss.

Faktische Voraussetzung hierfür ist allerdings eine Abkehr des BGH von seiner „Benutzerkennung"-Rechtsprechung, die auf Basis des unter Kapitel § 4 IV. 2. a) Gesagten argumentiert werden kann. Sollte der BGH eine Abkehr verweigern, wäre auf Grundlage der in Kapitel § 4 IV. 1. g) dargestellten Rechtsprechung des BVerfG eine Verfassungsbeschwerde zu erwägen.[117]

Als Antwort hierauf wäre es dem Gesetzgeber aber möglich, einen Anspruch auf Auskunft betreffend die Anschlusskennung ausdrücklich in § 101 UrhG aufzunehmen – die EnforcementRL würde dem, wie dargestellt[118], nicht entgegenstehen.

6. Kosten des Auskunfts- und Sicherungsverfahrens

Die Kosten des Auskunfts- und Sicherungsverfahrens muss gegenwärtig – über § 91 ZPO – der Anschlussinhaber tragen, wenn es zu einem Verletzungsverfahren kommt, in dem er unterliegt.[119] Das bedeutet für Abgemahnte einen erheblichen Unsicherheitsfaktor, da sie insbesondere keinen Einfluss darauf haben, wie viele IP-Adressen in einem Antrag auf einen Gestattungsbeschluss zusammengefasst werden, mithin auf wie viele Köpfe sich dessen Kosten aufteilen.[120] Weiterhin haben Abgemahnte auch keinen Einfluss dar-

[116] Kapitel § 5 IV. 3.

[117] Die Konturen der Argumentation eines Verstoßes gegen das Willkürverbot wären in diesem Fall freilich noch weniger vorgezeichnet als in dem in Kapitel § 4 IV. 1. g) dargestellten Fall. Ein Beschwerdeführer müsste aufzeigen, dass der BGH mit der Entscheidung „Benutzerkennung" bzw. mit der Verweigerung einer Abkehr hiervon gegen das Willkürverbot verstößt, weil er hiermit seinen eigenen Feststellungen in der Entscheidung „YouTube-Drittauskunft II" widerspricht und sich entsprechend gegen die Wertung des Gesetzgebers in der Begründung zum Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums stellt.

[118] Siehe Kapitel § 4 IV. 2. a).

[119] Siehe Kapitel § 2 III. 1. g).

[120] Siehe Kapitel § 2 III. 1. g). Dies wird verstärkt dadurch, dass nach hiesiger Auffassung die gängige Praxis, sehr viele IP-Adressen in einem Antrag zusammenzufassen rechtswidrig ist, mithin also nur wenige Adressen pro Antrag geltend gemacht werden dürfen. Dies erhöht aber automatisch die Kosten pro Abgemahntem.

auf, welche Kosten dem ISP für die Sicherung der Zuordnung der IP-Adresse zu einem Anschluss anfallen. Folglich sollte geregelt werden[121], dass nichtgewerbliche handelnde natürliche Personen die Kosten des Auskunfts- und Sicherungsverfahrens auch dann nicht tragen müssen, wenn sie in einem Verletzungsverfahren verurteilt werden.

7. Abschaffung des Auskunftsverfahrens?

Als letzte Option wäre denkbar, das Auskunftsverfahren bzw. den zivilrechtlichen Auskunftsanspruch gegen ISPs ganz abzuschaffen, soweit er sich auf Kunden des ISPs bezieht, die natürliche Personen sind und nicht mit kommerzieller Absicht handeln. Europarechtlich und verfassungsrechtlich wäre dies zulässig.[122] Auch völkerrechtlich ist dies unproblematisch: nach Art. 47 TRIPS sind zivilrechtliche Auskunftsverfahren fakultativ.

Das hätte zur Folge, dass Rechteinhaber wie früher auf strafrechtliche Ermittlungen und die Einsicht in die Strafakten angewiesen wären.[123] Die Realität des *filesharing* ist jedoch anders als damals: Ermittlungsverfahren wurden vor Einführung des zivilrechtlichen Auskunftsanspruches erst ab Überschreiten einer Bagatellgrenze geführt. In der Praxis führte dies dazu, dass Verfahren regelmäßig nur gegen solche *filesharer* angestrengt wurden, die über Systeme wie FastTrack oder Gnutella mehrere hundert Musikstücke in Alleintäterschaft öffentlich zugänglich gemacht hatten. Statistisch betrachtet müssten die Staatsanwaltschaften heute meist darüber entscheiden, ob sie ein Ermittlungsverfahren gegen eine Person anstrengen wollen, die im Verdacht steht, *ein* Filmwerk in *Mittäterschaft* (mit einer unübersehbaren Zahl von Mittätern) öffentlich zugänglich gemacht zu haben. Zwar ist auch nach heutiger Rechtslage das nicht-kommerzielle öffentliche Zugänglichmachen eines

[121] Passender Regelungsort wäre beispielsweise § 97a oder § 101 UrhG.
[122] Siehe Kapitel § 4 V. 2. a).
[123] Siehe Kapitel § 2 II.

Werkes gemäß § 106 Abs.1 UrhG eine Straftat[124], jedoch wäre davon auszugehen, dass die Staatsanwaltschaften – wie früher – Strafverfahren einstellen oder jedenfalls die Strafgerichte Akteneinsicht verweigern würden.[125] Von einer Notwendigkeit, die §§ 153, 153a StPO europarechtskonform dahingehend auszulegen, dass eine Einstellung in solchen Fällen nicht in Betracht kommt, ist nicht auszugehen. Insbesondere hatte der EuGH in der Entscheidung „Promusicae" die (damalige) Rechtslage in Spanien[126] als unproblematisch erachtet, obwohl *filesharing* dieser zu Folge nicht einmal materiell strafbar war.[127] Auch das Völkerrecht stünde der Verfahrenseinstellung nicht entgegen, da gemäß Art. 61 Satz 1 TRIPS strafrechtliche Ermittlungsverfahren nur gegen „*copyright piracy on a commercial scale*" zur Verfügung stehen müssen und es den Unterzeichnerstaaten überlassen ist, wie sie *commercial scale* definieren.[128]

Gleichwohl ist zu bedenken, dass die Abschaffung des zivilrechtlichen Auskunftsverfahrens die Verfolgung von Urheberrechtsverletzungen durch Endnutzer mittels *filesharing* unter den genannten Voraussetzungen nahezu vollständig unmöglich machen würde und dies, unter den in der Einleitung dieser Arbeit genannten Prämissen, nicht hinzunehmen wäre. Diese Option sollte daher lediglich als *ultima ratio* verstanden werden, die nur dann gezogen werden sollte, wenn sich das Abmahnwesen, das in seiner gegenwärtigen Form ebenfalls nicht hinnehmbar ist, nicht mit den in dieser Arbeit im Übrigen genannten Vorschlägen in den Griff bekommen lässt.

Als gangbarer Mittelweg ließe sich über die Abschaffung des Auskunftsan-

---

[124] *Sternberg-Lieben* in: Ahlberg/Götting, BeckOK UrhR, 30. Ed. 2021, § 106 UrhG, Rz. 23. Im Rahmen des Zweiten Korbs gab es Überlegungen, die materielle Strafbarkeit mit einer Bagatellgrenze zu versehen; diese wurden von der Bundesregierung jedoch verworfen, gerade weil es die Staatsanwaltschaften hier über §§ 153, 153a StPO in der Hand hätten, Bagatellen prozessual angemessen über Einstellungen zu berücksichtigen, siehe BR-Drs. 257/06, S. 34. Möglich wäre jedoch auch eine materielle Entkriminalisierung von BitTorrent-*filesharing*. Europäisches Recht stünde dem nicht entgegen. Die EnforcementRL berührt das Strafrecht nicht, vgl. dort Art. 2 Abs.3 lit. c).

[125] Siehe Kapitel § 2 II.

[126] Vgl. Kapitel § 3 XII. 3. d).

[127] EuGH, Urteil vom 29. Januar 2008, Rs. C-275/06, Rz. 29ff. – ECLI:EU:C:2008:54 - „Promusicae".

[128] *Huang*, Intellectual Property Infringement on a 'Commercial Scale' in Light of the Ongoing Multilateral Agreement, S. 2.

spruchs mit gleichzeitiger Einführung eines – im internationalen Vergleich nicht unüblichen[129] – *three strike*-Systems nachdenken. Dies wurde bereits im Gesetzgebungsverfahren zur Umsetzung der EnforcementRL angedacht[130], aber nicht weiter verfolgt. Eine im Auftrag des Bundesministeriums für Wirtschaft und Technologie erstellte und im Jahr 2012 veröffentlichte Studie kam zu dem Ergebnis, dass der einfachgesetzlichen Einführung eines solchen Systems höherrangiges Recht nicht entgegenstünde.[131] Dies kann hier nicht weiter vertieft werden, wäre aber als Alternative im Auge zu behalten, sofern auf Grund fortbestehender Probleme mit einem Abmahnwesen eine Abschaffung des Auskunftsanspruchs zur Debatte stehen sollte.

Einen Kompromiss *de lege ferenda* zwischen einem Warnhinweismodell einerseits und der bisherigen Rechtslage andererseits schlägt *Ohly* vor. Dem bisherigen Verfahren der Auskunftserteilung und Abmahnung könnte ein (einmal stattfindendes) Warnverfahren vorgeschaltet werden[132], also ein Modell ähnlich dem *notice-and-takedown*-Verfahren bei Hostprovidern. Der ISP soll auf eine Verletzung hin (die der Rechteinhaber diesem mitteilen muss) den entsprechenden Kunden per Email verwarnen; erst wenn dieser die Verletzung nicht abstellt, soll er vom Rechteinhaber kostenpflichtig[133] abgemahnt werden können.[134] Dies würde die Haftung von Anschlussinhabern gegenüber der gegenwärtigen Rechtslage, gemäß der sie bereits bei nur einer einzigen registrierten Verletzung als Täter oder jedenfalls nach § 7 Abs.4 TMG in Anspruch genommen werden können, abmildern. Ein solches Modell dürfte einen Ausgleich zwischen den einschlägigen Grundrechten schaffen, der fairer ist als die gegenwärtig geltend Haftung für jede erstmalige Verletzung.

---

129 Siehe Kapitel § 3 XII. 2. b).

130 BT-Drs. 16/8783, S. 45.

131 *Schwartmann*, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, S. 326. Kritisch dazu *Hoeren*, Kurzgutachten zur BMWi-Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, S. 36ff. Siehe auch *Brüggemann*, Der Drittauskunftsanspruch gegen Internetprovider, S. 320f.

132 *Ohly*, Urheberrecht in der digitalen Welt - Brauchen wir neue Regelungen zum Urheberrecht und dessen Durchsetzung?, S. 120, 129.

133 Nach gegenwärtiger Rechtslage wäre dabei das Verhältnis zu § 7 Abs.4 Satz 3 TMG zu klären.

134 *Ohly*, Urheberrecht in der digitalen Welt - Brauchen wir neue Regelungen zum Urheberrecht und dessen Durchsetzung?, S. 120, 120.

Nachzudenken wäre gegebenenfalls über ein eigenes Sanktionssystem für Anschlussinhaber, die innerhalb eines bestimmten Zeitraums mehrere Warnhinweise für die Verletzung verschiedener Werke empfangen.[135]

8. Europarechtswidrigkeit des Auskunftsverfahrens in *filesharing*-Konstellationen?

In der Rs. C-597/19 ist der Generalanwalt der Auffassung, dass Urheberrechtstrollen die Rechte der EnforcementRL nicht zustehen und diesen daher unter bestimmten Voraussetzungen auch nicht das Auskunftsrecht zukommt.[136] Jedoch sind Urheberrechtstrolle in Deutschland praktisch nicht tätig und scheitern jedenfalls schon an der Aktivlegitimation.[137] Zudem führt der Generalanwalt richtigerweise an, dass die EnforcementRL nur mindestharmonisierend ist, ein Auskunftsverfahren für Urheberrechtstrolle also zwar nicht europarechtlich geboten, allerdings europarechtlich erlaubt ist.[138]

V. Zukünftige Behandlung der sekundären Darlegungslast und des Anscheinsbeweises

1. Reichweite der Nachforschungspflicht nach „Bastei Lübbe“

Da die Nachforschungspflicht im Zuge der „Bastei Lübbe“-Entscheidung des EuGH auf familiäre und nicht-familiäre Konstellationen nunmehr einheitlich anzuwenden ist[139], ist zu fragen, welche Vorgaben der EuGH macht. Hierbei ist zu beachten, dass der EuGH an die Vorlagefragen gebunden war, die lediglich zum Gegenstand hatten, ob es zulässig ist, dass ein Anschluss-

[135] Also ähnlich wie zum Beispiel in Neuseeland, siehe Kapitel § 3 XII. 2. b) bb), wobei anders als dort die Eskalationsstufen nicht davon abhängig gemacht werden sollten, dass von jeder Verletzung ein und derselbe Rechteinhaber betroffen ist.

[136] Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 67 bis 122 – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

[137] Siehe Kapitel § 3 I.

[138] Schlussanträge vom 17. Dezember 2020, Rs. C-597/19, Rz. 88f. – ECLI:EU:C:2020:1063 - „M.I.C.M.“.

[139] Da der EuGH Art. 7 GRC im Bezug auf die Haftung des Anschlussinhabers generell hinter Art. 17 Abs.2 GRC zurücktreten lässt, ist nicht damit zu rechnen, dass er in Zukunft im Falle weiterer Vorlagefragen Differenzierungen zwischen der familiären und nicht-familiären Nutzung erlauben wird.

inhaber seine täterschaftliche Haftung allein dadurch abwenden kann, dass er auf Familienmitglieder verweist, ohne „*nähere Einzelheiten zu Zeitpunkt und Art der Nutzung*“ vorzutragen.[140] Durch die verneinende Antwort des EuGH steht also fest, dass Anschlussinhaber zumindest „nähere Einzelheiten zu Zeitpunkt und Art der Nutzung“ vortragen müssen.

Unter dieser Prämisse besteht für den BGH gegenwärtig ein erheblicher Spielraum, sodass auf seine diesbezügliche, bisherige Rechtsprechung, insbesondere die Urteile „Every time we touch“ und „Tauschbörse III“, zu rekurrieren ist:

a) Zeitpunkt der Nutzung

Fraglich ist, ob die BGH-Urteile „Tauschbörse III“ und „Every time we touch“ so zu lesen sind, dass grundsätzlich eine physische Anwesenheit der potentiellen Mitnutzer im Zugriffsbereich des Internetanschlusses zum Verletzungszeitpunkt nachgeforscht werden muss, um die Nachforschungspflicht überhaupt erfüllen zu können.[141]

Eine zufriedenstellende Antwort lässt sich aus den genannten Urteilen leider nicht ableiten:

In „Every time we touch“ hatte der BGH entschieden, dass es im Rahmen der sekundären Darlegungslast irrelevant ist, wenn der Anschlussinhaber vorträgt, dass er zum Tatzeitpunkt physisch nicht in Zugriffsreichweite des Internetanschlusses anwesend war.[142] Dem ist zuzustimmen, denn ein *filesharing*-Vorgang kann natürlich auf einem Gerät auch ohne physische Anwesenheit einer Person zum ermittelten Verletzungszeitpunkt ausgeübt werden, entweder weil der Vorgang vor dem ermittelten Zeitpunkt bereits in Gang gesetzt wurde oder weil das entsprechende Gerät ferngesteuert wird. Dies müsste dann auch für den Vortrag betreffend die potentiellen Mitnutzer gelten. Da auch diese *filesharing* auf ihren Geräten ohne physische Anwesenheit zum ermittelten Verletzungszeitpunkt betreiben können, kann es auf deren phy-

[140] EuGH, Urteil vom 18. Oktober 2018, Rs. C-149/17, Rz. 22 – ECLI:EU:C:2018:841 - „Bastei Lübbe“.

[141] Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 35, 40 – GRUR 2016, 191 - „Tauschbörse III“ und BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 34, 38 – GRUR 2016, 1280 - „Every time we touch“.

[142] BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 54 – GRUR 2016, 1280 - „Every time we touch“.

sische Anwesenheit in Reichweite des Anschlusses nicht ankommen. Folglich verwundert es zunächst, wenn der BGH in „Tauschbörse III“ und „Every time we touch“ die Beweiswürdigung des Berufungsgerichts billigt, die gerade auf die entsprechende Anwesenheit der Mitnutzer zum Tatzeitpunkt abstellt.[143] Dies dürfte aber auf die Besonderheiten der jeweiligen Sachverhalte zurückzuführen sein. Die Ausführungen des Beklagten in „Tauschbörse III“ waren höchst widersprüchlich und wirkten daher eher wie Schutzbehauptungen[144], weshalb der BGH wohl die Möglichkeit eines anderen Täters nicht gelten gelten lassen wollte. Darüber hinaus hatte die Familie in diesem Fall nur *einen* internetfähigen PC.[145] Letzteres gilt auch für „Every time we touch“.[146] Da die Eltern in „Every time we touch“ zudem ihren Kindern nur jeweils für kurze Zeit pro Tag den Zugang zu dem Computer gewährt hatten[147], scheint der BGH wohl davon auszugehen, dass unter *diesen* Voraussetzungen eine mögliche Täterschaft der Kinder nur bei deren physischen Anwesenheit am PC zum Verletzungszeitpunkt in Betracht kommt.

Welche Überlegungen den BGH genau dazu veranlasst haben, die Beweisaufnahme und Beweiswürdigung durch die Berufungsgerichte in diesen Fällen für ausreichend zu erachten, kann jedenfalls dahinstehen. Selbst unter Berücksichtigung von Einzelhaushalten weist der durchschnittliche deutsche Haushalt (Stand 2016) mehr als ein *filesharing*-fähiges Gerät (PC, Notebook, Tablet, Smartphone) auf.[148] Und selbst wenn sich in einem Verfahren ergeben sollte, dass der Haushalt des beklagten Anschlussinhabers nur ein *filesharing*-fähiges Gerät aufweist, kann aus den genannten Gründen eine Ortsan- oder Abwesenheit der Mitnutzer in Zugriffsreichweite des Internetanschlusses keine Rolle spielen.

---

143 Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 38ff. – GRUR 2016, 191 - „Tauschbörse III“; BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 40ff. – GRUR 2016, 1280 - „Every time we touch“.

144 *Solmecke/Rüther/Büring*, MMR 2016, 153, 155.

145 Vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 40f. – GRUR 2016, 191 - „Tauschbörse III“.

146 BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 38, 40 – GRUR 2016, 1280 - „Every time we touch“.

147 BGH, Urteil vom 12. Mai 2016, Az. I ZR 48/15, Rz. 40, 43 – GRUR 2016, 1280 - „Every time we touch“.

148 https://de.statista.com/statistik/daten/studie/320980/umfrage/geraete-fuer-den-medienkonsum-pro-haushalt-in-deutschland/ - Zugriff am 31.03.2021.

Dem BGH ist hier also wohl weniger ein dogmatischer Fehler, sondern mangelnde dogmatische Klarheit vorzuwerfen. Jedoch hätte er voraussehen müssen, dass sich alle Instanzgerichte an seinen Aussagen in „Tauschbörse III“ und „Every time we touch“ orientieren werden, auch wenn sie eigentlich nicht verallgemeinerbar sind. Die Wahrheit der Maxime *hard cases make bad law*[149] zeigt sich hier nur zu deutlich.

Im Rahmen dieser mangelnden Klarheit besteht für Instanzgerichte mithin in Zukunft noch Spielraum; beklagten Anschlussinhabern sollten vor diesem Hintergrund über § 139 Abs.1 ZPO umfangreiche Hinweise dahingehend erteilt werden, welcher Vortrag nach dem gegenwärtigen Stand der Rechtsprechung von ihnen erwartet wird. Das Unterlassen von Hinweisen sollte in Berufungsverfahren gerügt werden. Der bestehende Spielraum sollte weiterhin dahingehend genutzt werden, dass es hinsichtlich des zu ermittelnden Nutzungszeitraums der Mitnutzer als ausreichend anzusehen ist, dass diese zumindest die Möglichkeit hatten, auf den Internetanschluss im Verletzungszeitpunkt zuzugreifen, sei es, weil eines ihrer internetfähigen Geräte eine LAN-Verbindung zum Router des Anschlussinhabers aufwies oder ihnen das zu diesem Zeitpunkt gültige WLAN-Passwort bekannt war oder sie auf ein Gerät des Anschlussinhabers zugreifen konnten. Die physische Ortsanwesenheit der behaupteten Mitnutzer zum Verletzungszeitpunkt sollte dagegen irrelevant sein; sie kann allenfalls in bestimmten Ausnahmefällen mit der Zugriffsmöglichkeit auf den Anschluss korrelieren (nämlich dann, wenn der behauptete Mitnutzer einen Zugriff auf den Internetanschluss zum Verletzungszeitpunkt nur über ein Gerät des Anschlussinhabers gehabt haben und dieser bestätigen kann, dass das Gerät vor und nach Benutzung durch den Mitnutzer ausgeschaltet war).

b) Art der Nutzung

Nach jetzigem Stand der Rechtsprechung des BGH muss der Anschlussinhaber über das Nutzungsverhalten, die Kenntnisse oder die Fähigkeiten seiner Mitnutzer im Bereich der Internetnutzung vortragen. Ungeklärt ist jedoch, welcher Vortrag hierzu genau erforderlich ist. Da die Aufklärung dieser Umstände für die in *filesharing*-Verfahren relevante Beweisfrage eigentlich keinen

[149] https://en.wikipedia.org/wiki/Hard_cases_make_bad_law - Zugriff am 31.03.2021.

Erkenntniswert hat[150], wäre es wünschenswert, wenn der BGH in Zukunft von diesem Erfordernis abkehrt. Bis dahin sollten Instanzgerichte die Anforderungen an entsprechenden Vortrag jedenfalls gering halten und umfangreich Hinweise erteilen.

Ungeklärt ist weiterhin, ob der Anschlussinhaber die Geräte seiner Mitnutzer auf *filesharing*-Software hin untersuchen muss. Die Aufklärung dieses Umstandes ist ebenso wie das Nutzerverhalten ohne Erkenntniswert.[151] Sollte der BGH daher über diese Frage in Zukunft zu entscheiden haben, wäre sie richtigerweise zu verneinen.

c) Zusammenfassung und Bewertung

Die Reichweite der Nachforschungspflicht ist teilweise ungeklärt, teilweise unbefriedigend gelöst. Sollte also der Gesetzgeber einschreiten? Abgesehen davon, dass es untypisch wäre, die sekundäre Darlegungslast in einem Spezialbereich gesetzlich zu fixieren, wo sie doch sonst der Prägung durch die Rechtsprechung überlassen ist[152], steht nach der „Bastei Lübbe"-Entscheidung nunmehr fest, dass der EuGH auch im nationalen Prozessrecht mitreden möchte, soweit es den Anwendungsbereich der InfoSocRL und EnforcementRL berührt. Eine gesetzliche Regelung erscheint sinnlos, wenn nicht genau vorhergesagt werden kann, welche Fassung der Nachforschungspflicht der EuGH im Falle einer Vorlage als zu eng ansehen würde. Aus Perspektive der Anschluss- und Rechteinhaber mag es höchst unbefriedigend sein, wenn mit Rechtssicherheit in diesem Punkt erst in nicht allzu naher Zukunft gerechnet werden kann; nach der gegenwärtigen europäischen Rechtslage geht hieran aber kein Weg vorbei.

2. Reichweite der Mitteilungspflicht nach „Loud"

Klarer als die Reichweite der Nachforschungspflicht ist die der Mitteilungspflicht. Die Entscheidung „Bastei Lübbe" des EuGH gibt keinen Anlass zu glauben, dass die Entscheidung „Loud" des BGH nicht mit Europarecht vereinbar ist. Anschlussinhaber werden also auch in Zukunft nicht nur ihre allgemeine Pflicht zur Mitteilung der nachgeforschten Umstände erfüllen müssen,

[150] Siehe Kapitel § 4 VII. 3. b) dd).
[151] Siehe Kapitel § 4 VII. 3. b) dd).
[152] Siehe Kapitel § 4 VII. 1. c).

sondern auch mitteilen müssen, falls sich ein (volljähriger) Familienangehöriger oder ein sonstiger Mitnutzer als Täter gestellt hat, und sodann den jeweiligen Namen nennen. Gegen ein Einschreiten des Gesetzgebers gilt das zur Nachforschungspflicht Gesagte, mit der Maßgabe, dass – ausgehend von den Aussagen in „Bastei Lübbe“[153] – sogar damit zu rechnen wäre, dass der EuGH eine Besserstellung von Familien im Rahmen der Mitteilungspflicht nicht billigt; eine gesetzliche Regelung, die Familien vor den Folgen von „Loud“ schützt, scheint daher erst recht zwecklos.

3. Einzelfragen zur sekundären Darlegungslast *de lege lata*

a) Offenes WLAN

Ungeklärt ist, wie der BGH die sekundäre Darlegungslast bei einem offen betriebenen WLAN fassen wird.[154] In „Bearshare“ und „Afterlife“ hatte er unter Rückgriff auf „Sommer unseres Lebens“ geäußert, dass den Inhaber eines Anschlusses, den er entweder mit anderen teilt oder der nicht hinreichend gesichert ist, eine sekundäre Darlegungslast trifft[155]; eine inhaltliche Ausgestaltung der sekundären Darlegungslast erfolgte dann aber bezüglich dem „nicht hinreichend gesichertem“ Betrieb nicht, da dieser in den jeweiligen Fällen auch nicht streitgegenständlich war. In „Sommer unseres Lebens“ war der nicht hinreichend gesicherte Betrieb zwar streitgegenständlich, die Nichttäterschaft des Anschlussinhabers jedoch unstreitig.[156] Im prominenten Fall „McFadden“ war die Täterschaft des Anschlussinhabers bei gleichzeitig offen betriebenem WLAN streitig, jedoch äußerte sich das zur Entscheidung berufene LG München I nicht zur Anwendung der Grundsätze der sekundären

[153] Siehe Kapitel § 4 VII. 3. c).

[154] Bisher hat sich der BGH allein mit der Auswirkung eines ungesicherten Betriebs auf die Störerhaftung befasst, siehe hierzu zuletzt BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 51 – juris - „Saints Row“ mit weiteren Nachweisen. Ob diese Rechtsprechung auch für bewusst offen betriebenes WLAN gelten sollte, hat der BGH bisher nicht klargestellt. Ohnehin lassen sich aus Überlegungen zur Störerhaftung, der die Prämisse der Schaffung einer Gefährdungslage zu Grunde liegt, keine Rückschlüsse auf die sekundäre Darlegungslast ziehen, deren Prüfung der Störerhaftung ja vorgelagert ist; siehe hierzu auch nachfolgend Kapitel § 5 V. 3. b).

[155] BGH, Urteil vom 8. Januar 2014, Az. I ZR 169/12, Rz. 15 – GRUR 2014, 657 - „BearShare“ und BGH, Urteil vom 6. Oktober 2016, Az. I ZR 154/15, Rz. 15 – GRUR 2017, 386 - „Afterlife“.

[156] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08, Rz. 12 – GRUR 2010, 633 - „Sommer unseres Lebens“.

Darlegungslast.[157] Zuletzt war auch in der Entscheidung „WLAN-Schlüssel“, die den ungesicherten WLAN-Betrieb betrifft, die täterschaftliche Haftung des beklagten Anschlussinhabers nicht streitgegenständlich.[158]

Bisher konnten lediglich einzelne Instanzentscheidungen ermittelt werden, in denen der offene Betrieb im Rahmen der sekundären Darlegungslast behandelt wurde: das AG Charlottenburg und das KG haben den Vortrag über den Betrieb eines offenen WLAN als für die Erfüllung der sekundären Darlegungslast ausreichen lassen, weil ein Zeuge den offenen Betrieb bestätigen konnte.[159] Das LG Berlin hat den bloßen Vortrag über einen offen Betrieb nicht ausreichen lassen; der Anschlussinhaber müsse in diesem Fall umfangreich zu Signalstärke, Leistungsfähigkeit und technischer Konfiguration seines Routers vortragen sowie dessen Logfiles einsehen.[160]

Gegen diese Annahmen der Instanzgerichte bestehen erhebliche Bedenken. Das AG Charlottenburg und das KG scheinen es in den angeführten Entscheidungen für nötig zu erachten, dass zur Erfüllung der sekundären Darlegungslast bezüglich des offenen Betriebs dieser durch einen Zeugen bestätigt werden muss. Sekundär vorgetragene Tatsachen bedürfen jedoch keines Beweises durch den sekundär Vortragenden.[161] Dem LG Berlin ist zuzugeben, dass die Signalstärke des WLANs relevant sein kann, wenn diese mit Sicherheit ausschließt, dass irgendeine andere Person als der Anschlussinhaber als Nutzer des Anschlusses zum maßgeblichen Zeitpunkt in Betracht kommt. Außer in bestimmten Ausnahmefällen[162] dürfte dies jedoch selten in Betracht kommen. Sonstige Faktoren (Leistungsfähigkeit, technische Konfiguration des Routers) sind irrelevant, da eine einmal aufgebaute Verbindung technisch ohne weiteres die Nutzung von *filesharing* ermöglicht. Die Ein-

[157] Vgl. LG München I, EuGH-Vorlage vom 18. September 2014, Az. 7 O 14719/12, Rz. 75 – juris. Auch der BGH hat sich in der Revision hierzu nicht positioniert bzw. nicht positionieren müssen, vgl. BGH, Urteil vom 7. März 2019, Az. I ZR 53/18 – GRUR 2019, 947 - „Bring mich nach Hause“.

[158] Vgl. BGH, Urteil ist 24. November 2016, Az. I ZR 220/15, Rz. 5 – GRUR 2017, 617 - „WLAN-Schlüssel“.

[159] AG Charlottenburg, Urteil vom 28. August 2018, Az. 213 C 99/17, Rz. 17 – juris; KG, Urteil vom 8. Februar 2017, Az. 24 U 117/15, Rz. 4 – MMR 2017, 486.

[160] LG Berlin, Urteil vom 29. Juni 2018, Az. 15 O 440/17, Rz. 45 – juris. Bestätigt durch KG, Urteil vom 11. November 2019, Az. 24 U 92/18 – waldorf-frommer.de.

[161] Siehe Kapitel § 4 VII. 4. a).

[162] Plakatives Beispiel: der Anschlussinhaber wohnt abgeschieden auf dem Land.

sicht in die Logfiles[163] hat nur insofern eine Aussagekraft, sofern diese für den Tatzeitpunkt MAC-Adressen ausweisen, die dem Anschlussinhaber nicht bekannt sind.[164]

Die Nachforschungspflicht beim offenen Betrieb eines WLAN ist richtigerweise also dahingehend zu fassen, dass der Anschlussinhaber prüfen muss, ob auf das WLAN außerhalb seines räumlichen Herrschaftsbereich zugegriffen werden kann[165] sowie in die Logfiles seines Routers Einsicht nehmen muss, sofern dieser Logfiles anlegt. Sollten die Logfiles dem Anschlussinhaber unbekannte MAC-Adressen aufweisen, so ist eine weitere Nachforschung nur möglich, sofern der Anschlussinhaber weiß, dass bestimmte Personen (zum Beispiel Mitbewohner) sein offenes WLAN nutzen. Er muss dann aufklären, ob die MAC-Adressen zu Geräten gehören, die diese Personen besitzen. Nach Mitteilung dieser Nachforschungen an den Rechteinhaber ist die sekundäre Darlegungslast erfüllt. Ein Nachweis der Nichttäterschaft von Mitnutzern in der anschließenden Beweiswürdigung scheidet im Regelfall aus, da der Anschlussinhaber seine Mitnutzer nicht kennt. Einziger Ausnahmefall ist, wenn erstens Logfiles existieren und diese für den Tatzeitpunkt ausschließlich Geräte des Anschlussinhabers aufführen oder zweitens Logfiles existieren und diese für den Tatzeitpunkt (auch) Geräte von Dritten aufführen, die sämtlich im Besitz von, dem Anschlussinhaber bekannten, Mitnutzern sind. Im ersteren Fall scheiden Mitnutzer aus, daher ist die Täterschaft des Anschlussinhabers sofort zu vermuten. Im letzteren Fall kann wie beim geschlossenen Betrieb mit bekannten Mitnutzern verfahren werden (Zeugenvernahme der Mitnutzer).

Im Regelfall jedenfalls müsste die Darlegung eines offenen Betriebes also an sich bereits die Erfüllung der sekundären Darlegungslast ermöglichen. Da im Anschluss an die Erfüllung der sekundären Darlegungslast – anders als beim geschlossenen Betrieb – unter Umständen keine Zeugen vernommen werden können, würde ein offener Betrieb zudem wesentlich seltener zur täterschaftlichen Haftung des Anschlussinhabers führen als der geschlossene Betrieb. Man mag dies als falsche Anreizsetzung dafür ansehen, seinen An-

[163] Siehe zu Logfiles Kapitel § 1 V. 2. a) und § 5 V. 3. e).

[164] Sofern die Logfiles nur MAC-Adressen von Geräten des Anschlussinhabers ausweisen, scheidet die Täterschaft einer dritten Person aus.

[165] Tests vor der Haustür, Befragung von Nachbarn etc.

schluss grundsätzlich offen zu betreiben.[166] Rechtlich formulieren ließe sich diese Kritik dadurch, die Konsequenz der unterschiedlichen Haftungsrisiken als ungerechtfertigte Ungleichbehandlung einzustufen. Jedoch wird das verringerte Risiko der täterschaftlichen Haftung beim offenen Betrieb durch das – auf Grund der anonymen und potentiell großen Nutzerbasis – vergrößerte Risiko der technisch missbräuchlichen Verwendung sowie dem vergrößerten Risiko, aus § 7 Abs.4 TMG in Anspruch genommen zu werden, wieder aufgewogen, sodass im Ergebnis sowohl der geschlossene Betrieb als auch der offene Betrieb nicht pauschal als unterschiedlich vorteil- oder nachteilhaft angesehen werden können.[167] Zudem hat der Gesetzgeber im Rahmen der TMG-Reform die Zunahme des offenen Betriebs von WLAN-Anschlüssen ausdrücklich als Zielvorgabe formuliert.[168] Zwar hat er es versäumt, ausdrücklich das Verhältnis von § 7f. TMG zur sekundären Darlegungslast zu regeln[169]; dies hindert jedoch nicht daran, diese ausdrücklich formulierte Zielvorgabe im Sinne der Einheitlichkeit der Rechtsordnung als Argument für die hier vorgeschlagene Fassung der sekundären Darlegungslast beim offenen Betrieb heranzuziehen, da sie diese Fassung lediglich stützt, nicht aber begründet.

Zuletzt sollte man sich außerdem – als Kontrollüberlegung – fragen, ob die Tatsache, dass in Zukunft Anschlussinhaber ihr WLAN möglicherweise lieber offen betreiben, um der täterschaftlichen Haftung leichter entgehen zu können als beim geschlossenen Betrieb, weniger gegen die soeben vorgeschlagene Reichweite der sekundären Darlegungslast beim offenen Betrieb spricht, als vielmehr gegen die extremen Folgen, die die täterschaftliche Haftung eines Anschlussinhabers gegenwärtig zeitigt.

b) Gewerblich angebotene WLANs und Mischformen

Ungeklärt ist, ob Anschlussinhaber, die ihren Internetanschluss anderen Personen aus (teilweise) gewerblichen Motiven zur Verfügung stellen, im Rah-

166 *Spindler*, GRUR 2018, 16, 20.

167 Zu beachten ist, dass die gesetzliche Pflicht aus § 13 Abs.6 TMG, Nutzern den Zugang in anonymisierter Form zur Verfügung zu stellen, im Rahmen der Prüfung der sekundären Darlegungslast beim offenen Betrieb keine Rolle spielen kann, da vor Anwendung des § 13 Abs.6 TMG zunächst feststehen muss, ob der Diensteanbieter wegen der Durchleitung fremder oder eigener Informationen haftet.

168 BT-Drs. 18/6745, S. 1f.

169 Siehe hierzu Kapitel § 4 VIII. 4. b).

men der sekundären Darlegungslast anders zu stellen sind als Anschlussinhaber, bei denen dies nicht der Fall ist. Zu denken wäre daran, dass das Accessprovider-Privileg aus Art. 12 ECommerceRL eine entsprechende Vorgabe machen könnte. Jedoch soll über die sekundäre Darlegungslast ja zunächst ermittelt werden, ob der Anschlussinhaber überhaupt Zugangsvermittler war oder stattdessen eine streitige Urheberrechtsverletzung selbst begangen hat. Richtigerweise sind also die Inhaber von (auch teilweise) gewerblich angebotenen Anschlüssen gegenüber nicht-gewerblichen Anschlussinhabern nicht zu privilegieren.[170]

Ist Anschlussinhaber eine juristische Person oder eine Personengesellschaft, sollten diejenigen Organe als Äquivalent zum „natürlichen" Anschlussinhaber gesehen werden, die zum Tatzeitpunkt faktischen Zugriff auf die Zugangsdaten des Anschlusses hatten.

c) Nachforschungslücken bei Altfällen

Der BGH scheint in den Entscheidungen „Ego-Shooter-Spiel" und „Saints Row" anzudeuten, dass die Nachforschungspflicht ab Erhalt einer Abmahnung gelten kann.[171] Unabhängig davon schlagen Instanzgerichte vereinzelt in dieselbe Kerbe und werten es zu Lasten des Anschlussinhabers, wenn er nicht bereits ab Erhalt der Abmahnung seine Mitnutzer befragt oder keine Erinnerungen mehr zu dem abgemahnten Tag hat.[172] Gerade im Zuge der Aufarbeitung von Altfällen[173] dürften sich die Sachverhalte mehren, in denen eine befriedigende Nachforschung ab Klagezustellung schlicht nicht mehr möglich ist, weil die damaligen potentiellen Mitnutzer keine Erinnerung mehr daran haben, ob sie zum fraglichen Zeitpunkt den Anschluss nutzen konnten, oder – zum Beispiel im Falle von ehemaligen WG-Mitbewohnern – unbekannt

[170] Insofern ergibt sich auch aus der Privilegierung gewerblich angebotener WLANs im Rahmen der Störerhaftung gemäß BGH, Urteil vom 7. März 2019, Az. I ZR 53/18, Rz. 23 – GRUR 2019, 947 - „Bring mich nach Hause" dahingehend, dass diese nicht vor einem vorherigen Hinweis auf eine Verletzung entstehen kann, nichts anderes.

[171] Vgl. BGH, Urteil vom 27. Juli 2017, Az. I ZR 68/16, Rz. 18 – MMR 2018, 311 - „Ego-Shooter-Spiel". BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19 – juris - „Saints Row".

[172] Siehe beispielsweise AG Charlottenburg, Urteil vom 25. April 2018, Az. 231 C 382/17 – waldorf-frommer.de oder AG Magdeburg, Urteil vom 28. September 2017, Az. 114 C 247/16 (114) – waldorf-frommer.de.

[173] Siehe Kapitel § 3 XI. 1.

verzogen sind.

Nachforschungslücken können jedoch nicht zu Lasten des Anschlussinhabers gehen. Die Nachforschungspflicht als Teil der sekundären Darlegungslast entsteht erst als Teil eines Prozessrechtsverhältnisses, das selbst wiederum erst mit Zustellung einer Klage entsteht.[174]

Insbesondere im Fall der Unkenntnis der ladungsfähigen Anschrift eines unbekannt verzogenen Mitnutzers seitens des Anschlussinhabers muss dies auch aus folgenden Gründen gelten:

Mangels Zugriff auf das Melderegister für Privatpersonen ist dem Anschlussinhaber die Ermittlung der Anschrift nicht möglich, wenn der ehemalige Mitnutzer nicht freiwillig mitwirkt; es ist ein allgemeiner Rechtsgrundsatz, dass unerfüllbare Pflichten nicht bestehen können. Folglich ist der Anschlussinhaber dann lediglich gehalten, die Anschrift nach seinen Möglichkeiten durch Kontaktaufnahme mit dem Mitnutzer in Erfahrung zu bringen, und im Falle des Scheiterns dem Rechteinhaber Tatsachen mitzuteilen, die diesem eine Ermittlung der Anschrift ermöglichen, wie zum Beispiel Email-Adressen, Telefonnummern, Nutzerkonten in sozialen Medien etc. Da der Anschlussinhaber nicht die Beweislast trägt, müsste das Gericht in Folge dem Rechteinhaber eine Beibringungsfrist für die ladungsfähige Anschrift nach § 356 ZPO setzen. Kann auch der Rechteinhaber diese sodann nicht beibringen, so müsste die sekundäre Darlegungslast des Anschlussinhabers hilfsweise beinhalten, dass dieser andere Beweismittel anführt, die Hinweise auf die behauptete Anschlussnutzung des verzogenen Mitnutzers geben können. Die Hörung entsprechender Zeugen beispielsweise könnte der Rechteinhaber dann als Zeugen vom Hörensagen zulässiger Weise beantragen. Parallel wäre es dem Gericht von Amts wegen möglich, nach § 273 Abs.3 Nr. 2 ZPO eine Melderegisterauskunft einzuholen.[175]

Sollte trotz alldem die Ermittlung der ladungsfähigen Anschrift nicht gelingen, würde dies – da der Anschlussinhaber nicht die Beweislast trägt – zu Lasten des Rechteinhabers gehen, d.h. die (gewollte) Alleinnutzung und damit die Täterschaft des Anschlussinhabers wäre nicht bewiesen.

[174] Zu einer etwaigen Nachforschungspflicht nach Zugang der Abmahnung siehe Kapitel § 4 XII. und 5 X.

[175] Siehe zum Vorgesagten ausführlich *Khazaeli*, ZUM-RD 2019, 659, 660f.

d) Mehrheit von Anschlussinhabern

Wie bereits in Kapitel § 4 VII. 3. b) dd) festgehalten, ist es dogmatisch zunächst unbedenklich, wenn die Regeln der sekundären Darlegungslast auch zur Anwendung kommen, wenn die Inhaberschaft an einem Anschluss bei mehr als einer Person liegt. Jedoch sollte *de lege lata* die sekundäre Darlegungslast auch als erfüllt angesehen werden, wenn neben den Anschlussinhabern keine sonstigen Mitnutzer vorhanden sind, da ansonsten die Konstellation *mehrere Anschlussinhaber ohne Mitnutzer* gegenüber der Konstellation *ein Anschlussinhaber mit sonstigen Mitnutzern* ohne sachlichen Grund benachteiligt wäre. An die Stelle der Zeugenvernahme tritt dann – da der Rechteinhaber notwendigerweise alle Anschlussinhaber gemeinsam verklagen muss – eine zwingende Parteivernehmung.[176] Unterschiede ergeben sich bei Letzterer allerdings zwangsweise insoweit, als sich Anschlussinhaber wahrheitsgemäß zu dem Vorwurf der Tatbegehung erklären müssen (§ 138 ZPO), während hingegen Zeugen nicht direkt danach gefragt werden dürfen, ob sie die streitgegenständliche Urheberrechtsverletzung begangen haben, sondern nur zu ihrer Nutzung des Anschlusses im Tatzeitpunkt[177]. Erscheinen die Angaben des Anschlussinhabers und die Aussagen aller Zeugen in letzterer Konstellation gleich glaubwürdig, ist es beweisrechtlich dennoch notwendig, die Täterschaft des Anschlussinhabers anzunehmen[178]; erscheinen in ersterer Konstellation die Angaben aller Anschlussinhaber als gleich glaubwürdig, ist die Täterschaft keines Inhabers bewiesen[179], weshalb also keiner von diesen als Täter haftet.

Diese potentiell bei der Beweiswürdigung auftretende, leichte Bevorzugung der Konstellation *mehrere Anschlussinhaber ohne sonstige Mitnuter* gegenüber der Konstellation *ein Anschlussinhaber mit sonstigen Mitnutzern* dürfte gerade noch dadurch zu rechtfertigen sein, dass sich Anschlussinhaber – anders als Zeugen – durch ihre vertragliche Anschlussinhaberschaft einem höheren rechtlichen Risiko ausgesetzt sehen[180], und daher Nutzer eines Inter-

[176] Siehe Kapitel § 4 VII. 3. b) dd).
[177] Siehe Kapitel § 4 VII. 4.
[178] Siehe Kapitel § 4 VII. 4.
[179] § 830 Abs.1 Satz 2 BGB greift in diesem Fall nicht, da die Norm voraussetzt, dass lediglich die Kausalität ungeklärt ist, siehe *Spindler* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 830 BGB, Rz. 22.
[180] Beispielsweise dem Risiko der Haftung nach § 7 Abs.4 TMG. Zudem sind sie immer die Adressaten einer Abmahnung.

netanschlusses, die sich *qua* Inhaberschaft dieses Risiko teilen[181], bevorzugt werden dürfen.

e) Durchsuchung von Geräten, Logfiles, WLAN-Sniffer

Offen ist, wie der BGH Aspekte eher technischer Natur im Rahmen der Nachforschungspflicht behandeln wird.

In der Instanzrechtsprechung ist vereinzelt angenommen worden, der Anschlussinhaber müsse auf den Geräten seiner Mitnutzer nach der streitgegenständlichen Datei suchen.[182] Abgesehen von den möglichen datenschutzrechtlichen Bedenken hat die Durchsuchung von Geräten nach der streitgegenständlichen Datei auch dann keine Aussagekraft, wenn die Datei tatsächlich aufgefunden wird. Denn dies sagt nichts darüber aus, ob die Datei auch von der streitgegenständlichen *filesharing*-Aktivität stammt.[183] Die Durchsuchung von Geräten sollte daher nicht zum Gegenstand der Nachforschungspflicht gemacht werden.

Logfiles des Routers können eine Aussagekraft haben, da sich ihnen – soweit sie noch für den Verletzungszeitpunkt existieren – entnehmen lässt, welche MAC-Adressen zum Router verbunden waren.[184] Die potentieller Mitnutzer zum Tatzeitpunkt lassen sich dann auf die Besitzer der entsprechenden Geräte eingrenzen. Die Nachforschung nach Logfiles und Vorlage derselben sollte daher richtigerweise zum Gegenstand der sekundären Darlegungslast gemacht werden; umgekehrt aber darf es einem Anschlussinhaber nicht zum Nachteil gereichen, wenn diese zu Prozessbeginn nicht mehr existieren. Da die sekundäre Darlegungslast erst ab Zustellung einer Klage greift[185], würde

[181] Weil sie beispielsweise alle gemeinschaftlich für den Anspruch aus § 7 Abs.4 TMG haften.

[182] Beispielsweise AG Nürnberg, Urteil vom 25. Oktober 2017, Az. 32 C 3784/17, Rz. 21 – juris, unter Berufung auf „Tauschbörse III“. Der BGH hat jedoch die Suche nach der streitgegenständlichen Datei selber nicht für erforderlich gehalten, sondern lediglich insofern die vom Berufungsgericht gestellten Anforderungen akzeptiert, vgl. BGH, Urteil vom 11. Juni 2015, Az. I ZR 75/14, Rz. 41f. – GRUR 2016, 191 - „Tauschbörse III“. In „Morpheus“ hatte der BGH zudem nicht einmal die Durchsuchung des PCs eines minderjährigen Kindes für erforderlich gehalten, siehe BGH, Urteil vom 15. November 2012, Az. I ZR 74/12, Rz. 29 – GRUR 2013, 511 - „Morpheus“.

[183] Siehe Kapitel § 1 IV. 7. c) aa).

[184] Siehe Kapitel § 1 V. 2. a) und § 5 V. 3. a).

[185] Siehe zur Nachforschungspflicht ab Zugang der Abmahnung Kapitel § 4 XII. und § 5 X.

andernfalls ein Prozessverhältnis rückwirkend auf einen Zeitpunkt angewendet werden, zu dem es noch nicht bestand.

Aus diesem Grund kann auch der Einsatz von WLAN-Sniffern[186] nicht verlangt werden.[187] Andernfalls würde man die Nachforschungspflicht sogar bereits für einen Zeitpunkt annehmen, zu dem noch gar keine Verletzungshandlung stattgefunden hat.

4. Zur zukünftigen Beweiswürdigung nach Erfüllung der sekundären Darlegungslast

Aus der gegenwärtigen Rechtsprechung des BGH lässt sich ableiten, dass die Beweiswürdigung dogmatisch (richtigerweise) kein Teil der sekundären Darlegungslast ist.[188] Eine ausdrückliche Klarstellung durch den BGH wäre in Zukunft dennoch wünschenswert. Hinsichtlich der Beweiswürdigung an sich können den Gerichten nur wenige Vorgaben gemacht werden, gewisse Leitlinien können jedoch aufgestellt werden.[189]

Ungeklärt ist bisher allerdings, wie mit der Mischkonstellationen der Zeugnisverweigerung umzugehen ist, in der also der Anschlussinhaber als Mitnutzer Familienmitglieder und nicht familiär verbundene Personen hat, und Erstere die Aussage nach § 383 ZPO verweigern. Sonstigen Mitnutzern steht kein Recht zu, die Aussage insgesamt zu verweigern. Auf Basis von § 384 Nr.1 und Nr.2 ZPO dürfen sie zwar die Beantwortung der Frage, ob sie die streitgegenständliche Urheberrechtsverletzung selbst begangen haben, verweigern; im Übrigen müssen sie jedoch aussagen.[190] Der BGH hatte bisher nur über den Fall zu entscheiden, in dem alle Mitnutzer die Aussage nach § 383 ZPO

[186] Siehe Kapitel § 1 V. 2. a).

[187] Ob die Vorlage der von einem freiwillig eingesetzten WLAN-Sniffer ermittelten Daten datenschutzrechtlich verlangt werden kann, kann aus praktischen Gründen in dieser Arbeit dahinstehen, da nicht ersichtlich ist, dass WLAN-Sniffer in größerem Umfang eingesetzt werden.

[188] Siehe Kapitel § 4 VII. 4. a).

[189] Siehe Kapitel § 4 VII. 4. b).

[190] *Scheuch* in: Vorwerk/Wolf, BeckOK ZPO, 40. Ed. 2021, § 384 ZPO, Rz. 2. Dies gilt auch dann, wenn beispielsweise bei zwei Mitnutzern einer definitiv keine Nutzungsmöglichkeit zum Tatzeitpunkt hatte und der Anschlussinhaber seine Täterschaft verneint. Denn es verbleibt neben dem zweiten Mitnutzer immer noch der Anschlussinhaber als potentieller Täter, sodass sich der verbliebene, potentiell verdächtige Mitnutzer durch seine Aussage auch in dieser Konstellation nicht selbst belasten kann, solange er nicht direkt nach seiner Täterschaft gefragt wird.

verweigern konnten.[191] Theoretisch könnte ein Gericht auf die Idee kommen, wenn von beispielsweise zwei Mitnutzern einer die Aussage berechtigterweise nach § 383 ZPO verweigert und der andere Mitnutzer die Aussage nicht nach § 383 ZPO verweigern kann, aber mangels Nutzungsmöglichkeit zum Tatzeitpunkt nicht als Täter in Betracht kommt, den Anschlussinhaber als Täter anzusehen. Jedoch wäre dies eine mittelbare Wertung der Zeugnisverweigerung zu Lasten des Anschlussinhabers, da nach dieser Wertung der die Aussage verweigernde Zeuge als potentieller Täter ausscheidet, obwohl eine solche Wertung die Würdigung dessen Aussage voraussetzen würde. Im Ergebnis kann die Täterschaft eines Mitnutzers also bereits dann nicht ausgeschlossen werden, sobald ein Mitnutzer des Anschlussinhabers die Aussage verweigert. In solchen Mischkonstellationen haftet der Anschlussinhaber also unter den soeben genannten Bedingungen richtigerweise nie als Täter.

5. Zur zukünftigen Behandlung der tatsächlichen Vermutung

Gegenwärtig greift die tatsächliche Vermutung / ein Anscheinsbeweis für die Täterschaft des Anschlussinhabers dann, wenn die beabsichtigte oder gebilligte Mitnutzung seines Anschlusses durch Dritte ausgeschlossen werden kann. Um die Vermutung / den Anscheinsbeweis zu erschüttern, muss der Anschlussinhaber daher aufzeigen, dass die unberechtigte Nutzung des Anschlusses durch einen Dritten zum Tatzeitpunkt ernsthaft in Betracht kommt.[192] Solange kein allgemein bekannter Sachverhalt besteht, demzufolge Internetanschlüsse regelmäßig gehackt und sodann für Urheberrechtsverletzungen genutzt werden, muss ein Anschlussinhaber gegenwärtig für seinen konkreten Einzelfall einen entsprechenden Geschehensablauf (Hack des Anschlusses und Nutzung des Internetanschlusses für die streitgegenständliche Urheberrechtsverletzung durch den Hacker) darlegen können. Dies dürfte in den allermeisten Fällen nicht gelingen. Es ist daher damit zu rechnen, dass auch in Zukunft die tatsächliche Vermutung / der Anscheinsbeweis praktisch

[191] Siehe Kapitel § 2 XI. 4.
[192] Siehe Kapitel § 4 VII. 5.

nie entkräftet werden kann.[193]

VI. Änderung des TMG?

In Kapitel § 4 VIII. wurde aufgezeigt, dass die für Anschlussinhaber relevanten Vorschriften des TMG erhebliche Auslegungsschwierigkeiten mit sich bringen. Ist also eine Änderung durch den Gesetzgeber angezeigt? Zur Beantwortung dieser Frage ist zunächst zwischen den Aspekten zu differenzieren, bei denen europarechtlicher Spielraum besteht und bei denen kein solcher Spielraum besteht.

Nichts spricht dagegen, die Anschlussteilung mittels LAN der Anschlussteilung mittels WLAN ausdrücklich gleichzustellen[194], um Wertungswidersprüche zu vermeiden. Gleichfalls empfiehlt sich zur Beseitigung von Auslegungszweifeln eine ausdrückliche Gleichstellung der privaten, also nichtkommerziell veranlassten Anschlussteilung mit der kommerziell veranlassten (wobei Private auch vollständig aus dem Anwendungsbereich des § 7 Abs.4 iVm § 8 Abs.1 Satz 2 TMG herausgenommen werden können, hierzu sogleich). Hinsichtlich der Sperrmaßnahmen spricht nichts dafür, dass der EuGH Portsperren oder Datenmengenbegrenzungen für zulässig oder gar notwendig erachten würde. Da diese jedoch nur in der Gesetzesbegründung zum 3. TMGÄndG und nicht im Wortlaut des § 7 Abs.4 TMG genannt werden, können sie im Wege der Auslegung unberücksichtigt bleiben[195] , weshalb § 7 Abs.4 TMG in diesem Punkt nicht geändert werden muss.

Ob § 7 Abs.4 TMG generell abgeschafft werden könnte, hängt davon ab, ob und inwieweit der EuGH auf Anschlussinhaber seine Netzsperren-Rechtsprechung zu ISPs anwenden wird oder nicht. „McFadden“ hat dies

[193] Beim offenen Betrieb eines WLAN hingegen dürften sekundäre Darlegungslast und tatsächliche Vermutung auch theoretisch gleichlaufen, da es beim offenen Betrieb keine unberechtigten Mitnutzer des WLAN gibt. Kann der Anschlussinhaber also dort seine sekundäre Darlegungslast nicht erfüllen, wäre als einzige Verteidigung seinerseits noch denkbar, dass eine dritte Person unberechtigt seine *filesharing*-fähigen Geräte verwendet habe. Die tatsächliche Vermutung wäre in diesem Fall so zu fassen, dass auch dies nur eine theoretische Möglichkeit darstellt und daher die eigenhändige Täterschaft des Inhabers des offenen WLAN vermutet wird.

[194] Siehe zur Situation *de lege lata* Kapitel § 4 VIII. 2. a) bb).

[195] Siehe Kapitel § 4 VIII. 3. e) ff) und gg).

(wohl) wegen des begrenzten Umfangs der Vorlage offen gelassen.[196] Eine Abschaffung würde nach gegenwärtigem Stand eine Rückkehr zur Störerhaftung gemäß § 1004 BGB analog nach altem Muster bedeuten, da eine vollständige Abschaffung der Vermittlerhaftung für Anschlussinhaber (private und kommerzielle) nicht mit Art. 8 Abs.3 InfoSocRL vereinbar wäre.[197] Sollte der EuGH jedoch – unabhängig von der Geltung des § 7 Abs.4 TMG – seine Netzsperren-Rechtsprechung auch auf Anschlussinhaber erweitern, so wäre davon auszugehen, dass der BGH – den § 7 Abs.4 TMG hinweg gedacht – Ansprüche auf Netzsperren gegen Anschlussinhaber wie bei ISPs auch[198] auf Grundlage von § 1004 BGB analog zusprechen würde.[199] Tatsächlich würde es dann keinen Unterschied machen, ob § 7 Abs.4 TMG existiert oder nicht.[200]

Die Frage also, ob § 7 Abs.4 TMG in seinen europarechtlich relevanten Punkten geändert werden sollte, hängt maßgeblich davon ab, wie sich der EuGH in Zukunft zum Haftungsumfang von Anschlussinhabern äußern wird. Wünschenswert für die Rechtsklarheit wäre hier insbesondere, dass er auf die Unterschiede, die sich zwischen Netzsperren-Ansprüchen bei ISPs einerseits und Anschlussinhabern andererseits hinsichtlich des Subsidiaritätskriteriums und dem möglichen, ausufernden Umfang von Sperrmaßnahmen gegen Letztere,

196 Siehe Kapitel § 4 VIII. 3. e) hh).

197 Siehe hierzu auch Kapitel § 4 VIII. 10.

198 BGH, Urteil vom 26. November 2015, Az. I ZR 174/14 – GRUR 2016, 268 - „Störerhaftung des Access-Providers“.

199 Was, dies sei nebenbei bemerkt, dogmatisch jedenfalls deshalb verfehlt erscheint, weil § 1004 BGB als Rechtsfolge nur ein Unterlassen einer Rechtsverletzung zuspricht, Netzsperren aber ein aktives Tun erfordern. Netzsperren könnten nach hiesiger Auffassung daher *de lege lata* nur mittelbar im Rahmen von § 890 ZPO als erforderlich angesehen werden, d.h. die Nichtimplementierung von Netzsperren stellt einen schuldhaften Verstoß gegen die Unterlassungspflicht dar. Für eine ausdrückliche gesetzliche Regelung von Ansprüchen auf Netzsperren gegen ISPs siehe *Grisse*, Internetangebotssperren, S. 401ff.

200 § 7 Abs.4 TMG ist also nach gegenwärtigem Stand europarechtlich zulässig, nicht aber geboten. Sollte der EuGH die Netzsperren-Rechtsprechung auf Anschlussinhaber ausweiten, wäre § 7 Abs.4 TMG europarechtlich nicht notwendig, da dieselben Rechtsfolgen – wenn auch dogmatisch bedenklich – über § 1004 BGB erzeugt werden können.

eingeht und entsprechende Unterscheidungen trifft.[201] Dabei sollte er auch klären, wie sich das Europarecht zum Subsidiaritätskriterium verhält.[202]

Zuletzt sollte er auch klären, ob für die nicht-kommerziell veranlasste Anschlussteilung, die zwar in den Anwendungsbereich von Art. 8 Abs.3 InfoSocRL fällt, nicht aber in den Anwendungsbereich der ECommerceRL[203], die gleichen Maßstäbe gelten wie für die kommerziell veranlasste Anschlussteilung.[204] Denkbar wäre eine „Spaltung“ dahingehend, dass die kommerziell veranlasste Anschlussteilung (sofern der Anschlussinhaber nicht schon als Täter haftet) einen Anspruch auf Netzsperren auslöst, während hingegen die nicht-kommerziell veranlasste Anschlussteilung (sofern der Anschlussinhaber nicht schon als Täter haftet) einen Anspruch auf Unterlassung der Rechtsverletzung auf Grundlage der Störerhaftung auslöst[205], wobei der alte Maßstab gilt, dass es erstens einem Anschlussinhaber grundsätzlich selbst überlassen ist, wie er die Wiederholung der Rechtsverletzung verhindert und zweitens – unter Weitergeltung der Standards aus „BearShare“[206] und „Silver Linings Playbook“[207] – der Anschlussinhaber nicht schon bei der ersten Rechtsverletzung über seinen Anschluss als Störer haftet, wenn diese auf volljährige Mitnutzer zurückzuführen ist.

Für private Anschlussinhaber, die kein offenes WLAN betreiben, wäre dies unter Umständen besser als die Haftung nach § 7 Abs.4 TMG, da die Störerhaftung nach dem aktuellen Stand der BGH-Rechtsprechung letztlich bei

[201] Wie in Kapitel § 4 VIII. d) und e) aufgezeigt, sind diese Unterschiede technisch bedingt, da bei *filesharing*-Verletzungen der Kreis der „eigentlichen“ Verletzer sehr weit ist, entsprechend also auch diejenigen Ziele, auf die sich mögliche Sperrmaßnahmen richten.

[202] Bisher ungeklärt, siehe *Grisse*, Internetangebotssperren, S. 102. Nach Auffassung des Verfassers ist das vom BGH und dem 3. TMGÄndG formulierte Subsidiaritätskriterium zulässig, siehe Kapitel § 4 VIII. 10.

[203] Siehe Kapitel § 4 VIII. 2. c).

[204] Der BGH hat mittlerweile eine Gleichstellung angenommen, siehe BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 19 – GRUR 2018, 1044 - „Dead Island“. Die Begründung allein über die ECommerceRL ist jedoch unzutreffend, da diese nur auf gewerbliche Anschlussinhaber Anwendung findet, siehe Kapitel § 2 IX.

[205] Indem private Anschlussinhaber aus dem Anwendungsbereich des § 7 Abs.4 iVm § 8 Abs.1 Satz 2 TMG herausgenommen werden. Vollständig sollten auch diese nicht aus dem TMG heraus genommen werden, insbesondere damit § 7 Abs.2 TMG und § 13 Abs.6 TMG nach wie vor auf diese Anwendung finden können.

[206] Siehe Kapitel § 2 IV. 3.

[207] Siehe Kapitel § 2 VII. 3.

erstmaligen Rechtsverletzungen kaum noch greift[208], während hingegen § 7 Abs.4 TMG erstens bereits bei einer erstmaligen Rechtsverletzung über einen Anschluss zur Anwendung gelangt und zweitens ein größeres Druckmittel zur Erlangung eines außergerichtlichen Vergleichs als die Störerhaftung sein kann[209], was insbesondere dann gilt, wenn der Gesetzgeber auch den Vorschlägen in dieser Arbeit zur Begrenzung des Unterlassungsstreitwertes[210] und der BGH den Vorschlägen zur richtigen Anwendung der Begrenzung der Abmahngebühren (für die Geltendmachung des Unterlassungsanspruchs)[211] folgen sollte.

VII. Berechnung des lizenzanalogen Schadens

Da die Lizenzanalogie gemäß § 97 Abs.2 Satz 2 UrhG eine Form der Schadensberechnung ist, gilt § 287 Abs.1 Satz 1 ZPO, sodass der Tatrichter die Schadensberechnung – wie die Beweiswürdigung nach § 286 ZPO auch – in freier Überzeugung vornehmen darf. Entsprechend ist gemäß BGH eine rechtliche Überprüfung der Berechnung „nur“ daraufhin zulässig, ob „*der Tatrichter Rechtsgrundsätze der Schadensbemessung verkannt, wesentliche Bemessungsfaktoren außer Acht gelassen oder seiner Schätzung unrichtige Maßstäbe zugrunde gelegt hat*“[212]. Es ist offenkundig, dass es sich hierbei nicht um eine allzu starke Einschränkung des Prüfungsumfangs handelt und der BGH die Schadensberechnung in Instanzurteilen faktisch vollständig nachprüfen kann.

Nach einer, von der *filesharing*-Rechtsprechung aus der allgemeinen BGH-Rechtsprechung zum Urheberrecht übernommenen, und auch überzeugenden Formel, ist die freie Überzeugung auf Grundlage dessen zu bilden, was vernünftige Lizenzvertragsparteien bei objektiver Betrachtung sinnvollerwei-

[208] Siehe Kapitel § 4 II. 2. c). Zu denken wäre an eine Störerhaftung regelmäßig dann nur noch, wenn dasselbe Recht über einen Anschluss mehr als einmal verletzt wird; doch dies kommt praktisch nie vor, siehe Kapitel § 3 VI. Die Störerhaftung bei einer erstmaligen Verletzungshandlung über einen Anschluss kommt fast nur noch bei einem nicht mittels Passwort gesichertem WLAN in Betracht, vgl. BGH, Urteil vom 26. Juli 2018, Az. I ZR 64/17, Rz. 24 – GRUR 2018, 1044 - „Dead Island“.

[209] Siehe Kapitel § 4 VIII. 11.

[210] Siehe Kapitel § 5 XIV.

[211] Siehe Kapitel § 5 XI.

[212] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 57 – GRUR 2016, 176 - „Tauschbörse I“.

se vereinbart hätten.[213] Da die Überzeugungsbildung möglichst nah an der Wirklichkeit orientiert sein soll[214], muss der Tatrichter im Rahmen der Berechnung der fiktiven Lizenz die Bemessungsfaktoren nachvollziehen, auf die sich die Parteien, hätten sie eine Lizenz ausgehandelt, gestützt hätten.

Denkbare Bemessungsfaktoren sind der Umfang der Verletzungshandlung (also welche Datenmengen an wie viele Personen übertragen werden), die wirtschaftliche Sensibilität (öffentliche Zugänglichmachung innerhalb des wirtschaftlich relevanten Verwertungszeitraums des Werkes[215]), die Qualität der öffentlich zugänglich gemachten Datei[216] sowie der (gesetzlich zulässige[217]) fiktive Kundenstamm.

Es erscheint plausibel, dass Parteien in einer fiktiven Lizenzverhandlung sich primär für den Umfang der Verbreitung der Datei interessieren, der Fokus also auch auf diesem Bemessungsfaktor liegen sollte.[218] Gerade der Umfang der Verbreitung ist jedoch zugleich der schwierigste Faktor, da sich nicht ermitteln lässt, wie viele Dateifragmente an wie viele andere Nutzer

213 LG Düsseldorf, Urteil vom 13. Januar 2016, Az. 12 S 22/15, Rz. 15 – juris, mit weiteren Nachweisen.

214 OLG Hamburg, Urteil vom 7. November 2013, Az. 5 U 222/10, Rz. 63 – juris, mit Nachweisen der Rechtsprechung des BGH.

215 Bei Computerspielen also beispielsweise die ersten Wochen nach Veröffentlichung, vgl. nur LG Stuttgart, Urteil vom 24. Februar 2017, Az. 24 0 360/16 – aw3p.de.

216 Bei Filmen und Musik beispielsweise sollte eine verminderte Qualität der getauschten Datei gegenüber der Originalversion schadensmindernd berücksichtigt werden, vgl. als Beispiel der Rechtsprechung aus dem Ausland Gericht der ersten Instanz in Fredrikstad, CRi 2007, 77. Bei Computerspielen könnte die verminderte Funktionalität der „Raubkopie", insbesondere ein fehlender Online-Mehrspielermodus, berücksichtigt werden.

217 Bestehen für das betroffene Werk straf- oder jugendschutzrechtliche Altersbegrenzungen, würde die Annahme, dass alle Empfänger der Datei das entsprechende Werk legal hätten beziehen können, voraussetzen, dass diese das entsprechenden Alter aufweisen. Das AG Düsseldorf hat daher beispielsweise in einem Fall, der Pornographie betraf, einen pauschalen Abschlag von 30 Prozent gemacht, siehe AG Düsseldorf, Urteil vom 20. Mai 2014, Az. 57 C 16445/13, Rz. 20 – juris.

218 Die in der Rechtsprechung hiergegen vorgebrachten Argumente sind zirkulär. Das LG Düsseldorf äußerte beispielsweise die Auffassung, dass wegen der technischen Ermittlungsschwierigkeiten der Umfang der Verbreitung irrelevant sei und stattdessen darauf abgestellt werden müsse, was vernünftige Lizenzvertragsparteien vereinbart hätten, siehe LG Düsseldorf, Urteil vom 13. Januar 2016, Az. 12 S 22/15, Rz. 15 – juris. Allerdings ist ja gerade fraglich, was vernünftige Vertragsparteien vereinbart hätten.

hochgeladen wurden.[219] Der BGH begnügte sich in „Tauschbörse I“ mit der Feststellung, dass die Annahme (des Berufungsgerichts) eines vollständigen Uploads an 400 andere Nutzer vertretbar ist.[220]; in Folge etablierte sich auf Instanzebene die sogenannte „Faktorrechtsprechung“, nach der der angemessene Schadensersatz regelmäßig zwischen dem 50-fachen bis zu 227-fachen des Verkaufspreises des Werks anzusetzen ist.[221]

Für diese Annahme kam dem BGH zu Gute, dass er – mangels tatsächlicher Feststellungen hierzu – ausklammern konnte, welche Auswirkungen die Geschwindigkeit üblicher Internetanschlüsse auf diese Annahme hat.[222] Abgesehen davon aber, dass die Überlegungen des BGH auf BitTorrent ohnehin nicht übertragbar sind, ist jegliche Schätzung von möglichen Zugriffszahlen auch unter Einbeziehung der Leistungsfähigkeit eines Anschluss vollkommen willkürlich. Instanzgerichte hatten sich daher mit der Annahme beholfen, dass nicht entscheidend ist, auf wie viele Personen sich die hochgeladenen Dateifragmente verteilen, sondern allein, wie viele Dateifragmente insgesamt hochgeladen werden, was richtigerweise nur von der Geschwindigkeit des Internetanschlusses und nicht der Zahl der Empfänger von Fragmenten abhängt.[223] Die Schätzung der hochgeladenen Menge basierte implizit wiederum auf der – wohl zutreffenden[224] – Prämisse, dass der typische Nutzer einer (BitTorrent)-Tauschbörse sich ausklinkt, sobald er die Zieldatei vollständig heruntergeladen hat.[225] Da die Uploadgeschwindigkeit eines durchschnittlichen Internetanschlusses nur einen Bruchteil der Downloadgeschwindigkeit beträgt, lädt der Nutzer also während seiner Teilnahme an einer Tauschbörse

[219] Siehe Kapitel § 1 IV. 7. c) dd).

[220] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 60f. – GRUR 2016, 176 - „Tauschbörse I“.

[221] Siehe Nachweise bei *Lütke*, GRUR-RR 2020, 337, 340.

[222] BGH, Urteil vom 11. Juni 2015, Az. I ZR 19/14, Rz. 62 – GRUR 2016, 176 - „Tauschbörse I“.

[223] AG Düsseldorf, Urteil vom 20. Mai 2014, Az. 57 C 16445/13 – juris sowie AG Stuttgart-Bad Cannstatt, Urteil vom 13. Oktober 2015, Az. 8 C 1023/15 – juris.

[224] *Chiu/Chou*, International Journal of Business and Management, Bd. 6, 2011, S. 68, 75.

[225] Irrelevant ist daher die Annahme zum Beispiel des LG Frankenthal, dass für die Schadensberechnung nach Dateigröße zu differenzieren sei, also beispielsweise bei Computerspielen eine andere Schadensschätzung vorzunehmen sei als bei Musiktiteln, vgl. LG Frankenthal, Urteil vom 12. März 2019, Az. 6 O 313/18, Rz. 47 – juris. Denn die hochgeladene Menge an Dateifragmenten bleibt relativ zur heruntergeladenen Menge stets gering, unabhängig von der Gesamtgröße der Datei.

auch nur einen Bruchteil der Gesamtdatei in diese hoch. Ausgehend hiervon teilt das AG Düsseldorf die so ermittelte Gesamtmenge auf die Größe eines *piece*[226] auf und geht sodann – technisch unzutreffend – davon aus, dass jedes *piece* an einen unterschiedlichen Nutzer weitergegeben wird; auf Grund der Weitergabe eines *piece* an diese Nutzer sei in Bezug auf den vollständigen Download jedenfalls bei *diesen* Nutzern Mittäterschaft anzunehmen. Der Preis für einen legalen Online-Download sei dann mit der Zahl dieser Nutzer zu multiplizieren und sodann – wegen des allgemeinen Beitrags zur Aufrechterhaltung des Schwarms – noch zu verdoppeln (im konkreten Fall also EUR 6, 28 mal 14 mal zwei, insgesamt EUR 175, 84).[227]

Besser – weil auf technisch zutreffenden Annahmen basierend – ist demgegenüber der Lösungsweg des AG Stuttgart-Bad Cannstatt: statt eine hypothetische Verteilung der hochgeladenen Dateifragmente auf eine bestimmte Anzahl von Personen anzunehmen, sind in die Schadensberechnung stattdessen zunächst das Hochladen der Dateifragmente und sodann die Weiterverbreitung dieser Dateipakte an andere Nutzer, und die Weiterverbreitung von Letzteren wiederum an andere Nutzer usw. einzubeziehen.[228] Die Zurechnung der Weiterverbreitung durch andere Nutzer weiter hinten in der Kette erfordert rechtlich nicht die Annahme der Mittäterschaft, sondern gelingt durch Anwendung des hergebrachten schadensrechtlichen Grundsatzes, dass sich nach einem schädigenden Ereignis kausal auf dieses zurückführbare Schadensvergrößerungen dem Schädiger auch dann zurechnen lassen, wenn sie durch das (vorsätzliche) Eingreifen Dritter entstehen.[229] Was sich zunächst nach einer ausufernden Haftung anhört, ist tatsächlich keine: da der vom Schädiger hochgeladene Bruchteil der Datei von anderen Nutzern ebenfalls nur mit deren Uploadgeschwindigkeit, also einem Bruchteil deren Downloadgeschwindigkeit, weiterverbreitet werden kann und selbiges wiederum für Nutzer an dritter Stelle in dieser Kette gilt, also an zweiter Stelle nur ein Bruchteil des ersten Bruchteils weitergegeben wird und an dritter Stelle nur ein Bruchteil des letzteren Bruchteils usw., verliert die Weitergabe an späte-

[226] Siehe hierzu Kapitel § 1 II. 5. b).

[227] AG Düsseldorf, Urteil vom 20. Mai 2014, Az. 57 C 16445/13, Rz. 13ff. – juris.

[228] AG Stuttgart-Bad Cannstatt, Urteil vom 13. Oktober 2015, Az. 8 C 1023/15, Rz. 29 – juris.

[229] AG Stuttgart-Bad Cannstatt, Urteil vom 13. Oktober 2015, Az. 8 C 1023/15, Rz. 39 – juris, mit Nachweisen der Rechtsprechung des BGH.

ren Stellen in der Kette mathematisch schnell an Bedeutung.[230] Insgesamt ist damit jedem Teilnehmer – auch bei Berücksichtigung der Weitergabe der von ihm hochgeladenen Dateifragmente durch deren Empfänger usw. – insgesamt nur die Weitergabe eines Bruchteils der Gesamtdatei vorwerfbar. Im streitgegenständlichen Fall nahm das AG Stuttgart-Bad Cannstatt mithin an, dass – ausgehend von einem Ladenpreis für eine DVD des streitgegenständlichen Films von EUR 14,99 – von dem beklagten Anschlussinhaber letztlich möglicherweise nur ein Schaden in Höhe EUR 2,04 verlangt werden könne.[231]

Die Lösungen der beiden Gerichte gehen jedoch von der fehlenden Mittäterschaft der Teilnehmer eines Schwarms aus, was dem gegenwärtigen Konzept des BGH widerspricht. Nach „Konferenz der Tiere“ muss sich also von der Betrachtung des Umfangs der Weiterverbreitung durch *einen* Nutzer gelöst und auf den gesamten Schwarm abgestellt werden. Im BitTorrent-System ist die Anzahl der Empfänger einer Datei und der Teilnehmer des Schwarms identisch.[232] Die Gesamtteilnehmerzahl eines Schwarms lässt sich nicht ermitteln, da nicht feststellbar ist, wie viele Nutzer sich über den Bestand des Schwarms hinweg ausklinken und wie viele neue sich einklinken.[233] Immerhin könnte ein Ermittlungsdienst aber die Größe des Schwarms festhalten, soweit sie ihm im jeweiligen Ermittlungszeitraum vom Tracker / den Trackern mitgeteilt wird. Auf Basis dieser Zahl könnte dann der Gesamtschaden näherungsweise geschätzt werden. Der Einzelpreis für das Werk[234] wäre dann mit ermittelten Schwarmgröße zu multiplizieren. Ist also als Werk beispielsweise ein Computerspiel betroffen, das regulär EUR 50 kostet, und beträgt

[230] AG Stuttgart-Bad Cannstatt, Urteil vom 13. Oktober 2015, Az. 8 C 1023/15, Rz. 41f. – juris

[231] AG Stuttgart-Bad Cannstatt, Urteil vom 13. Oktober 2015, Az. 8 C 1023/15, Rz. 39 – juris. Das Gericht musste sich nicht festlegen, da es schon eine täterschaftliche Haftung des Anschlussinhabers verneinte. Die Ausführungen zum Schadensersatz erfolgten *obiter dictum*.

[232] Ausgehend davon, dass alle Teilnehmer die Datei vollständig herunterladen und es keine *free rider* gibt.

[233] Rechtlich wären – der Lösung des BGH folgend – *alle* Nutzer, also auch die, die zu unterschiedlichen Zeitpunkten an einem Schwarm teilnehmen, als Mittäter anzusehen, siehe Kapitel § 4 II. 4. b) ee).

[234] Von diesem wäre jedoch ein bestimmter Abzug zu machen, da berücksichtigt werden muss, dass der Rechteinhaber durch das *filesharing*-System auch eigene Distributionskosten einspart.

die Schwarmgröße 1000 Nutzer, wäre der Gesamtschaden EUR 50.000, wobei dieser auf Grund der Annahme der Mittäterschaft von nur einem Nutzer verlangt werden kann – und dieser wiederum in diesem Fall die anderen Nutzer in Regress nehmen müsste, was praktisch nicht möglich ist.

Die in der Instanzrechtsprechung im Entstehen begriffene Auffassung, dass den klagenden Rechteinhaber eine sekundäre Darlegungslast darüber trifft, gegen welche Mitnutzer er bereits vorgegangen ist und wer diese sind[235], ist richtig, vermag aber das soeben geschilderte Problem kaum zu lösen. Regelmäßig wird er zwar gegen ein paar Nutzer bereits erfolgreich im Klagewege oder außergerichtlich vorgegangen sein[236]; solange diese Zahl noch niedrig ist, bleibt die Summe, die theoretisch von einem einzelnen Mittäter verlangt werden kann, noch hoch – und entsprechend auch das Drohpotential, um diesen zu einem Vergleich zu drängen, dessen Betrag dann wahrscheinlich wieder über der Summe liegt, die dem Tatbeitrag des Nutzers eigentlich entsprechen würde. Regress gegen die anderen Nutzer ist praktisch ausgeschlossen. Hat im obigen Beispiel der Rechteinhaber beispielsweise 100 Nutzer erfolgreich auf EUR 50 in Anspruch genommen, nimmt aber einen weiteren Nutzer auf EUR 45.000 in Anspruch, da die übrigen 899 nicht ermittelt werden konnten, müsste Nutzer Nr. 101 die genannten 100 Nutzer auf jeweils EUR 50 in Anspruch nehmen[237]. Die übrigen 899 Nutzer könnte er aber nicht in Regress nehmen. Selbst also wenn er in diesem Beispiel alle bekannten 100 Nutzer erfolgreich in Regress nehmen kann, bleibt er immer noch auf EUR 39.950 „sitzen“.

Es ist offenkundig, dass Abmahnkanzleien dieses realistische Szenario in ihren Abmahnungen schildern werden. Kaum ein Abgemahnter wird das in Aussicht gestellten Risiko in Kauf nehmen. Das ohnehin schon problemati-

235 Siehe Kapitel § 4 II. 4. b) gg).

236 Weitere Probleme ergeben sich, wenn ein Vergleich geschlossen wurde, da dann unklar ist, wie die Vergleichssumme, die höher oder niedriger als der Betrag sein wird, der von jedem Mitnutzer einzeln betrachtet zu tragen wäre, auf die Tatbeiträge der anderen Nutzer anzurechnen ist.

237 Wobei sich auch hier jeweils die Frage der Täterschaft stellen würde, wenn diese mit der Zahlung der EUR 50 nicht zugleich ihre (Mit)täterschaft, mithin also Teilnahme am Schwarm eingestanden haben. Theoretisch müssten diese dann verklagt und dann der Problemkreis „sekundäre Darlegungslast“ in jedem einzelnen Prozess durchexerziert werden.

sche Drohpotential von Abmahnungen[238] wird durch die mittäterschaftliche Lösung des BGH also noch potenziert.

Nach hiesiger Auffassung wäre gegenüber der – dogmatisch und in ihren rechtspolitischen Konsequenzen kritikwürdigen Lösung – des BGH die Lösung des AG Stuttgart-Bad Cannstatt zu bevorzugen gewesen, auch wenn diese nicht perfekt ist[239]; jedoch ist *de lege lata* keine bessere Lösung denkbar. Gegen das AG Stuttgart-Bad Canstatt kann nicht eingewendet werden, dass es einen Rechteinhaber letztlich schlechter stellt, als wenn sich alle Nutzer eines Schwarms das entsprechende Werk legal gekauft hätten. Dieser Einwand würde übersehen, dass Rechteinhaber bisher nur die öffentliche Zugänglichmachung geltend machen, nicht aber die Vervielfältigung. Die Vervielfältigung wäre über die Erfassung des *bitfield* nachweisbar[240]; notfalls könnte sie stattdessen auch mittels eines Anscheinsbeweises vermutet werden, wenn der Ermittlungsdienst in unmittelbarer Nähe zum Ermittlungszeitpunkt die Datei vollständig aus dem Schwarm herunterladen konnte. Im Ergebnis könnten Rechteinhaber gegenüber jedem Nutzer des Schwarms also eine Vervielfältigung[241] und eine öffentliche Zugänglichmachung eines Bruchteils des Werkes[242] geltend machen, sodass sie also von jedem Nutzer den Einzelpreis für ein Werk plus einem Bruchteil hiervon als Schaden geltend machen könnten.[243]

Dieses Ergebnis zeigt jedoch wiederum auf, dass *de lege lata* – auch abseits des BGH – keine befriedigende, unkomplizierte Lösung möglich ist. In der Literatur ist unabhängig hiervon *de lege ferenda* vorgeschlagen worden, einfach den Schadensbetrag, der von einer natürlichen Person für eine Urheberrechtsverletzung verlangt werden kann, mit einer niedrigen Summe zu pauschalisie-

238 Siehe Kapitel § 3 VIII.

239 Da auch sie mit einigen Annahmen in tatsächlicher und rechtlicher Hinsicht operieren muss (Annahme des vollständigen Downloads zur Berechnung des Bruchteils des Uploads; Annahme einer hochgeladenen Dateimenge; Annahme der urheberrechtlichen Schutzfähigkeit der hochgeladenen Fragmente).

240 Siehe Kapitel § 1 IV. 7. c) dd).

241 Wobei hier das Problem besteht, dass die Vervielfätigung nur in Mittäterschaft stattfindet, siehe Kapitel § 4 II. 3. Das Regressproblem ist aber wegen der geringen Schadenssumme für eine Vervielfältigung vernachlässigbar.

242 Dessen Schutzfähigkeit vorausgesetzt.

243 Juristisch betrachtet dürfte dies keine Überkompensation sein, da zwei unterschiedliche urheberrechtliche Nutzungshandlungen abgegolten werden. Wirtschaftlich liegt noch eine leichte Überkompensation vor, die jedoch hinnehmbar sein dürfte.

ren.[244] Das würde das Problem der Schadensberechnung umschiffen, jedoch ist höchst fraglich, ob die EnforcementRL, in der eine solche Pauschalisierung nicht vorgesehen ist, diese erlauben würde. Die Bundesregierung hat im Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs[245] die Auffassung geäußert, dass im Lichte der EnforcementRL eine Pauschalisierung des Schadensersatzanspruches auch private Urheberrechtsverletzer betreffend unzulässig sei.[246]

Zu bevorzugen, aber nach gegenwärtigem Stand unrealistisch, wäre eine europäische Lösung, die nicht nur die Teilnahme an einer Tauschbörse als eigene urheberrechtliche Verwertungshandlung einführt[247], sondern hierfür zugleich eine Pauschalisierung des Schadensersatzes vornimmt, die sich am Preis für einen regulären Download orientiert.

Vorerst allerdings wird man mit der Lösung des BGH leben müssen. Eine denkbare Abmilderung der durch dessen Rechtsprechung verursachten Probleme wäre es, *de lege ferenda* ins Urheberrecht für natürliche, nichtgewerblich handelnde Personen eine Ausnahme von § 421 BGB einzuführen, die vorsieht, dass von jedem Mittäter nur ein Betrag verlangt werden kann, der dessen mittäterschaftlichen Beitrag widerspiegelt, nicht jedoch der von allen Mittätern zusammen verursachte Gesamtschaden.

VIII. Schnellere Verjährung

Insbesondere für Privatpersonen kann es eine psychische Belastung sein, wenn nach Jahren eine vergessen geglaubte Abmahnung (bzw. die dort geltend gemachten Forderungen gegen sie) wieder „ausgegraben“ wird.[248] Wie in Kapitel § 3 XI. 1. aufgezeigt, ist es nicht unüblich, dass Abmahnkanzleien die Verjährungsfristen maximal ausreizen. Zwar sollte der Zeitablauf im Rahmen der sekundären Darlegungslast zu Lasten der Rechteinhaber gehen[249],

[244] *Hofmann*, GRUR-Prax 2017, 20. In anderen Rechtsordnungen ist dies durchaus üblich, zum Beispiel in Kanada. Siehe dort Sec. 38.1 Abs.1 lit. b) Copyright Act (R.S.C., 1985, c. C-42).

[245] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_fairen_Wettbewerbs.html - Zugriff am 31.03.2021.

[246] Seite 14 des Regierungsentwurfs eines Gesetzes zur Stärkung des fairen Wettbewerbs.

[247] Siehe Kapitel § 5 II. 1.

[248] Der Verfasser kennt aus eigener Praxis solche Fälle.

[249] Siehe hierzu Kapitel § 5 V. 3. c).

jedoch ist nicht gesichert, dass der BGH dies ebenso sehen wird. In jedem Fall wäre es wünschenswert, dass Rechteinhaber gezwungen sind, gegen Privatpersonen eine schnelle Klärung der Rechtslage herbeizuführen. In § 102 Satz 1 UrhG sollte daher abweichend von § 195 BGB geregelt werden, dass Ansprüche aus § 97 UrhG – in Anlehnung an § 11 Abs.1 UWG – nach sechs Monaten verjähren, soweit sie gegen nicht-gewerblich handelnde, natürliche Personen gerichtet sind, wobei für den Verjährungsbeginn die Kenntnis (oder die fahrlässige Unkenntnis) der den Anspruch begründenden Tatsachen maßgeblich ist.[250] Gleichfalls sollten nicht-gewerblich handelnde, natürliche Personen aus dem Anwendungsbereich des § 102 Satz 2 UrhG heraus genommen werden, damit die sechsmonatige Verjährungsfrist nicht durch die zehnjährige Verjährungsfrist des Restschadensersatzanspruches konterkariert wird. Des Weiteren sollte auch in § 7 TMG eine sechsmonatige Verjährungsfrist für den Anspruch aus § 7 Abs.4 TMG statuiert werden, damit die möglichen Ansprüche gegen private Anschlussinhaber hinsichtlich ihrer Verjährung synchronisiert sind.

Dem Rechtsgedanken des Art. 169 EGBGB folgend würde die Verjährungsfrist auch für Schuldverhältnisse gelten, die vor dem Inkrafttreten der vorgeschlagenen Regelungen entstanden sind, bei denen also die Verletzungshandlung vor dem Inkrafttreten der vorgeschlagenen Regelungen begangen wurde. Die Ansprüche aus diesen Schuldverhältnissen würden also sechs Monate nach dem Inkrafttreten der vorgeschlagenen Regelungen verjähren.

IX. Erhöhung der Anforderungen an den Inhalt von Abmahnungen

Die in § 97a Abs.2 UrhG vorgeschriebenen Inhalte einer Abmahnung sind nicht ausreichend. Ein wichtiger rechtspolitischer Kritikpunkt an der gegenwärtigen Rechtslage ist die Möglichkeit abmahnender Rechteinhaber, durch selektives Zitieren der Rechtsprechung zwar kein falsches, jedoch ein unvollständiges Lagebild zu zeichnen und somit Abgemahnten die Aussichtslosigkeit einer Rechtsverteidigung zu suggerieren.[251] Da Abmahnungen, die diese Informationen nicht enthalten, nicht gemäß § 242 BGB rechtsmissbräuch-

[250] Verjährungsbeginn ist daher das Datum der Auskunftserteilung durch den ISP bzw. das Eingangsdatum der Auskunftserteilung beim Rechteinhaber.

[251] Siehe Kapitel § 3 VIII.

lich sind[252], sollte § 97a Abs.2 Satz 1 UrhG *de lege ferenda* um eine Nr. 5 erweitert werden, in der als weiterer, zwingender Inhalt der Abmahnung eine zusammenfassende, vollständige Darstellung der gegenwärtigen Rechtslage (also Gesetze und höchstgerichtliche Rechtsprechung) vorgeschrieben wird.[253] Insbesondere müssten nach gegenwärtigen Stand dann auch die Urteile „Afterlife“[254] und „Ego-Shooter-Spiel“[255] aufgeführt werden, auch wenn diese beim konkret Abgemahnten nicht einschlägig sind bzw. werden.

Streiten ließe sich über die Zumutbarkeit einer solchen Regelung, da sie nicht nur *filesharing*-Fälle betreffen würde; schließlich gilt § 97a UrhG für das gesamte Urheberrecht. Vorsichtshalber sollte sie daher dem Wortlaut nach auf Abmahnungen gegen Privatpersonen (entsprechend § 97a Abs.3 Satz 2 Nr.1 UrhG) beschränkt werden. Mit dieser Beschränkung wäre sie jedenfalls zumutbar, da von ihr praktisch dann fast ausschließlich *filesharing*-Abmahnungen betroffen wären[256] und diese wiederum fast ausschließlich von hierauf spezialisierten Kanzleien versandt werden[257].

Die hier vorgeschlagene Regelung dürfte mit Art. 12 GG vereinbar sein, auch wenn Rechtsanwälte damit dazu gezwungen werden, einer gegnerischen Partei eine Form von Rechtsberatung zu erteilen. Denn Rechtsanwälte sind nicht nur einseitige Parteivertreter, sondern gemäß § 1 BRAO auch Organe der Rechtspflege.[258] Die vorgeschlagene Einschränkung greift also in die Berufsfreiheit ein, ist aber noch verhältnismäßig.

X. Zur Pflicht zur Beantwortung von Abmahnungen

Wie oben in Kapitel § 4 XI. 1. dargestellt, hat der BGH in der Entscheidung „Saints Row“ eine Antwortpflicht auf Abmahnungen in *filesharing*-Konstellationen abgelehnt, d.h. der Umstand, dass der dort beklagte An-

252 Siehe Kapitel § 4 XI.

253 Sofern zu höchstrichterlich nicht entschiedenen Rechtsfragen einschlägige Instanzrechtsprechung zitiert wird, sollte auch hier das Verbot selektiven Zitierens gelten.

254 Siehe Kapitel § 2 XI. 1.

255 Siehe Kapitel § 2 XI. 4.

256 Siehe Kapitel § 3 IV.

257 Siehe Kapitel § 3 V. 5.

258 Vgl. BVerfG, Beschluss vom 12. Dezember 2006, Az. 1 BvR 2576/04, Rz. 25 – bverfg.de.

schlussinhaber den wahren Täter erst im Prozess mitgeteilt hatte, führte nicht zu einem materiellen Anspruch des Rechteinhabers auf Erstattung der Kosten des auf Grund dessen verlorenen Prozesses. Diesem Urteil lag aber die instanzgerichtliche Feststellung zu Grunde, dass der Anschlussinhaber weder als Täter noch als Störer hafte[259], sodass der BGH offen lassen konnte, ob die Haftung nach § 97 UrhG als gesetzliches Schuldverhältnis eine Antwortpflicht über § 241 Abs.2 BGB als Nebenpflicht enthält sowie, ob ein Anspruch aus Geschäftsführung ohne Auftrag dem Grunde nach gegeben ist.[260]

Folglich stellt sich die Frage, wie die Rechtslage ist, wenn eine gesetzliche Sonderverbindung besteht; relevant ist dabei allein der Anspruch aus § 7 Abs.4 TMG[261], da nach der aktuellen Rechtsprechung des BGH eine Störerhaftung des Anschlussinhabers regelmäßig nicht mehr in Betracht kommt[262] und bei einer Haftung des Anschlussinhabers als Täter sich die Frage nach dem wahren Täter nicht mehr stellt, auch wenn die Haftung des Anschlussinhabers lediglich prozessual fingiert ist.

Richtigerweise kann bei Bestehen des Anspruches aus § 7 Abs.4 TMG eine Antwortpflicht aus § 241 Abs.2 BGB angenommen werden; ein Kostenerstattungsanspruch über die Geschäftsführung ohne Auftrag kommt allerdings nicht in Betracht:

1. Nebenpflicht des Schuldverhältnisses aus § 7 Abs.4 TMG

Richtigerweise kann für den Anschlussinhaber vorgerichtlich eine Pflicht (als Nebenpflicht zum Anspruch aus § 7 Abs.4 TMG), den wahren Täter zu ermitteln und/oder mitzuteilen bestehen, sodass der BGH – sollte er hierüber anknüpfend an „Saints Row“ zu befinden haben – entsprechend entscheiden sollte.

Grund hierfür ist, dass § 241 Abs.2 BGB nach den vom BGH entwickelten Fallgruppen Aufklärungs- und Mitteilungspflichten des Schuldners auslösen

[259] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 43 – juris - „Saints Row“.

[260] BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 45ff., 61ff. – juris - „Saints Row“.

[261] Vom BGH lediglich andeutet in BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 52 – juris - „Saints Row“.

[262] Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 51f. – juris - „Saints Row“ sowie Kapitel § 2 XI. 6.

kann, solange diese (wie andere Nebenpflichten des § 241 Abs.2 BGB auch) hauptleistungsbezogen sind[263], was sich auch aus dem Wortlaut von § 241 Abs.2 BGB („[...] nach seinem Inhalt[...]“) ergibt.

Vorgerichtliche Aufklärungs- und Mitteilungspflichten nach § 241 Abs.2 BGB aus dem aus § 7 Abs.4 TMG entstehenden gesetzlichen Schuldverhältnis müssen mithin auf dessen Inhalt bezogen sein; beispielsweise können diese beinhalten, dass der Anschlussinhaber dem Rechteinhaber seine technischen Fähigkeiten und den Typ seines Routers mitteilt[264], sodass der Rechteinhaber besser einschätzen kann, was er gerichtlich von dem Anschlussinhaber im Rahmen von § 7 Abs.4 TMG verlangen kann.

Nach der in dieser Arbeit vertretenen Auffassung[265] ist die Haftung des Anschlussinhabers nach § 7 Abs.4 TMG aber subsidiär zur Haftung des wahren Täters, sodass dessen Ermittlung und Mitteilung hauptleistungsbezogen ist, da der Bestand der Hauptleistungspflicht hiervon abhängt.

Folgt man dieser Auffassung nicht, kann die vorgerichtliche Aufklärungs- und Mitteilungspflicht im Rahmen von § 7 Abs.4 TMG aber nicht dazu führen, dass der Anschlussinhaber dem Rechteinhaber Umstände mitteilen muss, die zur Begründung einer neuen Hauptleistungspflicht, nämlich einer täterschaftlichen Haftung nach § 97 UrhG eines Dritten, führen, da dies dann keinerlei Auswirkungen auf den Inhalt des Anspruchs nach § 7 Abs.4 TMG hätte, Auskunft und Mitteilung also nicht hauptleistungsbezogen wären.

Nimmt man vor dem Hintergrund des Vorgesagten eine vorgerichtliche Aufklärungs- und Mitteilungspflicht – und in Folge eine Pflicht zur Beantwortung der Abmahnung – an, so verbleibt für einen etwaigen Schadensersatzanspruch jedoch immer noch das Kausalitätsproblem.[266]

Was den Inhalt der Antwortpflicht anbelangt, so liegt nahe, einen Gleichlauf mit der sekundären Darlegungslast im Prozess herzustellen.

---

[263] Siehe *Sutschet* in: Hau/Poseck, BeckOK BGB, 57. Ed. 2021, § 241 BGB, Rz. 77ff.

[264] Siehe hierzu entsprechend zur sekundären Darlegungslast in einem Prozess Kapitel § 4 VIII. 4. a).

[265] Siehe Kapitel § 4 VIII. 3. d) bb).

[266] Siehe hierzu Kapitel § 4 XII. 1. c).

2. Geschäftsführung ohne Auftrag (§§ 677ff. BGB)

Die Anwendbarkeit der Regeln der Geschäftsführung ohne Auftrag (§ 677ff. BGB) sollte in *filesharing*-Konstellationen bereits deswegen ausscheiden, weil § 97a UrhG bezüglich Abmahnungen im Urheberrecht *lex specialis* gegenüber §§ 677ff. BGB ist.[267] Denn § 97a Abs.3 UrhG knüpft den Erstattungsanspruch an die Voraussetzungen des § 97a Abs.2 UrhG betreffend den Inhalt von Abmahnungen, die über einen Erstattungsanspruch auch nach der Geschäftsführung ohne Auftrag unterlaufen werden könnten.[268] Die vom BGH angedachte Anwendbarkeit der §§ 677ff. BGB für den Fall, in dem die Voraussetzungen des § 97a UrhG im Übrigen beachtet werden[269], dürfte zu einer methodisch unzulässigen Normderogation des § 97a UrhG führen.[270]

Selbst aber, wenn man die §§ 677ff. BGB neben § 97a BGB für anwendbar halten wollte, würde richtigerweise ein Schadensersatzanspruch ausscheiden. Gemäß § 683 BGB kann der Geschäftsführer lediglich Ersatz für seine Aufwendungen erhalten[271], *e contrario* daher nicht für seine Schäden. Die Rechtsprechung hat parallel zum Auftragsrecht im Wege der Rechtsfortbildung einen Schadensersatzanspruch über § 683 BGB iVm § 670 BGB analog lediglich für *geschäftsbesorgungsimmanente* Schäden anerkannt, also solche Schäden, die im Zusammenhang mit der Geschäftsführung stehen.[272] In den vorliegend betrachteten Konstellationen tritt der Schaden erst ein, wenn der klagende Rechteinhaber den Prozess verliert und hierauf von der entsprechenden Kostenfolge getroffen wird; die Geschäftsführung ist hingegen in der Abmahnung, nicht in der Prozessführung gegen den Anschlussinhaber zu sehen, da nur Erstere dem fingierten Interesse des Abgemahnten entsprechen kann (da der Anschlussinhaber gerade an einer Verhinderung eines Prozesses gegen sich interessiert ist). Folglich stellt die negative Kostenfolge auch

---

267 Vgl. *Specht* in: Dreier/Schulze/Specht, UrhG, 6. Aufl. 2018, § 97a UrhG, Rz. 12. aA *Röß*, NJW 2019, 1983, 1984. Offen gelassen von BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 65 – juris - „Saints Row".

268 Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 66f. – juris - „Saints Row".

269 Vgl. BGH, Urteil vom 17. Dezember 2020, Az. I ZR 228/19, Rz. 67 – juris - „Saints Row".

270 Vgl. hierzu auch *Hofmann*, GRUR-Prax 2020, 355, 356.

271 Die Prozesskosten sind aber keine Aufwendung für die Abmahnung.

272 *Schäfer* in: Säcker et al., MüKo-BGB, 8. Aufl. 2020, § 683 BGB, Rz. 38.

keinen geschäftsbesorgungsimmanenten Schaden dar.[273]

Im Übrigen würde auch bei Annahme eines Anspruchs aus Geschäftsführung ohne Auftrag die Kausalitätsproblematik verbleiben.[274]

XI. Richtige Anwendung des § 97a Abs.3 UrhG n.F.

Wie in Kapitel § 4 X. 2. ausgeführt, scheint das Auslegungsergebnis bei § 97a Abs.3 UrhG n.F. gegenüber § 97a Abs.2 UrhG a.F. eindeutiger zu sein, d.h. die Gebührenbegrenzung sollte in *filesharing*-Fällen immer Anwendung finden. Jedoch hat der Gesetzgeber mit § 97a Abs.3 Satz 4 UrhG n.F. ein „Schlupfloch" gelassen, das nun auch bereits vereinzelt von Instanzgerichten genutzt wird, um die Gebührenbegrenzung in *filesharing*-Fällen nicht anwenden zu müssen.[275]

Methodischer Hebel ist dabei – sofern nicht besondere Umstände des Einzelfalls Unbilligkeit begründen können[276] – eine europarechtskonforme Auslegung, derzufolge gemäß Art. 14 EnforcementRL eine Gebührenbeschränkung stets unzulässig sei.[277] Dogmatisch ist diese Vorgehensweise *prima facie* zulässig, da eine solche Ausdehnung der Unbilligkeitsklausel nicht gegen deren Wortlaut oder den Wortlaut des § 97a Abs.3 UrhG im Übrigen verstößt. Folglich ist auch irrelevant, ob die Gesetzesbegründung einen anderen Anwendungsbereich der Unbilligkeitsklausel nahelegt.

Strittig ist allerdings schon, ob Abmahngebühren nach § 97a UrhG in den Anwendungsbereich des Art. 14 EnforcementRL fallen, da sie zumindest „*sonstige Kosten*" im Sinne dieser Norm sein müssten. Der EuGH hat diesen unbestimmten Wortlaut in brauchbarer Weise dadurch eingegrenzt, dass er

[273] Dieser Punkt wird von *Röß* übersehen, vgl. *Röß*, NJW 2019, 1983, 1985.

[274] Siehe hierzu Kapitel § 4 XII. 1. c).

[275] Beispielsweise LG Stuttgart, Urteil vom 9. Mai 2018, Az. 24 O 28/18, Rz. 45 – juris. Weitere Beispiele siehe *Rathsack*, jurisPR-ITR 14/2018, Anm. 6.

[276] Siehe als Beispiel hierfür AG Düsseldorf, Urteil vom 6. Dezember 2017, Az. 10 C 101/17 – ZUM 2018, 739: Veröffentlichung des betroffenen Werkes ist erst kurze Zeit vor der Verletzungshandlung erfolgt; mehrere Verletzungshandlungen ermittelt. Ähnlich AG München, Urteil vom 6. April 2018, Az. 158 C 13140/17 – ZUM 2018, 742 sowie AG Düsseldorf, Urteil vom 7. August 2018, Az. 13 C 72/18, Rz. 34 – BeckRS 2018, 18535.

[277] LG Stuttgart, Urteil vom 09. Mai 2018, Az. 24 O 28/18, Rz. 45 – juris.

als „*sonstige Kosten*“ – wegen des prozessualen Kontextes der Norm („*obsiegende Partei*“) – nur solche Kosten ansieht, die unmittelbar und eng mit dem betreffenden Gerichtsverfahren zusammenhängen.[278]

Die Gebührenbegrenzung betrifft jedoch nur den Unterlassungsanspruch, der regelmäßig nicht gerichtlich geltend gemacht wird.[279] In diesen Fällen besteht dann richtigerweise ein Zusammenhang zwischen den außergerichtlichen Abmahnkosten die Unterlassung betreffend mit dem nachfolgenden Gerichtsverfahren nicht.[280]

Würde man dem nicht folgen, stünde Art. 14 EnforcementRL allerdings einer Pauschalierung wie in § 97 Abs.3 Satz 2 UrhG entgegen. Pauschalierungen sind nach Art. 14 EnforcementRL nicht generell unzulässig.[281] Jedoch hat der EuGH auch entschieden, dass Pauschalierungen, die Rechteinhabern letztlich einen Erstattungsanspruch einräumen, der weit niedriger als ein solcher ist, der ohne die Pauschalierung bestünde, unzulässig sind.[282] Dies trifft auf § 97a Abs.3 Satz 2 UrhG zu, da ohne diese Norm wegen der Möglichkeit der freien Streitwertschätzung weit höhere Gebühren verlangt werden könnten. Nicht argumentiert werden kann, dass § 97a Abs.3 Satz 2 UrhG zugleich das Ermessen des Rechtsanwalts dahingehend binde, welchen Streitwert er der Gebührenrechnung gegenüber seinem Mandanten (also dem Rechteinhaber) zu Grunde legt und somit schon von vornherein kein höherer Anspruch gegen den Abgemahnten in Betracht kommt, weil der Anspruch bereits im Innenverhältnis von Rechtsanwalt und Rechteinhaber begrenzt sei.[283] Tatsächlich lässt sich weder § 97a Abs.3 Satz 2 UrhG noch der zugehörigen Gesetzes-

[278] EuGH, Urteil vom 28. Juli 2016, Rs. C-57/15, Rz. 36 – ECLI:EU:C:2016:611 - „United Video Properties“.

[279] Siehe Kapitel § 3 VI. Eine Geltendmachung ist aber trotz § 7 Abs.4 TMG nach wie vor nicht ausgeschlossen, da eine täterschaftliche Haftung auf Unterlassung weiterhin möglich ist, siehe Kapitel § 4 VIII. 4.

[280] AG Frankenthal, Urteil vom 5. Juli 2018, Az. 3a C 73/18, Rz. 41 – juris. Für einen Zusammenhang in den Fällen, in denen der Unterlassungsanspruch noch geltend gemacht werden kann *Kiersch*, ZUM 2018, 667, 669.

[281] EuGH, Urteil vom 28. Juli 2016, Rs. C-57/15, Rz. 25 – ECLI:EU:C:2016:611 - „United Video Properties“.

[282] EuGH, Urteil vom 28. Juli 2016, Rs. C-57/15, Rz. 26 – ECLI:EU:C:2016:611 - „United Video Properties“. Der EuGH macht diese Überlegung an dem Zumutbarkeitskriterium in Art. 14 EnforcementRL fest, richtig wäre es jedoch, auf das Angemessenheitskriterium abzustellen.

[283] So aber AG Frankenthal, Urteil vom 5. Juli 2018, Az. 3a C 73/18, Rz. 41 – juris.

begründung irgendein Argument für diese Ansicht entnehmen; § 97a Abs.3 Satz 2 UrhG ist seinem Wortlaut nach auf das Verhältnis Rechteinhaber - Abgemahnter beschränkt. Zuletzt enthält Art. 14 EnforcementRL zwar noch ein Billigkeitskriterium; dieses deckt jedoch das Regel-Ausnahme-Verhältnis in § 97a Abs.3 UrhG nicht, da nach Art. 14 EnforcementRL nur im Einzelfall eine Kostendeckelung zulässig ist, nicht jedoch eine generelle Kostendeckelung wie in § 97a Abs.3 Satz 2 UrhG, die mit § 97a Abs.3 Satz 4 UrhG nur im Einzelfall durchbrochen werden kann.[284]

Im Ergebnis ist nach hiesiger Auffassung Art. 14 EnforcementRL bezüglich § 97a Abs.3 UrhG jedenfalls, wie dargestellt, in den Fällen, in denen kein Unterlassungsanspruch geltend gemacht wird, schon gar nicht einschlägig.

Jedoch ist der gesamte, soeben dargestellte Fragenkomplex gegenwärtig Gegenstand eines Vorlageverfahrens zum EuGH.[285] Die weiteren Entwicklungen sind daher abzuwarten.

XII. Sekundäre Darlegungslast betreffend die für die Abmahnung geleisteten Gebühren

In der Vergangenheit sind Fälle bekannt geworden, in denen abmahnende Kanzleien gegenüber Abgemahnten höhere Gebühren geltend gemacht ha-

[284] Vgl. EuGH, Urteil vom 28. Juli 2016, Rs. C-57/15, Rz. 31 – ECLI:EU:C:2016:611 - „United Video Properties“. aA allerdings OLG Celle, Beschluss vom 12. April 2019, Az. 13 W 7/19, Rz. 22 – MMR 2019, 450 und AG Frankenthal, Urteil vom 5. Juli 2018, Az. 3a C 73/18, Rz. 41 – juris sowie *Kiersch*, ZUM 2018, 667, 670ff. Nach OLG Frankfurt a.M., Urteil vom 31. März 2020, Az. 11 U 44/19, Rz. 64ff. – GRUR-RS 2020, 4852 soll § 97a Abs.3 UrhG zudem gar keine Umkehr eines Regel-Ausnahme-Verhältnisses darstellen, sondern lediglich eine Typisierung für bestimmte Fallgruppen (also *filesharing*), die die Abmahnkosten im übrigen Urheberrecht unberührt lässt. Zwischen diesen Auffassungen, mit Verweis auf EuGH, Urteil vom 28. Juli 2016, Rs. C-57/15, Rz. 32 – ECLI:EU:C:2016:611 - „United Video Properties“, *König*, ZUM-RD 2019, 452, 453, demzufolge Art. 14 EnforcementRL einer pauschalen Kostendeckelung nur dann entgegensteht, wenn der Pauschalbetrag im konkreten Fall hinter dem nichtpauschalierten Betrag zurückfällt.

[285] LG Saarbrücken, EuGH-Vorlage vom 21. Oktober 2019, Az. 7 S 2/19 – juris. Zudem wird dort ergänzend gefragt, ob die Abmahnkosten betreffend den Unterlassungsanspruch auch als Schadensersatz im Sinne des Art. 13 EnforcementRL angesehen werden können.

ben als der sie beauftragende Rechteinhaber an sie leisten musste.[286] Der BGH erachtet es dennoch als Bestreiten ins Blaue hinein, wenn Abgemahnte bestreiten, dass die ihnen gegenüber geltend gemachten Gebühren tatsächlich in der geltend gemachten Höhe angefallen sind.[287] Da der BGH seine Rechtsprechung in diesem Punkt wohl nicht ändern wird, ist eine gesetzliche Regelung vonnöten. Diese könnte in § 97a UrhG untergebracht werden und ausdrücklich statuieren, dass im Falle des Bestreitens der Rechteinhaber die Gebührenvereinbarung mit dem Rechteinhaber (gegebenenfalls in geschäftlich empfindlichen Bereichen geschwärzt) vorlegen muss. Eine solche ausdrückliche Regelung wäre zwar für das deutsche Recht eher untypisch, scheint aber in Anbetracht der Tatsache, dass Abgemahnte andernfalls Opfer eines Betruges werden können, und der BGH dies nicht berücksichtigt hat, gerechtfertigt.

XIII. Erstattungsanspruch des Anschlussinhabers

Wie in Kapitel § 4 X. 2. ausgeführt, ist der Gebührenerstattungsanspruch im Falle unberechtigter Abmahnungen gemäß § 97a Abs.4 Satz 1 UrhG zahnlos, da er nur dann greift, wenn für den Abmahnenden die fehlende Berechtigung der Abmahnung nicht erkennbar war, was praktisch nie der Fall ist, da der Abmahnende zum Zeitpunkt der Abmahnung nicht weiß, wie die Anschlussnutzungssituation beim Abgemahnten ist. Ein Erstattungsanspruch auf anderer Rechtsgrundlage[288] scheidet also aus, solange dem Abmahnenden keine Mutwilligkeit vorzuwerfen ist[289] – was bei *filesharing*-Abmahnungen jedoch regelmäßig nicht der Fall ist. In § 97a Abs.4 Satz 1 UrhG sollte daher der Halbsatz „*es sei denn, es war für den Abmahnenden zum Zeitpunkt der Abmahnung nicht erkennbar, dass die Abmahnung unberechtigt war*“ gestrichen werden, sodass abgemahnte Anschlussinhaber außergerichtliche Rechtsan-

[286] Siehe Kapitel § 3 VI.

[287] Siehe hierzu Kapitel § 4 X. 2.

[288] Zur Rechtslage außerhalb des Anwendungsbereichs des § 97a UrhG siehe BGH, Beschluss vom 15. Juli 2005, Az. GSZ 1/04 – GRUR 2005, 882 sowie BGH, Urteil vom 12. Dezember 2006, Az. VI ZR 224/05 – NJW 2007, 1458.

[289] Bei den *RedTube*-Abmahnungen wurde daher den Abgemahnten vereinzelt ein Anspruch auf Ersatz ihrer außergerichtlichen Rechtsanwaltskosten für die Abwehr der in der Abmahnung geltend gemachten Ansprüche aus § 826 BGB zugebilligt, siehe beispielsweise AG Regensburg, Urteil vom 8. Dezember 2015, Az. 3 C 451/14, Rz. 62ff. – juris.

waltskosten immer verlangen können, wenn sich die Abmahnung als unberechtigt herausstellt (was also typischerweise dann der Fall ist, wenn der Rechteinhaber klagt, der Anschlussinhaber jedoch nicht als Täter haftet). Dies würde Rechteinhaber dazu anhalten, sich statt dem harten Druckmittel Abmahnung häufiger der milderen Berechtigungsanfrage zu bedienen.[290]

XIV. Streitwertbegrenzung

Der Streitwert für die Geltendmachung des Schadensersatzanspruches sowie für die Geltendmachung von Abmahngebühren für die vorgerichtliche Geltendmachung des Schadensersatzanspruches richtet sich – wie im deutschen Recht üblich – nach der Höhe des geltend gemachten Anspruches, sodass hier nichts zu veranlassen ist.

Der Streitwert für § 7 Abs.4 TMG kann nach gegenwärtiger Rechtslage von Gerichten frei geschätzt werden.[291] Um die hier versteckten Kostenrisiken für Anschlussinhaber abzumindern, sollte ins GKG eine Vorschrift nach dem Vorbild von § 51 GKG aufgenommen werden, die den Streitwert für § 7 Abs.4 TMG auf einige wenige hundert Euro (zum Beispiel EUR 500, also die unterste Gebührenschwelle nach Anlage 2 GKG) begrenzt. An diese Begrenzung wären dann über § 23 Abs.1 Satz 1 RVG auch die Rechtsanwaltsgebühren gebunden.

Der Streitwert des Unterlassungsanspruches ist unter Geltung der § 97a Abs.3 Satz 2 UrhG und § 7 Abs.4 TMG praktisch bedeutungslos. Bedeutung könnte er allerdings wieder erlangen, sollte § 7 Abs.4 TMG in Zukunft abgeschafft und die Haftung auf Unterlassung auf Grundlage der Störerhaftung wiedereingeführt werden oder insbesondere dann, wenn der BGH den § 97a Abs.3 Satz 2 UrhG aus europarechtlichen Überlegungen nicht anwenden

[290] Bei der Berechtigungsanfrage wird lediglich die Verletzungshandlung geschildert und der Angefragte zu einem Austausch über die Sach- und Rechtsanlage angehalten; jedoch löst eine Berechtigungsanfrage keinerlei Rechtsfolgen in die eine oder andere Richtung aus, vgl. *Lampmann* in: Hoeren/Sieber/Holznagel, MultimediaR, 47. EL 2018, Teil 23, Rz. 47.

[291] Vgl. Kapitel § 4 VIII. 8.

sollte.[292] Bisher konnten Gerichte den Gebührenstreitwert für die Gerichtskosten gemäß § 48 Abs.1 Satz 1 GKG iVm § 3 ZPO, den Gebührenstreitwert für die gerichtlichen Rechtsanwaltskosten gemäß § 48 Abs.1 Satz 1 GKG iVm § 3 ZPO iVm § 23 Abs.1 Satz 1 RVG und den Gebührenstreitwert für die außergerichtlichen Rechtsanwaltskosten – den § 97a Abs.3 Satz 2 UrhG hinweg gedacht – gemäß § 23 Abs.3 Satz 2 RVG frei schätzen[293], was trotz des Umstandes, dass regelmäßig gegen Privatpersonen gestritten wird, zu sehr hohen Streitwerten führte.[294] Um dieses Kostenrisiko für Anschlussinhaber einzudämmen, sollte daher – wiederum in Anlehnung an § 51 Abs.3 GKG – eine Vorschrift ins GKG eingeführt werden, die letztlich dem § 97a Abs.3 UrhG entspricht, also bei Urheberrechtsstreitigkeiten, in denen es um Ansprüche gegen nicht-gewerblich handelnde Personen geht, den gerichtlichen Streitwert zwingend auf EUR 1.000 begrenzt.[295] Eine solche Vorschrift hätte zudem den Vorteil, dass sich der Streit darüber, ob § 97a Abs.3 UrhG mit Art. 14 EnforcementRL vereinbar ist[296], erledigt hätte, da der Gebührenersatzanspruch nach § 97a Abs.3 UrhG dann nicht niedriger sein könnte als der gesetzliche Gebührenanspruch des abmahnenden Rechtsanwalts gegen den ihn beauftragenden Rechteinhaber.[297]

---

[292] Siehe hierzu Kapitel § 5 XI. Sollte in dieser Variante allerdings § 7 Abs.4 TMG beibehalten werden, hätte der Streitwert nur für Altfälle vor dem Inkrafttreten des 3. TMGÄndG Bedeutung. Siehe umfangreich zur Berechnung des Streitwerts *Backes*, Der Streit- und Gegenstandswert bei Unterlassungsansprüchen im Urheberrecht, S. 53ff.

[293] Da § 97a Abs.3 UrhG, wie sich aus dessen Gesetzgebungshistorie ableiten lässt, in systematischer Hinsicht keinen Einfluss auf den gerichtlichen Streitwert hat, siehe *Backes*, Der Streit- und Gegenstandswert bei Unterlassungsansprüchen im Urheberrecht, S. 143f.

[294] Der BGH erachtet beispielsweise einen Streitwert von nicht unter EUR 15.000 für angemessen, wenn der Streitgegenstand ein durchschnittlich erfolgreiches Computerspiel, dessen Veröffentlichung noch nicht lange zurück liegt, ist, siehe BGH, Urteil vom 30. März 2017, Az. I ZR 124/16, Rz. 37 – ZUM-RD 2018, 68.

[295] Eine Billigkeitsklausel wie in § 97a Abs.3 Satz 4 UrhG ist dabei nicht vonnöten.

[296] Siehe Kapitel § 5 XI.

[297] Denn Art. 14 EnforcementRL kann nur dann einschlägig sein, wenn ein dem Grunde nach eigentlich höherer Gebührenersatzanspruch herabgesetzt wird, vgl. Kapitel § 5 XI.

XV. Übertragung der Entscheidung „Novembermann“ auf *filesharing*-Konstellationen

In der Entscheidung „Der Novembermann“ aus 2019 urteilte der BGH, dass das rechtsanwaltliche, außergerichtliche Vorgehen gegen durch verschiedene Personen begangene, in der Sache aber gleichartige Verletzungen des Urheberrechts eine einheitliche Angelegenheit im Sinne des § 15 Abs.2 RVG darstellen.[298] Er bestätigte damit die Entscheidung des Berufungsgerichts, derzufolge der Anspruch auf Erstattung von Abmahnkosten nicht aus einem Streitwert, der für jede Abmahnung gesondert gebildet wird, zu berechnen ist, sondern stattdessen die Streitwerte der Abmahnungen, die eine Angelegenheit im gebührenrechtlichen Sinne darstellen, zusammenzufassen sind, und der Erstattungsanspruch sodann in Höhe des proportionalen Bruchteils der aus diesem Streitwert errechneten Geschäftsgebühr besteht.[299] Da die Höhe der Geschäftsgebühr nicht linear mit der Höhe des Streitwerts steigt, sondern stattdessen abflacht, ist der Erstattungsanspruch des Abmahnenden somit niedriger als wenn jede Abmahnung eine abgeschlossene Angelegenheit im gebührenrechtlichen Sinne darstellen würde.[300]

Nach BGH setzt eine einheitliche Angelegenheit im gebührenrechtlichen Sinne voraus, dass zwischen den erbrachten Leistungen ein innerer Zusammenhang besteht und sie sowohl inhaltlich als auch in der Zielsetzung so weitgehend übereinstimmen, dass von einem einheitlichen Rahmen der anwaltlichen Tätigkeit gesprochen werden kann; dieser einheitliche Rahmen bestünde auch dann noch, wenn die Leistungen die Prüfung von in ihren Voraussetzungen voneinander abweichenden Anspruchsgrundlagen enthält oder mehrere getrennte Prüfungsaufgaben zu erfüllen sind. Insbesondere gelte als einheitlicher Rahmen im diesen Sinne, wenn an verschiedene Adressaten ein Abmahnschreiben zu richten ist, sofern diesen eine gleichgerichtete Verlet-

[298] BGH, Urteil vom 6. Juni 2019, Az. I ZR 150/18, Rz. 24ff. – GRUR 2019, 1044 - „Der Novembermann“.

[299] BGH, Urteil vom 6. Juni 2019, Az. I ZR 150/18, Rz. 22 – GRUR 2019, 1044 - „Der Novembermann“.

[300] Ein Konflikt dieser Rechtsprechung mit Art. 14 EnforcementRL ist nicht zu erwarten, da hier – anders als bei § 97a Abs.3 UrhG (siehe Kapitel § 5 XI.) – nicht ein zunächst in bestimmter Höhe, auf Seiten eines Rechtsanwalts entstandener Anspruch bei Durchsetzung gegenüber einem Dritten gekürzt wird, sondern quasi bereits „gekürzt entsteht“.

zungshandlung vorzuwerfen ist; dass es sich hierbei verfahrensrechtlich um verschiedene Streitgegenstände handle, sei irrelevant.[301]

In der Literatur ist daher zu recht aufgeworfen worden, dass diese Rechtsprechung auch für *filesharing*-Fälle gelten dürfte, da in diesen Gegenstand der Abmahnungen auf Grund der einheitlichen Ermittlungen und urheberrechtlichen Bewertung ebenfalls gleichgerichtete Verletzungshandlungen seien, sofern diese dasselbe Werk betreffen, und regelmäßig durch einen einheitlichen Auftrag des Rechteinhabers verklammert würden.[302]

Demgegenüber ist wiederum berechtigterweise eingewendet worden, dass die „Novembermann"-Rechtsprechung für Abmahnende zunächst allgemein das Problem aufwirft, wann sie den Kostenerstattungsanspruch durchsetzen können bzw. inwiefern sich Abmahnungen, die nach Durchsetzung von Erstattungsansprüchen ausgesprochen werden, auf die Höhe der bereits durchgesetzten Ansprüche nachträglich auswirken[303]. Weiterhin ist berechtigterweise eingewendet worden, dass bei *filesharing*-Fällen Probleme entstehen, wenn auf Grund von § 97a Abs.3 UrhG verringerte Streitwerte mit nicht verringerten Streitwerten verrechnet werden und dadurch die Begünstigung des § 97a Abs.3 UrhG ausgehebelt wird[304].

Letzteres Problem dürfte mehr theoretischer denn praktischer Natur sein, da die Streitwertverringerung des § 97a Abs.3 UrhG für alle natürlichen, nicht gewerblich tätigen Personen gilt und Abmahnungen gegenüber anderen Personen als diesen fast nicht vorkommen.[305] Letztlich ließe sich aber dieses Problem entweder dadurch lösen, dass die Privilegierung des § 97a Abs.3 UrhG auch in diesem Fall für den Abgemahnten die Haftungsobergrenze mitbestimmt[306], also die Anwendung der „Novembermann"-Rechtsprechung niemals zu einer Verteuerung führt, oder dass § 97a Abs.3 UrhG analog auch auf die vom Anwendungsbereich nicht erfassten Personen angewendet wird.[307].

[301] BGH, Urteil vom 6. Juni 2019, Az. I ZR 150/18, Rz. 24, 31 – GRUR 2019, 1044 - „Der Novembermann".

[302] *Kuntz*, JurPC WebDok. 13/2020, Abs. 8ff; die Anwendbarkeit bejahend auch *Verweyen*, WRP 2020, 12, 15.

[303] *Verweyen*, WRP 2020, 12, 15.

[304] *Verweyen*, JurPC WebDok. 29/2020, Abs. 5ff.

[305] Siehe Kapitel § 3 V. 3.

[306] Mitbestimmt, da § 97a Abs.3 UrhG nur für den Unterlassungsanspruch gilt.

[307] *Verweyen*, JurPC WebDok. 29/2020, Abs. 16f.

Ersteres „Problem“ dürfte sich in der Praxis nicht als solches darstellen, da der Abmahnende jederzeit nachvollziehen kann, wen er bereits abgemahnt hat, sodass bei bereits durchgesetzten Forderungen gegebenenfalls nachträglich der Rechtsgrund teilweise wegfällt und die dann also überzahlte Summe zurückzuerstatten ist.

Im Übrigen sollte die sekundäre Darlegungslast des Rechteinhabers bezüglich der von diesem für die Abmahnung bezahlten Rechtsanwaltskosten[308] auch in diesem Kontext gelten, sodass im Prozess der Rechteinhaber auf Verlangen auch darzulegen hat, wie viele Abmahnungen wegen Verletzung desselben Schutzrechts mit jeweils welchem Streitwert bereits versandt wurden, sodass der Empfänger berechnen kann, ob die von ihm verlangte Summe unter Anwendung der „Novembermann“-Rechtsprechung berechtigt ist.

[308] Siehe Kapitel § 5 XII.

Zusammenfassung der Gesamtergebnisse

Die Gesamtergebnisse dieser Arbeit lassen sich wie folgt zusammenfassen:

- Eine definitorische Bestimmung des spezifischen Phänomens des *filesharing* und Abgrenzung von anderen Methoden der Dateiübertragung ist in technischer Hinsicht möglich. Von hervorgehobener praktischer Bedeutung ist das BitTorrent-System, das sich in seiner Funktionsweise von anderen Systemen teils deutlich unterscheidet. Die Ermittlung von Teilnehmern in einem *filesharing*-System ist grundsätzlich möglich, jedoch mit Defiziten behaftet. Die Ermittlungsmöglichkeiten enden technisch grundsätzlich am Internetanschluss. Für den Anschlussinhaber, ISPs und zahlreiche weitere Akteure des Internets besteht die Möglichkeit, präventive Maßnahmen vorzunehmen, um insbesondere BitTorrent-*filesharing* zu erschweren oder gar vollständig zu unterbinden, insbesondere Letzteres jedoch nicht ohne Kollateralschäden.

- *filesharing* findet seit dem Jahr 2000 in der deutschen (und auch internationalen) rechtswissenschaftlichen Literatur beständig Beachtung. In der Praxis häufen sich in Deutschland insbesondere seit der Einführung eines zivilrechtlichen Auskunftsanspruches gegen ISPs deren Kunden betreffend im Jahr 2008 Abmahnungen und Gerichtsverfahren. Mittlerweile gibt es daher zahlreiche Entscheidungen des BGH und des EuGH, die sich insbesondere auch mit der Haftung des Inhabers des Anschlusses, über den *filesharing* betrieben wurde, befassen. Überdies ist der Gesetzgeber mehrfach aktiv geworden und hat zahlreiche Reformen mit explizitem und implizitem Bezug zum *filesharing* vorgenommen.

- *filesharing* ist nach wie vor ein Massenphänomen. Da es überwiegend

zur Verletzung von Urheberrechten verwendet wird, hat sich in Kombination der technischen Ermittlungsmöglichkeiten mit der Rechtsprechung betreffend die Haftung von Anschlussinhabern in Deutschland ein Phänomen herausgebildet, das als Abmahnwesen bezeichnet werden kann. Diese Bezeichnung ist gerechtfertigt, da es sich von regulärer rechtsanwaltlicher Tätigkeit dahingehend unterscheidet, dass anstatt dem Unterbinden und der Kompensierung von Urheberrechtsverletzungen eine eigene Profitquelle erschlossen und dabei ein strukturelles Machtungleichgewicht zwischen den in Anspruch genommenen Anschlussinhabern und den profitierenden Rechteinhabern ausgenutzt wird. Dieses Abmahnwesen lässt sich rechtspolitisch nicht rechtfertigen. Im internationalen Vergleich ist es zudem einzigartig. Beim Ausblick in die Zukunft kann festgehalten werden, dass ein Abmahnwesen auch in anderen Sachbereichen als dem Urheberrecht, wie beispielsweise dem Patentrecht, entstehen kann.

- Die Rechtsprechung des BGH zum *filesharing* ist dogmatisch überwiegend zu kritisieren; gleiches gilt für die Qualität der Gesetzgebung auf diesem Feld. In einem für das Abmahnwesen entscheidenden Kernaspekt, der Schadensersatzhaftung, ist nach einer neueren Entscheidung des BGH noch nicht vorhersehbar, welche Konsequenzen sich hieraus für das Abmahnwesen ergeben werden.

- Zuletzt wurde aufgezeigt, welche Alternativen *de lege ferenda* denkbar sind, die die Situation von Anschlussinhabern verbessern, aber zugleich einen Ausgleich mit den berechtigten Interessen der Urheberrechtsindustrie erzielen. Soweit in für das *filesharing* relevanten Bereichen noch keine höchstrichterliche Rechtsprechung existiert, wurde aufgezeigt, welche Auslegungsvarianten dort in rechtsdogmatischer Hinsicht zu bevorzugen sind.

Schlusswort

In seiner *concurring opinion* zu dem „Grokster"-Urteil des *US Supreme Court* schlug Richter *Breyer* der Urheberrechtsindustrie recht unverblümt vor, dass sie doch auch gegen die Endnutzer von *filesharing*-Diensten vorgehen könne, um „Online-Piraterie" zu bekämpfen.[309] Fast möchte man sich – am Ende dieser Arbeit und nach mehr als einer Dekade von *filesharing*-Verfahren gegen Endnutzer in Deutschland – wünschen, der BGH würde in einer zukünftigen Tauschbörsen-Entscheidung *obiter dictum* einen Ratschlag in die umgekehrte Richtung erteilen, und stattdessen auf die zahlreichen Intermediäre, die für das BitTorrent-„Ökosystem" relevant sind[310], verweisen. Damit soll auch die Frage, die sich dem ein oder anderen Leser dieser Arbeit stellen mag, nämlich inwiefern legitime Interessen der Urheberrechtsindustrie noch geschützt werden, wenn die Stellung der Internetanschlussinhaber gestärkt wird, beantwortet werden: es bleibt noch viel unausgeschöpftes Potential. Zwar wurde und wird viel gegen Intermediäre unternommen[311], aber dieses Vorgehen ist ausbaufähig.

Zumindest in der EU steht dem der gegenwärtige Rechtsrahmen nicht entgegen.[312] International wurden und werden (auch in Entwicklungsländern) die notwendigen rechtlichen Voraussetzungen geschaffen oder bereits genutzt – wenn auch häufig nicht mit politisch einwandfreien Mitteln.[313] Zukunfts-

---

309 MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (Breyer, J. concurring), Rz. 133 – h2o.law.harvard.edu.

310 Siehe hierzu Kapitel § 1 V. 4.

311 Siehe die Beispiele in Kapitel § 1 V. 4.

312 *Nordemann*, Liability of Online Service Providers for Copyrighted Content - Regulatory Action Needed?, S. 18.

313 Siehe Kapitel § 3 III.

weisend sind das Vorgehen gegen private Börsen[314], *seedboxen*[315], *initial seeder*[316] sowie das unter dem Stichwort *follow the money* vereinte Vorgehen gegen verschiedene Akteure, die für die Finanzierung insbesondere von BitTorrent-Indexseiten vonnöten sind.[317]

Eine Grenze sollte aber gezogen werden: die Entwicklung der BitTorrent-Technologie an sich[318] muss ungestört möglich sein. *filesharing*-Systeme haben ein großes Anwendungspotential, das durch eine übereifrige Durchsetzung des Urheberrechts nicht zunichte gemacht werden sollte. Der Verfasser wünscht sich somit für die Zukunft, dass – bei aller Berücksichtigung berechtigter Interessen verschiedener Akteure – das Primat der technologische Fortschritt bleibt. Hierbei ist auch anzumahnen, dass die Akzeptanz des Urheberrechts von seinem mäßigen Gebrauch abhängt – erst recht im Digitalzeitalter. Es würde einer gewissen geschichtlichen Ironie nicht entbeh-

[314] Siehe Kapitel § 1 II. 5. c).

[315] Siehe Kapitel § 1 IV. 6. b) bb).

[316] Der *initial seeder* eines Schwarms kann ermittelt werden, solange im Schwarm im Übrigen nur *leecher* vorhanden sind, siehe *Lai* et al., Peer-to-Peer Networking and Applications, Nr. 4, Bd. 7, 2014, S. 313, 317. Gerade in der Anfangszeit des BitTorrent-*filesharing* in Deutschland wurde das Vorgehen gegen *initial seeder* forciert, vgl. *Krempl*, GVU fordert Maßnahmenpaket gegen Urheberrechtsverletzer. Interessanterweise hört man hiervon seit 2010 – über die Gründe kann nur spekuliert werden – nichts mehr.

[317] Diese erzielen gegenwärtig Gewinne primär durch das Anbieten von Werbeplätzen sowie die Nutzung der PCs ihrer Besucher für *crypto mining*; siehe hierzu den Überblick bei *Rieck*, State of the Art: Über die Formen der Monetarisierung von illegalen Webseiten. Wie viel Geld mit Letzterem verdient wird, ist unbekannt. Zu Ersterem gibt es verschiedene Schätzungen. Nach einer Studie soll der mit Werbung erzielte Gewinn von allen Indexseiten insgesamt gegenwärtig über 111 Millionen US-Dollar pro Jahr betragen, wobei sich über die Zahlen – nach einem Abgleich mit anderen Studien – durchaus streiten lässt; siehe mit einer Übersicht *Van Der Sar*, „Pirate Sites Generate $111 Million In Ad Revenue a Year". Der ökonomischen Forschung zu Folge sind freiwillige Selbstverpflichtungen der Werbeindustrie dahingehend, auf Indexseiten und Ähnlichem keine Werbung zu schalten, nur bedingt erfolgreich, siehe *Batikas/Claussen/Peukert*, Follow The Money: Piracy and Online Advertising, S. 13f. Folglich rücken die Vermittler von Werbung als Haftungsobjekte in den Blick, siehe *Nordemann/Waiblinger*, MMR 2017, 211, 215f. Aktuelles Beispiel: das AG Leipzig hat einen Werbemakler wegen Beihilfe zur Urheberrechtsverletzung strafrechtlich verurteilt, siehe http://gvu.de/erstes-urteil-gegen-werbeagentur-auf-illegalen-online-portalen-in-deutschland/3984 - Zugriff am 31.03.2021.

[318] Oder anderer, neuer *filesharing*-Systeme.

ren, wenn das Urheberrecht, einst durch die Erfindung des Buchdrucks aus der Taufe gehoben, nun durch eine andere technischen Erfindung zu Grabe getragen würde.

Literaturverzeichnis

Abdallah, Tarek: Zur Weitergabe von Nutzerdaten an Schutzrechtsinhaber durch Gewährung von Akteneinsicht gemäß § 406e StPO - Preisgabe des Datenschutzes zugunsten eines verfassungswidrigen Opferschutzes? JurPC, 2006, JurPC WebDok. 149/2006, Abs. 1 – 22.

Abdallah, Tarek/Gercke, Björn: Strafrechtliche und strafprozessuale Probleme der Ermittlung nutzerbezogener Daten im Internet, Zeitschrift für Urheber- und Medienrecht, 2005, 368–376.

Achilles, Phillip: Die Verantwortlichkeit von Onlinediensteanbietern für das rechtsverletzende Verhalten Dritter unter Anwendung der Verkehrspflichtendogmatik, 2017 - zugleich Diss., ISBN 978–3–8300–9686–3.

Adolphsen, Jens/Mayer, Dominik/Möller, Frederik: Massenabmahnungen im Urheberrecht, Neue Juristische Online Zeitschrift, 2010, 2394–2399.

Ahlberg, Hartwig/Götting, Horst-Peter (Hrsg.): BeckOK Urheberrecht, 30. Auflage. 2021.

Ahmad, Mansur: Grundlagen über Peer-to-Peer, 2004 ⟨URL: wwwcs.uni-paderborn.de/StaffWeb/maho/.../T11_MansurAhmad-GrundlagenP2P.pdf⟩.

Ahrens, Claus: Napster, Gnutella, FreeNet & Co. – die immaterialgüterrechtliche Beurteilung von Internet-Musiktauschbörsen, Zeitschrift für Urheber- und Medienrecht, 2000, 1029–1038.

Albach, Gregor: Zur Verhältnismässigkeit der Strafbarkeit privater Urhe-

berrechtsverletzungen im Internet, 2015 - zugleich Diss., ISBN 3–734–77992–8.

Alberty, Tiffany: The New Ponzi Scheme: BitTorrent & Hardcore Pornography, The John Marshall Review of Intellectual Property Law, 15 2016, 799–826.

Alcock, Shane/Nelson, Richard: Measuring the Impact of the Copyright Amendment Act on New Zealand Residential DSL Users, In Proceedings of the 2012 Internet Measurement Conference, 2012, IMC '12, 551–558.

Allen-Robertson, James: Digital Culture Industry, 2013, ISBN 978–1–13703–346–8.

Amini, Seyavash: Digitale Kultur zum Pauschaltarif? 2017 - zugleich Diss., Abhandlungen zum Urheber- und Telekommunikationsrecht 62, ISBN 978–3–8487–4031–4.

Anderson, Steven: The A-list conspiracy: Did Hollywood tell Obama to take down internet entrepreneur Kim Dotcom? ⟨URL: https://ind.pn/2VHuvf4⟩ – Zugriff am 31.03.2021.

Aron, Jacob: Illegal filesharing goes 3D, New Scientist, 213 2012 Nr. 2850, 22.

Aschermann, Tim: Dynamische und statische IP-Adressen: Das sind die Unterschiede, ⟨URL: https://praxistipps.chip.de/dynamische-und-statische-ip-adressen-das-sind-die-unterschiede_13536⟩ – Zugriff am 31.03.2021.

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 2. Auflage. 2016.

Austin, Graeme W.; Dinwoodie, Graeme B. (Hrsg.): Common Law Pragmatism: New Zealand's Approach to Secondary Liability of Internet Service Providers, 2017, 213–227, ISBN 978–3–319–55030–5.

Backes, Timon: Der Streit- und Gegenstandswert bei Unterlassungsansprüchen im Urheberrecht, 2018 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 137, ISBN 978–3–16–156030–9.

Bailey, Jonathan: The Long, Slow Decline of BitTorrent, ⟨URL: https://www.plagiarismtoday.com/2017/06/01/the-long-slow-decline-of-bittorrent/⟩ – Zugriff am 31.03.2021.

Baker, Fred et al.: Addressing the challenge of IP spoofing, Internet Society 2015 – Technischer Bericht.

Balasubramanian, Aparna et al.; Daim, Tugrul/Kim, Jisun/Phan, Kenny (Hrsg.): Technology Forecasting: Case of 3D Printing, 2017, 89–104.

Balganesh, Shyamkrishna/Gelbach, Jonah B.: Debunking the Myth of the Copyright Troll Apocalypse, Iowa Law Review Online, 101 2016, 43–64.

Ballano, Vivencio O.: U.S. Global Hegemony in Intellectual Property and the Politics of Piracy and Resistance, 2016, 33–74.

Batikas, Michail/Claussen, Jörg/Peukert, Christian: Follow The Money: Piracy and Online Advertising, International Telecommunications Society (ITS) 2017 – 28th European Regional ITS Conference, Passau 2017 ⟨URL: https://ideas.repec.org/p/zbw/itse17/169448.html⟩.

Beckedahl, Markus: Abmahnindustrie: EU-Kommission bereitet Klage wegen Verletzung des EU-Rechts vor, ⟨URL: https://bit.ly/2VGyhp1⟩ – Zugriff am 31.03.2021.

Beckedahl, Markus: EU-Kommission kritisiert Gesetz-Entwurf zur Verschlimmbesserung der Störerhaftung, ⟨URL: https://bit.ly/1IIgzEI⟩ – Zugriff am 31.03.2021.

Behr, Volker: Strafschadensersatz im deutschen Recht - Wiederauferstehung eines verdrängten Phänomens, Zeitschrift für das Juristische Studium, 2010, 292–296.

Bell, Tom W.: Copyright Porn Trolls, Wasting Taxi Medallions, and the Propriety of „Property“, Chapman Law Review, 18 2015, 799–814.

Bender, Rolf: Einige Aspekte zu den Erfolgsbarrieren in der Justiz, Rabels Zeitschrift für ausländisches und internationales Privatrecht, 1976, 718–726.

Bershidsky, Leonid: Why Netflix Is Winning the Online Piracy Wars, ⟨URL: https://www.bloomberg.com/view/articles/2017-05-02/why-netflix-is-winning-the-online-piracy-wars⟩ – Zugriff am 31.03.2021.

Bhatia, Max/Rai, Mritunjay Kumar: Identifying P2P traffic: A survey, Peer-to-Peer Networking and Applications, 10 2017 Nr. 5, 1182–1203.

Bilton, Nick: Internet Pirates Will Always Win, ⟨URL: http://www.nytimes.com/2012/08/05/sunday-review/internet-pirates-will-always-win.html⟩ – Zugriff am 31.03.2021.

BITAG: Port Blocking, BITAG 2013 – Technischer Bericht ⟨URL: https://www.bitag.org/documents/Port-Blocking.pdf⟩.

Blackburn, David/Eisenach, Jeffrey A./Harrsion, David Jr.: Impacts of Digital Video Piracy on the U.S. Economy, 2019 ⟨URL: https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf⟩.

Blanke-Roeser, Constantin: 3D-Druck und das Patentrecht in Europa, Gewerblicher Rechtsschutz und Urheberrecht, 2017, 467–475.

Bleich, Holger: Briefkasten-Ermittlungen, ⟨URL: https://bit.ly/2JyYGlV⟩ – Zugriff am 31.03.2021.

Bleich, Holger: Bosse der Fasern: Die Infrastruktur des Internet, c't, 2005 Nr. 7, 88–93.

Bleich, Holger: Die Abmahn-Industrie, c't, 1 2010, 154–157.

Bleich, Holger: Fragwürdige Beweisführung, c't, 5 2010, 50–51.

Bleich, Holger: Bröckelndes Geschäftsmodell, c't, 11 2015, 152–155.

Bülte, Jens: Strafbarkeit von „aggressiven" Massenabmahnungen als Betrug oder Erpressung, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht, 2014, 41–49.

Bogedain, Clemens: Der Einfluss des US-Special 301-Verfahrens auf die Immaterialgüterrechtsgesetzgebung ausländischer Staaten am Beispiel der jüngsten Entwicklungen im ukrainischen Urheberrecht, GRUR International, 2019, 543–550.

Bohlen, Marc: Der Streitwert im Rahmen der urheberrechtlichen Abmahnung, Neue Juristische Wochenschrift, 2017, 777–779.

Borges, Georg: Pflichten und Haftung beim Betrieb privater WLAN, Neue Juristische Wochenschrift, 2010, 2624–2627.

Borges, Georg: Die Haftung des Internetanschlussinhabers für Urheberrechtsverletzungen durch Dritte, Neue Juristische Wochenschrift, 2014, 2305–2310.

Bosak, Jan Michael: Urheberrechtliche Zulässigkeit privaten Downloadings von Musikdateien, Computer und Recht, 2001, 176–181.

Brand, Peter-Andreas: Grenzen zivilprozessualer Wahrheit und Gerechtigkeit, Neue Juristische Wochenschrift, 2017, 3558–3563.

Braun, Ilja: Grundeinkommen statt Urheberrecht? 2014, ISBN 978–3–8376–2680–3.

Braun, Sven: Grundrechtswidrig bleibt grundrechtswidrig - Reaktionen zum zweiten EuGH-Urteil zur Vorratsdatenspeicherung, ⟨URL: https://bit.ly/2whUcbz⟩ – Zugriff am 31.03.2021.

Braun, Thorsten: „Filesharing"-Netze und deutsches Urheberrecht - Zugleich eine Entgegnung auf Kreutzer, GRUR 2001, 193ff. und 307ff. Gewerblicher Rechtsschutz und Urheberrecht, 2001, 1106–1111.

Brüggemann, Sebastian: Der Drittauskunftsanspruch gegen Internetprovider, 2012 - zugleich Diss., Schriftenreihe zu Medienrecht, Medienproduktion und Medienökonomie 20, ISBN 978–3–8329–7753–5.

Bridy, Annemarie: Graduated Response American Style: „Six Strikes" Measured Against Five Norms, Fordham Intellectual Property, Media & Entertainment Law Journal, 23 2013, 1–67.

Bridy, Annemarie: Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation, Washington and Lee Law Review, 74 2017, 1345–1385.

Briegleb, Volker: Vorratsdatenspeicherung: Provider warnen vor dem „Mittelstandskiller", ⟨URL: https://bit.ly/2WhjGoa⟩ – Zugriff am 31.03.2021.

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.): BeckOK Datenschutzrecht, 35. Auflage. 2021.

Brinkel, Guido: Filesharing, 2006 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 4, ISBN 978–3–16–148843–6.

Brodkin, Jon: BitTorrent: Netflix should defeat ISPs by switching to peer-to-peer, ⟨URL: https://arstechnica.com/information-technology/2014/04/bittorrent-netflix-should-defeat-isps-by-switching-to-peer-to-peer/⟩ – Zugriff am 31.03.2021.

Bäuerlein, Theresa: Sie mahnen ab. Sie kassieren. Wer sind Waldorf Frommer? ⟨URL: https://krautreporter.de/890--sie-mahnen-ab-sie-kassieren-wer-sind-waldorf-frommer?shared=eyJzaGFyZWRCeSI6IkxhcnMgRWdnZXJzZG9yZ⟩ – Zugriff am 31.03.2021.

Buford, John F./Yu, Heather: Peer-to-Peer Networking and Applications: Synopsis and Research Directions, In **Shen, Xuemin et al. (Hrsg.):** Handbook of Peer-to-Peer Networking, 1. Auflage. 2010, ISBN 978–0–387–09750–3, 3–37.

Buford, John F./Yu, Heather/Lua, Eng Keong: P2P networking and applications, 2009, ISBN 978–0–12–374214–8.

Bäumer, Ulrich/Rendell, Simon/Pühler, Alexander: Urheberrecht und Tauschplattformen im Internet, Computer Law Review International, 2004, 129–137.

Bundesamt, Statistisches: Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien, 2020 ⟨URL: https://bit.ly/3cJgVTO⟩.

Burkart, Patrick/Andersson Schwarz, Jonas: Gunboat Diplomacy and Pirate Sanctuaries: The Use of Trade Agreements to Promote Copyright Reform, In Communication and Media Policy in the Era of the Internet: Theories and Processes 1. Auflage. 2013, Schriften des Münchner Centrums für Governance-Forschung 9, ISBN 978–3–832–97842–6, 133–145.

Calliess, Christian/Ruffert, Matthies (Hrsg.): EUV/AEUV, 5. Auflage. 2016.

Cannon, Richard Michael: Enforcement of Media Piracy: America's Hardline Approach Versus Japan's Lackadaisical Approach and the Future of Enforcement in Japan Under the Trans-Pacific Partnership, Washington University Global Studies Law Review, 16 2017, 483–521.

Caraway, Brett: Piracy Cultures| Survey of File-Sharing Culture, International Journal of Communication, 6 2012, 564–584.

CDT: The Perils of Using the Domain Name System to Address Unlawful Internet Content, 2011 ⟨URL: https://cdt.org/files/pdfs/Perils-DNS-blocking.pdf⟩.

Champeau, Guillaume: Le transfert Hadopi - CSA n'est „plus l'axe prioritaire", ⟨URL: https://www.numerama.com/magazine/32267-le-transfert-hadopi-csa-n-est-plus-l-axe-prioritaire.html⟩ – Zugriff am 31.03.2021.

Chiu, Shun-Po/Chou, Huey-Wen: Investigating the User Behavior of Peer-to-Peer File Sharing Software, International Journal of Business and Management, 6 2011, 68–78.

Chothia, Tom et al.; Keromytis, Angelos D./Di Pietro, Roberto (Hrsg.): The Unbearable Lightness of Monitoring: Direct Monitoring in BitTorrent, 2013, 185–202.

Christin, Nicolas/Weigend, Andreas S./Chuang, John: Content Availability, Pollution and Poisoning in File Sharing Peer-to-peer Networks, In Proceedings of the 6th ACM Conference on Electronic Commerce, 2005, EC '05, 68–77.

Cisco: Cisco Visual Networking Index: Forecast and Methodology, 2009–2014, 2010 ⟨URL: http://large.stanford.edu/courses/2010/ph240/abdul-kafi1/docs/white_paper_c11-481360.pdf⟩.

Cisco: Cisco Visual Networking Index: Forecast and Methodology, 2013–2018, 2014 ⟨URL: http://www.anatel.org.mx/docs/interes/Cisco_VNI_Forecast_and_Methodology.pdf⟩.

Cisco: Cisco Visual Networking Index: Forecast and Methodolo-

gy, 2016–2021, 2017 ⟨URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf⟩.

Civil, Christopher: Mass Copyright Infringement Litigation: Of Trolls, Pornography, Settlement and Joinder, Syracuse Journal of Science & Technology Law, 30 2014, 2–55.

Clayton, Richard: Online traceability: who did that? Technical expert report on collecting robust evidence of copyright infringement through peer-to-peer filesharing, Consumer Focus 2012 – Technischer Bericht ⟨URL: https://www.cl.cam.ac.uk/~rnc1/Online-traceability.pdf⟩.

Clement, Reiner/Schreiber, Dirk: Internet-Ökonomie, 3. Auflage. 2016, 313–339, ISBN 978–3–662–49047–1.

Cohen, Brad: uTorrent Pro Tips: Faster Download & Upload Rates, ⟨URL: https://bit.ly/2KmZmM2⟩ – Zugriff am 31.03.2021.

Cohen, Bram: Incentives Build Robustness in BitTorrent, 2003 ⟨URL: www.bittorrent.org/bittorrentecon.pdf⟩.

Cserne, Péter: Consequence-Based Arguments in Legal Reasoning: A Jurisprudential Preface to *Law and Economics*, In **Mathis, Klaus (Hrsg.):** Efficiency, Sustainability, and Justice to Future Generations, 2011, 31–54.

Cumming, George/Freudenthal, Mirjam/Janal, Ruth: Enforcement of Intellectual Property Rights in Dutch, English and German Civil Procedure, 2008, International Competition Law Series, ISBN 978–9–04–112726–6.

Danaher, Brett/Smith, Michael D./Telang, Rahul: Copyright Enforcement in the Digital Age: Empirical Evidence and Policy Implications, Communications of the ACM, 60 2017 Nr. 2, 68–75.

Danaher, Brett/Smith, Michael D./Telang, Rahul: Piracy Landscape Study: Analysis of Existing and Emerging Research Relevant to Intellectual Property Rights (IPR) Enforcement of Commercial-Scale Piracy1, 2020 ⟨URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3577670⟩.

Danielis, Peter: Peer-to-Peer-Technologie in Teilnehmerzugangsnetzen, Dissertation, Universität Rostock, Fakultät für Informatik und Elektrotechnik 2012.

Dück, Hermann: Methodik der Delegationslücke, Zeitschrift für die gesamte Privatrechtswissenschaft, 2018, 76–120.

Delaney, Darragh: Tunnelling Bittorrent Over Port 80 - How to Detect Activity on Your Network, ⟨URL: https://bit.ly/2EnvE5E⟩ – Zugriff am 31.03.2021.

Depoorter, Ben: Copyright Enforcement in the Digital Age: When the Remedy is the Wrong, U.C.L.A. Law Review, 66 2019, 400–447.

Desai, Deven R./Magliocca, Gerard N.: Patents, Meet Napster: 3D Printing and the Digitization of Things, Georgetown Law Review, 102 2013, 1691–1720.

Dhungel, Prithula et al.: A Measurement Study of Attacks on BitTorrent Leechers, In Proceedings of the 7th International Conference on Peer-to-peer Systems, 2008, IPTPS'08, 1–6.

Ding, Choon Hong/Nutanong, Sarana/Buyya, Rajkumar: Peer-to-Peer Networks for Content Sharing, In **Subramanian, Ramesh/Goodman, Brian D. (Hrsg.):** Peer-to-Peer Computing: The Evolution of a Disruptive Technology, Hershey 2005, ISBN 1–59140–431–2, 28–65.

Dinger, Jochen/Waldhorst, Oliver P.: Decentralized Bootstrapping of P2P Systems: A Practical View, In Proceedings of the 8th International IFIP-TC 6 Networking Conference, 2009, NETWORKING '09, ISBN 978–3–642–01398–0, 703–715.

Dischinger, Marcel et al.: Detecting Bittorrent Blocking, In Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement, 2008, IMC '08, ISBN 978–1–60558–334–1, 3–8.

Dobusch, Leonhard/Quack, Sigrid; Dingwerth, Klaus/Kerwer, Dieter/Nölke, Andreas (Hrsg.): Internationale Beziehungen und Organisationsforschung, Band 1, Internationale und nichtstaatliche Orga-

nisationen im Wettbewerb um Regulierung: Schauplatz Urheberrecht, 2009, 233–262.

Dobusch, Leonhard/Schüßler, Elke: Copyright reform and business model innovation: Regulatory propaganda at German music industry conferences, Technological Forecasting and Social Change, 83 2014, 24 – 39.

Doherty, Davis: Downloading Infringement: Patent Law as a Roadblock to the 3D Priting Revolution, Harvard Journal of Law & Technology, 26 2012 Nr. 1, 353–373.

Donnerhacke, Lutz: Der Mythos von der dynamischen IP-Adresse, ⟨URL: https://www.heise.de/ct/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html?seite=2⟩ – Zugriff am 31.03.2021.

Doukoff, Norman: Grundlagen des Anscheinsbeweises, Straßenverkehrsrecht, 2015, 245–253.

Doyle, Jeff: Can Large Scale NAT Save IPv4? ⟨URL: https://www.networkworld.com/article/2227353/cisco-subnet/can-large-scale-nat-save-ipv4-.html⟩ – Zugriff am 31.03.2021.

Drakeman, Donald L.: Consequentialism and the limits of interpretation: do the ends justify the meanings? Jurisprudence, 9 2018 Nr. 2, 300–318.

Dreier, Thomas/Schulze, Gernot/Specht, Louisa (Hrsg.): Urheberrechtsgesetz, 6. Auflage. 2018.

Durumeric, Zakir et al.: Analysis of the HTTPS Certificate Ecosystem, In Proceedings of the 2013 Conference on Internet Measurement Conference, 2013, IMC '13, ISBN 978–1–4503–1953–9, 291–304.

Ehrenkranz, Toby/Li, Jun: On the State of IP Spoofing Defense, ACM Trans. Internet Technol. 9 2009 Nr. 2, 6:1–6:29.

Elberse, Anita: Bye-Bye Bundles: The Unbundling of Music in Digital Channels, Journal of Marketing, 74 2010 Nr. 3, 107–123.

Eliashberg, Jehoshua et al.: Of video games, music, movies, and celebri-

ties, International Journal of Research in Marketing, 33 2016 Nr. 2, 241–245.

Elton, Serona: A Survey of Graduated Response Programs to Combat Online Piracy, MEIEA, 14 2014 Nr. 1, 89–122.

Emnid: Bevölkerungsbefragung zum Thema Abmahnungen wegen Urheberrechtsverstößen, August 2016 ⟨URL: http://www.vzbv.de/sites/default/files/umfrage-urheberrechtsverstoesse-vzbv-2016.pdf⟩.

Ende, Martin van der et al.: Estimating displacement rates of copyrighted content in the EU, 2015 ⟨URL: https://op.europa.eu/en/publication-detail/-/publication/59ea4ec1-a19b-11e7-b92d-01aa75ed71a1⟩.

Engelhardt, Christian: Die rechtliche Behandlung von Urheberrechtsverletzungen in P2P-Netzwerken nach US-amerikanischem und deutschem Recht, 2007 - zugleich Diss., ISBN 978–3–63–15740–65.

Epping, Volker/Hillgruber, Christian (Hrsg.): BeckOK Grundgesetz, 46. Auflage. 2021.

Eres, Robert/Louis, Winnifred R./Molenberghs, Pascal: Why do people pirate? A neuroimaging investigation, Social Neuroscience, 12 2017 Nr. 4, 366–378.

Ermert, Monika: Gretchenfrage: NAT oder nicht NAT für IPv6? ⟨URL: https://www.heise.de/newsticker/meldung/Gretchenfrage-NAT-oder-nicht-NAT-fuer-IPv6-218971.html⟩ – Zugriff am 31.03.2021.

Ernicke, Katharina: Die Entstehung der dreifachen Schadensberechnung im deutschen Immaterialgüterrecht, Zeitschrift für Geistiges Eigentum, 2016, 84–132.

Ernst, Stefan/Seichter, Dirk: Die Störerhaftung des Inhabers eines Internetzugangs, Zeitschrift für Urheber- und Medienrecht, 2007, 513–519.

Ernsthaler, Jürgen/Weidert, Stefan (Hrsg.): Urheberrecht und Internet, 3. Auflage. 2017, ISBN 978–3–8005–1606–3.

Esser, Josef: Vorverständnis und Methodenwahl in der Rechtsfindung, 1970, ISBN 978–3–8072–6001–3.

EUIPO: European Citizens and Intellectual Property: Perception, Awareness and Behaviour 2017, 2017 ⟨URL: https://euipo.europa.eu/ohimportal/de/web/observatory/ip-perception-2017⟩.

EUIPO: European Citizens and Intellectual Property: Perception, Awareness and Behaviour 2020, 2020 ⟨URL: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Perception_study_2020/Perception_study_full_en.pdf⟩.

Fadaie, Farid: Building An Engine for Decentralized Communications, ⟨URL: http://blog.bittorrent.com/2014/07/30/building-an-engine-for-decentralized-communications/⟩ – Zugriff am 31.03.2021.

Fahy, Jo/DeVore, Veronica: US puts Switzerland on copyright watch list, ⟨URL: https://www.swissinfo.ch/eng/online-laxity_us-puts-switzerland-on-copyright-watch-list/42119418⟩ – Zugriff am 31.03.2021.

Farahbakhsh, Reza et al.: Understanding the evolution of multimedia content in the Internet through BitTorrent glasses, CoRR abs/1705.00548 2017.

Farina, Jason/Kechadi, M-Tahar/Scanlon, Mark: Project Maelstorm: Forensic Analysis Of The BitTorrent-Powered Browser, The Journal of Digital Forensics, Security and Law, 10 2015 Nr. 4, 115–124.

Farrand, Benjamin: Networks of power in digital copyright law and policy: political salience, expertise and the legislative process, 2014, ISBN 978–0–415–85442–9.

Faustmann, Jörg/Ramsperger, Gabriel: Abmahnkosten im Urheberrecht, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2010, 662–667.

Feilner, Markus: Entzaubert, iX, 7 2017, 86–92.

Felten, Ed/Sahi, Sauhard: Census of Files Available via Bit-

Torrent, 2010 ⟨URL: https://freedom-to-tinker.com/2010/01/29/census-files-available-bittorrent/⟩ – Zugriff am 31.03.2021.

Filby, Michael: Big Crook in Little China: The Ramifications of the Hong Kong BitTorrent Case on the Criminal Test of Prejudicial Effect, International Review of Law, Computers & Technology, 21 2007 Nr. 3, 275–283.

Fisher III, William W.: Promises to keep: Technology, law, and the future of entertainment, 2004, ISBN 978–08–04763–26–4.

Fleming, Piers et al.: Why do people file share unlawfully? A systematic review, meta-analysis and panel study, Computers in Human Behavior, 72 2017, 535–548.

Forch, Dana: Antwortpflicht des Abgemahnten bei privatem Filesharing? Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2014, 367–369.

Forch, Dana: Tatsächliche Vermutung, sekundäre Darlegungslast und prozessuale Wahrheitspflicht im Filesharing-Prozess, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2015, 49–51.

Forch, Dana: Filesharing: Sekundäre Darlegungslast in der jüngsten BGH-Rechtsprechung, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2017, 522–524.

Foreman, Violeta Solonova: Problems with BitTorrent Litigation in the United states: Personal Jurisdiction, Joinder, Evidentiary Issues, and Why the Dutch Have a Better System, Washington University Global Studies Law Review, 13 2014, 127–153.

Forouzan, Behrouz A.: TCP/IP protocol suite, 4. Auflage. 2010, McGraw-Hill Forouzan networking series, ISBN 978–0–07–337604–2.

Franck, Jens-Uwe: Vom Wert ökonomischer Argumente bei Gesetzgebung und Rechtsfindung für den Binnenmarkt, In **Riesenhuber, Karl (Hrsg.):** Europäische Methodenlehre, 2015, 70–93.

Frank, Thomas: MP3, P2P und StA - Die strafrechtliche Seite des Filesharing, Kommunikation und Recht, 2004, 576–581.

Freiwald, Sven: Die private Vervielfältigung im digitalen Kontext am Beispiel des Filesharing, 2003 - zugleich Diss., ISBN 978–3–8329–0446–3.

Freund, Bernhard/Schnabel, Christoph: Bedeutet IPv6 das Ende der Anonymität im Internet? Zeitschrift für IT-Recht und Recht der Digitalisierung, 2011, 495–499.

Frey, Harald: Massenabmahnungen und Social Norm Backlash im Urheberrecht, Zeitschrift für Urheber- und Medienrecht, 2014, 554–558.

Galetzka, Christian/Stamer, Erik: Beweislastverteilung und Haftungsgrundsätze beim Filesharing, Kommunikation und Recht, 2020, 486–493.

Garofoli, Chiara: Italy: No ISP Duty to Provide Customer Data, Computer Law Review International, 2007, 182–185.

GauthierDickey, Chris/Grothoff, Christian: Bootstrapping of Peer-to-Peer Networks, In 2008 International Symposium on Applications and the Internet, 2008, 205–208.

Geist, Michael: Canadian Hurt Locker Lawsuits Withdrawn, ⟨URL: http://www.michaelgeist.ca/2012/03/hurt-locker-suits-withdrawn/⟩ – Zugriff am 31.03.2021.

Geist, Michael: Rightscorp and BMG Exploiting Copyright Notice-and-Notice System: Citing False Legal Information in Payment Demands, ⟨URL: https://bit.ly/1DCknpA⟩ – Zugriff am 31.03.2021.

Geist, Michael: Why Copyright Trolling in Canada Doesn't Pay: Assessing the Fallout From the Voltage – TekSavvy Case, ⟨URL: http://www.michaelgeist.ca/2014/02/copyright-troll-economics/⟩ – Zugriff am 31.03.2021.

Geist, Michael: Wikileaks Cables Show Massive U.S. Effort to Establish Canadian DMCA, ⟨URL: http://www.michaelgeist.ca/2011/04/wikileaks-cables-on-us-copyright-lobby/⟩ – Zugriff am 31.03.2021.

Geist, Michael: Wikileaks on New Zealand Copyright: US Funds IP Enforcement, Offers to Draft Legislation, ⟨URL: http://www.michaelgeist.ca/2011/04/nz-wikileaks-copyright/⟩ – Zugriff am 31.03.2021.

Geppert, Martin/Schütz, Raimund (Hrsg.): Beck'scher TKG-Kommentar, 4. Auflage. 2013.

Gersdorf, Hubertus/Paal, Boris P. (Hrsg.): BeckOK Informations- und Medienrecht, 31. Auflage. 2021.

Giblin, Rebecca: The P2P Wars: How Code Beat Law, IEEE Internet Computing, 16 2012 Nr. 3, 92–94.

Gietl, Andreas: Störerhaftung für ungesicherte Funknetze - Voraussetzungen und Grenzen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2007, 630–634.

Gietl, Andreas/Mantz, Reto: Die IP-Adresse als Beweismittel im Zivilprozess, Computer und Recht, 2008, 810–816.

Giovanella, Federica; Caso, Roberto/Giovanella, Federica (Hrsg.): Effects of Culture on Judicial Decisions: Personal Data Protection vs. Copyright Enforcement, 2015, 65–98, ISBN 978–3–662–44648–5.

Goldman, Eric: Ad Network Defeats Secondary Copyright Claims - ALS Scan v. JuicyAds, ⟨URL: https://blog.ericgoldman.org/archives/2016/10/ad-network-defeats-secondary-copyright-claims-als-scan-v-juicyads.htm⟩ – Zugriff am 31.03.2021.

Gomes, João V. et al.: Detection and Classification of Peer-to-peer Traffic: A Survey, ACM Computing Surveys, 45 2013 Nr. 3, 1–40.

Gotthardt, Lukas: Zivilprozessuale Rechtsdurchsetzung in Filesharing-Fällen mit Familienbezug – Nachforschungspflichten im Rahmen der sekundären Darlegungslast unter Berücksichtigung aktueller Rechtsprechung, Zeitschrift für Urheber- und Medienrecht, 2021, 7–16.

Graf, Jürgen-Peter (Hrsg.): BeckOK StPO mit RiStBV und MiStra, 39. Auflage. 2021.

Graf Ballestrem, Johannes: Dreidimensionales Drucken - aus patentrechtlicher Sicht, Mitteilungen der deutschen Patentanwälte, 2016, 358 – 364.

Grahovec, Edward: What's Going on With Copyright Trolls? DePaul

Journal of Art, Technology & Intellectual Property Law, 30 2020, 69–89.

Greenberg, Andy: Why Google Is The New Pirate Bay, ⟨URL: https://www.forbes.com/2009/04/17/pirate-bay-google-technology-internet-pirate-bay/⟩ – Zugriff am 31.03.2021.

Greenberg, Brad A.: Copyright Trolls and the Common Law, Iowa Law Review Bulletin, 100 2015, 77–86.

Gregor, Stephan: Das Bereicherungsverbot, 2012 - zugleich Diss., Studien zum Privatrecht 18, ISBN 978–3–16–151704–4.

Grigorjew, Olga: Rechtssicherheit für WLAN-Anbieter? Computer und Recht, 2016, 701–706.

Grigorjew, Olga/Bile, Tamer: Änderung des TMG: Gelungene Nachbesserung für einen rechtssicheren offenen WLAN-Betrieb? ZD-aktuell, 2017, 05621.

Grinvald, Leah Chan: Policing the Cease-and-Desist Letter, University of San Francisco Law Review, 49 2015, 409–463.

Grisse, Karina: The Graduated Response System in the Digital Economy Act 2010, Zeitschrift für Geistiges Eigentum, 2014, 48–88.

Grisse, Karina: Was bleibt von der Störerhaftung? Gewerblicher Rechtsschutz und Urheberrecht, 2017, 1073–1081.

Grisse, Karina: Internetangebotssperren, 2018 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 131, ISBN 978–3–16–155695–1.

Gärtner, Anette: BGH: Pflicht des Spediteurs zur Einwilligung in die Vernichtung beschlagnahmter Verletzungsgegenstände, Gewerblicher Rechtsschutz und Urheberrecht, 2009, 1142–1148.

Guo, Yimeei: Modern China's Copyright Law and Practice, 2017, ISBN 978–981–10–5352–8.

Habel, Dominic/Briske, Robert: „Speichern auf Zuruf" verfassungsrechtlich abgesegnet, ⟨URL: https://bit.ly/31OCivJ⟩ – Zugriff am 31.03.2021.

Hadaller, David/Regan, Kevin/Russell, Tyrel: The Necessity of Supernodes, 2005 ⟨URL: www.cs.toronto.edu/~kmregan/files/proj_supernode_paper.pdf⟩.

Haedicke, Maximilian: Patente und Piraten, 2011, ISBN 978–3–406–61391–3.

Haedicke, Maximilian/Zech, Herbert: Technische Erfindungen in einer vernetzten Welt, Gewerblicher Rechtsschutz und Urheberrecht, Beilage, 2014, 52–57.

Haertel, Thilo: Registry, Registrar, Registrant: Die große Domainbegriffssammlung Teil 3, ⟨URL: https://bit.ly/2xfsixn⟩ – Zugriff am 31.03.2021.

Handke, Christian/Girard, Yann/Mattes, Anselm: Fördert das Urheberrecht Innovation? Eine empirische Untersuchung, 2015 ⟨URL: https://www.econstor.eu/handle/10419/156626⟩.

Hansen, Christian August Holm: Analysis of Client Anonymity in the Tor Network, 2015 ⟨URL: https://brage.bibsys.no/xmlui/handle/11250/2360027⟩.

Hardy, Wojciech/Krawczyk, Michal Wiktor/Tyrowicz, Joanna: Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, 2015 ⟨URL: https://ideas.repec.org/p/war/wpaper/2015-23.html⟩.

Hardy, Wojciech/Krawczyk, Michal Wiktor/Tyrowicz, Joanna: Friends or foes? A meta-analysis of the link between „online piracy“ and sales of cultural goods, 2020 ⟨URL: https://ideas.repec.org/p/fme/wpaper/45.html⟩.

Harhoff, Dietmar et al.: Nutzung urheberrechtlich geschützter Inhalte im Internet durch deutsche Verbraucher, 2018 ⟨URL: https://www.ip.mpg.de/fileadmin/ipmpg/content/projekte/Nutzerverhalten_Kurzbericht.pdf⟩.

Harris, Colin: Institutional solutions to free-riding in peer-to-peer networks: a case study of online pirate communities, Journal of Institutional Economics, 14 2018 Nr. 5, 901–924.

Hau, Wolfgang/Poseck, Roman (Hrsg.): BeckOK BGB, 57. Auflage. 2021.

Haun, Lukas: Geht es auch ohne? Offene Netze ohne Störerhaftung? - Zwischen politischen Zielen und rechtlichen Schranken, Wettbewerb und Recht in der Praxis, 2018, 780–784.

Haunss, Sebastian/Kohlmorgen, Lars: Lobbying or politics? Political claims making in IP conflicts, In **Haunss, Sebastian/Shadlen, Kenneth C. (Hrsg.):** Politics of Intellectual Property: Contestation Over the Ownership, Use, and Control of Knowledge and Information, 2009, ISBN 978–1–849–80206–2, 107–128.

Heckmann, Dirk (Hrsg.): jurisPK-Internetrecht, 7. Auflage. 2021.

Heckmann, Jörn/Nordmeyer, Arne: Pars pro toto: Verletzung des Urheberrechtsgesetzes durch das öffentliche Zugänglichmachen von Dateifragmenten ("Chunks") in Peer-to-Peer-Tauschbörsen? Computer und Recht, 2014, 41–45.

Heckmann, Oliver/Bock, Axel: The eDonkey 2000 protocol, TU Darmstadt 2003 – Technischer Bericht ⟨URL: ftp://dmz02.kom.e-technik.tu-darmstadt.de/papers/HB02-1-paper.pdf⟩.

Heckmann, Oliver et al.: The eDonkey FileSharing Network, In Proceedings of the Workshop on Algorithms and Protocols for Efficient Peer-to-Peer Applications, GI Jahrestagung 2004, 224–228.

Heghmanns, Michael: Musiktauschbörsen im Internet aus strafrechtlicher Sicht, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2004, 14–18.

Heidrich, Joerg/Brinkert, Maike: Der Provider als Hilfssheriff? Eine kritische Analyse von Warnhinweismodellen, In Law as a Service (LaaS) - Recht im Internet- und Cloud-Zeitalter - Tagungsband Herbstakademie 2013 2013, 461–483.

Heine, Robert/Schopp, Lisa: Alle Teilnehmer eines Filesharing-Netzwerks sind Mittäter - Konferenz der Tiere, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2018, 129–129.

Heinemeyer, Dennis et al.: Kampf gegen Filesharing als Modell verfehlter Mehrfachkompensation? Zeitschrift für IT-Recht und Recht der Digitalisierung, 2012, 279–284.

Hennemann, Moritz: Die Inanspruchnahme von Zugangsvermittlern: Von der Störerhaftung zum Sperranspruch, Zeitschrift für Urheber- und Medienrecht, 2018, 754–762.

Henry, Alan: Most Popular BitTorrent Client: uTorrent, ⟨URL: https://lifehacker.com/5813348/five-best-bittorrent-applications/1705622513⟩ – Zugriff am 31.03.2021.

Herzberg, Rolf: Kritik der teleologischen Gesetzesauslegung, Neue Juristische Wochenschrift, 1990, 2525–2530.

Herzog, Roman et al. (Hrsg.): Grundgesetz Kommentar, 92. Auflage. 2020.

Hänel, Frederike: Napster und Gnutella Probleme bei der Übertragung von MP3-Dateien nach deutschem Urheberrecht, JurPC, 2000, JurPC WebDok. 245/2000, Abs. 1 – 57.

Hoeren, Thomas: Kurzgutachten zur BMWi-Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, 2012 ⟨URL: https://www.eco.de/wp-content/blogs.dir/20/files/20120227-hoeren-eco-gutachten_final-2702.pdf⟩.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, 47. Auflage. 2018.

Hoffmann, Chris: 8 Legal Uses for BitTorrent: You'd Be Surprised, ⟨URL: https://www.makeuseof.com/tag/8-legal-uses-for-bittorrent-youd-be-surprised/⟩ – Zugriff am 31.03.2021.

Hoffmann, Jan Felix: Die Haftung in der Verletzerkette, Zeitschrift für Geistiges Eigentum, 2017, 72–97.

Hoffmann, Pierre-Christian Collins: Non-Commercial Online Copyright Infringement in Canada, Internet and E-Commerce Law in Canada, 16 2015, 105–131.

Hofmann, Franz: Schadensersatz auf Basis der Lizenzanalogie im Filesharingprozess, Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2016, 20.

Hofmann, Franz: Internetanschlussinhaberhaftung Vorprozessuale „Darlegungslasten“ (Teil 2), Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2020, 355–357.

Hofmeister, Dieter: Technische Durchführbarkeit der Blockierung von Filesharing-Diensten und Hindernisse bei der Beweisführung bei Urheberrechtsverletzungen, FH Heidelberg 2006 – Technischer Bericht ⟨URL: http://wwwfh.fh-heidelberg.de/forschung/IT-Recht/gutachten-p2p-homeister.pdf⟩.

Holtkamp, Heiko: Einführung in TCP/IP, 2002 ⟨URL: http://www.rvs.uni-bielefeld.de/~heiko/tcpip/tcpip.pdf⟩.

Holzapfel, Henrik: Zur Haftung einer Mehrheit von Verletzern, Gewerblicher Rechtsschutz und Urheberrecht, 2012, 242–248.

Holznagel, Daniel: Der Konflikt zwischen Art. 15 E-Commerce-RL und pro-aktiven Verhinderungspflichten von Host-Providern, Zeitschrift für Urheber- und Medienrecht, 2018, 350–357.

Höpfner, Clemens: Gesetzesbindung und verfassungskonforme Auslegung im Arbeits- und Verfassungsrecht, Recht der Arbeit, 2018, 321–337.

Huang, Danlu: Intellectual Property Infringement on a 'Commercial Scale' in Light of the Ongoing Multilateral Agreement, 2017 ⟨URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2990006⟩.

Hunter, Jennifer L.: Shutting Down the Ex Parte Party: How to Keep BitTorrent Copyright Trolls From Abusing the Federal Court's Discovery System, The John Marshall Journal of Information Technology & Privacy Law, 31 2014, 105–131.

Husovec, Martin/Peguera, Miquel: Much Ado about Little - Privately Litigated Internet Disconnection Injunctions, International Review of Intellectual Property and Competition Law, 2015, 10–37.

Ibosiola, Damilola et al.: Movie Pirates of the Caribbean: Exploring Il-

legal Streaming Cyberlockers, CoRR, abs/1804.02679 2018 ⟨URL: http://arxiv.org/abs/1804.02679⟩.

Idris, Tarik/Altmann, Jörn: A Market-Managed Topology Formation Algorithm for Peer-to-Peer File Sharing Networks, In **Stiller, Burkhard/Reichl, Peter/Tuffin, Bruno (Hrsg.):** Performability Has its Price: 5th International Workshop on Internet Charging and QoS Technologies, ICQT 2006, 2006, Lecture Notes in Computer Science 4033: Computer Communication Networks and Telecommunications, ISBN 978–3–540–35456–7, 61–77.

Ieong, Ricci S. C. et al.: Forensic Investigation of Peer-to-Peer Networks, In **Li, Chang-Tsun (Hrsg.):** Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions, 2010, 355–378.

Issa, Tarek Alexander: Das „1-und-1-Prinzip“: Zum Verfahren nach § 101 Abs. 9 UrhG und der zivilprozessualen Verwertbarkeit von Auskünften nach § 101 Abs. 2 Satz 1 Nr. 3 UrhG in sogenannten „Reseller“-Fällen, Zeitschrift für Urheber- und Medienrecht, 2017, 390–398.

Izal, Mikel et al.: Dissecting BitTorrent: Five Months in a Torrent's Lifetime, In **Barakat, Chadi/Pratt, Ian (Hrsg.):** Passive and Active Network Measurement: 5th International Workshop, 2004, ISBN 978–3–540–24668–8, 1–11.

Jackson, Emily: Copyright ruling called 'bad news for consumers, bad news for Canada', ⟨URL: https://bit.ly/2MZPZ7B⟩ – Zugriff am 31.03.2021.

Jakobsen, Søren Sandfeld: Kalkulation von Schadensersatz und Bewertung von Beweisen in Rechtsstreiten über illegales Filesharing, ⟨URL: http://merlin.obs.coe.int/iris/2011/6/article15.en.html⟩ – Zugriff am 31.03.2021.

Jandt, Silke: Kulturflatrate - eine zulässige Gestaltung der Medienverbreitung? In **Roßnagel, Alexander (Hrsg.):** Elektronische Medien zwischen Exklusivität und Grundversorgung, 2010, Schriftenreihe des Instituts für Europäisches Medienrecht 39, 93–105.

Jeong, Gicheol/Lee, Jongsu: Estimating consumer preferences for online music services, Applied Economics, 42 2010 Nr. 30, 3885–3893.

Jia, Adele L. et al.: Fast download but eternal seeding: The reward and punishment of Sharing Ratio Enforcement, In 2011 IEEE International Conference on Peer-to-Peer Computing, 2011, 280–289.

Jünemann, Konrad: Confidential Data-Outsourcing and Self-Optimizing P2P-Networks: Coping with the Challenges of Multi-Party Systems, 2015, ISBN 978–3–7315–0328–6.

Jüngel, Marc/Geißler, Tim: Der neue Auskunftsanspruch aus § 101 UrhG unter Berücksichtigung der bisherigen Rechtsprechung, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2008, 787–792.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.): Münchner Kommentar zum StGB - Band 7, 4. Auflage. 2020.

John, Nicholas A.: File Sharing and the History of Computing: Or, Why File Sharing is Called „File Sharing“, Critical Studies in Media Communication, 31 2014 Nr. 3, 198–211.

Kaps, Reiko: Datenschützer besorgt über IPv6, ⟨URL: https://www.heise.de/newsticker/meldung/Datenschuetzer-besorgt-ueber-IPv6-1382812.html⟩ – Zugriff am 31.03.2021.

Karaganis, Joe: Media Piracy in Emerging Economies, 2011, ISBN 0984125744.

Karagiannis, Thomas et al.: File-sharing in the Internet: A characterization of P2P traffic in the backbone, 2003 – Technischer Bericht.

Karbhari, Pradnya et al.: Bootstrapping in Gnutella: A Measurement Study, In **Barakat, Chadi/Pratt, Ian (Hrsg.):** Passive and Active Network Measurement: 5th International Workshop, Berlin, Heidelberg 2004, ISBN 978–3–540–24668–8, 22–32.

Karrenberg, Daniel: The Internet Domain Name System Explained for Non-Experts, 2004 ⟨URL: https://bit.ly/31OsGRz⟩.

Keßler, Markus: Wie Netzsperren umgangen werden können, ⟨URL: https://futurezone.at/digital-life/wie-netzsperren-umgangen-werden-koennen/77.618.442⟩ – Zugriff am 31.03.2021.

Kelly, Gerard: A court-ordered graduated response system in Ireland: the beginning of the end? Journal of Intellectual Property Law & Practice, 11 2016 Nr. 3, 183–198.

Kern, Ekkehard: Welche Versicherung schützt vor Online-Abmahnung? ⟨URL: https://www.welt.de/finanzen/verbraucher/article124010766/Welche-Versicherung-schuetzt-vor-Online-Abmahnung.html⟩ – Zugriff am 31.03.2021.

Kesari, Aniket/Hoofnagle, Chris/McCoy, Damon: Deterring Cybercrime: Focus on Intermediaries, Berkeley Technology Law Journal, 32 2017, 1093–1133.

Khazaeli, Ehssan: Inhalt und Reichweite der sekundären Darlegungslast in Tauschbörsenfällen – Anmerkung zu LG Berlin, Beschluss vom 25.3.2019 - 16 S 2/19 (ZUM-RD 2019, 657), Zeitschrift für Urheber- und Medienrecht - Rechtsprechungdiesnt, 2019, 659–661.

Köhler, Sebastian: Entgrenzung des Vortrags zur sekundären Darlegungslast im Lichte des Unionsrechts? Zeitschrift für Urheber- und Medienrecht, 2018, 861–865.

Köhler, Sebastian: Die Haftung des privaten Internetanschlussinhabers zwischen Haftungsprivilegien und effektiver Rechtsverfolgung, Zeitschrift für Urheber- und Medienrecht, 2018, 27–33.

Köhler, Sebastian: Die Haftung privater Internetanschlussinhaber, 2018 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 135, ISBN 978–3–16–155973–0.

Kiersch, Phillip: Deckelung der Abmahnkosten - Unvereinbar mit der EnforcementRL? Zeitschrift für Urheber- und Medienrecht, 2018, 667–673.

Kipshagen, Alexander: Haftung bei offenem WLAN, 2017 - zugleich Diss., Schriften zum Medien- und Informationsrecht 30, ISBN 978–3–8487–4322–3.

Kirchberg, Elena: Die Störerhaftung von Internetanschlussinhabern auf dem Prüfstand, Zeitschrift für Urheber- und Medienrecht, 2012, 544–550.

Kitz, Volker: Urheberschutz im Internet und seine Einfügung in den Gesamtrechtsrahmen, Zeitschrift für Urheber- und Medienrecht, 2006, 444–450.

Klaß, Christian: Betrugsversuch oder Patent-Wahnsinn? ⟨URL: https://www.golem.de/0310/28087.html⟩ – Zugriff am 31.03.2021.

Klein, Susanne: Der Auskunftsanspruch gemäß § 101 UrhG in der Praxis - eine Bestandsaufnahme, JurPC, 2011, JurPC Web–Dok. 131/2011, Abs. 1 – 189.

Kleinz, Torsten: Das Internet-Protokoll 6 verändert die Spielregeln, ⟨URL: http://www.zeit.de/digital/datenschutz/2011-01/ipv6-vorratsdaten/komplettansicht⟩ – Zugriff am 31.03.2021.

Kleinz, Torsten: Urheberrechtsverletzungen auf Streaming-Sites: Neuer Anlauf für DNS-Sperren, ⟨URL: https://bit.ly/3yA1C9n⟩ – Zugriff am 31.03.2021.

Knies, Bernhard: BaumgartenBrandt interne Gebührenabrede bei Abmahnungen, ⟨URL: https://www.new-media-law.net/baumgartenbrandt-interne-gebuehrenabrede-bei-abmahnungen/⟩ – Zugriff am 31.03.2021.

König, Maximilian: Deckelung der Abmahnkosten in Filesharing-Verfahren - Anmerkung zu OLG Celle, Beschluss vom 12.4.2019 - 13 W 7/19 (ZUM-RD 2019, 450), Zeitschrift für Urheber- und Medienrecht - Rechtsprechungdiesnt, 2019, 452–454.

Knops, Kai-Oliver: Die Unanwendbarkeit unionsrechtswidriger Normen in Privatrechtsstreitigkeiten, Neue Juristische Wochenschrift, 2020, 2297–2302.

Koch, Alexander/Lißek, Sebastian: Das Ende des Routerzwangs, Kommunikation und Recht, 2016, 572–577.

Koch, Tobias: AG Köln: Lizenzschaden bei Filesharing auf 10 Euro pro Musiktitel begrenzt! juris PraxisReport IT-Recht, 14 2015, Anm. 4.

Kondziela, Andreas: Staatsanwälte als Erfüllungsgehilfen der Musik- und Pornoindustrie? Zeitschrift für IT-Recht und Recht der Digitalisierung, 2009, 295–300.

Kozierok, Charles M.: The TCP/IP Guide, 3. Auflage. 2005 ⟨URL: http://www.tcpipguide.com/free/index.htm⟩.

Krempl, Stefan: Filmwirtschaft startet Abschreckungskampagne gegen Raubkopierer, ⟨URL: https://bit.ly/2MefvGb⟩ – Zugriff am 31.03.2021.

Krempl, Stefan: GVU fordert Maßnahmenpaket gegen Urheberrechtsverletzer, ⟨URL: https://www.heise.de/newsticker/meldung/GVU-fordert-Massnahmenpaket-gegen-Urheberrechtsverletzer-1126924.html⟩ – Zugriff am 31.03.2021.

Krempl, Stefan: Österreich: Neue schwarz-blaue Regierung will Überwachung ausbauen, ⟨URL: https://bit.ly/2HM87fB⟩ – Zugriff am 31.03.2021.

Kreutzer, Till: Filesharing von Musikstücken und deutsches Urheberrecht, Der IT-Rechts-Berater, 2001, 136–137.

Kreutzer, Till: Napster, Gnutella & Co.: Rechtsfragen zu Filesharing-Netzen aus der Sicht des deutschen Urheberrechts de lege lata und de lege ferenda - Teil 1, Gewerblicher Rechtsschutz und Urheberrecht, 2001, 193–204.

Krügel, Tina: Der Einsatz von Angriffserkennungssystemen im Unternehmen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2017, 795–799.

Kötter, Matthias: BVerfG: Das Ende der „objektiven" Auslegungsmethode? ⟨URL: https://verfassungsblog.de/bundesverfassungsgericht-auf-methodisch-neuen-wegen/⟩ – Zugriff am 31.03.2021.

Kuntz, Wolfgang: Haftung für Filesharing im Familienverbund - Besprechung EuGH, Urteil vom 18.10.2018, C-149/17, JurPC, 2019, JurPC Web–Dok. 162/2018, Abs. 1 – 87.

Kuntz, Wolfgang: Die BGH-Entscheidung „Der Novembermann" - Auswirkungen auf Abmahnungen wegen Filesharings? JurPC, 2020, JurPC WebDok. 13/2020, Abs. 1 – 17.

Kur, Annette: Der Mißbrauch der Verbandsklagebefugnis, Gewerblicher Rechtsschutz und Urheberrecht, 1981, 558–567.

Kur, Annette: Beweislast und Beweisführung im Wettbewerbsprozeß, 1981 - zugleich Diss., Schriftenreihe zum gewerblichen Rechtsschutz 56, ISBN 3–452–18947–3.

Kur, Annette: Haftung für Rechtsverletzungen Dritter: Reformbedarf im europäischen IPR? Wettbewerb und Recht in der Praxis, 2011, 971–982.

Kur, Annette: Wer ist Pirat? Probleme des Immaterialgüterrechts, Aus Politik und Zeitgeschichte, 48 2012, 21–28.

Kur, Annette/Bomhard, Verena von/Albrecht, Friedrich (Hrsg.): BeckOK Markenrecht, 24. Auflage. 2021.

Kurose, James F./Ross, Keith: Computer Networking: A Top-Down Approach, 6. Auflage. 2013, ISBN 978–0–13–285620–1.

Kurz, Constanze: Auf Knopfdruck wird die Realität kopiert, ⟨URL: https://bit.ly/2VAz2jf⟩ – Zugriff am 31.03.2021.

Lach, Kevin Philipp: Rechtsverlust des Anschlussinhabers durch Darlegung der Anschlussnutzung durch Dritte erst im Prozess (Filesharing)? juris PraxisReport IT-Recht, 17 2017, Anm. 3.

Lahmann, Henning: Urheberrechte in CETA, 2014 ⟨URL: https://irights.info/wp-content/uploads/2014/12/Kurzgutachten-Urheberrechte-in-CETA.pdf⟩.

Lai, Pierre K. Y. et al.: Modeling the initial stage of a file sharing process on a BitTorrent network, Peer-to-Peer Networking and Applications, 7 2014 Nr. 4, 311–319.

Lal, Niharika: Illegal downloaders, you might not be criminals in India, but be careful abroad, ⟨URL: https://bit.ly/2Qh4VfD⟩ – Zugriff am 31.03.2021.

Landenberg-Roberg, Michael von/Sehl, Markus: Genetische Argumentation als rationale Praxis, Zeitschrift für rechtswissenschaftliche Forschung, 2015, 135–166.

Laoutaris, Nikolaos/Carra, Damiano/Michiardi, Pietro: Uplink Allocation Beyond Choke/Unchoke: Or How to Divide and Conquer Best, In Proceedings of the 2008 ACM CoNEXT Conference, 2008, ISBN 978–1–60558–210–8, 1–12.

Lareida, Andri/Hoßfeld, Tobias/Stiller, Burkhard: The BitTorrent Peer Collector Problem, In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, 449–455.

Laumen, Hans-Willi: Die „Beweiserleichterung bis zur Beweislastumkehr“ - Ein beweisrechtliches Phänomen, Neue Juristische Wochenschrift, 2002, 3739–3746.

Laumen, Hans-Willi: Die sog. tatsächliche Vermutung, Monatsschrift für Deutsches Recht, 2015, 1–6.

Legout, Arnaud/Urvoy-Keller, Guillaume/Michiardi, Pietro: Rarest First and Choke Algorithms Are Enough, In Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, 2006, IMC '06, ISBN 1–59593–561–4, 203–216.

Leicht, Armin: Beweisprobleme bei Urheberrechtsverletzungen von Tauschbörsennutzern in P2P-Netzwerken, Verbraucher und Recht, 2009, 346–351.

Leistner, Matthias: Die „The Pirate Bay“-Entscheidung des EuGH: ein Gerichtshof als Ersatzgesetzgeber, Gewerblicher Rechtsschutz und Urheberrecht, 2017, 755–760.

Leistner, Matthias/Grisse, Karin: Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), Gewerblicher Rechtsschutz und Urheberrecht, 2015, 19–27.

Leitner, John: A Legal and Cultural Comparison of File-Sharing Disputes in Japan and the Republic of Korea and Implications for Future Cyber-Regulation, Columbia Journal of Asian Law, 22 2008 Nr. 1, 1–55.

Leyden, John: HideMyAss defends role in LulzSec hack arrest, ⟨URL: https://www.theregister.co.uk/2011/09/26/hidemyass_lulzsec_controversy/⟩ – Zugriff am 31.03.2021.

Liang, Jian et al.: Pollution in P2P file sharing systems, In Proceedings

IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Band 2, 2005, 1174–1185.

Liberatore, Marc et al.: Forensic Investigation of Peer-to-peer File Sharing Networks, Digital Investigation, 7 2010, 95–103.

Liebowitz, Stan J.: Why the Oberholzer-Gee/Strumpf Article on File Sharing Is Not Credible, Econ Journal Watch, 13 2016 Nr. 3, 373–396.

Liebowitz, Stan J.: Responding to Oberholzer-Gee and Strumpf's Attempted Defense of Their Piracy Paper, Econ Journal Watch, 14 2017 Nr. 2, 174–195.

Lienemann, Gerhard/Larisch, Dirk: TCP/IP Grundlagen und Praxis, 2. Auflage. 2014, ISBN 978–3–944099–02–6.

Liggenga, Jan: Dutch anti-piracy unit targets ISPs, ⟨URL: https://www.theregister.co.uk/2005/05/12/dutch_piracy_lawsuits/⟩ – Zugriff am 31.03.2021.

Link, Andreas: Abmahnungen für P2P-Streaming machen die Runde: Vorsicht bei Cuevana, Popcorn Time und Co. ⟨URL: http://www.pcgameshardware.de/Filesharing-Thema-209950/News/Abmahnungen-fuer-P2P-Streaming-1121270/⟩ – Zugriff am 31.03.2021.

Liogkas, Nikitas et al.: Exploiting BitTorrent For Fun (But Not Profit), In Proceedings of IPTPS, 2006, 1–6.

Lipowski, Tilo: Struktur, Aufbau und Funktionalität des P2P-Netzwerkprotokolls FastTrack, 2007 ⟨URL: https://bit.ly/2ZF4r6E⟩.

Liu, John Zhuang/Li, Xueyao: Legal Techniques for Rationalizing Biased Judicial Decisions: Evidence from Experiments with Real Judges, Journal of Empirical Legal Studies, 16 2019 Nr. 3, 630–670.

Liu, Zhengye et al.: Understanding and Improving Ratio Incentives in Private Communities, In 2010 IEEE 30th International Conference on Distributed Computing Systems, 2010, 610–621.

Liu, Zhuang: Quantifying the Heterogeneous Effects of Piracy on the Demand for Movies, 2019 ⟨URL: https://bit.ly/3mLc6wW⟩.

Livadariu, Ioana et al.: Inferring Carrier-Grade NAT Deployment in the Wild, In IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, 2249–2257.

Livadariu, Ioana/Elmokashfi, Ahmed/Dhamdhere, Amogh: On IPv4 transfer markets: Analyzing reported transfers and inferring transfers in the wild, Computer Communications, 111 2017, 105–119.

Locher, Thomas et al.: Free Riding in BitTorrent is Cheap, In HotNets, 2006 ⟨URL: https://bit.ly/2ZHjMDH⟩.

Loewenheim, Ulrich/Leistner, Matthias/Ohly, Ansgar (Hrsg.): Urheberrecht, 6. Auflage. 2020.

Lorenz, Bernd: Abmahn- und Verteidigungsstrategien in Filesharing-Fällen, JurPC, 2013, JurPC WebDok. 132/2014, Abs. 1 – 33.

Lorz, Ralph Alexander: Die Gesetzesauslegung im Blick des Gesetzgebers? In **Baldus, Christian/Theisen, Frank/Vogel, Friederike (Hrsg.):** „Gesetzgeber“ und Rechtsanwendung, 2013, 87–110.

Lütke, Hans-Josef: Die neuere Rechtsprechung zu Streitwerten bei der Verletzung von Rechten nach dem UrhG, Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report, 2020, 337–345.

Lütke, Hans Josef/Gramlich, Ludwig: Die Haftung nach dem Zweiten Gesetz zur Änderung des TMG, Neue Justiz, 2016, 413–418.

Luo, Hong/Mortimer, Julie Holland: Copyright Enforcement: Evidence from Two Field Experiments, Journal of Economics & Management Strategy, 26 2017 Nr. 2, 499–528.

Lutz, Stefan: Identifizierung von Urheberrechtsverletzern, Datenschutz und Datensicherheit, 2012, 584–590.

Maaßen, Stefan: Urheberrechtlicher Auskunftsanspruch und Vorratsdatenspeicherung, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2009, 511–515.

Maaßen, Stefan: Access-Provider darf bereits erhobene IP-Adressen bei offenkundiger Rechtsverletzung nicht löschen, Gewerblicher Rechts-

schutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht, 2017, 565–565.

Mackey, Aaron/Schoen, Seth/Cohn, Cindy: Unreliable Informants: IP Addresses, Digital Tips and Police Raids, Electronic Frontier Foundation 2016 – Technischer Bericht.

Mahlmann, Peter/Schindelhauer, Christian: Peer-to-Peer-Netzwerke: Algorithmen und Methoden, 2007, eXamen.press, ISBN 978–3–540–33991–5.

Mantz, Reto: Anmerkung zu LG Hamburg: Störerhaftung bei ungesichertem Funknetz, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2006, 763–766.

Mantz, Reto: Rechtsfragen offener Netze, 2008 - zugleich Diss., ISBN 978–3–8664–4222–1.

Mantz, Reto: Anmerkung zu BGH: Haftung des Internetanschlussinhabers mit WLAN – Sommer unseres Lebens, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2010, 568–570.

Mantz, Reto: Anmerkung zu LG Frankfurt/M.: Ersatz für Rechtsanwaltskosten zur Verteidigung gegen Filesharing-Abmahnung, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2011, 401–404.

Mantz, Reto: Die Haftung des Betreibers eines gewerblich betriebenen WLANs und die Haftungsprivilegierung des § 8 TMG, Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report, 2013, 497–499.

Mantz, Reto: Freund oder Feind auf meiner Leitung? (Un-)Zulässigkeit des Eingriffs in den Datenstrom durch TK-Anbieter mittels Deep Packet Injection, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2015, 8–13.

Mantz, Reto: Klage gegen unbekannte Inhaber einer ausländischen Domain im Zivilprozess? Neue Juristische Wochenschrift, 2016, 2845–2848.

Mantz, Reto: Die (neue) Haftung des (WLAN-)Access-Providers nach § 8 TMG, Gewerblicher Rechtsschutz und Urheberrecht, 2017, 969–977.

Mantz, Reto/Gietl, Andreas: Anmerkung zu OLG Frankfurt/M.: Haftung des Betreibers eines Funknetzwerks, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2008, 603–609.

Mantz, Reto/Sassenberg, Thomas: Die Neuregelung der Störerhaftung für öffentliche WLANs - Eine Analyse des TMG-RefE v. 11.3.2015, Computer und Recht, 2015, 298–306.

Masnick, Mike: No Surprise: Wikileaks Leak Shows US Entertainment Industry Wrote Spain's New Copyright Law, ⟨URL: https://bit.ly/2HChVZi⟩ – Zugriff am 31.03.2021.

Mathew, Ashwin J./Cheshire, Coye: Risky Business: Social Trust and Community in the Practice of Cybersecurity for Internet Infrastructure, 2017 ⟨URL: http://hdl.handle.net/10125/41438⟩.

Mathis, Klaus: Consequentialism in Law, In **Mathis, Klaus (Hrsg.):** Efficiency, Sustainability, and Justice to Future Generations, 2011, 3–29.

Maute, Lena: Dreifache Schadens(ersatz)berechnung, 2016 - zugleich Diss., Geistiges Eigentum und Wettbewerb 45, ISBN 978–3–4522–8710–6.

Maxwell, Andy: ACE Obtains DMCA Subpoena to Unmask Operators of Major Pirate Sites, ⟨URL: https://bit.ly/3wxxGJ0⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: BitChute is a BitTorrent-Powered YouTube Alternative, ⟨URL: https://torrentfreak.com/bitchute-is-a-bittorrent-powered-youtube-alternative-170129/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: BitTorrent Owner Accused of Profiting From Movie Piracy, ⟨URL: https://torrentfreak.com/bittorrent-owner-accused-of-profiting-from-movie-piracy-200128/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Canada Prohibits Piracy Settlement Demands in ISP Copyright Notices, ⟨URL: https://bit.ly/2QRbZEu⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Canada Set For Mass BitTorrent Lawsuits, Anti-Piracy

Company Warns, ⟨URL: https://bit.ly/2VI4VX3⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: China Says It Will „Severely Strike“ Websites Involved in Piracy, ⟨URL: https://bit.ly/2IB36Iu⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Copyright Trolls Abandon Sweden in a Blaze of Bad Publicity, ⟨URL: https://torrentfreak.com/copyright-trolls-abandon-sweden-in-blaze-of-bad-publicity-161101/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Copyright Trolls Killed Off in Denmark After Supreme Court Hearing Denied, ⟨URL: https://bit.ly/2wa2cLT⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Copyright Trolls Targeted 46,200+ Alleged BitTorrent Pirates in Sweden During 2020, ⟨URL: https://bit.ly/3vnF09g⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Dallas Buyers Club Gives Up Chasing Pirates in Australia, ⟨URL: https://torrentfreak.com/dallas-buyers-club-gives-up-chasing-pirates-in-australia-160210/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Dutch Film Distributor to Target BitTorrent Users For Cash 'Fines', ⟨URL: https://bit.ly/2M03pQw⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: EU Piracy Report Suppression Raises Questions Over Transparency, ⟨URL: https://bit.ly/2xbPeOh⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Global Entertainment Giants Form Massive Anti-Piracy Coalition, ⟨URL: https://bit.ly/2s7E7Cp⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Healthy Aussie Pirates Set To Face Cash 'Fines', Poor & Sick Should Be OK, ⟨URL: https://bit.ly/2HL6cHX⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Hollywood Says Only Site-Blocking Left to Beat Piracy in New Zealand, ⟨URL: https://bit.ly/2En46xo⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Huge Torrent Tracker Calls it Quits After 12 Years, Citing Article 13, ⟨URL: https://torrentfreak.com/huge-torrent-tracker-calls-it-quits-after-12-years-citing-article-13-181207/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: IP Address Fail: ISP Doesn't Have to Hand 'Pirates' Details to Copyright Trolls, ⟨URL: https://torrentfreak.com/ip-address-fail-isp-doesnt-have-to-hand-pirates-details-to-copyright-trolls-180414/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: ISP Bombarded With 82,000+ Demands to Reveal Alleged Pirates, ⟨URL: https://bit.ly/2wkWYgB⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: ISP Lands Supreme Court Win Over Copyright Trolls, ⟨URL: https://torrentfreak.com/isp-lands-supreme-court-win-over-copyright-trolls-170505/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: ISPs Win Landmark Case to Protect Privacy of Alleged Pirates, ⟨URL: https://torrentfreak.com/isps-win-landmark-case-protect-privacy-alleged-pirates-180508/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Japan Government Presents Pirate Website Blocking Proposals, ⟨URL: https://bit.ly/2DYCSPM⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Movie Companies File Lawsuits in Canada Targeting 3,348 Alleged BitTorrent Pirates, ⟨URL: https://bit.ly/2SxsXIr⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: MPAA Wins Movie Piracy Case in China After Failed Anti-Piracy Deal, ⟨URL: https://bit.ly/2wGszLT⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Multi-National Police Operation Shuts Down Pirate Forums, ⟨URL: https://torrentfreak.com/multi-national-police-operation-shuts-down-pirate-forums-171110/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: New Zealand Prepares Consultation to Modernize Copyright Laws, ⟨URL: https://bit.ly/2BsSPsx⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: OVPN Wins Court Battle After Pirate Bay Data Demands Rejected, ⟨URL: https://torrentfreak.com/ovpn-wins-court-battle-after-pirate-bay-data-demands-rejected-200911/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Peru Authorities Shut Down First 'Pirate' Websites, Three Arrested, ⟨URL: https://bit.ly/2WiHmbO⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: The Pirate Bay Tracker Shuts Down for Good, ⟨URL: https://torrentfreak.com/the-pirate-bay-tracker-shuts-down-for-good-091117/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Police Seize Hundreds of Computers Over Pirate Movie Download in 2013, ⟨URL: https://bit.ly/2JxaTsu⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: RIAA Asks BitTorrent Inc. to Block Infringing Content, ⟨URL: https://torrentfreak.com/riaa-asks-bittorrent-inc-to-block-infringing-content-150804/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Running a Torrent Tracker For Fun Can Be a Headache, ⟨URL: https://torrentfreak.com/running-a-torrent-tracker-for-fun-can-be-a-headache-160828/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Russia Blocks 500 'Pirate' Sites in Four Months, Without a Single Court Order, ⟨URL: https://bit.ly/2BYazdS⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Russia Orders Public Tracker to Block Itself, Site Refuses, ⟨URL: https://torrentfreak.com/russia-orders-public-tracker-block-site-refuses-170211/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Sci-Hub 'Pirate Bay For Science' Security Certs Revoked by Comodo, ⟨URL: https://bit.ly/2Hto4Z3⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Seven Years of Hadopi: Nine Million Piracy Warnings, 189 Convictions, ⟨URL: https://bit.ly/2HuId0L⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Sony, Universal and Warner Ask Sky to Disconnect Pirate Subscribers, ⟨URL: https://bit.ly/2OrhEet⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: T411, France's Most-Visited Torrent Site, Has Been Shut Down, ⟨URL: https://torrentfreak.com/t411-frances-most-visited-torrent-site-has-disappeared-170627/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: UK Copyright Trolls Cite Hopeless Case to Make People Pay Up, ⟨URL: https://bit.ly/30IL6D0⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: US Embassy Threatens to Close Domain Registry Over 'Pirate Bay' Domain, ⟨URL: https://bit.ly/2VAAgLn⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Vodafone Will Implement 'Three-Strikes' For Pirates, ⟨URL: https://torrentfreak.com/vodafone-will-implement-three-strikes-for-pirates-190410/⟩ – Zugriff am 31.03.2021.

Maxwell, Andy: Will Piracy-Focused Torrent & Streaming Sites Be Affected by Article 13/17? ⟨URL: https://bit.ly/2FukvAC⟩ – Zugriff am 31.03.2021.

Mayer, Christoph M.: Urheber- und haftungsrechtliche Fragestellungen bei peer-to-peer-Tauschbörsen, 2003, ISBN 3–89700–390–2.

McCarthy, Kieren: It's official: Tor's .onion domains must be kept off the public internet, ⟨URL: https://www.theregister.co.uk/2015/10/28/onion_kept_off_public_internet/⟩ – Zugriff am 31.03.2021.

McCoy, Damon et al.; Borisov, Nikita/Goldberg, Ian (Hrsg.): Shining Light in Dark Places: Understanding the Tor Network, 2008, 63–76, ISBN 978–3–540–70630–4.

McDonald, Heather: The Big Three Record Labels, ⟨URL: https://www.thebalance.com/big-three-record-labels-2460743⟩ – Zugriff am 31.03.2021.

McDonald, Paul: Hollywood, the MPAA, and the formation of anti-piracy policy, International Journal of Cultural Policy, 22 2016 Nr. 5, 686–705.

McGuire, Mary-Rose: Beweismittelvorlage und Auskunftsanspruch nach der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des Geistigen Eigentums - Über den Umsetzungsbedarf im deutschen und österreichischen Prozessrecht, GRUR International, 2005, 15–22.

McKenzie, Jordi: Graduated response policies to digital piracy: Do they increase box office revenues of movies? Information Economics and Policy, 38 2017, 1–11.

McKiernan, Michael: Focus: Feds must take action on copyright trolls, ⟨URL: http://www.lawtimesnews.com/author/michael-mckiernan/focus-feds-must-take-action-on-copyright-trolls-13126/⟩ – Zugriff am 31.03.2021.

Mendis, Dinusha/Secchi, Davide: A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour, 2015 ⟨URL: https://bit.ly/2J4Wukz⟩.

Menegus, Bryan: Download Utopia: A 17-Year-Old File-Sharing Program Is Still the Best Place to Find Obscure Music, ⟨URL: https://gizmodo.com/download-utopia-a-17-year-old-file-sharing-program-is-1769008601⟩ – Zugriff am 31.03.2021.

Meulpolder, Michel et al.: Public and Private BitTorrent Communities: A Measurement Study, In Proceedings of the 9th International Conference on Peer-to-Peer Systems, 2010, IPTPS'10.

Meyer, Trisha: The Politics of Online Copyright Enforcement in the EU: Access and Control, 1. Auflage. 2017, Information Technology and Global Governance, ISBN 978–3–319–50973–0.

Meyerdierks, Per: Personenbeziehbarkeit statischer IP-Adressen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2015, 705–708.

Mirghani, Suzannah: The War on Piracy: Analyzing the Discursive Battles of Corporate and Government-Sponsored Anti-Piracy Media Cam-

paigns, Critical Studies in Media Communication, 28 2011 Nr. 2, 113–134.

Möllers, Thomas: Juristische Methodenlehre, 2017, ISBN 978–3–406–71626–3.

Moody, Paul: US Embassy Support for Hollywood's Global Dominance: Cultural Imperialism Redux, International Journal of Communication, 11 2017, 2912–2925.

Moon, Sun-Young/Kim, Daeup: The „Three Strikes" Policy in Korean Copyright Act 2009: Safe or Out? Washington Journal of Law, Technology & Arts, 6 2011 Nr. 3, 171–182.

Morgenstern, Holger: Zuverlässigkeit von IP-Adressen-Ermittlungssoftware, Computer und Recht, 2011, 203–208.

Moss, Gary: *Media CAT v Adams*: the CAT that did not get the cream, Journal of Intellectual Property Law & Practice, 6 2011 Nr. 11, 813–820.

Murdoch, Steven J./Anderson, Ross: Tools and Technology of Internet Filtering, In **Deibert, Ronald et al. (Hrsg.):** Access Denied: The Practice and Policy of Global Internet Filtering, 2008, 57–72.

Musielak, Hans Joachim: Die sog. tatsächliche Vermutung, Juristische Arbeitsblätter, 2010, 561–566.

Musiol, Christian: Erste Erfahrungen mit der Anwendung des § 101 IX UrhG - wann erreicht die Verletzung ein „gewerbliches Ausmaß"? Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report, 2009, 1–4.

MUSO: Global Piracy Report, 2017 ⟨URL: https://www.muso.com/wp-content/uploads/2017/04/MUSO_2017_Global_Sample_Market_Insights_report.pdf⟩.

Neglia, Giovanni et al.; Chahed, Tijani/Tuffin, Bruno (Hrsg.): A Network Formation Game Approach to Study BitTorrent Tit-for-Tat, 2007, 13–22, ISBN 978–3–540–72709–5.

Ng, Yu: DNS Lookup: How a Domain Name is Translated to

an IP Address, ⟨URL: http://blog.catchpoint.com/2014/07/01/dns-lookup-domain-name-ip-address/⟩ – Zugriff am 31.03.2021.

Ngiwlay, Wanchai/Intanagonwiwat, Chalermek/Teng-amnuay, Yunyong: Bittorrent Peer Identification Based on Behaviors of a Choke Algorithm, In Proceedings of the 4th Asian Conference on Internet Engineering, 2008, AINTEC '08, 65–74.

Nicolai, Michael: Rechtssicherheit für WLAN-Anbieter: Neuer Versuch im 3. TMGÄndG, Zeitschrift für Urheber- und Medienrecht, 2018, 33–43.

Nietsch, Thomas: Anonymität und die Durchsetzung urheberrechtlicher Ansprüche im Internet, 2014 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 87, ISBN 978–3–16–153097–5.

Nümann, Peter/Mayer, Markus A.: Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken, Zeitschrift für Urheber- und Medienrecht, 2010, 321–331.

Nordemann, Jan Bernd: Nach TMG-Reform und EuGH „McFadden", Gewerblicher Rechtsschutz und Urheberrecht, 2016, 1097–1103.

Nordemann, Jan Bernd: EuGH-Urteile *GS Media*, *Filmspeler* und *The-PirateBay*: ein neues europäisches Haftungskonzept im Urheberrecht für die öffentliche Wiedergabe, GRUR International, 2018, 526–535.

Nordemann, Jan Bernd: Die Haftung allgemeiner Zugangsprovider auf Website-Sperren, Gewerblicher Rechtsschutz und Urheberrecht, 2018, 1016–1021.

Nordemann, Jan Bernd: Liability of Online Service Providers for Copyrighted Content - Regulatory Action Needed? 2018 ⟨URL: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282017%29614207⟩.

Nordemann, Jan Bernd: Neues zur Providerhaftung im Urheberrecht, Gewerblicher Rechtsschutz und Urheberrecht, 2021, 18–23.

Nordemann, Jan Bernd/Dustmann, Andreas: To Peer Or Not To Peer, Computer und Recht, 2004, 380–388.

Nordemann, Jan Bernd/Rüberg, Michael/Schaefer, Martin: 3D-

Druck als Herausforderung für die Immaterialgüterrechte, Neue Juristische Wochenschrift, 2015, 1265–1271.

Nordemann, Jan Bernd/Waiblinger, Julian: Werbung auf Websites mit urheberrechtswidrigen Internetangeboten, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2017, 211–216.

Obergfell, Eva Inés: Gesetzliches Fundament für offene WLAN-Netze - Alle guten Dinge sind drei? Kommunikation und Recht, 2017, 361–364.

Oberholzer-Gee, Felix/Strumpf, Koleman: The effect of file sharing on record sales, revisited, Information Economics and Policy, 37 2016, 61–66.

Odell, Jolie: Downloading Frenzy in China: Gov't Blocking All Torrent Sites Soon? ⟨URL: https://readwrite.com/2009/12/10/torrent-china-government/⟩ – Zugriff am 31.03.2021.

Oechsner, Simon et al.: Pushing the performance of Biased Neighbor Selection through Biased Unchoking, In 2009 IEEE Ninth International Conference on Peer-to-Peer Computing, 2009, 301–310.

Ohly, Ansgar: „Patenttrolle" oder: Der patentrechtliche Unterlassungsanspruch unter Verhältnismäßigkeitsvorbehalt? GRUR International, 2008, 787–798.

Ohly, Ansgar: Urheberrecht in der digitalen Welt - Brauchen wir neue Regelungen zum Urheberrecht und dessen Durchsetzung? 2014, ISBN 978–3–406–66236–2.

Ohly, Ansgar: Der weite Täterbegriff des EuGH in den Urteilen „GS Media", „GS Filmspeler" und „The Pirate Bay": Abenddämmerung für die Störerhaftung? Zeitschrift für Urheber- und Medienrecht, 2017, 793–802.

Ohly, Ansgar: The broad concept of „communication to the public" in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability? GRUR International, 2018, 517–526.

Ohly, Ansgar: Unmittelbare und mittelbare Verletzung des Rechts der öffentlichen Wiedergabe nach dem „Córdoba"-Urteil des EuGH, Gewerblicher Rechtsschutz und Urheberrecht, 2018, 996–1004.

O'Neill, Patrick Howell: Tor and the rise of anonmyity networks, ⟨URL: https://www.dailydot.com/debug/tor-freenet-i2p-anonymous-network/⟩ – Zugriff am 31.03.2021.

Ory, Stephan: Massenabmahnungen schaden der Akzeptanz des Urheberrechts, In **Bullinger, Winfried et al. (Hrsg.):** Festschrift für Artur-Axel Wandtke zum 70. Geburtstag, 2013, ISBN 978–3–110–28346–4, 475–482.

Pang, Yan/Guo, Zongming; Sheng, Quan Z. et al. (Hrsg.): Single-Hop Friends Recommendation and Verification Based Incentive for BitTorrent, 2012, 703–710.

Paschold, Florian: Unionsrechtskonformität der Rechtsprechung des BGH zur sekundären Darlegungslast des Anschlussinhabers im Rahmen von Filesharing-Fällen mit Familienbezug nach der Entscheidung *Afterlife*, GRUR International, 2018, 621–636.

Patalong, Frank: Deutscher KaZaA-Nutzer muss 8000 Euro zahlen, ⟨URL: https://bit.ly/2JUT2ei⟩ – Zugriff am 31.03.2021.

Patterson, Dan: Deep packet inspection: The smart person's guide, ⟨URL: https://www.techrepublic.com/article/deep-packet-inspection-the-smart-persons-guide/⟩ – Zugriff am 31.03.2021.

Pauly, Christian: Zentrale und dezentrale Peer-to-Peer-Filesharing-Systeme im Vergleich, 2002, ISBN 978–3–638–16323–1.

Payandeh, Mehrdad: Der Schutz der Meinungsfreiheit nach der EMRK, Juristische Schulung, 2016, 690–695.

Perrin, Stephen: A critical analysis of the effect of copyright infringement on the UK film and cinema industries, Diplomarbeit, University of Sheffield 2017, ⟨URL: http://etheses.whiterose.ac.uk/19709/⟩.

Pfitzmann, Andreas/Köpsell, Stefan/Kriegelstein, Thomas: Sperrverfügungen gegen Access-Provider, TU Dresden 2008 – Technischer Bericht ⟨URL: http://www.kjm-online.de/fileadmin/Download_KJM/Service/Gutachten/Gutachten_Sperrverfuegung_Technik_2008.pdf⟩.

Piatek, Michael/Kohno, Tadayoshi/Krishnamurthy, Arvind: Challenges and Directions for Monitoring P2P File Sharing Networks - or: Why My Printer Received a DMCA Takedown Notice, In Proceedings of the 3rd Conference on Hot Topics in Security, 2008, HOTSEC'08, 12:1–12:7.

Poort, Joost et al.: Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay, Telecommunications Policy, 38 2014 Nr. 4, 383–392.

Poort, Joost et al.: Global Online Piracy Study, 2018 ⟨URL: https://www.ivir.nl/projects/global-online-piracy-study/⟩.

Poort, Joost/Weda, Jarst: Elvis Is Returning to the Building: Understanding a Decline in Unauthorized File Sharing, Journal of Media Economics, 28 2015 Nr. 2, 63–83.

Post, David G./Sandefur, Timothy: „Nice Questions" Unanswered: *Grokster*, *Sony*'s Staple Article of Commerce Doctrine, and the Deferred Verdict on Internet File Sharing, Cato Supreme Court Review, 2005, 235–261.

Price, David: Sizing the Piracy Universe, 2013 ⟨URL: https://www.netnames.com/assets/shared/whitepaper/pdf/netnames-sizing-piracy-universe-FULLreport-sept2013.pdf⟩.

Prusty, Swagatika/Levine, Brian Neil/Liberatore, Marc: Forensic Investigation of the OneSwarm Anonymous Filesharing System, In Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, CCS '11, 201–214.

Pötters, Stephan und Christensen, Ralph: Richtlinienkonforme Rechtsfortbildung und Wortlautgrenze, JuristenZeitung, 2011, 387–394.

Röß, Simon: Das vorprozessuale Schweigen bei Urheberrechtsverletzungen, Neue Juristische Wochenschrift, 2019, 1983–1987.

Rathsack, Stefan: Zur Unbilligkeit der Streitwertbegrenzung nach § 97a Abs. 3 Satz 4 UrhG in Filesharingfällen, juris PraxisReport IT-Recht, 14 2018, Anm. 6.

Raue, Benjamin: Die dreifache Schadensberechnung, 2017 - zugleich Habil., Neue Schriften zum Zivilrecht 5, ISBN 978–3–8487–3251–7.

Rauscher, Thomas/Krüger, Wolfgang (Hrsg.): Münchner Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen - Band 1, 6. Auflage. 2020.

Röckrath, Luidger: Kollegialentscheidung und Kausalitätsdogmatik, Neue Zeitschrift für Strafrecht, 2003, 641–646.

Rebiger, Simon: Freifunk: Keine Anerkennung von Gemeinnützigkeit, ⟨URL: https://netzpolitik.org/2017/freifunk-keine-anerkennung-von-gemeinnuetzigkeit/⟩ – Zugriff am 31.03.2021.

Rehbinder, Manfred: Tauschbörsen, Sharehoster und UGC-Streamingdienste, Zeitschrift für Urheber- und Medienrecht, 2013, 241–264.

Reimer, Franz: Was ist die Frage, auf die die juristische Methodenlehre eine Antwort sein will? In **Reimer, Franz (Hrsg.):** Juristische Methodenlehre aus dem Geist der Praxis? Band 1, 2016, 11–34.

Reinbacher, Tobias: Die Strafbarkeit der Vervielfältigung urheberrechtlich geschützter Werke zum privaten Gebrauch nach dem Urheberrechtsgesetz, 2007 - zugleich Diss., ISBN 978–3–428–12431–2.

Reuter, Markus: Vorratsdatenspeicherung: Große Provider speichern erstmal nicht, ⟨URL: https://netzpolitik.org/2017/vorratsdatenspeicherung-grosse-provider-speichern-erstmal-nicht/⟩ – Zugriff am 31.03.2021.

Reuther, Alexander: Aktuelle Problemfelder bei Tauschbörsenfällen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2018, 433–436.

Röhl, Christoph/Bosch, Andreas: Musiktauschbörsen im Internet - Eine Analyse der aktuellen tatsächlichen und rechtlichen Entwicklungen, Neue Juristische Online-Zeitschrift, 2008, 1197–1215.

Röhrborn, Jens/Katko, Peter: Rechtliche Anforderungen an Wireless LAN, Computer und Recht, 2002, 882–889.

Richter, Philipp et al.: A Multi-perspective Analysis of Carrier-Grade NAT Deployment, CoRR abs/1605.05606 2016.

Richter, Phillip: Empirical Analysis of the Effects and the Mitigation of IPv4 Address Exhaustion, Dissertation, Technische Universtität Berlin 2017.

Rieble, Volker: Richterliche Gesetzesbindung und BVerfG, Neue Juristische Wochenschrift, 2011, 819–822.

Rieck, Volker: State of the Art: Über die Formen der Monetarisierung von illegalen Webseiten, ⟨URL: https://bit.ly/2YzcDou⟩ – Zugriff am 31.03.2021.

Rigg, Jamie: Is the UK's new piracy email alert program dead on arrival? ⟨URL: https://www.engadget.com/2017/01/30/uk-piracy-alerts-doa/⟩ – Zugriff am 31.03.2021.

Riordan, Jaani: The Liability of Internet Intermediaries, 2016, ISBN 978–0–19–871977–9.

Roder, Verena: Die Methodik des EuGH im Urheberrecht: Die autonome Auslegung des Gerichtshofs der Europäischen Union im Spannungsverhältnis zum nationalen Recht, 2016 - zugleich Diss., Geistiges Eigentum und Wettbewerbsrecht 114, ISBN 978–3–16–154281–7.

Roggenkamp, Jan Dirk: Haftung der Betreiber privater WLAN-Hotspots, juris PraxisReport IT-Recht, 12 2006, Anm. 3.

Rüthers, Bernd: Methodenfragen als Verfassungsrecht, Zeitschrift für Logik und Juristische Methodenlehre, Allgemeine Rechts- und Staatslehre, Kommunikations-, Normen- und Handlungstheorie, Soziologie und Philosophie des Rechts, 2009, 253–283.

Rüthers, Bernd: Trendwende im BVerfG? Über die Grenzen des „Richterstaates", Neue Juristische Wochenschrift, 2009, 1461–1462.

Rüthers, Bernd: Klartext zu den Grenzen des Richterrechts, Neue Juristische Wochenschrift, 2011, 1856–1858.

Rüthers, Bernd: Die heimliche Revolution vom Rechtsstaat zum Richterstaat, Band 2, 2016.

Rüthers, Bernd: Miniatur: „Das Gesetz ist oft klüger als seine Verfasser“, Zeitschrift für die gesamte Privatrechtswissenschaft, 2016, 383–384.

Rüthers, Felix: Konferenz der Tiere - Das jüngste BGH-Urteil zum Thema Filesharing, Kommunikation und Recht, 2018, 308–309.

Sachs, Marcus et al.: Securing IM and P2P Applications for the Enterprise, 1. Auflage. 2006, ISBN 1–59749–017–2.

Safferling, Christoph: Audiatur et altera pars - die prozessuale Waffengleichheit als Prozessprinzip? Neue Zeitschrift für Strafrecht, 2004, 181–188.

Sag, Matthew: Copyright Trolling, An Empirical Study, Iowa Law Review, 100 2015, 1105–1147.

Sag, Matthew/Haskell, Jake: Defense Against the Dark Arts of Copyright Trolling, Iowa Law Review, 103 2018, 571–661.

Sandor, René: Datenspeicherung und urheberrechtliche Durchsetzungsansprüche, 2012 - zugleich Diss., Geistiges Eigentum und Wettbewerb 30, ISBN 978–3–452–27820–3.

Sandvine: Global Internet Phenomena Report Spring 2011, 2011 ⟨URL: https://www.sandvine.com/hubfs/downloads/archive/2011-1h-global-internet-phenomena-report.pdf⟩.

Sandvine: Global Internet Phenomena Asia-Pacific & Europe 2016, 2016 ⟨URL: https://www.sandvine.com/hubfs/downloads/archive/2016-global-internet-phenomena-apac-mea.pdf⟩.

Sandvine: The Global InternetPhenomena Report COVID-19 Spotlight, 2020 ⟨URL: https://www.sandvine.com/covid-internet-spotlight-report⟩.

Saroiu, Stefan/Gummadi, P. Krishna/Gribble, Steven D.: A Measurement Study of Peer-to-Peer File Sharing Systems, SPIE Proceedings, 4673 2002 ⟨URL: https://people.mpi-sws.org/~gummadi/papers/p2ptechreport.pdf⟩.

Sassenberg, Thomas/Mantz, Reto: WLAN und Recht, 2014, ISBN 978–3–503–15660–3.

Sawall, Achim: Popcorn-Time-Nutzer zahlen in Vergleich 690 Euro, ⟨URL: https://bit.ly/3vpTeaf⟩ – Zugriff am 31.03.2021.

Scanlon, Mark/Hannaway, Alan/Kechadi, Tahar: A week in the Life of the Most Popular BitTorrent Swarms, 2010 ⟨URL: https://forensicsandsecurity.com/papers/AWeekInTheLifeOfTheMostPopularBitTorrentSwarms.pdf⟩.

Schaub, Renate: Sekundäre Darlegungslast und Interessenabwägung beim Filesharing über den Familienanschluss, Neue Juristische Wochenschrift, 2018, 17–19.

Scheder-Bieschin, Felix: Modernes Filesharing: Störerhaftung und Auskunftspflicht von Anonymisierungsdiensten, 2014 - zugleich Diss., ISBN 978–3–9559–9000–8.

Schäfer, Carsten: Strafe und Prävention im Bürgerlichen Recht, Archiv für die civilistische Praxis, 2002, 397–434.

Schiff, Brett: Copyright Alert System: Six-Strikes and Forced Arbitration Might Not Be the Answer, Cardozo Journal of Conflict Resolution, 16 2014, 909–938.

Schirrmacher, Dennis: Details zur KRACK-Attacke: WPA2 ist angeschlagen, aber nicht gänzlich geknackt, ⟨URL: https://bit.ly/2gMqDYo⟩ – Zugriff am 31.03.2021.

Schmitz, Sandra V.I.: The Struggle in Online Copyright Enforcement: Problems and Prospects, 2015, Luxemburger Juristische Studien, ISBN 978–3–8487–2428–4.

Schneider, Adrian: Wie IPv6 das Medienrecht verändern wird, ⟨URL: https://www.telemedicus.info/article/1934-Wie-IPv6-das-Medienrecht-veraendern-wird.html⟩ – Zugriff am 31.03.2021.

Schneider, Stefan: Was der Gesetzgeber wollte! In **Baldus, Christian/Theisen, Frank/Vogel, Friederike (Hrsg.):** „Gesetzgeber“ und Rechtsanwendung, 2013, 111–123.

Schoene, Volker: EuGH: Ausschluss der Weitergabe personenbezogener Internet-Verkehrsdaten für zivilrechtliche Verfolgung von Urheber-

rechtsverletzungen ist gemeinschaftsrechtskonform, Fachdienst Gewerblicher Rechtsschutz 2007.

Schoffer, Filemon: How expiring patents are ushering in the next generation of 3D printing, ⟨URL: https://tcrn.ch/2c4scwz⟩ – Zugriff am 31.03.2021.

Schreiner, Rüdiger: Computer-Netzwerke, 6. Auflage. München 2016, ISBN 978–3–446–44827–8.

Schöttle, Valeria: Das neue russische Anti-Piraterie-Gesetz zum Schutz von Filmen im Internet, GRUR International, 2014, 119–124.

Schäufele, Maximilian: Zur Strafbarkeit des Raubkopierens im Internet, 2013 - zugleich Diss., Kriminalwissenschaftliche Schriften 38.

Schulte-Nölke, Hans/Henning-Bodewig, Frauke/Podszun, Rupprecht: Evaluierung der verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, 2017 ⟨URL: https://bit.ly/2WZfkOW⟩.

Schulze, Hendrick/Mochalski, Klaus: ipoque Internet Study 2007, 2007.

Schulze, Hendrick/Mochalski, Klaus: ipoque Internet Study 2008/2009, 2009.

Schulzki-Haddouti, Christiane: Auswirkungen von Raubkopien: EU-Kommission unterdrückt Piraterie-Studie, ⟨URL: https://bit.ly/2wL5Iu6⟩ – Zugriff am 31.03.2021.

Schwartmann, Rolf: Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, 2012 ⟨URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/warnhinweise.html⟩.

Säcker, Franz Jürgen et al. (Hrsg.): Münchner Kommentar zum Bürgerlichen Gesetzbuch - Band 1, 8. Auflage. 2018.

Säcker, Franz Jürgen et al. (Hrsg.): Münchner Kommentar zum Bürgerlichen Gesetzbuch - Band 2, 8. Auflage. 2019.

Säcker, Franz Jürgen et al. (Hrsg.): Münchner Kommentar zum Bürgerlichen Gesetzbuch - Band 5/2, 8. Auflage. 2020.

Säcker, Franz Jürgen et al. (Hrsg.): Münchner Kommentar zum Bürgerlichen Gesetzbuch - Band 6, 8. Auflage. 2020.

Seekamp, Michalina: Die Trägheit der deutschen Musikunternehmen bei technologischem Wandel: Eine Analyse aus branchenkultureller Perspektive, 2018 - zugleich Diss., ISBN 978–3–658–20687–1.

Seemann, Michael: WLAN-Gastzugang einrichten - so geht's, ⟨URL: https://bit.ly/2Jyi1VA⟩ – Zugriff am 31.03.2021.

Senftleben, Martin: Filterverpflichtungen nach der Reform des europäischen Urheberrechts - Das Ende der freien Netzkultur? Zeitschrift für Urheber- und Medienrecht, 2019, 369–374.

Sesing, Andreas: Mehr Rechtssicherheit für Betreiber von (kostenlosen) Funknetzwerken? Zeitschrift für IT-Recht und Recht der Digitalisierung, 2015, 423–428.

Sesing, Andreas: Verantwortlichkeit für offenes WLAN, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2016, 507–512.

Sesing, Andreas: Die Reichweite des Richtervorbehalts für urheberrechtliche Auskunftsansprüche gegen Access-Provider, Neue Juristische Wochenschrift, 2018, 754–756.

Sesing, Andreas/Baumann, Jonas S.: Sperranspruch statt Störerhaftung? Eine Analyse zur Reichweite der Änderungen des 3. TMG-ÄndG, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2017, 583–589.

Sesing, Andreas/Baumann, Jonas S.: Die Haftung von Access-Providern unter Geltung des neuen § 8 TMG, Kommunikation und Recht, 2018, 461–466.

Severance, Charles R.: Introduction to Networking, 2015, ISBN 978–1–5116–5494–4.

Skogh, Hans-Emil et al.: Fast Freenet: improving Freenet performance by preferential partition routing and file mesh propagation, In Cluster

Computing and the Grid, 2006. CCGRID 06. Sixth IEEE International Symposium on, Band 2, 2006, 8–16.

Sobiraj, Lars: Share-Online.biz: Staatsanwaltschaft will Top-Uploader verfolgen, ⟨URL: https://tarnkappe.info/share-online-biz-staatsanwaltschaft-will-top-uploader-verfolgen/⟩ – Zugriff am 31.03.2021.

Solmecke, Christian: boerse.bz - Uploader wurden über die E-Mail Adressen ermittelt, ⟨URL: https://www.wbs-law.de/internetrecht/boerse-bz-57361/⟩ – Zugriff am 31.03.2021.

Solmecke, Christian: Duckload Premium Nutzer aufgepasst - Das LKA Dresden hat die Nutzerdaten ausgewertet, ⟨URL: https://bit.ly/2EjU7IP⟩ – Zugriff am 31.03.2021.

Solmecke, Christian: Filesharing - Straf- und zivilrechtliche Konsequenzen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2006, XXIII–XXIV.

Solmecke, Christian: Anmerkung zu AG Köln: Begrenzung des Lizenzschadens bei Filesharing, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2014, 483–486.

Solmecke, Christian: Der Redtube-Fall, Computer und Recht, 2014, 137–139.

Solmecke, Christian/Bärenfänger, Jan: Urheberrechtliche Schutzfähigkeit von Dateifragmenten, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2011, 567–573.

Solmecke, Christian/Rüther, Felix/Büring, Harald: Filesharing: Nachforschungspflichten des Anschlussinhabers Rechtsprechungsüberblick zu den Anforderungen an die sekundäre Darlegungslast, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2016, 153–156.

Solmecke, Christian/Rüther, Felix/Herkens, Thomas: Uneinheitliche Darlegungs- und Beweislast in Filesharing-Verfahren, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2013, 217–221.

Soppe, Martin: Wann und wie haften Sharehosting-Dienste? ⟨URL: https://bit.ly/2DJyJyW⟩ – Zugriff am 31.03.2021.

Spindler, Gerald: Urheberrecht und Tauschplattformen im Internet, Juristenzeitung, 2002, 60–70.

Spindler, Gerald: Rechtsprobleme und wirtschaftliche Vertretbarkeit einer Kulturflatrate, 2014, ISBN 978–3–86395–128–3.

Spindler, Gerald: Das neue Telemediengesetz - WLAN-Störerhaftung endgültig adé, Neue Juristische Wochenschrift, 2017, 2305–2309.

Spindler, Gerald: Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz - europarechtswidrig? Zeitschrift für Urheber- und Medienrecht, 2017, 473–487.

Spindler, Gerald: Fortentwicklung der Haftung für Internetanschlüsse, Gewerblicher Rechtsschutz und Urheberrecht, 2018, 16–20.

Spindler, Gerald: Störerhaftung für Access-Provider reloaded, Gewerblicher Rechtsschutz und Urheberrecht, 2018, 1012–1016.

Spindler, Gerald: Die neue Urheberrechts-Richtlinie der EU, insbesondere „Upload-Filter“ - Bittersweet? Computer und Recht, 2019, 277–291.

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 3. Auflage. 2015.

Spoenle, Jan: Haftet der Betreiber eines TOR-Exit-Nodes als Störer? juris PraxisReport IT-Recht, 25 2017, Anm. 4.

SSAC, ICANN: DNS Blocking: Benefits Versus Harms, 2011 ⟨URL: https://www.icann.org/en/system/files/files/sac-050-en.pdf⟩.

Stadler, Thomas: Filesharing: Wie zuverlässig ist die Ermittlung des Anschlussinhabers? ⟨URL: http://www.internet-law.de/2010/02/filesharing-wie-zuverlassig-ist-die-ermittlung-des-anschlussinhabers.html⟩ – Zugriff am 31.03.2021.

Stalla-Bourdillon, Sophie: Cartier et al v Sky et al 2014: what if the ISPs' blocking systems did not implement Shallow Packet Inspection technologies? ⟨URL: https://bit.ly/2YHkK2q⟩ – Zugriff am 31.03.2021.

Stalla-Bourdillon, Sophie/Papadaki, Evangelia/Chown, Tim: From porn to cybersecurity passing by copyright: How mass surveillance tech-

nologies are gaining legitimacy. . .: The case of Deep packet inspection technologies, Computer Law & Security Review, 30 2014, 670–686.

Stamatoudi, Irini: ACTA, internet service providers and the acquis communautaire, In **Rosén, Jan (Hrsg.):** Intellectual Property at the Crossroads of Trade, 2012, ATRIP Intellectual Property, ISBN 978–1–78195–168–2, 237–263.

Stang, Felix/Hühner, Sebastian: Haftung des Anschlussinhabers für fremde Rechtsverletzungen beim Betrieb eines ungesicherten WLAN-Funknetzes, Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report, 2008, 273–275.

Statt, Nick: Popcorn Time for your browser makes illegal movie streaming even easier, ⟨URL: https://www.theverge.com/2015/10/19/9571359/popcorn-time-online-browser-version-streaming⟩ – Zugriff am 31.03.2021.

Steele, Robert: If You Think Piracy Is Decreasing, You Haven't Looked at the Data... ⟨URL: https://www.digitalmusicnews.com/2015/07/16/if-you-think-piracy-is-decreasing-you-havent-looked-at-the-data-2/⟩ – Zugriff am 31.03.2021.

Stein, Ingmar: Der Auskunftsanspruch gegen Access-Provider nach § 101 UrhG, 2012 - zugleich Diss., Studien zum gewerblichen Rechtsschutz und zum Urheberrecht 95, ISBN 978–3–8300–6559–3.

Steinebach, Martin/Zmudzinski, Sascha: Auswirkung einer Bagatellklausel auf die Verfolgbarkeit von Urheberrechtsverletzungen in Internet-Tauschbörsen, August 2006 ⟨URL: www.mpr-frankfurt.de/presse/ipsi/fraunhofer_gutachten_bagatellklausel_final.pdf⟩.

Steinmetz, Ralf/Wehrle, Klaus: Peer-to-Peer Systems and Applications, Berlin, Heidelberg 2005, ISBN 978–3–540–29192–3.

Straube, Jens: Gnutella und BitTorrent: Eine Analyse der Filesharing-Protokolle Gnutella und BitTorrent, 2009, ISBN 978–3–6390–6123–9.

Strowel, Alain: Peer-to-peer file sharing and secondary liability in copyright law, Cheltenham 2009, ISBN 978–1–84720–562–0.

Sullivan, Andrew: IPv6 will allow them to track you down. Not! ⟨URL:

https://www.networkworld.com/article/2172931/tech-primers/ipv6-will-allow-them-to-track-you-down---not-.html⟩ – Zugriff am 31.03.2021.

Suwelack, Felix: Die ökonomische Analyse des Filesharings und ihre Bedeutung für das europäische Urheberrecht, 2018 - zugleich Diss., Studien zum gewerblichen Rechtsschutz und Urheberrecht 142, ISBN 978–3–8300–9755–6.

Tanenbaum, Andrew S./Wetherall, D.: Computer networks, 2011, ISBN 978–0–13–212695–3.

Tham, Irene: High Court throws out Hollywood movie piracy case, ⟨URL: https://www.straitstimes.com/singapore/high-court-throws-out-hollywood-movie-piracy-case⟩ – Zugriff am 31.03.2021.

Thiesen, Michael: Wie hoch ist der Preis der Anonymität? Zeitschrift für IT-Recht und Recht der Digitalisierung, 2014, 803–809.

Thoma, Jörg: IPv6 ist noch nicht genügend getestet, ⟨URL: https://www.golem.de/1112/88043.html⟩ – Zugriff am 31.03.2021.

TrustedShops: Abmahnungen im Online-Handel 2017, ⟨URL: https://cdn2.hubspot.net/hubfs/603347/1-TX_B2B/Whitepaper/171123_TEX_Abmahnstudie%202017.pdf⟩.

Tschmuck, Peter: 10 Jahre Napster - Ein Rückblick (Teil 5), ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2009/08/04/10-jahre-napster-ein-ruckblick-teil-5/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 1: KaZaA und Grokster, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/07/14/der-kampf-der-musikindustrie-gegen-filesharing-co-teil-1/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 2: LimeWire, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/07/14/

der-kampf-der-musikindustrie-gegen-filesharing-co-teil-1/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 3: Suprnova und EliteTorrent, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/08/04/der-kampf-der-musikindustrie-gegen-filesharing-co-teil-3/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 4: Torrentspy und isoHunt, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/08/21/der-kampf-der-musikindustrie-gegen-filesharing-co-teil-4/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 7: Usenet, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/09/15/der-kampf-der-musikindustrie-gegen-filesharing-co-teil-7/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Der Kampf der Musikindustrie gegen Filesharing & Co. - Teil 8: Rapidshare, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2014/09/25/der-kampf-der-musikindustrie-gegen-filesharing-co-teil-8/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Musik-Filesharing: Das Abmahnwesen in Deutschland – Teil 2, ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2015/11/12/musik-filesharing-das-abmahnwesen-in-deutschland-teil-2/⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Die US-Musikindustrie vs. die FilesharerInnen - Teil 1: Die RIAA vs. John Doe, ⟨URL: https://bit.ly/2JV8Ttp⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Die US-Musikindustrie vs. die FilesharerInnen - Teil 2: Der Fall Jammie ThomasRasset, ⟨URL: https://bit.ly/2LWqMum⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Die US-Musikindustrie vs. die FilesharerInnen - Teil 3: Der Fall Joel Tenenbaum, ⟨URL: https://bit.ly/2YJhjrX⟩ – Zugriff am 31.03.2021.

Tschmuck, Peter: Die US-Musikindustrie vs. die FilesharerInnen - Teil 4: Cui bono? ⟨URL: https://musikwirtschaftsforschung.wordpress.com/2015/03/25/die-us-musikindustrie-vs-die-filesharerinnen-teil-4-cui-bono/⟩ – Zugriff am 31.03.2021.

Tyra, Frank: Ausgewählte Probleme aus der Abmahnpraxis bei Privatnutzungen in Musiktauschsystemen, Zeitschrift für Urheber- und Medienrecht, 2009, 934–944.

Van Der Sar, Ernesto: Beating Internet Censors With BitTorrent's Maelstrom Browser, ⟨URL: https://bit.ly/2HGqlPu⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent and Tron Hope Other Clients Will Embrace 'Paid' Seeding, ⟨URL: https://bit.ly/2x9qm9L⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent 'Copyright Troll' Lawsuits Skyrocket In Sweden, ⟨URL: https://torrentfreak.com/bittorrent-copyright-troll-lawsuits-skyrocket-in-sweden-200214/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent Is Reportedly Selling for $ 140 Million (Update), ⟨URL: https://torrentfreak.com/bittorrent-is-reportedly-selling-for-140-million-180619/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent Piracy Lawsuit Morphs into Attack on Dragon Box and Resellers, ⟨URL: https://bit.ly/3wz9gib⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent Pirate Ordered to Pay $1.5 Million Damages For Sharing 10 Movies, ⟨URL: https://bit.ly/2YN9VMn⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent Still Dominates Inter-

net's Upstream Traffic, ⟨URL: https://torrentfreak.com/bittorrent-still-dominates-internets-upstream-traffic-151208/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent Unveils New Token to Pay for Faster Downloads, ⟨URL: https://torrentfreak.com/bittorrent-unveils-new-token-to-pay-for-faster-downloads-190103/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: BitTorrent's Future? DHT, PEX and Magner Links Explained, ⟨URL: https://torrentfreak.com/bittorrents-future-dht-pex-and-magnet-links-explained-091120/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Cloudflare Faces Lawsuit For Assisting Pirate Sites, ⟨URL: https://torrentfreak.com/cloudflare-faces-lawsuit-for-assisting-pirate-sites-160823/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Comcast Explains How It Deals With Persistent Pirates, ⟨URL: https://torrentfreak.com/comcast-explains-how-it-deals-with-persistent-pirates-180210/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Copyright Holders Want ISPs to Police Pirate Sites and Issue Warnings, ⟨URL: http://bit.ly/2JvH3V5⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: 'Copyright Trolls' Enter Brazil Demanding Money from Suspected Pirates, ⟨URL: https://bit.ly/3wvVBIT⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Copyright Trolls Obtained Details of 200,000 Finnish Internet Users, ⟨URL: http://bit.ly/2VKhzVS⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Court Orders Aussie ISPs to Block Dozens of Pirate Sites, ⟨URL: https://torrentfreak.com/court-orders-aussie-isps-to-block-dozens-of-pirate-sites-170818/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Court Orders PayPal to Restrain Pirate Site Funds, ⟨URL: https://torrentfreak.com/court-orders-paypal-to-restrain-pirate-site-funds-180709/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: COVID-19 'Lockdowns' Directly Impacted Torrent Download Numbers in Several Countries, ⟨URL: https://bit.ly/2RQ22HT⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Dallas Buyers Club Loses Piracy Lawsuit, IP-Address is Not Enough, ⟨URL: http://bit.ly/30Db2Q6⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Danish ISPs Stand Up Against „Mafia-Like" Copyright Trolls, ⟨URL: https://torrentfreak.com/danish-isps-stand-up-against-mafia-like-copyright-trolls-170530/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Dutch ISP Does Not Have to Expose Alleged Pirates, Court Rules, ⟨URL: https://bit.ly/3iKjn02⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: „Pirate Sites Generate $111 Million In Ad Revenue a Year", ⟨URL: https://torrentfreak.com/pirate-sites-generate-111-million-in-ad-revenue-a-year-171005/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: „Shut Down The Pirate Bay", Founder Says, ⟨URL: https://torrentfreak.com/shut-down-the-pirate-bay-founder-says-130708/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Fragmented Streaming Landscape Keeps Piracy Relevant, Research Suggests, ⟨URL: https://bit.ly/3fQ5eLN⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: French Minister of Culture Calls For Pirate Streaming Blacklist, ⟨URL: https://bit.ly/2IzPj4D⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Game of Thrones Sets New Tor-

rent Swarm Record, ⟨URL: https://torrentfreak.com/game-of-thrones-sets-new-torrent-swarm-record-140415/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Google Asked to Remove 3 Billion „Pirate“ Search Results, ⟨URL: https://torrentfreak.com/google-asked-to-remove-3-billion-pirate-search-results-171018/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Google Categorically Refuses to Remove The Pirate Bay's Homepage, ⟨URL: http://bit.ly/2Wg2z65⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Google Says It Can't Filter Pirated Content Proactively, ⟨URL: https://torrentfreak.com/google-says-it-cant-filter-pirated-content-proactively-171202/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Hollywood Studios Get ISP Blocking Order Against Rarbg in India, ⟨URL: http://bit.ly/2QhaTNS⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: How 'Anonymous' is a Seedbox Provider? ⟨URL: https://torrentfreak.com/how-anonymous-is-your-seedbox-provider-200725/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: How The US Pushed Sweden to Take Down The Pirate Bay, ⟨URL: https://torrentfreak.com/how-the-us-pushed-sweden-to-take-down-the-pirate-bay-171212/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Irish Supreme Court Okays Three-Strikes Anti-Piracy Scheme, ⟨URL: https://torrentfreak.com/irish-supreme-court-backs-three-strikes-anti-piracy-scheme-130704/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: ISP Doesn't Have to Expose Alleged BitTorrent Pirates, Finnish Court Rules, ⟨URL: http://bit.ly/2QhISWb⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: ISP Wants EU Court Ruling on Identifying „Pirating“ Subscribers, ⟨URL: https://bit.ly/2x6ro6s⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: ISPs and Movie Industry Prepare Canadian Pirate Site Blocking Deal, ⟨URL: http://bit.ly/2QgclQc⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: The KickassTorrents Shutdown, One Year Later, ⟨URL: https://torrentfreak.com/the-kickasstorrents-shutdown-one-year-later-170720/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Media Companies Track Pirated Downloads For Marketing Purposes, ⟨URL: http://bit.ly/30zu9e6⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Movie Company Has No Right to Sue, Accused Pirate Argues, ⟨URL: https://torrentfreak.com/movie-company-has-no-right-to-sue-accused-pirate-argues-171208/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Movie Studios Are Suing Canadian BitTorrent Users, But That's Nothing New, ⟨URL: https://bit.ly/3fjmWIu⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: National Assembly 'Kills' French Three-Strikes Anti Piracy Law, ⟨URL: https://torrentfreak.com/french-kill-three-strikes-anti-piracy-law-160502/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Nearly 4,000 Pirate Sites Are Blocked by ISPs Around The World, ⟨URL: https://torrentfreak.com/nearly-4000-pirate-sites-are-blocked-by-isps-around-the-world-190210/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: New MPA Subpoena Targets Private BitTorrent Tracker & Locally Significant Pirate Sites, ⟨URL: https://bit.ly/34iU3FZ⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: PeerTube: A 'Censorship' Resistent

YouTube Alternative, ⟨URL: https://torrentfreak.com/peertube-a-censorship-resistent-youtube-alternative-180623/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Piracy Debt Collectors Back Off After Massive Backlash in Finland, ⟨URL: https://bit.ly/3oPZjKN⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: The Pirate Bay Runs on 21 „Raid-Proof“ Virtual Machines, ⟨URL: https://torrentfreak.com/the-pirate-bay-runs-on-21-raid-proof-virtual-machines-140921/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Pirate Bay Simplifies Circumvention of ISP Blockades, ⟨URL: https://torrentfreak.com/pirate-bay-simplifies-circumvention-of-isp-blockades-120522/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: PureVPN Explains How it Helped the FBI Catch a Cyberstalker, ⟨URL: https://torrentfreak.com/purevpn-explains-how-it-helped-the-fbi-catch-a-cyberstalker-171016/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: RIAA Orders WhoisGuard to Identify Torrent Site Owner, ⟨URL: https://torrentfreak.com/riaa-orders-whoisguard-to-identify-torrent-site-owner-120114/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Sci-Hub Loses Domain Names, But Remains Resilient, ⟨URL: https://torrentfreak.com/sci-hub-loses-domain-names-but-remains-resilient-171122/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: South Korea Expands Site Blocking Efforts with SNI Eavesdropping, ⟨URL: https://bit.ly/3hY6ZsS⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Switzerland Hopes New Law Will Keep it Off U.S. 'Pirate Watchlist', ⟨URL: http://bit.ly/2LZe7qu⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Switzerland Urges U.S. to Remove it From its 'Pirate Watchlist', ⟨URL: https://torrentfreak.com/switzerland-urges-us-to-remove-pirate-watchlist-200228/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Tech Giants Warn US Govt. Against Onerous Copyright Laws, ⟨URL: https://torrentfreak.com/tech-giants-warn-us-govt-against-onerous-copyright-laws-190209/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Thunder Blasts uTorrent's Market Share Away, ⟨URL: https://torrentfreak.com/thunder-blasts-utorrents-market-share-away-091204/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Top 10 Most Popular Torrent Sites of 2017, ⟨URL: https://torrentfreak.com/top-10-most-popular-torrent-sites-of-2017-170107/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: UK „Piracy Warnings" Are Coming This Month; Here's How it Works, ⟨URL: https://torrentfreak.com/uk-piracy-warnings-coming-month-heres-works-170111/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: UK ISPs Sent a Million Piracy Alert Emails, ⟨URL: https://torrentfreak.com/uk-isps-sent-a-million-piracy-alert-emails-190208/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Ukraine Faces Call for US Trade Sanctions over Online Piracy, ⟨URL: https://torrentfreak.com/ukraine-faces-call-us-trade-sanctions-over-online-piracy-170918/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: US Online Piracy Lawsuits Break Record Numbers, ⟨URL: https://torrentfreak.com/us-online-piracy-lawsuits-break-record-numbers-180704/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: The US 'Six Strikes' Anti-Piracy

Scheme is Dead, ⟨URL: https://torrentfreak.com/the-us-six-strikes-anti-piracy-scheme-is-dead-170128/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: uTorrent & BitTorrent Surge to 150 Million Monthly Users, ⟨URL: https://torrentfreak.com/bittorrent-surges-to-150-million-monthly-users-120109/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: WebTorrent Brings BitTorrent to the Web, Impresses Netflix, ⟨URL: https://torrentfreak.com/webtorrent-brings-bittorrent-to-the-web-impresses-netflix-151213/⟩ – Zugriff am 31.03.2021.

Van Der Sar, Ernesto: Wrongfully Accused 'Pirate' Wants 62,818 Compensation, ⟨URL: https://torrentfreak.com/wrongfully-accused-pirate-wants-62818-compensation-180807/⟩ – Zugriff am 31.03.2021.

Van Hoecke, Mark: Methodology of Comparative Legal Research, Law and Method, 12 2015, 1–35.

Van Overwalle, Geertrui/Leys, Reinout: 3D Printing and Patent Law: A Disruptive Technology Disrupting Patent Law? International Review of Intellectual Property and Competition Law, 2017, 504–537.

Varvello, Matteo/Steiner, Moritz: Traffic Localization for DHT-Based BitTorrent Networks, In **Domingo-Pascual, Jordi et al. (Hrsg.):** NETWORKING 2011, 2011, ISBN 978–3–642–20798–3, 40–53.

Verweyen, Urs: Probleme bei der (notwendigen) Anwendung der Novembermann-Rechtsprechung des BGH auf Filesharing-Massenabmahnungen, JurPC, 2020, JurPC WebDok. 29/2020, Abs. 1 – 17.

Verweyen, Urs: Von Angelegenheiten und Gegenständen: Zur kostenrechtlich „selben Angelegenheit" i.S.v. § 15 Abs.2 RVG, Wettbewerb und Recht in der Praxis, 2020, 12–15.

Vincent, James: BitTorrent unveils new live-streaming platform for peer-to-peer broadcasts, ⟨URL: https://www.theverge.com/2016/5/

17/11689158/bittorrent-live-streaming-video-platform⟩ – Zugriff am 31.03.2021.

Völzmann-Stickelbrock, Barbara: Beweiserleichterungen durch tatsächliche Vermutungen - Eine Analyse der aktuellen Rechtsprechung zur Darlegungs- und Beweislast bei Urheberrechtsverletzungen via Internetanschluss, In **Meller-Hannich, Caroline (Hrsg.):** Rechtslage - Rechtserkenntnis - Rechtsdurchsetzung, Festschrift für Eberhard Schilken zum 70. Geburtstag, 2015, 539–552.

Vorwerk, Volker/Wolf, Christian (Hrsg.): BeckOK ZPO, 40. Auflage. 2021.

vzvb: Untersuchung der urheberrechtlichen Regelungen des Gesetzes gegen unseriöse Geschäftspraktiken, Oktober 2016 ⟨URL: https://www.vzbv.de/sites/default/files/untersuchung-gesetz_gegen_unserioese_geschaeftspraktiken-2016-10-04.pdf⟩.

Wagner, Gerhard: Prävention und Verhaltenssteuerung durch Privatrecht - Anmaßung oder legitime Aufgabe? Archiv für die civilistische Praxis, 2006, 352–476.

Wagner, Gerhard: Haftung von Plattformen für Rechtsverletzungen (Teil 1), Gewerblicher Rechtsschutz und Urheberrecht, 2020, 329–338.

Walz, Christian: Das Ziel der Auslegung und die Rangfolge der Auslegungskriterien, Zeitschrift für das Juristische Studium, 2010, 482–490.

Wander, Matthäus/Boelmann, Christopher/Weis, Torben: Domain Name System without Root Servers, 2017 ⟨URL: https://www.vs.uni-due.de/paper/2017_Wander_Rootless_DNS.pdf⟩.

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, Praxiskommentar zum Urheberrecht Auflage. 2014.

Wang, Liang/Kangasharju, Jussi: Measuring large-scale distributed systems: case of BitTorrent Mainline DHT, In IEEE P2P 2013 Proceedings, 2013, 1–10.

Wang, Peng et al.: Attacking the Kad network, 2008, ISBN 978–1–60558–241–2.

Watters, Paul A./Layton, Robert/Dazeley, Richard: How much material on BitTorrent is infringing content? A case study, Information Security Technical Report, 16 2011, 79–87.

Webb, Timothy/Key-Matuszak, Peter: Implications of the Dallas Buyers Club v iiNet decisions, ⟨URL: https://www.claytonutz.com/knowledge/2016/april/implications-of-the-dallas-buyers-club-v-iinet-decisions⟩ – Zugriff am 31.03.2021.

Weekly, David E.: Gnutella and the state of P2P, ⟨URL: http://blog.dweek.ly/gnutella-and-the-state-of-p2p/⟩ – Zugriff am 31.03.2021.

Wegener, Christoph/Heidrich, Joerg: Neuer Standard - Neue Herausforderungen: IPv6 und Datenschutz, Computer und Recht, 2011, 479–484.

Wenzl, Frauke: Musiktauschbörsen im Internet, 2005 - zugleich Diss., Wirtschaftsrecht und Wirtschaftspolitik 196, ISBN 978–3–8329–1391–5.

Wick, Gottlieb Rafael: Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter, 2010 - zugleich Diss., ISBN 978–3–941192–02–7.

Wielsch, Dan: Verantwortung von digitalen Intermediären für Rechtsverletzungen Dritter, Zeitschrift für Geistiges Eigentum, 2014, 1–34.

Wimmer, Barbara: Auch in Österreich werden Filesharer verklagt, ⟨URL: https://futurezone.at/netzpolitik/auch-in-oesterreich-werden-filesharer-verklagt/24.586.849⟩ – Zugriff am 31.03.2021.

Windau, Benedikt: Der Glaube an die Justizstatistik als Quelle der Erkenntnis, ⟨URL: https://bit.ly/2QRRPdA⟩ – Zugriff am 31.03.2021.

Windau, Benedikt: Justizminister wollen „Zivilprozess durch Reformen stärken“, ⟨URL: https://www.zpoblog.de/justizministerkonferenz-zivilprozess-kammerprinzip-spezialisierung/⟩ – Zugriff am 31.03.2021.

Wischmeyer, Thomas: Der „Wille des Gesetzgebers“, Juristenzeitung, 2015, 957–966.

Würdinger, Markus: Das Ziel der Gesetzesauslegung - ein juristischer Klassiker und Kernstreit der Methodenlehre, Juristische Schulung, 2016, 1–6.

Wu, Di et al.: Understanding Peer Exchange in BitTorrent Systems, In 2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P), 2010, 1–8.

Xu, Kunjie: Performance Modeling of BitTorrent Peer-to-Peer File Sharing Networks, CoRR abs/1311.1195 2013.

Yang, Nele: Die Leitentscheidung, 2018 - zugleich Diss., Beiträge zum ausländischen öffentlichen Recht und Völkerrecht, Bd. 266, ISBN 978–3–662–54864–6.

Zhang, Chao et al.: BitTorrent Darknets, In 2010 Proceedings IEEE INFOCOM, 2010, 1–9.

Zhang, Chao et al.: Unraveling the BitTorrent Ecosystem, IEEE Transactions on Parallel and Distributed Systems, 22 2011 Nr. 7, 1164–1177.

Zhu, Ji et al.: Stable and scalable universal swarms, Distributed Computing, 28 2015 Nr. 6, 391–406.

Zilka, Genan: The RIAA's Troubling Solution to File-Sharing, Fordham Intellectual Property, Media and Entertainment Law Journal, 20 2009, 667–713.

Zimmermann, Johannes: Tatsächliche Vermutung und sekundäre Darlegungslast in Filesharing-Prozessen, Zeitschrift für IT-Recht und Recht der Digitalisierung, 2014, 368–372.

Zimmermann, Johannes: Die unbeachtete Zweistufigkeit von Providerauskünften in Filesharingfällen, Kommunikation und Recht, 2015, 73–76.

Zisler, Harald: Computer-Netzwerke, 3. Auflage. Bonn 2015, ISBN 978–3–8362–3479–5.

Zombik, Peter: Der Kampf gegen Musikdiebstahl im Internet, Zeitschrift für Urheber- und Medienrecht, 2006, 450–457.

Zuozhi, Shao/Yue, Yan/Yunlang, Min: The Research of Protocol Iden-

tification Based on Traffic Analysis, In 2017 10th International Conference on Intelligent Computation Technology and Automation (ICICTA), 2017, 172–175.

Zwengel, Wolfgang: Kulturflatrates, 2012 - zugleich Diss., Hamburger Schriften zum Medien-, Urheber- und Telekommunikationsrecht 4, ISBN 978–3–8329–7992–8.