

Auszug aus

## **Überspannte Prüfpflichten für Host-Provider trotz BGH Internetversteigerung II? Vorschlag für eine Haftungsmatrix.**

NJW 2008, S. 1415

### **Einleitung**

Eine Vielzahl verschiedener landgerichtlicher Urteile zur Haftung von Providern<sup>1</sup> haben die Frage aufgeworfen, ob die Anforderungen an Prüfpflichten von Host-Providern nicht massiv überspannt werden. Erstmals wurde in einem Urteil sogar die Einstellung des Geschäftsbetriebs bei vermuteter umfangreicher rechtswidriger Nutzung eines Systems als zumutbar erachtet<sup>2</sup>. Der BGH hatte in seinem Urteil „Internetversteigerung II“<sup>3</sup> die Kriterien der Störerhaftung bei Onlineauktionen konkretisiert und bestätigt, dass Host-Provider der Störerhaftung unterliegen. Was dies jedoch im Einzelnen heißt, hängt im Wesentlichen davon ab, welche Verantwortung dem Provider aufgrund seines technischen Systems sowie der Rolle der speichernden Dritten und der abrufenden Dritten zuzuweisen ist<sup>4</sup>. Im Folgenden sollen daher zunächst die Arbeitsweise der gängigsten technischen Systeme dargestellt werden, um eine rechtliche Einordnung der Haftungskriterien aufzuzeigen. Der Schwerpunkt wird hierbei auf den Host-Provider-Systemen liegen, die im Fokus der „Web 2.0“-Diskussion stehen.

### **I. Technische Fragen der Speicherung und/oder Verwaltung fremder Inhalte im Internet / Web 2.0**

Unter dem schlagwortartig verwendeten Mode-Stichwort „Web 2.0“ wird – inhaltlich unscharf - vor allem verstanden, dass abrufbare Inhalte vorrangig von den Nutzern des Internet und nicht mehr von zentralen Content-Anbietern stammen, unabhängig davon, wo sie gespeichert und wie sie abzurufen sind.

<sup>1</sup> So zuletzt LG München I, Urt. V. 19.04.2007, Az.: 7 O 3950/07 (Usenet); OLG Köln (Urt. V. 21.03.2007, Az.: 28 O 19/07); LG Düsseldorf, Urt. v. 23.01.2008, Az.: 12 O 246/07 (GEMA); abgrenzend für Usenet-Anbieter OLG Düsseldorf, Urt. v. 15.01.2008, Az.: I-20 U 95/07

<sup>2</sup> LG Düsseldorf, Urt. v. 23.01.2008, Az.: 12 O 246/07 (GEMA) für Sharehoster.

<sup>3</sup> BGH GRUR 2007, S. 708 (Internetversteigerung II)

<sup>4</sup> S. Rössel / Kruse, Schadensersatzhaftung bei Verletzung von Verkehrspflichten, CR 2008, S. 35ff.

## 1) Providerbegriff im Allgemeinen

Nutzerinhalte können auf serverbasierten „Host-Provider“-Systemen gespeichert sein, die die Inhalte auflisten und für alle Nutzer zur Verfügung stellen (wie bei Auktionshäusern), sie kann aber auch unter den Internet-Nutzern verteilt werden, die lediglich über eine Austauschsoftware kommunizieren (Peer-to-Peer-System). Weiter gibt es Zugriffs- und Speichersysteme, die teilweise nur speichern, nicht aber Inhalte auflisten und freie Zugriffe Dritter erlauben (Share-Hoster), teilweise nichts selbst speichern, sondern nur auflisten, welche Inhalte bei Dritten abrufbar sind („Nur-Lister“). Im Folgenden soll die Situation im Umfeld der Host-Provider dargestellt werden, da diese im Zentrum der aktuellen Rechtsprechung zur Störerhaftung, insbesondere der Urteile zum Sharehosting stehen<sup>5</sup>.

## 2) Systeme zur Speicherung und zum Abruf fremder Inhalte im Internet

### a) Speicherung der Nutzerinhalte auf Servern der Host-Provider: Beispiel Online-Auktionshäuser, Forenanbieter

Beim klassischen Server-Hosting stellt der Provider einen Rechner zur Verfügung, auf dem von den registrierten Kunden Dateien abgelegt und von allen Internet-Nutzern wieder abgerufen werden können (Client-Server-Modell). Auktionshäuser wie ebay und ricardo bieten ihren Nutzern entsprechenden Speicherplatz auf der jeweiligen Anbieter-Auktionsseite an. Eine Änderung der gespeicherten Inhalte ist nur unter bestimmten Voraussetzungen möglich. Es steht den Nutzern daher nicht mehr völlig frei, über ihre Inhalte so zu verfügen, als ob sie auf eigenen Rechnern gespeichert wären.<sup>6</sup>

### b) Speicherung der Nutzerinhalte dezentral auf den Rechnern der Nutzer (Peer-to-Peer-Systeme)

Beim Filesharing, etwa beim früheren „Napster“-Musiktauschsystem, werden die Inhalte nicht auf einem zentralen Server gespeichert, sondern auf den Rechnern der sich jeweils online befindenden Benutzer. Diese werden lediglich über eine Software zu einem Netz zusammengeschlossen.

Ein Kunde kann in der zentralen System-Liste sehen, welche anderen Kunden, die gerade online sind, auf ihrem Rechner eine gesuchte Datei anbieten und es herunterladen. Gleichzeitig können – solange er selbst online ist – alle anderen Kunden die auf dem Rechner des Kunden bereit gestellten eigenen Dateien auffinden und herunterladen. Beispiele für Filesharing-Systeme sind Bit Torrent, eDonkey, Kademia (Azureus, eMule), Gnutella (LimeWire, Bearshare) oder FastTrack (Kazaa Lite K++).

### c) Speicherung der Nutzerinhalte ohne jede Listung von Inhalten und Zugriffsmöglichkeit für Dritte (Sharehoster)

---

<sup>5</sup> Zugangsprovider werden regelmäßig nicht als Störer oder als Teilnehmer einer Rechtsverletzung zu qualifizieren sein, siehe LG Kiel, Urt. V. 23.11.2007, Az.: 14 O 125/07; LG FFM, Urt. v. 05.12.2007, Az.: 2-03 O 526/07

<sup>6</sup> Dennoch wird auch bei Client-Server-basierten Providersystemen von einer fehlenden Prüfpflicht nach dem früheren TDG (und jetzigen TMG) ausgegangen, s. Volkmann, Der Störer im Internet, München 2005, S. 77)

Bei „Sharehostern“ kann der Kunde das System des Providers als externen Speicher nutzen.

Werden – wie etwa bei Systemen wie „Rapidshare“ oder „Sendmefile“ – keine Listing-Möglichkeiten angeboten, hängt es alleine von der Initiative der speichernden Nutzer ab, ob und wie leicht Dritte auf den Servern der Provider gespeicherte Inhalte abrufen können.

Welche Daten vom Kunden des Systems eingegeben werden, entzieht sich somit grundsätzlich der Kenntnis des Anbieters, da vom Kunden keinerlei zutreffende Qualifikation der Dateien erfolgen muss. Es bleibt dem Kunden überlassen, welchen Titel er seiner Datei gibt, in welchem Format es gespeichert wird und wem er es durch Weitergabe des Links wieder zugänglich macht. Der Sharehoster selbst hat keinen freien Zugriff auf und keine generelle Einsichtnahmemöglichkeit in die bei ihm gespeicherten Dateien.

#### **d) Sonderfall: Keine Speicherung von Nutzerinhalten, aber Zugang zu fremdgespeicherten Inhalten (Nur-Lister)**

Sogenannte „Nur-Lister“ bieten Link-Listen zu Dateien, die bei Host-Providern, meist bei Sharehostern, gespeichert sind. Sie machen damit (wie im Fall des OLG Köln und LG Düsseldorf<sup>7</sup>) fremde Speichersysteme durch eine eigene Such-Plattform überhaupt erst Dritten zugänglich. Dies setzt voraus, dass die Kunden der Sharehoster die Datei-Links entsprechend bei den „Nur-Listern“ verlinkt und gekennzeichnet haben. Die „Nur-Lister“ ermöglichen es also Dritten überhaupt erst durch eine systematische Veröffentlichung der Links, auf die Inhalte der Sharehoster-Kunden zuzugreifen. Über den Link kann der Internetnutzer dann die bei einem beliebigen dritten Host-Provider gespeicherten Dateien aufrufen und herunterladen.

Hier kann eine Störerhaftung zwar nicht an eine Speicherung fremder rechtswidriger Inhalte anknüpfen. Wenn eine solche Suchplattform jedoch gezielt angeboten wird, um z.B. auf fremden Systemen gespeicherte Musik-Files zu finden, kann hier eine aktive mittelbare Störereigenschaft gegeben sein.

Die technische Arbeitsweise der einzelnen Systeme führt somit zu sehr unterschiedlichen Zugriffsmöglichkeiten auf fremde Inhalte, die im Folgenden bei der rechtlichen Einordnung entsprechend zu berücksichtigen sind.

## **II. Rechtliche Zuordnung der zivilrechtlichen Störer-Haftung**

Die Haftung der Host-Provider für rechtswidrige, bei diesen gespeicherte oder abrufbare Inhalte steht im Spannungsfeld zwischen der Haftungsbeschränkung nach dem Telemediengesetz und den

---

<sup>7</sup> OLG Köln (Urt. V. 21.03.2007, Az.: 28 O 19/07); LG Düsseldorf, Urt. v. 23.01.2008, Az.: 12 O 246/07 (GEMA).

vom BGH bekräftigten Grundsätzen der Störerhaftung. Als Anbieter von Telemedien nach § 1 Abs. 1 TMG sind sowohl Content-, Access-, als auch Host-Provider zu qualifizieren<sup>8</sup>.

## 1) Filterfunktion des TMG

Das Telemediengesetz legt für die hier zu betrachtenden Host-Provider in § 7 Abs. 2 S. 1 – wie zuvor TDG und MDStV – fest, dass Diensteanbieter im Sinne der §§ 8 bis 10 nicht verpflichtet sind, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Im Zuge der Einführung des TMG hat der Gesetzgeber darauf hingewiesen<sup>9</sup>, dass trotz der Unsicherheiten über die Haftung der Provider aufgrund des Internetversteigerung-Urteils des BGH aus dem Jahr 2004 bewusst keine Änderungen gegenüber den Haftungsregelungen des TDG und des MDStV vorgenommen, sondern diese inhaltsgleich implementiert wurden<sup>10</sup>. Dies ist insofern unverständlich, als die Reformüberlegungen auf EU-Ebene und die Kritik der betroffenen Verbände sehr wohl eine nähere Regelung oder Überarbeitung der Haftungsregelungen gerechtfertigt hätte<sup>11</sup>. Erwägungsgrund 50 der EU-Richtlinie 2000/31/EG („E-commerce-Richtlinie“) weist darüber hinaus darauf hin, dass eine übersichtliche und transparente Abgrenzung der Verantwortlichkeiten zwischen „Filterregelung“ und urheberrechtlichen Ansprüchen zu erfolgen habe.

## 2) Unmittelbare und Mittelbare Störerhaftung

Die Störerhaftung basiert auf einer analogen Anwendung der §§ 823, 1004 BGB, wonach jeder, der – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Gutes beiträgt, als Störer für eine Schutzrechtsverletzung in Anspruch genommen werden kann<sup>12</sup>.

Für die Beurteilung der mittelbaren Störerhaftung durch Host-Provider sind die Kategorien des „Täters“ oder „Teilnehmers“ einer Störung nicht zentral, da diese die Verantwortung des Inhalte selbst einstellenden Content-Providers als unmittelbarem Störer treffen. Entscheidend ist vielmehr die Frage, inwiefern Host-Provider, die regelmäßig keine positive Kenntnis von den eingestellten Inhalten haben, mittelbare Störer sein können.

Der BGH hat in seinen „Internetversteigerung I und II“-Entscheidungen offen gelassen, ob bei einer Verletzung von Prüfpflichten eine unmittelbare Teilnahme oder eine mittelbare Störerhaftung vorläge<sup>13</sup>.

---

<sup>8</sup> Wobei Access- Provider zusätzlich dem Telekommunikationsrecht unterfallen, Hoeren aaO, S. 805.

<sup>9</sup> BT-Drs. 556/06, S. 14f.

<sup>10</sup> Begründet wurde dies damit, dass vor einer voreiligen Änderung der Haftungsregelungen erst europäische Harmonisierungsbestrebungen abzuwarten seien. Insbesondere wird auf den Evaluierungsbericht zur E-Commerce-Richtlinie verwiesen, der bis Ende 2007 vorliegen und eine Studie zu Fragen der Verantwortlichkeit enthalten sollte, BT-Drs. 556/06, S. 14f.

<sup>11</sup> s.a. Hoeren, NJW 2007, S. 805.

<sup>12</sup> BGH GRUR 2004, S. 860, BGH GRUR 2007, S. 708.

<sup>13</sup> BGH Z 158, 236, 250, kritisch dazu OLG Hamburg a.a.O., S. 586.

Die mittelbare Störerhaftung kennt zwei Anknüpfungspunkte: Zum einen als aktives Verantwortungselement die willentliche adäquat kausale Herbeiführung der Störung oder als passives Verantwortungselement die Aufrechterhaltung der Verletzung, obwohl deren Verhinderung zumutbar war.

Allein in der Zur-Verfügung-Stellung von Speicherplatz liegt weder eine Täterschaft oder Teilnahme an einer Vervielfältigung oder einer öffentlichen Zugänglichmachung (19a UrhG)<sup>14</sup>.

Grundlage einer Verletzung von Prüfpflichten können entweder Vorinformationen über Verstöße sein, die dem Provider aus allgemeinen Quellen oder aus dem eigenen Geschäftsbetrieb bekannt sein müssen, oder Informationen über einen ersten Verstoß von Dritter Seite, etwa durch Beschwerden von Nutzern oder durch eine Abmahnung/Beschwerde eines Rechteinhabers. In diesen Fällen wird die Prüfpflicht des Providers ausgelöst<sup>15</sup>, soweit sie zumutbar ist.

Zentrale Frage der mittelbaren Störerhaftung ist somit die Zumutbarkeit der Prüfung auf Vorliegen einer Störung. Der Umfang bestimmt sich danach, „ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist“<sup>16</sup>. Der BGH ging in seinen Entscheidungen „Internetversteigerung I“ und „Internetversteigerung II“ davon aus, dass etwa bei einem Online-Auktionshaus die Anwendung einer Filtersoftware mit anschließender manueller Prüfung von Verdachtsfällen genüge, um den Prüfpflichten im Hinblick auf Markenrechtsverletzungen nachzukommen. Dass darüber nicht sämtliche Verstöße aufgespürt werden könnten, sei hinzunehmen, und führe nicht zu einem Verschulden des Providers (mit Folgen etwa für ein Ordnungsmittelverfahren nach § 890 ZPO)<sup>17</sup>.

Bei der Zumutbarkeit spielt jedoch eine entscheidende Rolle, WIE denn überhaupt Rechtsverletzungen aufzuspüren sind. Das Anbieten einer Software, mit deren Hilfe das Opfer einer Rechtsverletzung selbst auf dem System eines Providers zugreifen und von ihm erkannte Verletzungen seiner Rechte entfernen kann, wird die Prüfpflichten des Providers, so sie bestehen, nicht ausräumen. Im Rahmen der Zumutbarkeit weiterer Maßnahmen wird ein solches Instrument jedoch „zumutbarkeitsmildernd“ zu berücksichtigen sein<sup>18</sup>.

Soweit das Geschäftsmodell selbst nicht auf der Nutzung der Rechtswidrigkeit eingestellter Inhalte beruht, ist dem Provider nicht zuzumuten, aufgrund der Prüfpflichten sein gesamtes Geschäftsmodell

---

<sup>14</sup> Witte a.a.O. S. 88 unter Berufung auf Erwägungsgrund 27 der Multimedia-Richtlinie ABl. EG Nr. C 344 v. 1.12.2001, S. 1

<sup>15</sup> OLG Hamburg a.a.O., S. 586, überspannt LG Düsseldorf, Urt. v. 23.01.2008, Az.: 12 O 246/07 (GEMA).

<sup>16</sup> BGH GRUR 1997, S. 313, 315; BGH GRUR 2004, S. 860, 864 (Internetversteigerung I)

<sup>17</sup> BGH GRUR 2004, S. 860; BGH GRUR 2006, S. 708.

<sup>18</sup> So wohl auch OLG Hamburg aaO, S. 587: („Diesen ... [Vorsorge-]... Pflichten kann sich die Beklagte nicht vollständig dadurch entledigen, dass sie auf die Möglichkeit der Teilnahme am VeRI-Programm verweist“ („VeRI“= entsprechendes „Verifiziertes Rechteinhaber-Programm, Anm. d. Verf.“), s. auch OLG HH, K&R 2006, S. 226 („Cybersky“), wonach der Rechteinhaber keine unzumutbaren finanziellen oder technischen Aufwendungen des Providers erwarten darf und zur Mitwirkung bei der Störungsbeseitigung, etwa durch das Senden bestimmter Erkennungssignale verpflichtet sein kann

in Frage zu stellen<sup>19</sup>. In die Wertung der Intensität der Prüfpflichten muss dennoch einfließen, ob und in welcher Weise der Provider direkt oder indirekt an den rechtswidrigen Inhalten mitverdient<sup>20</sup>.

Abwägungsgrundsatz bei der Frage der Zumutbarkeit ist auch die Frage, inwiefern eine rechtswidrige Nutzung eines Systems allgemein bekannt ist, darüber hinaus auch, in welche Rechte Dritter rechtswidrig eingegriffen wird. Wird das System – unabhängig von der Frage, ob der Provider direkt oder indirekt von den rechtswidrigen Inhalten profitiert – überwiegend zur Einstellung rechtswidriger Inhalte genutzt? Kann sich etwa ein Peer-to-peer-Anbieter darauf berufen, dass ihm die ausschließliche Nutzung seines Systems als Musiktauschbörse unbekannt sei? Soweit eine anteilig hohe rechtswidrige Nutzung gegeben ist, spricht dies für eine mittelbare Haftung des Providers.

Problematisch ist auch die Anwendung des § 53 UrhG, soweit in einer Weitergabe von Daten Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch vorliegen können. Zwar ist eine Verwendung von in zulässiger Weise hergestellten Vervielfältigungsstücke zur öffentlichen Wiedergabe nach §§ 15 Abs. 2; 19a UrhG unzulässig. Insofern dürfen die Kopien nicht in File-Sharing-Börsen oder Server-Systeme zum öffentlichen Download bereitgestellt werden. Soweit aber kein öffentliches Zugänglichmachen anzunehmen ist, wird das Einstellen einer Datei in ein solches System und der Abruf durch den berechtigten Personenkreis des § 53 UrhG als zulässige Vervielfältigung mit Hilfe des Provider-Rechners zu werten sein, da § 53 auch die Vervielfältigung auf beliebigen elektronischen Speichermedien umfasst<sup>21</sup>.

Fraglich ist, inwiefern durch die jeweiligen Systeme ein öffentliches Zugänglichmachen im Sinne des § 19a UrhG, der auf Ziffer 23 der Multimedia-Richtlinie zurückreicht, gegeben ist. Ein öffentliches Zugänglichmachen liegt vor, wenn Internetdienste Daten zum Download anbieten, die nach ihrer Bestimmung „öffentlich zugänglich“ sind<sup>22</sup>. Zur „Öffentlichkeit“ nach § 15 UrhG gehört dabei jeder, „der nicht mit demjenigen, der das Werk verwertet, oder mit anderen Personen, mit denen das Werk in unkörperlicher Form wahrnehmbar oder zugänglich gemacht wird, durch persönliche Beziehungen verbunden ist“<sup>23</sup>. Hier kann eine Analogie zu der Frage gezogen werden, wann Daten eines Intranet (etwa eines Firmen- oder Vereins-Intranet) „öffentlich“ zugänglich gemacht werden. Dies ist nur dann der Fall, wenn die Daten „Außenstehenden“ bestimmungsgemäß zugänglich sind<sup>24</sup>, Soweit etwa „Sharehoster“ in ihrem Geschäftsmodell also (wie in einem geschützten Intranet) gerade auf die Vertraulichkeit der gespeicherten Daten setzen und nicht etwa eine Verbreitung der Daten durch

---

<sup>19</sup> OLG Hamburg, K&R 2006, S. 586.

<sup>20</sup> Bei einer Auktionsplattform ist etwa zu berücksichtigen, dass der Plattform-Provider über Provisionen am Verkauf beispielsweise urheber- und markenrechtsverletzender Ware mitverdient, OLG Hamburg a.a.O., S. 586.

<sup>21</sup> Wandtke/Bullinger UrhG § 53, Rn. 11.

<sup>22</sup> Wandtke/Bullinger UrhG § 19a, Rn. 23.

<sup>23</sup> Wandtke/Bullinger UrhG § 15, Rn. 14.

<sup>24</sup> Wandtke/Bullinger UrhG § 19a, Rn. 25.

systematische Ermöglichung des Zugangs bewerben (oder dafür einen ihnen gehörenden „Nur-Lister“ einsetzen, s.u.), fehlt es am Merkmal der Zugänglichmachung für die Öffentlichkeit<sup>25</sup>.

Eine öffentliche Zugänglichmachung ist daher sowohl bei Client-Server-Systemen mit Plattformcharakter (z.B. Online-Auktionshäusern), als auch bei Peer-to-Peer-Systemen gegeben, bei denen keine Einschränkung des Nutzerkreises auf ein privates Umfeld, wie etwa den engen Freundeskreis, vorgesehen ist<sup>26</sup>. Anders verhält es sich beim Sharehosting. Hier gibt es keine Form der Mitteilung über die Inhalte der gespeicherten Daten durch den Provider an Dritte. Alleine der Kunde bestimmt, an wen er den Link zu den Dateien weiterleitet. Insofern kann von einer öffentlichen Wiedergabe durch den Provider nicht gesprochen werden, diese liegt vielmehr im Verantwortungsbereich des Kunden, der sowohl über Quellnamen, als auch über Quellinhalte und Quelllinks exklusiv verfügt. Die Inhalte der Sharehosting-Dateien sind über Suchmaschinen nicht aufzufinden, auch sagen die Dateinamen nicht notwendigerweise etwas über den Inhalt aus.

Einen Sonderfall bilden die „Nur-Lister“, bei denen die Kunden von Sharehostern ihre Links zu ihren bei den Sharehostern gespeicherten Dateien veröffentlichen können<sup>27</sup>. Im Unterschied zu Suchmaschinen, die grundsätzlich durch die Verlinkung auf fremde Inhalte keinen urheberrechtlichen Störerzustand schaffen<sup>28</sup>, findet hier eine deutliche Erhöhung der Gefahr einer rechtswidrigen Nutzung statt. Zum einen handelt es sich hier nicht um eine lediglich systematische Wiedergabe frei vorhandener Links<sup>29</sup>, zu denen der Allgemeinheit der Internetnutzer bereits der Zugang eröffnet wurde, sondern um die Sammlung von Links, die andernfalls gar nicht durch normale Suchmaschinen erreichbar wären. Zum anderen besteht das Geschäftsmodell der „Nur-Lister“ gerade darin, Kunden von Sharehostern zur Verbreitung der dort gespeicherten Inhalte zu animieren und diese ggf. zu bewerben. Insofern kann eine Suchmaschinenprivilegierung analog „Paperboy“ für „Nur-Lister“ nicht greifen, da diese gerade über eine besondere Nähe zum Inhalt verfügen und die Nähe zu rechtswidrigen Inhalten teilweise bewerben.

„Sharehoster“ werden sich andererseits im Hinblick auf das Setzen von Links durch „Nur-Lister“ kaum zur Wehr setzen können, soweit „Nur-Lister“ zulässigerweise „Deep-Links“ auf Inhalte sammeln, die von den Kunden der „Nur-Lister“ beim „Sharehoster“ eingesetzt wurden und bei denen die Mitteilung des – nur den Kunden des „Sharehosters“ zugängliche – Links von diesen Kunden selbst stammt<sup>30</sup>. Soweit – nach richtiger Einordnung – den „Sharehoster“ keine Störerhaftung für die bei ihm anonym eingestellten Inhalte trifft und er auch nicht in einer Geschäftsbeziehung zum „Nur-

---

<sup>25</sup> Verglichen werden kann die Situation auch mit einem Homepage-Inhaber, der die Seiten durch ein Codewort vor einem Zugriff durch Dritte schützt. Hier ist die Codierungsmöglichkeit allerdings durch den Kunden vorgegeben, der bei entsprechender Wahl des Filenamens verhindert, dass Dritte sinnvoll nach den Daten seines Files suchen und diese abrufen können (Filename „XXUZTZS“ statt „Urlaubsvideo“).

<sup>26</sup> Soweit der Provider auch etwa über Favoriten- oder Ordnerfunktionen anbietet, Inhalte Dritter verfügbar zu machen, stellt dies einen weiteren Schritt zur Unterstützung des Auffindens fremder rechtswidriger Inhalte dar.

<sup>27</sup> Es handelt sich damit um Suchmaschinen, die insbesondere Teile der bei Sharehostern gespeicherten Inhalte referenzieren, s.o. I2e).

<sup>28</sup> S. BGH K&R 2003, 556 („Paperboy“).

<sup>29</sup> BGH a.a.O.

<sup>30</sup> Mangels einer eigenen Listing-Datenbank werden entsprechende Rechte des Sharehosters nicht verletzt, denkbar wäre allenfalls eine wettbewerbswidrige Übernahme fremder Leistungen, da der „Nur-Lister“ die anonymen Speicherungen beim „Sharehoster“ teilveröffentlicht.

Lister“ steht, wird ihn auch keine Störerhaftung treffen, die ihn veranlasst, die Tätigkeit des „Nur-Listers“ zu unterbinden.

(...)

## **2) Fazit: Kriterien der Störerhaftung**

Die Störerhaftung muss sich nach verlässlichen Grundkriterien richten, um nicht zu einer Gefährdungshaftung auszuweichen. Hierbei müssen vor allem Quantität und Qualität der Rechtsverletzungen, die Werbung mit oder die Nähe der Anbieter zu denselben, die Frage des Profitierens an Rechtsverletzungen und die Schaffung alternativer Löschmöglichkeiten für Rechteinhaber (s.o. zum „VeRI“-System) eine Rolle spielen. Zugleich muss die technische Möglichkeit der Prüfung das Maß der Verhältnismäßigkeit darstellen, um nicht von vorne herein Geschäftsmodelle durch die Notwendigkeit manueller Durchsicherung von Inhalten zu konterkarieren, wie dies etwa das LG Düsseldorf bei Sharehostern verlangt<sup>31</sup>.

Zur Eindämmung der Störerhaftung sollten folgende einheitliche Kriterien für alle Provider gelten, die über die Problematik der Forenanbieter hinausweisen.

### **a) Quantität und Qualität der Rechtsverletzungen, Störernutzen durch rechtswidrige Inhalte**

In welchem Umfang manuelle Prüfpflichten als drastische Ausnahmen postuliert werden können, hängt von Quantität und Qualität der eingestellten Rechtsverletzungen ab. Das LG München I<sup>32</sup> hält manuelle Prüfpflichten nur dann für verhältnismäßig, wenn „ein Großteil der im Usenet vorhandenen Inhalte“ rechtswidrig wären. Hierfür wäre die Klägerin beweisbelastet. Liegt kein zentrales Listing der Inhalte eines Systems vor (wie bei einem Sharehoster), dann wird ein solcher Beweis – anders als das LG Düsseldorf es unterstellt<sup>33</sup> – kaum zu erbringen sein. Das weitere Kriterium des Störernutzens bestimmt sich nach der Art und Weise, in der der Provider von den Umständen der rechtswidrigen Nutzung seines Systems durch Dritte profitiert.

### **b) „Nähe“ des Providers zum Inhalt, Werbung mit rechtswidrigen Inhalten**

Liegt eine Werbung des Providers vor, die Anwendern einen Rechtsmissbrauch nahe legt, wird man von verschärften Prüfpflichten ausgehen müssen, wenn dann nicht ohnehin bereits ein Verschulden

---

<sup>31</sup> Jürgens (Von der Provider- zur Provider- und Medienhaftung, CR 2006, S. 188) schlägt das Kriterium der Dispositionshoheit als Zuordnungskriterium für „eigene Informationen“ i.S.d. TDG/MDSStV vor und differenziert aus der Rezipientenperspektive.

<sup>32</sup> München I, Urt. v. 19.04.2007, Az.: 7 O 3950/07, S. 18.

<sup>33</sup> LG Düsseldorf, Urt. v. 23.01.2008, Az.: 12 O 246/07, S. 16.



und damit eine bedingt vorsätzliche Teilnahme an den Handlungen des eigentlichen Störers gegeben ist<sup>34</sup>.

Eine abgeschwächte Form der Beziehung zu rechtswidrigen Inhalten ist gegeben, wenn das angebotene System zwangsläufig eine gewisse „Nähe zum Inhalt“ aufweist. Dies liegt etwa dann vor, wenn die Inhalte in vom Provider vorgegebene Kategorien einzuteilen sind wenn etwa sich anhand vorgegebener „News-Forentitel“ oder Auktionskategorien eine Prüfpflicht aufdrängt (siehe OLG HH, K&R 2006, S. 47ff (Heise)). Je nach „Gefahrneigung“ der Kategorien („Musik“, „Comedy“, „Nationales“ etc.) werden sich daraus gesteigerte Prüfpflichten ergeben<sup>35</sup>. Am „inhaltsfernsten“ werden Sharehoster zu qualifizieren sein, bei denen keine eigenen Listings bestehen und selbst der „Dateiname“, also der ausgeworfene Link, mit dem der Anwender seinen Inhalt aufrufen kann, zufällig generiert wird und nicht in Beziehung zum Dateinhalt steht. Da sie nicht einmal über Dateititel verfügen, die selbst Rechtsverletzungen darstellen oder signalisieren können, werden sie einer Störerhaftung mindestens so fern stehen wie die DENIC, die trotz bei ihr vorhandener Listings potenziell Namens- oder markenrechtsverletzender Domaintitel nicht zu einer vorbeugenden Filterung verpflichtet ist<sup>36</sup>.

### c) „Filterbarkeit“ der Rechtsverletzungen

Die Zumutbarkeitsgrenzen werden überspannt, wenn dem Provider auferlegt wird, nicht nach filterbaren Begriffen zu suchen, sondern ohne technische Möglichkeiten identische Inhalte in seinen Dateien aufzuspüren. Soweit dies etwa bei Bilderkennungsfiltern unklar ist, bleibt der jeweilige Rechteinhaber im Fall einer Klage durch diesen beweisbelastet<sup>37</sup>.

Der BGH hält eine Verpflichtung für unzumutbar, manuelles Suchen in den Fällen durchzuführen, in denen keine Suchbegriffe vorhanden sind, die sich in eine Filtersoftware eingeben ließen<sup>38</sup>.

Gelingt es dem Kläger nicht, eine Software zu benennen, die die entsprechende Filterleistung erbringen kann, ist der Beweis gescheitert<sup>39</sup>. Insofern muss jede Prüfpflicht unter den Vorbehalt der entsprechenden technischen Umsetzbarkeit stehen (s.u.). Eine andere Bewertung würde den Gedanken des „Web 2.0“ ad absurdum führen, weil dann jedes Hosting oder Listing unkontrolliert eingestellter, nicht automatisch filterbarer Inhalte ein unkontrolliertes Risiko für jeden Anbieter darstellen würde.

Auch die automatische Suche birgt jedoch Probleme: Wie soll der Provider, der manuell über einen Filterbegriff wie „Yesterday“-Dateien mit dem Musikstück der Beatles gefunden hat, reagieren: Handelt es sich um ein System, das einen beliebigen Download durch Dritte erlaubt, kann eine Sperrung nicht gegen das Recht des Einstellenden auf Weitergabe einer Privatkopie im Freundeskreis verstoßen. Wie aber soll ein Sharehoster eine manuelle Suche durchführen, da er keine Kenntnis von

<sup>34</sup> s. LG München I, Urt. V. 19.04.2007, Az.: 7 O 3950/07, S. 18, OLG HH, K&R 2006, S. 225 („Cybersky“).

<sup>35</sup> Gleiches gilt für Systeme, in denen die Daten mit Schlagwörtern versehen werden oder leicht filterbare Textdateien bestehen, aus denen sich Inhalte erschliessen oder Suchwörter ausfiltern lassen (wie dies etwa bei google-„Ad-Words“ der Fall ist, s. OLG HH, K&R 2006, S. 520).

<sup>36</sup> BGH Z 148, S. 13 („ambiente“)

<sup>37</sup> S. LG München I, Urt. V. 19.04.2007, Az.: 7 O 3950/07, S. 17; OLG München, Urt. V. 21.12.2006, Az. 29 U 4407/06, S. 15f. zur Beweislast für die Existenz von entsprechender Bildfiltersoftware.

<sup>38</sup> BGH Urt. v. 19.04.2007, Az. I ZR 35/04

<sup>39</sup> LG München I, a.a.O.

den Inhalten der Kundendateien hat? Er muss zunächst bei „Nur-Listern“ die entsprechenden Dateien ausfindig machen. Da diese aber nicht einem beliebig Dritten zur Verfügung gestellt werden, müsste er erst ab einem gewissen Zugriffszeitpunkt (mehr als 7 Zugriffe?) sperren, um nicht gegen das Recht auf „Privatkopie“ zu verstoßen. Außerdem müsste er die internen Zugriffe des Kunden ausfiltern, da es sein kann, dass dieser den Server des Sharehoster als externen Speicher bzw. Backup benutzt<sup>40</sup>.

#### d) Ergebnis

Sowohl die aktuelle Entwicklung der untergerichtlichen Rechtsprechung zur Störerhaftung als auch die unveränderte Haftungsregelung des TMG sind für Provider insofern unbefriedigend, als sie keine ausreichende Sicherheit bei der rechtlichen Einordnung der Haftung für funktional unterschiedliche Provider-Angebote bieten. Auch hat der BGH in seiner „Internetversteigerung-II“ Entscheidung<sup>41</sup> wenig dazu sagen können, wie im Einzelnen die Kriterien der Prüfpflichten auszugestaltet sind (insofern darf man auf die Entscheidung des Berufungsgerichts gespannt sein, an das der Fall zurückverwiesen wurde). In der Entscheidung „Jugendgefährdende Inhalte“ wurde (unter Bezug auf Wettbewerbsrecht) gefordert, dass vom Internetversteigerer nicht nur Vorsorge im Hinblick auf identische, sondern auch auf gleichartige Rechtsverletzungen getroffen werden müsse<sup>42</sup>:

Die überspannte Anwendung der Grundsätze der Störerhaftung führen in vielen Fällen bei der Instanzrechtsprechung zu einer die technischen Möglichkeiten der Provider ignorierenden Ausdehnung der Prüfpflichten<sup>43</sup> darauf, dass der Rechteinhaber keine unzumutbaren finanziellen oder technischen Aufwendungen des Providers erwarten darf. Sollen die – zu unrecht unveränderten – Filterregelungen des TMG nicht ausgehebelt werden, muss sich eine einheitliche Anwendung von Kriterien der Zumutbarkeit und der Prüfpflichten ergeben, die es Providern insbesondere des „web 2.0“ gestatten, ihre Haftungsrisiken abzuschätzen<sup>44</sup>. Es ist zu wünschen, dass die Vorlage der entsprechenden deutschen Urteile zur Providerhaftung durch die Bundesregierung an die EU-Kommission zur „Notifizierung“ erfolgreich ist<sup>45</sup>.

---

<sup>40</sup> Weiterhin wird eine Vielzahl der Dateien als „Zip“- oder ähnlich Datei komprimiert bzw. „gepackt“ vorliegen. Will man also nicht allein aufgrund des Dateinamens sperren – weil dieser zB einem aktuellen Kinofilm entspricht – müsste die Datei manuell entpackt und gesichtet werden, was zum einen zu Sicherheitsproblemen und zum anderen zur Vervielfachung des Arbeitsaufwandes führen würde.

<sup>41</sup> BGH Urt. v. 19.04.2007, Az. I ZR 35/04.

<sup>42</sup> BGH GRUR 2007, 890

<sup>43</sup> Siehe auch Hinweis des OLG HH, K&R 2006, S. 226 („Cybersky“)

<sup>44</sup> Hinzuweisen ist im Übrigen darauf, dass, soweit Anbieter weitergehende Prüfungen durchführen, als ihnen aufzuerlegen ist, kein Fall der selbst auferlegten Erweiterung der Prüfpflichten eintritt. Die überobligatorisch durchgeführten Filterungen bleiben freiwillig, LG München I, CR 2006, S. 496f.

<sup>45</sup> Die Vorlage bezweifelt die Übereinstimmung der Rechtsprechung mit den Vorgaben der E-Commerce-Richtlinie (s.o.) und kritisiert insbesondere die Ausweitung der Störerhaftung mit automatischen und manuellen Prüfpflichten (s. <http://www.heise.de/newsticker/meldung/91188>).



.berlin .frankfurt .hamburg . köln .münchen .brüssel