Jürgen Taeger / Andreas Wiebe (Hrsg.)

Aktuelle Rechtsfragen von IT und Internet

Tagungsband
zur Herbstakademie 2006

Sonderdruck:

Filesharing: Ermittlung, Verfolgung und Verantwortung der Beteiligten

Wiss. Ang. Rechtsanwalt Ralf Dietrich

O|WIR Oldenburger Verlag für Wirtschaft, Informatik und Recht

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie; detaillierte bibliografische
Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Umschlaggestaltung: Andreas Altvater, Oldenburg

Layout: Annika Bromund

Tagungsorganisation: Britta Lehmann

Oldenburger Verlag für Wirtschaft, Informatik und Recht

1. Aufl.

Edewecht 2006

3-939704-03-2

978-3-939704-03-4

Filesharing: Ermittlung, Verfolgung und Verantwortung der Beteiligten

Wiss. Ang. Rechtsanwalt Ralf Dietrich

Eberhard Karls Universität Tübingen
Lehrstuhl Prof. Dr. Hans-Ludwig Günther

dietrich@jura.uni-tuebingen.de
www.digitalrecht.de

Zusammenfassung

Mittels Filesharing werden massenhaft Daten über das Internet ausgetauscht. Ein Großteil dieser Daten sind dabei urheberrechtlich geschützte Werke wie Musiktitel und Kinofilme, die ohne Genehmigung getauscht werden. Das Anbieten von Werken ist urheberrechtswidrig und strafbar, das Herunterladen (noch) erlaubt. Die – meist alleine nachweisbare – Zurverfügungstellung eines Internetanschlusses reicht für eine Haftung grundsätzlich nicht aus. Rechtsinhaber und staatliche Verfolgungsbehörden sehen sich technischen und rechtlichen Hindernissen ausgesetzt, der Rechtsverletzer habhaft zu werden und sie zur Verantwortung zu ziehen. Technisch kann nur mit Hilfe des Zugangsproviders der benutzte Anschluss ermittelt werden. Der Zugangsprovider ist aber (noch) nur der Staatsanwaltschaft gegenüber zur Auskunft verpflichtet. Urheberrechtsverletzte zeigen daher beobachtete Vorgänge bei der Staatsanwaltschaft an, warten deren Ermittlung ab und fordern sodann Akteneinsicht, um gezielt gegen ihre Schädiger vorzugehen. Die bestehende straf- und zivilrechtliche prozessuale und materielle Regelung wird dem Massendelikt des illegalen Filesharing nicht gerecht. Rechtswidrige Handlungen, die isoliert betrachtet Bagatellen darstellen, gewinnen durch ihre Anzahl eine eigene Qualität. Eine ausgewogene praktikable Lösung muss – auch unter Berücksichtigung der Reformbemühungen – erst noch gefunden werden. Es gilt den Werkinhabern zu ihrem Recht zu verhelfen, ohne dabei das Maß auf Ermittlungs- wie Rechtsfolgenebene aus den Augen zu verlieren.

1. Einleitung

Illegales wie legales Filesharing konnte sich lange Zeit relativ „ungefährdet“ entwickeln. Mittlerweile sollen über 50 % des gesamten Internetdatenverkehrs von diesem netzbasierten Datenaustausch verursacht sein. In jüngerer Zeit werden die anbietenden Teilnehmer jedoch zunehmend von Urheberrechtsinhabern sowie Staatsanwaltschaften verfolgt.

Durch spektakuläre Einzel- sowie Massenverfahren sollen die Filesharer in die Pflicht genommen und abgeschreckt werden. Der Beitrag beleuchtet die Ermittlungsmöglichkeiten und -grenzen in technischer und rechtlicher Hinsicht. Die rechtliche Verantwortung der ermittelten Beteiligten wird

zivilrechtlich sowie strafrechtlich nach Beteiligungsgrad differenziert. Reformbedarf und –bemühungen werden aufgezeigt.

2. Ermittlung und Verfolgung

„Klassisches“ Filesharing bedient sich des Peer-to-Peer Prinzips (P2P), um Daten auszutauschen. Die jeweiligen zu tauschenden Daten liegen bei den beteiligten Nutzern; sie werden grundsätzlich weder zentral verwaltet noch gespeichert. Die beteiligten Rechner werden vielmehr direkt miteinander verbunden. Mittels frei verfügbarer und leicht handhabbarer P2P-Programme können auch technisch weniger versierte Nutzer leicht am globalen Austausch von Daten teilnehmen.

Grob vereinfacht dargestellt erfassen die P2P-Programme dazu die vom Nutzer bereitgestellten Daten und stellen die Liste dieser zur Abfrage bereit. „Im Gegenzug“ kann der Nutzer nach bereitgestellten Daten anderer Teilnehmer suchen und diese zum Herunterladen abrufen. Dazu durchsuchen die beteiligten Rechner sich gegenseitig (bzw. durch Server vermittelt ihre Listen) auf gewünschte Dateien. Für beide Vorgänge – Angebot und Suche – geben sie ihre Kennung und Adresse, die so genannte IP, an. Die IP (Kurzform für *I*nternet *P*rotokoll Adresse) ist eine eindeutige Zahlenfolge, einer Telefonnummer in herkömmlichen Telefonnetzen vergleichbar, die die Individualisierung des Anschlusses erlaubt und so notwendige Information zur Adressierung der Datenströme ist.

Will man nun etwa die Anbieter bestimmter urheberrechtlich geschützter Inhalte finden, so kann man – etwa unter Zuhilfenahme leicht modifizierter P2P-Programme – nach diesen Inhalten wie ein Tauschpartner suchen. Ergebnis ist eine Liste ihrer Anbieter und deren IP, so dass der gesuchte Inhalt geladen werden kann. Diese Angaben: Angebot und IP-Kennung können nun gespeichert werden. Es ist dabei sicherzustellen, dass es sich tatsächlich um das gesuchte Angebot handelt und nicht um einen weit verbreiteten „*fake*“, d. h. eine Datei, deren Bezeichnung nicht mit dem Inhalt übereinstimmt. Dazu muss die Dateiidentität anhand ihrer Kennung (Hashwert) überprüft oder (teilweise) herunter geladen werden. Ein anderer Weg der Ermittlung ist, direkt auf Knotenpunkte, die zur Beschleunigung Suchanfragen zuordnen, während des Betriebs zuzugreifen, um so schneller Daten zu erhalten.

Mittels dieser Kenntnisse kann aber noch nicht auf den Anschlussinhaber oder gar den Nutzer geschlossen werden. Die Klärung der Identität des Verantwortlichen wird in vierfacher Hinsicht erschwert:

2.1. Dynamik der IP

Welchem Anschlussinhaber die ermittelte IP zuzurechnen ist, kann nur der Zugangsprovider angeben, der diese zugewiesen hat. Problematisch ist dabei, dass meist ein und dieselbe IP nacheinander verschiedenen Anschlüssen temporär zugewiesen wird (dynamische IP).

Um ermitteln zu können, von welchem Anschluss ein Angebot bestand, ist die Kenntnis von IP *und* Moment ihrer Zuordnung Voraussetzung. Für diesen Ermittlungsschritt ist es notwendig, zumindest eine Datei (teilweise) herunter zuladen und *diesen* Moment zu speichern. Die Feststellung eines Angebots reicht nicht, denn Angebote sind oft schon im Moment des Empfangs veraltet, da sie von anderen Rechnern (zeitverzögert) weitergereicht werden. Es kann dann schon sein, dass der anbietende Rechner vom Netz gegangen ist und dieselbe IP einem anderen zugeteilt wurde.

2.2. Löschpflicht

Provider sind grundsätzlich verpflicht, die Verbindungsdaten nach Ende der Verbindung zu löschen – zu den Verbindungsdaten gehört dabei auch die vergebene IP.[1] Nur bei Kenntnis rechtswidrigen Gebrauchs darf gem. § 100 Abs. 3 TKG gespeichert werden.[2] Ermittelnde sind also gehalten, im Zeitpunkt des beobachteten Vorgangs, den Provider durch entsprechende Hinweise in Kenntnis zu setzen und diesen, wenn nicht zur Auskunft, zumindest zur Speicherung aufzufordern. Massenhafte Aufforderungen können allerdings die Provider überlasten und sind ihrerseits rechtswidrig.[3] In der Praxis allerdings wird der Löschverpflichtung seitens des größten deutschen Zugangsdienstleisters T-Online nicht unverzüglich, sondern erst nach ca. 90 Tagen nachgekommen – gegen das Urteil LG Darmstadt GRUR-RR 2006, 173, hat T-Online Revision eingelegt. Andere Provider dagegen löschen innerhalb einiger Tage und kommen so ihrer Verpflichtung nach.

2.3. (Noch) kein zivilrechtlicher Auskunftsanspruch

Hat der Provider die Daten noch nicht gelöscht und kann damit Auskunft über den fraglichen Anschlussinhaber erteilen, so ist er dazu nach obergerichtlicher Rechtsprechung zivilrechtlich nicht verpflichtet.[4] Selbst bei der Auskunft gegenüber der Staatsanwaltschaft ist der Richtervorbehalt zu be-

---

1 *Dietrich*, NJW 2006, S. 810 m.w.N. zur uneinheitlichen Rechtsprechung.

2 Säcker-*Klesczewsk* , Telekommunikationsrecht, 2006, § 100 Rdnr. 14 ff.

3 LG Flensburg, Urteil vom 25.11.2005, MMR 2006, 181, m. Anm. *Kazemi* = GRUR-RR 2006, S. 174, m. Anm. *Dietrich* GRUR-RR 2006, S. 145.

4 OLG Frankfurt, Urteil vom 25.1.2005, GRUR-RR 2005, 147 = MMR 2005, 241; OLG Hamburg, Urteil vom 28.4.2005, GRUR-RR 2005, 209 = MMR 2005, 453, jew. m. Anm.

achten, da die Daten zu den Verbindungsdaten zählen (zur uneinheitlichen Rechtsprechung, s. o.). Die Verletzten zeigen daher die beobachteten Vorgänge den Staatsanwaltschaften an. Diese ermitteln die Anschlussinhaber und gewähren den Verletzten Akteneinsicht, welche nun über diesen „Umweg“ gegen die Anschlussinhaber zivilrechtlich vorgehen können.

Ein eigener urheberrechtlicher Auskunftsanspruch soll den Verletzten unter Umsetzung der EU-Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums durch das nationale Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (nicht zu verwechseln mit dem 2. Korb der Urheberrechtsnovelle) in § 101 UrhG eingeräumt werden. Das Gesetz dient nicht zuletzt der Entlastung der Staatsanwaltschaften. Es bleibt freilich eine hohe Belastung der Justiz, wenn wegen des Richtervorbehalts die Gerichte massenhaft in Anspruch genommen werden. Der Richtervorbehalt wird bei Auskünften gegenüber Privaten von noch größerer Bedeutung sein. Seine Umgehung oder Streichung bei der Auskunft von Telekommunikationsverbindungsdaten stellt also keineswegs den richtigen Weg dar. Ein weiteres Problem ist die oben angesprochene Löschpflicht der Accessprovider, die in diesem Zusammenhang etwa zugunsten einer (schon für die Terrorfahndung) höchst umstrittenen Vorratsdatenspeicherung weichen müsste. Alternativ könnte ein durchsetzbarer Speicheranspruch für jede Verletzung eingeführt werden, der aber zu erheblichem Aufwand bei den nur indirekt beteiligten Providern führen würde. Änderungen sind im ElGVG (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz) geplant. § 14 dessen RefE behandelt dabei die Auskunft über die Bestandsdaten der Nutzer „zur Durchsetzung der Rechte am geistigen Eigentum“. Die geplante Auskunft über Nutzungsdaten (womit Verbindungsdaten gemeint sein dürften) zu diesem Zweck ist nicht mehr im Entwurf enthalten.[5] Insgesamt ist die Fassung eines zivilrechtlichen Auskunftsanspruches, seine praktische Umsetzung und Einpassung in das Spannungsgefüge von effektiver Rechtsverfolgung und Datenschutz hoch umstritten – die weitere Entwicklung bleibt abzuwarten.

2.4. Aussagekraft und Beweislage

Der Provider kann naturgemäß nur Auskunft geben, welcher Anschluss verwendet wurde und unter welchem Namen dieser bei ihm gemeldet ist. Kenntnis des Anschlusses bedeutet Kenntnis des Anschlussinhabers. Sie bedeutet jedoch nicht Kenntnis des Nutzers. Wie Telefonanschlüsse, so teilen sich auch oft – etwa in Familien oder (Studenten) Wohngemeinschaften – mehrere Personen einen Internetzugang. Auch andere Dritte, Nachbarn etwa, kommen als Nutzer in Betracht: WLAN-Funkverbindungen sind oft-

[5] Vergleiche zum Auskunftsanspruch insgesamt *Dietrich*, GRUR-RR 2006, S. 145, und *Splittgerber*, in diesem Band.

mals nicht oder nur unzureichend gesichert. Nachbarn können den Internetzugang unbemerkt mitbenutzen und für rechtswidrige Handlungen verantwortlich sein. Dementsprechend stellt die Staatsanwaltschaft – so jedenfalls nach Auskunft der in einem Massenverfahren federführenden Staatsanwaltschaft Köln – wenn der Anschlussinhaber einen persönlichen weiteren Beitrag abstreitet und auch nicht von sich aus auf den Anbieter der fraglichen Daten verweist, das Verfahren in aller Regel ein. Sie ermittelt nur weiter, wenn mehr als 500 Dateien angeboten wurden. Dann kommen Hausdurchsuchung und Computerbeschlagnahme in Betracht, um den oder die konkreten Täter zu ermitteln. Von diesen Maßnahmen wird jedoch wiederum dann unter Beachtung des Verhältnismäßigkeitsgrundsatzes abgesehen, soweit „zu viele Unbeteiligte“ mit betroffen wären, wie es etwa bei größeren Wohngemeinschaften oder Betrieben der Fall wäre.

3. Verantwortung der Beteiligten

Drei Formen der Beteiligung am Filesharinggeschehen kommen auf Nutzerseite in Betracht: Anbieten bzw. Hochladen, Herunterladen und bloßes Bereitstellen eines Anschlusses. Im Vordergrund stehen erstere Tatmodalitäten. Doch wie bereits dargelegt, kann aus den aus oben genannten Ermittlungsschritten gewonnenen Daten oft nur der Anschlussinhaber festgestellt werden, auf ihn ist daher gesondert einzugehen.

3.1. Zivilrechtliche Verantwortung

3.1.1. Anbieter und Hochladender

Schon das Anbieten – zum tatsächlichen Hochladen braucht es nicht zu kommen – urheberrechtlich geschützter Daten ohne Erlaubnis ist gem. §§ 15 Abs. 2, 52 Abs. 3 UrhG ein Rechtsverstoß. Es handelt sich um ein öffentliches Zugänglichmachen nach § 19a UrhG, wobei die P2P-„Gemeinschaft“ Öffentlichkeit ist, da nach der Neukonzeption des § 15 Abs. 3 UrhG nur dann keine Öffentlichkeit vorliegt, wenn die Teilnehmenden miteinander persönlich verbunden sind. In dem Moment, in dem andere Teilnehmer auf die Daten Zugriff nehmen können, sind sie öffentlich zugänglich gemacht.

Rechtsfolge sind Unterlassungs-, Beseitigungs-, Auskunfts-, Rechnungslegungs-, Besichtigungs- und verschuldensabhängige Schadensersatzansprüche gem. § 97 UrhG. Im Vordergrund steht naturgemäß der Schadensersatzanspruch, dessen Höhe grundsätzlich dreifach berechnet werden kann, wobei das Wahlrecht beim Geschädigten liegt:[6] Der entgangene Ge-

[6] *v. Wolff*, in: Wandtke/Bullinger (Hrsg.), Praxiskommentar zum Urheberrecht, München 2006, § 97 Rdnr. 56 f.

winn ist zu ersetzen, der vom Verletzer erlangte Gewinn herauszugeben oder die Höhe einer angemessenen Lizenz zu entrichten. Beim Filesharing bietet sich insbesondere der letztgenannte Weg an, denn wie viel Gewinn entgangen ist, lässt sich kaum beziffern. Filesharer werden auch regelmäßig keinen eigenen Gewinn erzielen, der herausgegeben werden könnte. Doch auch der Weg über die so genannte Lizenzanalogie führt selten zu genauen Ergebnissen, teils werden über diese Berechnungsart absurd hohe Summen geltend gemacht: Es wird von einem fiktiven Entgelt für die angemaßte Verwertung ausgegangen. Schon dies lässt sich aber nur dann genau bestimmen, wenn ein entsprechender Markt besteht. Ausgedehnt wird die Berechnungsart dennoch auch auf Fälle, in denen kein Markt für „Pirateriewaren" existiert.[7] Rechtsprechung und Literatur gingen herkömmlich dabei meist davon aus, dass die Verletzer eigene wirtschaftliche Interessen verfolgten. Dies ist beim Filesharing aber nicht der Fall. In der Regel wird zur weiteren Berechnung ein Betrag (5.000-15.000 Euro werden oft gefordert) pro angebotener Datei zu Grunde gelegt und dieser mit deren Anzahl multipliziert – dies ergibt bei oft mehreren hundert angebotenen Dateien Beträge im Millionen-Euro-Bereich. Da dies selbst den abmahnenden Kanzleien als offensichtlich übertrieben erscheint, gehen sie „aus Kulanz" pauschal von weitaus geringeren Beträgen aus. Eine solch schlichte Berechnung verkennt dabei die Eigenheiten des Filesharing: Ausreichend ist zwar grundsätzlich ein Angebot. Zu berücksichtigen ist jedoch, wenn nur Werkteile angeboten oder hochgeladen werden,[8] wie dies oft der Fall ist. Es können auch systembedingt nur einzelne Titel gleichzeitig an andere versandt werden, da die effektive Uploadbandbreite begrenzt ist. Eine Berechnung, die dies berücksichtigt, müsste also den Betrag berechnet aus maximaler effektiver Upstream-Geschwindigkeit des Tauschbörsenprogrammes multipliziert mit der nachgewiesenen Zeit in der Tauschbörse geteilt durch die durchschnittlich angebotene Dateigröße mal die veranschlagte Lizenzgebühr zumindest in die Überlegungen mit einbeziehen.

3.1.2. Herunterladender

Der Herunterladende handelt nach der jetzigen Fassung nicht urheberrechtswidrig: Das Herunterladen einer urheberrechtlich geschützten Datei ist zwar eine Vervielfältigung, § 16 Abs. 1 UrhG. Dies ist jedoch beim Filesharing kurioserweise und durch einen Redaktionsfehler veranlasst von § 53 Abs. 1 als private Vervielfältigung erlaubt: Privatkopien sind erlaubt, „soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte Vorlage verwendet wird." Das Gesetz stellt also nicht darauf ab, ob das Anbieten offensichtlich rechtswidrig ist, sondern wie die *Vorlage of-*

---

[7] Sehr anschaulich *Dreier*/Schulze, UrhG, 2006, § 97 Rdnr. 61 ff.

[8] Schricker/*Wild*, Urheberrecht, 2006, § 97 Rdnr. 63.

fensichtlich erlangt wurde. Selbst, wenn es der Lebenserfahrung entspricht, dass die allermeisten Vorlagen selbst rechtswidrig erlangt wurden, so reicht dies nicht. Das Gesetz erfordert Offensichtlichkeit. Der Nutzer auf der Gegenseite wird aber kaum Erkenntnisse haben, wie der andere an seine Version der Daten gelangt ist. Dieser mag seine Vorlage legal, etwa käuflich, erworben haben. Offensichtlichkeit ist also regelmäßig nicht gegeben.[9]

Diesem Missstand wird die Novelle des Urheberrechtsgesetzes (2. Korb) durch eine Änderung von § 53 Abs. 1 UrhG abhelfen. Rechtswidrig wird dann auch das Kopieren von einer Quelle sein, wenn diese eine „öffentlich zugänglich gemachte“ ist.

Dann wird sich auch die Frage nach der Rechtsfolge stellen. Für die Berechnung nach der Lizenzanalogie findet sich für den Download leichter ein vergleichbares Marktgeschehen: Einzelne Lieder, ganze Musikalben und Kinofilme können kostenpflichtig online bei legalen Anbietern herunter geladen werden.

3.1.3. Anschlussinhaber

Der Anschlussinhaber, der lediglich den Anschluss zur Verfügung stellt und von dessen Anschluss illegal Daten ohne sein Wissen oder weiteres Zutun angeboten werden, handelt nicht schuldhaft. Ein Schadensersatzanspruch scheidet danach aus.[10] Ein Anspruch könnte sich aber nach den Grundsätzen der Störer- und Veranlasserhaftung ergeben:

Eine Sonderregelung findet sich zunächst in § 100 UrhG. Da sich ein Arbeitgeber nicht hinter seinen Mitarbeitern „verstecken“ können soll und im betrieblichen Bereich gewisse Kontrollen erwartet werden, erweitert § 100 UrhG die Haftung akzessorisch auf ihn, allerdings nur, wenn die Verletzungshandlung „dienstlichen Charakter“ hat und nicht nur „bei Gelegenheit“ geschieht.[11]

Wer ansonsten – ohne eigenes Verschulden – willentlich adäquat kausal an der Herbeiführung oder Aufrechterhaltung einer Urheberrechtsverletzung mitgewirkt hat, ist Störer.[12] Kausal ist das Bereithalten eines Anschlusses, wenn dieser für die Verletzung genutzt wurde, unzweifelhaft. Die Störer*haftung* wird jedoch, um ihr Ausufern zu vermeiden, durch ein Korrektiv von Zumutbarkeitserwägungen eingegrenzt.[13] Maßgeblich ist

---

[9] *Lüft*, in: Wandtke/Bullinger (Hrsg.), Urheberrecht, 2006, § 53 Rdnr. 15 m.w.N.

[10] Vgl. Fromm/*Nordemann*, Urheberrecht, 1998, § 97 Rdnr. 31.

[11] *Bohne*, in: Wandtke/Bullinger, Urheberrecht, 2006, § 100 Rdnr. 3 f.

[12] *Wild*, in: Schricker, Urheberrecht, 2006, § 97 Rdnr. 35, 36e, vgl. BGH GRUR 2001, 1038, 1039.

[13] *v. Wolff* , in: Wandtke/Bullinger, Urheberrecht, 2006, § 97 Rdnr. 15.

hier zunächst das Maß des Störbeitrages. Bloße Hilfspersonen sollen als nur mittelbare Störer geringeren Pflichten ausgesetzt sein.[14]

Es stellt sich die Frage, wie weit der Anschlussinhaber die anderen Teilnehmer auf die Einhaltung der gesetzlichen Normen hinweisen, sie (stichprobenartig oder dauerhaft) kontrollieren und Fehlgebrauch unterbinden muss. Ist dem Anschlussinhaber positiv bekannt, dass Dritte seinen Anschluss für Verletzungshandlungen nutzen, so hat er dies zu unterbinden, so ihm dies zumutbar möglich ist.[15] Letzteres dürfte etwa im privaten (und damit für die hier einschlägigen Konstellationen typischen) Bereich dadurch möglich und zumutbar sein, dass dem Dritten der Gebrauch untersagt wird und notfalls auch entsprechende Vorkehrungen getroffen werden – etwa der Entzug der zugeteilten lokalen IP, das „Ausstöpseln" aus dem Router et cetera.

Hat der Anschlussinhaber dieses Wissen aber noch nicht, so ist fraglich, ob ihn schon vorbeugende Pflichten treffen.[16] Eine Störerhaftung ist dann nur bei einer Verletzung von Prüfungspflichten gegeben. Der BGH urteilte insofern in der „Möbelklassiker-Entscheidung": Es dürften „in die – nicht von einem Verschulden abhängige – Störerhaftung nach § 97 Abs. 1 S. 1 UrhG nicht über Gebühr Personen, die nicht selbst die rechtswidrige Nutzungsbehandlung vorgenommen haben, einbezogen werden. Die Bejahung der Störerhaftung Dritter nach § 97 Abs. 1 S. 1 UrhG setzt deshalb wie die wettbewerbsrechtliche Störerhaftung Dritter die Verletzung von Prüfungspflichten voraus. Wer nur durch Einsatz organisatorischer oder technischer Mittel an der von einem anderen vorgenommenen urheberrechtlichen Nutzungshandlung beteiligt war, muss demgemäß, wenn er als Störer in Anspruch genommen wird, ausnahmsweise einwenden können, dass er im konkreten Fall nicht gegen eine Pflicht zur Prüfung auf mögliche Rechtsverletzungen verstoßen hat. So muss er insbesondere geltend machen können, dass ihm eine solche Prüfung nach den Umständen überhaupt nicht oder nur eingeschränkt zumutbar war".[17]

Die Aufstellung einer Prüfungspflicht ist Frage des Einzelfalls, hat aber der Anschlussinhaber keinen konkreten Anlass, am Willen der anderen Nutzer der legalen Nutzung zu zweifeln, so ist eine Prüfpflicht im Privaten grundsätzlich zu verneinen. Es darf trotz vielfältigen Missbrauchs nicht darüber hinweggesehen werden, dass der größte Teil der Internetnutzung legal ist. Selbst die Nutzung von Datentauschsystemen ist nicht per se illegal. Eine über einen einmaligen Hinweis hinausgehende Pflicht, seine Familien-

[14] *Dreier*/Schulze, UrhG, 2006, § 97 Rdnr. 32 und 33.

[15] Ebenda, § 97 Rdnr. 33.

[16] Ebenda.

[17] BGH GRUR 1999, 418 = NJW 1999, 1960 = MMR 1999, 280.

mitglieder und Mitbewohner zu ermahnen und gar zu kontrollieren, ist überzogen. Ausgangspunkt sollte die gegenseitige Vermutung legaler Nutzung sein, wo nicht begründete tatsächliche Hinweise etwas anderes nahe legen. Die einschlägige Kommentarliteratur gibt mannigfaltige Hinweise, in welchen Bereichen eine Störerhaftung angenommen werden kann.[18] Für den Bereich unentgeltlichen privaten Zurverfügungstellens von Ressourcen, die in aller Regel legal genutzt werden, findet sich keine begründete Stütze für die Annahme von originären Kontrollpflichten.

Eine Störerhaftung ist daher erst dann anzunehmen, wenn der Anschlussinhaber – etwa vom Verletzten – einen Hinweis erhalten hat, dass unter seinem Anschluss illegale Nutzung geschieht. Er hat diese Nutzung – so ihm dies technisch möglich und zumutbar ist – zu verhindern. „Pro-aktive" Kontrollpflichten – ohne einen konkreten Anhaltspunkt für illegale Nutzung – hat er jedoch nicht.

Ist die Störerhaftung festgestellt, so löst dies keine Schadensersatzverpflichtung aus, sondern lediglich Unterlassungs- und Beseitigungsansprüche. Kommt es der Seite der Verletzten, insbesondere auch ihrer anwaltlichen Vertreter, auf finanzielle Leistungen an, wird daher oft der Weg eingeschlagen, eine strafbewehrte Unterlassungserklärung zu fordern und kostenpflichtig abzumahnen. Die Abmahnung (mit entsprechender Kostennote) wird maßgeblich, zumindest neben der behaupteten Verschuldenshaftung und unter Angabe eines entsprechenden Streitwertes, auch auf die behauptete Störerhaftung gestützt.

Nimmt sich der zu Unrecht Abgemahnte seinerseits einen Anwalt, so sind die Erfolgsaussichten, dessen Kosten ersetzt zu bekommen, als gering einzuschätzen.

3.2. Strafrechtliche Verantwortung

Die strafrechtliche Verantwortung läuft grundsätzlich parallel zur zivilrechtlichen und findet ihre Kodifikation in § 106 UrhG. Strafrechtliche Besonderheiten sind jedoch zu beachten, insbesondere die hier angesprochene Passivlegitimation wird erheblich enger gefasst und richtet sich nach dem strafrechtlichen Täterschafts- und Teilnahmemodell.

3.2.1. Anbieter und Hochladender

Ist das Anbieten urheberrechtswidrig, so ist dies erste Voraussetzung für die entsprechende Strafbarkeit. Nach der h. M. soll neben dem Upload schon das Anbieten gegenüber der Öffentlichkeit als Parallele zur zivilrechtlichen Wertung strafbar sein.[19] Zum Teil wird aber unter Hinweis auf

[18] *Dreier*/Schulze, UrhG, 2006, § 97 Rdnr. 33 f. mit zahlreichen Nachweisen.

[19] *Dreier*/Schulze, UrhG, 2006, § 106 Rdnr. 6 m.w.N.

das Analogieverbot die Strafbarkeit des reinen Anbietens verneint; erst das erfolgte Hochladen sei strafbar.[20] Weiter wird der Begriff der Öffentlichkeit teils als Vermutung verstanden, die dem Strafrecht fremd sei.[21]

In der Praxis wird schon das Anbieten verfolgt, allerdings stellen nach einer Empfehlung der Generalstaatsanwaltschaft Karlsruhe die Staatsanwaltschaften bei angenommenen Verstößen in bis zu 100 Fällen (Zahl der angebotenen Dateien) das Verfahren ein. Sind es mehr Fälle, jedoch unter 500, so sei nach der Empfehlung eine Beschuldigtenvernehmung angemessen. Bei mehr als 500 vorgeworfenen Verletzungen solle weiter ermittelt werden, insbesondere komme auch eine Hausdurchsuchung in Betracht. Als Strafen drohen meist Geldbußen, deren Höhe stark vom konkreten Vorwurf abhängt. Von Bundesland zu Bundesland sind große Unterschiede ersichtlich.

3.2.2. Herunterladender

Da das Herunterladen (noch) zivilrechtlich erlaubt ist, ist es auch (noch) nicht strafbar.[22]

In der Praxis wird der Herunterladevorgang daher in aller Regel nicht verfolgt.

3.2.3. Anschlussinhaber

Eine Störerhaftung kennt das Strafrecht nicht. Täterschaft und Teilnahme richten sich nach allgemeinen strafrechtlichen Grundsätzen.[23] Der Anschlussinhaber, dessen Verursachungsbeitrag sich in der zur Verfügungstellung des Anschlusses erschöpft und der von dem konkreten Verstoß nichts weiß, ist schon gar nicht Täter und auch eine akzessorische Beihilfe nach § 27 StGB scheidet aus, da der erforderliche Vorsatz bezüglich der konkreten Haupttat fehlt.

In der Praxis wird der Anschlussinhaber, so sich eine weitere Beteiligung nicht ermitteln lässt, als solcher daher nicht weiter verfolgt.

---

[20] *Hildebrandt*, in: Wandtke/Bullinger, Urheberrecht, 2006, § 106 Rdnr. 16, 18.

[21] *Hildebrandt*, in: Wandtke/Bullinger, Urheberrecht, 2006, § 106 Rdnr. 27.; Dreier/*Schulze*, UrhG, 2006, § 106 Rdnr. 6, § 15 Rdnr. 37, sieht den Begriff der „Öffentlichkeit" dagegen zu Recht als Definition.

[22] *Dreier*/Schulze, UrhG, 2006, § 106 Rdnr. 6; *Frank*, K&R 2004, S. 578; *Heghmanns*, MMR 2004, S. 15 f.; a. A. Schricker/*Vassilaki*, Urheberrecht, 2006, § 106 Rdnr. 9, nach der schon Zweifel an der Rechtmäßigkeit für die Offensichtlichkeit der Unrechtmäßigkeit ausreichen, m.w.N.

[23] Möhring/Nicolini-*Spautz,* UrhG, 2000, § 106 Rdnr. 3; Tröndle/*Fischer*, StGB, 2006, vor § 25 Rdnr. 1 ff. m.w.N.

Literatur

Dreier, Thomas/Schulze, Gernot (Hrsg.): Urheberrechtsgesetz, München 2006

Dietrich, Ralf: Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien, NJW 2006, S. 809-811

Dietrich, Ralf: Zur Auskunftspflicht des Access-Providers nach Urheberrechtsverletzungen im Internet, GRUR-RR 2006, S. 145-148

Frank, Thomas: MP3, P2P und StA – Die strafrechtliche Seite des Filesharing, MMR 2004, S. 576-585

Fromm, Friedrich Karl/Nordemann, Wilhelm (Hrsg.): Urheberrecht, Stuttgart 1998

Heghmanns, Michael: Musiktauschbörsen im Internet aus strafrechtlicher Sicht, MMR 2004, S. 14-18

Möhring, Philipp/Nicolini, Käte: Urheberrechtsgesetz (Hrsg. v. Käte Nicolini und Hartwig Ahlberg), München 2000

Säcker, Franz-Jürgen (Hrsg.): Berliner Kommentar zum Telekommunikationsrecht, Berlin 2006

Schricker, Gerhard (Hrsg.): Urheberrecht, München 2006

Tröndle, Herbert/Fischer, Thomas (Hrsg.): Strafgesetzbuch und Nebengesetze, München 2006

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, München 2006