CHRISTIAN SOLMECKE / JAN BÄRENFÄNGER

Urheberrechtliche Schutzfähigkeit von Dateifragmenten

Nutzlos = Schutzlos

Immaterialgüterrecht

Rund um Filesharing-Abmahnungen gibt es viele diskussionswürdige Themen – von Missbräuchlichkeit von Abmahnungen über Grenzen der Störerhaftung und Beweislastverteilung bis zur möglichen Deckelung von Abmahnkosten. Dieser Beitrag richtet den Fokus auf ein bislang noch vollkommen unbeachtetes Gebiet: Zu welchem Zeitpunkt wird beim Filesharing eigentlich die Urheberrechtsverletzung begangen? Können insbesondere bereits die Dateifragmente, die während des Downloads entstehen, taugliches Tatobjekt einer Urheberrechtsverletzung sein? Urheberrechtlicher Schutz und daran anschließend mögliche Sanktionen kommen nur in Betracht, wenn schon das Dateifragment als solches abgespielt werden kann. Vom Abmahnenden ist darzulegen und zu beweisen, dass im Zeitpunkt der Abmahnung ein solches schutzfähiges Fragment auf dem Rechner des Abgemahnten vorhanden war.

I. Einleitung

575.800 Abmahnungen wegen angeblicher Urheberrechtsverletzungen mit Schadensersatzforderungen von € 412 Mio. sollen 2010 verschickt worden sein.[1] Damit versuchen Urheber und Inhaber von Verwertungsrechten durch Abschreckung Urheberrechtsverletzungen in Internet-Tauschbörsen einzudämmen und gleichzeitig den dadurch erlittenen Schaden zu kompensieren.[2]

Ohne die Kontroverse um Redlichkeit und Sinnhaftigkeit der Massenabmahnungen aufzugreifen[3] oder in Frage zu stellen, dass in Tauschbörsen in großer Zahl Urheberrechtsverletzungen stattfinden, soll dieser Beitrag den Fokus auf eine andere, in Rechtsprechung und Literatur noch gänzlich unbehandelte Frage richten: Werden diese Urheberrechtsverletzungen eigentlich nach den Regeln der ZPO nachgewiesen? Oder, pointierter: Ergeht die Masse der Filesharing-Abmahnungen eigentlich zu Recht?

Denn bislang wird nur dokumentiert, dass irgendwie ein Up- oder Download eines Films oder Musikstücks über den Anschluss des Abgemahnten erfolgt ist, ohne Rücksicht darauf, ob diese Datei vollständig geladen wurde. Eine Abmahnung kann aber nur begründet sein, wenn die fragliche Datei, wegen deren Down- oder Upload abgemahnt wird, in diesem Moment dem Urheberschutz zugänglich ist.

In diesem Beitrag sollen zunächst die Funktionsweise der gängigen Tauschbörsen sowie der gängigen Dateiformate erläutert werden (dazu II.). Daran schließen sich die Beurteilung der Schutzfähigkeit von Dateifragmenten (III.) und Auswirkungen auf die Praxis (IV.) an.

II. Technische Vorfragen

1. Funktionsweise von Tauschbörsen

Beim „normalen" Herunterladen von Dateien im Internet stellt der sog. Hoster ein Musikstück, ein Video oder ein Softwareprogramm in Dateiform auf einem Server zur Verfügung. Durch eine Website wird auf diese Datei verlinkt, damit sie von Nutzern durch Suchmaschinen gefunden und dann heruntergeladen werden kann. Auch die One-Click-Hoster wie *RapidShare* funktionieren nach diesem Prinzip, das als „Server-Client" bezeichnet wird.[4]

Anders sieht es bei den Tauschbörsen, also den Filesharing-Netzwerken aus. Diese funktionieren nach dem „Peer-to-Peer"(P2P)-Prinzip. Dort werden die getauschten Dateien unter Verwendung besonderer Software direkt zwischen normalen Internetnutzern ausgetauscht. Dabei wird zwischen zwei Varianten unterschieden: Dem P2P mit Koordinationsserver – hier sind das BitTorrent- und das eDonkey-Netzwerk zu nennen – und dem vollständig dezentralen P2P, zu denen eMule, LimeWire und KaZaA gehören.[5]

a) P2P mit Koordinationsserver

Beim P2P mit Koordinationsserver verwaltet ein Server die Liste der von den Nutzern (Clients oder Peers genannt) angebotenen Dateien. Der Nutzer sendet eine Suchanfrage an einen solchen Server und übermittelt gleichzeitig, welche Dateien er selber anbietet. Der eigentliche Austausch der Datenblöcke erfolgt dann direkt zwischen den Clients.[6] Das Prinzip ähnelt einer Telefonauskunft mit Vermittlung: Der Nutzer fragt bei der Auskunft an, wo er eine bestimmte Datei bekommt, und wird an den entsprechenden Teilnehmer vermittelt, ohne dass die vermittelnde Stelle selber Teil des Datenaustauschs wird.

Dabei ist gleichzeitiger Download von mehreren Quellen möglich.[7] Das ist nötig, denn der Download des „saugenden" Peers ist aus Sicht des anbietenden Peers ein Upload – und die Upload-Geschwindigkeit beträgt bei normalen Anschlüssen oft weniger als 10% der Download-Geschwindigkeit. Durch den Download aus mehreren Quellen können so sehr hohe Geschwindigkeiten erreicht werden. Je weiter also eine bestimmte Datei verbreitet ist, umso schneller kann sie noch weiter verbreitet werden. Darin liegt eine Stärke des P2P-Prinzips gegenüber dem herkömmlichen Server-Client-System.[8]

Rein praktisch läuft das im Falle des populären BitTorrent-Netzwerks so, dass ein Anbieter zunächst eine Textdatei erstellt, in

1 Vgl. Jahresstatistik 2010 des *Vereins gegen den Abmahnwahn e.V.*, abrufbar unter: http://www.verein-gegen-den-abmahnwahn.de/zentrale/download/statistiken/2010/jahresstatistik_2010.pdf.
2 Vgl. dazu *Wiedermann*, Abmahnungen als Geschäft, Westfälische Rundschau v. 30.4.2011, abrufbar unter: http://www.derwesten.de/nachrichten/wirtschaft-und-finanzen/User-muessen-fuer-illegale-Downloads-zu-viel-zahlen-id4592455.html.
3 Vgl. dazu die Darstellung bei *Haedicke*, Patente und Piraten, 2011, S. 16 ff.
4 Vgl. hierzu auch http://de.wikipedia.org/wiki/Filesharing#Prinzip_Server-Client.
5 Vgl. hierzu auch http://de.wikipedia.org/wiki/Filesharing; vgl. auch *Widmaier*, Münchener Anwaltshdb. Strafverteidigung, 2006, Teil L Rdnr. 129.
6 Vgl. hierzu auch http://de.wikipedia.org/wiki/Filesharing#Peer-to-Peer_mit_Koordinationsserver.
7 Vgl. *Widmaier* (o. Fußn. 5), Rdnr. 128.
8 Vgl. hierzu auch http://de.wikipedia.org/wiki/BitTorrent#BitTorrent-Technik.

der Dateiname oder Dateinamen – beim Torrent-Netzwerk können mehrere Dateien in einem Paket angeboten werden, z.B. ganze Staffeln von TV-Serien, Musikalben oder die kompletten TOP-100 der Single-Charts –, die Größe und eine Beschreibung des Inhalts angegeben werden. Außerdem enthält diese Datei die IP-Adresse des Erstellers des Torrents und eine Liste mit einzelnen Dateisegmenten und deren Prüfsummen,[9] denn bei jedem Torrent wird der Inhalt, egal ob es sich um eine oder mehrere Dateien handelt, in viele kleine Teile aufgeteilt, die später unabhängig voneinander heruntergeladen werden. Diese Datei wird dann bei einem sog. „Tracker" – so werden die Koordinationsserver beim BitTorrent-Netzwerk genannt –, z.B. bei „The Pirate Bay",[10] mit der Dateiendung .torrent oder .tor hochgeladen.[11] Über diese Seite können andere Nutzer jetzt den Torrent herunterladen. Noch während der erste Nutzer die Datei fragmentarisch herunterlädt, stehen dem zweiten Nutzer bereits für diesen Teil zwei Quellen zur Verfügung – die ursprüngliche Quelle und der erste Nutzer. Dieser Vorgang potenziert sich, sodass kurze Zeit, nachdem die Datei einmal komplett von einem anderen geladen wurde, bereits eine weite Verbreitung erreicht werden kann. Dabei werden dann die einzelnen Segmente, die in der Torrent-Datei festgelegt sind, in einer willkürlichen Reihenfolge von verschiedenen Quellen geladen und erst auf dem Zielrechner zusammengesetzt. Es kommt so gut wie nie vor, dass in den P2P-Börsen ein Nutzer an einen anderen Nutzer ein gesamtes Werk übermittelt oder dass ein „1:1-Download" erfolgt.

Beim eDonkey-Netzwerk funktioniert es ähnlich, nur dass hierbei stets lediglich einzelne Dateien geladen werden können. Möglich ist aber der Download von Archivdateien, die zwar äußerlich eine einzige Datei sind, selbst wiederum aber mehrere komprimierte Dateien enthalten können.

b) Dezentrales P2P

Um den zentralen Server als störanfälliges Glied auszuschalten, werden in dezentralen P2P-Systemen sämtliche Koordinations- und Verwaltungsaufgaben unter den Peers selbst erledigt, indem Suchanfragen über Nachbarn hinweg gestartet werden, bis Quellen für den Download gefunden werden. Teilweise übernehmen aber bei diesen Systemen einzelne Nutzer („Supernodes") Aufgaben der Koordinationsserver, um die Suchfunktionen zu beschleunigen und das durch ständige Suchanfragen belastete Netz zu entlasten.[12]

Die bekanntesten dezentralen Filesharing-Netzwerke sind das eMule-Kademlia-Netzwerk (bekannteste Software: eMule), das gnutella-Netzwerk (bekannteste Software heute: LimeWire) und das FastTrack-Netzwerk (bekannteste Software: KaZaA/ Kazaa Lite).[13]

c) Verifizierung: Hashwert und Prüfsumme

Um die Verbreitung von Viren, Mal- und Spyware oder falsch benannter Dateien einzuschränken, fragen die Suchfunktionen der jeweiligen genutzten Tauschbörsenprogramme den sog. „Hashwert" ab. Dabei handelt es sich um den „digitalen Fingerabdruck" einer Datei: Mittels einer mathematischen Streuwertfunktion wird aus einer beliebig großen Quellmenge (der Ausgangsdatei, die viele MB groß sein kann) der sog. Hashwert oder Hashcode erzeugt, der nur wenige Zeichen umfasst und dennoch die große Datei eindeutig identifiziert. Diese Hashcodes werden in Tauschbörsen verwendet, um vor dem Download die richtige Datei zu finden und nach dem Download Übertragungsfehler zu erkennen, indem das Download-Programm die Prüfsumme ausrechnet und sie mit dem übermittelten Hashwert abgleicht.[14]

Jedes Teilsegment hat eine einzelne Prüfsumme, damit die einzelnen Segmente am Ende sinnvoll zu einer fertigen Datei zusammengesetzt werden können. Diese wird wiederum durch ihren Hashwert verifiziert. Hashwerte sind fälschungssicher, da sie nicht vergeben, sondern errechnet werden, und verwechslungssicher, weil nahezu niemals dasselbe Ergebnis herauskommen kann – daher die Bezeichnung als „digitaler Fingerabdruck" einer Datei. Es entsteht eine 1:1-Kopie, obwohl sie aus Hunderten Mosaiksteinchen aus verschiedenen Quellen zusammengesetzt ist.

Hashwerte sind für die Überwachung der Tauschbörsen durch Abmahner von größter Bedeutung, da die Rechteinhaber sicherstellen müssen, dass sie tatsächlich auf Grund des Tauschs eines von ihnen geschützten Werks abmahnen und nicht auf Grund eines getarnten Virus.

2. Arten von Dateifragmenten und Nutzbarkeit

Oft wird eine Datei nur fragmentarisch heruntergeladen, etwa bei einer großen oder seltenen Datei. Es kann Stunden, häufig gar Tage dauern, bis sie vollständig ist. Manche Downloads werden niemals fertiggestellt, wenn die Quelle aus irgendwelchen Gründen nicht mehr zur Verfügung steht. Bevor geklärt werden kann, ob – und wenn ja: wie – sich das auf die urheberrechtliche Bewertung auswirkt, soll kurz geschildert werden, welche Arten von Dateifragmenten es gibt.

Fast alle Tauschbörsen-Programme machen die fragmentarischen Dateien kenntlich, etwa indem an die Datei ein „.part", ein Ausrufezeichen oder ähnliches angefügt wird. Das führt dazu, dass das Betriebssystem diese Dateien ohne weiteres keiner Abspiel- oder Betrachtersoftware zuordnen kann und ausführbare Programme, etwa Setup-Dateien für Software, nicht erkennt. Diese Dateien sind zunächst unbrauchbar. Teilweise können diese Dateien dennoch betrachtet oder abgespielt werden. Das hängt davon ab, um was für eine Datei es sich handelt:

- **Musikdateien:** Die gängigen Musikformate können in der Regel schon als Fragment abgespielt werden. Die Technik ist ähnlich wie beim Magnetband einer Kassette: Wenn man einige Zoll bereits heruntergeladen hat, können sie auch abgespielt werden. Zum Abspielen kann die Fragment-Datei in .mp3 umbenannt oder direkt über die Funktion „Öffnen mit" im Kontextmenü mit einem Abspielprogramm geöffnet werden. Es kann aber sein, dass nur Sekundenbruchteile aus verschiedenen Stellen des Musikstücks aneinandergereiht werden – scratching statt Lady Gaga.
- **Videos:** Bei Videos muss differenziert werden: Die meisten aktuellen Formate können ähnlich wie Musikdateien als Teilstücke in der Regel abgespielt werden. Bei einigen Formaten ist ein Abspielen aber erst möglich, wenn die gesamte Datei vorliegt. Durch bloßes Umbenennen können diese Dateien somit nicht genutzt werden. Allerdings gibt es hierfür wieder Hilfsprogramme, die aus der Fragmentdatei die Videodaten dennoch in den meisten, aber nicht in allen Fällen extrahieren können.
- **Bilder:** Bei Bilddateien können die Formate JPEG, GIF und BMP in der Regel geöffnet werden, sofern sie eine bestimmte Dateigröße überschritten haben. Die Bilder enthalten dann schwarze Stellen.
- **Textdateien:** Textdateien können als Fragmente jedenfalls dann nicht geöffnet werden, wenn es sich um PDF-Dokumente handelt. Bei anderen Formaten kann es sein, dass über einen Texteditor einzelne Textpassagen nachvollzogen werden kön-

9 S. dazu unten c).

10 Die entgegen anderslautender Presseberichte nichts mit der Piratenpartei zu tun hat, s. http://www.bildblog.de/8976/wie-ein-pirat-dem-anderen und http://www.bildblog.de/8522/piratenpartei-bringt-medien-zum-kentern.

11 Vgl. hierzu auch http://de.wikipedia.org/wiki/BitTorrent_%28Protokoll%29#Funktion.

12 Vgl. *Widmaier* (o. Fußn. 5), Rdnr. 129.

13 Vgl. hierzu auch http://de.wikipedia.org/wiki/Filesharing#Peer-to-Peer:_vollst._C3.A4ndig_dezentrales_Filesharing.

14 Vgl. hierzu auch http://de.wikipedia.org/wiki/Hashfunktion.

nen. Eine vernünftige Anzeige etwa eines Word-Dokuments ist indes bei beschädigten Dateien – und um nichts anderes handelt es sich bei Teilfragmenten aus Sicht der Software – nicht möglich.

■ **Software und Archivdateien** (.zip, .rar etc.) sind fragmentarisch in jedem Fall nutzlos. Diese Dateien kennen ihre eigene Prüfsumme und können nur geöffnet bzw. ausgeführt werden, wenn diese stimmt.

■ **Charts-Container:** In der Praxis relevant sind insbesondere sog. „Charts-Container". Dabei werden gleich mehrere Dateien, z.B. die TOP-100 der aktuellen Charts, auf einmal angeboten. Auch hier sind zwei Fallgruppen zu unterscheiden: Charts-Container können entweder mittels BitTorrent-Technik als „offene Container" oder über eine Archivdatei, die mit allen Tauschbörsensystemen funktioniert, als „geschlossene Container" konzipiert werden. Bei der Variante des offenen Containers werden in einen „Torrent" beliebig viele Einzeldateien eingestellt, die entweder alle auf einmal, aber auch Stück für Stück heruntergeladen werden können. Dann kann der Nutzer entscheiden, ob er vielleicht nur die besten 20 Lieder oder seine 10 Lieblingslieder laden möchte. Dagegen liegen die Einzeldateien beim geschlossenen Container in einem ZIP- oder RAR-Archiv. Dabei ist der Download einzelner Lieder nicht möglich, es muss das gesamte Archiv vollständig sein, bevor der Inhalt des Containers ausgepackt werden kann. Vorher kann der Nutzer nicht einmal wissen, welche urheberrechtlich geschützten Dateien sich überhaupt in dem Archiv befinden – dafür muss er sich auf die Suchmaschine oder die Dateibeschreibung verlassen, die aber nicht stimmen muss.

III. Urheberrechtliche Schutzfähigkeit von Dateifragmenten

1. Ausgangsfrage: Urheberrechtsfähigkeit von Dateifragmenten?

Haben Nutzer von Tauschbörsen, die den Download noch nicht abgeschlossen haben, bereits eine Urheberrechtsverletzung begangen? Das hängt davon ab, ob die Dateifragmente dem Urheberschutz zugänglich sind.[15] Maßgeblich ist allein, ob das jeweilige Dateifragment den Werkbegriff des § 2 UrhG erfüllt.

a) Wahrnehmbarkeit

Für den Schutz eines Werks muss dieses in irgendeiner Form Gestalt annehmen, also in einer wahrnehmbaren Form vorliegen.[16] Zwar ist eine Vollendung des Werks nicht unbedingt nötig, sodass Vor- und Zwischenstufen sowie Fragmente schutzfähig sein können. Es ist aber anerkannt, dass „die Formgebung zumindest so weit fortgeschritten sein [muss], dass der geistige Gehalt bereits Gestalt gewonnen hat und die erforderliche Individualität zum Ausdruck bringt."[17] In diesem Sinne kann Wahrnehmbarkeit nur vorliegen, soweit das konkrete Dateifragment als solches irgendwie abgespielt oder betrachtet werden kann.

Damit fallen nach der obigen Darstellung als nutzlos einzustufende Fragmente, also Fragmente von Archivdateien, Software, den unvollständig nicht abspielbaren Videoformaten und PDF-Dateien, aus dem urheberrechtlichen Schutz: Sie sind nichts anderes als „Datenmüll", daher gilt die Devise „nutzlos = schutzlos" – was nicht als Werk erkennbar ist, also wahrgenommen und genossen werden kann, ist dem Urheberrechtsschutz nicht zugänglich.

b) Schöpfungshöhe

Bei den Dateien, die bereits als Fragment abgespielt werden können, hängt es von den weiteren Voraussetzungen des § 2 UrhG ab, ob ein Schutz des konkreten Dateifragments besteht. Das hängt vom zentralen Kriterium des Werkbegriffs ab: der Individualität[18] bzw. Schöpfungshöhe,[19] die im Einzelnen für die jeweiligen Dateifragmente zu untersuchen ist.[20]

■ **Musikdateien**

Eine „goldene Regel", ab wie vielen Tönen oder Takten ein Teil eines Musikstücks urheberrechtlich geschützt ist, gibt es nicht.[21] Jedenfalls ist ein niedriger Grad der Schöpfungshöhe ausreichend, sodass hier seit jeher auch die sog. „kleine Münze" geschützt wird.[22] Schutz ist jedenfalls dann anzunehmen, wenn die Melodie abgespielt werden kann.[23] Fraglicher wird es, je kürzer das zusammenhängend abspielbare Fragment ist, insbesondere wenn die Melodie oder Teile davon fehlen. Hier gelangt man irgendwann in den Bereich des Sampling, wo nur noch kürzeste Stücke bis hin zu einzelnen Akkorden oder Schlagzeugfolgen kopiert und verwendet werden. Eine Urheberrechtsverletzung bei Übernahmen im Bereich des Sampling wird nur angenommen, sofern die Tonfolge noch erkennbar individuell ist.[24] Das kann häufig durchaus fraglich sein: Wird ein normales Musikstück der Popmusik mit einer Länge von etwa 3 Minuten technisch bedingt durch die eingesetzte Software in 100 Segmente aufgeteilt, ist jedes Segment keine 2 Sekunden lang. Wenn davon 20 Segmente, also 20%, geladen wurden, kann es sein, dass nur genau jedes fünfte Segment erwischt wurde und beim Abspielen nur zerhackte Geräusche erklingen, die nicht einmal bei weiter Auslegung der „kleinen Münze" geschützt sind.

■ **Videodateien**

Videodateien können als Filmwerke gem. § 2 Abs. 2 Nr. 6 UrhG geschützt sein. Davon erfasst sind Kinofilme, Fernsehfilme und Fernsehserien, egal ob es sich um inszenierte Filme, Kultur- oder Dokumentationsfilme handelt.[25] Dagegen sind Showprogramme in der Regel nicht geschützt.[26] Bei Filmwerken gelten geringe Anforderungen an die Individualität, auch hier ist grundsätzlich die „kleine Münze" erfasst.[27] Wie bei Musikstücken muss sich die Individualität aus dem Fragment ergeben. Das ist bei Filmwerken jedoch stets der Fall, da in jeder Szene und jeder Kameraeinstellung die Individualität durch Gestaltung des Sets,

---

15 Verneinend *Hoeren*, CR 2009, 378, 379; *Gercke*, ZUM 2007, 791, 799; *Wick*, Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter, 2010, S. 40.

16 Vgl. *Loewenheim*, in: Schricker/Loewenheim, 4. Aufl. 2010, § 2 Rdnr. 20; *Bullinger*, in: Wandtke/Bullinger, 3. Aufl. 2009, § 2 Rdnr. 19; *Schulze*, in: Dreier/Schulze, 3. Aufl. 2008, § 2 Rdnr. 13 f.; *A. Nordemann*, in: Fromm/Nordemann, 10. Aufl. 2008, § 2 Rdnr. 23.

17 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 22 mit Verweis auf BGHZ 9, 237, 241 – Gaunerroman; *OLG München* GRUR 1956, 432, 434 – Solange Du da bist.

18 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 23; *Bullinger* (o. Fußn. 16), § 2 Rdnr. 21; *Schulze* (o. Fußn. 16), § 2 Rdnr. 20 f.; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 24; *BGH* GRUR 2004, 855, 857 – Hundefigur; *BGH* GRUR 1994, 206, 207 – Alcolix; *Häuser*, Sound und Sampling, 2002, S. 49.

19 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 24; *Bullinger* (o. Fußn. 16), § 2 Rdnr. 23; *Schulze* (o. Fußn. 16), § 2 Rdnr. 20; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 30.

20 So auch *Häuser* (o. Fußn. 18), S. 49; vgl. auch *Bullinger* (o. Fußn. 16), § 2 Rdnr. 42.

21 Vgl. *Häuser* (o. Fußn. 18), S. 58.

22 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 39, 124; *Bullinger* (o. Fußn. 16), Einl. Rdnr. 4, § 2 Rdnr. 71; *Schulze* (o. Fußn. 16), § 2 Rdnr. 1, 139; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 30, 131.

23 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 125; *Bullinger* (o. Fußn. 16), § 2 Rdnr. 71; *Schulze* (o. Fußn. 16), § 2 Rdnr. 25, 139; *A. Nordeman* (o. Fußn. 16), § 2 Rdnr. 131.

24 Vgl. *Häuser* (o. Fußn. 18), S. 58; *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 68, 128; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 51.

25 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 186 ff.; *Bullinger* (o. Fußn. 16), § 2 Rdnr. 122 f.; *Schulze* (o. Fußn. 16), § 2 Rdnr. 208 f.; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 203 f.

26 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 187, 192; *Bullinger* (o. Fußn. 16), § 2 Rdnr. 124 ff.; *Schulze* (o. Fußn. 16), § 2 Rdnr. 216; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 207.

27 Vgl. *Loewenheim* (o. Fußn. 16), § 2 Rdnr. 193; *Schulze* (o. Fußn. 16), § 2 Rdnr. 211, 139; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 207.

Auswahl der Kameraeinstellung und Beleuchtung erkennbar ist. Überdies ist jedes Standbild als Lichtbildwerk gem. § 2 Abs. 2 Nr. 5 UrhG geschützt,[28] nicht selbstständige Bildfolgen sind zumindest noch Laufbilder gem. § 95 UrhG.[29]

2. Urheberrechtsverletzungen durch Dateifragmente?

Für die Prüfung der Rechtsverletzungen ist zu differenzieren, und zwar je nach Verletzungshandlung und nach der Art der Dateifragmente. Als Verletzungshandlungen kommen der Download, also das Erstellen einer Kopie für eigene Zwecke, und der Upload, also das Zurverfügungstellen dieses Vervielfältigungsstückes, in Betracht.

a) Download: § 16 UrhG

Beim Download geht es um die Erstellung einer Kopie, sodass § 16 UrhG, das Vervielfältigungsrecht, betroffen ist. Fraglich ist, ob dieses bereits durch den fragmentarischen Download verletzt ist.

■ Schutzfähige Fragmente

Bei den schutzfähigen Fragmenten ist dies der Fall. Soweit diese einem urheberrechtlichen Schutz im Einzelfall tatsächlich zugänglich sind, liegt eine Verletzung des Vervielfältigungsrechts vor.

Eine Besonderheit gilt bezüglich der oben bereits angesprochenen offenen Charts-Container,[30] in denen mehrere Musikstücke oder Videos in Einzeldateien übertragen werden können. Bei diesen besteht die Möglichkeit eines urheberrechtlichen Schutzes der einzelnen Dateien und ggf. ihrer Fragmente. Urheberrechtsverletzungen müssen hier für jede Datei des Containers, also für jedes Musikstück oder ggf. Video, separat geprüft werden, sodass eine Verletzung des § 16 UrhG nur dann vorliegt, wenn ein schutzfähiges Fragment der konkreten Datei bereits heruntergeladen wurde.

■ Nicht schutzfähige Fragmente

Soweit es hingegen um Fragmente geht, die dem Urheberschutz nicht zugänglich sind, kommt eine Urheberrechtsverletzung erst dann in Betracht, wenn das Werk komplett heruntergeladen wurde. Der bloße Download von Teilen, die selbstständig keinem urheberrechtlichen Schutz unterfallen, kann kein Verstoß gegen Urheberrechte darstellen – nutzlos = schutzlos. In diese Gruppe fallen auch die geschlossenen Charts-Container in Form von Archivdateien.

■ Fragmente, die mit Hilfsprogrammen genutzt werden können

Zuletzt stellt sich die Frage, wie solche Fragmente zu bewerten sind, die nur durch den Einsatz von spezieller Software bereits in ihrer fragmentarischen Form abspielbar gemacht werden können. Der Fall ist mit der Umgehung sog. „Geo-Sperren" vergleichbar. Dabei werden im Internet gesendete TV-Streams mittels technischer Sperren nur den Nutzern aus einem bestimmten Land oder einer bestimmten Region freigegeben.[31] Diese Sperren können mit mehr oder weniger großem technischen Aufwand umgangen werden.[32]

Mitsdörffer/Gutfleisch kommen zu dem Ergebnis, dass bei Umgehung derartiger Schutzmechaniken tatbestandlich eine Vervielfältigung gem. § 16 UrhG vorliegt, diese aber durch die Schranke des § 53 Abs. 1 Satz 1 UrhG gedeckt ist, weil die Quelle rechtmäßig ins Internet gestellt wurde.[33] Das ist beim Filesharing anders, da die h.M. hier von einer „offensichtlich rechtswidrig öffentlich zugänglich gemachten Vorlage" i.S.d. § 53 Abs. 1 Satz 1 a.E. ausgeht.[34] Auch andere Schranken greifen wegen des Ausschlusses digitaler Nutzung bei der Privatkopierfreiheit gem. § 53 Abs. 2 Satz 3 nicht ein.[35] Somit sind die Fragmente, die mittels Hilfsprogrammen nutzbar gemacht werden können, im Ergebnis den schutzfähigen Fragmenten gleichgestellt, sofern gleichzeitig nachgewiesen wird, dass Software zum Einsatz kommt, mit der die Fragmente genutzt werden können.

b) Upload: § 19a

Indem der Tauschbörsennutzer eine Datei herunterlädt, hält er diese automatisch, zumindest bis der Download abgeschlossen ist,[36] anderen Nutzern zum Upload bereit. Darin kann ein öffentliches Zugänglichmachen gem. § 19a UrhG liegen.

■ Schutzfähige Fragmente

Bei schutzfähigen Fragmenten liegt bereits dann eine öffentliche Zugänglichmachung i.S.d. § 19a UrhG vor, wenn die Dateifragmente, während der Tauschbörsennutzer selbst noch lediglich herunterlädt, bereits wieder abrufbar sind.

Hinsichtlich der offenen Charts-Container gilt wieder, dass für jede Datei des Containers der mögliche Verstoß gegen § 19a UrhG separat geprüft werden muss. Es muss also ein schutzfähiges Fragment des konkreten Musikstücks vorliegen.

■ Nicht schutzfähige Fragmente

Soweit nur Fragmente zur Verfügung gestellt werden, die als solche dem Urheberschutz nicht zugänglich sind, liegt im unvollständigen Angebot eines Teils keine öffentliche Zugänglichmachung eines Werks. Eine Verletzung von § 19a UrhG kommt erst in Betracht, wenn der Nutzer die Datei vollständig auf seinem Rechner hat. Dann genügt selbstverständlich die bloße Möglichkeit, dass die Datei hochgeladen werden könnte, ein tatsächlicher Upload ist nicht erforderlich.[37]

■ Abweichende Beurteilung auf Grund der Struktur der Tauschbörsen?

Fraglich ist, ob auf Grund der Struktur der Tauschbörsen eine andere Beurteilung geboten ist. Denn für Dritte, die auf das für sich genommen unnütze, nicht schutzfähige Fragment zugreifen, ist dieses gar nicht so nutzlos, weil aus Hunderten anderer Quellen Zugriff auf die anderen Fragmente möglich ist. Beispiel: Ein Musikstück besteht aus 100 Dateifragmenten. 100 Nutzer haben jeweils genau ein verschiedenes Segment.

Hier könnten am Ende alle 100 Nutzer die vollständige Datei haben, ohne dass bis um Zeitpunkt der Beendigung des Downloads eine einzige Urheberrechtsverletzung begangen wurde. Aus der Gesamtschau betrachtet ist also das einzelne Fragment zumindest aus der Sicht eines Dritten gar nicht so nutzlos wie bei isolierter Betrachtung.

---

28 Vgl. *Schulze* (o. Fußn. 16), § 2 Rdnr. 213.
29 Vgl. *Schulze* (o. Fußn. 16), § 2 Rdnr. 212; *A. Nordemann* (o. Fußn. 16), § 2 Rdnr. 209.
30 S.o. II.2.
31 Vgl. *Mitsdörffer/Gutfleisch*, MMR 2009, 731.
32 Vgl. *Mitsdörffer/Gutfleisch*, MMR 2009, 731, 732.
33 Vgl. *Mitsdörffer/Gutfleisch*, MMR 2009, 731, 733 f.
34 Vgl. *Loewenheim* (o. Fußn. 16), § 53 Rdnr. 24; *Lüft*, in: Wandtke/Bullinger (o. Fußn. 16), § 53 Rdnr. 16; *Dreier*, in: Dreier/Schulze (o. Fußn. 16), § 53 Rdnr. 11 f.; BT-Drs. 16/1828, S. 26.
35 Vgl. *Loewenheim* (o. Fußn. 16), § 53 Rdnr. 54; *Lüft* (o. Fußn. 34), § 53 Rdnr. 33; *Dreier* (o. Fußn. 34), § 53 Rdnr. 35; *W. Nordemann*, in: Fromm/Nordemann (o. Fußn. 16), § 53 Rdnr. 27.
36 Viele Tauschbörsenprogramme ermöglichen, Dateien nach Beendigung des Downloads sofort automatisch in andere Ordner zu verschieben, wodurch diese nicht mehr für andere zugänglich sind. Während des Downloads lässt sich bei den meisten Programmen der Upload nicht unterbinden.
37 Vgl. *Dreier* (o. Fußn. 34), § 19a Rdnr. 6 a.E.

Das darf aber an der urheberrechtlichen Beurteilung nichts ändern. Denn hier geht es letztlich um Täterschaft. Würde man eine Gesamtbetrachtung vornehmen, liefe das darauf hinaus, auf Tatbestandsseite die Handlungen von vollkommen fremden Dritten zuzurechnen. Eine solche Zurechnung fremden Handelns erfolgt auch sonst nur bei mittäterschaftlicher Begehung, wenn also eine Verbundenheit zwischen den Tätern und Handeln auf Grund eines gemeinsamen Tatentschlusses und -plans vorliegen. Dazu ist entsprechender Vorsatz erforderlich,[38] fahrlässige Mittäterschaft ist ausgeschlossen.[39] Tauschbörsennutzer kennen einander aber nicht, gerade die Anonymität ist prägend für das Wesen der Tauschbörsen. Bereits daran scheitert ein gemeinsamer Tatentschluss und somit der Vorsatz, denn für den gemeinsamen Tatplan ist ein gegenseitiges Einvernehmen erforderlich.[40] Zudem ist vielen Nutzern nicht klar, dass sie gleichzeitig mit dem Download den Upload ermöglichen – das fehlende kognitive Element schließt ebenfalls den Vorsatz aus. Damit liegt lediglich Nebentäterschaft vor, bei der es für eine Rechtsverletzung erforderlich ist, dass jeder Täter selbstständig alle gesetzlichen Merkmale erfüllt.[41] Dies ist aber wie oben ausgeführt auf Grund der fehlenden Schutzfähigkeit der Fragmente nicht der Fall.

Das ist auch richtig, denn der Tatbestand des § 19a UrhG ist in gewisser Weise Spiegelbild der Vervielfältigung nach § 16 UrhG. Im Beispiel begehen die 100 Nutzer erst im Moment des Abschlusses des Downloads eine Urheberrechtsverletzung. Erst dann liegt eine Vervielfältigung gem. § 16 UrhG und ab diesem Zeitpunkt eine öffentliche Zugänglichmachung nach § 19a UrhG vor.

■ Fragmente, die mit Hilfsprogrammen genutzt werden können

Anders als beim Download verhält es sich hingegen mit den Fragmenten, die mittels spezieller Software nutzbar gemacht werden können. Denn die Nutzung dieser Fragmente erfordert ein aktives Einschreiten des Nutzers „am anderen Ende", also ein vorsätzliches deliktisches Handeln. Dieses lässt auch sonst in der Regel einen Zurechnungszusammenhang entfallen.[42] Sonst müsste auch ein Anbieter von verschlüsseltem Pay-TV gegenüber dem Urheber, der nur der verschlüsselten Sendung zugestimmt hat, aus §§ 97, 19a UrhG haften, wenn die Verschlüsselung durch Dritte „geknackt" wird. Diese Gesichtspunkte müssen hier ebenfalls gelten, sodass Anbieter von an sich nutzlosen Fragmenten, die nur mittels Hilfsprogrammen abgespielt werden können, noch keine öffentliche Zugänglichmachung eines geschützten Werks begehen.

IV. Auswirkungen auf die Praxis

1. Anspruch aus § 97 Abs. 1 UrhG auf Unterlassung

Der Unterlassungsanspruch nach § 97 setzt eine Urheberrechtsverletzung voraus. Daraus folgt, dass auf Grund von nicht schutzfähigen Fragmenten nicht abgemahnt werden kann. Denn soweit die Abmahnung Dateien betrifft, die als Fragmente dem Urheberschutz nicht zugänglich sind, ist eine Urheberrechtsverletzung nur denkbar, wenn der Nutzer die fragliche Datei vollständig auf seinem Rechner hat.

Anderes kann nur gelten, wenn nach der obigen Untersuchung ein schutzfähiges Fragment vorliegt. Hier ist § 97 UrhG anwendbar, wobei für die Wiederholungsgefahr ein Verstoß gegen § 19a UrhG zu fordern ist, weil eine Wiederholung des Verstoßes gegen das Vervielfältigungsrecht nicht mehr droht, wenn der Nutzer das Werk vollständig heruntergeladen hat.

2. Anspruch aus § 97 Abs. 2 UrhG auf Schadensersatz

Der Anspruch aus § 97 Abs. 2 UrhG auf Schadensersatz setzt neben einer Urheberrechtsverletzung Verschulden voraus, welches jedoch, zumindest solange der Abgemahnte selbst die Urheberrechtsverletzung durch eigenes Tun begangen hat, in Form von bedingtem Vorsatz, jedenfalls aber Fahrlässigkeit, vorliegen wird.

Als Rechtsfolge sieht § 97 Abs. 2 UrhG die dreifache Schadensberechnung vor. In der Praxis spielt nur die Lizenzentschädigung eine Rolle. Hierbei werden teils erhebliche Beträge angesetzt. Diese sind aber nur gerechtfertigt, soweit die Abmahnung auf § 19a UrhG gestützt wird, da dann eine Art „Sendelizenz" berechnet wird. Wenn nur Fragmente von solchen Dateien, die nur mittels technischer Hilfsprogramme nutzbar gemacht werden können, beim Abgemahnten nachgewiesen werden, ist oben der Tatbestand des § 19a UrhG verneint worden. In diesen Fällen kann die Lizenzanalogie nur auf die Vervielfältigung nach § 16 UrhG gestützt werden – das dürfte dann den Ladenpreis der CD oder den Preis des legalen Downloads bei *iTunes* oder *amazon* – ggf. zuzüglich eines moderaten Strafzuschlags – nicht überschreiten. Tatsächlich müsste dieser Preis sogar unterschritten werden, da ein Teilstück weniger wert ist als die gesamte Datei. Es darf nicht verkannt werden, dass die Lizenzanalogie keinen „Strafschadensersatz" darstellen darf – auch wenn das in der Praxis manchmal kaum zu unterscheiden ist.

3. Auswirkungen auf die Beweisführung

a) Maßstab

Die differenzierte Betrachtungsweise hat insbesondere Auswirkungen auf die Beweislast. Bisher war es in den urheberrechtlichen Rechtsstreitigkeiten so, dass von der Content-Industrie nur nachgewiesen wurde, dass ein als Ganzes urheberrechtlich geschütztes Werk in irgendeiner Form angeboten wurde. Die Frage, ob die Datei zu diesem Zeitpunkt vollständig war oder ob bei einem Fragment dieses für sich genommen urheberrechtsfähig war, wurde vollkommen übergangen. Damit ist bislang der eigentliche Tatbestand der Urheberrechtsverletzung nicht nachgewiesen worden.

Das kann nicht sein. Wer abmahnt und klagt, muss darlegen und beweisen, dass eine Urheberrechtsverletzung vorliegt. Für Beweiserleichterungen ist an dieser Stelle kein Raum. Auch im Urheberrecht gilt, dass der Anspruchsteller grundsätzlich alle Tatbestandsmerkmale der Anspruchsnorm darlegen und beweisen muss.

b) Folge

Der Abmahner muss daher bei den Dateien, die in Fragmenten nutzlos sind, beweisen, dass die Datei beim Abgemahnten vollständig heruntergeladen bzw. vollständig angeboten wurde. Der bloße Nachweis, dass über einen Zeitraum von 5 Minuten irgendein Down- oder Upload im Gange war, wie es derzeit der gängigen Praxis entspricht, reicht nicht aus.

Bei Dateien, die fragmentarisch theoretisch nutzbar sein könnten, muss dargelegt und bewiesen werden, dass das konkret

38 Vgl. *Kudlich*, in: BeckOK-StGB, 14. EL 2011, § 25 Rdnr. 48 ff.; *Kühl*, in: Lackner/Kühl, StGB, 27. Aufl. 2011, § 25 Rdnr. 9; *Fischer*, StGB, 56. Aufl. 2009, § 25 Rdnr. 22.

39 Vgl. *Kudlich* (o. Fußn. 38), § 25 Rdnr. 57; *Kühl* (o. Fußn. 38), § 25 Rdnr. 13; *Fischer* (o. Fußn. 38), § 25 Rdnr. 25.

40 Vgl. *Kühl* (o. Fußn. 38), § 25 Rdnr. 9.

41 Vgl. *Fischer* (o. Fußn. 38), § 25 Rdnr. 27.

42 Vgl. *Fischer* (o. Fußn. 38), vor § 13 Rdnr. 27; *Heinrichs*, in: Palandt, BGB, 70. Aufl. 2011, vor § 249 Rdnr. 73, 76.

beim Nutzer vorhandene Fragment im Zeitpunkt der Abmahnung urheberrechtlich schutzfähig war. Da die Abmahnenden nicht wissen können, welche konkreten Fragmente einer Datei bereits heruntergeladen wurden und ob bei Musikdateien die Melodie dabei war, darf entweder nur abgemahnt werden, wenn der Nachweis erbracht wird, dass der Download abgeschlossen wurde, oder wenn irgendwie in lückenloser Dokumentation der Nachweis erbracht wird, dass ein schutzfähiges Werkstück vorlag – wie auch immer das möglich sein soll.

Besonderheiten müssen wieder bei den Charts-Containern[43] gelten: Bei geschlossenen Containern (Archivdateien) muss zwingend der Nachweis geführt werden, dass der Download zu 100% abgeschlossen ist, da zuvor technisch bedingt kein dem Urheberrecht zugänglicher Teil vorliegt. Bei den offenen Containern (*BitTorrent*) ist der Nachweis zu führen, dass ein schutzfähiger Teil des konkreten Musikstücks, auf Grund dessen abgemahnt wird, vorhanden ist.

Alle Nachweise sind bereits im gerichtlichen Verfahren betreffend den Auskunftsanspruch nach § 101 Abs. 2 Nr. 3 UrhG gegen den jeweiligen Internetprovider zu erbringen, da es ansonsten am Merkmal der „offensichtlichen Rechtsverletzung" fehlt.[44] Das wird auf Grund der derzeitigen Technik den Nachweis darüber erfordern, dass der Download zu 100% abgeschlossen wurde, da es nicht möglich ist nachzuweisen, welche einzelnen Dateien aus einem offenen Container geladen wurden und welche nicht. Da es bei offenen Containern keine Vermutung gibt, dass jemand wirklich alle Musikstücke haben möchte – im Gegenteil ist wahrscheinlich, dass Stücke, die der Nutzer nicht mag oder kennt, nicht geladen werden –, sind Beweiserleichterungen an dieser Stelle in besonderem Maße abzulehnen.

Im Prozess muss ein einfaches Bestreiten des Abgemahnten, er habe den Download nie beendet, ausreichen, um Ansprüche abzuwehren, wenn nicht ein lückenloser Beweis geführt werden kann, dass der Download abgeschlossen oder das Fragment schutzfähig war.

4. Auswirkungen auf den Streitwert

Bereits die Frage, ob wegen eines Fragments oder wegen des gesamten Werks abgemahnt wird, muss sich auf den Streitwert auswirken. Nicht zuletzt auf Grund der (zu) hohen Streitwerte und den daraus resultierenden Gerichts- und Anwaltskosten werden Massenabmahnungen in der Gesellschaft immer wieder kontrovers diskutiert. *Haedicke* spricht von „struktureller Überlegenheit der Rechteinhaber", da die Kosten im Falle einer Niederlage manchen Abgemahnten von der Verteidigung abhalten.[45]

Wenn nur wegen eines Fragments abgemahnt wird, muss der Streitwert reduziert werden, da das Teilstück schlicht weniger wert ist. Eine Höhe von maximal bis zu 50% des üblichen Streitwerts erscheint angemessen.

Außerdem ist beim Streitwert zu berücksichtigen, welcher Verstoß abgemahnt wird: Geht es ausnahmsweise nur um § 16 UrhG (oder ist die Abmahnung nur insofern begründet), muss der Streitwert niedriger sein als im Fall des § 19a UrhG, da dort intensiver in Urheberrechte eingegriffen und ein potenziell höherer Schaden hervorgerufen wird.

V. Resümee/Ausblick

Bislang wird von den Abmahnern nur ein Downloadvorgang nachgewiesen. Die Rechtsprechung hat dies bislang für ausreichend befunden. Dabei wird nicht nachgewiesen, ob auf der Festplatte des Abgemahnten ein dem Urheberschutz zugängliches Fragment vorhanden ist – ganz zu schweigen von einem Nachweis, welche Dateien aus einem offenen Container geladen wurden und ob deren Fragmente im Zeitpunkt der Abmahnung schutzfähig waren. Es fehlt also in allen derzeit anhängigen Verfahren am Nachweis der eigentlichen Urheberrechtsverletzung.

So ist eine sehr urheberfreundliche Rechtsprechung entstanden, die gegenüber Tauschbörsennutzern streng ist, frei nach dem Motto: „Es trifft immer den Richtigen". Zwar mag der Verdacht naheliegen, dass jemand, der eine Tauschbörse nutzt und bei dem der Download eines urheberrechtlich geschützten Werks im Gange ist, diesen Download zu Ende bringen und spätestens dann eine Urheberrechtsverletzung begehen wird. Eine dahingehende rechtliche Vermutung gibt es aber nicht, denn der Download kann jederzeit vom Nutzer abgebrochen werden – sei es, weil die Internetverbindung freiwillig oder unfreiwillig getrennt oder der Nutzer sich seines Unrechts bewusst wird.

Bereits heute wird im Filesharing-Bereich hinsichtlich der Frage nach der Täterschaft vom Beweissystem der ZPO abgewichen – davon zeugt die Rechtsprechung des *BGH* zur sekundären Darlegungslast nach dem „Sommer unseres Lebens"-Urteil.[46] Immer wieder gefordert und teils unter Verweis auf vereinzelt gebliebene untergerichtliche Rechtsprechung aus der Zeit vor dem „Sommer unseres Lebens"-Urteil bis heute in Abmahnschriftsätzen behauptet wird diesbezüglich sogar ein Anscheinsbeweis.[47] Auch bei der Anwendung des § 97a Abs. 2 UrhG, mit dem der Gesetzgeber einen Ausgleich zwischen den Interessen der Content-Industrie und den Abgemahnten schaffen wollte, ist die Rechtsprechung sehr zurückhaltend und damit urheberfreundlich (oder doch nur anwaltsfreundlich?).[48]

Es ist nicht einzusehen, warum man auf Tatbestandsseite ebenfalls freigiebig sein sollte. Deshalb ist kein Anscheinsbeweis dahingehend, dass jemand, der einen möglicherweise illegalen Download beginnt, diesen beendet, statthaft. Eine dahingehende Vermutung, die zu einer sekundären Darlegungslast führt, besteht ebenfalls nicht.

Die vorstehende Untersuchung zeigt vielmehr, dass (weitere) Beweiserleichterungen zu Gunsten der Content-Industrie nicht angezeigt sind. Zumindest besteht kein Grund dafür, dass neben der Täterschaft noch die Tatbestandsmäßigkeit der möglichen Rechtsverstöße irgendwie vermutet oder fingiert wird. Die ZPO verlangt, dass der Anspruchsteller darlegt und beweist, dass eine Urheberrechtsverletzung vorliegt. Dafür ist es erforderlich, dass nachgewiesen wird, dass sich in dem Moment, auf den sich die Abmahnung bezieht, ein dem Urheberschutz zugängliches Fragment auf dem Computer des Abgemahnten befunden hat – und, bei den offenen Charts-Containern: dass ein solches dem Urheberschutz zugängliches Fragment des konkret abgemahnten Musikstücks im Abmahnzeitpunkt vorhanden war.

Bei aller Sympathie für die Rechte der Urheber und die Verluste der Content-Industrie durch Urheberrechtsverletzungen bleibt zu hoffen, dass die Rechtsprechung in Zukunft etwas genauer hinsieht. Für Urheber und Leistungsschutzberechtigte müssen dieselben Beweisregeln gelten wie für jeden anderen. Es ist nicht angezeigt, aus normativen Gründen hiervon abzuweichen, weil es sich bei den Abgemahnten häufig um „Rechtsbrecher" han-

---

43 S.o. II.2.

44 So auch *Wick* (o. Fußn. 15), S. 42 f.

45 Vgl. *Haedicke* (o. Fußn. 3), S. 21 f.

46 Vgl. *BGH* MMR 2010, 565 m. Anm. *Mantz* – Sommer unseres Lebens.

47 Vgl. *AG Frankfurt/M.* MMR 2010, 263 (Ls.); unklar *OLG Köln* MMR 2010, 281, 283 m. Anm. *Solmecke/Kalberg*, das nicht erkennbar zwischen Anscheinsbeweis und sekundärer Darlegungslast differenziert.

48 Für die Anwendung von § 97a Abs. 2 UrhG in Filesharing-Fällen vgl. *Hoeren* (o. Fußn. 15), S. 380 f. sowie speziell für Massenabmahnungen *Ewert/v. Hartz*, MMR 2009, 84, 87; vgl. auch *Haedicke* (o. Fußn. 3), S. 22 ff.

delt. Deshalb dürfen die berechtigten Ansprüche der Urheber durch Beweiserleichterungen, überhöhte Streitwerte und überzogene Schadensersatzforderungen[49] nicht zu dem deutschen Recht fremden Bestrafungsmitteln werden. Damit würde auch dem Ansehen des Urheberrechts in der Öffentlichkeit weiter geschadet.[50] Im Übrigen nähme man Nutzern die Möglichkeit, durch Abbruch des Downloads i.S.d. § 24 Abs. 1 1. Var. StGB zurückzutreten.

49 Vgl. *Haedicke* (o. Fußn. 3), S. 163.
50 Vgl. *Haedicke* (o. Fußn. 3), S. 10 f., 13 ff., 162 ff.


Christian Solmecke, LL.M.
ist Rechtsanwalt und Partner der Kölner Medienrechtskanzlei Wilde Beuger Solmecke.


Dr. Jan Bärenfänger
ist Rechtsreferendar im Landgerichtsbezirk Münster.

PATRICK BREYER

(Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung

Grenzen des Rechts auf Anonymität

Telekommunikations- und Medienrecht

Dürfen Anbieter von Internetzugängen ohne Anlass und flächendeckend auf Vorrat protokollieren, welcher ihrer Kunden wann unter welcher Kennung (IP-Adresse) das Internet genutzt hat? Der Verfasser untersucht die gesetzlichen, verfassungsrechtlichen und europarechtlichen Grenzen des Rechts auf Anonymität im Internet.

I. Einleitung

Der *BGH* hatte am 13.1.2011 erstmals über die Klage eines Internetnutzers gegen einen Internet-Zugangsanbieter (*Deutsche Telekom AG*) auf Löschung der jeweils zur Nutzung zugewiesenen Internetkennung zu entscheiden.[1] Die Entscheidung könnte man mit Fug und Recht mit „Vorratsdatenspeicherung II" betiteln, geht sie doch in entscheidenden Punkten über die Grenzen hinaus, die das *BVerfG* am 2.3.2010 einer Vorratsdatenspeicherung gezogen hatte:[2] Der *BGH* hält eine Vorratsspeicherung von Internetverbindungsdaten nun nicht mehr nur für Zugriffe öffentlicher Strafverfolgungs- und Gefahrenabwehrbehörden für verfassungsmäßig, sondern schon zur Nutzung durch private TK-Unternehmen für deren eigenen Bedarf. Diese Auffassung stellt das „Recht des Internetnutzers auf Anonymität"[3] im Verhältnis zu seinem Internet-Zugangsanbieter, zu öffentlichen Stellen (§ 113 TKG) und zu privaten Urhebern (§ 101 UrhG) grundlegend in Frage und macht eine nähere Untersuchung der Rechtslage erforderlich.

II. Bedeutung von Internetkennungen (IP-Adressen)

Zur Fernkommunikation per Internet wie auch per Telefon bedarf es aus technischen Gründen einer eindeutigen Kennung der Kommunikationspartner. Während z.B. ein persönliches Gespräch auf der Straße, der Kauf einer Zeitung oder der Empfang von Rundfunk keine Identifizierung der Beteiligten erfordert, erfordern vergleichbare Tätigkeiten im Internet die Bekanntgabe einer eindeutigen Kennziffer (IP-Adresse) des Teilnehmers an den Kommunikationspartner. Anders als bei Telefonnummern lässt sich die Übermittlung solcher Internetkennungen an den Empfänger nicht unterdrücken.

Anbieter von Internetdiensten wie dem *T-Online-Portal*, dem Marktplatz *eBay* oder dem E-Mail-Dienst *web.de* protokollieren nun regelmäßig unter Verstoß gegen § 15 TMG[4] oder außerhalb dessen territorialen Anwendungsbereichs jede Eingabe und jeden Klick im Internet mitsamt der Internetkennung des jeweiligen Nutzers. Die Anonymität der Internetkennung entscheidet deshalb regelmäßig darüber, ob Strafverfolgungsbehörden, Gefahrenabwehrbehörden, Nachrichtendienste und Urheberrechtsinhaber die Internetnutzung einer Person rekonstruieren und zum Anlass für Abmahnungen, Ermittlungen (z.B. Hausdurchsuchung) und sonstige Eingriffe nehmen können, welche schwere Nachteile auch für unschuldig Verdächtigte nach sich ziehen können. Die Anonymität der Internetadresse als Schlüssel zu Internet-Nutzungsprotokollen hängt davon ab, ob es Internet-Zugangsanbietern erlaubt ist, jede Internetverbindung samt der dem Teilnehmer zur Internetnutzung zugewiesenen Kennung zu protokollieren.

III. Löschungspflicht (§ 96 TKG)

Die dem TK-Anbieter bei seiner Tätigkeit bekannt gewordene Information, wer wann unter welcher IP-Adresse mit dem Internet verbunden ist oder war, ist als TK-Verkehrsdatum einzuordnen (§ 3 Nr. 30 TKG).[5] Es handelt sich zugleich um einen näheren Umstand der Telekommunikation, der den Schutz des verfassungsrechtlichen (Art. 10 GG) und des einfachgesetzlichen (§ 88 TKG) Fernmeldegeheimnisses genießt.[6]

Ein TK-Anbieter hat Verkehrsdaten nach § 96 Abs. 2 Satz 2 TKG grundsätzlich sofort[7] mit Verbindungsende zu löschen, wenn er

1 *BGH* MMR 2011, 341 m. Anm. *Karg*.
2 *BVerfG* MMR 2010, 356 m. Anm. *Bär*.
3 *BGH* MMR 2009, 608 m. Anm. *Greve/Schärdel*.
4 *Breyer*, NJW-aktuell 11/2010, 18.
5 *BGH* (o. Fußn. 1), Rdnr. 28.
6 *BGH* (o. Fußn. 1), Rdnr. 32.
7 *BGH* (o. Fußn. 1), Rdnr. 15.