Fachhochschule Köln
Cologne University of Applied Sciences
Fakultät für Wirtschaftswissenschaften
Kölner Forschungsstelle für Medienrecht

Professor Dr. iur. habil. Rolf Schwartmann

Unterausschuss Neue Medien
Öffentliches Gespräch zum Thema
„Vermarktung und Schutz kreativer Inhalte im Internet“
21. Mai 2012, 13.00 Uhr, PLH E.300

Stellungnahme

Fragenkatalog[1]

Teil 1: Modelle zur Versendung von Warnhinweisen (aktuelle Gutachten)

1) Wie bewerten Sie das von Prof. Schwartmann im Rahmen des Wirtschaftsdialogs des BMWi vorgestellte vorgerichtliche Mitwirkungsmodell? Welche Alternativen böten sich aus Ihrer Sicht dazu an? Wie bewerten Sie die Gegenargumentation der Studie „Vergleich von Modellen zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen“ von Prof. Hoeren?

A. Frage 1: Das Modell der vorgerichtlichen Mitwirkung

In der öffentlichen Debatte werden verschiedene Warnhinweismodelle diskutiert. Ähnlich der ACTA-Diskussion erfolgt diese Debatte aber oft nicht auf der Grundlage des im Wirtschaftsdialog tatsächlich diskutierten Modells. So schreibt *Constanze Kurz* in einem Artikel in der FAZ vom 11.5.2012[2]:

> „Daher versucht nun eine heimliche große Koalition, angefeuert von der Inhalteindustrie und neuerdings auch den Kulturschaffenden, ein anderes Warnmodell, auch „Two-Strikes“ genannt, durchzusetzen.
>
> Dieses „Warnmodell“ setzt bei den Internetanbietern an, die Hilfsdienste leisten sollen. Auf die Idee, den Autobauer für die Fahrgewohnheiten seiner Käufer haftbar zu machen, würde zwar niemand kommen. Im Internet soll das aber nach der Logik der zukünftigen großen Stabilitätskoalition anders sein. Das Warnmodell würde die Provider zwingen, ihre Kunden flächendeckend zu überwachen, Filter einzubauen und diejenigen Kunden mahnend anzuschreiben, die sich anschicken, urheberrechtlich geschützte Dateien zu tauschen.

[1] Im Rahmen dieser Stellungnahme werden allein die aus rechtlicher Sicht relevanten Fragen beantwortet.

[2] „Aus dem Maschinenraum. Die neuen Hilfssheriffs der Nation“; abrufbar unter: http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/aus-dem-maschinenraum-die-neuen-hilfssheriffs-des-internets-11746770.html., alle Online-Quellen zuletzt aufgerufen am 14.05.2012.

> Die dabei anfallenden Daten ließen sich nur schwerlich vor dem Zugriff der Abmahnanwälte schützen. Denn was nach der zweiten „Warnung“ passieren würde, ist absehbar: Abmahnungen, Klagen, Prozesse. Und genau darum geht es beim „Warnmodell“: Es sind Pläne zur Privatisierung der Rechtsdurchsetzung. Sind die Internetanbieter erst einmal zum Hilfssheriff degradiert, gibt es keine nennenswerten Hürden mehr, sie auch zur automatischen Datenweiterleitung an die Verwerteranwälte zu zwingen.“

Es ist nicht ersichtlich, dass ein solches Modell ernsthaft rechtspolitisch diskutiert, geschweige denn von einer „heimlichen großen Koalition“ vorangetrieben wird. Das Warnhinweismodell in der BMWi-Studie kann damit nicht gemeint sein. Anderenfalls wäre es völlig unzutreffend beschrieben und dahinter stünde ein grundlegendes Missverständnis des Warnhinweismodells der Studie.[3]

Zur Klarstellung und zum besseren Verständnis soll das Modell der vorgerichtlichen Mitwirkung deshalb noch einmal kurz dargestellt und erläutert werden[4]:

I. Das Modell

1. Schritt: Ermittlung eines Rechtsverstoßes durch den Rechteinhaber

Wie schon zurzeit gängige Praxis, ermitteln vom Rechteinhaber beauftragte Unternehmen Urheberrechtsverletzungen in P2P-Netzwerken.

2. Schritt: Meldung des Rechtsverstoßes an den Provider

Der Rechteinhaber meldet sodann den Verstoß an den Provider unter Übermittlung von Datum, Uhrzeit, IP-Adresse, des geschützten Materials, etc.

3. Schritt: Identifizierung des Anschlussinhabers

Der Provider ordnet die IP-Adresse dem Anschlussinhaber intern zu.

4. Versendung des Warnhinweises

Der Provider sendet dem Anschlussinhaber einen Warnhinweis.

5. Anlegen der Verstoßliste

Der Provider legt eine Verstoßliste zu dem Anschlussinhaber an, auf dem jeder versendete Warnhinweis geführt wird. Die Identität des Nutzers ist dabei zu verschlüsseln.

6. Herausgabe der Verstoßliste

Ab einer gewissen Anzahl versendeter Warnhinweise wird die Verstoßliste entweder automatisiert an Rechteinhaber übermittelt oder kann von diesen herausverlangt werden.

---

[3] Siehe auch noch unten unter C.

[4] Siehe hierzu schon das im Rahmen des Wirtschaftsdialoges des BMWi am 15.03.2012 verteilte Papier, abrufbar unter http://www.medienrecht.fh-koeln.de/Schwartmann_BMWi_Modell%20der%20vorgerichtlichen%20Mitwirkung.pdf.

7. Geltendmachung des Auskunftsanspruchs

Auf Grundlage der Verstoßliste können Rechteinhaber nunmehr nach den bisherigen Voraussetzungen des § 101 UrhG gerichtlich Auskunft über die Identität des Nutzers verlangen.

II. Erläuterungen

1. Erste Neuerung: Sanktionslose Versendung von Warnhinweisen an den Anschlussinhaber - Zugangsanbieter als „Bote“ einer von dem Rechteinhaber behaupteten Urheberrechtsverletzung

- Der Zugangsanbieter ist nach Meldung eines Rechtsverstoßes durch einen Rechtinhaber zur Versendung eines Warnhinweises an seinen Kunden verpflichtet.

- Der Warnhinweis ist **lediglich** eine **Behauptung des Rechteinhabers** (nicht des Zugangsanbieters) gegenüber dem Anschlussinhaber, dass eine Rechtsverletzung stattgefunden hat. Er warnt den Anschlussinhaber zudem, dass er (im Falle weiterer Verletzungshandlungen über seinen Anschluss) mit einer Rechtsverfolgung durch den Rechteinhaber rechnen muss.

- Der Warnhinweis gibt neben der behaupteten Rechtsverletzung auch den geltend machenden Rechteinhaber bekannt. Dieser kann einen Ansprechpartner für den Fall benennen, dass der Anschlussinhaber meint, den Warnhinweis zu Unrecht erhalten zu haben, und dadurch die Kommunikation zwischen Rechteinhaber und Anschlussinhaber eröffnen.

- Der Warnhinweis sollte weitere Informationen zum Sinn und Zweck des Urheberrechts, zu legalen Alternativen zur Nutzung kultureller Inhalte im Internet sowie zur Sicherung des Anschlusses vor der rechtsverletzenden Benutzung durch andere enthalten.

- Der Warnhinweis selbst ist unmittelbar mit **keiner Sanktion** (z. B. Internet-Sperre oder Drosselung des Zugangs) verbunden.

- Der Zugangsanbieter als privater Dritter wird deshalb **nicht** als **„Hilfssheriff“ bei der Durchsetzung der Urheberrechte der Rechteinhaber** tätig, sonder nur als „Bote“.

- Mangels einer mit einem Warnhinweis verbundenen Sanktion bedarf es im Rahmen des Warnhinweisverfahrens keines gerichtsfesten Nachweises einer Urheberechtsverletzung und keiner rechtlichen Prüfung im Einzelfall, ob die behauptete Rechtsverletzung tatsächlich vorliegt. Dementsprechend ist auch kein Rechtsschutz des mit der Behauptung konfrontierten Anschlussinhabers notwendig.

2. Zweite Neuerung: Führen einer „Verstoßliste“ durch den Zugangsanbieter als Sammlung behaupteter Rechtsverstöße

- Der Zugangsanbieter ist verpflichtet, mit jeder Warnhinweisversendung zugleich den Namen des Anschlussinhabers und die behauptete Rechtsverletzung bzw. den Verstoßvorwurf in eine intern geführte Liste aufzunehmen.

- **Ab einer bestimmten Anzahl** von dokumentierten (angeblichen) Urheberrechtsverletzungen über den Anschluss ein und desselben Kunden muss der Provider **dem Rechteinhaber die Liste bekannt geben**.

- Die bekanntgegebene Liste enthält nicht die Klarnamen oder die Anschrift mehrfach „auffällig“ gewordener Anschlussinhaber, sondern ein von dem Zugangsanbieter festgelegtes **Pseudonym**.

- Der Inhaber des betreffenden Anschlusses ist über die Aufnahme in die Verstoßliste sowie die Bekanntgabe der Liste gegenüber dem Rechteinhaber zu informieren.

- Die offen gelegte Verstoßliste gibt lediglich die Behauptung wieder, dass sich hinter den vermeintlichen Rechtsverletzungen dieselbe Person, nämlich zum Beispiel das Pseudonym XY verbirgt. Ob diese Behauptung zutrifft oder nicht, ist in diesem Rahmen nicht zu klären.

- Um in Erfahrung zu bringen, wer sich hinter einem Pseudonym verbirgt, muss der Rechteinhaber den Zugangsanbieter im Wege **richterlicher Anordnung auf Auskunft in Anspruch nehmen**.

3. Verbindung des neuen Warnhinweisverfahrens mit dem bestehenden Auskunftsanspruch und der bestehenden zivilrechtlichen Rechtsverfolgung als Sanktion

- Das **Warnhinweisverfahren** ist **einem Auskunftsersuchen** gegenüber Zugangsanbietern und einer Rechtsverfolgung gegenüber Anschlussinhabern **vorgeschaltet**, so dass zum Beispiel kostenpflichtige Abmahnungen erst nach einem (oder mehreren) Warnhinweis(en) zulässig wären.

- Der Rechteinhaber kann **aus der Verstoßliste ersehen**, **welche** (unter einem Pseudonym geführte) **Person besonders häufig oder gravierend Urheberrecht verletzt** haben soll und auf dieser Basis seinen Auskunftsanspruch gegen den Provider gezielt auf relevante Fälle in gewerblichem Ausmaß beschränken.

4. Beibehaltung des bisherigen richterlichen Auskunftsanspruchs des Rechteinhabers gegenüber dem Zugangsanbieter und der zivilrechtliche Rechtsverfolgung gegenüber dem Rechteinhaber

- Will der Rechtinhaber seine Rechte durchsetzen, muss er auch nach dem vorgerichtlichen Mitwirkungsmodell den (vermeintlichen) Rechtsverletzer abmahnen (§ 97a UrhG) oder auf Unterlassung oder Schadensersatz in Anspruch nehmen (§ 97 UrhG). Er ist dafür darlegungs- und beweispflichtig.

- Um an den Klarnamen und die Adresse des Anschlussinhabers als (vermeintlichen) Rechtsverletzer zu gelangen, muss der Rechteinhaber zuvor im Wege richterlicher Anordnung den Zugangsanbieter auf Auskunft in Anspruch nehmen (§ 101 Abs. 1, 2 und 9 UrhG), der allein in der Lage ist, eine ermittelte IP-Adresse einem Kunden zuzuordnen und damit die entsprechenden Angaben zu liefern. Danach besteht **schon heute** eine **Mitwirkungspflicht des Zugangsanbieters**.

III. Bewertung des Modells

1. Regelungsziel

Hierzu heißt es in der BMWi-Studie[5]:

> „Das Regelungsziel des vorgerichtlichen Mitwirkungsmodells ist es, Urheberrechtsverstöße im Internet zu verhindern oder zu reduzieren und Bewusstsein für den Wert geistigen Eigentums als zentrale Voraussetzung der kulturellen und wirtschaftlichen Basis des Staates zu schaffen oder wieder herzustellen. Ziel ist es dementsprechend, den Urheberrechtsschutz durch ein Mittel zu stärken, das *nicht unmittelbar* mit einer rechtlichen Konsequenz verbunden ist, sondern das zunächst insbesondere durch Aufklärung Bewusstsein für die Illegalität von nicht autorisierten Downloads im Internet schafft.“[6]

Denn das Unrechtsbewusstsein bei der Nutzung illegaler Angebote im Internet hat sich, so weiter in der BMWi-Studie[7]:

> „[…] in weiten Teilen der Bevölkerung noch nicht durchgesetzt. Die Ursachen hierfür sind vielschichtig. Ein wesentlicher Grund ist die Komplexität des Urheberrechts. Nutzer können nicht jede Erscheinungsform und jede Handlung sicher rechtlich einordnen. Hinzu kommt der Eindruck beim Nutzer, dass Inhalte im Netz einen geringeren Schutz beanspruchen können, als verkörperte Gegenstände. Strukturprobleme entstehen dadurch, dass anders als in der körperlichen Welt, die Technik massenhaften, unautorisierten und unbezahlten Konsum von Inhalten ermöglicht. Die Grenze zwischen legal und illegal ist im Internet schwer zu ziehen, weil vieles janusköpfig ist: Was technisch gleich funktioniert kann rechtlich unterschiedlich zu bewerten sein und umgekehrt.“[8]

Insofern bewirkt die Versendung eines Warnhinweises durch den Zugangsanbieter, dass Anschlussinhaber vor einer kostenpflichtigen Abmahnung (§ 97a UrhG) sowie einer Inanspruchnahme auf Unterlassung und Schadensersatz (§ 97 UrhG) sanktionslos aufgeklärt und verwarnt werden. Der Anschlussinhaber wird zunächst nur darauf hingewiesen, dass über seinen Anschluss Rechtsverletzungen begangen wurden und er die Möglichkeit hat, diese Tätigkeiten einzustellen.

2. Defizite des gegenwärtigen Rechtsschutzes

Das geltende Recht gibt den Rechteinhabern mit dem Auskunftsanspruch gegenüber dem Zugangsanbieter nach § 101 UrhG und der sich daran anschließenden Möglichkeit, den Verletzer kostenpflichtig abzumahnen sowie auf Unterlassung und Schadensersatz in Anspruch zu nehmen, Mittel zur Rechtsdurchsetzung an die Hand. Die geltende Rechtslage ist aber aus verschiedenen Gründen unbefriedigend.

Zunächst läuft der Auskunftsanspruch der Rechteinhaber häufig leer, da die Zugangsanbieter nach § 100 Abs. 1 TKG zur Speicherung der zur Auskunftserteilung erforderlichen Daten lediglich berechtigt, nicht aber verpflichtet sind.

---

[5] BMWi-Studie, S. 303.

[6] Siehe hierzu auch *Schwartmann* in GRUR 2012, 158, 161.

[7] BMWi-Studie, S. 303.

[8] Vgl. hierzu ausführlich *Schwartmann* in K&R Beihefter 2/2011, S.22.

Zudem verlangt der Auskunftsanspruch nach § 101 UrhG ein „gewerbliches Ausmaß“, das hinsichtlich der für die Rechtsverletzung genutzten Dienstleistung des Zugangsanbieters (§ 101 Abs. 2 Nr. 3 UrhG) und – nach h. M. – auch hinsichtlich der rechtsverletzenden Tätigkeit selbst vorliegen muss. Nicht geklärt ist dabei allerdings die Frage, wann die Rechtsverletzung ein „gewerbliches Ausmaß“ erreicht.[9] So wird etwa teilweise vertreten, dass ein „gewerbliches Ausmaß“ in der Regel nur in Betracht kommt, wenn das geschützte Werk innerhalb der relevanten Verwertungsphase von bis zu 6 Monaten nach der Veröffentlichung in einer Internettauschbörse angeboten wird.[10]

Vor allem aber, und darauf kommt es wesentlich an, werden Anschlussinhaber mit Kostenforderungen konfrontiert, die häufig als unverhältnismäßig empfunden werden. Mit der Abmahnung und dem Anspruch auf Aufwendungsersatz nach § 97a UrhG wird in der Regel auch Schadensersatz nach § 97 Abs. 2 UrhG geltend gemacht. Da bei Urheberrechtsverletzungen in P2P-Netzwerken Fälle des unberechtigten öffentlichen Zugänglichmachens verfolgt werden (nämlich die unautorisierte Freigabe von geschütztem Material für andere zum Download) ist Berechnungsgrundlage für den Schadensersatz grundsätzlich die angemessene Lizenzgebühr (§ 97 Abs. 2 S. 3 UrhG). Zuzüglich der Anwaltsgebühren sehen sich Anschlussinhaber deshalb erheblichen Forderungen ausgesetzt. Diese werden gegen sie geltend gemacht unabhängig davon, ob sie selbst den Rechtsverstoß begangen haben oder etwa andere Haushaltsmitglieder mit Zugang zum Anschluss (z. B. ein mittelloses, minderjähriges Kind), und unabhängig davon, ob sie bspw. zum ersten Mal illegales Filesharing betrieben haben oder ob es sich um notorische Rechtsverletzer handelt. Die gegenwärtige Rechtslage differenziert insoweit nicht hinreichend und erscheint daher unausgewogen bzw. unangemessen.

Schließlich dürfte die präventiv-verhaltenssteuernde Wirkung, die von den derzeitigen Rechtsschutzmöglichkeiten der Rechteinhaber ausgeht, als eher gering einzuschätzen sein. Sie setzt voraus, dass der betreffende Anschlussinhaber in der konkreten Situation eine Rechtsverletzung überhaupt für möglich und gegebenenfalls auch eine Rechtsdurchsetzung für wahrscheinlich hält. Nach rechtstatsächlichem Befund ist allerdings zumindest ersteres keineswegs immer der Fall.[11]

3. Vor- und Nachteile des vorgeschlagenen Modells

Das Modell der vorgerichtlichen Mitwirkung beschneidet die Rechtsschutzmöglichkeiten der **Rechteinhaber** nach gegenwärtigem Rechtsstand insoweit, als Nutzer/Anschlussinhaber zunächst ohne Sanktion Warnhinweise erhalten. Weil das Warnhinweisverfahren dem Auskunftsanspruch und der zivilrechtlichen Rechtsverfolgung vorgeschaltet ist, kann der Rechteinhaber also nicht schon bei erstmaliger Urheberechtsverletzung kostenpflichtig abmahnen. Er muss es hinnehmen, dass „folgenlos“ das Warnhinweisverfahren durchlaufen wird. Allerdings macht das Modell den Rechtschutz auch effektiver, indem es den Auskunftsanspruch über die Verstoßliste mit dem Warnhinweisverfahren verbindet.

Die BMWi-Studie führt hierzu aus:

> „Das vorgeschlagene Modell effektiviert also das bestehende System von Auskunftsanspruch und nachfolgender zivilrechtlicher Durchsetzung des urheberrechtlichen Anspruchs gegenüber dem Nutzer. Die Zugangsanbieter trifft zum einen die Pflicht, Warnhinweise an die Anschlussinhaber zu versenden, deren IP-Adresse im Zusammenhang mit

[9] Siehe dazu im Einzelnen mit Nachweisen der uneinheitlichen instanzgerichtlichen Rechtsprechung die Ausführungen der BMWi-Studie, S. 255 ff.

[10] OLG Köln, GRUR-RR 2012, 227, 228.

[11] Vgl. BMWi-Studie, S. 43 ff.

> der gemeldeten Rechtsverletzung ermittelt wurde. Zum anderen müssten sie, eine gegenüber Dritten anonymisierte Verstoßliste führen und diese ab einer bestimmten Anzahl von festgehaltenen Verstößen, dem Rechteinhaber bekannt zu geben. Dieser kann dann, wie bisher, im Wege eines gerichtlichen Auskunftsverlangens Namen und Anschrift des Rechteinhabers heraus verlangen."[12]

Der besondere Nutzen der Verstoßliste liegt also darin, dass der Rechteinhaber hieraus ersehen kann, welche für ihn anonyme Person häufig oder gravierend Urheberrecht verletzt hat. Auf dieser Basis kann er seinen Auskunftsanspruch gegen den Provider gezielt mit Blick auf solche Fälle beschränken, in denen seine Rechte mehrfach verletzt wurden. Insoweit lässt sich dann auch ohne Schwierigkeiten feststellen, ob eine Rechtsverletzung im „gewerblichen Ausmaß" vorliegt.

Im Hinblick auf die **Anschlussinhaber** ist festzustellen, dass diese im Rahmen des Warnhinweisverfahrens zwar mit der unter Umständen unzutreffenden Behauptung einer Urheberrechtsverletzung konfrontiert werden. Auf der anderen Seite sehen sie sich nicht unvermittelt einer kostenpflichtigen Abmahnung sowie gegebenenfalls einem Schadensersatzanspruch ausgesetzt. Nach Aufklärung und (mehrfacher) Warnung erscheinen diese scharfen Mittel nicht unangemessen. Das Warnhinweisverfahren kommt dabei in erster Linie solchen Anschlussinhabern zugute, die in Unkenntnis der Rechtslage oder der tatsächlichen Umstände urheberrechtswidrig handeln oder über deren Anschluss ohne Wissen andere Personen Urheberrechtsverletzungen begehen. Würde einer Abmahnung ein sanktionsloser Warnhinweis vorausgehen, so könnten zum Beispiel Eltern Maßnahmen gegen das illegale Verhalten ihrer Kinder ergreifen; erstmalige Filesharer könnten ihr Verhalten einstellen, bevor die vollen Konsequenzen der zivilrechtlichen Rechtsdurchsetzung sie träfen. Somit wäre es möglich Fälle zu vermeiden, in denen die kostenintensive Abmahnung als besonders unverhältnismäßig empfunden wird. Nutzern, die bewusst gegen Urheberrecht verstoßen, wird mit den Warnhinweisen und der Verstoßliste immerhin deutlich gemacht, dass sie einer zivilrechtlichen Inanspruchnahme entgegensehen, wenn sie ihr Verhalten nicht ändern.[13] Filesharer, die trotz Erhalt eines oder mehrerer Warnhinweise ihr rechtswidriges Verhalten fortsetzten, träfen die erheblichen Rechtsfolgen damit jedenfalls nicht unvorbereitet. Falls sie dann auf Schadensersatz in Anspruch genommen werden (§ 97 Abs. 2 UrhG), wird in der Regel das notwendige Verschulden anzunehmen sein.

Zugangsanbietern wird die Pflicht auferlegt, auf Mitteilung von Rechtsverletzungen Warnhinweise zu versenden und eine Verstoßliste zu führen. Über die Kostentragungslast ist dabei nicht entschieden.

Das Warnhinweisverfahren nach dem vorgeschlagenen Modell wird insoweit zu einer Entlastung der **Gerichte** führen, als Anschlussinhaber bereits nach Aufklärung und Warnung ihr Verhalten ändern. Da der Zugangsanbieter im Rahmen des Warnhinweisverfahrens anders als für eine Abmahnung und weitere Rechtsverfolgung dem Rechteinhaber keine Auskunft erteilen und dieser daher keine gerichtliche Anordnung nach § 101 Abs. 9 UrhG erwirken muss, werden schon die hierfür zuständigen Landgerichte nicht beansprucht.[14]

B. Frage 2: Alternativen zum vorgerichtlichen Mitwirkungsmodell

I. Versendung von Warnhinweisen durch die Rechteinhaber

[12] BMWi-Studie, S. 305.

[13] BMWi-Studie, S. 306.

[14] Über den Auskunftsanspruch entscheidet gem. § 101 Abs. 9 S. 3 eine mit drei Richtern besetzte Kammer des Landgerichts.

Eine nach Veröffentlichung der BMWi-Studie viel diskutierte Alternative ist die Versendung eines Warnhinweises durch die Rechteinhaber selbst. Denn schon nach geltender Rechtslage könnten die Rechteinhaber anstelle einer Abmahnung zunächst einen sanktionslosen Warnhinweis versenden. Dieses Vorgehen entspräche einem durch die Rechteinhaber selbst durchgeführten Warnhinweisverfahren.

Das Warnhinweisverfahren nach dem Modell der vorgerichtlichen Mitwirkung soll einem Verfahren auf Auskunftserteilung nach § 101 UrhG und einer sich daran anschließenden Rechtsverfolgung durch den Rechteinhaber gegenüber einem Anschlussinhaber vorgeschaltet sein. Denn schon die erfolgreiche Geltendmachung des gerichtlichen Auskunftsanspruchs stellt die Rechteinhaber in der Praxis vor hohe Hürden. Sie ist zudem kostenintensiv. Die erfolgreiche Geltendmachung des Auskunftsanspruchs wäre aber Voraussetzung vor einer Versendung eines Warnhinweises durch Rechteinhaber. Dabei bestehen die oben aufgeführten Probleme der fehlenden Datenspeicherung der Zugangsanbieter sowie der Vorraussetzung des „gewerblichen Ausmaßes“ der Rechtsverletzung nach § 101 Abs. 1 UrhG. Würde die Geltendmachung des gerichtlichen Auskunftsanspruchs der Warnhinweisversendung vor- anstatt gegebenenfalls nachgelagert, blieben die angestrebten Vorteile des schnelleren, unkomplizierteren und kostengünstigeren Warnhinweisverfahrens, das zudem zu einer spürbaren Entlastung der nach § 101 Abs. 9 UrhG zuständigen Gerichte führen dürfte, aus.

Die Versendung von Warnhinweisen durch die Rechteinhaber würde einen freiwilligen Rechtsverzicht ihrerseits voraussetzen, ohne dass dabei die Zugangsanbieter im Rahmen ihrer technischen Möglichkeiten in die Verhinderung von Rechtsverletzungen eingebunden würden. Dies liefe dem Anliegen, Urheberrechtsverletzungen im Internet durch eine Kooperation von Rechtinhabern und Zugangsanbietern zu begegnen, zuwider. Die Versendung von Warnhinweisen durch die Rechteinhaber ist daher keine geeignete Alternative.

II. Anspruch auf Versendung eines Warnhinweises gegen den Zugangsanbieter

Eine weitere Alternative wäre die Schaffung eines Anspruchs der Rechteinhaber gegen die Zugangsanbieter, der sie berechtigt, anstelle der Auskunftserteilung die Versendung eines Warnhinweises zu verlangen. Dabei wäre kein Verfahren der mehrfachen Warnhinweisversendung zu durchlaufen, sondern die Rechteinhaber könnten jeweils entscheiden, ob sie wegen einer Rechtsverletzung Auskunft **oder** die Versendung eines Warnhinweises verlangen.

Der Vorteil dieses Verfahrens wäre, dass keine Verstoßliste bei den Providern geführt werden müsste. Dies ist unter datenschutzrechtlichen Gesichtspunkten begrüßenswert, aufgrund der grundrechtlichen Sensibilität dieses Bereichs und dem darauf basierenden Gebot der Datensparsamkeit. Außerdem bedürfte es nicht der Schaffung einer entsprechenden Ermächtigungsgrundlage für die Datenverwendung. Erwogen worden ist, ob die Aufnahme in die Verstoßliste eine Beschwer für den Betroffenen bedeutet, gegen die dann Rechtsmittel vorgesehen werden müssten. Dies wäre bei dem Alternativvorschlag entbehrlich. Allerdings wird nach dem vorgeschlagenen Modell der vorgerichtlichen Mitwirkung der Betroffene mit seiner Aufnahme in die Liste schon nicht beschwert. Denn diese stellt nur eine unter einem Pseudonym geführte Sammlung der von den Rechteinhabern bloß behaupteten Rechtsverletzungen dar, mit der selbst keine Sanktion verbunden ist.

Ein deutlicher Nachteil dieser Alternative gegenüber dem vorgerichtlichen Mitwirkungsmodell besteht darin, dass ohne die Führung der Verstoßliste und das Durchlaufen eines mehrstufigen Warnhinweis-

verfahrens die anschließende zivilrechtliche Verfolgung nicht gezielt auf besonders hartnäckige Rechtsverletzer beschränkt werden könnte.

C. Frage 3: Bewertung der Argumente des eco-Auftragsgutachtens

Zu den im eco-Auftragsgutachten vorgebrachten Argumenten, ist eine Stellungnahme unter http://www.medienrecht.fh-koeln.de/Schwartmann_StN_eco-Auftragsgutachten15032012.pdf abrufbar. Es beruht in wesentlichen Teilen auf Missverständnissen, worauf insbesondere *Agnes Krumwiede*, Sprecherin für Kulturpolitik Bündnis 90/Die Grünen hingewiesen hat[15]:

> „In falsche Kontexte gestellte Fachgutachten wirken manipulativ und dürfen nicht den notwendigen breiten gesellschaftlichen Diskussionsprozess im Interessenausgleich zwischen UrheberInnen und NutzerInnen bestimmen.“, so lautet ihr Fazit.

Auf folgende Punkte soll an dieser Stelle gesondert eingegangen werden:

I. Keine Privatisierung der Rechtsdurchsetzung

Im eco-Auftragsgutachten wird die Ansicht vertreten, durch das vorgerichtliche Mitwirkungsmodell werde die Rechtsdurchsetzung im Hinblick auf Urheberrechtsverletzungen im Internet privatisiert. Wörtlich heißt es:

> „Das von den Verfassern der BMWi-Studie vorgeschlagene Warnhinweismodell führt im Kern dazu, dass Private Befugnisse erhielten, die eigentlich (Strafverfolgungs-)Behörden oder den Gerichten vorbehalten sein sollten.“[16]

Eine etwaige „Privatisierung der Rechtsdurchsetzung“ ist indes kein Ergebnis der BMWi-Studie. Für Kunden von Internetzugangsanbietern sind mit einem Warnhinweis sowie der Aufnahme in die Verstoßliste und selbst mit deren Bekanntgabe gegenüber dem Rechteinhaber unmittelbar gerade **keine Rechtsfolgen** verbunden. Ein Provider als privater Dritter erlangt durch den Ansatz keine Befugnis, Urheberrechte durchzusetzen. Er ist lediglich verpflichtet, die seitens der Rechteinhaber aufgestellte Behauptung einer Rechtsverletzung über die ermittelte IP-Adresse an den betreffenden Anschlussinhaber zu übermitteln bzw. weiterzuleiten. Da Zugangsanbieter bei der Warnhinweisversendung nur als **„Boten“** tätig werden, bedarf es in diesem Stadium keines gerichtsfesten Nachweises einer Urheberrechtsverletzung.[17] Auch der Postbote überbringt eine fremde Nachricht, offen für die Post, ohne dass er oder das Postunternehmen mit deren Inhalt in Verbindung gebracht werden.
Auch eine rechtliche Einzelfallprüfung, ob tatsächlich eine solche Rechtsverletzung vorliegt, kann mangels eines rechtlich erheblichen Vorwurfes nicht erfolgen. Die Rechtsdurchsetzung beginnt erst und nur dann, wenn der Rechteinhaber wie nach dem geltenden Recht mit richterlicher Hilfe Auskunft über Klarnamen und Anschrift erhält, um sodann zivilrechtliche Ansprüche gegenüber dem Anschlussinhaber geltend zu machen. Insoweit ergibt sich also keine Änderung gegenüber der derzeitigen Rechtslage, und eine Verlagerung der Rechtsdurchsetzung auf Private wird durch das vorgerichtliche Mitwirkungsmodell nicht veranlasst. Wenn die Aufklärung durch den ersten oder zweiten Hinweis greift, kommt es dazu ohnehin nicht mehr.

---

[15] Pressemittelung vom 5. März 2012, abrufbar unter http://www.medienrecht.fh-koeln.de/20120321_PM%20Die%20Gruenen%20BMWi_eco.pdf.

[16] eco-Auftragsgutachten, S.10.

[17] *Schwartmann* in GRUR 2012, 158, 160.

II. Kein Unterlaufen der Voraussetzungen des § 101 UrhG

Das eco-Auftragsgutachten kritisiert, dass im Rahmen der Auskunftserteilung nach dem vorgerichtlichen Mitwirkungsmodell die Voraussetzungen des gerichtlichen Auskunftsanspruchs nach § 101 UrhG unterlaufen würden. Danach

> „widerspricht das Warnhinweismodell dem [...] Institut des Auskunftsverfahrens nach § 101 UrhG. Denn im Gegensatz zu der dortigen Formulierung wird in dem Warnhinweismodell keine Gewerbsmäßigkeit verlangt. […] Das Warnhinweismodell würde daher das gesetzlich geregelte Auskunftsverfahren – das gem. § 101 Abs. 9 UrhG nicht ohne Grund unter Richtervorbehalt steht – unterlaufen."

Das trifft nicht zu, denn durch das Warnhinweismodell werden die Voraussetzungen des gerichtlichen Auskunftsanspruchs nach § 101 Abs. 2 und 9 UrhG nicht berührt. Am Ende des Warnhinweisverfahrens steht die Geltendmachung des Auskunftsanspruchs nach § 101 Abs. 9 UrhG, dessen Voraussetzungen unverändert bleiben. Hierzu heißt es in der BMWi-Studie:

> „[Der Auskunftsanspruch] soll aber nur den zivilrechtlichen Ausgleich zwischen Rechteinhaber und Nutzer ermöglichen, der mit Hilfe des vorhandenen gerichtlichen Auskunftsanspruchs vorbereitet wird."[18] […] „[Der Rechteinhaber] kann dann, wie bisher, im Wege eines gerichtlichen Auskunftsverlangens Namen und Anschrift des Nutzers heraus verlangen."[19]

Ob eine Klarstellung der in der gerichtlichen Praxis weit ausgelegten Voraussetzungen des Auskunftsanspruchs erfolgen soll, ist eine vom vorgerichtlichen Mitwirkungsmodell unabhängige Entscheidung des Gesetzgebers.

III. Auslegung der EuGH-Entscheidung „Scarlet-Extended"

Zur Auslegung von „*Scarlet-Extended*"[20] stellt das eco-Auftragsgutachten zutreffend fest:

> „Aus dem Umstand, dass der EuGH nicht ausdrücklich entschieden hat, dass auch ein Warnhinweismodell rechtswidrig sei, lässt sich nicht das Gegenteil schließen. Der EuGH war in der fraglichen Rechtssache schlicht nicht dazu berufen."[21]

Sodann leitet das eco-Auftragsgutachten seinerseits aus dem Urteil die Unzulässigkeit eines Warnhinweismodells ab:

> „Obgleich sich das Scarlet-Urteil auf sogenannte „Netzsperren" bezieht, sind beide Ansätze doch ähnlich gelagert. Denn aus Sicht des Zugangsanbieters macht es keinen grundlegenden Unterschied, welche Pflichten ihm im Detail auferlegt werden, sofern sie von ihren Auswirkungen auf den Zugangsanbieter vergleichbar sind. […] [Daraus] lässt sich […] erkennen, dass der EuGH die einseitige Verpflichtung von Providern zu Gunsten der Rechteinhaber als generell unwirksam erachtet."[22]

---

[18] BMWi-Studie, S. 304.

[19] eco-Auftragsgutachten, S.10.

[20] EuGH v. 24.11.2011, C-70/10.

[21] eco-Auftragsgutachten, S.19.

[22] eco-Auftragsgutachten, S.20.

Diese Deutung findet in dem Urteil keine Stütze. Tatsächlich führt der EuGH in Sachen *Scarlet-Extended* folgendes aus:

> „Wie aus […] *Promusicae*[23], hervorgeht, ist der Schutz des Grundrechts auf Eigentum, zu dem die an das geistige Eigentum anknüpfenden Rechte gehören, gegen den Schutz anderer Grundrechte abzuwägen.[24] […] [D]ie nationalen Behörden und Gerichte [haben] im Rahmen der zum Schutz der Inhaber von Urheberrechten erlassenen Maßnahmen ein angemessenes Gleichgewicht zwischen dem Schutz dieses Rechts und dem Schutz der Grundrechte von Personen, die von solchen Maßnahmen betroffen sind, sicherzustellen […].[25] Im vorliegenden Fall bedeutet die Anordnung der Einrichtung des streitigen Filtersystems jedoch, dass im Interesse dieser Rechteinhaber sämtliche elektronischen Kommunikationen im Netz des fraglichen Providers überwacht werden, wobei diese Überwachung zudem zeitlich unbegrenzt ist, sich auch auf jede künftige Beeinträchtigung bezieht und nicht nur bestehende Werke schützen soll, sondern auch Werke, die zum Zeitpunkt der Einrichtung dieses Systems noch nicht geschaffen waren.[26] […] [Es] steht nämlich fest, dass die Anordnung, das streitige Filtersystem einzurichten, eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um geschützte personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen.“[27]

Die BMWi-Studie leitet daraus ab, dass der EuGH ausdrücklich nur das streitige Filtersystem für unzulässig hält. Andere Maßnahmen ohne Überwachung der vom Diensteanbieter übermittelten Informationen, könnten aber im Rahmen einer Abwägung der berechtigten Interessen der Beteiligten zulässig sein.[28] Die Zulässigkeit eines Warnhinweismodells wurde in dieser Entscheidung nicht behandelt.

Anders als im eco-Auftragsgutachten vertreten, unterscheidet sich ein Warnhinweismodell jedoch grundlegend von dem streitgegenständlichen System in *„Scarlet Extended“*. Die Entscheidung basiert in diesem Punkt wesentlich auf Art. 15 Abs. 1 Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr.[29] Hiernach dürfen Mitgliedstaaten Diensteanbietern keine allgemeinen Verpflichtungen auferlegen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Warnhinweismodelle, wie das vorgeschlagene, erfordern keine Überwachung in diesem Sinne. Sie verlangen von den Diensteanbietern gerade nicht die Überprüfung und Kontrolle übermittelter Informationen. Die „Überwachung“ zur Aufspürung von Rechtsverletzungen wird von Seiten der Rechteinhaber durchgeführt, die aber nicht Diensteanbieter im Sinne der Richtlinie sind. Zudem fehlt es für sie an einer rechtlichen Verpflichtung, sie sind zu diesem Vorgehen nur berechtigt. Diensteanbieter empfangen demgegenüber „passiv“ die Meldung von Rechtsverstößen. In der Versendung eines Warnhinweises durch Diensteanbieter liegt ebenfalls keine „Überwachung“ in diesem Sinne. Der Diensteanbieter übermittelt dem Anschlussinhaber lediglich die Meldung eines vom Rechteinhaber behaupteten Verstoßes. Die

[23] EuGH v. 29.01.2008, C-275/06.

[24] EuGH v. 24.11.2011, C-70/10, Rz. 44.

[25] EuGH v. 24.11.2011, C-70/10, Rz. 45.

[26] EuGH v. 24.11.2011, C-70/10, Rz. 47.

[27] EuGH v. 24.11.2011, C-70/10, Rz. 51.

[28] BMWi-Studie, S.279 f.

[29] Umgesetzt in § 7 Abs. 2 TMG.

Verpflichtung des Providers bezieht sich also nicht auf eine Überwachung zur Ermittlung von Rechtsverstößen, sondern allein auf die Identifizierung des Anschlussinhabers.[30]

IV. Sach- und Verantwortungsnähe der Zugangsanbieter

Im Rahmen einer Angemessenheitsprüfung wird im eco-Auftragsgutachten

> „die besondere Sach- und Verantwortungsnähe der Zugangsanbieter"

zu den Rechtsverletzungen der Anschlussinhaber verneint. Hierzu heißt es:

> „Die Annahme, dass Zugangsanbieter eine strukturbedingte Nähe zu Urheberrechtsverletzungen ihrer Kunden aufweisen, weil sie diese technisch ermöglichen, [ist] schon grundsätzlich abwegig. Dieser Logik folgend, wäre beinahe jedem Unternehmen eine Verantwortung für Verletzungen der Rechtsordnung durch ihre Kunden zurechenbar."[31]

Die besondere Sachnähe des Zugangsanbieters zur Rechtsverletzung seiner Anschlussinhaber ist eine Tatsache. Diese hat der deutsche Gesetzgeber bereits mit Schaffung des Auskunftsanspruchs nach § 101 UrhG anerkannt. Auch hier besteht ein Anspruch der Rechteinhaber gegen den Provider aufgrund einer Rechtsverletzung eines Dritten, an welcher der Provider nicht schuldhaft mitgewirkt, sondern lediglich die technischen Mittel bereitgestellt hat.

Es ist insoweit zwischen einer Verpflichtung zur Mitwirkung bei der Verhinderung von Rechtsverletzungen und einer haftungsbegründenden Verantwortung zu unterscheiden. Dabei handelt es sich um eine Einschränkung der Berufsfreiheit, die im Wirtschaftsverwaltungsrecht an der Tagesordnung ist (z.B. Produktverantwortung im Umweltrecht).[32] Das eco- Auftragsgutachten verkennt hier, dass es bei der Inpflichtnahme des Zugangsanbieters nicht um eine rechtliche Verantwortlichkeit im Sinne einer Störerhaftung geht, die auf einer Verletzung von Prüfungspflichten beruht. Entscheidend ist, ob sich auf die Nähe des Zugangsanbieters zur Rechtsverletzung durch seinen Kunden eine Inpflichtnahme der Provider zur Warnhinweisversendung und Listenführung stützen lässt, die angemessen erscheint.

Der Gemeinschaftsgesetzgeber löst diese Problematik auf, indem er den Mitgliedstaaten gestattet, einen „angemessenen Ausgleich" zu schaffen, der Gerichten und Verwaltung erlaubt, von Providern das Abstellen oder Verhindern von Rechtsverletzungen zu verlangen, solange der Diensteanbieter nicht selbst für die Rechtsverletzung haftet.[33] Nach Art. 12 Abs. 1 und 2 Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (E-Commerce RL)[34] darf ein Internetzugangsanbieter nicht für die von ihm übermittelten Inhalte verantwortlich gemacht werden, soweit er keine weitere Verbindung zu ihnen oder dem veranlassenden Nutzer aufweist. Eine Verantwortlichkeit würde dazu führen, dass der Provider, neben oder anstelle des eigentlichen Rechtsverletzers, Schadensersatz an den Verletzten zahlen muss oder dass ein Anspruch auf vorbeugendes Unterlassen besteht. Im Gegensatz dazu begründet das Warnhinweismodell keine Störerhaftung der Provider. Die Möglichkeit, unter bestimmten Voraussetzungen vom Provider zu verlangen, dass dieser eine Rechtsverletzung verhindert oder zu-

[30] So auch: High Administrative Court, [2011] EWHC 1021 (Admin), par. 116 ff.

[31] eco-Auftragsgutachten, S. 24.

[32] *Schwartmann* in GRUR 2012, 158, 160.

[33] High Administrative Court, [2011] EWHC 1021 (Admin), par.103. Mit dieser Wertung hinsichtlich der Inpflichtnahme auch das Bundesverfassungsgericht im Hinblick auf die Verpflichtung von Telekommunikationsunternehmen zur Speicherung von Kommunikationsdaten. BVerfGE 125, 260ff., BMWi Studie, S.310.

[34] Umgesetzt in § 8 TMG.

künftige gleichgelagerte Rechtsverletzungen abstellt, ist in diesem Rahmen zulässig. Denn der Provider wird nicht entgegen Art. 12 E-Commerce RL für die „übermittelten Informationen“ verantwortlich gemacht. Er wird lediglich verpflichtet, die allein ihm gegebenen technischen Möglichkeiten zu ergreifen, um gegen Rechtsverstöße Dritter vorzugehen.

V. Schaffung einer Ermächtigungsnorm zur Datenverarbeitung

Das eco-Auftragsgutachten nimmt schließlich zu Fragen der datenschutzrechtlichen Einwilligung Stellung. So heißt es:

> „Da es an einer gesetzlichen Ermächtigung mangelt, wäre die einzig übrige Alternative für das in der BMWi-Studie vorgeschlagene Warnhinweismodell eine Einwilligung der Anschlussinhaber zur Verwendung ihrer Verkehrsdaten“.[35]

Dies ist eine Fehldeutung, denn das Modell der vorgerichtlichen Mitwirkung kommt datenschutzrechtlich nicht ohne gesetzliche Eingriffsermächtigung aus. Datenschutzrechtlich relevante Eingriffe bedürfen der Einwilligung oder einer gesetzlichen Ermächtigung. Dazu heißt es in der BMWi-Studie:

> „Ausgehend von der Klassifizierung der IP-Adresse als personenbezogenes Datum bedürfte es für alle datenschutzrechtlich relevanten Handlungen einer gesetzlichen Grundlage“. […] „Die Diensteanbieter wären in diesem Zusammenhang dazu verpflichtet, nicht nur Bestands-, sondern auch Verkehrsdaten, namentlich die IP-Adresse und den Zeitpunkt des Zugriffs, ihrer Anschlusskunden zu speichern und gegebenenfalls einer berechtigten Person herauszugeben. Datenschutzrechtlich und, soweit einschlägig, vor dem Hintergrund der Gewährleistung des Fernmeldegeheimnisses zulässig ist dies nur dann, wenn eine entsprechende Ermächtigungsgrundlage hierzu vorliegt.“[36]

2) Welche Vor- und Nachteile sehen Sie für Ihre Branche hinsichtlich einer möglichen Umsetzung eines vorgerichtlichen Mitwirkungsmodells im Gegensatz zum heute üblichen Vorgehen einer sofortigen Abmahnung unter Nutzung des Auskunftsanspruchs aus § 101 UrhG?

-

3) Das vorgerichtliche Mitwirkungsmodell würde vor allem bei P2P-Filesharing greifen. Man geht davon aus, dass dieser Bereich 20 % der Urheberrechtsverletzungen ausmacht. Hat sich die Nutzung von dezentralen Kopierbörsen durch das Zurückdrängen von Streamhosting-Angeboten wie kino.to oder Megaupload wieder erhöht?

-

4) Welchen Beitrag leisten die Netzwerkprovider zur Bewusstseinsstärkung und Rechtsdurchsetzung im Falle von Urheberrechtsverletzungen? Wie bewerten Sie die Forderungen aus Wirtschaft und Politik, dass diese einen Beitrag auch aus Gründen der Corporate Social Responsibility leisten sollten?

In die Rechtsdurchsetzung sind die Zugangsanbieter im Wege des gerichtlichen Auskunftsanspruchs nach § 101 Abs. 9 UrhG von Gesetzes wegen eingebunden. Dazu sind sie berechtigt, dynamische IP-Adressen bis zu 7 Tagen zu speichern, aber nicht hierzu verpflichtet. Manche Zugangsanbieter, wie

[35] eco-Auftragsgutachten, S. 35.

[36] BMWi-Studie, S. 300.

bspw. die Deutsche Telekom, unterstützen die Rechteinhaber bei der Rechtsdurchsetzung, indem sie von der 7-tägigen Speicherungsberechtigung in vollem Umfang Gebrauch machen. Andere Zugangsanbieter begegnen dem Auskunftsersuchen der Rechteinhaber mit dem Einwand, die Daten würden nicht oder nur kurzzeitig gespeichert, so dass deren Anspruch ins Leere läuft.

Die Forderung nach einer stärkeren Einbeziehung der Zugangsanbieter ist zu begrüßen. Eine Mitwirkung der Zugangsanbieter ist aus technischen und strukturellen Gründen erforderlich, aber auch aus Gründen des Gemeinwohls.[37]

5) Welche Konsequenzen hätte die Implementierung von Filter- und Analysetechniken in die Netzwerke hinsichtlich Vertraulichkeit und Integrität von Datenübertragungen aus Ihrer Sicht?

-

6) Welche Filtermaßnahmen werden bisher von den Diensteanbietern – vertraglich oder standardisiert – vorgenommen? Gibt es bereits eine Deep-Packet-Inspection?

-

7) Sind sie der Auffassung, dass ein Warnhinweismodell bzw. ein vorgerichtliches Mitwirkungsmodell angesichts der damit einhergehenden Grundrechtseingriffe auf freiwilliger Basis im Rahmen einer Selbstregulierung umgesetzt werden könnte oder sollte dies auf gesetzlicher Grundlage erfolgen?

Die Grundrechte sind grundsätzlich Abwehrrechte gegen staatliche Maßnahmen. Grundrechtseingriffe durch den Staat bedürfen bei Wesentlichkeit einer gesetzlichen Ermächtigung. Bei einer freiwilligen Verpflichtung der Zugangsanbieter sind diese in ihren Grundrechten nicht betroffen.

Telekommunikationsvorgänge sind grundrechtlich über das Fernmeldegeheimnis des Art. 10 Abs. 1 GG vor staatlicher Kenntnisnahme geschützt. Über § 88 TKG wird das grundrechtliche Fernmeldegeheimnis einfachgesetzlich auf Telekommunikationsunternehmen auch im Verhältnis zu ihren Kunden ausgeweitet. Daher stellt sich die Frage, ob im Rahmen eines freiwilligen Warnhinweismodells die insoweit grundrechtlich betroffenen Anschlussinhaber der Verwendung ihrer Daten zustimmen können. Im Ergebnis wäre eine freiwillige Beteiligung aller Anschlussinhaber wohl nicht umsetzbar. Es bedürfte ihrer freiwilligen Einwilligung, die weder in AGB noch konkludent erfolgen dürfte.[38]

Das Fernmeldegeheimnis schützt Kommunikationsvorgang, -inhalt und -umstände.[39] Die freiwillige Umsetzung des vorgerichtlichen Mitwirkungsmodells würde eine Datenverwendung erfordern, die dieses Recht berührt. Diese Datenverwendung ist nach den geltenden §§ 96ff. TKG nicht zulässig. Es bedürfte hier insofern auch bei einer freiwilligen Umsetzung zwischen Zugangsanbietern und Rechteinhabern der Schaffung entsprechender Ermächtigungsgrundlagen. Insofern wäre in dieser Hinsicht der Gesetzgeber gefragt.

[37] Vgl. BVerfGE 7, 377, 406.

[38] Siehe hierzu ausführlich eco-Auftragsgutachten, S. 35 f.

[39] BVerfGE 125, 260, 309, m.w.N.

8) Wie bewerten sie das „vorgerichtliche Mitwirkungsmodell“ im Hinblick auf seine verfassungsrechtliche und europarechtliche Vereinbarkeit?

Eine vollständige rechtliche Bewertung kann nur anhand eines konkreten Gesetzesentwurfs erfolgen und würde zudem den hier zur Verfügung stehenden Rahmen sprengen. Folgende Aspekte sollen hier jedoch knapp erörtert werden:

A. Verfassungsrechtliche Vereinbarkeit

I. Eingriff in Grundrechte der Zugangsanbieter

1. Art. 12 GG

Zur verfassungsrechtlichen Vereinbarkeit des vorgerichtlichen Mitwirkungsmodells mit Art. 12 GG wird in der Studie ausgeführt[40]:

> „Während der Schutz des geistigen Eigentums über Art. 14 Abs. 1 GG gewährt wird, ist ein Warnhinweismodell unter Mitwirkung der Zugangsanbieter insbesondere an deren Berufsfreiheit aus Art. 12 Abs. 1 GG zu messen. Verfassungsrechtlich betrachtet, handelt es sich um eine Inpflichtnahme Privater zur Aufgabenerfüllung.
>
> a) Voraussetzungen einer Inpflichtnahme Privater
>
> Die Verpflichtung zur Versendung von Warnhinweisen durch Zugangsanbieter ist als Berufsausübungsregelung einzuordnen, weil sie „die eigentliche Berufstätigkeit als Grundlage der Lebensführung unberührt lässt“[41] und in den Schutzbereich von Art. 12 Abs. 1 GG einzuordnen ist. Ob es sich bei der Versendung von Warnhinweisen um eine staatliche oder private Aufgabe handelt kann *dahin stehen, weil die Verfassung keine kategorische Trennung von „Staatsaufgaben“ und „privaten* Aufgaben“ kennt und dem Gesetzgeber einen weiten Gestaltungsspielraum zuerkennt, „welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt.“[42] Bei der Entscheidung welche Private er in Dienst nimmt, hat der Staat einen weiten Beurteilungsspielraum. Anbieter öffentlich zugänglicher Telekommunikationsdienste können etwa verpflichtet werden, die Daten ihrer Kunden für sechs Monate zu speichern.[43] Die Frage der Entschädigung und Kostenverteilung im Rahmen der Indienstnahme bedürfte einer eingehenden Prüfung, nachdem eine Abschätzung der Kosten möglich ist. Eine einseitige Kostentragungspflicht zu Lasten der Provider, ohne dass die Rechteinhaber an den Kosten beteiligt werden, wäre aber unverhältnismäßig.
>
> b) Eingriff in die Berufsfreiheit
>
> Ein Eingriff in die Berufsausübungsfreiheit unterliegt nach der Dreistufentheorie des Bundesverfassungsgerichts der Schranke des Übermaßverbotes. Er ist zulässig, wenn er in einem vernünftigen Verhältnis zu dem gegebenen Anlass und dem damit verbundenen Zweck steht. Das ist bei einer Berufsausübungsregelung der Fall, wenn sich „vernünftige Gründe des Gemeinwohls dafür finden lassen. Gesichtspunkte der Zweckmäßigkeit sind

[40] BMWi-Studie, S. 310 ff.

[41] BVerfGE 75, 246, 274.

[42] Vgl. BVerfGE 109, 64, 85; BVerfGE 125, 260, 261 f.

[43] Vgl. BVerfGE 95, 173, 187.

ausreichend, wenn die Regelung für die Betroffenen zumutbar und nicht übermäßig belastend ist".[44]

Bei der Abwägung ist nach einem legitimen Zweck des Eingriffs, sowie nach seiner Eignung und Erforderlichkeit zur Erreichung des Zwecks zu fragen, so wie nach dessen Zumutbarkeit für den Betroffenen. Einen **legitimen Zweck** würde das staatliche Handeln im Wege eines vorgerichtlichen Mitwirkungsmodells allein deswegen verfolgen, weil Urheberrechtsverletzungen im Internet urheberrechtswidrig sind. Bei der Frage nach der **Eignung** eines Eingriffs in Rechtsgüter hat der Gesetzgeber einen weiten Entscheidungsspielraum. Die Grenze zur Verfassungswidrigkeit ist überschritten, wenn Maßnahme sich als offensichtlich oder schlechthin ungeeignet darstellt. Auch wenn die Wirksamkeit von Warnhinweisen noch nicht abschließend geklärt ist, lässt diese sich jedenfalls grundsätzlich nicht ausschließen. Die Eignung der Maßnahme ist danach zu beurteilen, ob das Mittel einen Schritt in die richtige Richtung weist. Die kurzzeitigen Erfahrungen aus Frankreich und Irland erlauben nur begrenzt Rückschlüsse auf die Effizienz von Warnhinweisen. Während für Irland keine Daten verfügbar sind, ist die Peer-to-Peer-Nutzung in Frankreich zwischen April 2010 und April 2011 um insgesamt 31 Prozent gesunken, wobei ein deutlicher Einbruch zum Zeitpunkt der Versendung der ersten Warnhinweise zu verzeichnen war. Eine Untersuchung für Schweden hat ergeben, dass die Furcht vor Sanktionen von Internetpiraterie zu einem Rückgang von Urheberrechtsverletzungen im Internet führt, mit der ein Anstieg des Umsatzes legaler Angebote einher ging. Dieser Effekt ließ nach, nachdem von einer Durchsetzung von Sanktionen abgesehen wurde. Der Eignung des vorgerichtlichen Mitwirkungsmodells steht eine Beschränkung auf P2P-Netzwerke nicht entgegen, weil über diese Nutzungsform weltweit mit 16,37 Prozent die mit Abstand meisten unautorisierten Downloads erfolgen. Im Vereinigten Königreich geht man von 37 Prozent der Urheberrechtsverletzungen im Internet durch illegales P2P-Filesharing aus während in Deutschland von etwa 20 Prozent ausgegangen werden kann.

Das Übermaßverbot verpflichtet den Staat dazu, sich bei den Bürger belastenden Maßnahmen auf das Notwendige zu beschränken. Im Rahmen der **Erforderlichkeitsprüfung** ist nach Mitteln zu suchen, die das Ziel des Staates bei gleicher Wirksamkeit weniger belasten. Als Handlungsvarianten kommen ein Vorgehen ohne Mitwirkung der Zugangsanbieter, ein Agieren nur im Rahmen des Auskunftsanspruchs, eine sanktionslose Versendung von Warnhinweisen sowie eine anlasslose Warnhinweise und Netzsperren in Betracht.

Ein Vorgehen im Wege von Warnhinweisen ohne Mitwirkung der Zugangsanbieter wäre tatsächlich unmöglich, da die Zuordnung von durch die Rechteinhaber ermittelten Daten allein durch die Zugangsanbieter erfolgen kann. Ein Auskunftsanspruch als alleiniges Mittel entfaltet seine aufklärende Wirkung erst im Zusammenhang mit einer gerichtlichen Inanspruchnahme und ist damit nicht präventiv. Zudem ist dieses Mittel schärfer als das hier vorgeschlagene Mittel, weil es nicht auf Warnung zielt. Das Vorgehen im Rahmen des Auskunftsanspruchs mag zwar im Verhältnis zum Zugangsanbieter milder sein; es ist aber mit Blick auf das Regelungsziel nicht ebenso effektiv wie das hier vorgeschlagene Modell und im Verhältnis zum Nutzer schärfer. Ein völlig ohne Blick auf eine Konsequenz – also den Auskunftsanspruch - gerichtetes Warnhinweismodell wäre zwar milder, aber nicht effektiv. Auch das anlasslose Versenden von standardisierten Informationen durch die Zugangsprovider an ihre Kunden, in denen auf das Verbot von Urheberrechtsverstößen ohne konkreten Anlass hingewiesen wäre nicht effektiv, weil es für den Nutzer allein mit einer „Belästigung" verbunden wäre. Ob eine anlasslose Warnung angesichts einer Vielzahl täglich eingehender Emails überhaupt die Wahrnehmungsebene des Nutzers erreichen würde ist fraglich. Netzsperren sind nicht vom Gegenstand der vorliegenden Studie. Sie würden zwar möglicherweise ein effektiveres Mittel zur Aufklärung über

[44] Vgl. BVerfGE 7, 377, 406.

und die Bekämpfung von Rechtsverletzungen im Internet sein, sind aber wegen der mit ihnen verbundenen rechtlichen Härten in Hinblick auf inhaltliche Zensur von Inhalten und ihre datenschutzrechtliche Eingriffsintensität keineswegs grundrechtsschonender und damit im Verhältnis zum vorgerichtlichen Mitwirkungsmodell kein milderes Mittel.

Abschließendes Kriterium des Verhältnismäßigkeitsgrundsatzes ist die **Angemessenheit** oder auch der Verhältnismäßigkeit im engeren Sinne, die auch Zumutbarkeit genannt wird. In deren Rahmen werden Zweck und Mittel in Relation gestellt. Bei der Frage nach der Zumutbarkeit des mit dem hier vorgeschlagenen Modell verbundenen Eingriff in die Kundenbeziehung zwischen Zugangsanbieter und Nutzer sind die Nähe der in die Pflicht genommenen Zugangsanbieter zur Rechtsverletzung und deren vertraglichen Befugnisse im Verhältnis zum Anschlussinhaber im Falle des Rechtsmissbrauchs zu berücksichtigen. Eine besondere Nähe der Zugangsanbieter zur Rechtsverletzung liegt insofern auf der Hand, als sie diese technisch über ihr Angebot ermöglichen. Das Vertrauensverhältnis zum Kunden würde durch ein Warnhinweismodell deshalb nicht in unzumutbarer Weise gestört, als nach den im Privatkundengeschäft geltenden AGB der großen in Deutschland tätigen Internet-Service-Provider die Kunden diesem gegenüber vertraglich dazu verpflichtet, bei Inanspruchnahme der Leistung bestehende Gesetze, insbesondere Urheberrechte bzw. Rechte Dritter einzuhalten. Die Vertragsbedingungen sehen vor, dass der Provider im Falle einer Pflichtverletzung berechtigt ist, den Zugang zum Internet zu sperren und/oder den Vertrag fristlos zu kündigen. Die Voraussetzungen für ein solches Recht variieren dabei im Einzelnen. Ist für die Internetnutzung eine Flatrate vereinbart, steht nach dem Provider vielfach das Recht zu, die Geschwindigkeit der Datenübertragung für den Rest des Abrechnungszeitraums zu drosseln, falls der Kunde das ihm nach dem Tarif für diesen Zeitraum zustehende Datenvolumen überschritten hat. Ein Sonderkündigungsrecht des Kunden oder eine Reduzierung des zu leistenden Entgelts ist für den Fall einer solchen Sperre des Anschlusses oder Drosselung der Übertragungsgeschwindigkeit nicht vorgesehen. Nach dem hier vorgeschlagenen Ansatz stehen derartige vertraglich vorgesehenen und im Vergleich zum vorgerichtlichen Mitwirkungsmodell schärferen Maßnahmen wie Sperrung, Kündigung oder Drosselung durch den Zugangsanbieter in Folge von Urheberrechtsverletzungen nicht in Rede. Die Inpflichtnahme von Zugangsanbietern zur Mitwirkung im Rahmen eines vorgerichtlichen Mitwirkungsmodells in diesem Rahmen ist daher zumutbar.

Insgesamt wäre der Eingriff in das Grundrecht der Berufsfreiheit der Zugangsanbieter mit der im Rahmen des vorgerichtlichen Mitwirkungssystem vorgeschlagenen Inpflichtnahme vor dem Hintergrund von Art. 12 GG verfassungsrechtlich nicht zu beanstanden."

2. Art. 14 GG

Ein Eingriff in Art. 14 GG kommt unter dem Gesichtspunkt des „Rechts am eingerichteten und ausgeübten Gewerbebetriebs" in Betracht. Ob allerdings Art. 14 GG überhaupt das Recht am eingerichteten und ausgeübten Gewerbebetrieb schützt, ist umstritten[45] und wurde vom Bundesverfassungsgericht bislang offen gelassen.[46] Bejaht man dies, so könnte eine gesetzliche Regelung, die den Zugangsanbietern durch das Warnhinweismodell verursachte Kosten auferlegt, einen Eingriff in Art. 14 GG bedeuten. Ein solcher Eingriff ist als Inhaltsbestimmung zulässig, wenn er verhältnismäßig ausgestaltet wird. Dies kann beispielsweise durch eine angemessene Beteiligung der Rechteinhaber an den entstehenden Kosten erfolgen.[47]

[45] Siehe hierzu ausführlich *Wieland* in *Dreier*, Grundgesetz Kommentar, Art. 14, Rn. 50 ff.; *Axer* in *Epping/Hillgruber*, Beck`scher Online-Kommentar GG, Art. 14, Rn. 51ff.

[46] BVerfGE 105, 252, 278; BVerfG NVwZ 2009, 1426, 1428; BVerfG NJW 2010, 3501, 3502.

[47] Siehe zur Kostenverteilung im Rahmen des gesetzlichen Warnhinweismodells im Vereinigten Königreich BMWi-Studie, S. 128 ff.

II. Eingriff in Grundrechte der Anschlussinhaber

1. Art. 10 GG

Art. 10 Abs. 1 GG gewährleistet das Fernmeldegeheimnis, welches die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunkationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt.[48] Im Zuge der Privatisierung des Fernmeldewesens wurde der Schutz einfachgesetzlich in § 88 TKG gegenüber Diensteanbietern ausgeweitet.[49] § 88 TKG ist daher entsprechend Art. 10 GG auszulegen.[50]

Geschützt sind neben dem Inhalt der Kommunikation auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen, Telekommunikationsverkehr stattgefunden hat.[51]

Im Rahmen des vorgerichtlichen Mitwirkungsmodells wären verschiedene Vorgänge erforderlich, die einen Eingriff in diesen Schutzbereich darstellten. So wäre die kurzzeitige Speicherung der IP-Adresse mit den jeweiligen Vergabezeitpunkten und Benutzerkennungen erforderlich, wie sie den Zugangsanbietern schon nach geltendem Recht gestattet, aber nicht verpflichtend ist. Dies wäre zunächst eine anlasslose Speicherung, die datenschutzrechtlich besonders schwer wiegt. Die bloße Speicherung der IP-Adresse stellt aber noch keinen schwerwiegenden Grundrechtseingriff dar.[52] Der BGH entschied hierzu, da die Identität des jeweiligen Nutzers nicht erkennbar sei, sei die Persönlichkeitsrelevanz gering.[53] Der Eingriff sei daher von geringer Intensität, so der BGH.

In einem nächsten Schritt im Rahmen des Warnhinweismodells wäre die identifizierende Zuordnung dynamischer IP-Adressen vonnöten. Diese fällt in den Schutzbereich des Fernmeldegeheimnisses.[54] Denn die Zuordnung erfordert Zugriff und Auswertung der gespeicherten Verkehrsdaten, die dem Schutz des Telekommunikationsgeheimnisses unterliegen. Diese hält das Bundesverfassungsgericht für zulässig, wenn eine hinreichend normenklaren Entscheidung des Gesetzgebers getroffen wird, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt werden soll.[55]

Auch das Anlegen der Verstoßliste betrifft das Telekommunikationsgeheimnis, da Zeitpunkt und Art des Verstoßes dokumentiert werden, welche Inhalt und Umstände der Kommunikation betreffen.

Solche Eingriffe sind nur aufgrund einer gesetzlichen Ermächtigung zulässig. Auch hier bedarf es einer hinreichend bestimmten, ausdrücklichen und verhältnismäßigen Normierung, die die Voraussetzungen der Datenverwendung festlegt, wie sie die §§ 96 ff. TKG bereits für andere Fälle enthalten.

---

[48] BVerfGE 125, 260, 309, m.w.N.

[49] *Eckhardt* in *Spindler/Schuster*, Recht der elektronischen Medien, § 88 TKG, Rn. 2.

[50] *Eckhardt* a.a.O., Rn. 4.

[51] BVerfGE 125, 260, 309, m.w.N.

[52] Vgl. BVerfGE 121, 1, 20.

[53] BGH MMR 2011, 341, 344.

[54] BVerfG, Beschluss v. 24.01.2012 – 1 BvR 1299/05, Rz. 173.

[55] BVerfG, Beschluss v. 24.01.2012 – 1 BvR 1299/05, Rz. 174.

2. Art. 2 i.V.m Art. 1 GG

Das Recht auf informationelle Selbstbestimmung aus Art. 2 i.V.m. Art. 1 GG ist gegenüber dem Fernmeldegeheimnis subsidiär.[56]

B. Europarechtliche Vereinbarkeit

I. Charta der Grundrechte der europäischen Union

Die gesetzliche Regelung eines Warnhinweismodells würde einen Eingriff in Art. 16 EU-Grundrechtecharta gegenüber den Zugangsanbietern darstellen. Die Anschlussinhaber wären in datenschutzrechtlichen Grundrechten aus Art. 8 und Art. 11 EU-Grundrechtecharta betroffen. Eine entsprechende gesetzliche Regelung müsste verhältnismäßig ausgestaltet werden.

II. EU-Grundfreiheiten

Eine gesetzliche Regelung zur Warnhinweisversendung würde nur im Inland tätige Zugangsanbieter berechtigen und verpflichten. Da dies die Dienstleistungsfreiheit nach Art. 56 AEUV berührt, wäre die Regelung entsprechend vertragskonform auszugestalten.

III. Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (E-Commerce RL)

1. Art. 15 E-Commerce RL

Nach Art. 15 Abs. 1 Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr (E-Commerce RL) dürfen Mitgliedstaaten Diensteanbietern keine allgemeinen Verpflichtungen auferlegen, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Nach Abs. 2 können die Mitgliedstaaten Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten, oder dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können.

Diensteanbieter können demnach nicht verpflichtet werden, eine anlassunabhängige (sog. proaktive) Kontrolle der von ihnen übermittelten oder gespeicherten Informationen vorzunehmen.[57] Aus diesem Grund hatte der EuGH in der Entscheidung „*Scarlet Extended*“[58] das streitgegenständliche Filtersystem für unzulässig erklärt.[59] Die Anforderung an den Zugangsanbieter zur Versendung eines Warnhinweises auf Meldung eines Rechteinhabers im Rahmen des vorgeschlagenen Warnhinweismodells verlangt keine Überwachung in diesem Sinne. Denn sie erfordert gerade nicht die Überprüfung und Kontrolle übermittelter Informationen. Die „Überwachung“ zur Aufspürung von Rechtsverletzungen wird von Seiten der Rechteinhaber durchgeführt. Diese sind aber keine Diensteanbieter im Sinne der Richtlinie. Zudem sind diese auch hierzu nicht rechtlich verpflichtet, sondern lediglich berechtigt. Die Zugangsanbieter empfangen nur „passiv“ die Meldung der Rechtsverstöße. Die Versendung eines Warnhinweises durch den Zugangsanbieter ist ebenfalls keine „Überwachung“ in diesem Sinne. Der

[56] *Kühling/Seidel/Sivridis*, Datenschutzrecht, S.64.

[57] *Altenhain* in MüKo zum StGB, § 7, Rn.6.

[58] EuGH v. 24.11.2011, C-70/10.

[59] Siehe hierzu oben unter Frage 1)C.III.

Zugangsanbieter berichtet nur gegenüber dem Anschlussinhaber die Meldung eines Rechtsverstoßes durch einen Rechteinhaber.[60] Das Wissen, dass der Provider hierbei möglicherweise über das Nutzungsverhalten eines Anschlussinhabers erlangt, ist nicht das Ergebnis seiner „Überwachung", sondern das Nebenprodukt einer von der Überwachung unabhängigen anderweitigen Verpflichtung. Die Verpflichtung des Providers bezieht sich nicht auf die Überwachung zur Ermittlung von Rechtsverstößen, sondern lediglich auf die Identifizierung eines bereits als Rechtsverletzer festgestellten Anschlussinhabers.[61]

2. Art. 12 E-Commerce RL

Nach Art. 12 Abs. 1 und 2 E-Commerce RL darf ein Internetzugangsanbieter nicht für die von ihm übermittelten Inhalte verantwortlich gemacht werden, soweit er keine weitere Verbindung zu ihnen oder dem veranlassenden Nutzer aufweist. Nach Abs. 3 lässt Artikel 12 die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.

Die Haftungsprivilegierung beruht darauf, dass sich die Tätigkeit des Dienstanbieters auf rein technische, nicht von ihm veranlasste, automatisch ablaufende Vorgänge beschränkt, bei denen er keine Kenntnis von den durchgeleiteten oder kurzzeitig zwischengespeicherten Informationen erlangen oder dieselben kontrollieren kann.[62] Art. 12 der Richtlinie soll einen angemessen Ausgleich zwischen den Interessen der Rechteinhaber, welche sich bestmöglichen Schutz ihrer urheberrechtlichen Produkte wünschen, und den Interessen der Provider, welche eine möglichst effiziente Datenübermittlung gewährleisten und dabei so wenig wie möglich für die übermittelten Inhalte verantwortlich gemacht werden wollen, schaffen.[63] Die Frage der Verantwortlichkeit für übermittelte Informationen stellt sich immer dann, wenn eine andere Person als der Provider selbst, geschütztes Material über den Dienst des Providers unrechtmäßig öffentlich zugänglich macht oder herunterlädt. Es ist dann fraglich, ob auch der Provider als bloßer Übermittler der Daten für die Rechtsverletzung verantwortlich gemacht werden kann. Eine Verantwortlichkeit könnte dazu führen, dass der Provider Strafe oder Schadensersatz an den Verletzten zahlen muss oder dass ein Anspruch auf vorbeugendes Unterlassen besteht. Eine solche Haftung träfe ihn neben einer anderen Person oder nachrangig für den Fall, dass der eigentliche Rechtsverletzer nicht aufgefunden werden kann, es zu umständlich wäre, ihn zu ermitteln oder er insolvent ist. Ein Warnhinweissystem begründet indes keine solche Verantwortlichkeit. Kommt ein Zugangsanbieter seinen Verpflichtungen aus der gesetzlichen Regelung zur Warnhinweisversendung nicht nach, so verstößt er damit gegen das Gesetz und ihn treffen die entsprechenden Konsequenzen (z.B. in der Warnhinweisregelung selbst vorgesehene Sanktionen für die Nicht-Einhaltung oder wettbewerbsrechtliche Rechtsfolgen). Er würde aber nicht haften in dem von Art. 12 Abs. 1 E-Commerce RL verfolgten Sinn, dass er für die Rechtsverletzungen anderer verantwortlich gemacht würde. Denn den Zugangsanbieter trifft keine solche Verantwortung. Er wird lediglich verpflichtet, seine technischen Möglichkeiten zu ergreifen, um an der Verhinderung von Rechtsverstößen Dritter mitzuwirken.

---

[60] Siehe hierzu schon oben unter 1)C.III.

[61] So auch: High Administrative Court, [2011] EWHC 1021 (Admin), par.118.

[62] BT-Drs. 14/6098, S.24 zu § 9 TDG.

[63] High Administrative Court, [2011] EWHC 1021 (Admin), par.100.

IV. Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums (Enforcement-RL)

Art. 3 Abs. 1 RL 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums bestimmt, dass Maßnahmen, Verfahren und Rechtsbehelfe der Mitgliedstaaten, die zur Durchsetzung der Rechte des geistigen Eigentums erforderlich sind, fair und gerecht sein müssen. Außerdem dürfen sie nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen.

In der Entscheidung „*Scarlet Exteneded*" entschied der EuGH (und bestätigte dies in „*SABAM*"[64]), dass die Verpflichtung eines Diensteanbieters ein kompliziertes, kostspieliges, auf Dauer angelegtes und allein auf seine Kosten betriebenes Informatiksystem einzurichten, gegen die Voraussetzungen des Art. 3 Abs. 1 der Richtlinie 2004/48 verstieße.[65]

Diesen Anforderungen wäre bei gesetzlicher Ausgestaltung des Warnhinweismodells hinreichend Rechnung zu tragen, insbesondere im Wege einer Kostenbeteiligung der Rechteinhaber.

V. Novellierung der Richtlinie zur Durchsetzung der Rechte am geistigen Eigentum (IPRED)

Aufgrund von rechtspolitischen Initiativen wie dem Grünbuch „Erschließung des Potenzials der Kultur- und Kreativindustrien" oder dem Gallo-Bericht arbeitet die EU-Kommission derzeit an der Novellierung der Richtlinie zur Durchsetzung der Rechte am geistigen Eigentum (IPRED). Sie erwägt unter anderem ein schärferes Vorgehen gegen Webseiten mit Inhalten, die gegen Urheberrechte verstoßen. Ob auch ein Warnhinweismodell in Betracht gezogen wird, ist derzeit noch unklar. Jedenfalls aber soll die „Kooperation" zwischen Rechteinhabern und Zugangsanbietern verstärkt werden. Ein offizieller Vorschlag zur Novellierung der Richtlinie soll im September dieses Jahres erfolgen.

VI. Europäisches Datenschutzrecht

1. Datenschutzrichtline 2002/58/EG für elektronische Kommunikation (E-Privacy RL)

Neben der allgemeinen Datenschutzrichtline 95/46/EG existiert speziell für den Bereich der Telekommunikation die E-Privacy RL, die den EU-Mitgliedstaaten einen Rechtsrahmen für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Anbieten elektronischer Kommunikationsdienste vorgibt.[66]

Nach Art. 5 Abs. 1 der Richtlinie 2002/58/EG haben die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen.

[64] EuGH, Urt. V. 16.02.2012 - C-360/10, Rz. 46.

[65] EuGH, Urt. v. 24.11.2011, C-70/10, Rz. 48.

[66] Vgl. die Zusammenfassung der EU, abrufbar unter:
http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_de.htm.

Für Verkehrsdaten gilt gemäß Art. 6 der Richtlinie 2002/58/EG der Grundsatz, dass diese zu löschen oder zu anonymisieren sind, sobald sie für die Übertragung einer Nachricht bzw. für die Gebührenabrechnung nicht mehr benötigt werden.

Ausnahmen von diesem Grundsatz lässt Art. 15 Abs. 1 der Richtlinie 2002/58/EG zu. Danach können die Mitgliedstaaten Rechtsvorschriften erlassen, nach denen die Verkehrsdaten aus bestimmten Gründen länger aufbewahrt werden müssen.

Die Voraussetzungen für eine solche weitergehende Speicherpflicht sind danach:

- Erlass einer nationalen Ermächtigungsgrundlage.

- Die Speicherung darf nur aufgrund der Gründe gem. Art. 13 Abs. 1 der Richtlinie 95/46/EG erlaubt werden: für die nationale Sicherheit, (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen (vgl. Art. 15 Abs. 1 2002/58/EG).

Art. 15 Abs. 1 der RL 2002/58/EG verweist insoweit auf Art. 13 Abs. 1 der RL 95/46/EG, dennoch stimmen die in beiden Vorschriften aufgezählten Gründe nicht vollständig überein. So enthält Art. 15 Abs. 1 der Richtlinie 2002/58/EG etwa zusätzlich den Grund „unzulässiger Gebrauch von elektronischen Kommunikationssystemen“, der nicht in Art. 13 Abs. 1 der RL 95/46/EG aufgezählt ist. Andersherum ist in Art. 13 Abs. 1 der Richtlinie 95/46/EG u.a. in Ziff. g) noch aufgeführt: „Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen“.

Wie bereits auch der EuGH in seinem Urteil *Promusicae*[67] festgestellt hat, betreffen die in Art. 15 Abs. 1 der Richtlinie 2002/58/EG genannten Ausnahmen nur spezifische Tätigkeiten der Staaten oder staatlichen Stellen, die nichts mit den Tätigkeitsbereichen von Einzelpersonen zu tun haben.[68] Der Erlass einer Rechtsvorschrift zur Speicherung von Daten zum Zwecke der Verfolgung von Urheberrechtsverletzungen durch die Rechteinhaber könnte demnach nicht auf Grundlage des Art. 15 Abs. 1 der Richtlinie 2002/58/EG erfolgen.

Zugleich hat der EuGH im Urteil *Promusicae* aber entschieden, dass die in Art. 15 Abs. 1 der RL 2002/58/EG genannte Aufzählung durch den Verweis auf Art. 13 Abs. 1 der RL 95/46/EG nicht abschließend ist und die Mitgliedstaaten auf Grundlage von Art. 15 Abs. 1 der RL 2002/58/EG auch Rechtsvorschriften erlassen können, die die Pflicht zur Wahrung der Vertraulichkeit personenbezogener Daten beschränken, sofern diese Beschränkung u.a. für den Schutz der Rechte und Freiheiten anderer Personen notwendig ist. Dazu hat der EuGH weiter ausgeführt:

> „Da diese Bestimmungen des Art. 15 Abs. 1 der Richtlinie 2002/58/EG die betreffenden Rechte und Freiheiten nicht benennen, sind sie dahin auszulegen, dass sie den Willen des Gemeinschaftsgesetzgebers zum Ausdruck bringen, weder das Eigentumsrecht noch Situationen von ihrem Anwendungsbereich auszuschließen, in denen sich die Urheber im Rahmen eines zivilrechtlichen Verfahrens um diesen Schutz bemühen.“[69]

[67] EuGH, Urteil v. 29.1.2008 – C-275/06.

[68] EuGH, Urteil v. 29.1.2008 – C-275/06 Rz. 51.

[69] EuGH, Urteil v. 29.1.2008 – C-275/06 Rz. 53.

Mit dem EuGH könnte demnach auch der Erlass einer Rechtsvorschrift zur Verfolgung von Urheberrechtsverletzungen durch die Rechteinhaber unter den nachstehenden Voraussetzungen auf Art. 15 Abs. 1 der RL 2002/58/EG gestützt werden.

- Die Speicherung muss in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sein.

- Die Speicherung darf nur für eine begrenzte Zeit erfolgen (Art. 15 Abs. 1 S. 2).

- Die Speicherung muss den allgemeinen Grundsätzen des Gemeinschaftsrechts, einschließlich den in Art. 6 Abs. 1 und 2 EUV niedergelegten Grundsätzen, entsprechen.

2. Vorratsdatenspeicherungsrichtlinie 2006/24/EG

Von der sich aus Art. 15 Abs. 1 der Richtlinie 2002/58/EG ergebenden Möglichkeit hatten nach Erlass der Richtlinie einige Mitgliedstaaten Gebrauch gemacht und Rechtsvorschriften zur Aufbewahrung von Verkehrsdaten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen, wobei diese nationalen Vorschriften sich jedoch erheblich unterschieden.[70]

Diese Unterschiede führten nach Ansicht der EU zu einer Beeinträchtigung des Binnenmarkts für elektronische Kommunikation.[71] Die Vorschriften der Vorratsdatenspeicherungsrichtlinie sollten entsprechend sicherstellen, dass die für die Ermittlung, Feststellung und Verfolgung von Straftaten bedeutenden Verkehrs- und Standortdaten von den Kommunikationsdiensteanbietern und Kommunikationsnetzbetreibern unter bestimmten Bedingungen auf Vorrat gespeichert werden müssen (vgl. Art. 1 Abs. 1 der RL 2006/24/EG).

Art. 3 der Richtlinie 2006/24/EG normiert entsprechend eine Vorratsspeicherungspflicht. Nach dessen Abs. 1 müssen die Mitgliedstaaten dafür Sorge tragen, dass die in Art. 5 genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, auf Vorrat gespeichert werden.

Betreffend den Internetzugang müssen entsprechend Art. 5 der Richtlinie 2006/24/EG folgende Daten auf Vorrat gespeichert werden:

- Zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten: der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine IP-Adresse zum Zeitpunkt der Nachricht zugewiesen war.

- Zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten: Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder registrierten Benutzers.

[70] Erwägungsgrund Nr. 5 der Richtlinie 2006/24/EG.

[71] Erwägungsgrund Nr. 6 der Richtlinie 2006/24/EG.

- Zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten: die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss, der digitale Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs.

Nach Abs. 2 der Richtlinie dürfen Daten, die Aufschluss über den Inhalt der Kommunikation geben, nicht auf Vorrat gespeichert werden.

Nach Art. 6 der Richtlinie 2006/24/EG müssen die nach dieser Richtlinie auf Vorrat gespeicherten Daten mindestens sechs aber höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert werden. Die nach Art. 3 auf Vorrat gespeicherten Daten dürfen nach Art. 4 der Richtlinie 2006/24/EG nur in bestimmten Fällen und in Übereinstimmung mit dem jeweiligen innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Somit dürfen die von den Zugangsanbietern auf Grundlage der Vorratsdatenspeicherungsrichtlinie gespeicherten Daten bereits nur an Behörden und nicht an die privaten Rechteinhaber weitergegeben werden.

Dementsprechend beschränkt sich die Vorratsdatenspeicherungspflicht nach der Richtlinie 2006/24/EG auf die Speicherung von Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Weitergabe an Behörden. Eine Rechtsvorschrift, die die Zugangsanbieter zur Speicherung der Daten zum Zwecke der Verfolgung von Urheberrechtsverletzungen durch die Rechteinhaber verpflichtet, könnte demnach nicht auf Grundlage der Vorratsdatenspeicherungsrichtlinie erlassen werden.

Fraglich ist, ob die Vorratsdatenspeicherungsrichtlinie nur selbst eine Datenspeicherung zu privatrechtlichen Zwecken nicht erlaubt oder diese sogar generell verbietet. Denn soweit eine Richtlinie einen bestimmten Anwendungsbereich reglementiert, ist den Mitgliedstaaten der Erlass entgegenstehender Rechtsvorschriften verwehrt. Wie weit der Anwendungsbereich der Vorratsdatenspeicherungsrichtlinie tatsächlich reicht und inwieweit die Mitgliedstaaten andere Speicherverpflichtungen regeln dürfen, war Gegenstand des erst kürzlich ergangenen Urteils „Bonnier Audio“ [72] des EuGH. In dem Verfahren ging es um die Frage, ob die Vorratsdatenspeicherungsrichtlinie 2006/24/EG, insbesondere ihre Art. 3 bis 5 und 11, der Anwendung einer nationalen Vorschrift entgegensteht, die die Weitergabe von Daten in einem Zivilverfahren zur Feststellung einer Urheberrechtsverletzung erlaubt.

Der EuGH hat hierzu ausgeführt, dass die Richtlinie 2006/24/EG ausschließlich die Verarbeitung und Vorratsspeicherung von Daten betreffe, die von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten erzeugt oder verarbeitet werden, sowie ihre Weitergabe an nationale Behörden. Der so festgelegte Anwendungsbereich der Vorratsspeicherungsrichtlinie werde durch ihren Art. 11 bestätigt, nach dem Art. 15 Abs. 1 der RL 2002/58/EG nicht für Daten gelte, die ausdrücklich zu den in Art. 1 Abs. 1 der Vorratsdatenspeicherungsrichtlinie aufgeführten Zwecken auf Vorrat gespeichert werden. Hingegen gelte Art. 15 Abs. 1 der RL 2002/58/EG nach Erwägungsgrund Nr. 12 der Vorratsdatenspeicherungsrichtlinie weiterhin für Daten, die zu anderen als den ausdrücklich in Art. 1 Abs. 1 der Vorratsdatenspeicherungsrichtlinie genannten Zwecken auf Vorrat gespeichert werden.[73]

[72] EuGH, Urteil v. 19.04.2012 – C – 461/10.

[73] EuGH, Urteil v. 19.04.2012 – C – 461/10, Rz. 42 ff.

Mit dem EuGH regelt die Vorratsdatenspeicherungsrichtlinie somit gerade nicht sämtliche Speicherpflichten bezüglich der elektronischen Kommunikation abschließend, sondern beschränkt sich dabei auf den Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten und die Weitergabe an die zuständigen nationalen Behörden, so dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG weiterhin für Daten anwendbar bleibt, die nicht zu diesen Zwecken gespeichert werden. Eine Rechtsvorschrift, die die Speicherung von Daten auf Vorrat zum Zwecke der Verfolgung von Urheberrechtsverletzungen durch die Rechteinhaber vorsieht, verfolgt einen anderen Zweck, als die Vorratsdatenspeicherung nach der Richtlinie 2006/24/EG.

Unter den oben genannten Voraussetzungen[74] können die Mitgliedstaaten demnach nach Art. 15 Abs. 1 der Richtlinie 2002/58/EG Rechtsvorschriften erlassen, nach denen die Verkehrsdaten länger als nach der Richtlinie 2002/58/EG grundsätzlich vorgesehen, aufzubewahren sind.

9) Welche Konsequenzen ergeben sich für das „vorgerichtliche Warnhinweismodell" aus der Entscheidung des Bundesverfassungsgerichtes vom 24. Januar 2012 (1 BvR 1299/05), in der die Zuordnung von dynamischen IP-Adressen ausdrücklich als ein Eingriff in Art. 10 Abs. 1 GG festgestellt wurde?

Das Bundesverfassungsgericht entschied, dass § 113 Abs. 1 S. 1 TKG verfassungskonform so auszulegen ist, dass die Vorschrift nicht zu einer Zuordnung von dynamischen IP-Adressen berechtigt. Die identifizierende Zuordnung von dynamischen IP-Adressen stelle einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG dar. Denn die Zuordnung zur anschließenden Auskunftserteilung erfordere eine Auswertung der gespeicherten Verkehrsdaten. Eine solche Befugnis müsse hinreichend normenklar geregelt werden. Diesen Anforderungen genüge § 113 Abs. 1 S. 1 TKG nicht. Das Bundesverfassungsgericht stellt hierzu klar:

> „Insoweit bedarf es einer hinreichend klaren Entscheidung des Gesetzgebers, ob und unter welchen Voraussetzungen eine solche Identifizierung erlaubt werden soll." (BVerfG, Beschluss v. 24.01.2012 – 1 BvR 1299/05, Rn. 174).

Das vorgerichtliche Mitwirkungsmodell erfordert nicht die Herausgabe von Verbindungsdaten oder die Auswertung solcher als Vorfrage für eine Auskunftserteilung an staatliche Stellen, wie in dem der Entscheidung zugrundeliegenden Fall. Es erfordert aber die Zuordnung einer dynamischen IP-Adresse und damit die Deanonymisierung eines Kommunikationsvorgangs innerhalb des Telekommunikationsunternehmens. Der Deanonymisierung bedarf es zur Versendung des Warnhinweises. Die IP-Adresse und die Metadaten zu einer Rechtsverletzung werden durch die Rechteinhaber gemeldet. Das Telekommunikationsunternehmen muss daraufhin ungeprüft einen Warnhinweis an den entsprechenden Anschlussinhaber versenden. Zu diesem Zwecke bedarf es der Zuordnung der IP-Adresse zu dem Anschlussinhaber, der sie zu dem Zeitpunkt des infrage stehenden Kommunikationsvorgangs verwendet hat. Wegen § 88 TKG gilt des Fernmeldegeheimnis auch im Verhältnis von Telekommunikationsunternehmen zu ihren Kunden. Ein Eingriff läge somit auch hier vor. Das Bundesverfassungsgericht hat aber einen solchen Eingriff nicht als grundsätzlich unzulässig erklärt. Vielmehr hat es Anforderungen für eine gesetzliche Regelung aufgestellt. Eine derartige Befugnis müsste dementsprechend hinreichend normenklar sein und die Voraussetzungen nennen, unter denen die Zuordnung einer dynamischen IP-Adresse zulässig sein soll. Das Zitiergebot des Art. 19 Abs. 1 S. 2 GG ist zu beachten.

[74] Siehe oben bei 2002/58/EG.

10) Sind sie der Auffassung, dass ein Warnhinweis- oder vorgerichtliches Mitwirkungsmodell als eine Kooperationsmöglichkeit anzusehen ist, die der Verpflichtung im ACTA-Abkommen entspricht, Kooperationsbemühungen im Wirtschaftsleben zu fördern, die darauf gerichtet sind, Verstöße gegen Marken, Urheberrechte oder verwandte Schutzrechte wirksam zu bekämpfen?

Gem. Art. 27 Abs. 3 ACTA ist jede Vertragspartei bestrebt, Kooperationsbemühungen im Wirtschaftsleben zu fördern, die darauf gerichtet sind, Verstöße gegen Marken, Urheberrechte oder verwandte Schutzrechte wirksam zu bekämpfen und gleichzeitig den rechtmäßigen Wettbewerb und – in Übereinstimmung mit den Rechtsvorschriften der jeweiligen Vertragspartei – Grundsätze wie freie Meinungsäußerung, faire Gerichtsverfahren und Schutz der Privatsphäre zu beachten. Die notwendige Kooperation zwischen Zugangsanbietern und Rechteinhabern im Rahmen eines Warnhinweismodells ist eine solche Kooperationsmöglichkeit entsprechend ACTA.

11) Können ihrer Meinung nach bereits heute Warnhinweise anstelle kostenintensiver Abmahnungen verschickt werden? Bedarf es hierfür einer zusätzlichen Inpflichtnahme der Internetzugangsanbieter?

Schon nach geltender Rechtslage könnten die Rechteinhaber anstatt einer Abmahnung zunächst einen sanktionslosen Warnhinweis versenden. Diese Alternative weist aber eine Anzahl von Nachteilen gegenüber der Warnhinweisversendung durch die Zugangsanbieter auf. Hierzu ausführlich bereits unter Frage 1) B.I.

12) Das BMWi- Gutachten spricht davon, dass "die Effizienz von Warnhinweisen in den Referenzstaaten nicht zur vollen Überzeugung nachgewiesen ist". Aus welchem Grund sollte dann ein Warnhinweismodell zur Vorbereitung eines Auskunftsanspruchs geschaffen werden und welche Sanktionen fordern die Verbände der Unterhaltungsindustrie für illegale Nutzungen jenseits von Peer-to-Peer, die ebenfalls nicht durch das im Gutachten vorgeschlagene "vorgerichtliche Warnhinweismodell“ erfasst würden?

Der Begriff der „vollen Überzeugung“ ist ein juristischer Terminus aus dem Prozessrecht und meint die Gewissheit, dass eine bestimmte Tatsache wahr ist. Zu einem solchen Ergebnis konnte die Studie allerdings aufgrund der Ausgangssituation gar nicht gelangen. Zur Bewertung der Effizienz von Warnhinweisen diente als einziger Referenzstaat Frankreich. Dort war das Warnhinweismodell noch nicht so lange in Kraft, dass auf verschiedene verlässliche Studien zu den Auswirkungen zugegriffen werden konnte.

Indes bestehen verschiedene Anhaltspunkte für die Effizienz der Warnhinweisversendung. Ein deutliches Anzeichen ist, dass in Frankreich die Versendung erster Warnhinweise bereits zu einem relevanten Rückgang rechtswidrigen Verhaltens im Internet geführt hat. So heißt es in der BMWi-Studie auf:

> „Eine vergleichbare Frage wurde in einer im Auftrag der Hadopi im Frühjahr 2011, also mehr als ein Jahr später, durchgeführten Untersuchung gestellt, in deren Rahmen 1.500 Internetnutzer einbezogen waren.[75] Von den Befragten erklärten **sieben Prozent**, dass sie

[75] *Hadopi*, biens culturels et usages d’internet: pratiques et perceptions des internautes français, 2ème vague barométrique (Zweite Untersuchung der Hadopi, vorgelegt am 18.5.2011), abrufbar unter: http://www.hadopi.fr/sites/default/files/page/pdf/t1_etude_longue.pdf.

selbst, eine Person aus ihrem Haushalt oder jemand aus ihrem näheren Umfeld bereits einen **Warnhinweis von der Hadopi erhalten** hätten.[76] Von diesen Internetnutzern gab die **Hälfte** an, seitdem **keine illegale Nutzung** von Inhalten im Internet mehr zu tätigen, und weitere 22 Prozent, die illegale Nutzung zumindest eingeschränkt zu haben. Ein Viertel gab sich unbeeindruckt.[77]"

Und weiter in Bezug auf Frankreich:

„Nach Daten der IFPI ist die Peer-to-Peer-Nutzung in Frankreich im Zeitraum zwischen April 2010 und April 2011 um insgesamt **31 Prozent** gesunken mit einem deutlichen Einbruch zum Zeitpunkt der Versendung der ersten Warnhinweise.[78]"

Sodann auf S. 211 der BMWi-Studie:

„Nach Daten der IFPI hat der generelle Anstieg der Internetaktivität keine Entsprechung gefunden in der Nutzung unlizenzierter Dienste im Internet. Trotz einer Steigerung der Internetaktivität im Zeitraum von April 2010 bis April 2011 um zehn Prozent sei eine Verringerung des Zugriffs auf unlizenzierte Angebote um sieben Prozent zu verzeichnen gewesen: Während im April 2010 etwa 24 Prozent der Internetnutzer unlizenzierte Angebote konsumiert hätten, seien es im April 2011 rund 20 Prozent gewesen. Seit Beginn der Versendung der ersten Warnhinweise sei die Nutzung um zwölf Prozent zurückgegangen.[79]

Weitere wesentliche Aspekte für die Effizienz sind in der Studie dargestellt:

„Erhebungen aus Schweden zeigen, dass sich im Bereich Musik, das Nutzerverhalten und auch der Umsatz mit digitalem Content unmittelbar in Richtung legaler Angebote ändern, wenn Nutzer mit einer Rechtsfolge rechnen müssen. Sobald eine Rechtsverfolgung nicht mehr droht, findet teilweise wieder eine Abkehr von der Legalität statt, wobei da, wo legale Substitute zu den Piraterieangeboten existierten, die Abkehr von der Illegalität dauerhaft war. Die Betrachtungen der verschiedenen Länder führen jedenfalls nicht zu dem Ergebnis, dass die Maßnahmen ineffizient seien. Eine aktuelle Studie aus den USA kommt für das Warnhinweismodell in Frankreich zu dem Ergebnis, dass die Kombination aus Sanktionsandrohung, Medienaufmerksamkeit und Aufklärung über die Rechtswidrigkeit von Filesharing sowie der Hinweis auf legale Alternativen den Nutzern den Weg in die Legalität geöffnet hat. So kam es in Frankreich schon in Ansehung der Einführung des Warnhinweissystems zu einer Umsatzsteigerung bei den Musikverkäufen über die Online Vertriebsplattform iTunes." [80]

Nicht zu unterschätzen ist die durch die Warnhinweisversendung erzielbare Aufklärung der Nutzer bei der Einordnung von Angeboten und die Funktion der Aufklärungsarbeit. Weiter heißt es dazu:

„Unabhängig von jeder gezielten Einwirkung auf die Nutzer und deren Verhaltensschemen kann Aufklärung dazu beitragen, die offenbar nicht immer klar umrissenen rechtlichen Rahmenbedingungen und die Konsequenzen rechtswidrigen Handelns zu vermitteln. Die vorliegenden Daten zeigen, dass einerseits ein Bedürfnis besteht, dem Nutzer die Un-

[76] *Hadopi*, 2ème vague barométrique, a.a.O., Folie 27.

[77] S. 210; zwei Prozent gaben an, dass Internet noch verstärkt für die illegale Nutzung von Werken zu nutzen. *Hadopi*, 2ème vague barométrique, a.a.O., Folien 26, 28.

[78] *IFPI*, Measuring the Impact of Graduate Response, July 2011, S. 2.

[79] *IFPI*, Measuring the Impact of Graduate Response, July 2011, S. 2.

[80] BMWi-Studie, S. 334.

terscheidung von legalen und illegalen Angeboten zu vereinfachen. Dazu können Kennzeichnungen legaler Angebote beitragen. Es zeigt sich aber, dass die Handlungsmöglichkeiten des aktiven Internetnutzers nicht immer der rechtlich richtigen Bewertung zugeordnet werden. Auch hier besteht Aufklärungsbedarf. Kenntnis der Rechtslage, der zu erwartender Folgen bzw. Sanktionen des Handelns sowie Auswirkungen des eigenen Handelns auf Dritte und die Allgemeinheit setzen dabei im Rahmen der Aufklärung unterschiedliche Impulse, indem sie Rechtskenntnis, Unrechtsbewusstsein und Gerechtigkeitsempfinden fördern. Jedenfalls können durch Aufklärung Sachverhalte vermieden werden, die nach derzeitiger Rechtslage als ungerecht empfunden werden. Ein Warnhinweissystem kann verhindern, dass ein Rechtsverletzer in Unkenntnis der rechtlichen Konsequenzen sanktioniert wird, wenn er etwa Peer-to-Peer-Filesharing zum ersten Mal durchführt. Dies gilt auch für den in Anspruch genommenen Anschlussinhaber, dem die über seinen Anschluss begangenen Rechtsverletzungen unbekannt sind."[81]

[81] BMWi-Studie, S. 335.

Teil 2: Neue Geschäftsmodelle

Für alle Branchen:

1) Wie entwickelte sich der Umsatz in den Branchen Musik, Film und Buch in den letzten fünf Jahren hinsichtlich der verschiedenen Speichermedien? Bitte stellen Sie insbesondere die Entwicklungen in den letzten zwei Jahren dar.

2) Allein 70 lizenzierte Plattformen bestehen in der Musikindustrie (Quelle: Digital Music Report 2011). Welche neuen Geschäftsmodelle haben sich in den Branchen Musik, Film und Buch in den letzten Jahren entwickelt? Welche Marktchancen sehen Sie für weitere Geschäftsmodelle? Welche Geschäftsmodelle werden sich aus Ihrer Sicht besonders positiv entwickeln?

3) Welchen Schwierigkeiten und Hemmnissen sehen Sie sich bei neuen Geschäftsmodellen ausgesetzt?

4) Welche Hinweise wurden von Nutzerseite an Sie herangetragen hinsichtlich Hemmungen bei der Nutzung legaler Portale? Werden von Nutzern eher wirtschaftliche Gründe (zu hoch empfundene Preise) oder eher technische Gründe (schlechte Bedienbarkeit der Portale; fehlende Kompatibilität/eingeschränkte Nutzbarkeit der erworbenen Medien/Dateien) genannt, sich (noch) nicht für eine (stärkere) Nutzung legaler Portale zu entscheiden?

5) Welche wirtschaftlichen und rechtlichen Rahmenbedingungen müssen für Sie vorliegen oder verbessert werden, damit Sie in neue Techniken und/oder neue Dienste investieren?

Für die Branche Musik:

6) Laut aktuellen Zahlen der Brenner-Studie (Quelle: Musik im digitalen Wandel. Eine Bilanz aus zehn Jahren Brenner Studie) hat sich die Anzahl der verfügbaren legalen Musikdienste von 2006 bis 2011 mehr als verdreifacht, der Umsatz beim digitalen Musikverkauf hat sich von 82 Millionen im Jahr 2006 auf 204 Millionen Euro Umsatz im Jahr 2010 gesteigert. Wie wird sich dieser Markt in den kommenden Jahren weiter entwickeln? Wie reagieren Sie auf diese Veränderungen?

7) Vor dem Hintergrund, dass die Umsätze im digitalen Musikverkauf in den vergangenen Jahren kontinuierlich gestiegen sind, laut Brenner-Studie (Quelle: Musik im digitalen Wandel. Eine Bilanz aus zehn Jahren Brenner Studie), BVMI) die Anzahl der Nutzer illegaler Downloads zwischen 2004 und 2010 jedoch mit rund 3 Mio. Nutzern stabil geblieben ist, welche Vor- und Nachteile sehen Sie bei der Einführung eines Warnhinweismodells für die Entwicklung der Umsätze bei legalen digitalen Musikinhalten?

8) Wie hoch sind die Kosten für die Produktion eines Musikwerkes im Verhältnis zum Vertrieb – analog bzw. digital? Wie groß ist also die „digitale Dividende“?

9) Wie groß ist der Schaden durch One-Click-Hoster wie Rapidshare? Wie sehr behindern solche Dienste die Etablierung legaler Download- und Streaming-Dienste? Wie können Urheber-

rechtsverletzungen auf solchen Plattformen am schnellsten und nachhaltigsten verhindert werden?

Für die Branche Buch:

10) Welche Potentiale sehen Sie im Ausbau einheitlicher technischer Standards (angesichts der vielen unterschiedlichen Formate von Readern und Software)?

11) Wie hoch ist der Anteil an eBooks an allen Buchveröffentlichungen? Wie ist das Verhältnis in den verschiedenen Bereichen, wie z.B. Wissenschaftsliteratur, Sachbuch oder Belletristik?

12) Gibt es auch DRM-, Streaming- oder Cloud-Angebote?

Für die Branche Film:

13) Welche legalen Angebote existieren? Wo sehen Sie hier die Zukunft? Welche Nutzerstudien existieren?

14) Welche Nutzungsbedingungen sind für den Dienst „Ultraviolet“ bei seinem Markteintritt in Deutschland geplant? Welche Erfahrungen gibt es in den USA?

15) Funktionieren Cloud- und Streamingdienste auch ohne DRM?