bühr führen und diese womöglich weit übersteigen. Es gibt keinen Grund für die Annahme, dass die Ergebnisse der unterschiedlichen Schadensausgleichsmethoden deswegen auseinanderfallen dürften oder gar sollten, weil der Abschöpfung des Verletzergewinns eine nur ihr eigene Abschreckungswirkung zukommen müsse.[44] Dies liegt vielmehr umso ferner, als Art. 13 Abs. 2 der Durchsetzungsrichtlinie als Option für den nationalen Gesetzgeber die Gewinnherausgabe auch bei schuldlosem Handeln des Verletzers vorsieht.

IV. Ergebnis

Die Durchsetzungsrichtlinie und die zu ihrer Umsetzung neu gefassten Schadensersatzbestimmungen des Markengesetzes und der übrigen Gesetze zum Schutz des geistigen Eigentums haben den Gedanken gestärkt, dass die herkömmlich als Schadensberechnungsmethoden, besser aber als Schadensausgleichsmethoden bezeichneten verschiedenen Ansätze (Ersatz des entgangenen Gewinns, Herausgabe des Verletzergewinns, Lizenzanalogie) ein und demselben Ziel dienen, nämlich der Kompensation des Schadens, den der Schutzrechtsinhaber dadurch erleidet, dass der Verletzer in sein ausschließliches Recht zur Nutzung des immateriellen Schutzgegenstands eingreift. Sachgerecht angewandt müssen daher die unterschiedlichen Methoden auch zu (im Wesentlichen) übereinstimmenden Ergebnissen führen. Das zwingt dazu, Übertreibungen entgegenzuwirken, die sich im Gefolge des Urteils „Gemeinkostenanteil" bei der Ermittlung des als Verletzergewinn herauszugebenden Betrages ergeben können, wenn der Kompensationsgedanke aus dem Auge verloren wird. Auf der anderen Seite ist es geboten, auch bei der Lizenzanalogie den Grundsatz zu beachten, dass der auf die Benutzung des Schutzrechts beruhende Gewinn in vollem Umfang allein dem Schutzrechtsinhaber gebührt. Das der Lizenzanalogie zugrunde liegende fiktive Lizenzverhältnis dient daher nicht dem beiderseitigen Nutzen von „Lizenzgeber" und „Lizenznehmer"; vielmehr ist auch die Lizenzgebühr zur „Herausgabe des Verletzergewinns" und damit zur vollen Schadenskompensation bestimmt und geeignet und führt idealerweise zu einem im Wesentlichen mit den beiden anderen Methoden übereinstimmenden Ergebnis.

44) Vgl. auch *Fezer* (Fn. 13) § 14 Rn. 1028: Schadensberechnung nach der angemessenen Lizenzgebühr bestimmt den Schaden unter dem Gesichtspunkt der Prävention und Sanktion normativ; Rn. 1044: Folge einer Gewinnberücksichtigung ist eine Erhöhung der Schadensersatzlizenzgebühr im Regelfall.

Prof. Dr. Thomas Hoeren und Arne Neubauer, Münster*

Der EuGH, Netlog und die Haftung für Host-Provider

INHALT

Der EuGH hat sich nach langjähriger Abstinenz in gleich drei Entscheidungen mit der Haftung von Internetprovidern beschäftigen müssen.[1] Im jüngsten Urteil („Netlog/SABAM") hat der EuGH herausgearbeitet, dass der Betreiber eines sozialen Netzwerkes im Internet nicht gezwungen werden kann, ein generelles, alle Nutzer dieses Netzwerkes erfassendes Filtersystem einzurichten, um die unzulässige Nutzung musikalischer und audiovisueller Werke zu verhindern.[2] Im Weiteren sollen die wesentlichen Grundzüge der Netlog/SABAM-Entscheidung im Lichte der bisherigen Entscheidungspraxis herausgearbeitet und problematisiert werden.

I. Ausgangslage

Ausgangspunkt der EuGH-Entscheidung ist die E-Commerce-Richtlinie.[3] Die Art. 12–15 regeln die Verantwortlichkeit von Providern. Demnach sind Dienste, die reine Durchleitungsfunktionen übernehmen, sog. Access-Provider, nach Art. 12 nicht für die übermittelten Informationen verantwortlich. Ebenso beschränkt Art. 14 die Verantwortlichkeit von Host-Providern, sofern diese nach Kenntniserlangung von illegalen Inhalten unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu sperren. Die Richtlinie will damit dem Umstand Rechnung tragen, dass Access- und Host-Provider aufgrund der Masse der Inhalte nur begrenzte Möglichkeiten zur Einflussnahme auf das Nutzerverhalten haben.

Gleichzeitig schützt die Enforcement-Richtlinie[4] die Rechte der Urheber. Nach den Art. 8 und 11 der Richtlinie haben diese das Recht, Auskunft über die Verletzer auch von Providern zu verlangen. Der Gerichtshof hat nun einige Vorgaben zur Auslegung

* Professor Dr. Thomas Hoeren ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) der Universität Münster. Arne Neubauer ist wissenschaftlicher Mitarbeiter am ITM. Mehr über die Autoren erfahren Sie auf S. 624.

1) EuGH, 12.07.2011 – C-324/09, WRP 2011, 1129 ff. – L'Oréal/eBay; EuGH, 24.11.2011 – C-70/10, MMR 2012, 174 ff. – Scarlet/SABAM sowie EuGH, 16.02.2012 – C-360/10, WRP 2012, 429 ff. – Netlog/SABAM.

2) EuGH, 16.02.2012 – C-360/10, WRP 2012, 429 ff. – Netlog/SABAM.

3) Richtlinie 2000/31/EG vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs.

4) Richtlinie 2004/48/EG vom 29.04.2004 zur Durchsetzung der Rechte des geistigen Eigentums.

der E-Commerce-Richtlinie unter Berücksichtigung der Enforcement-Richtlinie gemacht und damit Klarheit geschaffen, bis zu welchem Umfang Host-Provider für die Vorbeugung und Verfolgung von Urheberrechtsverletzungen verantwortlich gemacht werden können.

II. Verantwortlichkeit der Host-Provider

Die Rechtslage bei fremden Inhalten, die Provider zur Nutzung bereithalten (sog. Host-Providing) ist komplex. Nach § 10 TMG sind Diensteanbieter für fremde Informationen, welche sie für einen Nutzer speichern, nicht verantwortlich, sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird oder sofern sie bei Kenntniserlangung unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren. Entscheidend für die Haftung des Host-Providers für Rechtsverletzungen, die unter Nutzung seiner Dienste begangen wurden, ist das Vorliegen der anspruchsbegründenden Tatbestandsmerkmale „Kenntnis" und „offensichtliche" Rechtswidrigkeit. Der Anspruchsteller trägt die volle Darlegungs- und Beweislast für das Vorliegen der Kenntnis.[5] Damit soll die Haftung der Host-Provider auf Vorsatzstraftaten und -delikte beschränkt werden. Das OLG Düsseldorf verneint deshalb Überprüfungspflichten des Host-Providers und sieht eine Haftung erst ab Kenntnis der Rechtswidrigkeit als begründet an.[6] Fraglich ist, wann von einer offensichtlichen Rechtswidrigkeit ausgegangen werden kann. Dies sei der Fall, wenn die Rechtsverletzungen durch die Kunden der Host-Provider für juristische Laien ohne weitere Nachforschungen offenkundig sind. Daher können die Host-Provider auch nur dann auf Schadensersatz in Anspruch genommen werden.

Mit der Regelung des § 10 TMG konterkariert der Gesetzgeber seine eigenen Bemühungen, die Provider zur innerbetrieblichen oder verbandsseitigen Selbstkontrolle zu verpflichten. Denn wenn die bloße Kenntnis vom Inhalt als subjektives Element ausreichen soll, wird niemand daran Interesse haben, Personal mit der Sichtung des Online-Angebots zu beauftragen. Er wird vielmehr auf jedwede Selbstkontrolle verzichten – getreu dem Motto: Nichts gesehen, nichts gehört. Auch das LG München hat dieses Problem gesehen. Seiner Auffassung nach würden bei der amtlichen Auslegung des TMG sowohl Art. 14 GG als auch die Regelungen in Art. 8, 10 und 14 WIPO-Vertrag unterlaufen. Selbst „bewusstes Wegschauen" würde zu einem Haftungsausschluss führen. Dies könne nicht zugelassen werden.[7] Das Landgericht fordert, Prüfungspflichten auch hinsichtlich der die Rechtswidrigkeit begründenden Umstände anzunehmen. Es hätte sich darüber hinaus angeboten, wenigstens für die Fälle eine Prüfungspflicht zu bejahen, in denen ein Verstoß gegen Strafgesetze nahe liegt (etwa bei der Bezeichnung einer Newsgroup als „alt.binaries.children-pornography"). Eine solche Prüfungspflicht bei eklatanter Missbrauchsgefahr hätte zudem der geltenden Rechtslage im Zivil- und Strafrecht entsprochen. Art. 15 Abs. 1 der E-Commerce-Richtlinie sieht jedoch ausdrücklich von einer Prüfungspflicht ab.

5) BGH, 23.09.2003 – VI ZR 335/02, MMR 2004, 166 zu § 5 Abs. 2 TDG a. F.; *Spindler*, NJW 1997, 3193; sowie auch *Spindler*, NJW 2002, 921.

6) OLG Düsseldorf, 07.06.2006 – I-15 U 21/06, CR 2006, 682.

7) LG München I, 30.03.2000 – 7 O 3625/98, MMR 2000, 431.

§ 10 TMG stellt für das Bewusstsein der Rechtswidrigkeit auf die tatsächliche Kenntnis von der rechtswidrigen Tätigkeit ab. Die bloße Tatsache, dass ein Rechenzentrumsmitarbeiter eine Newsgroup gesichtet hat, heißt ja noch nicht, dass er deren Inhalt richtig, d. h. als Rechtsverstoß, bewerten kann. Zumindest für die zivilrechtliche Haftung schließt Vorsatz neben dem Wissen und Wollen der Tatbestandsverwirklichung auch das Bewusstsein von der Rechtswidrigkeit des Angebots mit ein. Da diese Wertung gerade im fließenden E-Commerce-Recht schwierig zu ziehen ist, hat es der Gesetzgeber bei Schadensersatzansprüchen für erforderlich erachtet, dass der Anbieter sich der Tatsachen und Umstände bewusst ist, aus denen die Rechtswidrigkeit der Information offensichtlich wird.[8]

Der BGH hat bislang eine Anwendung von § 10 TMG nur für Schadensersatzansprüche zugelassen. Bei Unterlassungsansprüchen sei das TMG überhaupt nicht einschlägig. Vielmehr sollen dann die allgemeinen Grundsätze der Störerhaftung gelten. Daher ist das Haftungsprivileg gem. § 10 S. 1 TMG unanwendbar, wenn ein Unterlassungsanspruch gegen den Anbieter besteht. Dies gilt sowohl für den auf eine bereits geschehene Verletzung gestützten[9] als auch für den vorbeugenden Unterlassungsanspruch.[10]

Als Störer haftet derjenige,

- der in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung oder Aufrechterhaltung einer rechtswidrigen Beeinträchtigung mitgewirkt hat,
- dem es rechtlich und tatsächlich möglich und zumutbar ist, die unmittelbare Rechtsverletzung zu verhindern und
- der zumutbare Prüfungspflichten verletzt hat.[11]

In einem aktuellen Urteil[12] hat der BGH ein dem Notice-and-Take-Down-Verfahren vergleichbares, neues Haftungsmodell für Host-Provider bei der Verletzung von Persönlichkeitsrechten durch fremde Inhalte geschaffen. Der Beklagte hatte die technische Infrastruktur für einen Blog zur Verfügung gestellt, auf dem Tatsachen behauptet wurden, die der Kläger für unwahr und ehrenrührig hielt. Das Gericht hat in diesem Fall zur Begründung der Störerhaftung auf Unterlassen die Verletzung folgender Pflichten angenommen: Der Hinweis auf die rechtswidrigen Inhalte müsse so konkret sein, dass der Rechtsverstoß auf dessen Grundlage unschwer bejaht werden kann, das heißt ohne eingehende rechtliche und tatsächliche Überprüfung. Dieser Hinweis müsse dann an den für den Inhalt Verantwortlichen mit Aufforderung zur Stellungnahme weitergeleitet werden. Bleibe eine Stellungnahme aus, sei der Eintrag zu löschen. Werde allerdings der Berechtigung der Beanstandung so substantiiert widersprochen, dass sich berechtigte Zweifel ergeben, müsse der Provider dies dem Betroffenen mitteilen und von diesem Nachweise verlangen, aus denen sich die Rechtsverletzung ergibt. Bleibe dieser Nachweis aus, könne von einer weiteren Prüfung abgesehen werden. Ergebe sich allerdings daraus eine rechts-

8) Falsch ist m. E. die Auffassung von *Tettenborn u. a.*, Beilage K&R 12/2001, S. 1, 32, wonach durch diese Formulierung eine Haftung für grob fahrlässige Unkenntnis eingeführt worden sei.

9) BGH, 11.03.2004 – I ZR 304/01, WRP 2004, 1287 – Internet-Versteigerung = CR 2004, 763 m. Anm. *Volkmann*.

10) BGH, 19.04.2007 – I ZR 35/04, WRP 2007, 964 – Internetversteigerung II = CR 2007, 523 m. Anm. *Rössel*.

11) BGH, 10.10.1996 – I ZR 129/94, WRP 1997, 325; dazu *Fürst*, WRP 2009, 378; *Leistner/Stang*, WRP 2008, 533; *Leistner*, GRUR-Beilage 2010, 1.

12) BGH, 25.10.2011 – VI ZR 93/10, WRP 2012, 217 – Prüfpflichten und Störerhaftung des Hostproviders = MMR 2012, 124 m. Anm. *Hoeren*.

widrige Persönlichkeitsrechtsverletzung, sei der Eintrag vom Provider zu löschen.

Für den Bereich des Wettbewerbsrechts hat der BGH dagegen eine Störerhaftung von Host-Providern abgelehnt und stattdessen auf die Täterhaftung abgestellt.[13] In der jüngsten Entscheidung „Kinderhochstühle im Internet"[14] hat der BGH den Abschied von der Störerhaftung im Wettbewerbsrecht ausdrücklich bekräftigt. In Fällen des Verhaltensunrechts komme eine Störerhaftung nicht in Betracht. Vielmehr sei nach einer täterschaftlichen Verletzung wettbewerbsrechtlicher Verkehrspflichten zu fragen.[15] Im Übrigen entsprechen die Verkehrspflichten inhaltlich den vorherigen Prüfpflichten im Rahmen der Störerhaftung, da der BGH für die Erläuterung dieser Pflichten die zur Störerhaftung entwickelten Grundsätze heranzieht.[16] Unterschiede bestehen vor allem bei der Geltendmachung von Auskunftsansprüchen, die nunmehr bei einer täterschaftlichen Konstruktion anders als bei der Störerhaftung bejaht werden können. Im Urheber- und Markenrecht bleibt es jedenfalls für den Host-Provider bei der Figur der Störerhaftung.[17] Anders denkt allerdings noch das OLG Hamburg, das bei Host-Providern dazu neigt, eine Unterlassungshaftung aufgrund einer Gehilfenstellung zu bejahen.[18]

III. Filtersysteme im Internet

Hinsichtlich der praktischen Nutzbarkeit von Filtersystemen ist zu fragen, inwieweit tatsächlich effektive Möglichkeiten der Vorbeugung, Verhinderung und nachträglichen Beseitigung inklusive Verhinderung einer Wiederholung der Verbreitung von urheberrechtlich geschütztem Material bestehen. Das Videoportal YouTube arbeitet zum Beispiel mit einem automatischen Sicherungssystem, genannt „Content ID", das die ungenehmigte Veröffentlichung von urheberrechtlich geschützter Musik unterbinden soll. Dieses System erkennt anhand eines digitalen Fingerabdrucks die geschützten Stücke schon anhand weniger Takte.[19] Die Sperrungen durch die Rechteinhaber gehen dabei offenbar außerordentlich weit. Berichtet wurde von einem Fall, in dem ein Familienvideo aufgrund der gerade noch erkennbaren Hintergrundmusik gelöscht wurde.[20] Damit verfestigt sich der Eindruck, dass die Nutzung automatischer Filtersysteme häufig über das vorgegebene Ziel hinaus schießt und regelmäßig auch zur Sperrung rechtmäßig veröffentlichter Inhalte führt.

Soweit das Geschäftsmodell selbst nicht auf der Nutzung der Rechtswidrigkeit eingestellter Inhalte beruht, ist dem Provider nicht zuzumuten, auf Grund der Prüfpflichten sein gesamtes Geschäftsmodell in Frage zu stellen.[21] Eine Sperrung bestimmter Dateinamen erscheint ungeeignet. Denn Dateinamen sind jederzeit veränderbar. Aus diesem Grund scheidet auch eine Sperrung aller Dateinamen, die bestimmte Begriffe enthalten, aus. Im Übrigen sind die Nutzer selbst nicht auf den Dateinamen zum Auffinden der gesuchten Datei angewiesen, da sie die Datei über einen externen Link abrufen, welcher auf einer anderen Internetseite mit dem entsprechenden Begriff versehen und dadurch auffindbar ist. Die Forderung nach einer menschlichen, gezielten Überprüfung von Inhalten, bei denen eine gesteigerte Wahrscheinlichkeit für Rechtsverletzungen besteht, lässt sich wegen des damit verbundenen Personalaufwands in der Praxis regelmäßig nicht realisieren. Sie führt lediglich dazu, dass die zu prüfenden Dateien oder Nutzerkonten ohne menschliche Überprüfung automatisiert gelöscht werden. Als Anknüpfungspunkt dienen nur bestimmte Schlüsselwörter im Dateinamen. Angesichts der Vielzahl der Dateien und der Mehrdeutigkeit der einzelnen Begriffe, sowie der leichten Umgehbarkeit steht eine manuelle Überprüfung nicht im Verhältnis zum Erfolg. Eine Anknüpfung an IP-Adressen ist abzulehnen, da eine IP-Adresse regelmäßig von so vielen verschiedenen Personen genutzt wird, dass die Wahrscheinlichkeit, eine weitere Rechtsverletzung festzustellen, unverhältnismäßig gering ist. Aus diesem Grund ist auch eine Sperrung von IP-Adressen nicht wirkungsvoll.

Selbst der Betreiber eines Rechners (z. B. ein Content-Provider) kann nicht mit hinreichender Sicherheit feststellen, welche Information sich hinter einer Bitfolge verbirgt, die ein Benutzer auf diesem Rechner abgelegt hat.[22] Dies gilt selbst dann, wenn man filmspezifische Suffixe verwendet (wie z. B. .mov, .avi, .mpeg, .divx). So kann in Microsoft-Betriebssystemen problemlos durch den Benutzer eingestellt werden, dass .jpg-Dateien mit dem ASCII-Editor, .txt-Dateien jedoch mit einer Bildbetrachtungssoftware zu öffnen sind. Es besteht für den Nutzer folglich kein Zwang, überhaupt ein Suffix zu benutzen oder sich an diese Bequemlichkeitsstandards zu halten.[23]

Ferner ist auch eine inhaltliche Kontrolle der auf den Servern eines Host-Providers gespeicherten Daten in der Regel ausgeschlossen. Urheberrechtlich geschützte Inhalte werden von Nutzern vor dem Upload meist verschlüsselt, so dass der Inhalt für den Serverbetreiber ohne den Schlüssel nicht mehr erkennbar ist. Wie in der Literatur beschrieben, sind Daten, die mit modernen Verschlüsselungsprogrammen codiert wurden, mit heutigen Entschlüsselungstechniken nicht zu „knacken".[24] Erfahrungen aus anderen Ländern zeigen, dass Nutzer beispielsweise statt der Verwendung von BitTorrent-Systemen vermehrt zur Nutzung anderer Methoden übergehen, um einer Haftung zu entgehen. Ausweislich eines Arbeitspapiers der EU-Kommission führte das HADOPI-Gesetz dazu, dass sich Internetnutzer vor allem Verkehrsverschlüsselungstechniken, VPN-Verbindungen und Proxies bedienten, um ihre Anonymität zu wahren.[25]

IV. Die bisherigen EuGH-Entscheidungen

Alles begann mit dem Promusicae-Urteil.[26] Eine spanische Verwertungsgesellschaft beantragte, Telefónica die Offenlegung von Name und Anschrift bestimmter Personen aufzugeben, denen Telefónica einen Internetzugang gewährt und von denen Promusicae die IP-Adresse sowie der Tag und die Zeit der Verbindung bekannt sind. Nach Ansicht von Promusicae verwendeten diese Personen das Programm KaZaA zum Austausch von Dateien und ließen den Zugriff auf Musikdateien zu, die sich im gemeinsam

13) BGH, 12.07.2007 – I ZR 18/04, WRP 2007, 1173 – Jugendgefährdende Medien bei eBay; siehe bereits BGH, 15.05.2003 – I ZR 292/00, WRP 2003, 1350 – Ausschreibung von Vermessungsleistungen; BGH, 14.06.2006 – I ZR 249/03, WRP 2006, 1225 – Stadt Geldern.
14) BGH, 22.07.2010 – I ZR 139/08, WRP 2011, 223 – Kinderhohstühle im Internet.
15) Ähnlich LG München I, 04.11.2008 – 33 O 20212/07, WRP 2009, 491; LG Frankfurt a. M., 13.01.2010 – 2-06 O 521/09, MMR 2010, 336; OLG Köln, 27.08.2010 – 6 U 43/10, GRUR-Prax 2010, 566. Ähnlich für eine vollständige Abkehr vom Störermodell zum Tätermodell *Folkmann*, CR 2008, 232; *Leistner*, GRUR-Beilage 2010, 1.
16) *Engels*, MMR 2011, 175, 176.
17) BGH, 17.05.2001 – I ZR 251/99, WRP 2001, 1305 – ambiente.de; BGH, 11.03.2004 – I ZR 304/01, WRP 2004, 1287 – Internet-Versteigerung.
18) OLG Hamburg, 24.07.2008 – 3 U 216/06, WRP 2008, 1569; dazu auch *Fürst*, WRP 2009, 378.
19) Heise, Meldung vom 07.12.2011, Sperr-Posse um die „Sonnenallee" auf YouTube, abrufbar unter: http://heise.de/-1391704.
20) Heise, Meldung vom 21.07.2008, Tanzendes Baby beschäftigt weiter die US-Justiz, abrufbar unter: http://heise.de/-188768.
21) *Willmer*, NJW 2008, 1845.
22) *Schnetder*, MMR 2004, 18.
23) OLG Düsseldorf, 27.04.2010 – I-20 U 166/09, MMR 2010, 483 – Rapidshare.
24) *Gercke*, MMR 2008, 291.
25) European Commission Staff Working Paper on Online services, including e-commerce, in the Single Market, S. 51, abrufbar unter: http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.
26) EuGH, 29.01.2008 – C-275/06, WRP 2008, 334 = NJW 2008, 743 ff.

genutzten Ordner (Shared Folder) ihres Computers befanden und für die die Urheber- und Lizenzrechte bei den Mitgliedern von Promusicae lagen. Der EuGH lehnte eine solch umfassende Auskunftspflicht der Access-Provider ab. Das Gemeinschaftsrecht gebiete es den Mitgliedstaaten nicht, im Hinblick auf den effektiven Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen. Das wirft die Frage auf, wie die Erfordernisse des Schutzes verschiedener Grundrechte, nämlich zum einen des Rechts auf Achtung des Privatlebens und zum anderen des Eigentumsrechts und des Rechts auf einen wirksamen Rechtsbehelf, miteinander in Einklang gebracht werden können.

Der Gerichtshof stellte insoweit fest, dass die Mitgliedstaaten sich bei der Umsetzung der Richtlinien im Bereich des geistigen Eigentums und des Schutzes personenbezogener Daten auf eine Auslegung derselben stützen müssen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien hätten die Behörden und Gerichte der Mitgliedstaaten auch darauf zu achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Gemeinschaftsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiere.

Diese Auslegungsprinzipien zog der EuGH jetzt auch für die Beurteilung von Haftungsfragen im Web heran. Der Grund dafür, dass sich der EuGH schon mehrfach mit der Frage herumschlagen musste, welche Haftungsmaßstäbe für Intermediäre gelten, ist naheliegend. Die eigentlich Verantwortlichen für Rechtsverstöße entziehen sich der Verantwortlichkeit rein faktisch durch Nichterreichbarkeit und Flucht in Rechtsoasen. Insofern ist es verständlich, dass die Betroffenen dann versuchen, Host- und Access-Provider für Rechtsverstöße in Anspruch zu nehmen und/oder von ihnen vorsorgliche Maßnahmen zur Verhinderung von Rechtsverstößen einzufordern. Immerhin hat der Host-Provider die Möglichkeit, den auf seinen Rechnern befindlichen Inhalt zu prüfen und entsprechende Schutzmaßnahmen einzuleiten. Und auch dem Access-Provider wird häufig unterstellt, er könne doch durch Eingriffe in die Telekommunikationsverbindungen den Zugang zu einzelnen rechtsverletzenden Inhalten stoppen. Allerdings stehen solchen Überlegungen die Vorgaben der E-Commerce-Richtlinie entgegen. Denn hierin ist geregelt, dass solche Intermediäre nur sehr eingeschränkt in die Verantwortlichkeit genommen werden können.

1. L'Oréal/eBay

Die drei jüngeren Entscheidungen des EuGH zur Verantwortlichkeit von Host-Providern begannen mit dem L'Oréal/eBay-Urteil.[27] Dem Urteil lag ein typischer Fall von Markenrechtsverletzungen im Internet zugrunde. Mehrere eBay-Händler hatten bei dem Online-Auktionshaus unter Benutzung von L'Oréal-Marken Parfüms in rechtsverletzender Weise zum Kauf angeboten. Nach der Vorlage des britischen High Court hatte der Gerichtshof zu entscheiden, ob und in welchem Umfang eBay für diese Markenrechtsverletzungen haften muss. Zentraler Punkt des Urteils war die Auslegung von Art. 14 Abs. 1 der E-Commerce-RL und die Klärung der Frage, ob eBay von dem Haftungsprivileg für Host-Provider profitiert.

Der Gerichtshof stellte im Rahmen seines Urteils fest, dass eBay von der Haftungsbeschränkung profitieren könne. Das sei aber dann nicht mehr der Fall, wenn der Anbieter des Dienstes statt einer neutralen eine „aktive Rolle" spiele, die ihm Kenntnis der rechtsverletzenden Daten oder eine Kontrolle über sie verschaffen könne. Der EuGH überließ es allerdings dem vorlegenden Gericht zu prüfen, ob eBay in Bezug auf die fraglichen Verkaufsangebote diese aktive Rolle gespielt hat. Diese soll jedenfalls dann vorliegen, wenn die Präsentation der betreffenden Verkaufsangebote optimiert oder diese Angebote beworben werden. Außerdem sei Kenntnis im Sinne des Art. 14 Abs. 1 lit. a E-Commerce-RL bereits dann gegeben, wenn sich ein Hostprovider etwaiger Tatsachen oder Umstände bewusst war, auf deren Grundlage ein sorgfältiger Wirtschaftsteilnehmer die Rechtswidrigkeit hätte feststellen müssen. Das führt im Ergebnis zu einer deutlichen Verschärfung der Internethaftung.

Darüber hinaus hat der Gerichtshof auch die Reichweite der Verantwortlichkeit des Diensteanbieters ausgeweitet. Dem Verletzten muss auch die Durchsetzung zukunftsgerichteter Unterlassungsansprüche möglich sein.[28] Allerdings wurde die Frage offen gelassen, was mit jemandem geschieht, der die Grenzen des Hostprivilegs überschreitet. Ist er dann für alle Inhalte voll verantwortlich? Im Ergebnis ist genau dies anzunehmen. Betreibt der Host-Provider aktives Marketing für die rechtsverletzenden Angebote, verlässt er die Privilegierung des Art. 14 der E-Commerce-RL und ist unter Haftungsgesichtspunkten nach den allgemeinen Regelungen zu beurteilen.[29] Aus deutscher Sicht wäre es außerdem wünschenswert gewesen, wenn der EuGH die Frage nach der Täter- und Störerhaftung thematisiert hätte. Das vom BGH entwickelte Haftungsmodell wurde jedoch mit keinem Wort erwähnt. Insofern ist das Urteil insgesamt enttäuschend.

Allerdings befasste sich der BGH in seinem Urteil „Stiftparfüm"[30] mit der L'Oréal/eBay-Entscheidung des EuGH. Der BGH entschied, dass eBay ab der Kenntnis der Rechtswidrigkeit eines Angebots auf seiner Plattform für dieses verantwortlich sei, und eBay die durch einen Unterlassungsanspruch durchsetzbare Verpflichtung treffe, künftige derartige Verletzungen zu verhindern. Weiter konkretisierte er die Anforderungen an den Hinweis durch den Verletzten, der dem Adressaten die Feststellung des Rechtsverstoßes ermöglichen soll. Im konkreten Falle fehlte es allerdings nach Meinung des BGH an der für den Unterlassungsanspruch erforderlichen Begehungsgefahr. Im Lichte von L'Oréal/eBay ist diese Einschätzung jedoch nicht haltbar, schon die Erstverletzung indiziert die Begehungsgefahr.[31]

2. Scarlet/SABAM

Vier Monate später folgte das Scarlet/SABAM-Urteil.[32] Die belgische Verwertungsgesellschaft SABAM, die sich wenig später auch mit der Klage gegen Netlog hervorgetan hat, beantragte vor dem Tribunal de première instance de Bruxelles eine zwangsgeldbewehrte Anordnung, mit der der Access-Provider Scarlet verpflichtet werden sollte, Rechtsverletzungen abzustellen, die

27) EuGH, 12.07.2011 – C-324/09, WRP 2011, 1129 = MMR 2011, 596 m. Anm. *Hoeren*.
28) *Hacker*, GRUR-Prax 2011, 391, 392.
29) So mit guten Argumenten *Lehment*, WRP 2012, 149, 155.
30) BGH, 17.08.2011 – I ZR 57/09, WRP 2011, 1609 ff. – Stiftparfüm.
31) Dazu *Lehment*, WRP 2012, 149, 157, der sich in seinem Aufsatz ausführlich mit den Konsequenzen der EuGH-Rechtsprechung für das Modell der Täter- und Störerhaftung des BGH befasst.
32) EuGH, 24.11.2011 – C-70/10, MMR 2012, 174 ff.

mittels Inanspruchnahme der Dienste von Scarlet begangen werden.[33] Dies sollte durch die Einrichtung eines Filtersystems geschehen, das die gesamte elektronische Kommunikation über den Provider auf urheberrechtsverletzende Inhalte überprüft. Dieses System sollte präventiv auf alle Kunden von Scarlet Anwendung finden, und zwar zeitlich unbegrenzt auf Kosten des Providers. Die begehrte Anordnung wurde zunächst erlassen. Im Berufungsverfahren legte die Cour d'appel de Bruxelles dem EuGH die Frage vor, ob insbesondere die E-Commerce-RL der Anordnung, eine solches Filtersystem einzurichten, entgegensteht.

Zwar stellte der Gerichtshof unter Hinweis auf das L'Oréal/eBay-Urteil erneut fest, dass es den nationalen Gerichten möglich sein müsse, auch Providern Maßnahmen aufzugeben, die neuen Verletzungen vorbeugen. Allerdings würde die konkrete Anordnung den Provider zu einer allgemeinen Überwachung verpflichten, die nach Art. 15 Abs. 1 der E-Commerce-RL verboten sei. Das Eigentumsrecht, unter das auch das Urheberrecht falle, sei nicht schrankenlos gewährleistet und in ein Gleichgewicht mit anderen Grundrechten zu bringen. Zum einen würde die Anordnung die unternehmerische Freiheit des Providers unverhältnismäßig beeinträchtigen, zum anderen sei nicht ausgeschlossen, dass das System nicht hinreichend zwischen unzulässigen und zulässigen Inhalten unterscheiden könne. Das gefährde die Informationsfreiheit. Außerdem sei der Schutz personenbezogener Daten nicht hinreichend gewährleistet.

Inhaltlich ist die Entscheidung äußerst knapp geraten. Richtigerweise hat der EuGH die in Rede stehende Anordnung als unvereinbar mit der E-Commerce-RL eingestuft. Doch erneut versäumte er es, konkrete Vorgaben zu machen, unter welchen Voraussetzungen und in welchem Umfang den Providern Maßnahmen aufgegeben werden dürfen, die begangene Rechtverletzungen beenden und neue verhindern sollen. Das spielt der Musikindustrie in die Hände, die argumentieren wird, die vorliegende Entscheidung habe über den konkreten Fall hinaus keinerlei Auswirkungen. Bemerkenswert ist allerdings, dass der Gerichtshof diesmal auch auf den Schutz personenbezogener Daten abstellt, der aufgrund der Identifizierung der IP-Adressen der Nutzer gefährdet sei.[34] Noch im L'Oréal/eBay-Urteil stellte der EuGH fest, dass der Verletzer, sofern er im geschäftlichen Verkehr tätig werde, klar identifizierbar sein müsse. Es bleibt weiter unklar, ob gewerblichen Händlern der Datenschutz versagt werden soll. Aber immerhin scheint sich der EuGH mit dieser Entscheidung wieder deutlich an die Existenz der EU-Datenschutzrichtlinie zu erinnern.

3. Netlog/SABAM

Im jüngsten Fall hatte die belgische Musikverwertungsgesellschaft SABAM gegen Netlog NV. geklagt, eine Plattform für soziale Netzwerke im Internet (vergleichbar mit Facebook). SABAM verlangte von Netlog die Einrichtung eines Systems, mit der präventiv Inhalte und Informationen der Dienstenutzer auf verdächtige Dateien hin gefiltert werden konnten. Der EuGH hat eine solche Filterpflicht abgelehnt. Eine solche Überwachung laufe auf eine aktive Beobachtung der von den Nutzern bei dem Betrieb des sozialen Netzwerks gespeicherten Dateien hinaus. Eine solche allgemeine Überwachungspflicht widerspräche der E-Commerce-Richtlinie. Bei einer Güterabwägung zwischen dem Urheberrecht und den Grundrechten von Netlog bemängelt der EuGH die qualifizierte Beeinträchtigung der unternehmerischen Freiheit von Netlog, da dieses Unternehmen verpflichtet werde, ein kompliziertes, kostspieliges, auf Dauer angelegtes IT-System zur Filterung und Überwachung einzurichten. Auch seien die Grundrechte der Nutzer beeinträchtigt, insbesondere deren Rechte auf Datenschutz und freien Empfang oder freie Sendung von Informationen nach der EU-Grundrechte-Charta. Es sei nicht sichergestellt, dass die verlangten Systeme hinreichend zwischen unzulässigen und zulässigen Inhalten unterschieden, so dass auch erlaubte Inhalte eventuell gesperrt würden. Auch seien die Nutzerprofile geschützte personenbezogene Daten, auf die der Zugriff nicht ohne Weiteres möglich sei. Der EuGH wiederholt hier in vielen Passagen das Scarlet/SABAM-Urteil. Er sieht Host- und Access-Provider in einer ähnlichen Lage, was deren Privilegien nach der E-Commerce-Richtlinie angeht. In der Tat wären beide Intermediäre schwerwiegend in ihren Diensterbringungsmöglichkeiten eingeschränkt, wenn man von ihnen auf ihre Kosten solch eine proaktive Überwachung verlangen würde. Die beiden Urteile sind insofern entscheidende Richtungsweiser in Sachen europäischer Netzfreiheit. Gleichzeitig dämmen sie die unerträglichen Begehrlichkeiten der Musikindustrie ein, die alle und jeden für die Einhaltung ihrer urheberrechtlichen Verwerterinteressen in die Verantwortung ziehen möchte.

Anders hat der EuGH allerdings die Verantwortlichkeit eines Host-Providers noch im Fall L'Oréal/eBay gesehen.[35] Dort hatte der EuGH bekanntlich die These aufgestellt, dass ein Host-Provider-Privileg gar nicht gegeben werden könne, wenn jemand über die neutrale Speicherung von Fremdinformationen hinaus eine aktive Rolle bei der Gestaltung seines Dienstes spiele. Auch sei eBay zu mehr als nur der nachträglichen Sperrung konkreter Inhalte verpflichtet, etwa zur Identifizierung und Auskunft über gewerbliche Kunden. Diese Entscheidung beurteilt also die Rolle des Host-Providers anders und führt damit auch zu der Frage der Abgrenzung zwischen Netlog/SABAM und L'Oréal/eBay. Zunächst einmal lässt sich eine Abgrenzung über die unterschiedlichen Rechtsgebiete vornehmen. Markenrechtsverletzungen spielen sich im B2B-Bereich ab, Urheberrechtsverletzungen gehen weit über den Bereich des gewerblichen Handels hinaus. Das Markenrecht kann daher durchaus haftungsmäßig schärfer konturiert sein und gesteigerte Haftungspflichten mit sich bringen. Allerdings unterscheidet die E-Commerce-Richtlinie nicht zwischen Marken- und Urheberrecht, sondern sieht sich als so genannte horizontale Haftungsprivilegierung, also als eine Querschnitts-Regelung, die die Verantwortlichkeit für sämtliche Haftungsbereiche erfassen will. Ein weiterer Unterschied mag aber auch darin liegen, dass eBay eine Sonderrolle im Hostgeschäft spielt, da der Dienst entgeltlich ist und letztendlich über die Plattform hinaus auch als Online-Auktionshaus auftritt. Diese vom EuGH im Fall L'Oréal/eBay so genannte „aktive Rolle" von eBay ist bei Netlog nicht vorhanden. Es handelt sich vielmehr um eine im Kern nicht kommerzielle Plattform für Privatleute, die sich mit ihren Freunden freizeitmäßig z. B. über ihre Interessen austauschen wollen. Darin mag man einen relevanten Unterschied sehen; allerdings findet sich auch dieser nicht in der E-Commerce-Richtlinie angelegt. Eine weitere Möglichkeit zur Abgrenzung kann darauf hinaus laufen, dass man den alten lex posterior-Grundsatz zur Anwendung bringt. Dann hätte der EuGH seine im Juli 2011 noch vorhandene harsche Rechtsprechung durch die beiden späteren SABAM-Entscheidungen aufgelockert. Wie auch immer, es wird in der Haftungsdiskussion jedenfalls spannend bleiben.

33) Beachte zu diesem Urteil auch *Maaßen*, GRUR-Prax 2011, 535.

34) Der EuGH führt aus, dass „eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen des Nutzer" erfolge; „bei diesen Adressen" handele es sich um personenbezogene Daten, die die genaue Identifizierung der Nutzer ermöglichten. Der Verweis auf „diese Adressen" kann sich nur auf die IP-Adressen beziehen, so dass entsprechende Versuche, die Entscheidung anders auszulegen, wenig erfolgversprechend sein dürften. Vgl. dazu auch die Entscheidungsbesprechung von *Meyerdierks*, ZD 2012, 29.

35) EuGH, 12.07.2011 – C-324/09, WRP 2011, 1129 ff. – L'Oréal/eBay.

V. Zusammenfassung und Bewertung

In der Entscheidung Netlog/SABAM knüpft der EuGH an die Scarlet/SABAM-Entscheidung an und übernimmt die Entscheidungsgründe fast vollständig. Dabei war schon bei der Scarlet/SABAM-Entscheidung aufgefallen, dass die Entscheidungsgründe sehr knapp geraten sind. Und so wird auch das jetzige Urteil wieder zu Mutmaßungen anregen, wie weit die Entscheidungsgründe tragen. Die Musikindustrie ihrerseits wird ihre Interpretation des Netlog/SABAM-Falles in die Welt posaunen und darauf abstellen, dass die Entscheidung sehr auf die Besonderheiten des vorliegenden Falles bezogen sei und sich nur auf die „ultimativen" Netzsperren beziehe, die die Klägerin in Belgien in den entsprechenden Rechtsverfahren[36] erlangen wollte. Bei einer differenzierten Verteilung von Kosten und Pflichten könnte das Urteil demzufolge gar nicht zur Anwendung kommen. Dann liest sich die Entscheidung so, dass eine Generalüberwachung des Internets ohne inhaltliche, zeitliche oder personelle Einschränkungen mit Art. 15 der E-Commerce-Richtlinie und dem EU-Grundrecht nicht vereinbar sein soll. Das wäre aber in der Tat keine sehr überraschende Entscheidung, die Vieles verändern würde. Auffällig ist auch, dass der EuGH im Kern bei den Verantwortlichkeiten von Access- und Host-Providern kaum noch differenziert, obwohl es sich hierbei um sehr unterschiedliche Business-Konzepte handelt. In vielen Punkten wurden die Entscheidungsgründe des Scarlet/SABAM-Urteils in der Netlog/SABAM-Entscheidung schlicht wiederholt, obwohl es sich in dem ersten Fall um einen Access- und im zweiten Fall um einen Host-Provider handelte. Zumindest liegt der Schluss nahe, dass die Maßnahmen, die einem Host-Provider nicht zugemutet werden dürfen, erst Recht nicht auf einen Access-Provider Anwendung finden dürfen. Denn diese stellen bloß einen Zugang zur Verfügung, während Host-Provider immerhin fremde Inhalte anbieten. Überdies stellt sich die Frage, wie künftig mit bereits bestehenden Filtersystemen von Host-Providern umgegangen werden soll. Zu denken wäre etwa an das Content-ID System von YouTube oder das Hashtag-Prüfsystem von RapidShare. Der EuGH betont jedenfalls, dass nationale Gerichte den Providern weiterhin Maßnahmen aufgeben können, die „nicht nur die mittels ihrer Dienste (...) begangenen Verletzungen (...) beenden, sondern auch neuen Verletzungen vorbeugen sollen".[37]

Insofern ist zu klären, bis zu welchen Grenzen Host-Provider in die Verantwortung genommen werden können. In seiner Netlog/SABAM-Entscheidung hat der Gerichtshof eine Reihe von Kriterien genannt, die bei der Herstellung eines „angemessenen Gleichgewichts" zwischen dem Schutz der Inhaber von Urheberrechten und dem Schutz der Grundrechte von Personen, die von Filtermaßnahmen betroffen sind, zu berücksichtigen sind.

Die Richtlinie zur Harmonisierung des Urheberrechts[38] sowie die Enforcement-RL[39] sollen den Rechteinhabern einen weitreichenden Schutz gewähren. Nach Art. 8 Abs. 3 der RL zur Harmonisierung des Urheberrechts und Art. 11 Satz 3 der Enforcement-RL müssen die Mitgliedstaaten gewährleisten, dass die Rechteinhaber gerichtliche Anordnungen gegen die Vermittler beantragen können.[40] „Geistiges Eigentum" wird außerdem nach Art. 17 Abs. 2 der EU-Grundrechte-Charta geschützt. Gleichzeitig betont der EuGH, dass die genannten Regelungen bei ihrer Anwendung gegen den Schutz anderer Grundrechte abzuwägen sind.

1. Schutz der unternehmerischen Freiheit

Im Falle des streitigen Filtersystems sah der Gerichtshof die unternehmerische Freiheit in qualifizierter Weise beeinträchtigt. Insbesondere monierte er die Komplexität des Systems, die unbegrenzte Dauer und die hohen Kosten, die ausschließlich vom Host-Provider zu tragen wären. Damit wurden gleich mehrere Kriterien genannt, die im Rahmen von Anordnungen gegen die Vermittler beachtet werden müssen und technischen Maßnahmen gegen Urheberrechtsverletzungen im Internet enge Grenzen setzen.

Eine einseitige Begünstigung der Rechteinhaber wird künftig nicht mehr möglich sein, jedenfalls dürfen die Kosten nicht mehr ausschließlich den Providern auferlegt werden.[41] Das in Deutschland geltende Auskunftsverfahren entspricht der Rechtsauffassung des EuGH. Die Kostentragungslast trifft gem. § 101 Abs. 2 S. 3, Abs. 9 S. 5 UrhG zunächst den Verletzten, also die Rechteinhaber, die die Kosten später direkt bei dem Verletzer als Schaden geltend machen können.[42] Zwar schließt das Urteil die Beteiligung der Provider an den Kosten für die Rechtsverfolgung nicht aus, doch die einseitige Bevorzugung der Musikindustrie ist damit endlich vom Tisch. Maßnahmen gegen Host-Provider müssen außerdem zeitlich befristet und in ihrer praktischen Durchführbarkeit so gestaltet sein, dass deren Kapazitäten und Angebote nicht übermäßig eingeschränkt werden.

2. Datenschutz

Derartige Überprüfungssysteme müssen stets den Schutz der personenbezogenen Daten der Nutzer gewährleisten. Die syste-

36) Cour d'Appel de Bruxelles, Beschluss vom 28.01.2010 – 2007/AR/2424 9ème chambre n° 192; Tribunal de premièreinstance de Bruxelles, 29.06.2007 – 04/8975/A, MMR 9/2007, S. XXI.

37) EuGH, 16.02.2012 – C-360/10, WRP 2012, 429, 432, Rn. 29 – Netlog/SABAM.

38) Richtlinie 2001/29/EG vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

39) Richtlinie 2004/48/EG vom 29.04.2004 zur Durchsetzung der Rechte des geistigen Eigentums.

40) Zur Umsetzung der Enforcement-RL in deutsches Recht siehe *Nordemann*, GRUR 2011, 977, 979.

41) *Hoeren*, Kurzgutachten zur BMWi-Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, S. 15, abrufbar unter: http://politik.eco.de/files2012/03/20120227-Hoeren-eco-Gutachten_final-2702.pdf.

42) BT-Drucks. 16/5048, S. 40.

matische und verdachtsunabhängige Überprüfung jeglicher Profile eines sozialen Netzwerks beeinträchtigt nach Ansicht des Gerichtshofs die Rechte der Nutzer. Gleiches gilt für IP-Adressen im Hinblick auf deren Überprüfung durch Access-Provider, wie der EuGH nochmals unter Verweis auf das Scarlet/SABAM-Urteil betont. Dies liest sich als klarer Hinweis auf die Beachtung des Gebots der Datensparsamkeit, dem folglich im Rahmen gerichtlicher Anordnungen gegen Host-Provider Rechnung getragen werden muss.[43] Jedenfalls kann Art. 11 S. 3 der Enforcement-RL nicht als Ermächtigungsgrundlage für die verdachtsunabhängige Überprüfung aller Nutzerprofile eines sozialen Netzwerks auf mögliche Urheberrechtsverletzungen herangezogen werden. Vor diesem Hintergrund wurden die Möglichkeiten der Musikindustrie weiter eingeschränkt, mit denen sie Host-Provider bei der Verfolgung von Urheberrechtsverstößen ihrer Nutzer zur Verantwortung ziehen können.

3. Informationsfreiheit

Sowohl im Scarlet/SABAM- als auch im Netlog/SABAM-Urteil sah der EuGH ferner die durch Art. 11 der EU-Grundrechte-Charta geschützte Informationsfreiheit gefährdet. Sofern die Rechteinhaber also gerichtliche Maßnahmen gegen Host-Provider zur Verhinderung von Urheberrechtsverletzungen beantragen, müssen die zu verwendenden Systeme so beschaffen sein, dass sie eindeutig zwischen zulässigen und unzulässigen Inhalten unterscheiden können. Nur solche Dateien dürfen gesperrt werden, die tatsächlich einen rechtsverletzenden Inhalt aufweisen. Es stellt sich dann natürlich die Frage, ob überhaupt ein Filtersystem vorstellbar ist, das diesen Anforderungen entspricht. Will man jegliche Blockierung zulässiger Inhalte verhindern, wird wohl eine menschliche Überprüfung der ausgewählten Dateien nötig sein, was aber wiederum die Effizienz des Systems stark beeinträchtigen wird.

VI. Fazit und Ausblick

Die Vorgabe der Gewährleistung eines angemessenen Ausgleichs zwischen den Interessen der Rechteinhaber und denen der Host-Provider sowie der Nutzer schränkt den Umfang möglicher gerichtlicher Anordnungen gegen die Host-Provider erheblich ein. Es gilt, den Schutz der unternehmerischen Freiheit, das Datenschutzrecht sowie den Schutz der Informationsfreiheit in angemessener Weise zu berücksichtigen. Mit den Entscheidungen Scarlet/SABAM und Netlog/SABAM hat der EuGH der einseitigen Bevorzugung der Interessen der Rechteverwerter eine deutliche Absage erteilt. Diese müssen an den entstehenden Kosten beteiligt werden. Darüber hinaus sind nur solche Maßnahmen zulässig, die zeitlich befristet sind. Ebenso widerspricht die verdachtsunabhängige Überprüfung von Nutzerprofilen dem geltenden Datenschutzrecht. Zulässige Inhalte genießen außerdem besonderen Schutz, der nicht durch unausgereifte Filtersysteme unterlaufen werden darf.

Den Begehrlichkeiten dieser so genannten Kreativindustrie ist nach diesen Urteilen dennoch nicht Genüge getan, versuchen die lobbyistischen Strippenzieher dieser Branche doch schon wieder an anderen Stellen und Ecken dieser Welt ihre Interessen unter Ausschluss der Öffentlichkeit durchzusetzen. Erinnert sei hier nur an das Warnhinweismodell in Frankreich (so genanntes HADOPI-System, das mittels einer eigenen Behörde Access-Provider zur Herausgabe der Daten der jeweiligen Nutzer verpflichtet).

Im Rahmen dieses Systems werden die betroffenen Nutzer von HADOPI in einem zweistufigen Verfahren abgemahnt, zunächst per E-Mail dann per Einschreiben. Sofern es bei dem Anschluss zu drei Urheberrechtsverletzungen binnen sechs Monaten kommt, kann der Internetzugang durch richterlichen Beschluss für einen Zeitraum von bis zu einem Jahr gesperrt werden. Auch Großbritannien denkt mit dem Digital Economy Act an die Etablierung eines ähnlichen Systems.[44] Darüber hinaus wird noch in anderen Ländern wie Irland, Schweden, Finnland oder Belgien über Warnhinweismodelle nachgedacht. Zuletzt ist das Warnhinweissystem durch eine sehr umstrittene BMWi-Studie in Deutschland in die Diskussion eingebracht worden.[45] Mit solchen Warn-Träumen sollte jetzt nach den beiden SABAM-Entscheidungen[46] Schluss sein. Denn schließlich erachtet der EuGH einseitige Verpflichtungen von Providern zugunsten der Rechteinhaber als generell unwirksam.

Der BGH könnte schon bald die Gelegenheit erhalten, auf die SABAM-Urteile des EuGH zu reagieren. Das OLG Hamburg modifizierte sein eigenes Haftungsmodell in Bezug auf Host-Provider.[47] Mit Spannung bleibt abzuwarten, ob der BGH im Rahmen einer möglichen Revision die weitgehenden Prüf- und Handlungspflichten, die RapidShare auferlegt wurden, bestätigt, oder ob er diese unter Berücksichtigung der EuGH-Rechtsprechung weiter einschränkt. Insbesondere ist fraglich, ob die unternehmerische Freiheit von RapidShare noch hinreichend gewährleistet wird.

Während in der Europäischen Union der Musikindustrie nun klare Grenzen aufgezeigt wurden, planen die Internet Service Provider in den USA gemeinsam mit den Verbänden der Film- und Musikindustrie gigantische Sperrungsmaßnahmen.[48] Gegen verdächtige Kunden soll durch nervende Warnungen bis hin zur zeitweiligen Deaktivierung des Internet-Zugriffs vorgegangen werden. Tatsächlich werden die ISPs wohl deutlich über die Hälfte der Kosten zu tragen haben. Wirksame Rechtsschutzmöglichkeiten sind für die Kunden nicht vorgesehen. Gegen Zahlung einer Gebühr von 35 US-Dollar könne eine unabhängige Überprüfung des Vorgangs durch Anwälte eingeleitet werden, die aber in keiner Weise rechtlich bindend sei. Diese Entwicklungen gefährden die freie Kommunikation im Internet in einer unerreichten Weise und geben erneut ein erschreckendes Beispiel für die maßlosen Begehrlichkeiten der Rechteverwerter.

43) Vgl. *Hoeren/Franck*, Die Musikindustrie schlägt zweimal zu – Datenschutzrechtliche Überlegungen zu Netzsperren, in: FS Rüßmann (im Erscheinen).

44) Beachte dazu Heise, Meldung vom 06.03.2012, Klage gegen britische Internetsperren endgültig gescheitert, abrufbar unter: http://heise.de/-1464345.

45) *Schwartmann*, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen, abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/warnhinweise-lang,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

46) EuGH, 16.02.2012 – C-360/10, WRP 2012, 429 ff. – Netlog/SABAM; EuGH, 24.11.2011 – C-70/10, MMR 2012, 174 ff – Scarlet/SABAM.

47) OLG Hamburg, 14.03.2012 – 5 U 87/09, n. v.

48) Heise, Meldung vom 15.03.2012, US-Provider sollen Urheberrechtsverletzer „umerziehen", abrufbar unter: http://heise.de/-1473159.