Das Urheberrecht – verloren im Netz? – Aktuelle Fragen zur Rechtsdurchsetzung bei Urheberrechtsverletzungen im Internet*

Björn Frommer

Rechtsanwalt, München

* In Zusammenarbeit mit Rechtsanwältin Elzbieta Bisle.

Inhaltsübersicht Seite

A. Über File- und Streamhoster begangene Urheberrechtsverletzungen

I. Die einzelnen Akteure

1. Die File- und Streamhoster

File- und Streamhoster[1] gehören im technischen und juristischen Sinne zur Gruppe der Host-Provider. Als Host-Provider werden Diensteanbieter bezeichnet, die im Internet Speicherplatz zur Verfügung stellen.

Da der Upload auf den Server des Host-Providers direkt über dessen Webseite erfolgt, benötigen die Nutzer in der Regel lediglich einen Internetzugang und einen Webbrowser, um ihre Inhalte auf dem Server des Host-Providers speichern zu können.

Zur Nutzung des Dienstes muss zwar häufig ein Benutzerkonto mit einem Benutzernamen eröffnet werden. Die Angabe „echter" personenbezogener Daten ist jedoch mangels gesetzlich normierter Registrierungs- bzw. Speicherpflichten in der Regel nicht erforderlich. Vielmehr können Pseudonyme oder gefälschte Daten eingetragen werden, da regelmäßig weder Identitätsprüfungen vorgenommen noch Anschriften abgefragt werden. Auch die beim Upload oder bei der späteren Einwahl verwendeten IP-Adressen der Nutzer werden von den Host-Providern vielfach – zumindest vorgeblich – nicht gespeichert.

Bei *Filehostern* erhält der Nutzer nach dem Upload einen Link, über den die Datei jederzeit wieder heruntergeladen werden kann. Dieser Link kann anschließend – beliebig oft – an Dritte weitergegeben werden, um ihnen so einen Zugriff auf die hochgeladene Datei zu ermöglichen. Populäre Filehoster sind u.a. Uploaded, Share-Online, Oboom, MEGA, Uploadable, Zippyshare, FreakShare, KingFiles, Rapidgator und BitShare.

---

[1] Filehoster werden auch als Cyberlocker, Share- oder One-Click-Hoster bezeichnet.

Bei *Streamhostern* wird die hochgeladene Datei zum Abruf als „Stream" bereitgestellt. Daneben ist in aller Regel aber auch ein Download der Datei mittels spezieller, im Internet frei zugänglicher Software möglich. Bekannte Streamhoster sind u.a. YouTube, MyVideo, Clipfish, BitShare, MovShare, NowVideo, Sockshare, FlashX und Streamcloud.

Gewinne erzielen Host-Provider insbesondere mit Werbeeinnahmen, die über die Schaltung von Werbebannern auf ihren Seiten generiert werden. Zudem bieten die meisten Host-Provider kostenpflichtige „Premium-Accounts" an, bei denen beispielsweise ein größerer Speicherplatz zur Verfügung gestellt wird[2] und Downloads ohne Beschränkung der Downloadgeschwindigkeit oder mehrere Downloads parallel möglich sind. Dies geht oft mit finanziellen Anreizmodellen für Uploader einher, indem etwa für von Dritten besonders häufig abgerufene bzw. herunter geladene Inhalte Bonuspunkte oder Prämien vergeben werden.

Sofern ein Uploader für den massenhaften Download bzw. Abruf der von ihm illegal bereit gestellten Dateien durch Dritte eine Prämie vom Host-Provider erhält bzw. der Downloader für den noch umfassenderen Zugriff auf die „Schließfächer" anderer Nutzer zahlen muss, ist regelmäßig auch die Grenze zu strukturell rechtsverletzenden Angeboten überschritten. In diesen Fällen wird die illegale Weiterverbreitung der Inhalte bewusst gefördert, jedenfalls aber billigend in Kauf genommen.[3]

Gefahrgeneigte Host-Provider lassen sich daher insbesondere anhand dieser oder vergleichbarer Kriterien von legalen Diensten im Bereich des Cloud Computing abgrenzen. Klassische Cloud-Angebote stellen nicht nur Speicherplatz bereit, sondern schützen die gespeicherten Daten insbesondere vor dem Zugriff Dritter und verlangen für diese Dienstleistung ein Entgelt. Der durch Belohnungs- oder Anreizsysteme geförderte Fremdzugriff steht im Widerspruch zum Geschäftszweck dieser Dienste.

---

2 So umfasst der kostenlose Account bei MEGA 50 GB, der Premium-Account dagegen 4 TB.

3 BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

Über die Webseiten der Host-Provider können Links zu hochgeladenen Inhalten in der Regel weder gezielt gesucht noch direkt weiter verbreitet werden. Die Provider fungieren vielmehr wie Anbieter von Schließfächern, wodurch sich auch der Name Cyberlocker erklärt. Im Gegensatz zum herkömmlichen Schließfach kann der Schlüssel zu einer Datei, der Link, beliebig oft weiter verbreitet werden. Dies geschieht in der Regel über eigenständige Portalseiten oder Plattformen[4]. Diese werden zum Teil vom Betreiber des Host-Providers geführt bzw. gesteuert[5], zum Teil aber auch von Dritten betrieben.

2. Die Portalseiten und Plattformen

Linksammlungen in Form von sog. Portalseiten oder sonstigen Plattformen veröffentlichen täglich neue Links zu den Speicherorten der Host-Provider. Sie dienen dabei nicht nur als digitale Wegweiser zu den Fundorten, sondern ermöglichen den Nutzern vielmehr auch eine direkte Suchfunktion. Überdies werden die illegalen Inhalte optisch ansprechend – dem Vorbild legaler Onlineshops folgend – platziert, redaktionell aufbereitet und mit Suchmaschinen-Keywords verknüpft, um deren Auffindbarkeit zu fördern. Die Angebotspalette ist vielfach umfassender als die der legalen Anbieter, die naturgemäß lizenzvertraglichen Beschränkungen unterworfen sind.

Obwohl die Portalseiten bzw. Plattformen deutschsprachig und auf deutsche Nutzer ausgerichtet sind, sind sie häufig im (nichteuropäischen) Ausland registriert. Beliebt sind Top-Level-Domains wie „.bz“ (Belize), „.to“ (Tonga), „.sx“ (Sint Maarten), „tv“ (Tuvalu) oder „.cc“ (Kokosinseln). Die Domainregistrierungsstellen dieser Länder akzeptieren bei der Registrierung auch gefälschte oder anonyme Anmeldedaten. Da diese Registrierungsstellen zudem keine Whois-Datenbanken zum

---

4 Neben Portalseiten und Plattformen werden Links auch über Foren, Blogs oder sonstige Linksammlungen verbreitet.

5 Die Betreiber der illegalen Portalseite kino.to haben zugleich eigene Filehoster (archiv.to, speedload.to, quickload.to sowie freeload.to) betrieben, auf deren Servern die zu den Links gehörenden Raubkopien der urheberrechtlich geschützten Werke gespeichert wurden, vgl. LG Leipzig, 14.06.2012, Az. 11 KLs 390 Js 191/11.

Abruf der Domaininhaber zur Verfügung stellen, scheidet eine Identifizierung der Domaininhaber in der Regel aus.

Bekannte Portalseiten und Plattformen sind beispielsweise boerse.bz, kinox.to, movie4k.to, lul.to oder boerse.sx. Bei der Suche nach einem Filmtitel oder bei der Eingabe von Suchbegriffen wie *„Filme umsonst"* werden die illegalen Medien-Angebote vielfach vor den legalen Bezahlangeboten durch die Suchmaschinen aufgelistet.

Schätzungen des Webseitendienstes Similarweb zufolge wurden die Portale movie4k.to, kinox.to und boerse.bz allein im August 2014 ca. 120 Millionen Mal besucht.[6] Gegen die Verantwortlichen von boerse.bz, kinox.to und movie4k ermitteln aktuell die Staatsanwaltschaften Köln und Dresden wegen gewerbsmäßig begangener Urheberrechtsverletzungen.[7]

3. Die Access-Provider

Neben den Host-Providern und den Portalseiten bzw. Plattformen leisten aber auch die Access-Provider[8] durch ihre Dienstleistung zwangsläufig einen kausalen Beitrag zur illegalen Verbreitung der Inhalte, indem sie den Zugang zum Internet und damit auch zu den illegalen Angeboten vermitteln.

---

6 Vgl. http://www.similarweb.com/website/kinox.to, http://www.similarweb.com/website/movie4k.to und http://www.similarweb.com/website/boerse.bz.

7 Vgl. Pressemitteilungen WALDORF FROMMER (http://news.waldorf-frommer.de/boerse-bz-massiver-schlag-gegen-groesste-illegale-musik-film-und-buch-boerse) bzw. GVU (http://www.gvu.de/media/pdf/932.pdf); Die Betreiber von boerse.bz haben ihr Angebot aufgrund der strafrechtlichen Verfolgung zwischenzeitlich eingestellt.

8 Beispielsweise die Deutsche Telekom AG, die Vodafone GmbH oder die Telefónica Germany GmbH & Co. KG.

II. Die Inanspruchnahme der File- und Streamhoster

1. Die Inanspruchnahme auf Drittauskunft

a. Der Anspruch aus § 101 UrhG und seine Grenzen

Für das illegale Angebot zum Download bzw. Abruf per Stream sind in erster Linie diejenigen Personen verantwortlich, die die Inhalte auf die Server der Host-Provider hochladen und die hierbei generierten Links auf Plattformen bzw. Portalseiten der Öffentlichkeit zugänglich machen. Diese Personen sind aufgrund der lukrativen Belohnungssysteme zumeist für eine Vielzahl von Rechtsverletzungen verantwortlich (sog. Heavy-Uploader).[9] Da die Rechtsverletzungen jedoch unter dem Schutz der Anonymität begangen werden, setzt deren Inanspruchnahme zwingend eine Identifizierung voraus.

Die Identität der Uploader kann ausschließlich mit Hilfe der Host-Provider festgestellt werden, da nur sie die im Benutzerkonto angegeben Klardaten bzw. die beim Upload der Dateien verwendeten IP-Adressen kennen können.

Ein entsprechender Anspruch auf Beauskunftung von *„Namen und Anschrift"* der Rechtsverletzer ist in § 101 Abs. 2 Nr. 3, Abs. 3 Nr. 1 UrhG normiert.

Gegenüber Host-Providern läuft der Auskunftsanspruch jedoch regelmäßig ins Leere. Denn der Anspruch führt nur dann zum Erfolg, sofern der Provider Klardaten seiner Nutzer oder zumindest die vom Uploader verwendete IP-Adresse erhebt und speichert.

Nachdem es bis zum heutigen Tage an jedweder gesetzlichen Verpflichtung zur Erhebung und Speicherung der für eine Identifizierung erforderlichen Daten fehlt, verzichten die meisten Host-Provider jedoch entweder ganz auf eine Registrierung oder prüfen die angegebenen Daten nicht auf ihre Richtigkeit. Auch die beim Upload bzw. einer späteren Einwahl verwendeten IP-Adressen werden überwiegend

---

9 Erfahrungsgemäß können Heavy-Uploader monatlich „steuerfreie" Einnahmen im bis zu fünfstelligen Bereich erzielen.

nicht gespeichert[10]. Werden doch ausnahmsweise Daten mit Einwilligung des Nutzers erhoben und gespeichert, so handelt es sich hierbei meistens um eine E-Mail-Adresse oder Zahlungsdaten. Nur vereinzelt erfolgt die Abfrage einer Telefonnummer[11].

Ungeachtet vom Fehlen einer entsprechenden Verpflichtung wird teilweise angezweifelt, ob Diensteanbieter ohne Einwilligung des Nutzers überhaupt zu einer Speicherung personenbezogener Bestands- und Nutzungsdaten berechtigt sind.

Seitens der Host-Provider wird gegen eine Registrierung und Speicherung eingewandt, dass sie nach § 13 Abs. 6 TMG die Nutzung von Telemedien und deren Bezahlung anonym oder unter einem Pseudonym zu ermöglichen hätten, soweit dies technisch möglich und zumutbar sei. Soweit es sich um personenbezogene Daten handelt, stünde vor allem auch § 12 Abs. 1 TMG einer Erhebung und Speicherung entgegen. Die Daten seien in der Regel weder für die Begründung des Dienstverhältnisses (§ 14 TMG), noch für die Nutzung des Dienstes oder zu Abrechnungszwecken (§ 15 TMG) erforderlich.

Zur Klärung, inwieweit die angeführten Normen eine Speicherung ohne Einwilligung des Nutzers ausschließen können, wird eine Entscheidung des Gerichtshofs der Europäischen Union im Rahmen einer Vorlagefrage des Bundesgerichtshofs beitragen.[12]

In einem Verfahren, in dem es um die Speicherung von IP-Adressen beim Aufruf einer Webseite geht, hat der Bundesgerichtshof dem EuGH zwei Fragen zur Vorabentscheidung vorgelegt:

---

10 Dies wird zumindest vielfach behauptet. Ob bzw. inwieweit gleichwohl eine Speicherung der IP-Adressen erfolgt, lässt sich seitens der Rechteinhaber faktisch nicht aufklären.

11 Bei YouTube ist die Angabe der Mobilfunknummer zwingend, wenn der Uploader audiovisuelle Inhalte mit einer Länge von über 15 Minuten hochladen möchte. Der Uploader erhält dann einen Bestätigungscode per Anruf oder SMS.

12 BGH, 28.10.2014, Az. VI ZR 135/13 betreffend die Auslegung der Richtlinie 95/46/EG (Datenschutz-Richtlinie).

Zunächst möchte der Bundesgerichtshof die heftig umstrittene Frage klären lassen, ob eine IP-Adresse für einen Diensteanbieter überhaupt ein personenbezogenes Datum darstellt, wenn nicht er selbst, sondern lediglich ein Dritter (etwa der Access-Provider) über die zur Identifizierung der betroffenen Person erforderlichen Klardaten verfügt. Denn nur dann wären die Beschränkungen der §§ 12 ff. TMG überhaupt einschlägig.

Mit seiner zweiten Frage möchte der Bundesgerichtshof geklärt wissen, ob die Speicherung von Logdaten, soweit es sich dabei um personenbezogene Daten handelt, überhaupt auf Fälle der Einwilligung und auf Abrechungszwecke beschränkt werden kann, wie dies in der nationalen Regelung des § 15 TMG erfolgt, oder ob einer solchen Beschränkung Art. 7 der Datenschutz-Richtlinie[13] entgegen steht, der die Verarbeitung personenbezogener Daten – über die in § 15 TMG genannten Zwecke hinaus – auch zur Verwirklichung eines berechtigten Interesses[14] erlaubt.

Unabhängig davon dürfte jedenfalls die Auskunftserteilung selbst datenschutzrechtlich zulässig sein, da § 14 Abs. 2 TMG den Host-Providern (als Telemediendiensten) die Übermittlung der Bestandsdaten ihrer Nutzer gestattet, sofern dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.[15]

---

13 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 29.09.2003, S. 31.

14 In dem gegenständlichen Verfahren wurde als berechtigtes Interesse die Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit der Telemedien angeführt.

15 Zscherpe in Taeger/Gabel, BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, § 14 TMG, Rn. 50, 52; ablehnend in Bezug auf einen Auskunftsanspruch aus Persönlichkeitsrechtsverletzung, da diese im Gegensatz zu Verletzungen geistigen Eigentums nicht vom Normzweck umfasst ist: BGH, 01.07.2014, Az. VI ZR 345/13.

Entsprechendes gilt über § 15 Abs. 5 S. 4 TMG auch für Nutzungsdaten, wie etwa die Logdaten. Diese Befugnisse wurden insbesondere im Hinblick auf die Umsetzung der Enforcement-Richtlinie[16] und die Einführung der Drittauskunftsansprüche (§ 101 UrhG u.a.) geschaffen.[17]

Gleichwohl ist der Auskunftsumfang umstritten, namentlich ob neben dem bürgerlichen Namen und der Postanschrift auch andere (mit Einwilligung des Nutzers oder sonst zulässig gespeicherte) Daten von § 101 Abs. 2 Nr. 3, Abs. 3 Nr. 1 UrhG umfasst sind. Bei der IP-Adresse nebst Zeitpunkt des Uploads[18] sowie der E-Mail-Adresse[19] wird dies teilweise bejaht. Inwieweit auch Auskunft über die hinterlegte Telefonnummer erteilt werden muss, ist bisher zwar ungeklärt. Der Fall dürfte jedoch mit den sog. Reseller-Auskünften vergleichbar sein. Dort ist anerkannt, dass ein Access-Provider über die Daten eines Kunden seines Resellers dadurch Auskunft erteilen muss, dass er statt des (nicht bei ihm gespeicherten) Namens die bei ihm hinterlegte, vom Reseller vergebene Benutzerkennung mitzuteilen hat.[20] Wie die Benutzerkennung ist auch die Telefonnummer eine feste Anschlusskennung, so dass diese ebenfalls vom Auskunftsanspruch umfasst sein müsste.

---

16 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29.04.2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. Nr. L 157 vom 30.04.2004, S. 45.

17 BT-Drs. 16/3078, S. 16.

18 LG Hamburg, 26.11.2009, Az. 308 O 647/09; Nordemann in Fromm/Nordemann, Urheberrecht, 11. Aufl. 2014, § 101 Rn. 32; Spindler in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 101 UrhG Rn. 1.

19 OLG Köln, 25.03.2011, Az. 6 U 87/10; Nordemann in Fromm/Nordemann, Urheberrecht, 11. Aufl. 2014, § 101 Rn. 32; Spindler in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 101 UrhG Rn. 1.

20 Vgl. hierzu die Mitteilung des Bundesdatenschutzbeauftragten, abrufbar unter: http://www.bfdi.bund.de/DE/ Datenschutz/Themen/Telefon_Internet/InternetArtikel/AuskunftsrechtsBeiUrheberrechtsverstoss.html.

Einer Identifizierung des Nutzers anhand seiner Zahlungsdaten dürfte dagegen nach der weit überwiegenden Ansicht § 101 Abs. 2 S. 1 HS. 1 UrhG entgegen stehen, da Kreditinstitute nach § 383 Abs. 1 Nr. 6 ZPO zur Zeugnisverweigerung berechtigt sind.[21]

b. Gesetzgeberischer Handlungsbedarf

Das System der Speicherung aktueller Medieninhalte bei einem Host-Provider in Verbindung mit deren massenhafter illegaler Verbreitung über Portalseiten und Plattformen funktioniert zunächst einmal nur deshalb, weil Uploader im Schutze der Anonymität und damit sicher vor jeglicher Verfolgung agieren können. Dass eine Verfolgung dieser Personen zum einen an den Profitinteressen der Host-Provider und zum anderen am fehlenden gesetzgeberischen Willen scheitert, endlich effektive Speicher- und Auskunftspflichten zu normieren, ist für Geschädigte mehr als unbefriedigend.

Für eine nachhaltige Inanspruchnahme der Uploader ist die Schaffung einer Rechtsgrundlage erforderlich, die den Host-Provider verpflichtet, die Klardaten und die Nutzungsdaten jedenfalls der Uploader zu erheben und zu speichern.

Dass ein generelles Recht auf anonyme Internetnutzung nicht anzuerkennen ist, wurde auch im Rahmen des 69. Deutschen Juristentages beschlossen. Bei aktiver Nutzung des Internets mit eigenen Beiträgen dürfe der Nutzer nicht anonym bleiben, sondern müsse im Rahmen einer Verwendung von Pseudonymen zumindest identifizierbar sein. Nur dann ließen sich Rechtsverstöße wirksam verfolgen. Internet-Dienste sollten daher nach Ansicht des 69. Deutschen Juristentags den Klarnamen und die Internetverbindung ihrer Nutzer registrieren.[22]

---

21 OLG Naumburg, 15.03.2012, Az. 9 U 208/11; OLG Stuttgart, 23.11.2011, Az. 2 W 56/11; OLG Köln, 25.03.2011, Az. 6 U 87/10.

22 Beschluss des 69. Deutschen Juristentags München 2012, Abteilung IT- und Kommunikationsrecht, S. 28, Ziff. I.6.b).

Auch der Gesetzgeber hatte bereits im Zuge der Umsetzung der Vorratsdatenspeicherung im Jahr 2007 erkannt, dass die Speicherung von Daten eine grundlegende Voraussetzung für die Wirksamkeit jedweden Drittauskunftsanspruchs darstellt. Der Bundesrat hatte damals davor gewarnt, Geschädigte von einem Zugriff auf die im Rahmen der Vorratsdatenspeicherung zu speichernden Daten auszunehmen, da andernfalls sämtliche zivilrechtlichen Drittauskunftsansprüche leerlaufen würden. Damit würde ein wesentliches Anliegen des Gesetzesentwurfs zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums konterkariert. [23]

Gleichwohl hat der Gesetzgeber bis heute weder für die strafrechtliche Verfolgung noch für zivilrechtliche Auskunftsverfahren eine Speicherpflicht eingeführt. Und dies, obwohl keine generellen Zweifel an der Zulässigkeit einer Vorratsdatenspeicherung bestehen, sondern lediglich am ursprünglich zu weitgehenden Inhalt der europäischen Vorgaben[24] bzw. der deutschen Umsetzung[25].

Darüber hinaus sollte in § 101 UrhG eine gesetzliche Klarstellung zum Auskunftsumfang erfolgen. Der Auskunftsanspruch muss auch sonstige beim Host-Provider gespeicherte, der Identifizierung dienende Daten umfassen. Insbesondere in Telekommunikations- bzw. Funknetzen dienen der Klarname und die postalische Anschrift allenfalls nachrangig der Identifikation, der Kontaktaufnahme und der Kommunikation. Regelmäßig werden in Telekommunikationsnetzwerken bzw. im Internet anstelle der Klarnamen und postalischen Anschriften nahezu ausschließlich E-Mail-Adressen, IP-Adressen und sonstige Telefondienste, wie etwa SMS, verwendet.

Eine Beschränkung des Auskunftsumfangs auf die klassische Briefkastenanschrift würde jedwede Rechtsverfolgung weitgehend ins Leere laufen lassen. Hierdurch würden Sinn und Zweck der u.a. mit § 101 UrhG umgesetzten Enforcement-Richtlinie verfehlt. Die Enforcement-Richtlinie gebietet den Mitgliedstaaten zwar nicht, die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivil-

---

23 BT-Drs. 16/5846, S. 86.

24 EuGH, 08.04.2014, Rs. C-293/12 und C-594/12, Digital Rights Ireland Ltd/Minister for Communications u.a.

25 BVerfG, 02.03.2010, Az. 1 BvR 256/08 u.a.

rechtlichen Verfahrens vorzusehen. Vielmehr sind Richtlinienbestimmungen grundsätzlich allgemein gehalten, da sie auf unterschiedliche Sachverhalte in allen Mitgliedstaaten Anwendung finden sollen. Sie enthalten daher Regelungen, die zwar hinsichtlich des zu erreichenden Ziels verbindlich sind, den Mitgliedstaaten jedoch bei der Wahl der zur Erreichung dieses Ziels erforderlichen Maßnahmen einen Beurteilungsspielraum überlassen.[26] Nachdem der deutsche Gesetzgeber jedoch das in Art. 8 der Enforcement-Richtlinie normierte Recht auf Auskunft mit dem zivilrechtlichen Auskunftsanspruch in § 101 UrhG ins nationale Recht umgesetzt hat, muss dieser Anspruch insbesondere den Grundsatz effektiven Urheberrechtsschutzes wahren, wie ihn Art. 3 der Enforcement-Richtlinie und Art. 8 Abs. 1 der Infosoc-Richtlinie[27] aufstellen.

Der Auskunftsanspruch muss also wirksam und abschreckend sein. Dieses Erfordernis ist insbesondere vor dem Hintergrund, dass der urheberrechtliche Auskunftsanspruch gerade für Fallgestaltungen in der digitalen Welt geschaffen wurde, jedoch nur dann erfüllt, wenn der Anspruch die im Internet verwendeten Kommunikationsadressen umfasst. Hierzu gehören insbesondere E-Mail-Adressen, Logdaten und Telefonnummern.

---

26 EuGH, 29.01.2008, Rs. C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.

27 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, Abl. Nr. L 167 vom 22.06.2001, S. 10.

2. Die Inanspruchnahme auf Unterlassung und Beseitigung

a. Der Anspruch aus § 97 UrhG[28] und seine Grenzen

Eine Inanspruchnahme des Host-Providers auf Unterlassung und Beseitigung würde voraussetzen, dass der Host-Provider entweder Täter oder Teilnehmer der Urheberrechtsverletzung ist oder aber nach den Grundsätzen der Störerhaftung für die Urheberrechtsverletzung einzustehen hat.

aa. Die Haftung als Täter oder Teilnehmer

Jedenfalls eine Täterschaft des Host-Providers scheidet regelmäßig aus. Denn für die Beurteilung der Frage, ob eine Beteiligung als Täter, Mittäter, Anstifter oder Gehilfe an einer Rechtsverletzung eines Dritten vorliegt, sind nach der Rechtsprechung des Bundesgerichtshofs die im Strafrecht geltenden Grundsätze heranzuziehen[29].

Eine Verantwortung als Täter erfordert somit, dass der Host-Provider die Rechtsverletzung entweder selbst, in mittelbarer Täterschaft oder in Mittäterschaft begangen hat, wobei Mittäterschaft nur bei einer gemeinschaftlichen Begehung, also einem bewussten und gewollten Zusammenwirken, anzunehmen ist.[30] Der Host-Provider macht jedoch – von Ausnahmen abgesehen[31] – weder selbst noch gemeinsam mit einem Dritten die Dateien öffentlich zugänglich und vervielfältigt sie auch

---

28 Teilweise wird als Anspruchsgrundlage für die Störerhaftung auch § 1004 BGB analog herangezogen, vgl. Nordemann in Fromm/Nordemann, Urheberrecht, 11. Auflage 2014, § 97 Rn. 154; nach a.A. ist seit Einführung des § 97 UrhG diese Norm die richtige Anspruchsgrundlage, vgl. Reber in Möhring/Nicolini, Urheberrecht, 3. Auflage 2014, § 97 Rn. 42; Spindler in Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage 2011, § 97 UrhG Rn. 1, 18, 67.

29 BGH, 22.07.2010, Az. I ZR 139/08 – Kinderhochstühle im Internet I.

30 BGH, 22.07.2010, Az. I ZR 139/08 – Kinderhochstühle im Internet I.

31 So im Fall der Betreiber von kino.to (vgl. LG Leipzig, 14.06.2012, Az. 11 KLs 390 Js 191/11).

nicht.[32] Die konkrete Datei wird vielmehr vom Nutzer selbständig hochgeladen, ohne dass es einer Mitwirkung des Host-Providers bedarf.

Auch eine Verantwortlichkeit als Teilnehmer kann in der Regel nicht begründet werden, solange der Host-Provider keine Kenntnis von der konkreten Rechtsverletzung hat.[33] Zwar kann in dem Bereitstellen des Servers eine objektive Beihilfehandlung des Host-Providers erblickt werden. Daneben setzt die Gehilfenhaftung nach den im Strafrecht geltenden Grundsätzen jedoch zumindest einen bedingten Vorsatz in Bezug auf die konkrete Haupttat und deren Rechtswidrigkeit voraus.[34] Der Gehilfe muss also mit einem doppelten Gehilfenvorsatz handeln. Auch wenn der Host-Provider mit Rechtsverletzungen über seinen Dienst rechnet, so wird es ihm jedoch in aller Regel an einem Vorsatz in Bezug auf das konkrete rechtsverletzende Angebot (Datei) mangeln.[35]

bb. Die Haftung als Störer

In Betracht kommt somit lediglich eine Inanspruchnahme als Störer auf Unterlassung. Zu berücksichtigen sind insofern jedoch die §§ 7, 10 TMG, die in Umsetzung der Art. 14, 15 der E-Commerce-Richtlinie[36] Haftungsprivilegien für Speicherdienste normieren.

---

32 BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark.

33 Hanseatisches OLG, 13.05.2013, Az. 5 W 41/13.

34 BGH, 11.03.2004, Az. I ZR 304/01 – Internet-Versteigerung I; BGH, 19.04.2007, Az. I ZR 35/04 – Internet-Versteigerung II; BGH, 22.07.2010, I ZR 139/08 – Kinderhochstühle im Internet I.

35 Für den Fall eines Zueigenmachens der fremden Inhalte wird auf die Ausführungen bei A.III.1 verwiesen.

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

§ 7 TMG verbietet dabei allgemeine Überwachungsmaßnahmen. Nach § 10 S. 1 Nr. 1 TMG sind Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, solange sie keine (positive) Kenntnis von der rechtswidrigen Handlung haben. Auch nach Kenntniserlangung entfällt die Haftung, sofern die Rechtsverletzung unverzüglich unterbunden wird, § 10 S. 1 Nr. 2 TMG.

Bislang wurden Unterlassungsansprüche nicht unter den unmittelbaren Anwendungsbereich der Haftungsprivilegien in den §§ 7, 10 TMG gefasst. Vielmehr wurde angenommen, dass diese allein die Haftung auf Schadenersatz und die strafrechtliche Verantwortlichkeit betreffen.[37] Im Ergebnis spielt dies im Rahmen der Störerhaftung allerdings nur eine geringe Rolle, da der Bundesgerichtshof bei der Zumutbarkeit von Prüfpflichten auf das generelle Verbot von Überwachungsmaßnahmen und das Erfordernis der Kenntniserlangung abstellt und somit jedenfalls auf Zumutbarkeitsebene die Wertungen der §§ 7, 10 TMG mit einbezieht.

Auch ein Host-Provider kann somit als Störer auf Unterlassung in Anspruch genommen werden, wenn er – auch ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung des geschützten Rechtsguts beigetragen hat. Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden soll, die die rechtswidrige Beeinträchtigung nicht selbst vorgenommen haben, setzt auch die Störerhaftung des Host-Providers die Verletzung von Prüfpflichten voraus.[38]

---

37 BGH, 11.03.2004, Az. I ZR 304/01 – Internet-Versteigerung I; BGH, 19.04.2007, Az. I ZR 35/04 – Internet-Versteigerung II; BGH, 30.04.2008, Az. I ZR 73/05 – Internet-Versteigerung III; BGH, 22.07.2010, Az. I ZR 139/08 – Kinderhochstühle im Internet I.

38 BGH, 30.08.2008, Az. I ZR 73/05 – Internetversteigerung III; BGH, 12.05.2010, Az. I ZR 121/08 – Sommer unseres Lebens; BGH, 18.11.2011, Az. I ZR 155/09 – Sedo; BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

Überwachungspflichten allgemeiner Art sind hierbei wegen § 7 Abs. 2 TMG zwar ausgeschlossen (vgl. auch Art. 15 E-Commerce-Richtlinie).[39] Nicht ausgeschlossen sind jedoch Überwachungspflichten in spezifischen Fällen.[40] Diese können beim Host-Provider nach der Rechtsprechung des Bundesgerichtshofs jedoch grundsätzlich erst ab Kenntnis von einer klaren Rechtsverletzung in Bezug auf ein konkretes Werk entstehen.[41]

Ab Kenntnis ist der Host-Provider nicht nur verpflichtet, das konkrete Angebot unverzüglich zu sperren (sog. *notice and take down*), sondern ihm obliegen auch Sorgfalts- und Prüfpflichten zur Verhinderung weiterer *gleichartiger* Rechtsverletzungen (sog. *notice and stay down*). Gleichartig sind dabei Verletzungshandlungen, durch die dasselbe Urheberrecht erneut verletzt wird. Auf die Person des Rechtsverletzers kommt es dagegen nicht an.[42] Vielmehr muss der Host-Provider auch gleichartige Rechtsverletzungen Dritter verhindern. Welche konkreten Maßnahmen hierbei zumutbar sind, ist im konkreten Einzelfall zu beurteilen. Zumutbar kann z.B. der Einsatz von Wortfiltern sein, die sowohl genaue Titel als auch ähnliche Begriffe umfassen müssen.[43]

---

39 BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

40 BGH, 18.11.2011, Az. I ZR 155/09 – Sedo; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

41 BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; LG Hamburg, 02.10.2014, Az. 310 O 464/13, lässt für Kenntnis ausreichen, dass dem Host-Provider der Hinweis im Sinne des § 130 BGB zugegangen ist, also derart in seinen Machtbereicht gelangt ist, dass er unter normalen Verhältnissen die Möglichkeit hat, vom Inhalt der Erklärung Kenntnis zu nehmen. Anderenfalls könnte der Host-Provider die Prüfpflichten umgehen, indem er die Hinweisschreiben der Rechteinhaber schlichtweg nicht zur Kenntnis nimmt.

42 BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

43 BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

Darüber hinaus können bei besonderer Gefahrgeneigtheit des Dienstes weitergehende Prüfungspflichten beim Host-Provider bestehen. Hiervon ist etwa dann auszugehen, wenn das Geschäftsmodell von vornherein, also strukturell, auf Rechtsverletzungen der Nutzer angelegt ist. Eine Gefahrgeneigtheit ist aber auch (schon) dann anzunehmen, wenn der Host-Provider durch eigene Maßnahmen die Gefahr einer rechtsverletzenden Nutzung fördert, indem er beispielsweise Premium-Accounts anbietet oder Bonuspunkte bzw. Prämien für besonders attraktive Inhalte vergibt.[44]

Dementsprechend ist gefahrgeneigten Diensten auch eine umfassende regelmäßige Kontrolle von Linksammlungen zuzumuten, die auf Dateien verweisen, die auf den Servern des Host-Providers gespeichert sind.[45] Einschränkungen einer legalen Nutzung sind im Interesse eines wirksamen Urheberrechtsschutzes in geringem Umfang hinzunehmen, solange das Geschäftsmodell des Host-Providers dadurch nicht grundlegend in Frage gestellt wird.[46]

Seit der Entscheidung des Gerichtshofs der Europäischen Union L'Oréal/ebay[47] und den ihr nachfolgenden Entscheidungen des ersten Zivilsenats des Bundesgerichtshofs[48] bestehen zum Teil zwar Zweifel[49], ob der Bundesgerichtshof eine unmittelbare Anwendung des § 10 TMG auf Unterlassungsansprüche auch weiterhin verneint. Dies ist jedoch im Ergebnis unerheblich, da der Bundesgerichtshof jeden-

---

44 BGH, 15.01.2009, Az. I ZR 57/07 – Cybersky; BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark; BGH, 15.08.2013, Az. I ZR 79/12 – Prüfpflichten; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

45 BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst.

46 BGH, 12.07.2012, Az. I ZR 18/11 – Alone in the Dark.

47 EuGH, 12.06.2011, Rs. C-324/09 – L'Oréal/ebay.

48 BGH, 17.08.2011, Az. I ZR 57/09 – Stiftparfüm; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst; BGH, 12.07.2012, Az.I ZR 18/11 – Alone in the dark; BGH, 16.05.2013, Az. I ZR 216/11 – Kinderhochstühle im Internet II.

49 KG Berlin, 16.04.2013,Az. 5 U 63/12; von Ungern-Sternberg, GRUR 2012, 321, 327; Köhler in Köhler/Bornkamm, UWG, 32. Aufl. 2014, § 8 Rdnr. 2.28.

falls auch in seinen aktuellen Entscheidungen[50] zu dem Ergebnis kommt, dass der Host-Provider ab Kenntnis von einer Rechtsverletzung nicht nur verpflichtet ist, das rechtsverletzende Angebot zu beseitigen, sondern auch weitere gleichartige Rechtsverletzungen zu verhindern. Im Hinblick auf diese gleichartigen Rechtsverletzungen besteht eine Störerhaftung des Host-Providers auf Unterlassung somit auch weiterhin ohne vorherige Kenntnisverschaffung.

Unabhängig davon dürften darüber hinaus gehende Prüfpflichten, die das Geschäftsmodell als solches unmöglich machen, allenfalls dann zumutbar sein, wenn der Host-Provider die illegalen Nutzungsmöglichkeiten seines Dienstes besonders hervorhebt bzw. bewirbt.[51]

Im Ergebnis ist unerheblich, wo die Haftungsbeschränkungen systematisch verortet werden. Jedenfalls führen die vom BGH aufgestellten Kriterien in der Praxis – schon aufgrund der schieren Masse an Rechtsverletzungen – nur relativ selten dazu, dass Host-Provider wegen der zahllosen Pflichtverletzungen nachhaltig in Anspruch genommen werden können. Eine echte Eigenverantwortung der Host-Provider, einen Missbrauch ihrer Systeme zu verhindern, ist hiermit jedenfalls nicht zu erreichen.

Um es anhand eines Beispieles zu verdeutlichen: Soweit ein Host-Provider über die illegale Verbreitung einer bei ihm hinterlegten Datei informiert wird, ist er zwar nicht nur verpflichtet, die konkrete Datei, sondern – im Rahmen des Zumutbaren – auch weitere Dateien gleichen Inhaltes zu entfernen bzw. deren künftige Verbreitung zu verhindern. Soweit es sich bei dieser Datei aber um einen einzelnen Song handelt, ist bereits fraglich, ob die weiteren Songs dieses Albums von der Prüf- und Überwachungspflicht des Host-Providers umfasst sind, da hier jedenfalls nach restriktiver Rechtsprechung die Grenze der Kerngleichheit überschritten sein dürfte. In jedem Fall dürften aber andere Alben desselben Künstlers nicht erfasst sein. Entsprechendes gilt für Filmwerke: Bei den sich größter Beliebtheit erfreuenden

---

50 BGH, 17.08.2011, Az. I ZR 57/09 – Stiftparfüm; BGH, 15.08.2013, Az. I ZR 80/12 – File-Hosting-Dienst; BGH, 12.07.2012, Az.I ZR 18/11 – Alone in the dark; BGH, 16.05.2013, Az. I ZR 216/11 – Kinderhochstühle im Internet II.

51 BGH, 15.01.2009, Az. I ZR 57/07 – Cybersky.

TV-Serien ist ebenfalls fraglich, ob sich die Prüf- und Überwachungspflicht auch auf weitere Episoden derselben Staffel, erst recht auf weitere Staffeln derselben Serie erstreckt.[52]

Im Übrigen sind selbst gefahrgeneigte Host-Provider lediglich verpflichtet, ausgewählte Linksammlungen dahingehend zu überprüfen, ob derselbe Song auch über andere Links verbreitet wird, die auf seinen Dienst verweisen. Dass auf diese Weise etliche weitere „Fundorte" gar nicht erst entdeckt werden, liegt auf der Hand.

Aus Sicht eines Geschädigten ist es folglich nie damit getan, eine einzige Rechtsverletzung mitzuteilen und im Übrigen auf die Mithilfe des Providers zu hoffen. Aktuell müssen Rechteinhaber das Internet vielmehr fortlaufend auf eigene Kosten nach neuen Rechtsverletzungen durchsuchen und die Host-Provider zur Beseitigung jeder einzelnen Rechtsverletzung konkret auffordern.[53]

Nachdem die Uploader regelmäßig nicht zu identifizieren und damit nicht zur Verantwortung zu ziehen sind, können sie jederzeit weitere Werke hochladen oder dasselbe Werk bei einem der zahlreichen anderen Host-Provider anbieten. Die Host-Provider trifft im Ergebnis vielfach gar keine Haftung, da die meisten Rechtsverletzungen entweder nicht kerngleich oder nicht mittels der zumutbaren Maßnahmen zu unterbinden sind.

Die geschädigten Rechteinhaber sind folglich einem kostspieligen „Katz-und-Maus-Spiel" ausgesetzt, während Host-Provider und Uploader keinerlei ernsthafte Konsequenzen für ihre parasitären Geschäftsmodelle zu befürchten haben.

---

52 Inwieweit der BGH über die in der Entscheidung vom 20.06.2013, Az. I ZR 55/12 – Restwertbörse II, aufgestellten Grundsätze hinaus eine Kerngleichheit bejaht, ist offen.

53 Allein die von WALDORF FROMMER vertretenen Medienunternehmen werden bis zum Ende des Jahres 2014 auf über 5 Millionen gesperrte Dateien kommen.

b. Gesetzgeberischer Handlungsbedarf

Um die Rechteinhaber nicht schutzlos zu stellen, muss bei jeder Rechtsverletzung entweder der primär verantwortliche Uploader oder zumindest der mittelbar verantwortliche Host-Provider in Anspruch genommen werden können.

Erste Bestrebungen dahingehend sind auf politischer Ebene bereits zu verzeichnen. So sehen sowohl der Koalitionsvertrag als auch die Digitale Agenda der Regierungskoalition vor, die rechtlichen Rahmenbedingungen zum Schutz des geistigen Eigentums an die rasante technische Digitalisierung in Wirtschaft und Gesellschaft anzupassen. Insbesondere sollen sich Diensteanbieter, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut, nicht länger auf das Haftungsprivileg des Host-Providers zurückziehen können. Dieses Ziel werde auch auf europäischer Ebene verfolgt.[54]

Der Gesetzgeber verfolgt dabei offenbar das Ziel, sog. (besonders) gefahrgeneigte Host-Provider generell von den Privilegierungen der §§ 7, 10 TMG bzw. den vom Bundesgerichtshof aufgestellten Haftungsgrundsätzen auszunehmen.

Diesem Ansatz ist grundsätzlich zuzustimmen, da sich gefahrgeneigte Host-Provider ein Haftungsregime zu nutze machen, das nicht für die von ihnen betriebenen Geschäftsmodelle geschaffen wurde. Die E-Commerce-Richtlinie und das Telemediengesetz wurden zweifelsohne nicht zum Zweck der Förderung von Rechtsverletzungen eingeführt. Genau dies geschieht jedoch, wenn Host-Provider sich hinter Haftungsprivilegien verstecken können, obwohl sie Rechtsverletzern grenzenlose Anonymität und finanzielle Anreizmodelle für illegale Uploads bieten.

---

54 Digitale Agenda 2014-2017, dort S. 15 (abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf) und Koalitionsvertrag, dort S.93 (abrufbar unter: https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf).

Um die Durchsetzung der Rechte des geistigen Eigentums im Internet zu gewährleisten, genügt es jedoch nicht, wenn man besonders gefahrgeneigten Diensten die Haftungsprivilegien entzieht. Darüber hinaus ist es vielmehr erforderlich, auch nicht gefahrgeneigte Dienste dazu anzuhalten, die Identifizierung ihrer Nutzer zu ermöglichen, wenn diese Rechtsverletzungen begehen.

Zur Umsetzung dieses Ziels müsste noch nicht einmal eine ausdrückliche Registrierungs- und Speicherpflicht eingeführt werden. Ausreichend wäre vielmehr, dass Haftungsprivilegien generell nur noch dann gewährt werden, wenn Host-Provider den verantwortlichen Uploader identifizieren oder nachweisen können, dass zumindest alle zumutbaren Maßnahmen ergriffen wurden, um eine Identifizierung zu ermöglichen.[55] Die Host-Provider könnten dann in jedem Einzelfall selbst entscheiden, ob sie sich durch die Benennung des Uploaders exkulpieren oder für den Uploader die Haftung übernehmen wollen. In beiden Alternativen wären die verletzten Rechteinhaber jedenfalls nicht mehr gänzlich schutzlos gestellt, wie dies heute regelmäßig der Fall ist.

3. Die Inanspruchnahme auf Schadenersatz

a. Der Anspruch aus § 97 UrhG und seine Grenzen

Einer Inanspruchnahme des Host-Providers auf Erstattung der Kosten für die Ermittlung der Rechtsverletzungen sowie auf Leistung von (Lizenz-)Schadenersatz steht grundsätzlich die Haftungsprivilegierung der §§ 7, 10 TMG entgegen.

Eine Schadenersatzpflicht besteht jedoch dann, wenn der Host-Provider trotz konkreter Kenntnis ein rechtswidriges Angebot nicht sperrt. Jedenfalls ab Kenntnis von einer konkreten Rechtsverletzung liegt Beihilfe vor und zwar durch Unterlassen der Entfernung.[56] Darüber hinaus kommt ein Schadenersatzanspruch aber auch dann in Betracht, wenn der Host-Provider die ihm zumutbaren Maßnahmen unterlässt,

---

55 Herwig, ZD 2012, 558 (sog. ABC-Approach).

56 LG München I, 11.07.2014, Az. 21 O 854/13; LG Frankfurt a.M., 05.02.2014, Az. 2-06 O 319/13; Hanseatisches OLG, 13.05.2013, Az. 5 W 41/13.

um gleichartige Rechtsverletzungen zu verhindern bzw. zu unterbinden.[57] Der Host-Provider hat auch hier einen doppelten Gehilfenvorsatz, denn er bleibt wissentlich untätig und nimmt dabei zumindest billigend in Kauf, dass er hierdurch eine kerngleiche fremde Rechtsverletzung unterstützt.

b. Gesetzgeberischer Handlungsbedarf

Gefahrgeneigte Dienste, die Rechtsverletzungen aktiv fördern und für eigene wirtschaftliche Vorteile ausnutzen, sollten nicht nur auf Unterlassung, sondern auch auf Schadenersatz haften. Auch insofern sollten sie daher vom Haftungsprivileg des § 10 TMG ausgeschlossen werden.

Dies gilt insbesondere für Dienste, die mit dem Angebot von rechtsverletzenden Inhalten ihrer Nutzer über Werbung, Prämiensysteme etc. Einnahmen erzielen. Ein Rechtsstaat darf keine Geschäftsmodelle dulden, welche systematisch auf dem massenhaften Angebot und der Weiterverbreitung rechtsverletzender Inhalte basieren, auch wenn diese Inhalte nicht vom Anbieter selbst, sondern von dessen Nutzern hochgeladen werden.

III. Die Inanspruchnahme der Portal- und Plattformbetreiber

1. Die Inanspruchnahme auf Drittauskunft

a. Der Anspruch nach § 101 UrhG und seine Grenzen

Auch gegen Portalseiten und Plattformen besteht bei offensichtlichen Rechtsverletzungen grundsätzlich ein Auskunftsanspruch aus § 101 UrhG. Bei der Durchsetzung des Anspruchs sehen sich Rechteinhaber jedoch ähnlichen Hindernissen ausgesetzt, die ihnen auch bei Host-Providern begegnen.

---

57 LG München I, 11.07.2014, Az. 21 O 854/13.

Denn auch hier fehlt eine gesetzliche Verpflichtung zur Registrierung der Nutzer sowie zur Erhebung und Speicherung ihrer Daten. Gerade strukturell rechtsverletzende Plattformen verzichten daher naturgemäß auf jegliche Registrierung sowie Speicherung von Nutzungsdaten. Ist eine Registrierung vorgesehen, reicht in den meisten Fällen die bloße Angabe einer E-Mail-Adresse aus.

Entsprechend scheitert die Durchsetzung des Auskunftsanspruchs auch hier daran, dass weder Klardaten (Name und Anschrift) noch sonstige Daten, wie beispielsweise Logdaten, Telefonnummern oder E-Mail-Adressen, vorhanden sind bzw. unter Berufung auf datenschutzrechtliche Aspekte nicht beauskunftet werden. [58]

b. Gesetzgeberischer Handlungsbedarf

Um dem Anspruch auf Drittauskunft auch im Verhältnis zu Portalseiten und Plattformen zur Geltung zu verhelfen, bedarf es einer Rechtsgrundlage, die zur Erhebung und Speicherung von Nutzerdaten derjenigen Personen verpflichtet, die die Links zu den Speicherorten auf einer Portalseite oder sonstigen Plattform öffentlich zugänglich machen. Auch der Auskunftsumfangs in § 101 Abs. 3 Nr. 1 UrhG bedarf gleichermaßen einer gesetzlichen Klarstellung.[59]

2. Die Inanspruchnahme auf Unterlassung

a. Der Anspruch aus § 97 UrhG und seine Grenzen

aa. Die Haftung als Täter oder Teilnehmer

Wie schon Host-Provider sind auch Betreiber von Portalseiten und Plattformen für eigene Informationen verantwortlich. Eine Haftung als Täter ist dann anzunehmen, wenn die Betreiber der Seiten selbst für die Bereitstellung der urheberrechtsverletzenden Inhalte verantwortlich sind, es sich also um eigene Inhalte handelt.[60]

---

58 Vgl. A.II.1.a.

59 Vgl. A.II.1.b.

60 Beispielsweise bei den Verantwortlichen der Portalseite kino.to, vgl. Fn. 6, 32.

Als eigene Inhalte gelten jedoch auch Inhalte Dritter, die sich der Betreiber einer Internetseite zu eigen macht.[61] Ob ein Zueigenmachen und somit ein tatsächliches und nach außen sichtbares Übernehmen der Verantwortung vorliegt, ist aus Sicht eines objektiv verständigen Nutzers auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände zu beurteilen.[62]

Die bloße Bereitstellung einer Plattform reicht nicht aus, um ein Zueigenmachen von Beiträgen Dritter anzunehmen, vielmehr müssen weitere Umstände hinzukommen. Solche Umstände können eine redaktionelle Aufbereitung der Inhalte oder deren Veröffentlichung unter einem eigenen Logo sein. Sind die Inhalte ein redaktioneller Kerngehalt der Seite oder gar ein wesentlicher Bestandteil des Geschäftsmodells, spricht dies ebenfalls für ein Zueigenmachen.

Ein haftungsbegründendes Zueigenmachen liegt selbst dann vor, wenn die Inhalte erkennbar von einem Dritten stammen.[63] Dies gilt auch bei einer Einbindung von rechtsverletzenden Inhalten Dritter auf einer Internetseite, etwa als Stream bzw. über Hyperlinks.[64]

Bei Portalseiten und Plattformen, welche die angebotenen Inhalte bzw. Links zu offensichtlich rechtswidrigen Inhalten selbst „redaktionell" aufbereiten, strukturieren und präsentieren, kann daher aus gutem Grund von einem Zueigenmachen ausgegangen werden. Hierfür spricht insbesondere auch, dass das Zurverfügungstellen urheberrechtsverletzender Inhalte das Geschäftsmodell dieser Seiten ausmacht und zu ihrem „redaktionellen" Kerngehalt gehört.[65]

---

61 BT Drs. 13/7385, dort S. 19.

62 BGH, 12.11.2009, Az. I ZR 166/07 – marions-kochbuch.de; OLG Köln, 28.05.2002, Az. 15 U 221/01.

63 BGH, 12.11.2009, Az. I ZR 166/07 – marions-kochbuch.de; BGH, 18.10.2007, Az. I ZR 102/05 – ueber18.de.

64 BGH, 01.04.2004, Az. I ZR 317/01 – Schöner Wetten; BGH, 18.10.2007, Az. I ZR 102/05 – ueber18.de.

65 Nordemann in Fromm/Nordemann, Urheberrecht, 11. Aufl. 2014, § 97 Rn. 165.

Hieran dürfte auch die aktuelle Rechtsprechung des Gerichtshofs der Europäischen Union nichts ändern.[66] Nach Ansicht des Gerichtshofs liegt keine öffentliche Wiedergabe i.S.v. Art. 3 Abs. 1 der Infosoc-Richtlinie vor, wenn Dritte auf einer Webseite (per Linking bzw. Framing) ein bereits auf einer anderen Website mit Erlaubnis der Urheberrechteinhaber für alle Internetnutzer frei zugänglich gemachtes Werk einbinden.

In den hier gegenständlichen Konstellationen handelt es sich bei der eingebundenen Quelle jedoch gerade nicht um ein mit Zustimmung des Rechteinhabers für die Öffentlichkeit bestimmtes kostenloses Angebot. Zum einen werden die Werke regelmäßig bereits auf die Server der Host-Provider ohne Zustimmung der Rechteinhaber hochgeladen. Zum anderen werden Werke eingebunden, die von den Rechteinhabern nur gegen Entgelt angeboten werden und somit denknotwendig nur für das erwerbende Publikum, nicht jedoch für jedermann bestimmt sind.

Neben einer Haftung für eigene oder zu eigen gemachte Inhalte kommt auch bei Portalseiten und Plattformen eine Haftung als Gehilfe in Betracht, etwa wenn rechtswidrige Inhalte nach Kenntniserlangung nicht gelöscht oder gleichartige Rechtsverletzungen nicht verhindert werden.[67]

Auch wenn eine Haftung als Täter oder Teilnehmer somit an sich zu bejahen wäre, können die Verantwortlichen meist jedoch nicht in Anspruch genommen werden. Denn die Angebote werden regelmäßig anonym aus dem (nichteuropäischen) Ausland betrieben und sind unter ausländischen Top-Level-Domains registriert, so dass die Domaininhaber nicht identifiziert werden können.

Unabhängig von den vorstehenden juristischen Überlegungen sind die Betreiber solcher Angebote daher faktisch kaum zu fassen und folglich zivilrechtlich nahezu nie zur Verantwortung zu ziehen.

---

66 EUGH, 21.10.2014, Az. C-348/13 – BestWater International/Mebes u.a.; EuGH, 13.02.2014, Az. C-466/12 – Svensson u.a./Retriever Sverige AB.

67 Vgl. A.II.2.a.; LG Frankfurt a.M., 05.02.2014, Az. 2-06 O 319/13.

bb. Die Haftung als Störer

Bei Portal- und Plattformbetreibern, deren Dienste auf Rechtsverletzungen ihrer Nutzer angelegt sind, wird in der Regel von einem Zueigenmachen der entsprechenden Inhalte auszugehen sein.

Soweit für fremde Inhalte im Einzelfall dennoch eine täterschaftliche Haftung ausscheiden sollte, ist bei Verletzung zumutbarer Prüfpflichten weiterhin eine Haftung als Störer möglich.[68] Dies gilt genauso bei einer Einbindung rechtswidriger Inhalte, z.B. per Hyperlink.[69]

Der Umfang der Prüfungspflichten, die denjenigen treffen, der einen Hyperlink setzt oder aufrechterhält, richtet sich nach der Erkennbarkeit der Rechtswidrigkeit der eingebundenen Inhalte, dem Gesamtzusammenhang, in dem der Hyperlink verwendet wird und dem Zweck des Hyperlinks.[70] Die Zumutbarkeit einer Prüfung ist zumindest nach Kenntnisverschaffung gegeben.[71]

b. Gesetzgeberischer Handlungsbedarf

Anders als beim Betrieb von Host-Providern, die teilweise zumindest über ein Impressum (im Ausland) verfügen, erweist sich die Inanspruchnahme weniger aufgrund bestehender Haftungsprivilegien[72] als schwierig. Es ist vielmehr die auf technisch höchstem Niveau erfolgende Verschleierung der Identität der Betreiber von Portalseiten und Plattformen, die eine an sich zivilrechtlich unkomplizierte Inanspruchnahme verhindert.

---

68 Vgl. hierzu oben unter A.II.2.a.bb.

69 BGH, 01.04.2004, Az. I ZR 317/01 – Schöner Wetten.

70 BGH, 01.04.2004, Az. I ZR 317/01 – Schöner Wetten.

71 Vgl. Nordemann in Fromm/Nordemann, Urheberrecht, 11. Aufl. 2014, § 97 Rn. 165.

72 Diese dürften beim Setzen von Hyperlinks schon nicht einschlägig sein, vgl. Art. 21 Abs. 2 S. 1 E-Commerce Richtlinie; BGH, 01.04.2004, Az. I ZR 317/01 – Schöner Wetten; BGH, 18.10.2007, Az. I ZR 102/05 ueber18.de; Reber in Möhring/Nicolini, Urheberrecht, 3. Aufl. 2014, § 97 Rn. 76.

Um eine zivilrechtliche Rechtsdurchsetzung gegen die zahlreichen hochgradig kriminell agierenden Plattformen zu ermöglichen, wäre die Schaffung einheitlicher Rechtsstandards im Hinblick auf die Vergabe von Top-Level-Domains daher sicherlich eine der effektivsten Maßnahmen. So sollte weltweit eine den Domainrichtlinien der DENIC[73] entsprechende Klardatenpflicht bei der Domainregistrierung eingeführt werden, um die Identifizierung und Inanspruchnahme der Domaininhaber zu ermöglichen. Die Pflicht zur Erhebung und Verifizierung von Klardaten bei der Domainregistrierung wird auch von der weltweit für die Vergabe von Namen und Adressen im Internet übergeordnet zuständigen ICANN[74] angestrebt.[75] Zur Vermeidung der Angabe von Falschdaten sollten zudem entsprechende Kontroll- bzw. Verifizierungsverfahren vorgesehen werden.

Eine Domain-Vergabe nach diesen Standards würde zwar nicht verhindern, dass Rechtsverletzer ihre Domains mit falschen Daten registrieren. Die Top-Level-Domains ließen sich dann jedoch durch die jeweiligen Registrierungsstellen bei nachweislich missbräuchlicher Anmeldung löschen.

Da eine zivilrechtliche Inanspruchnahme aktuell an der fehlenden Möglichkeit einer Identifizierung der Verantwortlichen scheitert, sind Rechteinhaber seit Jahren gezwungen, auf das Strafrecht zurückzugreifen. Da es sich vielfach um hochprofitable „Geschäftsmodelle" handelt, die mit erheblicher krimineller Energie und teils auch mit Methoden des organisierten Verbrechens betrieben werden, ist dies auch angemessen. Neben gewerbsmäßigen Urheberrechtsverletzungen werden den Betreibern derartiger Seiten nicht selten auch schwere Straftaten, wie räuberische Erpressung oder Nötigung vorgeworfen.[76]

---

73 Vgl. insbesondere die Domainrichtlinien VI. bis IX., abrufbar unter http://www.denic.de/domainrichtlinien.html.

74 Internet Corporation for Assigned Names and Numbers.

75 Abrufbar unter: http://www.spiegel.de/netzwelt/web/domainregistrierung-icann-will-vorratsdatenspeicherung-durchsetzen-a-893542.html.

76 Vgl. hierzu http://www.welt.de/wirtschaft/article133912583/So-brutal-laeuft-das-Geschaeft-hinter-Kinox-to.html.

Das Urheberstrafrecht als Teil des sog. Nebenstrafrechts hängt jedoch vielfach noch im analogen Zeitalter fest. Die Behörden klagen nicht nur über eine ungenügende personelle Ausstattung. Vielmehr müssten Polizei und Staatsanwaltschaft eine technische Expertise aufweisen, die es ihnen ermöglicht, mit den sehr dynamischen Veränderungen im Internet mitzuhalten.[77] Hieran fehlt es vielfach genauso wie an der erforderlichen technischen Infrastruktur. Nicht zuletzt bedarf es auch einer Erweiterung der rechtlichen Befugnisse der Strafverfolgungsbehörden.[78]

Es wird daher bereits seit Jahren die Einrichtung von Schwerpunkt-Staatsanwaltschaften für (Urheberrechts-)Straftaten im Internet gefordert, die über die zur Verfolgung von Internetdelikten erforderliche Ausstattung und Sachkenntnis verfügen.

Gleichermaßen wäre die Schaffung einheitlicher Rechtsstandards zur Verbesserung der internationalen Zusammenarbeit bzw. Rechtsdurchsetzung eines der wesentlichen umzusetzenden politischen Vorhaben.

Allgemeine Aussagen dazu finden sich zumindest im Koalitionsvertrag[79] und in der digitalen Agenda[80] wieder. Neben dem Ausbau verbindlicher internationaler Vereinbarungen zum Schutz vor Rechtsverletzungen soll auch das nationale Strafrecht eine Anpassung an das digitale Zeitalter erfahren. Verbunden damit ist die geplante Verbesserung der sachlichen und personellen Ausstattung der deutschen Sicherheitsbehörden.

---

77 Vgl. hierzu etwa http://www.heise.de/newsticker/meldung/Polizeigewerkschaften-Bayern-fehlen-Cybercops-2403188.html.

78 Vgl. hierzu etwa http://www.sueddeutsche.de/digital/cyberkriminalitaet-die-lampe-wird-schwaecher-1.2230165

79 Koalitionsvertrag, dort S. 103 (abrufbar unter: https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf).

80 Digitale Agenda 2014-2017, dort S. 35 (abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf).

3. Die Inanspruchnahme auf Schadenersatz

Eine Haftung auf Schadenersatz kommt grundsätzlich nur bei der rechtswidrigen öffentlichen Zugänglichmachung eigener oder zu eigen gemachter fremder Inhalte in Betracht.[81]

Strukturell rechtsverletzende Portalseiten und Plattformen dürften regelmäßig täterschaftlich haften. Auch wenn ein Schadenersatzanspruch demnach häufig zu bejahen sein dürfte, stellt sich auch hier vor allem die Problematik der mangelnden zivilrechtlichen Verfolgbarkeit aufgrund professionell verschleierter Strukturen.

Vor diesem Hintergrund kommt insbesondere der im Strafrecht verankerten Schadenswiedergutmachung und dem Täter-Opfer-Ausgleich gemäß §§ 46, 46a StGB vielfach eine besondere Bedeutung zu. Die Schadenswiedergutmachung und der Täter-Opfer-Ausgleich sollen die Belange der Geschädigten, insbesondere deren Interesse an einer Schadenskompensation, berücksichtigen.[82]

IV. Die Inanspruchnahme der Access-Provider

1. Die Inanspruchnahme auf Unterlassung und Beseitigung

a. Der Anspruch aus § 97 UrhG und seine Grenzen

Gemäß Art. 8 Abs. 3 der Infosoc-Richtlinie sowie Art. 11 S. 3 der Enforcement-Richtlinie haben die Mitgliedstaaten sicher zu stellen, dass „gerichtliche Anordnungen gegen Vermittler“ möglich sind, deren Dienste zu Urheberrechtsverletzungen genutzt werden. Als Vermittler werden insofern auch Access-Provider angesehen, die den Zugang zum Internet und damit auch zu illegalen Angeboten vermitteln.[83]

---

81 Vgl. A.III.2.a.aa.

82 BT-Drs. 12/6853, S. 21.

83 EuGH, 24.11.2011, Rs. C-70/11 – Scarlet Extended/SABAM.

Die gerichtlichen Anordnungen beinhalten Maßnahmen, die sowohl bereits begangene Rechtsverletzungen beenden, als auch neue Rechtsverletzungen verhindern.[84] Im Falle eines Access-Providers läuft dies auf eine Verhinderung bzw. Erschwerung des Zugangs zu den entsprechenden Inhalten im Wege einer „Sperrverfügung" hinaus.

Weder Art. 8 Abs. 3 der Infosoc-Richtlinie noch Art. 11 S. 3 der Enforcement-Richtlinie wurden ins deutsche Recht umgesetzt. Der deutsche Gesetzgeber sah keinen Umsetzungsbedarf, da die Möglichkeit der Inanspruchnahme von Vermittlern auf Beseitigung und Unterlassung bereits durch das allgemeine Rechtsinstitut der Störerhaftung ausreichend gewährleistet sei.[85]

Einer Inanspruchnahme der Access-Provider als Störer auf Unterlassung stehen die Haftungsprivilegien der §§ 7 ff. TMG zwar nicht direkt entgegen, da diese auf Unterlassungsansprüche keine unmittelbare Anwendung finden.[86] Die grundsätzlichen Wertungen der §§ 7 ff. TMG – beim Access-Provider der §§ 7, 8 TMG – fließen jedoch im Rahmen der Zumutbarkeit von Prüfpflichten ein.[87]

So schließt auch das Hanseatische Oberlandesgericht die Möglichkeit einer Inanspruchnahme von Access-Providern als Störer nicht von vornherein aus. Filterungen, IP-, URL- und DNS-Sperren hält das Oberlandesgericht allein auf Grundlage der Störerhaftung jedoch für unzulässig. Um den Verhältnismäßigkeitsgrundsatz zu wahren, müsste vielmehr eine hinreichend konkrete Rechtsgrundlage die Voraussetzungen der Maßnahmen im Einzelnen bestimmen.[88]

---

84 EuGH, 24.11.2011, Rs. C-70/11 – Scarlet Extended/SABAM; Dies ergibt sich zudem aus Art. 12 Abs. 3 sowie den Erwägungsgründen 40, 45, 47 und 48 der E-Commerce-Richtlinie.

85 BT-Drs. 14/6098, S. 23; BT-Drs. 15/38, S. 39f.; BT-Drs. 16/5048, S. 30 f.

86 Siehe oben unter A.II.2.a.bb.

87 Hanseatisches OLG, 21.11.2013, Az. 5 U 68/10 (Sperrung von 3dl.am).

88 Hanseatisches OLG, 21.11.2013, Az. 5 U 68/10 (Sperrung von 3dl.am).

Eine solche Rechtsgrundlage existiert im deutschen Recht derzeit jedoch nicht. Auch eine unmittelbare Anwendung des Art. 8 Abs. 3 der Infosoc-Richtlinie als Anspruchsgrundlage scheidet bereits mangels horizontaler Drittwirkung aus.[89]

Dagegen erachtet das Oberlandesgericht Köln das Institut der Störerhaftung zwar grundsätzlich als ausreichende Anspruchsgrundlage für DNS- und IP-Sperren. Lediglich für Filtermaßnahmen sei aufgrund der besonderen Schutzwürdigkeit des Fernmeldegeheimnisses (auch wenn Art. 10 GG nicht unmittelbar zwischen Privaten gilt) eine spezialgesetzliche Grundlage erforderlich. In einer Abwägung der betroffenen Interessen wird im Ergebnis jedoch die Zumutbarkeit von DNS- und IP-Sperren abgelehnt.[90]

Eine höchstrichterliche Klärung der Zulässigkeit von Sperrverfügungen nach deutschem Recht steht bislang noch aus; es sind jedoch bereits zu beiden Entscheidungen Revisionen beim Bundesgerichtshof anhängig[91].

b. Gesetzgeberischer Handlungsbedarf

Jedenfalls in Fällen, in denen weder die primär verantwortlichen Uploader noch die Betreiber der Portalseiten und Plattformen für die Geschädigten greifbar sind, sollte zumindest der Zugang zu den rechtsverletzenden Inhalten gesperrt werden können.

Hierfür bedarf es der Normierung einer Anspruchsgrundlage, mit der Access-Provider zur Sperrung von Internetseiten bzw. zur Erschwerung des Zugangs zu rechtsverletzenden Inhalten verpflichtet werden können. Denkbar wäre es, derartige Sperrungen mit einem Warnhinweis bzw. weiteren Informationen zur Aufklärung der Nutzer zu verbinden.

---

89 Vgl. EuGH, 07. 06. 2007, Rs. C-80/06, Carp Snc di L. Moleri e V. Corsi/Ecorad Srl.; EuGH, 05.10.2004, Rs. C-397/01 bis C-403/01 Bernhard Pfeiffer u.a./Deutsches Rotes Kreuz, Kreisverband Waldshut e.V.; EuGH, 14.07.1994, Rs. C-91/92, Faccini Dori.

90 OLG Köln, 18.07.2014, Az. 6 U 192/11 (Sperrung von Goldesel.to).

91 Az. I ZR 3/14, Vorinstanz Hanseatisches OLG, 21.11.2013, Az. 5 U 68/10; Az. I ZR 174/14, Vorinstanz OLG Köln, 18.07.2014, Az. 6 U 192/11.

Alternativ sollte zur Umsetzung der europarechtlichen Vorgaben gemäß Art. 8 Abs. 3 der Infosoc-Richtlinie sowie Art. 11 S. 3 der Enforcement-Richtlinie das Institut der Störerhaftung richtlinienkonform ausgelegt werden. Denn nach ständiger Rechtsprechung des Gerichtshofs der Europäischen Union obliegt die Verpflichtung der Mitgliedstaaten, das in einer Richtlinie vorgesehene Ziel zu erreichen, allen Trägern öffentlicher Gewalt und damit auch den nationalen Gerichten. Ebenso verhält es sich mit der Pflicht aus Art. 4 Abs. 3 EU, alle zur Erfüllung dieser Verpflichtung geeigneten Maßnahmen allgemeiner oder besonderer Art zu treffen (sog. effet utile).[92] Die nationalen Gerichte sind somit verpflichtet, das innerstaatliche Recht richtlinienkonform auszulegen, um so dem Umsetzungsgebot in Art. 288 Abs. 3 AEUV sowie dem effet utile nachzukommen und dem Europarecht zur Geltung zu verhelfen.[93]

Die Zulässigkeit solcher (in Bezug auf die zu treffenden Maßnahmen nicht näher bestimmter) Sperranordnungen gegenüber Access-Providern hat der Gerichtshof der Europäischen Union im Frühjahr 2014 in einem Vorabentscheidungsverfahren bestätigt.[94] Der Gerichtshof hat dabei klargestellt, dass die zur Durchführung der Anordnung vom Access-Provider getroffenen Maßnahmen hinreichend wirksam sein müssen, um einen wirkungsvollen Schutz der Rechte des geistigen Eigentums sicherzustellen. Internetnutzer, die die Dienste des Access-Providers in Anspruch nehmen, müssen vor einem Zugriff auf die ihnen unter Verletzung dieser Rechte zugänglich gemachten Schutzgegenstände zuverlässig abgehalten werden.

---

92 EuGH, 14.07.1994, Rs. C-91/92, Faccini Dori.

93 EuGH, 05.10.2004, Rs. C-397/01 bis C-403/01 Bernhard Pfeiffer u.a./Deutsches Rotes Kreuz, Kreisverband Waldshut e.V.

94 EuGH, 27.03.2014, Rs. C-314/12 – UPC Telekabel Wien/Constantin Film Verleih auf Vorlage des Obersten Gerichtshofes der Republik Österreich mit Beschluss vom 11.05.2012, Az. 4 Ob 6/12d. Im konkreten Fall ging es um die Zulässigkeit einer Sperrverfügung gegenüber einem Access-Provider bezogen auf die strukturell rechtsverletzende Internetseite kino.to.

Weist der Access-Provider nach, alle zumutbaren Maßnahmen ergriffen zu haben, muss allerdings die Möglichkeit einer Haftungsbefreiung bestehen. Dies muss der Provider geltend machen können, bevor ihm eine Sanktion auferlegt wird. Um in das Grundrecht der Internetnutzer auf Informationsfreiheit nicht in ungerechtfertigter Weise einzugreifen, darf Internetnutzern nicht unnötig die Möglichkeit vorenthalten werden, in rechtmäßiger Weise Zugang zu den verfügbaren Informationen zu erlangen.

Angesichts dieser Entscheidung bleibt zu hoffen, dass der Bundesgerichtshof dem europarechtlichen Auftrag auch über das Rechtsinstitut der Störerhaftung genügen und die Zulässigkeit sowie Zumutbarkeit entsprechender Anordnungen bejahen wird.

In anderen europäischen Ländern, wie etwa in Belgien, Dänemark, Finnland, Frankreich, Großbritannien, Irland, Italien, den Niederlanden, Schweden, Spanien und Österreich[95] sind entsprechende gerichtliche Anordnungen jedenfalls bereits an der Tagesordnung. Wollte man die in Europa vorherrschende Maxime in Worte fassen, so würde sie vermutlich lauten: *„Ist das Löschen an der illegalen Quelle unmöglich, muss wenigstens der Zugang zur Quelle gesperrt werden“.* Diese Maxime sollte auch in Deutschland als Leitbild dienen.

2. Die Inanspruchnahme auf Schadenersatz

Nach § 8 TMG ist der Access-Provider bei einer reinen Durchleitung von Informationen von der Schadenersatzhaftung freigestellt, sofern er nicht aktiv in die Kommunikation eingreift.

[95] In Österreich hat der OGH nach Beantwortung der Vorlagefrage durch den EuGH die (nicht näher bestimmte) Anordnung gegenüber UPC Telekabel Wien auf Sperrung der Internetseite kino.to mit Beschluss vom 24.06.2014, Az. 4 Ob 71/14s für zulässig erklärt. Der OGH betonte dabei die Notwendigkeit einer europarechtskonformen Auslegung des nationalen Rechts.

B. Mittels Filesharing begangene Urheberrechtsverletzungen

Die zweite wesentliche Erscheinungsform von im Internet begangenen Urheberrechtsverletzungen ist das Filesharing[96].

Im Gegensatz zum File- und Streamhosting, bei dem die Inhalte auf einem Server des Host-Providers gespeichert werden, liegen beim Filesharing die Inhalte dezentral auf den Rechnern der Nutzer. Um die Inhalte tauschen zu können, müssen sich die Nutzer über eine spezielle Peer-to-Peer-Software miteinander verbinden. Diese Programme sind so konzipiert, dass ein Download von Inhalten regelmäßig nur möglich ist, wenn zugleich auch ein Upload erfolgt. Auf diese Weise ist gewährleistet, dass stets neue Inhalte zum Tausch angeboten werden.

I. Die Akteure

1. Die Access-Provider

Der Access-Provider leistet auch beim Filesharing einen zwangsläufig kausalen Beitrag zur illegalen Verbreitung der Inhalte, indem er den Zugang zum Internet und damit auch zu den illegalen Angeboten vermittelt. Entscheidend ist insoweit, dass der Access-Provider auf Basis seiner bestehenden Kundenverhältnisse als einziger in der Lage ist, die Rechtsverletzungen einem bestimmten Anschlussinhaber zuzuordnen.

2. Die Hotspot-Betreiber

Tauschbörsen werden jedoch nicht nur über (privat) registrierte Internetanschlüsse genutzt. Zunehmend werden auch (kostenlose) Hotspots missbraucht, um im Schutz der Anonymität Rechtsverletzungen zu begehen.

---

96 Filesharing-Netzwerke werden auch als Tauschbörsen oder Peer-to-Peer-Netzwerke bezeichnet.

Dabei gibt es Hotspots, die von den Access-Providern selbst oder von öffentlicher Hand betrieben werden (etwa in Rathäusern). Darüber hinaus werden kostenlose Hotspots häufig – mit oder ohne eine vorhergehende Registrierung – in Cafés oder Hotels angeboten, da hierdurch die Attraktivität des Lokals gefördert wird.

Daneben betreiben aber auch Privatpersonen kostenlose offene WLAN-Netze ohne jedwede Registrierung der Nutzer. Hierbei wird der eigene Internetzugang meist aus ideellen Gründen der Allgemeinheit zur Verfügung gestellt. Häufig gehören die Betreiber der offenen WLAN-Netze zu Initiativen, die die Förderung offener Netze um jeden Preis forcieren.[97]

3. Die Uploader

Die Nutzer der Tauschbörsen bieten anderen Nutzern urheberrechtlich geschützte Inhalte über eine eigens installierte Peer-to-Peer-Software Dritten zum Download an und machen diese hierdurch illegal öffentlich zugänglich. Der Upload ist unweigerlich mit dem eigentlich bezweckten Download eines Werkes verbunden, der für sich genommen ebenfalls eine unzulässige Vervielfältigung darstellt.

Ab dem Zeitpunkt des illegalen Angebots hat ein Nutzer die weitere Verbreitung der Datei nicht mehr in der Hand, da sich diese – zumeist lawinenartig – weiter verbreitet.[98]

Wie bei der Darstellung der Rechtsverletzungen über File- und Streamhosting sollen sich auch die nachfolgenden Ausführungen auf die Durchsetzung der Inanspruchnahme gegenüber den Intermediären konzentrieren.

97 Etwa die Initiative „Freifunk“, abrufbar unter: www.freifunk.net.

98 OLG Köln, 07.10.2013, Az. 6 W 84/13.

II. Die Inanspruchnahme der Access-Provider

1. Die Inanspruchnahme auf Drittauskunft

a. Der Anspruch aus § 101 UrhG und seine Grenzen

aa. Gewerbliches Ausmaß der Rechtsverletzung nicht (mehr) erforderlich

Auch beim Filesharing setzt die Inanspruchnahme des Uploaders zwingend dessen Identifikation voraus. Im Gegensatz zum File- und Streamhosting kann im Rahmen der Tauschbörsenkommunikation die IP-Adresse des Internetanschlusses, von dem aus die Rechtsverletzung begangen wurde, vom Rechteinhaber selbst ermittelt werden. Anders als beim File- und Streamhosting stehen andere als die zwangsläufig bei jeder Internetkommunikation anfallenden Logdaten von vornherein nicht zur Verfügung.

Exakt diesen Fall regelt § 101 Abs. 2 Nr. 3, Abs. 3 Nr. 1 i.V.m. Abs. 9 UrhG: Der Rechteinhaber kann den Access-Provider unter Verwendung dieser Logdaten gemäß § 101 Abs. 2 Nr. 3, Abs. 3 Nr. 1 UrhG nach Erlass einer richterlichen Gestattungsanordnung auf Beauskunftung desjenigen Kunden in Anspruch nehmen, über dessen Internetanschluss die Rechtsverletzung begangen wurde.

Darüber hinaus umfasst der Auskunftsanspruch in Reseller-Konstellationen auch die Benutzerkennung, mit deren Hilfe der Reseller Namen und Anschrift seines zugehörigen Kunden beauskunften kann.[99]

---

[99] OLG Köln, 27.11.2012, Az. 6 W 181/12; OLG Köln, 27.11.2012, Az. 6 W 191/12; LG München I, 10.11.2014, Az. 7 O 21345/14; AG Koblenz, 05.01.2012, Az. 131 C 2114/11; LG Frankenthal, 13.09.2012, Az. 6 S 2/12; Mitteilung des Bundesdatenschutzbeauftragten, http://www.bfdi.bund.de/DE/Datenschutz/Themen/ Telefon_Internet/InternetArtikel/AuskunftsrechtsBeiUrheberrechtsverstoss.html.

Nach der früher herrschenden Rechtsprechung war neben der Offensichtlichkeit der Rechtsverletzung auch deren gewerbliches Ausmaß erforderlich. Streit bestand jedoch darüber, wann von einem gewerblichen Ausmaß der Rechtsverletzung auszugehen war.[100]

Diesen Meinungsstreit hat schließlich der Bundesgerichtshof mit einer Grundsatzentscheidung aus dem Jahr 2012 überflüssig gemacht: Nach Ansicht des BGH ist für den Auskunftsanspruch nach § 101 Abs. 2 S. 1 Nr. 3 UrhG generell nicht erforderlich, dass die rechtsverletzenden Tätigkeiten das Urheberrecht oder ein anderes nach dem Urheberrechtsgesetz geschütztes Recht in gewerblichem Ausmaß verletzt haben. Ebenso setze daher auch die Begründetheit des Antrags nach § 101 Abs. 9 UrhG kein besonderes und insbesondere kein gewerbliches Ausmaß der Rechtsverletzung voraus, sondern bestehe vielmehr bei *jeder* Rechtsverletzung.[101]

bb. Anspruch wegen fehlender Speicherpflicht oftmals nicht durchsetzbar

Um die für eine Identifizierung erforderliche Auskunft erteilen zu können, muss durch den Access-Provider eine Speicherung der Verbindungsdaten, also die Zuordnung des Anschlusses zu einer dynamischen IP-Adresse zu einem bestimmten Zeitpunkt, erfolgen.

---

100 Nach Ansicht des OLG Köln war das gewerbliche Ausmaß der Rechtsverletzung nur während der „aktuellen Verkaufs- und Verwertungsphase" des Werkes erreicht. Die aktuelle Verkaufs- und Verwertungsphase begrenzte das OLG Köln dabei in aller Regel auf die ersten sechs Monate nach Erstveröffentlichung des Werkes auf DVD/Blu-Ray, CD etc. Vgl. hierzu exemplarisch OLG Köln, 05.07.2011, Az. 6 W 121/11. Dagegen hatte nach der Rechtsprechung des OLG München eine Rechtsverletzung über eine Internettauschbörse grundsätzlich ein gewerbliches Ausmaß, ohne dass es weiterer Umstände bedurfte, vgl. exemplarisch Az. 26.07.2011, Az. 29 W 1268/11.

101 BGH, 19.04.2012, Az. I ZB 80/11 – Alles kann besser werden; BGH, 19.04.2012, Az. I ZB 77/11.

Nachdem der Gerichtshof der Europäischen Union die Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt hat[102], ist eine Verpflichtung der Access-Provider zur Speicherung der Daten zu Strafverfolgungszwecken vorerst nicht absehbar. Eine Speicherpflicht, die mit den verschiedenen zivilrechtlichen Drittauskunftsansprüchen korrespondiert, bestand ohnehin zu keinem Zeitpunkt.

Aktuell besteht daher weder unter straf- noch zivilrechtlichen Gesichtspunkten eine gesetzliche Verpflichtung der Access-Provider zur Speicherung von Verbindungsdaten. Die Entscheidung für oder gegen eine Speicherung liegt allein im Ermessen eines Access-Providers.

Die Speicherpraxis der Provider reicht von einer Dauer von 48 Stunden bis zu 7 Tagen. Teilweise werden die Verbindungsdaten aber auch nur während der laufenden Verbindung vorgehalten. Die Durchsetzung des Auskunftsanspruchs scheitert daher häufig daran, dass die zur Auskunftserteilung erforderlichen Daten im Zeitpunkt des Auskunftsersuchens bereits gelöscht wurden.

Dies führt zu dem unter rechtsstaatlichen Gesichtspunkten unbilligen Ergebnis, dass Rechtsverletzungen bzw. Straftaten beim einen Provider aufgedeckt und geahndet werden können, beim anderen hingegen sanktionslos bleiben (sog. safe harbour).[103]

Damit die Daten vor Erteilung der Auskunft nicht gelöscht werden, werden Access-Provider mittels gerichtlicher Anordnung zur Speicherung der Daten verpflichtet. Denn ein Anspruch auf Speicherung von Verkehrsdaten rein auf Zuruf (sog. Quick-Freeze) wird nach überwiegender Rechtsprechung von § 101 Abs. 2 Nr. 3, Abs. 9 UrhG nicht begründet. Wird der Access-Provider während laufender Verbindung lediglich davon in Kenntnis gesetzt, dass der Rechteinhaber eine Gestattung der Auskunft über bestimmte Verkehrsdaten nach § 101 Abs. 9 UrhG bean-

---

102 EuGH, 08.04.2014, Rs. C-293/12 und C-594/12, Digital Rights Ireland Ltd./Minister for Communications u.a.

103 Da nicht speichernde Access-Provider jedenfalls für diejenigen Kunden attraktiver sind, die über ihren Internetanschluss Rechtsverletzungen begehen wollen, dürfte dieser Umstand auch zu einer Wettbewerbsverzerrung führen.

tragen möchte, muss er diese Daten somit nicht speichern. Zur Begründung wird angeführt, dass erst die Gestattung bewirke, dass der Access-Provider die Daten nicht mehr sanktionslos löschen dürfe, da er sich sonst schadenersatzpflichtig mache.[104]

Derartige Sicherungsanordnungen werden von sämtlichen aktuell mit Verfahren nach § 101 Abs. 9 UrhG befassten Gerichten ohne Weiteres als zulässig erachtet. Gestützt werden die Anordnungen zumeist auf § 49 FamFG oftmals in Verbindung mit § 101 Abs. 2, 9 UrhG.

Nach der überwiegenden Rechtsprechung[105] ist dabei unerheblich, ob der Access-Provider auf gespeicherte Daten oder lediglich auf Daten aus laufenden Verbindungen zugreifen kann.

Lediglich nach Ansicht des Oberlandesgerichts Düsseldorf kann ein speicherunwilliger Access-Provider nicht mittels einstweiliger Anordnung zur Speicherung der Daten während der laufenden Verbindung verpflichtet werden. Dem Access-Provider sei es nicht zumutbar, dass er Daten, die er zu eigenen Zwecken nicht benötigt, allein zum Zwecke der Drittauskunft erheben muss. Denn das reine Vorhandensein der Daten in den Systemen des Access-Providers stelle noch keine Erhebung der Daten dar. Die hierfür erforderliche willentliche Kenntnisnahme durch aktives Handeln würde vielmehr erst im Zuge der (manuellen) Ermittlung der Daten zum Zwecke der Speicherung erfolgen. Erst die Speicherung und die ihr notwendig vorgelagerte Ermittlung der Daten wären somit eine Erhebung im Sinne von § 3 Abs. 3 BDSG. Für eine Erhebung zum Zweck der Auskunftserteilung würde es zudem an einer legitimierenden gesetzlichen Grundlage fehlen.[106]

---

104 OLG Frankfurt a.M., 17.11.2009, Az. 11 W 54/09 – Speicherung auf Zuruf; OLG Hamm, 02.11.2010, Az. I-4 W 119/10; OLG München, 21.11.2011, Az. 29 W 1939/11; OLG Düsseldorf, 30.05.2011, Az. I-20 W 127/10.

105 Etwa LG München I, 30.08.2011, Az. 21 O 18938/11; OLG Köln, 09.06.2011, Az. 6 W 159/10; Hanseatisches OLG, 17.02.2010, Az. 5 U 60/09 und 5 W 78/09.

106 OLG Düsseldorf, 07.03.2013, Az. I-20 W 162/11.

Nach zutreffender Ansicht findet die Erhebung der Daten jedoch bereits mit der Bereitstellung der Internetverbindung statt. „Erheben" im datenschutzrechtlichen Sinn ist gem. § 3 Abs. 3 BDSG das Beschaffen von Daten über den Betroffenen. Dies ist die gezielte Kenntniserlangung und Begründung der Verfügungsgewalt über die Daten zu eigenen Zwecken. Das Tätigwerden der erhebenden Stelle kann dabei mittels automatisierter Abrufverfahren erfolgen und es genügt selbst die bloße Wahrnehmbarkeit eines Datums (wie z.B. beim Aufstellen einer Überwachungskamera).[107] Während der Aufrechterhaltung der Internetverbindung werden die Daten auch (zwischen)gespeichert.[108]

Sowohl die Erhebung als auch die im Zuge dessen erfolgende temporäre Speicherung der IP-Adressen (sowie der weiteren zur Internetverbindung bzw. Session gehörigen Daten, wie z.B. Start- und Ende der Verbindung, übertragenes Datenvolumen, Nutzerkennung) erfolgt zum Aufbau und zur Aufrechterhaltung der Internetverbindung und somit im Einklang mit § 96 Abs. 1 S. 1, 2 Alt. 1 TKG, der eine datenschutzrechtliche Erlaubnisnorm im Sinne des § 4 BDSG darstellt.

cc. Prohibitive Höhe der Gerichtsgebühren

Die Identifizierung der Rechtsverletzer ist für Rechteinhaber vielfach mit derart hohen Gerichtskosten verbunden, dass eine Rechtsverfolgung an hohen Gerichtsgebühren scheitert, obwohl der in § 101 Abs. 9 UrhG vorgesehene Richtervorbehalt verfassungsrechtlich noch nicht einmal geboten wäre.[109]

Verantwortlich hierfür ist eine bundesweit uneinheitliche Bemessung der Gerichtskosten für Anträge nach § 101 Abs. 9 UrhG.

---

107 LG Hamburg, 11.03.2009, Az. 308 O 75/09; Buchner in Taeger/Gabel, BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, § 3 BDSG Rn. 25 f.

108 Buchner in Taeger/Gabel, BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, § 3 BDSG Rn. 28 f.

109 BVerfG, 02.03.2010, Az. 1 BvR 256/08 – Vorratsdatenspeicherung.

Vor Inkrafttreten des Zweiten Kostenrechtsmodernisierungsgesetzes im August 2013 waren Gerichtskosten für Anträge nach § 101 Abs. 9 UrhG in § 128e KostO geregelt. Gemäß § 128e Abs. 1 KostO fiel für die *Entscheidung* über den Antrag nach § 101 Abs. 9 UrhG eine Festgebühr in Höhe von 200,- Euro an. Die neue Gebührenregelung in Ziff. 15213 KV GNotKG setzt die Gebühr von 200,- Euro nunmehr für *Verfahren* über den Antrag an.

Umstritten ist seit jeher, wie die Begriffe *Entscheidung* bzw. *Verfahren über den Antrag* auszulegen sind:

Nach Ansicht des Oberlandesgerichts München ist sowohl nach § 128e KostO als auch nach Ziff. 15213 KV GNotKG hinsichtlich der Festgebühr auf formale und nicht auf inhaltliche Kriterien abzustellen. Unabhängig von der Anzahl der von einem Antrag nach § 101 Abs. 9 UrhG umfassten urheberrechtlich geschützten Werke fällt die Gebühr daher in einem formellen Verfahren stets nur einmal an.[110] Dieser Ansicht folgen bis auf das Oberlandesgericht Köln sämtliche weiteren, aktuell mit Gestattungsverfahren befassten Gerichte.[111]

Nach Ansicht des Oberlandesgerichtes Köln war „Entscheidung" i.S.d. § 128e Abs. 1 Nr. 4 KostO dagegen nicht als ein formeller, das Verfahren abschließender Beschluss zu verstehen. Vielmehr sei die Entscheidung in der Verbescheidung eines materiellen Antrages nach § 101 Abs. 9 UrhG zu sehen, mit der Folge, dass bei mehreren Werken in einem Beschluss mehrere Entscheidungen in dem genannten Sinne zu treffen seien.[112]

Obwohl in Ziff. 15213 KV GNotKG der Begriff der Entscheidung durch den rein formellen Begriff des Verfahrens ersetzt wurde, hält das Oberlandesgericht Köln auch weiterhin an seiner Rechtsprechung fest und wendet die zu § 128e KostO vertretenen Grundsätze auf Ziff. 15213 KV GNotKG uneingeschränkt an. Der mehrfache Ansatz der Festgebühr wird also weiter damit begründet, dass bei mehreren Werken mehrere materielle Anträge vorlägen, die nunmehr mehrere Verfahren zur

110 OLG München, 19.06.2013, Az. 11 W 701/13.

111 Aktuell sind dies insbesondere die Landgerichte Flensburg, München I sowie Stuttgart.

112 OLG Köln, 23.01.2013, Az. 2 Wx 328/12.

Folge hätten.[113] Das Oberlandesgericht Köln geht folglich gebührenrechtlich von mehreren selbständigen Verfahren aus, obwohl prozessual stets nur ein Verfahren mit einer Akte und einem Aktenzeichen geführt wird.[114]

Im Ergebnis kostet ein Gestattungsantrag nach § 101 Abs. 9 UrhG mit beispielsweise zehn Werken in München 200,- Euro, in Köln fallen dagegen für denselben Antrag Gerichtskosten in Höhe von 2.000,- Euro an.[115]

b. Gesetzgeberischer Handlungsbedarf

aa. Einführung einer Kurzzeitspeicherpflicht

Die Verteidigung von Rechtsgütern mit Verfassungsrang[116] darf nicht daran scheitern, dass die vom Gesetzgeber angesichts massiver Rechtsverletzungen im Internet eingeführten Drittauskunftsansprüche mangels korrespondierender Speicherpflicht vielfach ins Leere laufen.

Access-Provider sollten daher gesetzlich verpflichtet werden, Verbindungsdaten für zivilrechtliche Auskunftsverfahren für einen kurzen Zeitraum – beispielsweise für sieben Tage – vorzuhalten. Einer solchen kurzfristigen Speicherung würde auch nicht entgegenstehen, dass der Gerichtshof der Europäischen Union die Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt[117] hat. Der Bundesgerichtshof hat insofern erst kürzlich entschieden, dass an der Zulässigkeit einer sie-

113 OLG Köln, 11.02.2014, Az. 2 Wx 307/13.

114 Eine tragfähige Erklärung hierzu bleibt das OLG Köln in seiner Entscheidung schuldig.

115 Da bei manchen Access-Providern aufgrund der sehr kurzen Speicherfristen zum Teil täglich Anträge nach § 101 Abs. 9 UrhG gestellt werden müssen, führt diese Rechtsprechung zu einer enormen Potenzierung der Gerichtskosten am LG Köln. Bei fünf Anträgen mit beispielsweise jeweils zehn Werken belaufen sich die Gerichtskosten in Köln auf 10.000,- Euro wöchentlich, während in München für dieselben Anträge nur 1.000,- Euro anfallen.

116 BGH, 19.04.2012, Az. I ZB 77/11; BGH, 19.04.2012, Az. I ZB 80/11 – Alles kann besser werden.

117 EuGH, 08.04.2014, Rs. C-293/12 und C-594/12, Digital Rights Ireland Ltd./Minister for Communications u.a.

bentägigen Speicherung von IP-Adressen auf Grundlage des § 100 TKG kein Zweifel besteht. Eine Speicherfrist von sieben Tagen ist auf das zur Erreichung der legitimen Zwecke des § 100 Abs. 1 TKG notwendige Maß begrenzt. Diese erheblich kürzere Dauer bleibt weit hinter der in der Richtlinie über die Vorratsspeicherung von Daten bestimmten Mindestfrist von sechs Monaten zurück.[118]

Ein generelles Bedürfnis nach einer Speicherung der Verbindungsdaten wird auch auf politischer Ebene weiterhin anerkannt: So hat das Bundesministerium des Innern im August 2014 den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme veröffentlicht[119]. Dieser sieht u.a. Anpassungen im Telemedien- sowie im Telekommunikationsgesetz vor, die den Telemedien- und Telekommunikationsdiensten erlauben, zum Erkennen, Eingrenzen oder Beseitigen von Störungen Nutzungs- bzw. Bestands- und Verkehrsdaten zu erheben und zu speichern. Kritiker schlussfolgern daraus, dass damit die Vorratsdatenspeicherung über die Hintertür wieder eingeführt werden solle.[120]

118 BGH, 03.07.2014, Az. III ZR 391/13; vgl. hierzu auch Leitfaden des BDFI, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile.

119 Abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf;jsessionid=7208BE9ED5CCD1D4BDC4861BB52CED15.2_cid373?__blob=publicationFile.

120 Vgl. hierzu etwa http://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-datenschuetzer-kritisieren-plan-von-de-maiziere-a-987582.html und http://www.handelsblatt.com/politik/deutschland/kritik-an-it-sicherheitsgesetz-vorratsdatenspeicherung-durch-die-hintertuer/7912900.html.

Auch auf der diesjährigen Herbsttagung des Bundeskriminalamts wurde abermals der Ruf nach einer Vorratsdatenspeicherung laut, da mit den herkömmlichen Methoden der Telekommunikationsüberwachung vielfach den neuen Straftaten im bzw. über das Internet nicht mehr beizukommen sei.[121]

bb. Klarstellung der Gerichtskostenregelung in Ziff. 15213 KV GNotKG

Gem. Art. 3 der Enforcement-Richtlinie müssen Verfahren zur Durchsetzung der Rechte des geistigen Eigentums wirksam und dürfen nicht unnötig kompliziert oder kostspielig sein. Mit diesen Vorgaben der Richtlinie ist die von den Kölner Gerichten vorgenommene Auslegung der Ziff. 15213 KV GNotKG nicht vereinbar. Denn das Gestattungsverfahren nach § 101 Abs. 9 UrhG (und damit das Auskunftsverfahren) ist aufgrund der Gebührenmultiplikation nicht nur unnötig kostspielig, sondern verhindert darüber hinaus in zahlreichen Fällen (insbesondere bei kleineren, weniger finanzstarken Rechteinhabern) die Durchsetzung des Drittauskunftsanspruchs zur Ermittlung der Rechtsverletzer.

Eine höchstrichterliche Überprüfung der an den Kölner Gerichten praktizierten Gerichtsgebührenmultiplikation scheidet von Gesetzes wegen aus, da eine (weitere) Beschwerde zum Bundesgerichtshof in Kostensachen gem. § 81 Abs. 3 und 4 GNotKG nicht statthaft ist.

Um die von den anderen Gerichten abweichende Abrechnungspraxis zu beenden, ist somit eine noch deutlichere Klarstellung in Ziff. 15213 KV GNotKG dahingehend geboten, dass die Festgebühr in Höhe von 200,- Euro in einem formellen Verfahren unabhängig von der Anzahl der materiellen Anträge nur einmal anfallen kann.

---

121 Vgl. hierzu http://www.sueddeutsche.de/digital/cyberkriminalitaet-die-lampe-wird-schwaecher-1.2230165

2. Die Inanspruchnahme auf Schadenersatz

Eine Inanspruchnahme des Access-Providers auf Schadenersatz kommt in aller Regel nur bei einer falschen bzw. unvollständigen Auskunft in Betracht. Einfache Fahrlässigkeit genügt hierfür nicht, vielmehr muss der Access-Provider gem. § 101 Abs. 5 UrhG vorsätzlich oder grob fahrlässig gehandelt haben. Derartige Fälle dürften in der Praxis jedoch nahezu ausgeschlossen sein.

III. Die Inanspruchnahme der Hotspot-Betreiber

1. Die Inanspruchnahme auf Drittauskunft

a. Der Anspruch aus § 101 UrhG und seine Grenzen

§ 101 Abs. 2 Nr. 3 UrhG normiert zwar einen Anspruch auf Drittauskunft, dieser Anspruch besteht jedoch gegenüber einer Person, die in gewerblichem Ausmaß für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbringt. Hiervon kann bei einem Betreiber eines für jedermann geöffneten, privaten WLAN-Netzes jedenfalls nicht ohne Weiteres ausgegangen werden.

Doch selbst wenn man einen entsprechenden Anspruch bejahen wollte, wäre der Anspruch nicht durchsetzbar. Denn ähnlich einem Access-Provider müsste auch der Hotspot-Betreiber Bestands- und Verbindungsdaten seiner Nutzer speichern, um eine Auskunft zu einem Nutzer erteilen zu können.

Zwar halten Hotspot-Router in sog. NAT[122]-Tabellen fest, welchem Endgerät bzw. Nutzeraccount eine IP-Adresse nebst Port intern zugewiesen ist. Die Betreiber von Hotspots sind jedoch weder zu einer Registrierung noch zu einer Speicherung der Bestands- und Verbindungsdaten gesetzlich verpflichtet. Eine Registrierung und Speicherung erfolgt daher nur selten freiwillig.

[122] NAT steht für Network-Address-Translation.

b. Gesetzgeberischer Handlungsbedarf

Der Wunsch nach einem allzeit ohne Registrierungshürden zugänglichen Internet ist sicherlich verständlich. Ungeachtet dessen sollten die Interessen der Nutzer mit den Interessen der durch missbräuchliche Nutzungen Geschädigten in einen fairen und gerechten Ausgleich gebracht werden.

Die effektivste Möglichkeit, einen Rechtsverletzer bei Nutzung eines Hotspots zu identifizieren, ist die Erhebung und Speicherung der Klardaten des Nutzers samt der diesem bei Einwahl über den Hotspot zugewiesenen IP-Adresse nebst Port. Alternativ könnte die Registrierung der Nutzer auch über eine Mobilfunk- oder Kreditkartennummer[123] erfolgen, so wie dies zum Teil schon heute im Ausland praktiziert wird. Darüber hinaus sollte in § 101 Abs. 2 Nr. 3 UrhG klargestellt werden, dass Hotspot-Betreiber ihre Dienstleistung stets in gewerblichem Ausmaß i.S.d. § 101 UrhG erbringen. Inhalte der Kommunikation müssen dagegen nicht gespeichert werden, um eine Identifizierung zu ermöglichen.

Auch außerhalb Deutschlands müssen sich Nutzer vielfach registrieren, um offene WLAN-Netze nutzen zu können. So können etwa in Großbritannien Hotspots einerseits über sog. „Pay-As-You-Go"-Modelle genutzt werden.[124] Hierbei zahlt der Nutzer ein Entgelt dafür, dass er sich für eine bestimmte Dauer über den WLAN-Zugang ins Internet einwählen kann. Andererseits stellen Betreiber von Hotels oder Cafés ihren Gästen einen kostenlosen WLAN-Zugang häufig durch spezialisierte Drittanbieter zur Verfügung. Diese übernehmen gegenüber dem Hotel- oder Café-Betreiber die Haftung für über den WLAN-Zugang begangene Rechtsverletzungen. Um ihrerseits den Verantwortlichen in Anspruch nehmen zu können, wird der Nutzer beim erstmaligen Zugriff auf das Netzwerk authentifiziert, indem ihm Zugangsdaten beispielsweise per SMS auf das Handy geschickt werden. Bereits registrierte Nutzer können sich dann mit ihrer E-Mail-Adresse und einem

123 Insofern müsste eine Klarstellung in § 101 UrhG erfolgen, dass auch die Kreditkartennummer vom Auskunftsanspruch umfasst ist und sich Zahlungsdienstleister insoweit nicht auf ihr Zeugnisverweigerungsrecht berufen können.

124 Zum Beispiel bei BT-Wifi (https://my.btwifi.com/selfcare/purchase/chooseProduct.htm)

Passwort anmelden. Der Nutzer ist also stets personalisiert und kann im Falle von Rechtsverletzungen identifiziert werden.[125]

Derartige Dienstleistungen werden inzwischen auch in Deutschland angeboten.[126] Auch in anderen EU-Staaten, etwa in Polen oder in Italien, werden Hotspots in öffentlichen Transportmitteln nur bei einer Registrierung der Nutzer angeboten.[127] In Italien muss dabei eine Mobilfunknummer eingegeben werden, an die die Zugangsdaten per SMS geschickt werden. Nutzer, die keine italienische Mobilfunknummer besitzen, erhalten den Zugangscode für einen symbolischen Cent, der über ihre Kreditkarte abgerechnet wird.[128]

Anders als teilweise behauptet, tragen somit auch in anderen Ländern Betreiber offener WLAN-Netze ein Haftungsrisiko. Auch im Ausland versuchen daher Betreiber solcher WLANs, ihr Haftungsrisiko durch Zugangsbeschränkungen zu reduzieren.[129]

---

125 Horvath/Dr. Albers, Haftungsrisiken von Betreibern öffentlicher WLAN-Anschlüsse in Deutschland und ausgewählten Ländern, Wissenschaftliche Dienste des Deutschen Bundestages, WD 10-3000-075-013, S. 14.

126 Vgl. http://www.thecloud.eu/de/hospitality/rechtssicherheit/.

127 Vgl. hierzu http://ztm.waw.pl/informacje.php?i=971&c=98&l=1und http://www.businesstraveller.de/News-Magazin/Top-News/Gratis-Wi-Fi-in-Frecciarossa-Zuegen.

128 Vgl. hierzu http://www.businesstraveller.de/News-Magazin/Top-News/Gratis-Wi-Fi-in-Frecciarossa-Zuegen.

129 Horvath/Dr. Albers, Haftungsrisiken von Betreibern öffentlicher WLAN-Anschlüsse in Deutschland und ausgewählten Ländern, Deutscher Bundestag – Wissenschaftliche Dienste, WD 10-3000-075-013, S. 14.

2. Die Inanspruchnahme auf Unterlassung

a. Der Anspruch aus § 97 UrhG und seine Grenzen

aa. Die Haftung als Täter oder Teilnehmer

Eine täterschaftliche Haftung des Hotspot-Betreibers scheidet in aller Regel aus, sofern die urheberrechtlich geschützte Datei nicht vom Hotspot-Betreiber selbst oder gemeinschaftlich mit einem Dritten öffentlich zugänglich gemacht wird. Der Hotspot-Betreiber ist auch nicht Teilnehmer einer durch einen unbekannten Dritten begangenen Urheberrechtsverletzung, da ihm hierfür regelmäßig der erforderliche doppelte Gehilfenvorsatz fehlen wird.[130]

bb. Die Haftung als Störer

Von klassischen Access-Providern betriebene Hotspots fallen unter das Haftungsprivileg des § 8 TMG, dessen Wertungen bei Unterlassungsansprüchen jedenfalls im Rahmen der Zumutbarkeitserwägungen zu berücksichtigen sind.[131] Für die bloße Zugangsvermittlung scheidet eine Störerhaftung des Access-Providern daher grundsätzlich aus. Denkbar ist nur die Pflicht zur Sperrung des Zugangs zu bestimmten Inhalten.[132]

Der private Inhaber eines ungesicherten WLAN-Anschlusses haftet nach der Rechtsprechung des Bundesgerichtshofs hingegen als Störer auf Unterlassung, wenn Dritte über seinen Anschluss Urheberrechtsverletzungen begehen.[133] Denn Privatpersonen kann insoweit zugemutet werden, ihren Router vor der Inbetriebnahme eines WLAN-Anschlusses darauf zu überprüfen, ob dieser durch marktübliche Sicherungen vor einem Missbrauch außenstehender Dritter geschützt ist. Die Zumutbarkeit ergibt sich dabei aus dem Eigeninteresse des Anschlussinhabers, seine Daten vor

130 BGH, 12.05.2010, Az. I ZR 121/08 – Sommer unseres Lebens.
131 Hanseatisches OLG, 21.11.2013, Az. 5 U 68/10 (Sperrung von 3dl.am).
132 Vgl. A.IV.1.a.
133 BGH, 12.05.2010, Az. I ZR 121/08 – Sommer unseres Lebens.

unberechtigtem Zugriff von außen zu schützen. Unterbleiben die gebotenen Sicherungsmaßnahmen, ist diese Prüfpflicht mit der Folge der Störerhaftung verletzt.

Dabei besteht die Prüfpflicht bereits ab Inbetriebnahme des Anschlusses und nicht erst ab Kenntnis von einer über den Anschluss begangenen Urheberrechtsverletzung, da die Auferlegung präventiver Prüfpflichten hier nicht zu einer Gefährdung eines Geschäftsmodells führt. Das Interesse, über WLAN leicht und räumlich flexibel Zugang zum Internet zu erhalten, ist zwar hoch zu bewerten. Dieses Interesse wird durch die Anwendung marktüblicher Sicherungsmaßnahmen gegen unbefugte Nutzung jedoch nicht in Frage gestellt.[134]

Die Entscheidung des Bundesgerichtshofs erging zu einem Fall, bei dem ein privater Anschlussinhaber seinen WLAN-Anschluss nicht hinreichend gesichert hatte. Ungeklärt und umstritten ist hingegen, ob im Falle der bewussten Öffnung eines privaten bzw. gewerblichen WLAN-Anschlusses für die Öffentlichkeit der Anschlussinhaber als Zugangsvermittler bzw. Telekommunikationsanbieter nach § 8 TMG haftungsprivilegiert ist.

Mit der Klärung dieser Rechtsfrage hat das Landgericht München I den Gerichtshof der Europäischen Union im Rahmen eines Vorabentscheidungsverfahrens befasst.[135] In dem konkreten Fall hatte ein Anschlussinhaber (ein Mitglied der Piratenpartei Deutschland) den für sein Gewerbe (Licht- und Tontechnik) genutzten Internetanschluss bewusst nicht mit einem Passwortschutz versehen, um der Öffentlichkeit einen unmittelbaren öffentlichen Zugang zum Internet zu ermöglichen. Als über diesen Internetanschluss eine Urheberrechtsverletzung festgestellt wurde, berief sich der Anschlussinhaber auf § 8 TMG.

Das Landgericht München I legte dem Gerichtshof der Europäischen Union neun Fragen zur Vorabentscheidung vor. Dabei möchte das Landgericht u.a. wissen, inwieweit die Haftungsprivilegierung nach Art. 12 Abs. 1 der E-Commerce-Richtlinie (bzw. nach § 8 TMG) auf Anbieter offener WLANs Anwendung findet.

134 BGH, 12.05.2010, Az. I ZR 121/08 – Sommer unseres Lebens.

135 LG München I, 18.09.2014, Az. 7 O 14719/12.

b. Gesetzgeberischer Handlungsbedarf

Würde der Inhaber eines privaten bzw. gewerblichen WLAN-Anschlusses allein durch die bewusste Öffnung für jedermann zum Zugangsvermittler i.S.d. § 8 TMG werden, hätte dies ein paradoxes Ergebnis zur Folge: Der Inhaber eines absichtlich ungesicherten Internetanschlusses hätte bei Urheberrechtsverletzungen Dritter keinerlei Haftung zu befürchten, während der Inhaber eines versehentlich ungesicherten Internetanschlusses nach der Rechtsprechung des Bundesgerichtshofs als Störer auf Unterlassung haften würde.

Sofern man den Betreiber eines offenen WLANs allerdings gleichwohl als Zugangsvermittler im Sinne des § 8 TMG verstehen wollte, müssten für ihn zumindest dieselben Registrierungspflichten (§ 111 TKG) und Auskunftspflichten (§ 101 UrhG) gelten, die von kommerziellen Access-Providern zu beachten sind, die ihre Dienstleistung geschäftsmäßig bzw. im gewerblichen Ausmaß anbieten. Darüber hinaus müsste auch der private WLAN-Anbieter generell dazu verpflichtet werden, die Verbindungsdaten für einen gewissen Zeitraum zu speichern, um eine Identifizierung von Uploadern nach § 101 UrhG zu gewährleisten.

Ein Haftungsprivileg hat nur dort seine Berechtigung, wo der Privilegierte auch seiner gesellschaftlichen Verantwortung und damit einhergehender Pflichten gerecht wird. Die Ermöglichung einer Auskunftserteilung ist dabei ebenso geboten, wie die weiteren Pflichten, die einem Access-Provider obliegen, z.B. der Einsatz technischer Schutzmaßnahmen (§ 109 TKG) oder Maßnahmen zur Gewährleistung der Datensicherheit (§ 109a TKG).

Ob und in welcher Richtung der Gesetzgeber hier regelnd tätig wird, ist noch vollkommen offen. In der Digitalen Agenda 2014-2017 wurde zwar bereits ein Gesetzesentwurf angekündigt, mit dem eine Haftungsprivilegierung für Anbieter offener WLANs im öffentlichen Bereich geschaffen werden sollte.[136] Es ist jedoch davon auszugehen, dass der Gesetzgeber die Ergebnisse des vom Landgericht München I

[136] Digitale Agenda 2014-2017, S. 15 (abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/ digitale-agenda-2014-2017,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf).

eingeleiteten Vorabentscheidungsverfahrens abwarten wird, um diese in einem Gesetz berücksichtigen zu können.[137]

C. Ausblick: Politische Entwicklungen auf europäischer Ebene

Aufgrund der Herausforderungen, die sich im Zusammenhang mit einem digitalen Binnenmarkt stellen, erfolgt auf europäischer Ebene derzeit eine Überprüfung des gemeinschaftlichen Rechtsrahmens zum Urheberrecht. Teil dieser Überprüfung war auch eine von Dezember 2013 bis März 2014 durchgeführte öffentliche Konsultation.[138] Mit über 9.500 Antworten sowie weiteren 11.000 Anmerkungen und Fragen[139] wurde dabei eine der höchsten Beteiligungsraten an einer Konsultation zur europäischen Gesetzgebung überhaupt erzielt.[140]

Auf Grundlage dieser Konsultation arbeitet die Kommission derzeit an einer Folgenabschätzung, welche u.a. das grenzüberschreitende Zurverfügungstellen von Inhalten, die bestehenden urheberrechtlichen Schranken und die Rechtsdurchsetzung in Bezug auf digitale Technologien adressieren wird. Die anhand der Folgenabschätzung festgelegten, allgemeinen und konkreten Ziele sowie eine Auswahl an

---

137 Bislang eingebracht wurde ein Gesetzesentwurf der Fraktionen BÜNDNIS 90/DIE GRÜNEN und DIE LINKE, mit dem eine Haftungsfreistellung sämtlicher WLAN-Betreiber angestrebt wird, vgl. BT-Dr. 18/3047. Ausweislich des Plenarprotokolls 18/67 vom 14.11.2014 solle sich der Gesetzesentwurf der Regierungskoalition in Vorbereitung befinden. Im Gegensatz zum Oppositionsentwurf solle sich dieser jedoch umfassend mit allen Interessen auseinandersetzen. Auch die SPD beabsichtigt, einen eigenen Gesetzesentwurf vorlegen.

138 Konsultation zur Überprüfung der Regeln zum EU-Urheberrecht (abrufbar unter http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/index_de.htm).

139 Vgl. report on the responses to the Public Consultation on the Review of the EU Copyright Rules (abrufbar unter http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf).

140 Pressemitteilung der Vertretung der Europäischen Kommission in Deutschland vom 24.07.2014 (abrufbar unter http://ec.europa.eu/deutschland/press/pr_releases/12585_de.htm).

Optionen zu deren Verwirklichung sollen von der Kommission in einem Weißbuch zur Urheberrechtspolitik zusammengefasst werden.[141]

Die gegenwärtige Entwurfsfassung des Weißbuches hebt hervor, dass Rechte des geistigen Eigentums, die nicht effektiv durchgesetzt werden können, keinen wirtschaftlichen Wert besitzen. Dabei müsse eine effektive Rechtsdurchsetzung den Herausforderungen der grenzüberschreitenden Natur des Internets, den verbleibenden Unterschieden in der Rechtsdurchsetzung in den Mitgliedstaaten sowie der Geschwindigkeit, mit der in gewerblichem Ausmaß agierende Rechtsverletzer die Quellen ihres Angebots wechseln, begegnen können.[142]

Als Lösungsansatz werden besondere für alle Akteure geltende Sorgfaltspflichten bei Angeboten mit digitalen Inhalten genannt. Zudem wird eine Fokussierung auf einen „follow the money"-Ansatz gefordert. Danach soll gewerbsmäßigen Schutzrechtsverletzern die Einnahmequelle entzogen werden, indem bei Zahlungsdienstleistern und Werbung angesetzt wird. [143]

Eine erste konkrete aus vorgenannten Bestrebungen resultierende Maßnahme stellt der im Sommer 2014 von der Kommission vorgestellte Aktionsplan für einen neuen Konsens über die Durchsetzung von Immaterialgüterrechten dar.[144] Der Aktionsplan befasst sich insbesondere mit der Frage, auf welche Weise der Schutz geistigen Eigentums konkret gewährleistet werden kann. In diesem Zusammenhang

---

141 Draft Impact Assessment on the modernisation of EU copyright rules (abrufbar unter http://statewatch.org/news/2014/may/eu-draft-impact-assessment-copyright-acquis.pdf).

142 Draft White Paper – A Copyright Policy for Creativity and Innovation in the European Union (abrufbar unter http://www.ip-watch.org/weblog/wp-content/uploads/2014/07/White-Paper-internal-draft-1.pdf).

143 Draft White Paper – A Copyright Policy for Creativity and Innovation in the European Union (abrufbar unter http://www.ip-watch.org/weblog/wp-content/uploads/2014/07/White-Paper-internal-draft-1.pdf).

144 Mitteilung der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss vom 01.07.2014 - EU-Aktionsplan für einen neuen Konsens über die Durchsetzung von Immaterialgüterrechten, COM(2014) 392 final (abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52014DC0392&from=DE).

werden zehn Maßnahmen vorgestellt, die in erster Linie gewerbsmäßigen Schutzrechtsverletzungen entgegenwirken sollen. Darin integriert ist auch bereits der in der Entwurfsfassung des Weißbuches enthaltene „follow the money"-Ansatz. Im Hinblick darauf, dass Schutzrechtsverletzungen ihrem Wesen nach grenzübergreifend erfolgen, soll zudem die Zusammenarbeit zwischen den nationalen (Strafverfolgungs-) Behörden in Europa gestärkt werden. Bei Verhandlungen über Freihandelsabkommen sollen darüber hinaus Drittstaaten dazu bewegt werden, die Gewährleistung eines hohen Schutzes für die Rechte des geistigen Eigentums zuzusichern.

Darüber hinaus kündigte der EU-Kommissar für digitale Wirtschaft und Gesellschaft, Günther Oettinger, kürzlich an, bis 2016 einen Gesetzesentwurf für ein an das digitale Zeitalter angepasstes, europäisches Urheberrecht vorzulegen. Daneben beabsichtigt er eine Abgabe auf das geistige Eigentum einzuführen, die nicht nur von den europäischen Nutzern sondern auch von amerikanischen Unternehmen wie Google zu entrichten wäre.[145]

[145] Abrufbar etwa unter http://www.handelsblatt.com/politik/international/schutz-geistigen-eigentums-bis-2016-eu-plant-urheberrechtsabgabe-im-internet/10900130.html und http://www.zeit.de/digital/2014-10/oettinger-eu-urheberrecht.