

Von Rechtsanwalt
Christian Solmecke,
LL.M. (Leuven)

Der Verfasser ist
Rechtsanwalt in der Kölner
Medienrechtskanzlei
WILDE & BEUGER. Mehr
über ihn erfahren Sie
auf S. VIII.

Rechtliche Beurteilung der Nutzung von Musiktauschbörsen

Mit pauschalen Schadensersatzforderungen in Höhe von mehreren Tausend Euro sehen sich derzeit tausende Nutzer von Internettauschbörsen konfrontiert. Geltend macht diese Ansprüche die Musikindustrie in Deutschland und hält auf diese Weise Gerichte und Anwälte auf Trab. Da die Urheberrechtsverletzungen meist von Kindern begangen worden sind, wenden sich die Tonträgerhersteller an deren Eltern und fordern diese im Wege der Störerhaftung zur Unterlassung auf. Das Gros der Fälle hatte das Landgericht Hamburg zu entscheiden, das sich auf die Seite der Rechteinhaber geschlagen hat. Mittlerweile haben sich auch andere Gerichte zu der Problematik geäußert und weichen von der Rechtsprechung der Hanseaten ab. Nachfolgend sollen die rechtlichen Problemfelder des Filesharing eingehend erörtert werden.

I. Ausgangslage

Nachdem die Staatsanwaltschaft Köln im Mai 2006 insgesamt 130 Wohnungen wegen des Verdachts auf Urheberrechtsverletzung durchsuchen ließ, war das Medieninteresse an der Aktion überwältigend. Kein Wunder, die International Federation of the Phonographic Industry (IFPI) hatte die Ermittlungen schließlich ins Rollen gebracht und flankierend mit entsprechenden Pressemitteilungen unterstützt. Insgesamt wurde gegen 3500 Menschen ermittelt, die über so genannte Filesharing-Börsen Musik getauscht haben sollen.¹ Mittlerweile ist das Medienecho abgeklungen und die juristische Aufarbeitung dieser bislang einmaligen Aktion beginnt.

II. Technische Aspekte

Der rechtlichen Analyse soll zunächst eine ausführliche Darstellung der technischen Aspekte von so genannten Peer-to-Peer (P2P, Peer = engl. für „Gleichgestellter“, „Ebenbürtiger“) Tauschbörsen vorausgehen. Es existiert eine Vielzahl unterschiedlicher Systeme, mit denen Musik über das Internet getauscht werden kann.

1. Serverbasierte Filesharing-Systeme

a) Napster

Als Mutter aller Filesharing-Systeme kann wohl die Ende 1998 von dem US-Amerikaner Shawn Fanning program-

mierte Musiktauschbörse Napster bezeichnet werden. Revolutionär war seinerzeit die Verwendung der Peer-to-Peer-Technologie.² Nach der Installation auf dem Heim-PC (Client) durchsuchte die Napster-Software den Rechner, auf dem sie installiert war, nach Musikstücken und meldete das Suchergebnis an einen zentralen Napster-Server im Internet. Auf diesem Server meldeten auch die anderen Teilnehmer die bei ihnen vorhandenen Songs. Die einzelnen mit dem Server verbundenen Computer werden Clients genannt. Wenn nun ein bestimmtes Musikstück gesucht wird, startet der Client eine Anfrage beim Server. Dieser teilt dem anfragenden Client mit, auf welchen anderen Computern das gesuchte Stück vorhanden ist. Über den anfragenden Client konnte dann direkt eine Verbindung zu dem anbietenden Client hergestellt werden. Über diese Direktverbindung erfolgte der Austausch der Daten. Das zentrale Server-Client-System war zwar eine äußerst effektive, aber genauso angreifbare Lösung. Mit Erfolg klagte die Musikindustrie gegen Napster und erreichte im Jahr 2001 die Stilllegung des Napster-Servers. Seit einiger Zeit wird Napster in anderer Gestalt wieder als kostenpflichtiger Dienst betrieben.

b) edonkey2000

Nach Napster konzentrierte sich die Internetgemeinde insbesondere auf das Tauschnetzwerk edonkey2000. Vom

¹ Vgl. den ausführlichen Bericht zu der Aktion auf <http://www.heise.de/newsticker/meldung/73446> (Stand: 18. 1. 2007).

² Gamp, GRUR Int 2003, 991 ff.

Prinzip her funktionierte dieses Netzwerk ähnlich wie Napster. Entscheidender Unterschied ist jedoch, dass der zentrale Server zur Verwaltung der Suchanfragen abgeschafft worden ist. Vielmehr existierten nun mehrere hundert – meist auf kleineren privaten PCs betriebene – Server, die die unterschiedlichen Anfragen der Clients verwalten. Da die verschiedenen Server nun überall auf der Welt verteilt standen, konnte das Schließen eines Servers schnell durch die anderen Server aufgefangen werden. Aufsehen erregte Ende Februar 2006 die belgische Polizei, als sie den zu diesem Zeitpunkt größten edonkey2000-Server „Razoback 2.0“ vom Netz trennte. Die Arbeit dieses Rechners wurde allerdings schnell von anderen Servern übernommen. Im Rahmen der oben geschilderten aktuellen Ermittlungsverfahren hatte die Musikindustrie gemeinsam mit der Staatsanwaltschaft Köln mehrere Monate Zugriff auf einen edonkey2000-Server im Erft-Kreis. Wie genau dieser Zugriff ausgestaltet war, ist bislang öffentlich noch nicht bekannt geworden. Es ist aber davon auszugehen, dass für die Staatsanwaltschaft bzw. die Phonindustrie jederzeit die Möglichkeit bestand, den Server abzuschalten und ein weiteres Tauschen zu unterbinden. Stattdessen wurde zunächst offenbar nichts unternommen und das Tauschverhalten der einzelnen Nutzer wurde beobachtet beziehungsweise durch den Betrieb des Servers erst ermöglicht.

Der Tausch im edonkey2000 Netzwerk kann sowohl über die gleichnamige Software als auch über Abwandlungen davon namens eMule, Sharezaa oder MLDonkey betrieben werden.³ Mit dieser Software wurde eine weitere Neuerung eingeführt. Während früher ein anfragender Client von einem anbietenden Client geladen hat, ist nunmehr die Möglichkeit des multiplen Ladens gegeben. Fragt ein Client nach einem bestimmten Musikstück an, werden ihm meist mehrere Anbieter dieses Songs angezeigt. Um nun die Downloadgeschwindigkeit verbessern zu können und um nicht von einem einzigen Anbieter „abhängig“ zu sein, können Teilstücke eines Songs parallel von verschiedenen Anbietern heruntergeladen werden. Ein Lied wird beispielsweise in fünf Teilstücke (Chunks) zerlegt und gleichzeitig von fünf anbietenden Clients heruntergeladen. Auf dem Rechner des anfragenden Clients werden dann alle Teilstücke wieder zusammengesetzt. An dieser Stelle sei schon einmal darauf hingewiesen, dass es sich bei diesen Teilstücken quasi um „Datenmüll“ handelt. Fehlt auch nur ein Teilstück, kann das Gesamtwerk nicht mehr zusammengesetzt werden und ist unbrauchbar. Die urheberrechtlich relevante Werkqualität eines solchen Teilstücks erscheint bereits fraglich.⁴

Auch an einer anderen Stelle⁵ werden diese Chunks juristisch noch von Bedeutung sein. Sobald ein Teilstück komplett auf dem anfragenden Rechner angekommen ist, steht es bereits weiteren Tauschbörsennutzern zum Download bereit. Ein Tausch könnte dann etwa wie folgt aussehen; Nutzer A lädt von Nutzer B das erste Teilstück des Songs XY. Sobald dieses Teilstück auf der Festplatte von Nutzer A angekommen ist, wird dieser automatisch selbst zum Anbieter und stellt dieses Teilstück Nutzer C zur Verfügung. Dies funktioniert sogar dann, wenn auf der Festplatte des Nutzers A noch nicht alle Teilstücke angekommen sind. Es existiert allerdings edonkey2000 Software, bei der diese Upload-Funktion abgestellt werden kann.

Alle heruntergeladenen (Teil-)Stücke landen in dem so genannten Shared-Folder (auch Inbox genannt) des anfragenden Nutzers. Nur Musikstücke, die sich in diesem Ordner befinden, werden auch wieder zum Upload bereitgestellt. Lädt sich ein Nutzer z. B. 100 Musikstücke über das Netzwerk herunter und verschiebt er diese Songs aus der Inbox in einen anderen Ordner seines Computers, bietet er ab diesem Zeitpunkt auch keine Lieder mehr zum Upload an. Immer dann, wenn sich ein Nutzer am Server anmeldet, teilt er diesem automatisch den Inhalt seines Shared-Folders mit. Bei Überwachungsmaßnahmen durch die Staatsanwaltschaft kann somit auch nur der Inhalt dieses Ordners überprüft werden. Andere Ordner des Computers sind quasi „unsichtbar“.

Neuere edonkey2000 Software lässt nicht einmal mehr den „Blick“ in den Shared-Folder eines Nutzers zu. Hier kann das vom Nutzer angebotene Musikrepertoire tatsächlich nur noch überprüft werden, wenn eine Zugriffsmöglichkeit auf den Server besteht. In den aktuellen Fällen kann die Musikindustrie auf zwei Weisen an den Inhalt der Inbox des einzelnen Nutzers gelangt sein: Entweder der betroffene Nutzer verwendete noch eine veraltete edonkey2000 Software, bei der noch der Inhalt des Shared-Folder für jedermann sichtbar war oder der Musikindustrie war über die Kontrolle des Servers im Erft-Kreis die Einsichtnahme in die Inbox des Nutzers möglich. Auf diese Weise wird dann festgestellt, welche weiteren Musikstücke der Betroffene noch anbietet. Dabei werden die weiteren Lieder allein anhand des vom jeweiligen Anbieter gewählten Dateinamens identifiziert.

2. Serverlose Filesharing-Systeme

Der ursprüngliche Entwickler des edonkey2000 Netzwerkes schuf mit Overnet eine neue Client-Software, die völlig ohne Server auskommt. Die Kommunikation funktioniert hier nur von Client zu Client. Dabei ist ein Client immer mit mehreren weiteren Clients verbunden. Die Suche nach einem Musikstück funktioniert in diesem Netzwerk wie folgt: Nutzer A fragt die mit ihm verbundenen Nutzer B, C, D nach einem bestimmten Song. Ist auf der Festplatte eines dieser Nutzer das angefragte Lied vorhanden, wird es an Nutzer A übermittelt. Hat keiner der mit Nutzer A verbundenen Clients das gewünschte Musikstück, wird die Suchanfrage weitergeleitet. Nutzer B, C und D fragen dann alle mit ihnen verbundenen Nutzer nach dem von Nutzer A gewünschten Song XY. Ein solches Servernetzwerk kann von außen kaum überwacht werden. Über jeden einzelnen Nutzer geht nur ein Bruchteil der gesamten Suchanfragen. Der Nachteil an diesem System ist, dass die Suche nach Dateien nur sehr langsam vorangeht. Darüber hinaus wird ein großer Teil der Bandbreite, die den einzelnen Clients zur Verfügung steht, allein für die Suchanfragen verbraucht. Insofern haben solche serverlosen Tauschbörsen, zu denen neben Overnet auch Gnutella zählt, nie die Beliebtheit der serverbasierten Systeme erreicht. Um allerdings die große Last auf den Servern zu entlasten, werden derzeit eDonkey-Hybridclients entwi-

3 Vgl. <http://de.wikipedia.org/wiki/EDonkey2000> (Stand: 18. 1. 2007).

4 Vgl. V. 2.

5 Vgl. IV. 2.

ckelt, die Suchanfragen sowohl über zentrale Server als auch von Client zu Client durchführen.

3. Die IP-Adresse

Wichtigstes Element beim Tausch über Filesharing-Netzwerke stellt die so genannte IP-Adresse dar. Sie ist auch der erste Ansatzpunkt für eine spätere staatsanwaltschaftliche Ermittlungstätigkeit. Die IP-Adresse ist als eine Art Telefonnummer anzusehen, über die jeder Computer in einem Netzwerk angewählt und identifiziert werden kann. Wählt sich ein Nutzer über seinen Accessprovider (zum Beispiel T-Online) ins Internet ein, wird seinem Computer für die Zeit der „Online-Sitzung“ eine einmalige und unverwechselbare Nummer zugeteilt. Bei der Nutzung eines Tauschnetzwerks teilt ein Client dem Server nicht nur die in seiner Inbox vorhandenen Daten bzw. Musikstücke mit; er übermittelt gleichzeitig auch die IP-Adresse des Rechners, auf dem sich diese Daten befinden. Anfragende Clients können dann diese IP-Adresse anwählen und sich mit dem dahinter stehenden Computer verbinden.

Dem normalen Nutzer wird bei jeder „Online-Sitzung“ immer wieder eine neue IP-Adresse zugeteilt. Hierbei handelt es sich um so genannte dynamische IP-Adressen. Größere Unternehmen, die ständig mit dem Internet verbunden sind, haben meist feste IP-Adressen. Hier muss man also nur die IP-Adresse wissen und kann sie einem bestimmten Unternehmen zuordnen. Bei dynamischen Adressen müssen zusätzlich noch der Tag und die Uhrzeit der Nutzung bekannt sein, damit eine Zuordnung erfolgen kann. Nur der jeweilige Internet-Provider selbst weiß, welchem seiner Kunden er zu welcher Uhrzeit eine gewisse IP-Adresse zugeordnet hat. Hat sich der Kunde über die normale Telefonleitung oder per ISDN ins Internet eingewählt, kann der Provider noch zusätzlich Auskunft darüber geben, über welche Telefonnummer die Einwahl erfolgte. Bei einer Einwahl über ADSL ist dies nicht möglich. Wählt sich also Nutzer A mit dem ADSL Kennwort des Nutzers B ins Internet ein, so erweckt dies für den Provider den Anschein, als habe sich Nutzer B hier eingewählt. Anders als bei der Einwahl über die normale Telefonleitung oder ISDN kann eine örtliche Zuordnung nicht vorgenommen werden. Noch schwieriger kann die Zuordnung sein, wenn im Haus des Nutzers selbst ein kleines Netzwerk vorhanden ist (so ist es meist bei Wohngemeinschaften) und die Einwahl ins Internet über einen Router erfolgte. Nach außen hin erhält dieser Router nur eine einzige IP-Adresse. Bilden also beispielsweise drei Computer ein kleines Heimnetzwerk, so haben diese drei Rechner zwar innerhalb des Mini-Netzes jeweils eigene IP-Adressen, treten allerdings nach außen als ein Rechner auf.

III. Auskunftsansprüche

Den Schlüssel zum Erfolg bietet die IP-Adresse allerdings nicht nur für die Tauschbörsennutzer, sondern auch für die Musikindustrie und die Staatsanwaltschaft. Aus der Überwachung eines bestimmten Servers ist ersichtlich, unter welcher IP-Adresse zu einem bestimmten Zeitpunkt welche Musikstücke angeboten worden sind. Nur wenn herausgefunden werden kann, welcher Nutzer sich hinter einer solchen IP-Adresse verbirgt, können weitere

strafrechtliche und zivilrechtliche Maßnahmen eingeleitet werden.

1. Auskunftsanspruch der Musikindustrie gegen die Provider

In der Vergangenheit wurde versucht, einen Auskunftsanspruch der Musikindustrie gegenüber dem Provider auf § 101 a UrhG zu stützen. Einen solchen Anspruch lehnten allerdings kürzlich das OLG Frankfurt a.M. und das OLG Hamburg ab.⁶ Dieser Anspruch ist allerdings in Planung und soll schon bald kodifiziert werden.⁷ Der entsprechende Referentenentwurf, der der Umsetzung des Art. 8 der Richtlinie 2004/48/EG dient, sieht einen eigenen Auskunftsanspruch des Rechteinhabers vor, sofern das Angebotsvolumen des Verletzers ein gewerbliches Ausmaß erreicht hat. Angesichts der Tatsache, dass beispielsweise Musikstücke in Tauschbörsen kostenlos getauscht werden, stellt sich die Frage, ob hier überhaupt ein gewerbliches Ausmaß erreicht werden kann. Sollte der vorliegende Referentenentwurf zu § 100 UrhG tatsächlich in dieser Form umgesetzt werden, müssen die Rechteinhaber zur Durchsetzung des Auskunftsanspruchs noch eine weitere Hürde überwinden: Der so genannte Richtervorbehalt sieht vor, dass die Nutzerdaten erst nach vorheriger richterlicher Anordnung (entsprechend §§ 100 g, h StPO) herausgegeben werden dürfen. In der Literatur wird bereits bezweifelt, dass die Rechteinhaber die hohen Hürden dieses Auskunftsanspruchs auf sich nehmen werden. Vielmehr werde wohl auch weiterhin der Umweg über das Strafverfahren präferiert.⁸

2. Der Umweg über das Strafverfahren

Da es einen solchen direkten Auskunftsanspruch der Musikindustrie derzeit noch nicht gibt, erstatten die Rechteinhaber derzeit zunächst Strafanzeige gegen Unbekannt wegen Urheberrechtsverletzung und beantragen dann gemäß § 406e StPO Einsicht in die Ermittlungsakten. Das erforderliche berechnete Interesse ist bereits mit dem geplanten Zivilverfahren gegeben. Auch zukünftig wird dies wohl der Weg sein, den die Musikindustrie wählen wird. Für eine Auskunft der IP-Adresse verlangt beispielsweise T-Online rund 35 €. Bei tausenden Strafanzeigen kommen schnell astronomische Summen zu Stande, die von den Staatsanwaltschaften in Deutschland zu tragen sind. Beim Weg über den geplanten zivilrechtlichen Auskunftsanspruch hätten die Rechteinhaber diese Kosten zu tragen.

a) Notwendigkeit eines richterlichen Beschlusses

Umstritten ist derzeit ob die Staatsanwaltschaft gegen Vorlage von IP-Adresse und Uhrzeit direkt vom Provider die Herausgabe der Nutzerdaten verlangen kann oder ob dafür zunächst ein richterlicher Beschluss notwendig ist.⁹ Das hängt davon ab, ob man die begehrten Daten als Ver-

6 OLG Frankfurt a.M., Urt. v. 25. 1. 2005 – 11 U 51/04, GRUR-RR 2005, 147 sowie OLG Hamburg, Urt. v. 28. 4. 2005 – 5 U 156/04, GRUR-RR 2005, 209.

7 Ausführlich dazu: *Dietrich*, Anm. zu LG Flensburg, Urt. v. 25. 11. 2005 – 6 O 108/05, GRUR-RR 2006, 145.

8 Vgl. *Frommer*, FAZ v. 12. 7. 2006, S. 23.

9 Ausführlich dazu: *Sankol*, MMR 2006, 361.

bindungsdaten oder nur als Bestandsdaten einordnet. Bei Bestandsdaten kann gemäß § 113 TKG formlos die Auskunft verlangt werden.¹⁰ Handelt es sich um Verbindungsdaten, so erfordert das Auskunftsverlangen der Staatsanwaltschaft gemäß §§ 100 g, h StPO einen richterlichen Beschluss. Bestandsdaten sind solche Daten, die sich schon allein dem Vertragsverhältnis zwischen dem Provider und dem Kunden entnehmen lassen. Verbindungsdaten sind dagegen diejenigen Daten, die bei jeder Verbindung anfallen; zu den Verbindungsdaten zählt also die bei jeder Einwahl neu zugewiesene IP-Adresse. Die Landgerichte Ulm und Bonn¹¹ gehen davon aus, dass eine Auskunft nur im Rahmen des Richtervorbehalts erteilt werden kann, die Landgerichte Köln, Stuttgart und Hamburg vertreten die gegenteilige Auffassung.¹² In etlichen Verfahren gehen die Staatsanwaltschaften davon aus, dass ein richterlicher Beschluss nicht benötigt wird. Dies wurde wie folgt begründet: Zwar werde anerkannt, dass die IP-Adresse zu den Verbindungsdaten gehöre. Die IP-Adresse sei jedoch bereits von der Staatsanwaltschaft bzw. der Musikindustrie protokolliert worden und liege daher schon vor. Auskunft werde nur über die zugehörigen Nutzerdaten verlangt, diese gehörten den Bestandsdaten an. In den wenigen Fällen, in denen sich die Provider zur Wehr setzten und einen entsprechenden richterlichen Beschluss forderten, beantragte die Staatsanwaltschaft Karlsruhe diesen und gelangte so ebenfalls an die Nutzerdaten. Eine pragmatische, wenn auch nicht unbedingt konsequente Lösung des Problems. In diesem Zusammenhang sei – wie später noch zu erörtern sein wird¹³ – schon einmal darauf hingewiesen, dass die Provider nicht zur Speicherung der Daten verpflichtet sind. Insofern speichern manche Provider die Daten überhaupt nicht oder nur über einen kurzen Zeitraum. Das Erfordernis eines Richtervorbehalts beim Auskunftsverlangen durch die Staatsanwaltschaft verzögert den Auskunftsprozess in der Regel ungemein. Dies führt dazu, dass bei Vorliegen des entsprechenden Beschlusses die Verbindungsdaten meist bereits gelöscht sind und nicht mehr herausgegeben werden können. Selbst wenn man allerdings die Auffassung vertritt, dass die Staatsanwaltschaft die entsprechenden Nutzerdaten nicht rechtmäßig erlangt hat, so führt dies nicht zu einem Beweisverwertungsverbot.

*Dietrich*¹⁴ rät dazu, den Provider zumindest zu drängen, einen richterlichen Beschluss zu fordern. Dieser könne nach der Rechtsprechung des BVerfG¹⁵ möglicherweise untersagt werden. Dann dürften die Daten nicht herausgegeben und dem Provider könnten zivilrechtliche und strafrechtliche (§ 206 StGB) Folgen vorgehalten werden. Dem ist jedoch entgegenzuhalten, dass der einzelne Betroffene meist erst im Nachhinein erfährt, dass seine Daten herausgegeben worden sind. Es ist kein Fall bekannt, in dem ein Provider zunächst den Nutzer über das laufende Strafverfahren informiert hat, bevor die Daten herausgegeben wurden.

b) Datenspeicherung durch den Provider

Um zu verhindern, dass der Provider zum Zeitpunkt des Auskunftsverlangens bereits die Verbindungsdaten gelöscht hat und somit eine Zuordnung der IP-Adresse zu einem bestimmten Nutzer nicht mehr möglich ist, fordern die Rechteinhaber die Provider schon bei Protokollierung der IP-Adresse zu Datenspeicherung auf. Dies führt dazu,

dass die Provider in Deutschland täglich hundertfach per E-Mail zur Datenspeicherung aufgefordert werden. Gegen dieses Vorgehen wehrte sich der Provider Verizon mit Erfolg vor dem LG Flensburg.¹⁶ Die Flensburger Richter verneinten einen Anspruch des Rechteinhabers auf Datenspeicherung und sahen in dem massenhaften Zusenden von E-Mails einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb.¹⁷

In diesem Zusammenhang sollte übrigens beachtet werden, dass Provider zumindest bei ihren Flatrate-Kunden die IP-Adresse nicht speichern dürfen.¹⁸ Gegen eine solche Speicherpraxis des Anbieters T-Online hatte sich ein Benutzer gewehrt und vor dem LG Darmstadt Recht bekommen.¹⁹ Sofern dies nicht für abrechnungstechnische Zwecke im Sinne von § 96 TKG erforderlich sei, dürfe bei Flatrate-Kunden eine Speicherung der IP-Adresse nicht erfolgen, entschieden die Darmstädter Richter. Mit Beschluss von 26. 10. 2006 (BGH III ZR 40/06, K&R 2006, 578 ff.) hat der BGH dieses Urteil mittlerweile bestätigt.²⁰

Schon bald könnte der Streit über die Speicherung der IP-Adresse allerdings hinfällig werden. Die am 3. 5. 2006 in Kraft getretene EU Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) sieht vor, dass Verbindungsdaten bis zu 24 Monate gespeichert werden dürften.²¹ Irland und die Slowakei versuchen derzeit, diese Richtlinie vor dem EuGH zu Fall zu bringen.²²

IV. Strafrechtliche Aspekte des Filesharing

In strafrechtlicher Hinsicht hat Bundesjustizministerin Brigitte Zypries zunächst geplant, im Rahmen der anstehenden nächsten Urheberrechtsnovelle (2. Korb) eine so genannte Bagatellklausel für geringfügige Urheberrechtsverletzungen in Tauschbörsen einzuführen. Diese Klausel wurde jedoch auf Druck der CDU/CSU aus dem Regierungsentwurf gestrichen.²³ Eine Art Bagatellklausel hat die Staatsanwaltschaft Köln bei den aktuellen Verfahren aber dennoch angewandt: Hausdurchsuchungen wurden nur bei denjenigen Nutzern durchgeführt, in deren In-

¹⁰ *Dietrich*, NJW 2006, 809 ff.

¹¹ LG Ulm, Beschl. v. 15. 10. 2003 – 1 Qs 1088/03, MMR 2004, 187; LG Bonn, DuD 2004, 628, m. Anm. *Köbele*, DuD 2004, 609.

¹² LG Köln, Beschl. v. 30. 6. 2004 – 111 Qs 124/04; LG Stuttgart, Beschl. v. 4. 1. 2005 – 13 Qs 89/04, NJW 2005, 614 = CR 2005, 598 m. Anm. *Gercke*; LG Hamburg, Beschl. v. 23. 6. 2005 – 631 Qs 43/05, MMR 2005, 711.

¹³ Vgl. III. 2. b).

¹⁴ *Dietrich*, NJW 2006, 809, 810.

¹⁵ BVerfG, Urte. v. 12. 3. 2003 – 1 BvR 330/96 u. 1 BvR 348/99, 1 BvR 330/96, 1 BvR 348/99, NJW 2003, 1787.

¹⁶ LG Flensburg, Urte. v. 25. 11. 2005 – 6 O 108/05, GRUR-RR 2006, 174 ff.

¹⁷ Vgl. auch *Dietrich*, Anm. zu LG Flensburg, Urte. v. 25. 11. 2005 – 6 O 108/05, GRUR-RR 2006, 145.

¹⁸ Vgl. dazu auch *Solmecke*, MMR 2006, Heft 7, XXIII.

¹⁹ LG Darmstadt, Urte. v. 25. 1. 2006 – 25 S 118/2005, K&R 2006, 290 ff.

²⁰ Allerdings hat der BGH die Beschwerde bereits aus formellen Gründen abgelehnt und sich in der Sache nicht mit dem Darmstädter Urteil beschäftigt. Nach Ansicht der Bundesrichter hatte T-Online nicht die für die Beschwerde erforderliche Mindestbeschwerde von 20 000 € ausreichend dargelegt (vgl. § 26 Nr. 8 EGZPO).

²¹ *Vassilaki*, MMR 2006, Heft 2, XIII.

²² Vgl. ausführliche Berichterstattung zur Vorratsdatenspeicherung: <http://www.heise.de/ct/hintergrund/meldung/66857> (Stand: 18. 1. 2007).

²³ Heise online, Bundesregierung will bis zu drei Jahre Haft für illegale Filesharer, News vom 22. 3. 2006, abrufbar unter: <http://www.heise.de/newsticker/meldung/71125> (Stand: 18. 1. 2007).

box mehr als 500 Musikstücke gesichtet worden sind. In den meisten dem Verfasser vorliegenden Fällen erfolgte eine Einstellung des Strafverfahrens gemäß § 153 StPO, wobei die Einstellung damit begründet wurde, dass es sich bei den Betroffenen um Ersttäter handele, die durch das Strafverfahren nachhaltig beeindruckt worden seien.

Als strafrechtlich relevante Handlungsmöglichkeiten kommen grundsätzlich der Upload und der Download von Musik in Betracht. Zu berücksichtigen ist dabei allerdings, dass bei Tauschbörsen der Upload und der Download eng miteinander verknüpft sind. Heruntergeladene Teilstücke werden automatisch wieder zum Upload angeboten. Vielen Nutzern ist diese Tatsache allerdings nicht bekannt, so dass bezüglich des Uploads bereits der Vorsatz fraglich ist. Bei einigen edonkey2000 Clients lässt sich der Upload komplett sperren.

1. Download

Durch das Herunterladen eines urheberrechtlich geschützten Musikstücks wird auf der Festplatte eine Kopie hergestellt. Darin ist zunächst einmal eine unerlaubte Verwertung urheberrechtlich geschützter Werke im Sinne von §§ 106, 16 Abs. 1 UrhG zu sehen. Für den Eigengebrauch ist eine solche Kopie als Privatkopie im Sinne von § 53 UrhG erlaubt, „soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte Vorlage verwendet wird“. Ob die Vorlage, die über Musiktauschbörsen angeboten wird, rechtswidrig hergestellt worden ist oder ob es sich um eine Originalvorlage handelt, ist dem herunterladenden Nutzer in der Regel nicht ersichtlich. Insofern gehen Literatur und Rechtsprechung derzeit davon aus, dass in den meisten Fällen der Download von Musik nicht strafbar ist. Dieser Aspekt soll allerdings bei der bevorstehenden Urheberrechtsreform berücksichtigt werden. Dann soll nicht mehr nur noch darauf abgestellt werden, ob die Vorlage offensichtlich rechtswidrig ist; vielmehr soll die Privilegierung der Nutzer durch § 53 UrhG auch dann nicht greifen, wenn ein urheberrechtlich geschütztes Werk in offensichtlich rechtswidriger Weise angeboten wurde. Bei einem bekannten Musikstück ist dann wohl offensichtlich, dass ein kostenloses Angebot in Musiktauschbörsen nicht gewünscht und damit rechtswidrig ist. Problematischer könnte dies schon bei Songs von unbekanntem Bands sein. Diese bieten ihre Lieder oft kostenfrei an, um auf sich aufmerksam zu machen.²⁴

2. Upload

Quasi alle Tauschbörsennutzer beabsichtigen vornehmlich den Download von Musik; dabei bieten sie allerdings (unbewusst oder bewusst) diese Musik meist auch automatisch zum Upload an. Darin ist eine strafbare Handlung zu sehen. Seit der Urheberrechtsnovelle im Jahr 2003 erfasst § 15 Abs. 2 UrhG ausdrücklich auch das Recht der öffentlichen Zugänglichmachung (§ 19a UrhG). Strafbar macht sich ein Nutzer gemäß § 106 UrhG bereits in dem Moment, in dem er sich mit seinem edonkey2000 Client am Server anmeldet oder bei der serverlosen Version Kontakt zum nächsten Client aufnimmt. In diesem Moment hat die Öffentlichkeit Zugriff auf das in der Inbox des Nutzers liegende urheberrechtlich geschützte Musikrepertoire.

Pikant ist in diesem Zusammenhang die Tatsache, dass es in den aktuellen Ermittlungsverfahren erst durch den Betrieb des Servers im Erft-Kreis möglich war, urheberrechtlich geschütztes Material öffentlich zugänglich zu machen. Anders als die Musikindustrie behauptet, ist der Betrieb eines solchen Servers zumindest als strafrechtlich relevante Beihilfehandlung anzusehen.²⁵ Noch vor einigen Jahren hat übrigens auch die Musikindustrie eine Verantwortlichkeit des Serverbetreibers gesehen.²⁶ Aktuell ist nicht bekannt, ob die proMedia GmbH den von ihr kontrollierten Server auch betrieben hat. Insofern sollen hierzu nähere rechtliche Ausführungen – zu denken wäre eventuell an eine Tatprovokation durch einen agent provocateur – zunächst unterbleiben.

3. Beweisfragen

Wurde bei dem Betroffenen keine Hausdurchsuchung durchgeführt, kann sich die Beweissituation für die Staatsanwaltschaft mitunter als schwierig darstellen. Über die protokollierte IP-Adresse und die ihr zugeordneten Nutzerdaten kann lediglich festgestellt werden, über welchen Nutzeraccount die Einwahl ins Internet erfolgte. Welche Person sich tatsächlich eingewählt hat, bleibt offen. In einem Mehrpersonenhaushalt – insbesondere bei Familien mit Kindern – wird oft nur schwer zu ermitteln sein, wer die Tat tatsächlich begangen hat. Gleiches gilt für Wohngemeinschaften, bei denen sich mehrere Nutzer über einen Router ins Internet einwählen. In WLAN Funknetzen besteht darüber hinaus die Möglichkeit, dass sich Dritte unbemerkt eingewählt und die Urheberrechtsverletzung begangen haben. Wurde von der Musikindustrie nicht einmal ein Song zu Testzwecken heruntergeladen, so muss dem Nutzer zunächst einmal nachgewiesen werden, dass er den Upload – und damit die derzeit einzig strafbare Handlung – überhaupt angeboten und nicht etwa gesperrt hat.

V. Zivilrechtliche Aspekte des Filesharing

Zweifelsohne liegt das Hauptinteresse der Musikindustrie nicht in der Durchführung eines Strafverfahrens. Das Strafverfahren dient nur als Vehikel zur Erlangung der Nutzerdaten und gegebenenfalls zur Abschreckung. In den aktuellen Verfahren beantragte die Hamburger Kanzlei Rasch Akteneinsicht und forderte dann von den Betroffenen die Abgabe einer strafbewehrten Unterlassungserklärung sowie die Zahlung eines pauschalierten Schadensersatzanspruchs. Die Höhe des angesetzten Schadensersatzanspruchs richtet sich jeweils nach der Anzahl der angebotenen Musikstücke. Sie schwankt zwischen 2000 € und 10000 €. Ausführungen dazu, wie sich dieser Schadensersatzanspruch zusammensetzt, werden in dem Abmahnschreiben nicht gemacht.

24 Selbst Chart-Stürmer wie die Sportfreunde Stiller bieten mitunter ihre Hits kostenfrei im Netz an. Zuletzt stand ihr WM-Hit, der Platz 1 der deutschen Charts erobert hatte, kostenfrei zum Download im Netz, vgl. *Hottes, Sascha*, 54, 74, 90, 2010: Sportfreunde Stiller verschenken MP3, *Netzwelt* vom 7. 7. 2006, abrufbar unter: <http://www.netzwelt.de/news/74314-54-74-90-2010-sportfreunde.htm> (Stand: 18. 1. 2007).

25 *Heghmanns*, MMR 2004, 14, 16; *Solmecke*, MMR 2006, Heft 7, XXIII.

26 *Braun*, GRUR 2001, 193 ff. und 307 ff., GRUR 2001, 1106, 1110.

1. Unterlassungsanspruch

Ein Unterlassungsanspruch steht den Rechteinhabern zunächst einmal gemäß § 97 UrhG gegen den eigentlichen Verletzer zu. Soweit ersichtlich, hat sich bislang vornehmlich das LG Hamburg mit einem solchen Anspruch im Rahmen des Filesharings auseinandergesetzt. Das Gericht lässt auch einem Unterlassungsanspruch gegen den Inhaber des Telefon- bzw. Internetanschlusses, über den die Einwahl ins Internet erfolgte, im Wege der Störerhaftung zu.²⁷ In dem vom LG Hamburg entschiedenen Fall ging es darum, dass Eltern ihren Kindern die Internetnutzung ohne weitere Einschränkungen gestattet hatten. Die Richter fordern, dass Eltern bzw. jeder, der seinen Internetanschluss einem Dritten zur Verfügung stellt, alles Erdenkliche tut, um Urheberrechtsverletzungen zu verhindern. Insbesondere solle durch die Einrichtung von Nutzerkonten verhindert werden, dass überhaupt Filesharing-Software auf dem Rechner installiert werden kann. Firewalls sollten die gängigen P2P-Ports sperren.

Dabei übersehen die Richter, dass Filesharing Software an sich nicht illegal ist. Das beliebte Betriebssystem Linux wird beispielsweise zum Großteil im Wege des Filesharings vertrieben. Insofern ist schon nicht ersichtlich, warum Eltern ihren Kindern etwa die Installation von Filesharing Software verbieten sollen. Selbiges gilt für die Sperrung der gängigen Filesharing-Ports, die im Übrigen höchstwahrscheinlich ohnehin den meisten Eltern schon technisch nicht möglich sein dürfte.

Die urheberrechtliche Störerhaftung von Personen, die nicht selbst die rechtswidrige Nutzungshandlung vorgenommen haben, setzt die Verletzung von Prüfungspflichten voraus. Diese Prüfungspflichten beziehen sich nach Auffassung des BGH²⁸ lediglich auf grobe und unschwer zu erkennende Verstöße. Eltern müssen aber ohne Anlass nicht damit rechnen, dass ihre Kinder den Internetanschluss zu Urheberrechtsverletzungen nutzen werden. Eine solche Auffassung hat auch das OLG Hamburg²⁹ vertreten. In dem vergleichbaren Fall ging es darum, dass ein Kind in einer Zeitung annonciert und Raubkopien zum Tausch angeboten hatte. Seinerzeit wurde versucht, die Eltern auf Unterlassung in Anspruch zu nehmen. Der Junge hatte sich die getauschten Raubkopien an die Anschrift seiner Eltern schicken lassen. Das OLG Hamburg verneinte eine Adäquanz gerade mit dem Hinweis darauf, dass die Eltern mit einer Rechtsverletzung nicht rechnen mussten.

²⁷Diese Auffassung vertritt offenbar auch das LG Mannheim, das mit Urteil vom 29. 9. 2006 (Az. 7 O 76/06) eine Mitstörerhaftung von Eltern für P2P-Urheberrechtsverletzungen ihres volljährigen Sohnes verneinte und sich damit gegen die Rechtsprechung des LG Hamburg stellt.

Abgesehen davon kann eine Störerhaftung wenn überhaupt nur dann in Betracht kommen, wenn die betreffende Handlung überhaupt hätte verhindert werden können. Das ist gerade bei Urheberrechtsverletzungen in Zusammenhang mit dem Internet nicht der Fall. Es gibt mannigfaltige Möglichkeiten, ein geschütztes Werk ins Internet zu stellen.³⁰ Das Filesharing ist nur eine dieser Möglichkeiten. Ohnehin sind Kinder ihren Eltern meist technisch überlegen und können die aufgestellten Hürden problemlos umgehen. Anders als das LG Hamburg

meint, ist es Eltern nicht zuzumuten, gegebenenfalls die Hilfe eines IT-Experten zur entsprechenden Überprüfung und Konfiguration des Rechners in Anspruch zu nehmen.

2. Schadensersatzanspruch

Sofern vom vermeintlichen Verletzer die Zahlung eines pauschalierten Schadensersatzes verlangt wird, sollten die Rechteinhaber zunächst dazu aufgefordert werden, den Schaden genau aufzuschlüsseln. Denkbar sind drei vom Verletzten wählbare Kalkulationsarten: Der Ersatz des entgangenen Gewinns, die Herausgabe des vom Schädiger erlangten Gewinns oder die Zahlung einer angemessenen Lizenzgebühr. Da der Tausch kostenlos erfolgte, wird der Schädiger in der Regel keinerlei Gewinne erlangt haben. Auch die Berechnung des entgangenen Gewinns dürfte sich für den Rechteinhaber als schwierig darstellen. Eine Harvard-Studie vom März 2004³¹ kommt zu dem Ergebnis, dass der Schaden, der durch Musiktauschbörsen entstanden ist, gegen Null tendiert. Der Rechteinhaber wird demnach bei der Berechnung des Schadens auf die Lizenzanalogie zurückgreifen. Dabei wird allerdings zu berücksichtigen sein, dass nicht nachvollzogen werden kann, wie oft und wie lange ein Musikstück tatsächlich vom Verletzer verbreitet worden ist. Hinzu kommt, dass oft nur Teilstücke verbreitet worden sind, die jedes für sich genommen noch keine Werkqualität aufweisen.³²

VI. Fazit

In der Rechtsprechung nimmt die Zahl der Filesharing-Fälle rapide zu. Die Musikindustrie hat eine deutlich schärfere Gangart eingeschlagen und geht mit ungewohnter Härte gegen Tauschbörsennutzer vor. Dabei ist die juristische Lage alles andere als geklärt. Insbesondere die Störerhaftung wird die Gerichte in Zukunft noch zuhauf beschäftigen. Sollte sich die derzeitige Rechtsprechung des LG Hamburg durchsetzen, ist niemandem mehr anzuraten, seinen Internetzugang auch Dritten zur Verfügung zu stellen. Es bestünde permanent die Gefahr, auf Unterlassung einer – durch den Dritten begangenen – Urheberrechtsverletzung in Anspruch genommen zu werden.

Hinweis der Redaktion:

Lesen Sie hierzu auch das Urteil des LG Mannheim, K&R 2007, 174 ff. (in diesem Heft) zur Frage der Aktivlegitimation bei Klagen wegen Urheberrechtsverletzungen durch Filesharing.

27 LG Hamburg, Beschl. v. 25. 1. 2006 – 308 O 58/06, MMR 2006, 700.

Vgl. zu Störerhaftung auch *Leistner*, GRUR 2008, 801–814.

28 BGH, Urt. v. 15. 10. 1998 – I ZR 120/96, NJW 1999, 1960 = WRP 1999, 211.

29 OLG Hamburg, Urt. v. 18. 5. 1995 – 3 U 279/94, CR 1995, 603.

30 Vgl. dazu das Gutachten von Prof. Dr. Dieter Homeister von der Fachhochschule Heidelberg (Fakultät für Informatik) „Technische Durchführbarkeit der Blockierung von Filesharing Diensten und Hindernisse bei der Beweisführung bei Urheberrechtsverletzungen“ abrufbar unter <http://www.wbe-law.de/news/it-telekommunikationsrecht/40/filesharing-gutachten/> (Stand: 18. 1. 2007).

31 Abrufbar unter: http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf (Stand: 18. 1. 2007).

32 *Gutman*, MMR 2003, 706.